DRAFT v.5

NRI-6 (2010)

3CA

FORM C
GRAPHICAL

Control Change Cause Analysis

Investigator's Manual

Produced by

The Noordwijk Risk Initiative Foundation

In partnership with

The Health and Safety Executive

DRAFT v.5

Published and distributed by:

The Noordwijk Risk Initiative Foundation
P.O. Box 286,
2600 AG Delft,
The Netherlands.

Email: Info@nri.eu.com
Website: www.nri.eu.com

ISBN

DRAFT v.5

3CA
Control Change
Cause Analysis

Form C

June 2010

Authors: J. Kingston, F. Koornneef, R. Frei
and P. Schallier
The Noordwijk Risk Initiative Foundation,
P.O. Box 286, 2600 AG Delft, Netherlands.
www.nri.eu.com

[This page is intentionally left blank]

Preface

The Noordwijk Risk Initiative was founded to promote sharing of knowledge in the field of risk management. Based on the belief that a virtuous circle exists between making tools and developing theoretical understanding, the Foundation develops tools for risk management and maintains them in the public domain.

Purpose of this document

The Noordwijk Risk Initiative Foundation publishes this document to encourage the efficient and effective investigation of incidents. It is intended for line managers and supervisors, as well as specialists in various disciplines such as occupational safety, environmental protection and quality management.

The NRI Foundation intends to maintain this manual in the public domain. Our motivations are:

1. to help decision-makers identify from unwanted events the lessons they need to learn;
2. to provide a reference point for investigators, tool developers, researchers and students.

Status of this manual

3CA was produced to provide supervisors and line managers in industry with an easy-to learn, easy-to-apply method for identifying the underlying causes of accidents and incidents.

3CA now comes in three versions, Forms A, B and C. The manual for the A-form of 3CA was produced in 2002 following a co-operative project run in 2000 by Humber Chemical Focus and the UK Health & Safety Executive (HSE). The manual for the A-form is available at www.nri.eu.com/NRI3.pdf.

In 2008, the NRI Foundation and HSE worked in partnership to produce the B-form of 3CA. Initially, this project aimed at revising the original 2002 manual. However, the revision process produced sufficient changes in the method itself for the result to be considered as something new. This is the origin of the B-form of 3CA. The manual for the B-form is available at www.nri.eu.com/NRI5.pdf.

In 2009/10, the NRI Foundation developed a graphical worksheet to support the B-form of 3CA. This was written-up (a worksheet and a procedure) as an appendix to the B-form manual. However, as the graphical approach is for some users the main way of applying 3CA routines, the authors decided to produce a dedicated manual – the C-form of 3CA.

Acknowledgements

The C-form of 3CA is based closely on the B-form to which many people contributed. Our particular thanks go to the project workers at the UK Health and Safety Executive, Dr Celeste Jacinto (New University of Lisbon, Portugal), and; Dr Mark Cooper (European Institute of Health Studies, Surrey University).

[This page is intentionally left blank]

Forward

3CA began in 2000 as a method to help first-line supervisors in the UK Chemical Industry. The aim was to make a tool that helped supervisors to analyse root causes of incidents. They wanted a tool that was quick to learn and that helped them produce insightful and useful findings quickly. The result is still available, albeit slightly refined and now called "Form A".

Eight years later, NRI published a new version of 3CA (Form B). This time, we had safety professionals in mind, but still wanted a method that could be used by others. We took the opportunity to make the process more thorough and less prone to judgmentalism. The new form prompts the user to see things from the point of view of the individuals involved. 3CA also cues the user to think about how the wider culture may have influenced the decisions of those individuals. These insights set the scene for evaluating the system of management controls.

The other innovation was to help the analyst to avoid certain problems associated with "counterfactual reasoning". This type of reasoning is not bad as such, in fact it is essential, but it is easily biased. Looking at someone else's choices in the cold light of day, from your own perspective, and with the benefit of knowing how those choices turned out, is difficult to do fairly and thoroughly. It is especially easy to focus on what the person did not do. One problem with the "did not" type of explanation is that it is biased towards reinforcing rules. Often there is more to an accident than disobedience. Moreover, a preoccupation with what people did not do can block gaining insights that come from examining what they actually did. 3CA analysis is designed to help the analyst to understand why an accident happened even though relevant rules existed.

In training situations, we saw that people could use 3CA to produce insightful analysis and good questions. However, in practice, many would-be analysts found the tabular worksheet got in the way. For some, it imposed a "form filling" mentality; an inflexible, linear approach which stemmed the flow of their creative, analytical thought.

The solution to this problem emerged during a training session. When training new users, I explain the concepts of 3CA using a set of graphics. "Why…" suggested one such user in early 2009, "don't you create a worksheet around those graphics"? After a Homer Simpson, "D'oh!" moment of realisation, the trainers set about testing the idea. After nine months and trials involving some 200 users, we decided the format for the new worksheet and added it as an appendix to the Form-B, 3CA manual.

This new graphical format, unlike its tabular cousin, invites users to move back and forth between the various headings. In this way, analysts explore the issues using 3CA routines as guidelines and the 3CA worksheet as a notepad. Another advantage seems to be that people who have not been involved in the investigation and who don't know 3CA can intuitively follow the information recorded on a 3CA worksheet. So you might find it useful as a briefing tool, as well.

We hope you find this new approach to 3CA simple and helpful. Let us know how you get on and how 3CA can be improved. If you find 3CA useful, perhaps you might consider making a donation to the NRI Foundation: we are a not for profit organisation and every little helps.

John Kingston, 12th June 2010.
Noordwijk Risk Initiative Foundation

[This page is intentionally left blank]

Analysing incidents using 3CA

3CA analysis is designed to help you to:

- *thoroughly examine a significant event from a number of perspectives;*
- *record your thinking, insights and questions.*

Using 3CA is an iterative process. As you analyse the facts, questions will emerge. You will need to revise your analysis in the light of the answers. For these reasons, do not expect to complete the analysis at one sitting.

It's best to start the analysis as soon as you know the basic facts about what happened. You are more likely to find answers early on in the investigation than later.

1 Before you start the analysis

You will need to make sure that you have everything in place to make the process efficient. This means having the right people involved, a suitable place to work and the right equipment; these are discussed below. You also need to budget enough time. 3CA is not a heavy tool, but even so, each significant event will take about 30-60 minutes to analyse. It is usual to analyse two, or sometimes, three significant events, each on a separate graphical worksheet. So a half-day is realistic when breaks and other interruptions are taken into account. Bear in mind that you might want to spend some more time later on revising your analyses in the light of new information.

1.1 Team Requirements

Analysis is about applying knowledge to facts. You need to make sure that you have knowledge of the:

- technical standards that apply to the activity under investigation;
- procedures and policies of the organisations(s) involved in the incident;
- structure of the organisation, its culture and management systems;
- 3CA procedure.

One person generally can't cover all these bases and so you will need to put together a team. A team approach also helps to explore the issues through discussion and it will often improve the quality of the analysis.

A team approach is often effective but needs to be managed to ensure efficiency. Try to balance airing ideas with making progress. In particular, note down questions on the worksheet. This captures good ideas without getting bogged down in speculation.

Even when addressing issues systematically, it is possible to miss points or make unwarranted assumptions. So, consider having the analysis challenged by a 'critical friend'.

1.2 Physical Requirements

3CA analysis doesn't require anything unusual, but try to ensure that you have:

- arranged a room with suitable security where you can work undisturbed and without disturbing others;
- documents on hand for ready reference (e.g. witness statements, reports, diagrams and photographs etc.).
- 3CA worksheets (use complete sentences)
  - If working with pen and paper, use A3 sized copies of the 3CA worksheet[1]. Colour is not essential, but might help;
  - If working via a computer[2], a suitable (e.g. quiet, bright, high resolution) data projector can help team work;

It is VITAL to make notes during the discussion, otherwise you'll forget points. The 3CA worksheet is designed for this purpose.

Write in complete sentences, that way others will be able to understand your analysis and you'll be able to reconstruct your reasoning when reporting your findings.

Remember to note-down questions as well as facts.

1.3 Information about the accident

Start the 3CA process as soon as you have the basic facts about what happened. It is useful, though not essential, to have applied a systematic sequencing method before starting 3CA. Sequencing methods like STEP and ECFA+ help to describe actions, identify actors and to identify any gaps in the factual picture of what happened.

2 Choose subjects to analyse

Your investigation may require several 3CA analyses, one for each significant event that you decide to include. Starting with the highest priority, analyse one significant event following the steps described below. Repeat the process for any other significant events that require analysis, each on a different graphical worksheet.

A significant event is one that significantly increases risks or decrease control, or both. **Identify all the significant events in the accident sequence.** Be careful not to miss events that are not yet obvious; the sequencing methods mentioned earlier are one way of support this.

Choose which significant event to analyse first. One way is to order the whole set in one go and then to work your way through the list. This allows you to work-out how much time will be needed for the whole set of analyses. Another way is to choose the most significant event, analyse it, and then repeat the selection process to choose the next significant event that you think warrants analysis.

[1] Blank forms can be downloaded from NRI
[2] Use the word-processing template available from NRI.

It is difficult to be precise about the criteria for prioritising significant events, but the box below gives examples found from practice. The effect should be to put effort into events that you believe hold the most potential for learning.

Criteria for prioritising events for analysis

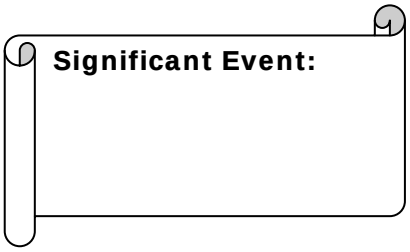
- *the size of the change in risk or control created by the event;*
- *the extent of risk reduction achievable by the expected way of working;*
- *the currency and importance in other settings of the expected way of working;*
- *the potential for identifying valuable lessons to be learned;*
- *the extent to which the investigators are surprised by the facts of the event.*

3 Describe the significant event

3CA analysis has two parts, the first part is *descriptive*. 3CA analysis uses a method of "contrasting statements": a statement of what actually happened is contrasted with a statement of what is expected to happen. The second part of the analysis flows from trying to *explain* why the actual situation was different from what was expected.

3.1 State the Significant Event

In the scroll-shaped box on the worksheet, describe the significant event. State what or who is acting (e.g. the person or machine) and what was done.



3.2 Describe the Actual Performance

In the relevant box, describe what the actor actually did. Phrase your description to include the actor and the action. Make this a simple, positive statement. If you have used ECFA+, use the phrase from the ECFA+ event.

Often this description starts out worded exactly as it appears in the "significant event" scroll box. As your analysis goes on, you may recognise other contextual facts to be important. These extra details should be added to the description. Actual Performance can include facts about the situation, not just facts about behaviour. The aim is to provide an accurate and meaningful snapshot of the event you are analysing.

It is **very important to avoid** statements of the type 'did not', 'failed to', etc. These statements:

- discourage investigators to look into why people acted as they did;
- over-emphasise individual responsibility;
- under-emphasise the relevance of context.

3.3 Describe the Expected Performance

The significant event will contain an actor and an action; focus on the action: **in the relevant box, describe what performance was expected**.

There may be one or more alternative expectations; **write down every option** that can be justified.

You will have two types of expected performance:

- 'Prescribed' options that are normal requirements; those that 'should' have been in place according to some regulation or procedure.
- 'Non-prescribed' options that are not obligatory but which nonetheless might be justified in the context in which the accident occurred.

To help you identify 'non-prescribed' options, take a 'first principles' approach[3]. Develop a list of possible options, and then crop it down to only those options that you can justify.

If the significant event is describing a moment in which harm or injury occurs (or is a near miss) you could use the list below to identify non-prescribed options:

1. *Do not use…*
2. *Use less of…*
3. *Use safer form of…*
4. *Prevent build-up of (or divert)…*
5. *Barrier on…*
6. *Barrier between…*
7. *Separate in time or space.*
8. *Use stronger…*
9. *Evasion by…*
10. *Less people exposed*
11. *Use less valuable thing…*

3.4 State the Standard/Benchmark that justifies the expectation

Refer to a specific standard, code, procedure or documented good practice that justifies each statement of expected performance. This is to ensure that only legitimate comparisons are made between actual and expected performance.

If relying on a general code or standard, you should also explain how this relates to the specific context of the significant event. As well as providing a defendable basis for your analysis, this may also deepen your insight into the context of the accident.

What if you are not sure? If you don't know how a general code relates to the specific context of the accident, write this as a question. Similarly, write a question if you believe that an expectation is plausible, but you do not have enough information to evaluate its practicality.

[3] *The list shown is applicable if the significant event is an accident or near-miss. The list is adapted from: Haddon, J. (1973) Energy Damage and the Ten Countermeasure Strategies. Human Factors, 355-366, August 1973*

4 Explain the difference between actual and expected performance

In this part of the analysis, the goal is to explain why the actual performance was different from the expected performance. You need to explain the difference in terms of the individuals involved, the culture and organisation in which they work and management systems:

- Individuals' goals and their knowledge at the time they acted;
- any relevant cultural patterns (e.g. set by individual's peer group) and the influence of organisational factors;
- the systems of control that could have pre-empted, detected and corrected the significant event or its circumstances.

As well as gaining insights under each of these three headings, look for interactions between the headings. For example, if the difference between the expected and actual performance has become established as a cultural pattern, try to explain under the heading of 'systems' why the pattern had become established.

More than one option for Expected Performance?

Consider each option of expected performance singly. This is to avoid the confusion created by explaining the difference between actual performance and two or more options of expected performance simultaneously.

Teamwork may be helpful to the analysis; group discussion naturally makes conversational connections between topics.

4.1 Original Logic

In the relevant box, identify (or pose questions about) why it made sense to the individual to do the job this way.

State whose reasoning is the subject of discussion. Often this is a person named in the significant event. Try to discriminate "original logic" from post-accident rationalisations and alibis.

More than one decision-maker?

Sometimes, the significant event is the outcome of several decisions made by different people. The logic for each decision needs to be considered, as does the context of the decision (i.e. in terms of culture, organisational factors and management system).

A non-human actor (e.g. a machine) acts in the significant event?

Often the 'original logic' to be considered is that of the person who 'acted' in the significant event. But not always. If the actor is a machine or a component, consider the logic of the machine's designer and/or controller.

4.2 Cultural patterns and organisational factors

Normally an actor is influenced by existing attitudes or patterns of behaviour in their peer group.

In the relevant box, describe attitudes or behaviours in the actor's peer group that may have established a pattern for the actual performance.

Describe any organisational factors that may explain his/her individual logic or behaviour. Organisational factors include properties such as management structure, leadership, politics, and change.

4.3 Systems

Identify each system relevant to the significant event. For each system, explain, or ask, why it did not ensure that the actual performance would be the same as the expected performance.

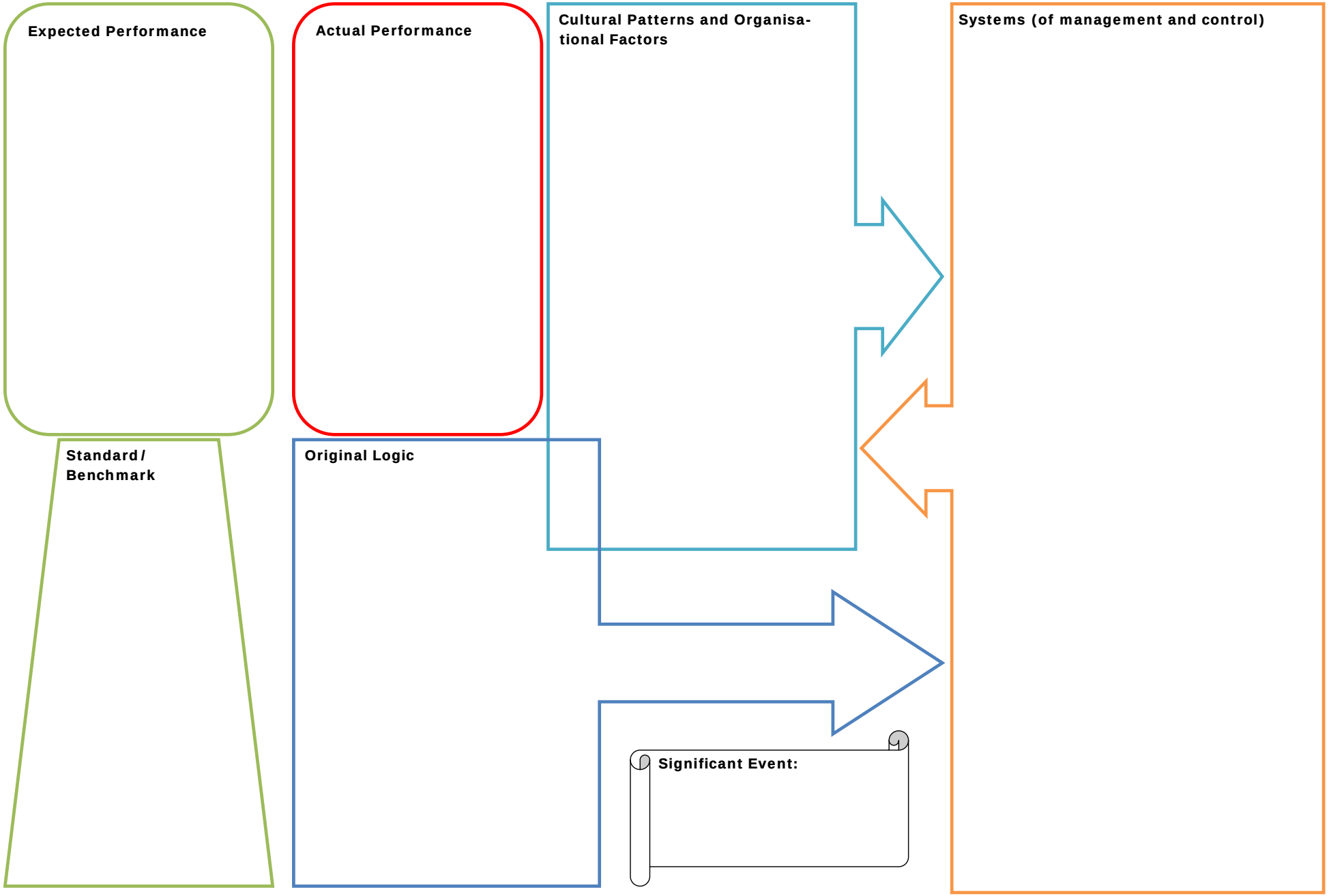
Try to go "a spade deeper" in your explanations. Suppose, for example, that you concluded that the difference between actual and expected performance was due to over-prescriptive procedures. Try also to explain what it is about the system(s) that allowed them to produce this problem. In the example given, you could look into how the procedure was researched, developed, tested and maintained. In this way, you can identify general lessons for the organisation.

An illustrative list of Generic Systems

- *Verifying Readiness before use/start of work*
- *Housekeeping*
- *Briefings and task allocation*
- *Personnel selection*
- *Competence Assurance*
- *Inspection*
- *Maintenance*
- *Motivation*
- *Co-ordination between groups*
- *Supervision*
- *Design of Hardware and premises*
- *Procurement and Supply*
- *Risk Assessment*
- *Procedures & Technical Information*
- *Planning*
- *Budgeting*
- *Monitoring*
- *Change control systems*
- *Emergency systems*
- *Audit and review*

[This page is intentionally left blank]

Appendix 1: Example of Blank Worksheet



Graphical worksheet [paper and pencil version] for use with 3CA (Form C) Manual, available www.nri.eu.com/NRI6.pdf

Appendix 1 (Ready Reference)

Expected Performance

Insert text here (and delete below)

The significant event will contain and actor and an action; focus on the action and describe what performance was expected. Note the basis for this expectation in the "Standard" box.

If there is more than option, describe each of the alternatives.

Write questions if you need to.

Actual Performance

Insert text here (and delete below)

Describe what the actor actually did. Phrase your description to include the actor and the action. Make this a simple, positive statement.

NOTE: Often this description is exactly same as the "significant event", but sometimes it is different.

Cultural Patterns and Organisational Factors

Insert Text here (and delete below)

Describe attitudes or behaviours in the actor's peer group that may explain his/her individual logic or behaviour.

Sometimes an actor's "original logic" is truly unique and without precedent, but normally he or she is influenced by existing attitudes or patterns of behaviour in their peer group.

Describe ORGANISATIONAL factors that may explain his/her individual logic or behaviour. (e.g. management structure, leadership, politics, change).

To help you make a note of your thinking, use COMPLETE SENTENCES. Write questions if you need to.

Systems (of management and control)

Insert text here (and delete below)

Identify each system relevant to the problems noted. For each system, explain why the system did not pre-empt, detect or correct the problems. To help you make a note of your thinking, use COMPLETE SENTENCES. Write questions if you need to.

Systems include:-

- *Verifying Readiness before use/start of work*
- *Housekeeping*
- *Briefings and task allocation*
- *Personnel selection*
- *Competence Assurance*
- *Inspection*
- *Maintenance*
- *Motivation*
- *Co-ordination between groups*
- *Supervision*
- *Design of Hardware and premises*
- *Procurement and Supply*
- *Risk Assessment*
- *Procedures & Technical Information*
- *Planning*
- *Budgeting*
- *Monitoring*
- *Change control systems*
- *Emergency systems*
- *Audit and review*

Standard / Benchmark

Insert text here (and delete below)

Describe your justification for believing that the performance stated in the "expected performance" is reasonable and relevant to the actor's situation. Justification might include reference to a procedure, expert opinion of good-practice, a regulation, or other types of norm. It must be something for which you can provide evidence.

Write questions if you need to.

Original Logic

Insert text here (and delete below)

Describe the perceptions and reasoning of the actor (or the controller or designer, if the actor is a thing). This should explain why the 'actual performance' seemed (to the actor) to be a good course of action.

To help you make a note of your thinking, use COMPLETE SENTENCES.

Write questions if you need to.

Significant Event:

Insert text here (and delete below)
Describe the event; say what is acting (e.g. the person or machine) and what action is being performed.

2 Appendix: Comparison between the 3CA Graphical and Tabular worksheets

The tabular and graphical formats support the 3CA method in different ways, although the underlying logic is the same.

For some people, filling-in a table imposes an inflexible, linear approach and stems the flow of their creative, analytical thought. A graphical format, in contrast, invites users to move back and forth between the various headings and encourages divergent thinking. Also, the graphical worksheet can handle only just one significant event, and this may help users to stay focused. There, NRI has developed a graphical worksheet as a way of improving the usability of 3CA.

2.1 Handling multiple significant events

The tabular format allows several significant events to be seen together, compared and connected to common themes. The graphical format allows only one significant event to be considered at a time. To conduct a full 3CA analysis, which may need to consider several significant events, the user will need several graphical sheets, one for each significant event.

Themes common to two or more significant events

The tabular format allows several significant events to be analysed on the same page. This means that themes common to more than one significant event need be written only once. This is particularly relevant for issues noted by the analyst in columns 5(a) to (c) of the B-form.

The graphical format limits the analyst to considering one significant event on each worksheet. It is possible for the analyst to cross-refer between sheets. If more than one sheet is used, the user will need to develop a system for doing this.

Overview of the full set of significant events

Analysis using 3CA table results in a list of significant events. This constitutes a concise summary of the accident. Users of the graphical format should consider making first a comprehensive "master list" of the significant events.

Prioritisation occurs 'off-the-page'

Using graphical format means that any prioritisation of significant events occurs 'off-the-page'. Whether the analyst is going to consider all the significant events, or just a selection of them, prioritisation still needs to occur in the tabular or graphical format.

2.2 Handling 'Could' and 'Should' Barriers and Controls

In the tabular form of 3CA, the analyst is prompted to consider barriers and controls that could have prevented or mitigated a significant event. This list will include two sorts of options:

1) 'prescribed' options that are normal requirements, those that 'should' have been in place according to some regulation or procedure.
2) 'non-prescribed' options that are not obligatory but which nonetheless might be justified in the context in which the accident occurred.

In the graphical form of the method, identifying 'non-prescribed' options for preventing or mitigating significant events needs to be done 'off-the-page'. In practice, this is done when analysing "expected performance" by taking a 'first-principles' approach.

[This page is intentionally left blank]

DRAFT v.5

NRI Document Improvement Proposal		
1. Document reference NRI-6 Draft v.5	**2. Document date** 25 June 2010	**3. Document title** 3CA Manual, C-Form
4. Recommended improvement *(identify page, paragraph and include modified text or graphic, attach pages as necessary)*		
5. Reason for recommendation		
6. Originator of recommendation		
Name:	Organisation:	
Address:	Phone: Fax: E-mail:	**7. Date of submission**
8. Send to NRI Secretariat		
Name: J.Kingston	***Address:*** Noordwijk Risk Initiative Foundation P.O. Box 286 2600 AG Delft The Netherlands	Phone: +44 (0)121 288 3206 Fax: +44 (0)797 009 1890 email: info@nri.eu.com

DRAFT v.5

IAEA-TECDOC-632

ASSET guidelines

Revised 1991 Edition

Reference material
prepared by the International Atomic Energy Agency
for Assessment of Safety Significant Events Teams

INTERNATIONAL ATOMIC ENERGY AGENCY IAEA

The IAEA does not normally maintain stocks of reports in this series. However, microfiche copies of these reports can be obtained from

INIS Clearinghouse
International Atomic Energy Agency
Wagramerstrasse 5
P.O. Box 100
A-1400 Vienna, Austria

Orders should be accompanied by prepayment of Austrian Schillings 100,— in the form of a cheque or in the form of IAEA microfiche service coupons which may be ordered separately from the INIS Clearinghouse.

ASSET GUIDELINES: REVISED 1991 EDITION
IAEA, VIENNA, 1991
IAEA-TECDOC-632
ISSN 1011–4289

Printed by the IAEA in Austria
December 1991

FOREWORD

The IAEA Assessment of Safety Significant Events Team (ASSET) Service provides advice and assistance to Member States to enhance the overall level of plant safety while dealing with the policy of prevention of incidents at nuclear power plants. The ASSET programme, initiated in 1986, is not restricted to any particular group of Member States, whether developing or industrialized, but is available to all countries with nuclear power plants in operation or approaching commercial operation.

Conservative design, careful manufacture and good construction are all prerequisites for safe nuclear power plants. However, their safety depends on the capability to prevent any incident during operation.

ASSET missions consider this aspect in assessing a facility's operational practices in comparison with those used successfully in other countries and when exchanging, at the working level, ideas for enhancing prevention of incidents.

The IAEA Safety Series publications form common basis for the ASSET reviews, including the Nuclear Safety Standards (NUSS), the Basic Safety Principles (Recommendations of Safety Series No. 75-INSAG-3) and Safety Culture (Safety Series No. 75-INSAG-4). The ASSET Guidelines provide overall guidance for the experts to ensure the consistency and comprehensiveness of their review of incident investigations. Additional guidance and reference material is provided by the IAEA to complement the expertise of the ASSET members.

ASSET reviews accept different approaches that contribute to ensuring an effective prevention of incidents at plants. Suggestions are offered to enhance plant safety performance. Commendable good practices are identified and generic lessons are communicated to other plants, where relevant, for long term improvement.

The present publication is an updated version of the ASSET Guidelines, IAEA-TECDOC-573, published in 1990. Sections 5 and 6 include revised definitions and investigation guidelines for identification of both direct and root causes. These revisions were recommended by a Consultants Meeting held in Vienna on 3-7 December 1990.

EDITORIAL NOTE

In preparing this material for the press, staff of the International Atomic Energy Agency have mounted and paginated the original manuscripts and given some attention to presentation.

The views expressed do not necessarily reflect those of the governments of the Member States or organizations under whose auspices the manuscripts were produced.

The use in this book of particular designations of countries or territories does not imply any judgement by the publisher, the IAEA, as to the legal status of such countries or territories, of their authorities and institutions or of the delimitation of their boundaries.

The mention of specific companies or of their products or brand names does not imply any endorsement or recommendation on the part of the IAEA.

CONTENTS

1. INTRODUCTION

Stimulating and contributing to the on-going process of striving for excellence in the area of operational safety of nuclear power plants worldwide is one of the essential duties of International Atomic Energy Agency.

Since 1986, in the frame of its operating experience feedback system, the IAEA has been offering the ASSET service (Assessment of Safety Significant Events Team) as an international mechanism to draw and to disseminate specific and generic lessons for enhancement of the level of operational safety. Several operating organizations have already benefitted from such an in-depth technical exchange of experience directed to the improvement of policies of prevention of incidents at NPPs.

1.1 Purpose of the ASSET guidelines

An ASSET working session concentrates on issues selected by the operating organization and reviews the various steps of the analysis performed by the operating organization. The final goal of an ASSET review is to provide conclusions on the appropriateness and completeness of the planned and implemented corrective actions. Generic lessons are drawn and suggestions are offered when necessary to improve plant management control on prevention of incidents thus enhancing the overal level of operational safety.

For this purpose, comprehensive expertise and a systematic analysis methodology are both indispensable for the conduct of conclusive investigations. The following guidelines are developed to ensure consistency in the application of the ASSET analysis methodology.

This guidance is not intended to infringe an expert's prerogative to investigate additional items. Its main purpose is to provide a basic structure and ensure consistency in the assessments. Use of the ASSET guidelines should also facilitate comparisons between the observations made in different nuclear power plants and harmonize the reporting of generic ASSET results. The guidelines should always be used with a critical attitude and a view to possible improvements.

1.2 Application of the ASSET guidelines

The ASSET guidelines are provided to guide the systematic review of each issue submitted by the operating organization. The provided instructions within the guidelines are not intended to be used as a check list with an obligation to check each item individually or with a prohibition from adding more items.

1.3 Structure of the ASSET guidelines

The ASSET guidelines are based on the application of the "in-depth defence concept" for prevention of incidents at nuclear power plants.

The level of quality required for safe operation is expected to be reached prior to operation through an effective quality assurance programme. However, the ultimate barrier consists of the plant surveillance programme which should be capable of timely detection of any latent weakness and of prompt restoration of the level of reliability, in such way diminishing the potential for incidents.

2. ASSET APPROACH TO PREVENTION OF INCIDENTS

The ASSET approach is based on the following:

- EVENTS (deviation, anomaly, issue, incident or accident) occurred always because of a
- FAILURE (occurrence) to perform as expected due to a
- LATENT WEAKNESS (direct cause) which was not timely eliminated due to
- DEFICIENCIES OF PLANT SURVEILLANCE PROGRAMME (Detection and Restoration) on equipment, personnel, procedures (root cause)

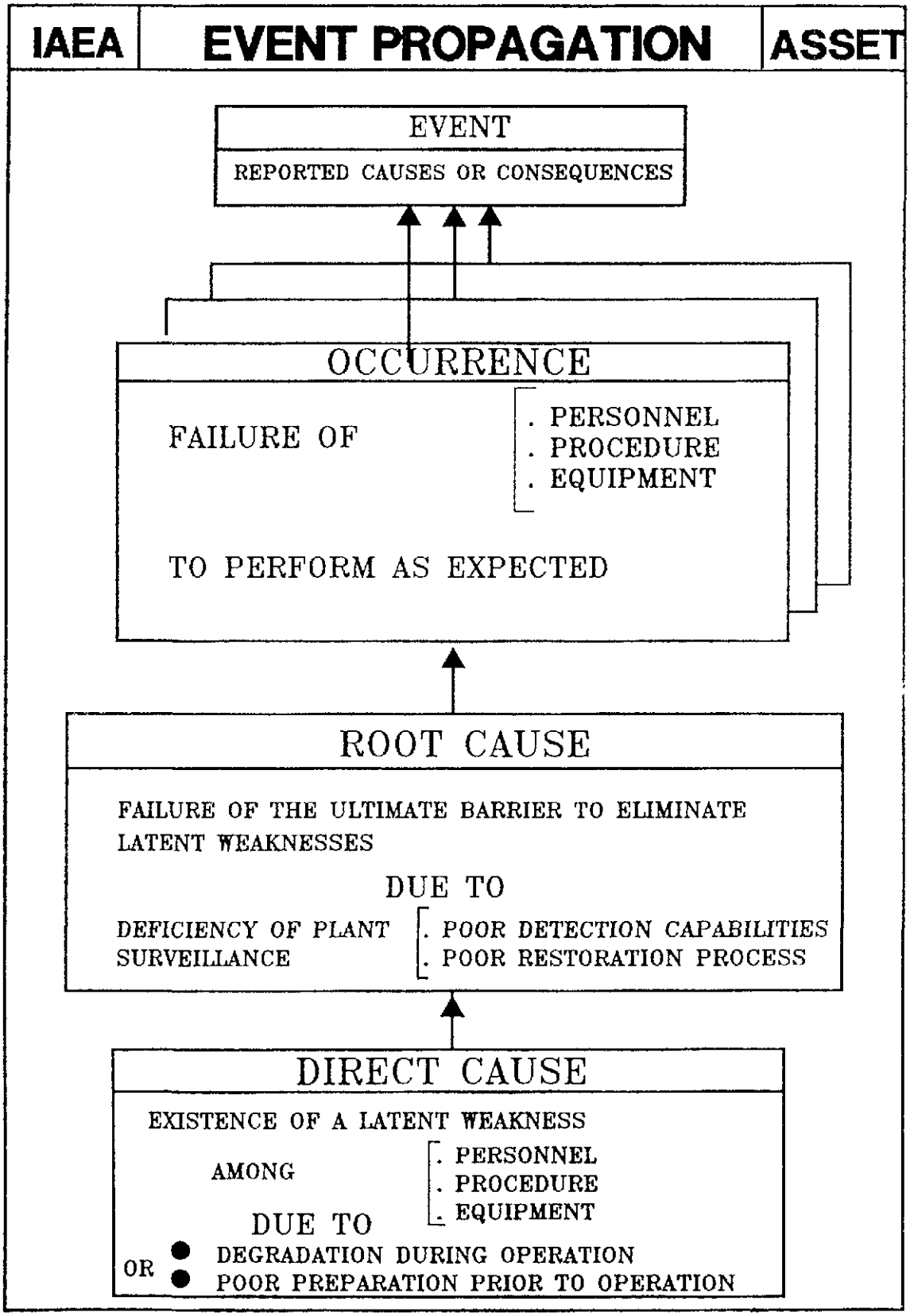
Striving for safe and reliable operation is the primary goal of any operating organization. Prevention of any negative impact on safety and reliability is the primary target of plant management: "NO INCIDENT".

The effectiveness of the policy of prevention of incidents is therefore the focal point of the ASSET approach based on commonly shared principles. (International Nuclear Safety Advisory Group (INSAG) Safety Series document No. 75-INSAG-3: Basic Safety Principles).

Safe operation and good performance at nuclear power plants require at all time the full operability of the three basic operational functions "man", "machine" and "interface man-machine".

The objective of full operability of the basic operational functions is met through compliance with the following requirements:

- At the stage of design: The necessary provisional redundancies (hardware and software) are provided in accordance to the average level of quality expected from personnel, equipment and procedure to ensure safe operation.
- At the stage of preparation prior to operation: A quality assurance programme ensures that, during the off-line plant activities aiming at preparation for safe and reliable operation, the resulting quality of operating personnel, equipment and procedures has reached the expected level prior to putting these elements into operation.


IAEA
EVENT PROPAGATION
ASSET
EVENT
REPORTED CAUSES OR CONSEQUENCES
OCCURRENCE
FAILURE OF
. PERSONNEL
. PROCEDURE
. EQUIPMENT
TO PERFORM AS EXPECTED
ROOT CAUSE
FAILURE OF THE ULTIMATE BARRIER TO ELIMINATE LATENT WEAKNESSES
DUE TO
DEFICIENCY OF PLANT SURVEILLANCE
. POOR DETECTION CAPABILITIES
. POOR RESTORATION PROCESS
DIRECT CAUSE
EXISTENCE OF A LATENT WEAKNESS
AMONG
. PERSONNEL
. PROCEDURE
. EQUIPMENT
DUE TO
OR
DEGRADATION DURING OPERATION
POOR PREPARATION PRIOR TO OPERATION

- At the stage of operation : A prevention maintenance programme ensures that the necessary actions are properly taken to prevent any degradation of the level of quality of personnel, equipment and procedures. A surveillance programme (Detection and Restoration) ensures that, during plant operation, any latent weakness, which might affect the expected quality of operating personnel, equipment and procedures, is detected and corrected through permanent assessment and prompt restoration.

Current plant designs are generally considered acceptable even if hardware provisions have to be supplemented by operational provisions to reach an optional level of safety. Preparation for operation and plant operation are the areas where weaknesses may usually happen.

The occurrence of events (incidents or accidents) demonstrates only that existing latent weaknesses were not detected and corrected on time. Personnel, equipment or procedures should therefore not be held responsible for failing to perform as expected. Quality assurance during preparation prior to operation and surveillance during plant operation were simply not effective enough to detect or to correct latent weaknesses among personnel, equipment or procedures.

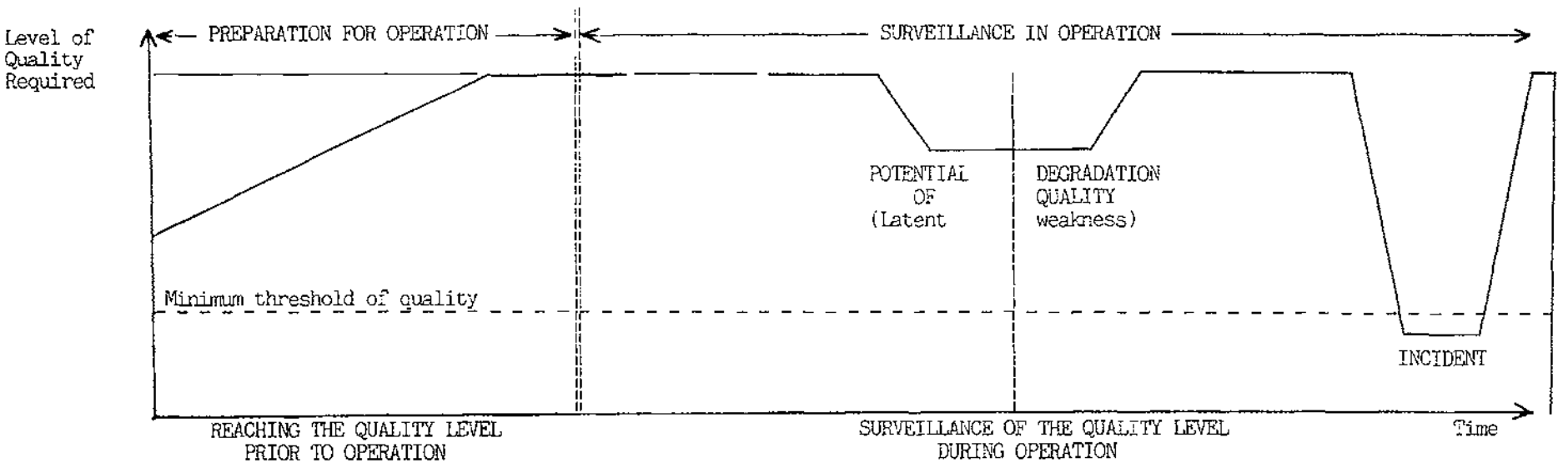
Timely detection of latent weaknesses and effective restoration provide therefore the ultimate barrier of the defence in-depth concept dedicated to prevention of incidents.

The detection programme should aim at thoroughly assessing proficiency of personnel, usability of procedures, operability of equipment to be capable of identifying latent weaknesses which might lead to personnel, equipment or procedures failure, under adverse circumstances.

The restoration process should aim at eliminating the latent weaknesses detected in order to fully recover operability of the functions "man", "machine", "interface man-machine" and at preventing any recurrence of such weaknesses:

- Either by eliminating the deficiencies of the programme of quality assurance of the various preparatory activities involved in quality of personnel (recruiting, training, motivating and licensing) of equipment (designing, manufacturing, storing, installing, maintaining and qualifying), of procedures (writing and validating)
- or by eliminating the deficiencies of the programme of surveillance of quality of these elements in the course of operation.

ASSET APPROACH TO PREVENTION OF INCIDENTS
(REACH AND MAINTAIN THE REQUIRED LEVEL OF QUALITY)



	PREPARING	CHECKING	DETECTION OF DEGRADATION	RESTORATION OF LEVEL OF QUALITY
PERSONNEL	Proficient personnel	Proficiency of personnel	Assessment of proficiency	Improvement and reverification of personnel proficiency
PROCEDURE	Usable procedure	Usability of procedure	Assessment of usability	Improvement and reverification of procedure usability
EQUIPMENT	Operable equipment	Operability of equipment	Assessment of operability	Improvement and reverification of equipment operability

3. ASSET METHODOLOGY FOR ANALYSIS OF EVENTS

The analysis of an event is conducted step by step through the application of a systematic methodology that concentrates on the five following areas:

- Selection of the occurrences to be analyzed: What is the occurrence (element that failed to perform as expected) or the combination of occurrences most significant to safety in the sequence of the event?

- Identification of the direct cause: What was the latent weakness which was affecting the element (personnel, equipment or procedure) that failed to perform as expected?

- Identification of the root causes: Why was the latent weakness (of the element which failed to perform as expected) not eliminated earlier by the plant surveillance (detection or restoration) programme?

- Determination of the corrective actions: What are the areas of improvements and the corrective actions needed to enhance both, quality and surveillance of quality of the element which failed to perform as expected?

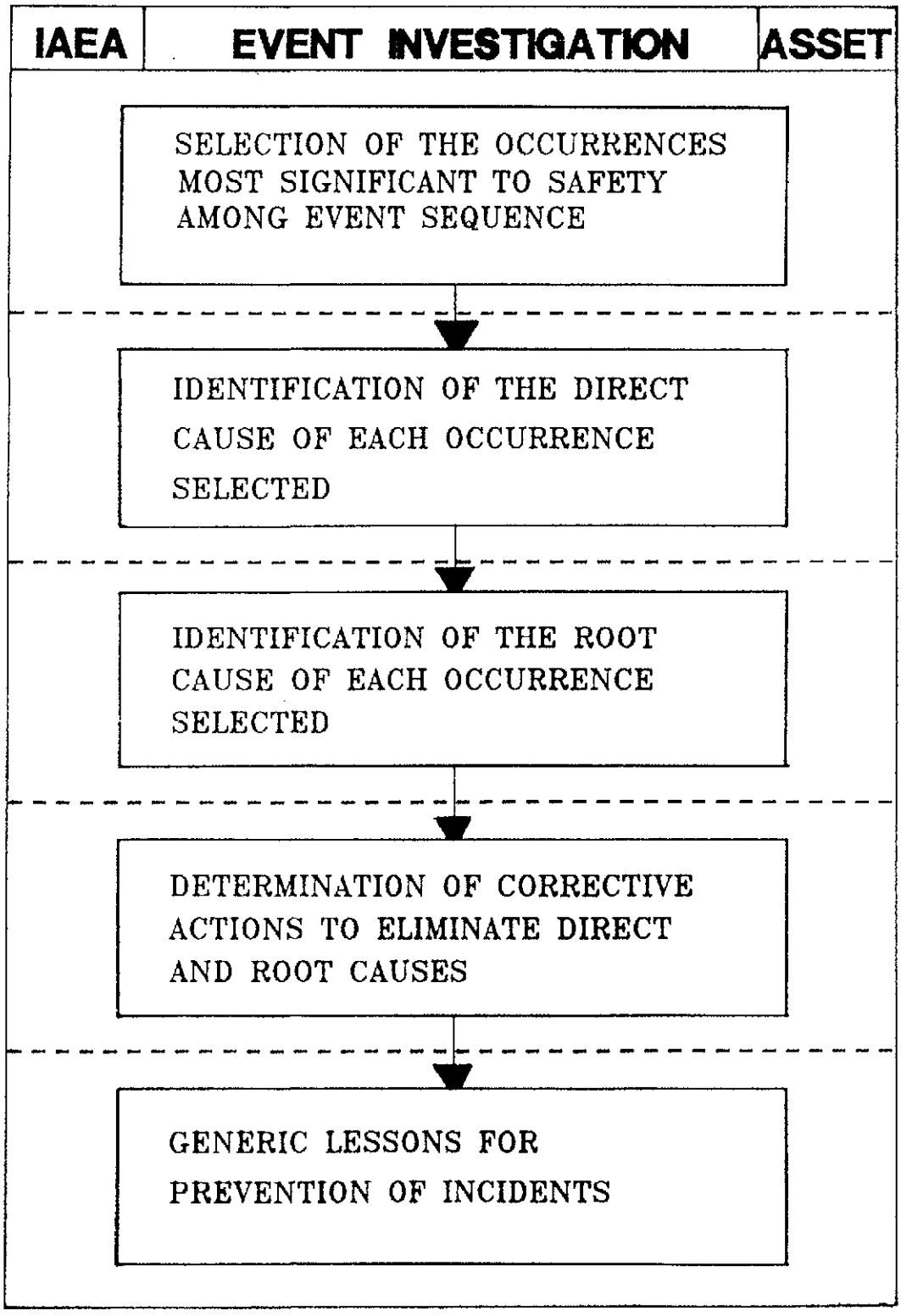
- Generic lessons: What are the generic lessons to be disseminated for further enhancement of prevention of incidents?

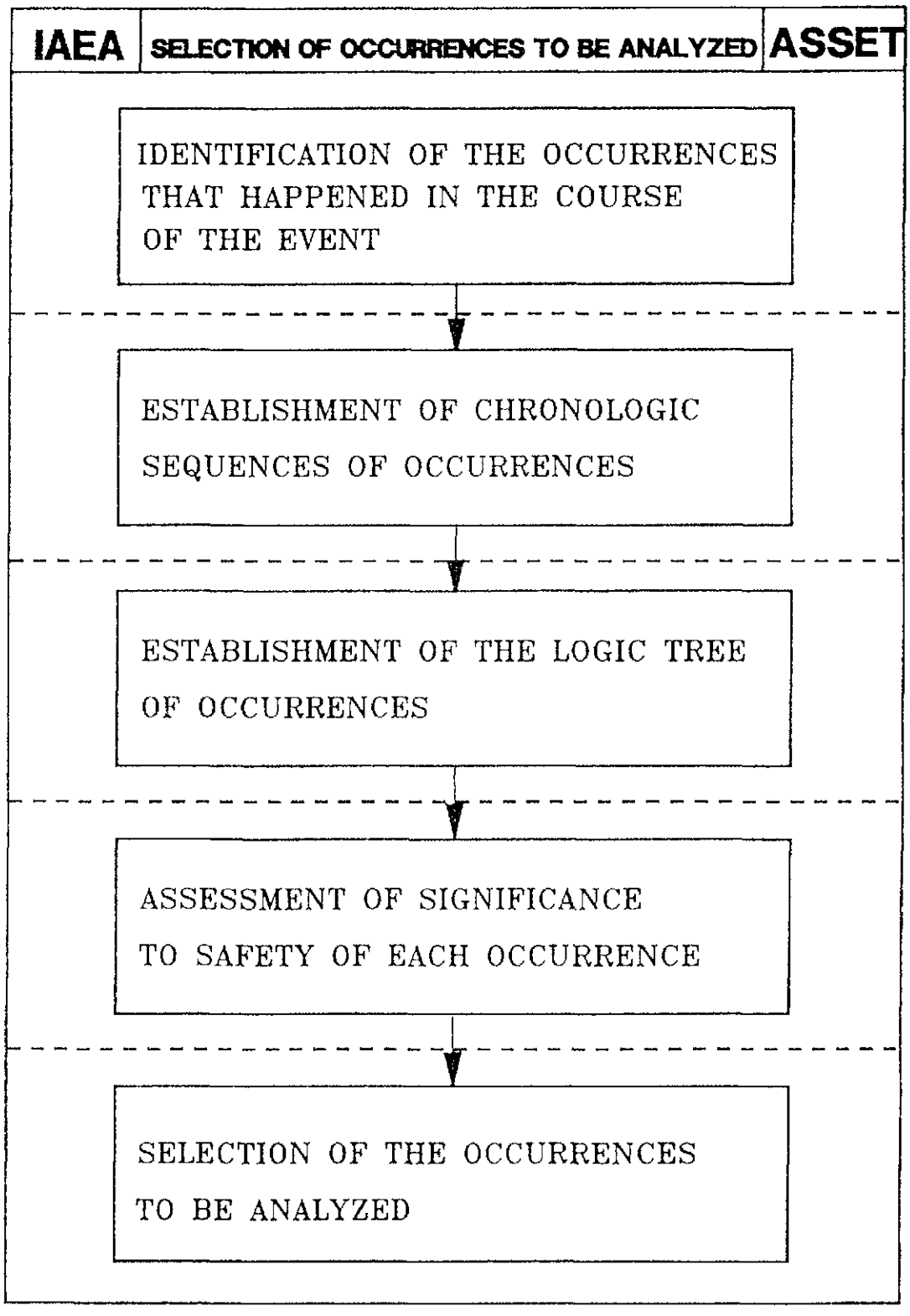
3.1 Selection of the occurrences to be analyzed

- An event (incident, accident) is a reportable situation defined by reporting criteria related to either causes or consequences.

- The title of an event may greatly vary according to the emphasis given to the various aspects of the event: actual consequences, failures to perform as expected, causes, contributors, significance to operational safety, etc.

- Events are very often a combination of several occurrences.


IAEA
EVENT INVESTIGATION
ASSET
SELECTION OF THE OCCURRENCES MOST SIGNIFICANT TO SAFETY AMONG EVENT SEQUENCE
IDENTIFICATION OF THE DIRECT CAUSE OF EACH OCCURRENCE SELECTED
IDENTIFICATION OF THE ROOT CAUSE OF EACH OCCURRENCE SELECTED
DETERMINATION OF CORRECTIVE ACTIONS TO ELIMINATE DIRECT AND ROOT CAUSES
GENERIC LESSONS FOR PREVENTION OF INCIDENTS


IAEA
SELECTION OF OCCURRENCES TO BE ANALYZED
ASSET
IDENTIFICATION OF THE OCCURRENCES THAT HAPPENED IN THE COURSE OF THE EVENT
ESTABLISHMENT OF CHRONOLOGIC SEQUENCES OF OCCURRENCES
ESTABLISHMENT OF THE LOGIC TREE OF OCCURRENCES
ASSESSMENT OF SIGNIFICANCE TO SAFETY OF EACH OCCURRENCE
SELECTION OF THE OCCURRENCES TO BE ANALYZED

- An occurrence is a failure to perform as expected of one of the basic elements (personnel, equipment or procedure) involved in plant operation.

- A chronological sequence of the various occurrences of the event may be established from the narrative description of the event.

- Each occurrence in the chronological sequence of the event is either independent or connected to other occurrences.

- The logic tree of occurrences shows the interconnections between occurrences and enables concentrating on the main branch of occurrences related to the reported event.

- Each occurrence of the logic tree has a different weight to be assessed in connection with potential and actual significance to safety.

- The assessment of the significance to safety of each occurrence is based on both aspects, potential and actual consequences to safety.

  + The potential significance to safety may be assessed through an:

    o Quantitative evaluation of the increase of the probability of occurrence of unacceptable situations such as harm to public, harm to plant personnel, uncontrolled radioactive releases, core damages, inoperability of safety functions, etc.

    o Evaluation qualitative of the potential consequences to safety of the occurrence under circumstances different from the event considered.

  + The actual significance to safety may be assessed through an:

    o Evaluation of the actual consequences to safety of the occurrence under the present circumstances of the event (impact on environment, radioactive releases, core damages, inoperability of safety and support functions).

- o Evaluation based on the regulatory reporting criteria .

- o Evaluation based on the exceeding of the plant operational limits and conditions (technical specifications) for safe operation.

- Only a probabilistic approach enables a detailed quantitative assessment of the potential significance to safety of an occurrence provided that it takes into account the contribution of the three basic elements (personnel, procedure and equipment).

- On the other hand, operational limits and conditions (technical specifications) might also be used as a sound basis for evaluating potential significance to safety if their consistency with a plant probabilistic safety assessment has been checked.

- In case a probabilistic assessment is not available and cannot be performed to assess potential significance, occurrences to be analyzed may be selected on the basis of their actual significance versus the following ranking criteria.

- Criteria of high significance to safety:

1. Impact on the environment (public and plant personnel)
   - o death
   - o injury
   - o irradiation superior to 50 mSv

2. Uncontrolled radioactive releases
   - o Iodine 131 superior to 10E10 Bq
   - o Gas and aerosols superior to 10E10 Bq
   - o Liquids superior to 10E10 Bq

3. Core damages
   - o melting superior to 10^{-3} of core

4. Inoperability of safety functions
   - o Loss of the function "Reactor shutdown"
   - o Loss of the function "Cooling of fuel"
   - o Loss of the function "confinement"

5. Inoperability of the support functions
   - o Loss of the function "off-site electrical power"
   - o Loss of the function "on-site electrical power"
   - o Loss of the function "Cooling water"
   - o Loss of the function "instrument air"

6. Potential for one of the above events.

- The occurrences selected are always a personnel deficiency, a procedure deficiency or an equipment deficiency which happened in the course of the event.

- Caution should be taken at this stage to identify clearly the element requested for on-line operation which did not perform as expected.

3.2 Identification of the direct cause of an occurrence

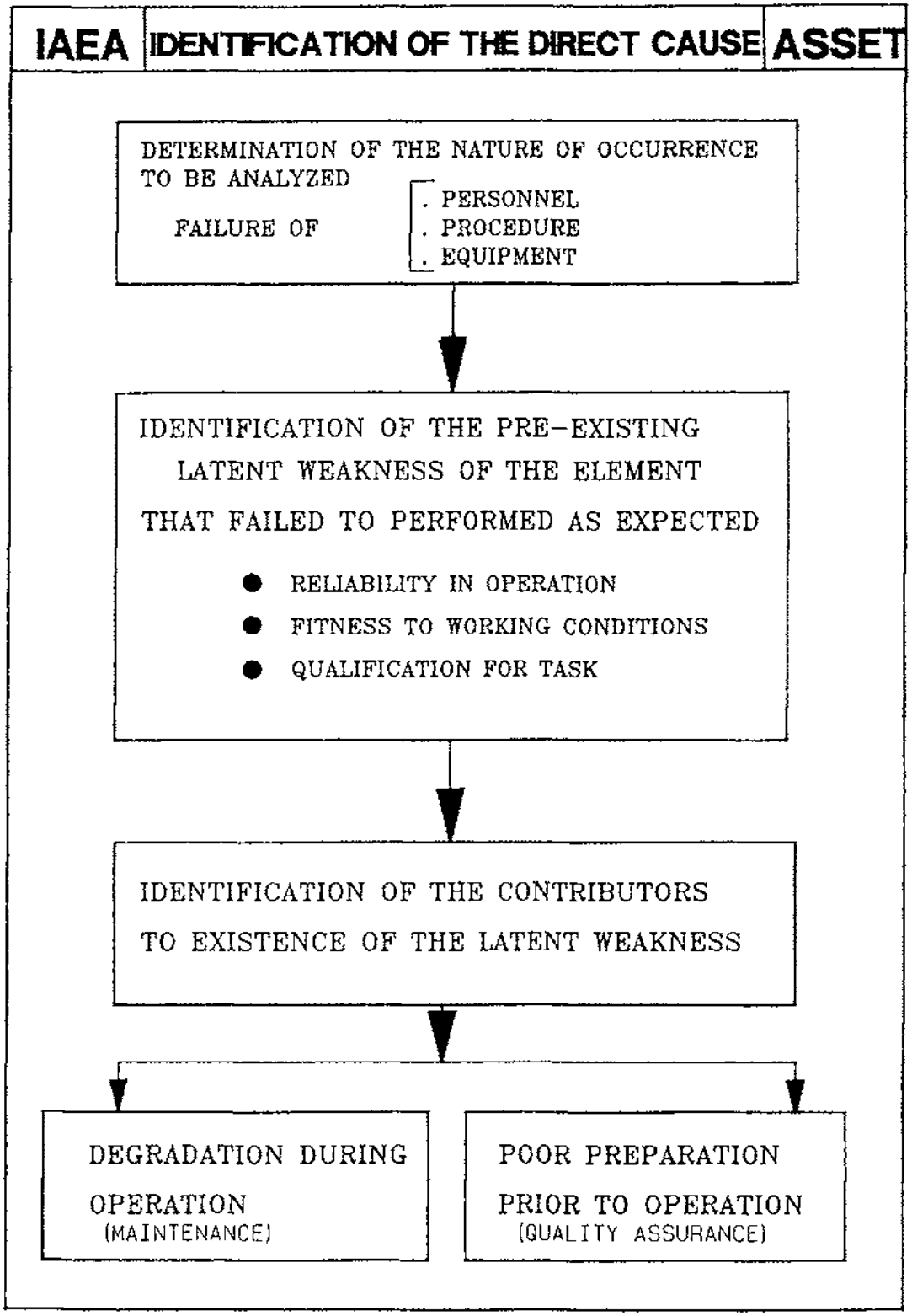
- The starting point of the investigation is the selected occurrence either a personnel deficiency, or a procedure deficiency or an equipment deficiency.

- The direct cause of an occurrence is the pre-existing latent weakness of the basic element (personnel, procedure, equipment) that failed to perform as expected in the course of the event associated with the contributors to the existence of the latent weakness.

- The latent weakness of the element which failed to perform as expected affected either proficiency of personnel, or usability of procedure or operability of equipment.

- Identification of the latent weakness of the personnel involved is carried out by referring to the characteristics of personnel proficiency required for the task where the individual failed to perform, as expected:

- Identification of the latent weakness of the equipment involved is carried out by referring to the characteristics of equipment operability required for the task where the equipment failed to perform as expected.


IAEA
IDENTIFICATION OF THE DIRECT CAUSE
ASSET
DETERMINATION OF THE NATURE OF OCCURRENCE TO BE ANALYZED
FAILURE OF
. PERSONNEL
. PROCEDURE
. EQUIPMENT
IDENTIFICATION OF THE PRE-EXISTING LATENT WEAKNESS OF THE ELEMENT THAT FAILED TO PERFORMED AS EXPECTED
RELIABILITY IN OPERATION
FITNESS TO WORKING CONDITIONS
QUALIFICATION FOR TASK
IDENTIFICATION OF THE CONTRIBUTORS TO EXISTENCE OF THE LATENT WEAKNESS
DEGRADATION DURING OPERATION
(MAINTENANCE)
POOR PREPARATION PRIOR TO OPERATION
(QUALITY ASSURANCE)

- Identification of the latent weakness of the procedure involved is carried out by referring to the characteristics of procedure usability required for the task where the procedure failed to provide proper guidance as expected:

- The existence of a latent weakness is the result of a discrepancy which happened in the course of :

  - o either preparation prior to operation of personnel, procedure, equipment.
  - o or plant operation due to unforeseen reasons.

- The existence of the latent weakness is due to various contributors which are identified among the following areas:

  - o Preparation prior to operation: The quality assurance programme was not effective enough to ensure that the expected level of quality was reached.

    - + Uncomprehensive verification of personnel proficiency, equipment operability, procedure usability prior to operation

    - + Inadequate acceptability criteria
    - + Ineffective correction of detected discrepancies

  - o Degradation in operation: The level of quality required prior to operation was reached but due to unforeseen reasons a degradation occurs in the course of operation because of:

    - + Inconducive environmental conditions beyond the specifications taken as reference for preparation prior to operation of personnel, procedure and equipment.

    - + Premature degradation of personnel proficiency, of procedure usability or equipment operability (poor maintenance programme).

- The contributors to the existence of the latent weakness of the element which failed to perform as expected are usually a combination

of several factors that have to be addressed to prevent any recurrence.

- Caution should be taken at this stage to identify clearly the factors that are under plant management control and those which are not.

- Limitations in the depth of the search for contributing factors have to be considered. Although the origin of any latent weakness is always due to human factors, only those which are related to plant personnel under plant management control are investigated.
Human factors having contributed to any latent weakness in the course of the activities of preparation for operation that are outside plant management control are not addressed. Surveillance in operation is the the plant management tool expected to detect and correct latent weaknesses which were not identified by commissioning tests. They generally resulted from activities such as designing, manufacturing, installing equipment.

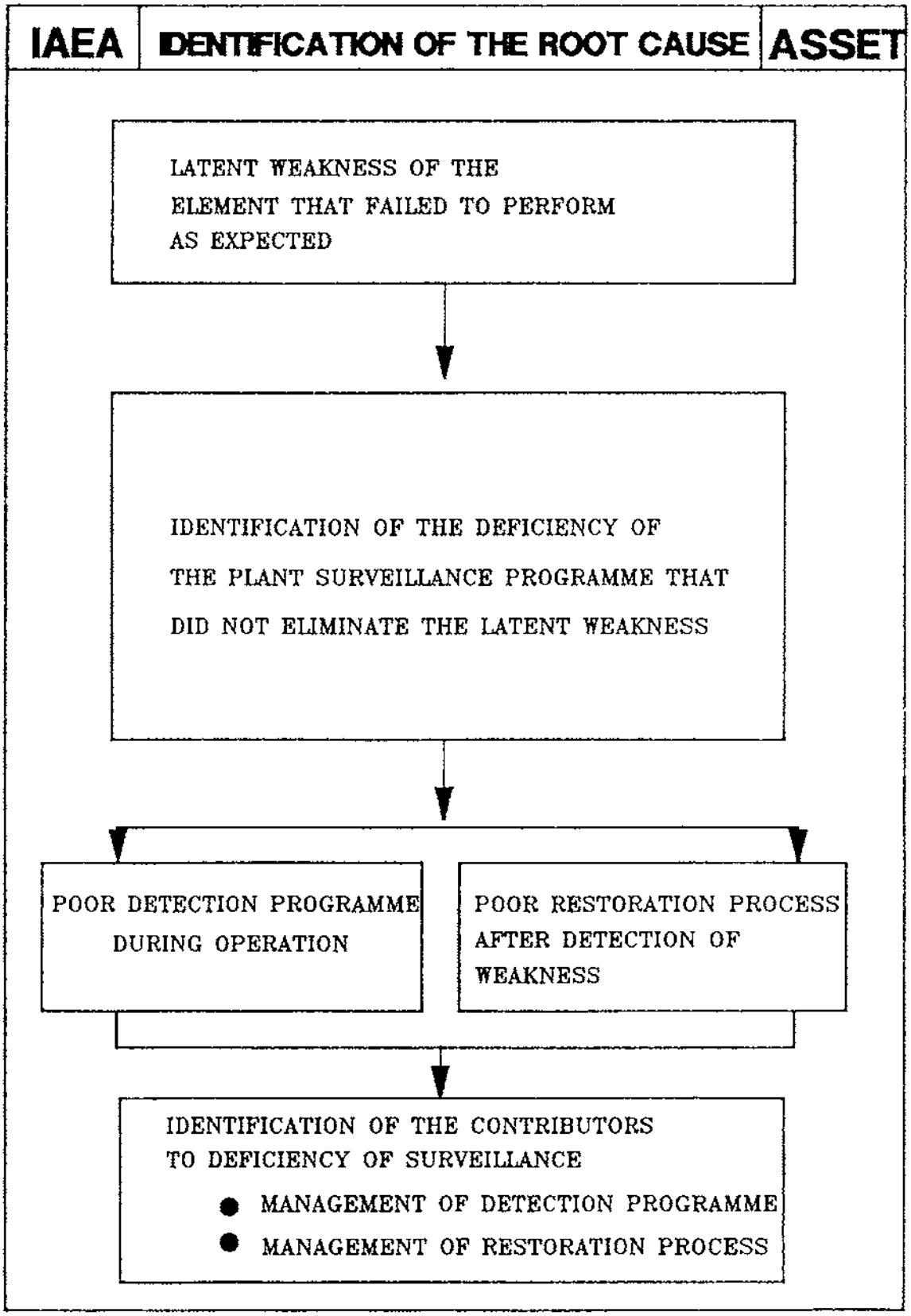
3.3 Identification of the root causes of an occurrence

- The starting point of the investigation is the identified direct cause (latent weakness and contributors to personnel, equipment or procedure deficiency) responsible for the occurrence analyzed .

- Whatever the origin of the latent weakness is (poor preparation prior to operation or degradation during operation),an effective plant surveillance programme should be capable of detecting any latent weakness and of restoring the level of quality required for safe operation.

- The root cause of any occurrence is therefore a failure to eliminate the pre-existing latent weakness in due time.

- The root cause of an occurrence is precisely a deficiency of the plant surveillance programme (detection and restoration) in operation which did not play its expected role of ultimate barrier regarding prevention of incidents.


IAEA
IDENTIFICATION OF THE ROOT CAUSE
ASSET
LATENT WEAKNESS OF THE ELEMENT THAT FAILED TO PERFORM AS EXPECTED
IDENTIFICATION OF THE DEFICIENCY OF THE PLANT SURVEILLANCE PROGRAMME THAT DID NOT ELIMINATE THE LATENT WEAKNESS
POOR DETECTION PROGRAMME DURING OPERATION
POOR RESTORATION PROCESS AFTER DETECTION OF WEAKNESS
IDENTIFICATION OF THE CONTRIBUTORS TO DEFICIENCY OF SURVEILLANCE
MANAGEMENT OF DETECTION PROGRAMME
MANAGEMENT OF RESTORATION PROCESS

- The deficiency of surveillance of personnel proficiency, of procedure usability or of equipment operability is always related to:

  - o either poor detection capabilities
  - o or a poor restoration process

- Identification of the deficiency of the plant detection programme is carried out by referring to the characteristics required for timely detection of any latent weakness:

  - o Testing
  - o Trending of performance
  - o Criteria of acceptability

- Identification of the deficiency of the restoration process is carried out by referring to the characteristics required for prompt and relevant correction of any latent weakness:

  - o analysis of detected latent weaknesses
  - o determination of improvements
  - o implementation of improvements

- The existence of a deficiency of the plant surveillance programme is due to various contributors which are identified among the following areas:

  - o management of the detection programme
  - o management of the restoration process

- The various contributors to the deficiency of the plant surveillance programme are usually a combination of human factors under plant management control.

3.4 Determination of corrective actions related to an occurrence

- Corrective actions should aim at addressing all the occurrences of the event sequence.

- The objectives of the corrective actions related to a specific occurrence are:

  - o to eliminate the actual consequences of the occurrence (damage, etc.)

  - o to eliminate and prevent reappearance of the latent weakness (direct cause) of the element that failed to perform as expected

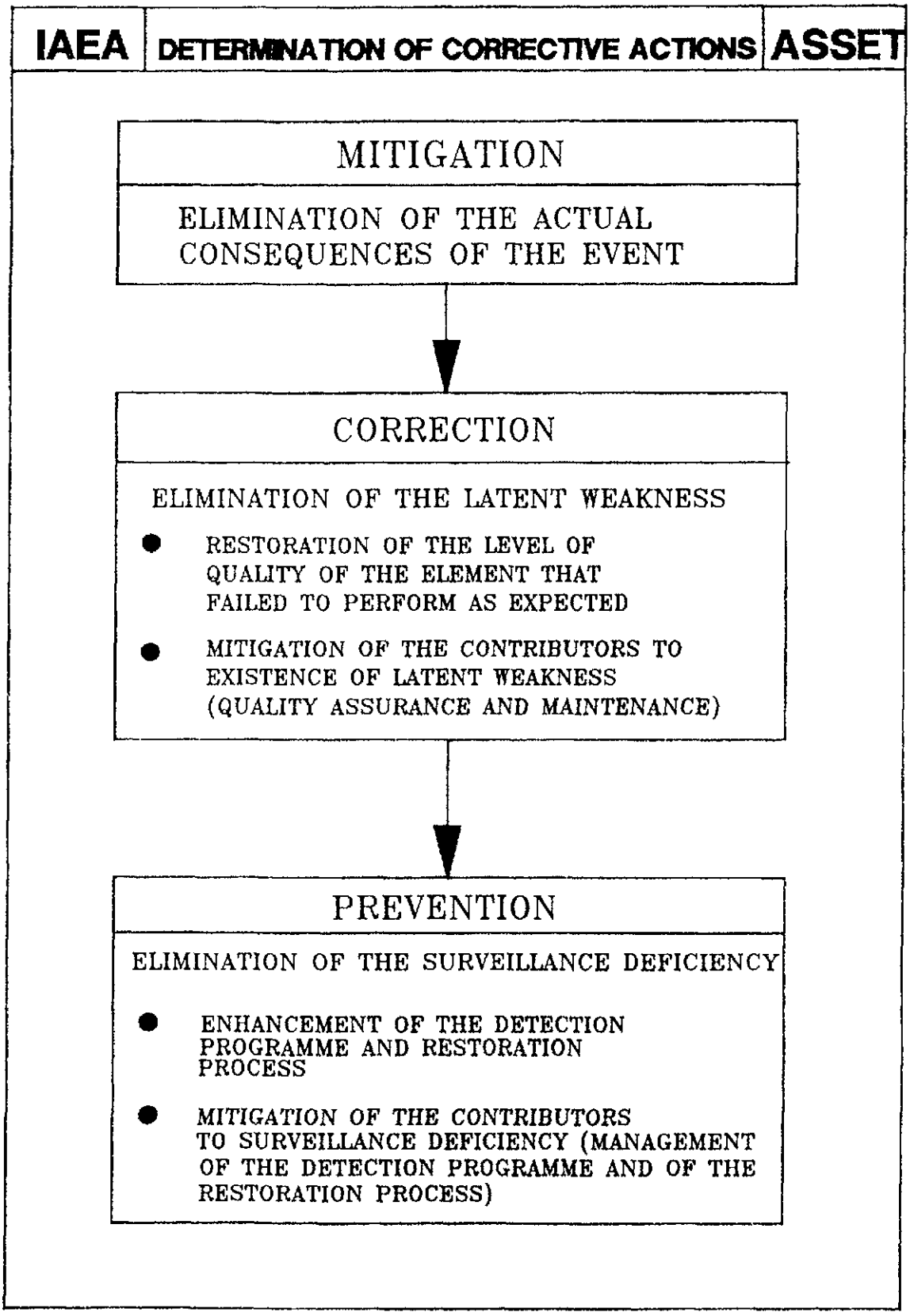
  - o to eliminate and prevent reappearance of the deficiency of the plant surveillance programme (root cause) that failed to eliminate the latent weakness in due time.

- Elimination and prevention of the latent weakness (direct cause) is achieved:

  - o by restoring the level of quality of the element which failed to perform as expected (personnel, procedure, equipment)

  - o by preventing reappearance of latent weakness which led to failure to perform as expected through
    - + improvement of the quality assurance programme prior to operation, and
    - + mitigation of the contributors to degradation of the level of quality during operation.

N.B.: The above corrective actions may provide reasonable assurances that the level of quality required is reached and will be maintained. However, it cannot be ignored that due to unforeseen reasons quality may not reach the level expected prior to operation or may degrade during operation. Safety requires therefore an effective tool of surveillance to timely detect and promptly correct any latent weakness to achieve an effective prevention of incidents at nuclear power plants.


IAEA
DETERMINATION OF CORRECTIVE ACTIONS
ASSET
MITIGATION
ELIMINATION OF THE ACTUAL CONSEQUENCES OF THE EVENT
CORRECTION
ELIMINATION OF THE LATENT WEAKNESS
RESTORATION OF THE LEVEL OF QUALITY OF THE ELEMENT THAT FAILED TO PERFORM AS EXPECTED
MITIGATION OF THE CONTRIBUTORS TO EXISTENCE OF LATENT WEAKNESS (QUALITY ASSURANCE AND MAINTENANCE)
PREVENTION
ELIMINATION OF THE SURVEILLANCE DEFICIENCY
ENHANCEMENT OF THE DETECTION PROGRAMME AND RESTORATION PROCESS
MITIGATION OF THE CONTRIBUTORS TO SURVEILLANCE DEFICIENCY (MANAGEMENT OF THE DETECTION PROGRAMME AND OF THE RESTORATION PROCESS)

- Elimination and prevention of the deficiency of the plant surveillance programme (root cause) is achieved:

    - o by improving the detection programme in order to make it capable of detecting any latent weakness among personnel proficiency, procedure usability and equipment operability
    - o by improving the restoration process in order to make it capable of implementing appropriate corrective actions
    - o by preventing reappearance of the deficiency of plant surveillance that led to the non elimination of the latent weakness through
        - + improvement of the general surveillance policy related to personnel proficiency, procedure usability and equipment operability, and
        - + mitigation of the contributors to ineffective surveillance (detection and restoration) during operation

- Selection of areas needing improvements is based on the logic tree including the latent weakness with its contributors and the deficiency of surveillance with its contributors.

- Selection of areas needing improvements to eliminate the latent weakness and possibility of recurrence includes all the contributors identified

    - o to poor preparation prior to operation under plant management control such as recruiting, training, licensing personnel, preparing, validating procedure, maintaining, qualifying equipment.
    - o to degradation in operation due to management, environmental and ageing conditions.

- Selection of areas needing improvements to eliminate the deficiency of the surveillance programme and possibility of recurrence includes all the contributors identified

    - o to poor management of the detection programme
    - o to poor management of the restoration process.

- Determination of corrective actions aim at enhancing quality of the element which failed and at enhancing surveillance of the quality of this element.

- Corrective actions are implemented indifferently in the software or the hardware area.

3.5 Generic lessons

- Generic lessons from the event under investigation are drawn in connection with the general policy of prevention of incidents at the plant.

  - o Good practices that have prevented the event to be worse and that will prevent recurrence of similar events

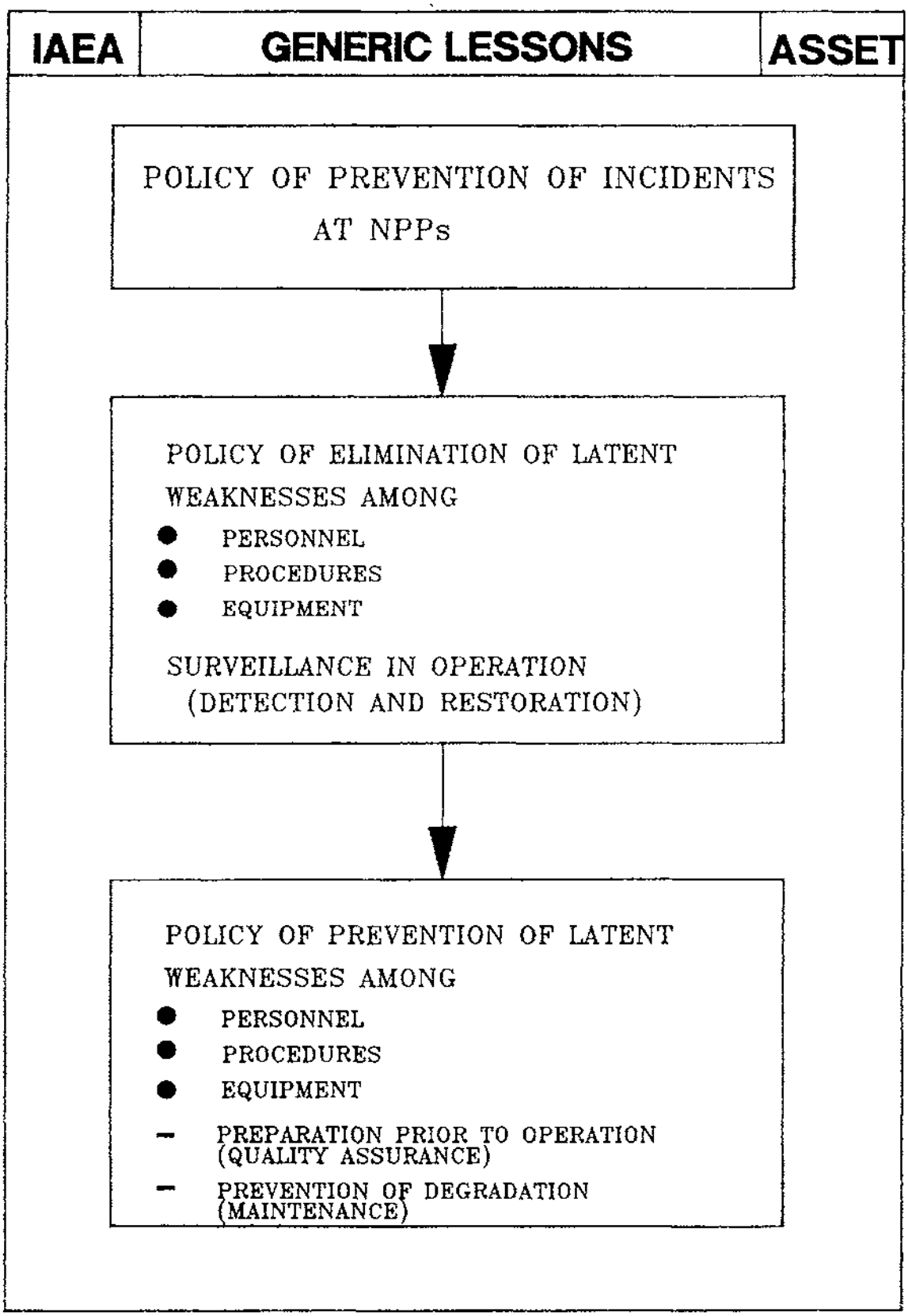
  - o Suggestions for enhancement of appropriateness and completeness of corrective actions to prevent recurrence of similar events.

- Generic recommendations to the nuclear community are prepared and disseminated to stimulate:

  - o Elimination of existing latent weakness among personnel, procedure and equipment through more effective surveillance during operation (detection and restoration)

  - o Prevention of appearance of latent weakness among personnel, procedures and equipment through more effective:

    - + preparation prior to operation (quality assurance) and
    - + prevention of degradation during operation (maintenance)


IAEA
GENERIC LESSONS
ASSET
POLICY OF PREVENTION OF INCIDENTS AT NPPs
POLICY OF ELIMINATION OF LATENT WEAKNESSES AMONG
PERSONNEL
PROCEDURES
EQUIPMENT
SURVEILLANCE IN OPERATION (DETECTION AND RESTORATION)
POLICY OF PREVENTION OF LATENT WEAKNESSES AMONG
PERSONNEL
PROCEDURES
EQUIPMENT
PREPARATION PRIOR TO OPERATION (QUALITY ASSURANCE)
PREVENTION OF DEGRADATION (MAINTENANCE)

4. SELECTION OF THE OCCURRENCES TO BE ANALYZED WITHIN THE EVENT SEQUENCE

4.1 Objectives

The objectives of this review are:

1) to provide independent identification of the occurrences among the event sequence, that are most significant to safety and should be analyzed in depth.

2) to assess the adequacy of the operating organization's process and results in identifying the most safety significant occurrences.

4.2 Preparatory work

- Collect and review the procedures available at the plant related to identification of occurrences significant to safety (assessment techniques and ranking criteria).

- Collect and review the regulatory body reporting criteria and/or the event severity scale relevant for the considered plant.

- Collect and review the narrative description of the event under investigation.

4.3 Investigations

In order to identify the occurrences most significant to safety which should be submitted to an in-depth review for direct and root causes the following steps should be followed:

- identification of occurrences as reported in the narrative description of the event.

- establishment of the chronological sequence of these occurrences.

- establishment of the logical interdependence of the occurrences by building a logic tree of occurrences.

- assessment of the safety significance of each occurrence.

- selection of the occurrence most significant to safety for further in-depth review.

Note: The assessment of the operating organization's process and results of determining the most safety significant occurrences can be done in parallel with this effort - see section 4.4.

4.3.1 Identification of the occurrences

The starting point of this investigation is the narrative description of the reported event.

At a nuclear power plant, the activities are governed by a work process. According to the ASSET methodology this work process has three basic elements: people, procedures and equipment. If an error arises in the performance of a work process, it can be attributed to one of the two following categories:

(1) equipment failure i.e. an equipment fails to perform as expected during the course of the event under investigation.

(2) inappropriate action also sometimes called personnel error (not be confounded with personnel deficiency) i.e. a person makes an error during the course of the event; this error can be attributed to lack of proficiency of the individual involved or to a deficiency in the procedural guidance related to the task involved; this difference between deficiency of personnel proficiency or deficiency of procedural guidance is already the subject of a more in-depth analysis introducing the search for direct causes and will be addressed in section 5.3.0.

According to the ASSET methodology these errors are called occurrences.

Review the event report and identify errors arising during the course of the event which can be attributed to one of the two abovementioned categories.

List these occurrences according to the sequence of reporting.

4.3.2 Establishment of the chronological sequence of occurrences

The starting point of this investigation is the list of occurrences as identified at the end of section 4.3.1.

The sequence according to which the identified occurrences are reported in the original narrative description of the event, is not necessarily a chronological one.

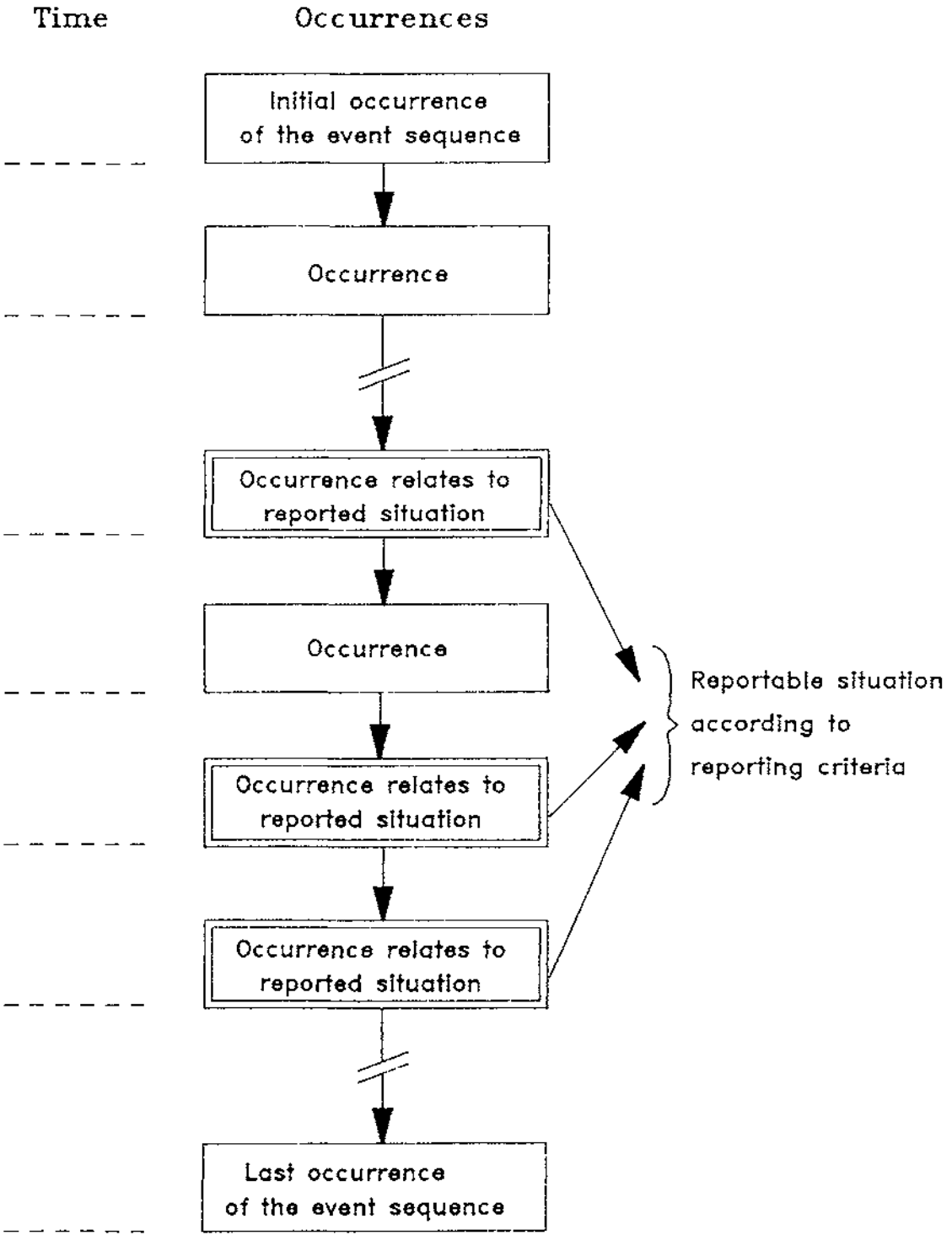
The establishment of a chronological sequence of occurrences is the first step of analysis of the event under investigation.

Review the event report or any other documentation related to the event for any indication of the chronological sequence of events (e.g. time schedule attached to the occurrences in the course of the event, other time indications in the narrative part of the event report). Review process computer output if necessary and review involved plant staff interview records if available.

Check the obtained chronological sequence of occurrences for logical consistency.

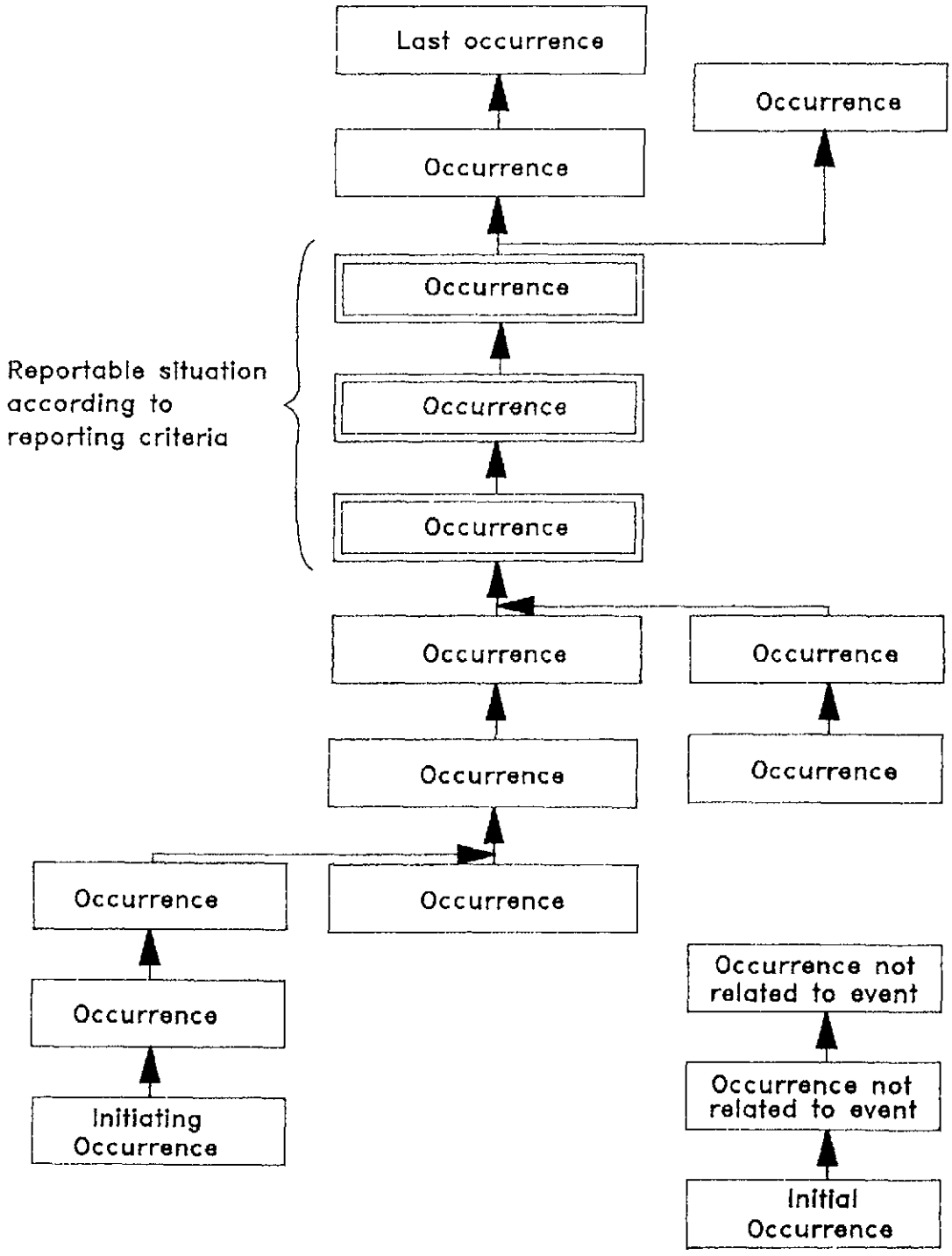
EVENT (INCIDENT OR ACCIDENT)

EXAMPLE OF CHRONOLOGICAL SEQUENCE OF OCCURRENCES



EVENT (INCIDENT OR ACCIDENT)

EXAMPLE OF LOGIC TREE OF OCCURRENCES



4.3.3 Establishment of the logic tree of occurrences

The establishment of the logic tree of occurrences, by searching for the logic (causal) interdependence of reported occurrences is the next step of the analysis process. The aim is to force the analyst to think in a logical and structured way when describing the event. This structuring process is helpful when an assessment of the safety significance of occurrences will be made and is essential when this assessment will be done on the basis of Probabilistic Safety Assessment (PSA) (see section 4.3.4).

Consequently the analyst can more easily identify any relevant missing information. The event reports as presented to the ASSET members will not always contain all information necessary for a complete understanding of the event, including the identification of all causal links between the reported occurrences or the identification of underlying occurrences contributing to the present situation (e.g. status of equipment) that are not reported in the event report and related cause analysis reports. This missing information should be obtained by interviews of plant staff, review of relevant plant operation records, review of examination reports of failed equipment, on-site visits of plant systems and equipment, etc.

The starting point of this investigation is the chronological sequence of occurrences as obtained in section 4.3.2. The result is a graphical display of the event as shown in the next figure.

Additional guidance for the establishment of the logic tree of occurrences is provided by the following instructions:

- Review if a logic tree of occurrences is available in the event report.
- Identify the initiating occurrences i.e. those occurrences, for which no other occurrences, leading up to the occurrences under consideration, can be identified.
- Identify logical (causal) interdependence between reported occurrences, respecting chronological sequence, and establish independent branches. Identify in this process the nodes (if any) of the logic event tree:
    - o where independent occurrences are necessary conditions to lead up to the next occurrence.

- o or where an occurrence leads up to two or more independent occurrences.

- Verify that the occurrences range from beginning to end of the event sequence.

- Verify that each occurrence is based on valid information.

4.3.4 Assessment of safety significance of the occurrences

General remarks:

The assessment of safety significance of the occurrences within a reported event sequence is generally a "comparison" of the characteristics of the observed occurrences with available reference material e.g. Tech. Specs, operating limits and conditions, regulatory body reporting criteria.

Dependent on the available reference material seven different "comparisons" are possible and very often questioned (see Fig. 4.3.1).

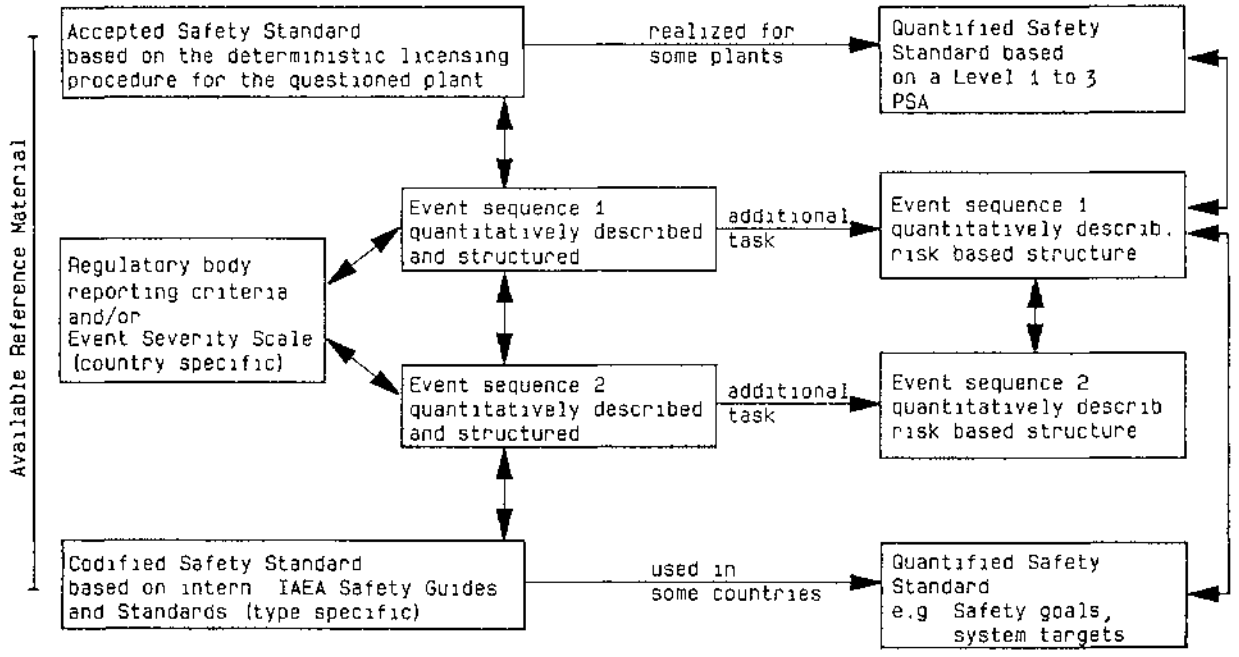


FIG. 4.3.1. Different options (A to G) for 'comparisons' for the assessment of the safety significance of different occurrences.

A: A qualitative comparison between the occurrences and the Regulatory Body Reporting Criteria or an "Event Severity Evaluation Scale" relevant for the given plant.

B: A qualitative comparison between the occurrences and the plant specific accepted safety standards (e.g. Tech. specs, operational limits and conditions) based on the licensing procedure.

C: A qualitative comparison between the occurrences and the codified international, type specific IAEA safety guides and standards.

D: A quantitative comparison between the occurrences on the basis of risk measures (e.g. core damage frequency, system availability, individual risk) derived from a plant specific Level 1 to 3) Probabilistic Safety Assessment (PSA).

E: A quantitative comparison between the occurrences on the basis of risk measures derived from probabilistic "Safety Goals" or "System Targets").

F: A qualitative comparison between occurrences in different event sequences of the questioned plant, based on the plant specific accepted safety standard.

G: A quantitative comparison between occurrences in different event sequences on the basis of importance measures (e.g. risk achievement worth) calculated in a plant specific PSA.

For practical application three different options for comparisons, namely A, B, and D will be discussed in more detail.

The decision which option should be used is case dependent. If no plant specific PSA is available then the qualitative options A or B must be used. If a PSA is available then the probabilistic approach enables a quantitative assessment in one model and therefore a real importance ranking of different occurrences.

First Option: Assessment of safety significance of the occurrences based on comparison with Regulatory Body Reporting (RBR) Criteria and/or an Event Severity Scale (see Fig. 4.3.1., A).

The RBR-Criteria in the different countries are mainly focused on actual radioactive release, and/or actual failures on safety systems, and/or actual harm to workers or public. In some countries (e.g. Japan, France), there exist activities setting up a so-called Event Severity Scale. In such a multi-dimensional scale a criterion related to the status of the reactor facility is included. If such a scale is used then subjective judgment by an experienced system engineer will be necessary to classify the different occurrences in a given event sequence (e.g. to classify between: an occurrence which does not affect the safety of the reactor facility but may be related to it, and, an occurrence which does not affect the safety of the reactor facility but is related to it). Finally, the scale of classified occurrences answers the question related to the safety significance.

The assessment in this context is a straightforward check of the observed occurrences versus the RBR Criteria.

For assessment of safety significance some important questions are listed below.

- Which criteria and/or scale were used?
- Was an assessment of significance to safety carried out for each of the occurrences?

- Was potential significance to safety considered?

Second Option: Assessment of safety significance of the occurrences based on the plant specific accepted safety standards (see Fig. 4.3.1, B)

If no Event Severity Scale and no plant specific PSA are available then the assessment must be done on the basis of the deterministic licensing procedure represented by design basis accident concept, tech-specs and the operating limits and conditions. In this context, scaling examples are:

- A failure in a safety system is more severe as in a non-safety system.

- Double failures are more severe as a single failure.

- A failure in a Class I component (see ASME-code definition e.g. Reactor Pressure Vessel) is more severe as a failure in a Class II component (e.g. Residual Heat Removal Pump).

- A failure of a component (element) involved in the course of a design basis accident is more severe as a failure of a component (element) involved in a no-name sequence.

All these examples are not outcomes of an overall risk model (PSA model) and therefore this procedure has some weaknesses. A typical example for these weaknesses is the first example. From PSA we know today that a failure of one non-safety system (e.g. a ventilation system) is also safety significant if this non-safety system interacts with different safety systems.

For assessment of safety significance some important questions are listed below:

- Was the event sequence similar to a sequence taking into account in the design basis accident evaluation?
- Which tech-specs and/or operational limits and conditions were considered?
- Which additional insights from PSAs were used to assess the significance of the occurrences?
- Do operational limits and conditions address in addition to equipment but also personnel and procedures?
- Was potential significance to safety considered?

Third Option: Assessment of safety significance of occurrences based on plant specific PSA insights (see Fig. 4.3.1, D).

For many NPPs (about 80) exist a PSA and in some countries, it is decided to prepare for each plant - as a minimum - a Level 1 study (e.g. FRG, Sweden). Therefore, this approach has a great potential to be in future the leading one for the assessment of safety significance of occurrences.

If a PSA is available for the considered plant then the following tasks are necessary.

• Structuring the event sequence

It is of utmost importance to fully understand the event sequence, including the operation of the systems involved as well as their intended function. A logical structuring of the event sequence is then accomplished in a PSA compatible way, which means the identification of systems and functions

involved and the definition of the initiating event. It is likely that some information is missing from the event report, preventing a thorough listing of logical steps. It is important to recognize that the structuring phase, depending on the event, could go in two ways: towards, identifying the consequences, which is normally done, and in a counter-current manner, backwards, identifying the causes. This is a sort of interface between event tree and fault tree logic (see Fig. 4.3.2).

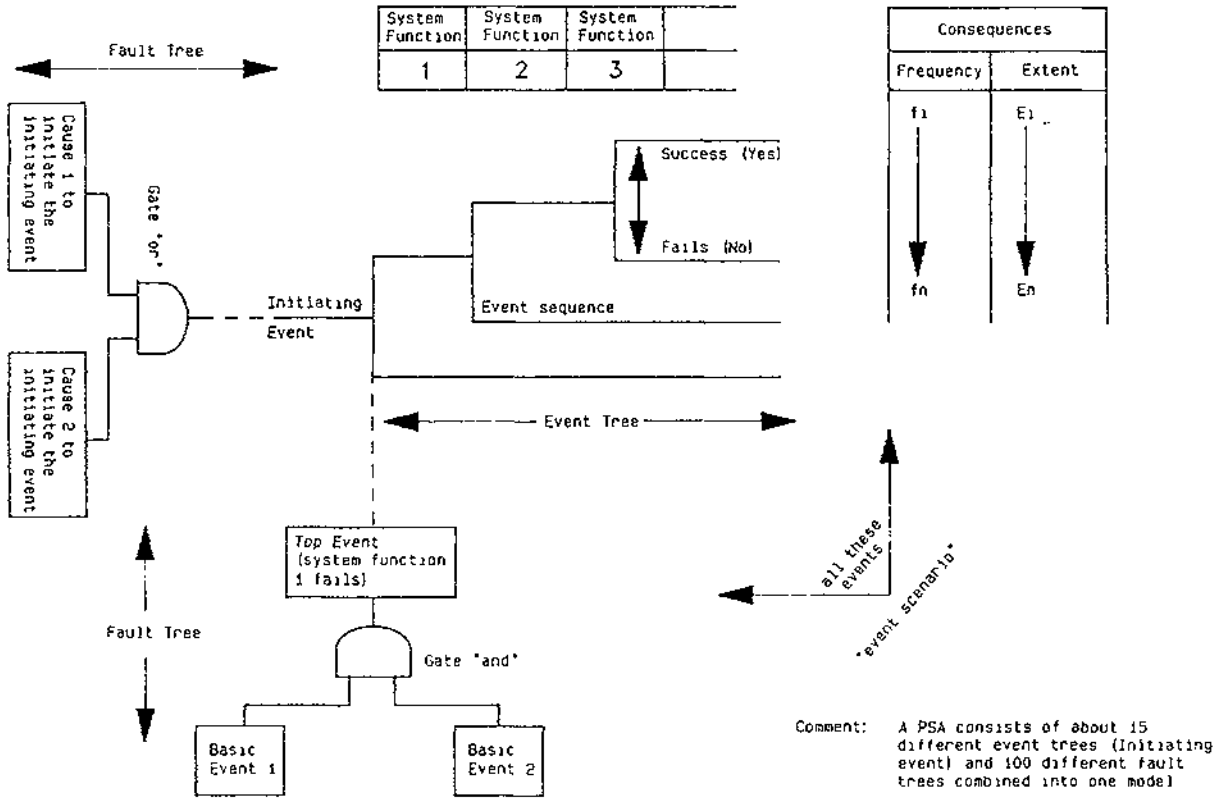


FIG. 4.3.2. Simplified PSA logic and terminology.

The typically used logic and definitions in PSA are summarized in Fig. 4.3.2. Initiating events, normally analyzed in PSA, are listed in Table 4.3.1.

- Selection of applicable PSA event trees

If the event being analyzed involves the initiating event (which is usually the case) and the initiating event is being identified in the previous step, then an applicable event tree from the PSA can be selected. Usually each of the PSA event trees covers a number of individual initiating events which are grouped in accordance with the plant response.

There is a possibility that the PSA available for the plant considered does not cover all chains making up the event sequence being analyzed. In that case a reasonable compromise is necessary in choosing an

Table 4.3.1 In PSA typically analyzed event scenarios (event trees)

Initiating Event:		
Small-break	loss of coolant accident	"LOCAs"
Medium-break	loss of coolant accident	
Large-break	loss of coolant accident	
Interfacing system	loss of coolant	
Steam line break		
Feedwater line break		
Loss of off-site power		"TRANSIENTS"
Loss of heat sink		
Station black out		
Loss of feedwater		
Anticipation transient without scram		

Comment: This list can be slightly different in the various PSAs. Additional assumption of a system function failure creates sometimes slightly modified initiating events (e.g. steam line break with steam generator heating tube rupture, loss of coolant via pressurizer relief valves).

event tree which describes the event sequence as good as possible for assessing the safety significance of occurrences.

- Overlaying the structured event sequence on the selected PSA event tree/fault tree

At this point the failed component(s) (equipment or human) should be located as basic occurrence in the fault trees for the chosen event sequence. In some cases when the component is not found in the pre-established fault trees of the plant specific PSA one can make some reasonable compromise. For example, the faulty element might be an element of a larger component (element) which is included in the PSA.

- Quantification of the event sequence

Assumed that the missing information had been provided, it would now be possible to overlay the structured event sequence on the pre-established fault tree(s)/event tree. The probability of the basic occurrences that has really happened are changed to "1" e.g. they are in a failed state during quantification. The result is then a new top event unavailability figure which reflects the plant degradation during the considered event sequence. Based on this quantification, it should be possible to identify which occurrence in the considered event sequence is quantitatively dominant. Such an identification process is normally done by using so-called importance measures (e.g. risk achievement worth, risk reduction worth, Vesely-Fussel importance, Birnbaum importance).

For assessment of the safety significance of the occurrences some important questions are listed below:

- Which PSA-type logic model(s) (e.g. cause-consequence diagram, event tree/fault tree) were used?
- Does this logic model take into account the contribution to risk of all three basic elements: personnel, procedure, equipment?
- Which risk measures were considered:
  - o risk of harm to public
  - o risk of harm to plant personnel
  - o risk of radioactive releases
  - o risk of core damage
  - o unavailability of a safety function
  - o failure probability of an operational system
  - o etc.
- If a fully quantitative assessment was done, which importance measures were used:
  - o risk achievement worth
  - o Fussel-Vesely importance
- If common mode failures were observed, which model was used in the quantitative assessment.

It should be remarked that this assessment method requires sometimes an iterative evaluation process. After identification of direct causes and root causes of the selected occurrences, it can become necessary to update the initial assessment if different assumptions were made.

4.3.5 Selection of the occurrences most significant to safety

The occurrences most significant to safety should be selected on the basis of the assessment above. Some additional questions can support this process.

- Is the selection of the occurrences most significant to safety based on criteria?
- Are there criteria for potential significance to safety?
- Are these criteria quantitative such as thresholds on margin to risk?
- Are these criteria qualitative such as level of severity (gravity scales).
- Are there criteria for actual significance to safety?
- Are these criteria quantitative such as operational limits and conditions?
- Are these criteria qualitative such as reporting criteria?
- Which is the occurrence of the highest potential significance to safety?
- What is the occurrence of the highest actual significance to safety?
- Which is the occurrence of the highest potential and actual significance to safety?
- Which occurrence was selected for in depth analysis?
- Was the occurrence selected for in-depth analysis identified on the basis of the judgement of
  - o the analyst
  - o the plant safety committee
  - o the plant management
  - o the safety authority

On which criteria was based the judgement which led to the selection

- o Impact on environment (death,injury irradiation)
- o Uncontrolled radioactive releases (I-131, gas and aerosols, liquids)
- 0 Core melting (fuel element)
- o Loss of safety functions (reactor shutdown, cooling of fuel, confinement)
- o Loss of support functions (off-site power, on-site power, cooling water, instrumentation)
- o Significant degradation of a safety system
- o Violation of operational limits and conditions (Tech. Specs).
- o degradation of fuel cladding
- o degradation of reactor coolant boundary
- o common cause or common mode failures
- o unforeseen system interaction
- o others

4.4 Conclusions on the process of selection of the occurrences to be analyzed

- Was the occurrence or the combination of the highest actual and potential significance to safety selected by the operating organization for in-depth analysis?

- If the answer is not fully affirmative, what could have enhanced the effectiveness of the selection process?

  - o better identification of all occurrences involved in the event through the establishment of thorough chronological sequence of occurrences.

  - o better understanding of the interconnection between occurrences through the establishment of a detailed logic tree of occurrences.

  - o quantitative assessment of both potential and actual significance to safety through a probabilistic approach evaluating margins to risk of occurrence of unacceptable situations.

  - o precise selection through the use of quantitative criteria for ranking the significance to safety.

5. IDENTIFICATION OF THE DIRECT CAUSE OF AN OCCURRENCE

5.1 Objectives

The objectives of the review are:

1) to provide independent identification of the direct cause of the occurrence, and

2) to assess the adequacy of the process for identifying the direct cause, as already performed at the nuclear power plant.

5.2 Preparatory work

For each selected occurrence to be investigated:

- collect and review all available documentation at the plant which can help in identifying the direct cause of the occurrence (operating and maintenance logs, drawing charts, process computer outputs, applicable administrative and task oriented procedures, work authorization documents, quality assurance manual and quality assurance procedures, personnel records, inspection records, material evidence etc.)

- collect and review all available plant procedures and analysis reports that deal with the identification of the direct cause of the occurrence

- collect list of plant personnel to be interviewed at the plant in connection with the occurrence

- collect and review past history of the plant to identify any precursors or contributors to this occurrence (equipment failure history records, incident records and analysis reports, etc.).

5.3 Investigations

For each occurrence selected for in-depth review, the following should be investigated:

- the nature of the occurrence
- the latent weakness which directly caused the deficiency
- the contributors to the existence of the latent weakness.

According to the determination of the nature of the occurrence made in section [5.3.0] methodology described in the following sections should be used:

5.3.1 Equipment deficiency
5.3.2 Personnel deficiency
5.3.3 Procedural guidance deficiency

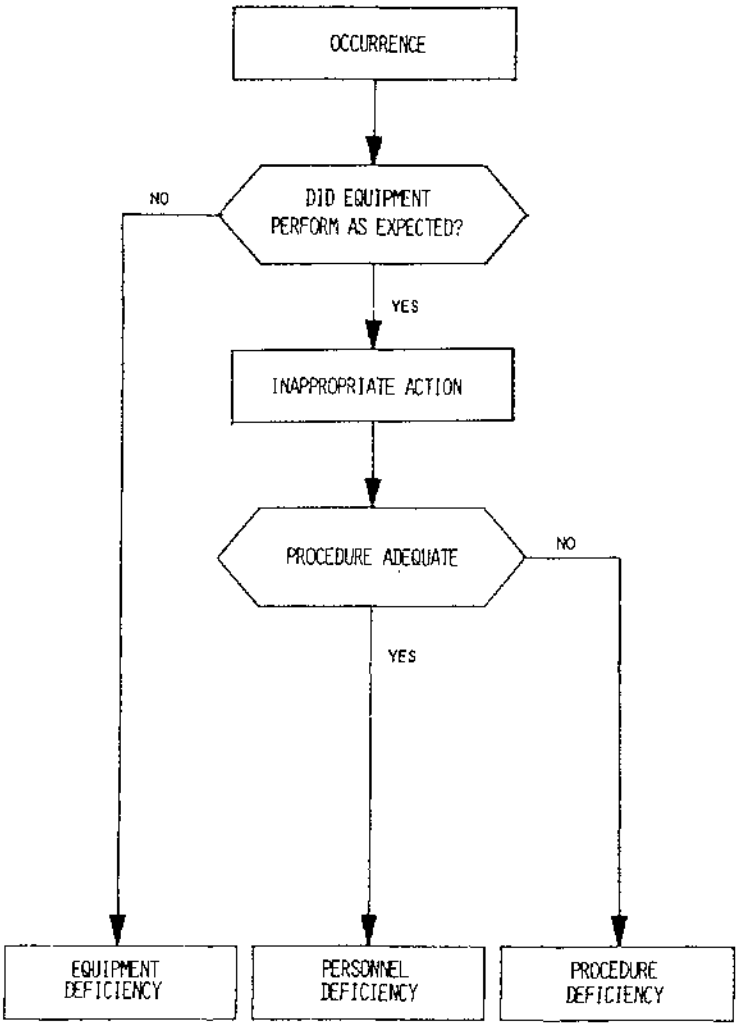
5.3.0 Identification of the nature of the occurrence

At a nuclear power plant, the activities are governed by a work process. According to the ASSET methodology, this work process has three basic elements: people, procedures and equipment. If an error arises in the performance of a work process, the reason for that error must be a deficiency in one, or several of these basic elements.

The idea of the ASSET methodology is to break up the event under investigation in logically connected occurrences which can each be attributed to a single failure of one out of those three basic elements. The nature of the occurrence, which was selected for in-depth investigation, is determined in accordance to the basic element of the work process that failed. The identification of this nature is the starting point for the investigation process of the direct cause of the occurrence.

To help the investigator in this identification process, a flowchart is provided which guides the reviewer in following an elimination process. Additional guidance at each step of this elimination process is given in sections 5.3.0.1 to 5.3.0.3 which should support and confirm the result of this process. The investigator should be aware that the proper identification of the real nature of the occurrence can be an iterative process. Further in-depth investigation of the weak aspects of the basic elements considered,

Decision making diagram for identification of
the nature of the occurrence



as performed in section 5.3.1, 5.3.2 or 5.3.3, could induce the investigator to reconsider the initially chosen nature according to this section.

5.3.0.1 Identification of operability of the equipment

To investigate the operability of the equipment involved at the time of the event, data from all available sources should be gathered and reviewed.

- Interview plant operators involved with the occurrence and have them provide their observations regarding the behaviour of the equipment before, during and after the event.

- Review all plant data and identify those that could provide insight to the equipments' behaviour (for example announciator points, computer inputs, operator's logs, recorder data, sequence of events, etc.).

- Also review the operating organization's report for the observed failure they have identified.

- Personally inspect the failed equipment, if available. When possible, inspect the location where the equipment operated in order to assimilate the operating surroundings of the equipment. View photographs and other pertinent data of the failed equipment.

5.3.0.2 Identification of the nature of the inappropriate action

If no evidence for an equipment failure can be found according to section 5.3.0.1, attention should be turned to the possibility of the involvement of an inappropriate action. This inappropriate action could be of a double nature: a performance error was committed due to the inadequacy of the procedural guidance involved, or the procedures were adequate but the individual involved made nonetheless a mistake (incorrect action or error in judgement). Guidance to the initial assessment of procedural guidance adequacy is given in section 5.3.0.3. This section helps the investigator to look for the involvement of a pure personnel deficiency. In this respect the following classification should help, which is illustrated by some non exclusive examples:

- o training deficiency
  - failing to detect situation
  - misinterpreting or improper diagnosis
  - making inadequate decisions
  - inadvertent operation of manual control
  - selecting wrong controls

- o procedure non compliance
  - failing to use procedure
  - failing to follow procedure
  - omitting steps or substeps in procedure
  - taking action not required by procedure

- failing to respect operational rules or limits
- failing to respect technical specifications
- failing to follow maintenance work request
- taking two actions at the same time

o lapse of mental attention
- forgetting to take action
- a correct action on wrong equipment
- a correct action performed at the wrong time
- using wrong procedure

To investigate personnel deficiency involvement at the time of the inappropriate action, data from all available sources should be gathered and reviewed.

- interview plant personnel involved with the occurrence and have them provide their observations regarding the sequence of events

- review all plant data and identify those that could provide insight into the nature of the considered inappropriate action (involved plant procedure, sequence of events, etc.)

- review the operating organization's report for the observed personnel deficiencies they have discovered.

5.3.0.3 Identification of adequacy of procedural guidance

To investigate the adequacy of procedural guidance at the time of the inappropriate action, data from all available sources should be gathered and reviewed.

- interview plant operators involved with the occurrence and have them provide their observations regarding the adequacy of guidance provided by the concerned procedure(s).

- review all plant data and identify those that could provide insight to the nature of appliance and the adequacy of the procedural guidance (for example: verify check off of involved procedures, review frequency of procedure revisions, computer inputs, operator's logs, recorder data, sequence of events, etc.).

- also review the operating organization's report for the observed procedure deficiencies they have identified.

- review the organization of operating and administrative procedures at the plant. Locate the procedures under investigation in this organization.

5.3.1 Identification of the direct cause of an equipment deficiency

When it is determined (in accordance with section 5.3.0) that the occurrence involved an equipment deficiency, the following should be considered in the process of identifying the direct cause of the deficiency:

1. The latent weakness in the operation of the equipment that led to its failure to perform as expected.

2. The contributors to the existence of this weakness.

Note: The assessment of the operating organization's process and results of determining the direct cause of the occurrence can be done in parallel with this effort - Section 5.4.

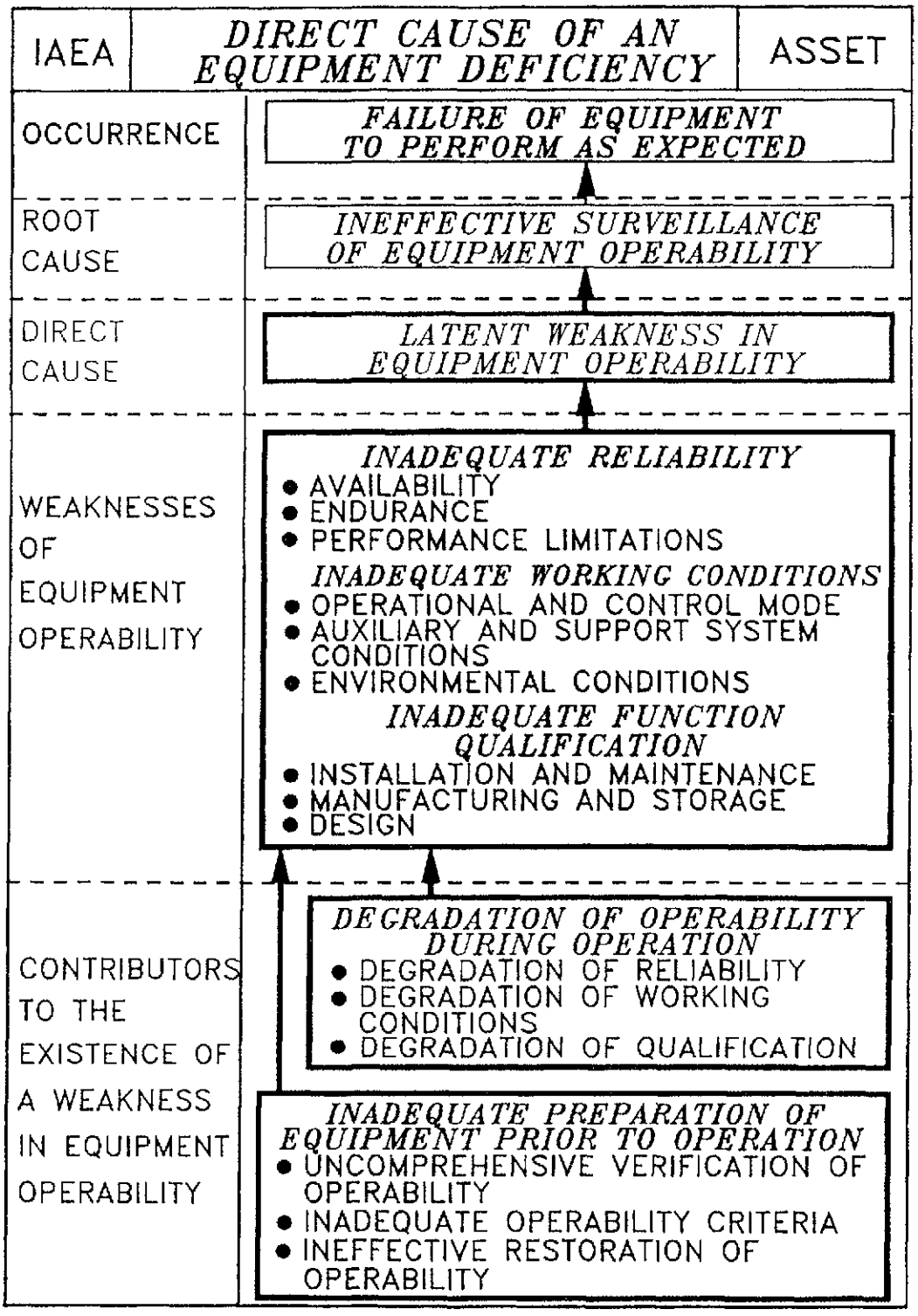
5.3.1.1 Identification of Equipment Latent Weakness

The starting point is the observed failure of the equipment. From there, proceed to find the true latent weakness that caused the failure by identifying the weak aspects of equipment operability.

5.3.1.1.1 Basic characteristics of equipment operability

For the purposes of systematic investigations of the equipment operability and the process of identification of the direct and root causes of the observed equipment failure, the following basic characteristics of equipment operability should be analyzed.

A. Reliability
   - A1. Availability
   - A2. Endurance
   - A3. Performance limitations


IAEA
DIRECT CAUSE OF AN EQUIPMENT DEFICIENCY
ASSET
OCCURRENCE
FAILURE OF EQUIPMENT TO PERFORM AS EXPECTED
ROOT CAUSE
INEFFECTIVE SURVEILLANCE OF EQUIPMENT OPERABILITY
DIRECT CAUSE
LATENT WEAKNESS IN EQUIPMENT OPERABILITY
WEAKNESSES OF EQUIPMENT OPERABILITY
INADEQUATE RELIABILITY
• AVAILABILITY
• ENDURANCE
• PERFORMANCE LIMITATIONS
INADEQUATE WORKING CONDITIONS
• OPERATIONAL AND CONTROL MODE
• AUXILIARY AND SUPPORT SYSTEM CONDITIONS
• ENVIRONMENTAL CONDITIONS
INADEQUATE FUNCTION QUALIFICATION
• INSTALLATION AND MAINTENANCE
• MANUFACTURING AND STORAGE
• DESIGN
CONTRIBUTORS TO THE EXISTENCE OF A WEAKNESS IN EQUIPMENT OPERABILITY
DEGRADATION OF OPERABILITY DURING OPERATION
• DEGRADATION OF RELIABILITY
• DEGRADATION OF WORKING CONDITIONS
• DEGRADATION OF QUALIFICATION
INADEQUATE PREPARATION OF EQUIPMENT PRIOR TO OPERATION
• UNCOMPREHENSIVE VERIFICATION OF OPERABILITY
• INADEQUATE OPERABILITY CRITERIA
• INEFFECTIVE RESTORATION OF OPERABILITY

B. External influences

B1. Auxiliary and support systems conditions

B2. Physical environment

B3. Operating practices

C. Function qualification

C1. Commissioning, maintenance and testing

C2. Manufacture, storage and installation

C3. Specification and design

5.3.1.1.2 **Weak aspects of equipment operability**

Proceed to identify the equipment weaknesses that led to its failure by reviewing for inadequacies in all aspects of equipment operability related to the basic characteristics as summarized in Section 5.3.1.1.1.

For this purpose review documentation and perform interviews of plant staff as specified in Sections 5.2 and 5.3.0.1. Additional guidance is provided by the following instructions.

A. Reliability of equipment

A1. Availability

- Check past history of equipment operating performance. Review operating logs, results of surveillance tests and maintenance records. Determine if actual equipment performance problems are identified during system start-up, shutdown, normal or emergency operations.

A2. Endurance

- Check equipment data (e.g. operation records, maintenance data, inspection records, etc.,) for any trends that indicate degradation in performance, due to aging, changes in operation or maintenance programmes, inadequacies in installations, modifications or design.

A3. Performance limitations

- Check equipment specifications against actual performance data to determine whether the equipment was operated beyond design

specifications or rating and how this operation affected the reliability (e.g. loading conditions like flowrates and pressure ranges, voltage, amperes, temperatures, etc.)

B. External influences

B1. Auxiliary and support systems conditions

- Review operating logs, maintenance records and other data associated with the performance of subcomponents and support systems and other relevant systems that could interact with failed components (e.g. auxiliary support systems like HVAC, electrical power, control power, cooling water, lub oil, instrument air, etc.; subcomponents like governers, pressure reducers, flow control valves, etc.).
  Did a degraded condition of an auxiliary or support system contribute to the equipment failure?

B2. Physical environment

- Determine if the component operating environment contribute to failure. Did uncorrected maintenance problems on components located adjacent to the failed component contribute to the failure (e.g. uncorrected steam, water and oil leaks, high temperatures, humidity, etc.) ?

B3. Operating practices

- Determine if good operating practices such as proper housekeeping, timely performance of work orders, regular in-service inspection, operation in accordance with design specification and approved procedures are established and performed.

C. Inadequate function qualification

C1. Commissioning, maintenance and testing

- Review available records to determine if the system was properly maintained and tested prior to commissioning (commissioning is the date at which the component was

originally placed in service or returned to service following an overhaul).

Determine if prior to commissioning

- o testing acceptance criteria was specified and performed
- o test results were reviewed
- o tests performed were appropriate
- o preventive maintenance requirements were specified and performed

C2. Manufacture, storage and installation

- Review available equipment documentation related to the manufacture, storage and installation of the component.

Determine if

- o inappropriate manufacturing standards were applied or improperly applied
- o material and/or fabrication deficiencies existed
- o adequate storage requirements existed to prevent degradation
- o the component was installed correctly.

C3. Specification and design

- Review available equipment documentation related to system design in order to verify:

  - o accuracy of design specifications when compared to actual operation requirements of capacity, flow, voltage, amperes, pressure temperatures, etc.

  - o compatibility of design requirements with actual working conditions like mode of operation (e.g. frequent starts, intermittent operation, variable flowrates, etc.), environment (e.g. ambient temperature, humidity, etc.) and auxiliary system support (e.g. cooling water temperatures and flow rates, system condition, etc.).

5.3.1.1.3 Conclusions on the latent weakness of the equipment

Note: If no weak aspects were identified for the equipment involved please reconsider the nature of the occurrence.

As a result of completing the review according to sections 5.3.0.1 and 5.3.1.1.2, the involvement of equipment failure can be confirmed and the weak aspects of equipment operability can be determined.

- If more than one weak aspect is identified, then consider a relative weight (based on engineering judgement) for each weak aspect according to its contribution to the failure.

- Based on the combination of these weighted weak aspects, establish the latent weakness in equipment operability.

5.3.1.2 Identification of the contributors to the latent weakness in equipment operability

The starting point of this investigation is the latent weakness identified at the conclusion of the review done in accordance with section 5.3.1.1. The end result of this review will be to establish the direct cause of the equipment failure based on the review of the following contributors to the latent weakness:

o inadequate preparation of the equipment for operation

o degradation of the equipment during operation.

5.3.1.2.1 Inadequate preparation of the equipment for operation

- Review all the contributors that affect operability of the equipment prior to its operation. Identify inadequacies in the following areas:

  o Verification of the equipment operability

  o Detection of discrepancies in the equipment operability

  o Correction of detected discrepancies

5.3.1.2.1.1 Inadequacies in verification of operability of the equipment

- Verify that records are available at the plant proving that the equipment passed successfully the test of operability prior to operation.

- Review those records and verify that the demonstration of operability deals with the basic characteristics of equipment operability as specified in section 5.3.1.1.1.

- Review the content of each specific test data regarding the weak aspects identified in operability of the equipment involved (section 5.3.1.1.2) and verify its adequacy.

5.3.1.2.1.2 Inadequacies in detection of discrepancies in equipment operability

- Verify that criteria are available at the plant to detect possible discrepancies in equipment operability prior to operation.

- Review the list and definition of the criteria related to the weak aspects identified in operability of the equipment (section 5.3.1.1.2).

  o Are the criteria adequate to ensure readiness for operation?

  o Were any discrepancies detected in the operability of the equipment involved? If so, were they forwarded to the correction process?

5.3.1.2.1.3 Inadequacies in the correction of discrepancies detected in the operability of the equipment

- Verify that procedures are available at the plant that provide guidance on correction of discrepancies detected in equipment operability.

- Review these procedures and review specifically the proposed actions undertaken regarding the weak aspects identified in operability of the equipment (section 5.3.1.1.2).

- Verify that those actions are appropriate and complete to ensure operability of the equipment.

5.3.1.2.2 Degradation of operability of the equipment during operation

Review the unforseen contributors that might degrade operability of the equipment involved. The contributors to be considered are in the area of

- Reliability of the equipment
- Working conditions of the equipment
- Function qualification of the equipment

Concentrate your effort according to the weak aspects identified in section 5.3.1.1.2.

Note: The intent here is to look for contributors which may not have been considered in the original design and operation of the equipment.

Review equipment history records and modification records, applicable operation, testing and maintenance procedures, staff history records if necessary. Review successive procedure versions. Interview plant staff on this matter.

5.3.1.2.2.1 Degradation of reliability of the equipment

- Were there any changes in operation, testing, or corrective maintenance activities that could have affected the availability, endurance, or performance of the equipment?

5.3.1.2.2.2 Degradation of working conditions of the equipment

- Were there any changes in operating procedures or personnel training that could have affected the operational mode of the equipment (e.g. continuous operation, standby, emergency operation, etc.)?

- Were there any changes in the equipment environmental conditions that contributed to degradation of the equipment during operation?

- Were there any changes in the equipments auxiliary support system conditions that could have affected equipment operation (e.g. HVAC, cooling water, tube oil, electric power, instrument air, etc.)?

5.3.1.2.2.3 Degradation of function qualification of the equipment

- Were there any adjustments or modifications that affected the installation of the equipment?

- Was the manufacturing of the equipment affected by any modification, like spare parts, specification change, etc.?

- Was the design of the equipment affected by any modifications of the equipment, its operation or testing?

5.3.1.2.3 Conclusion on the contributors to the latent weakness in equipment operability

As a result of completing the review according to section 5.3.1.2.1 and 5.3.1.2.2, the contributors to the latent weakness in the equipment operability can be determined.

- List the contributors to inadequate preparation of the equipment for operation.

- List the contributors to the degradation of equipment operability during operation.

- Consider a relative weight (based on engineering judgement) to each contributor.

5.3.1.3 Determination of the direct cause of the occurrence

Logically combine the findings of the latent weakness (conclusions in 5.3.1.1.3) and of the contributors to the latent weakness (conclusions in 5.3.1.2.3), to establish the direct cause of the occurrence.

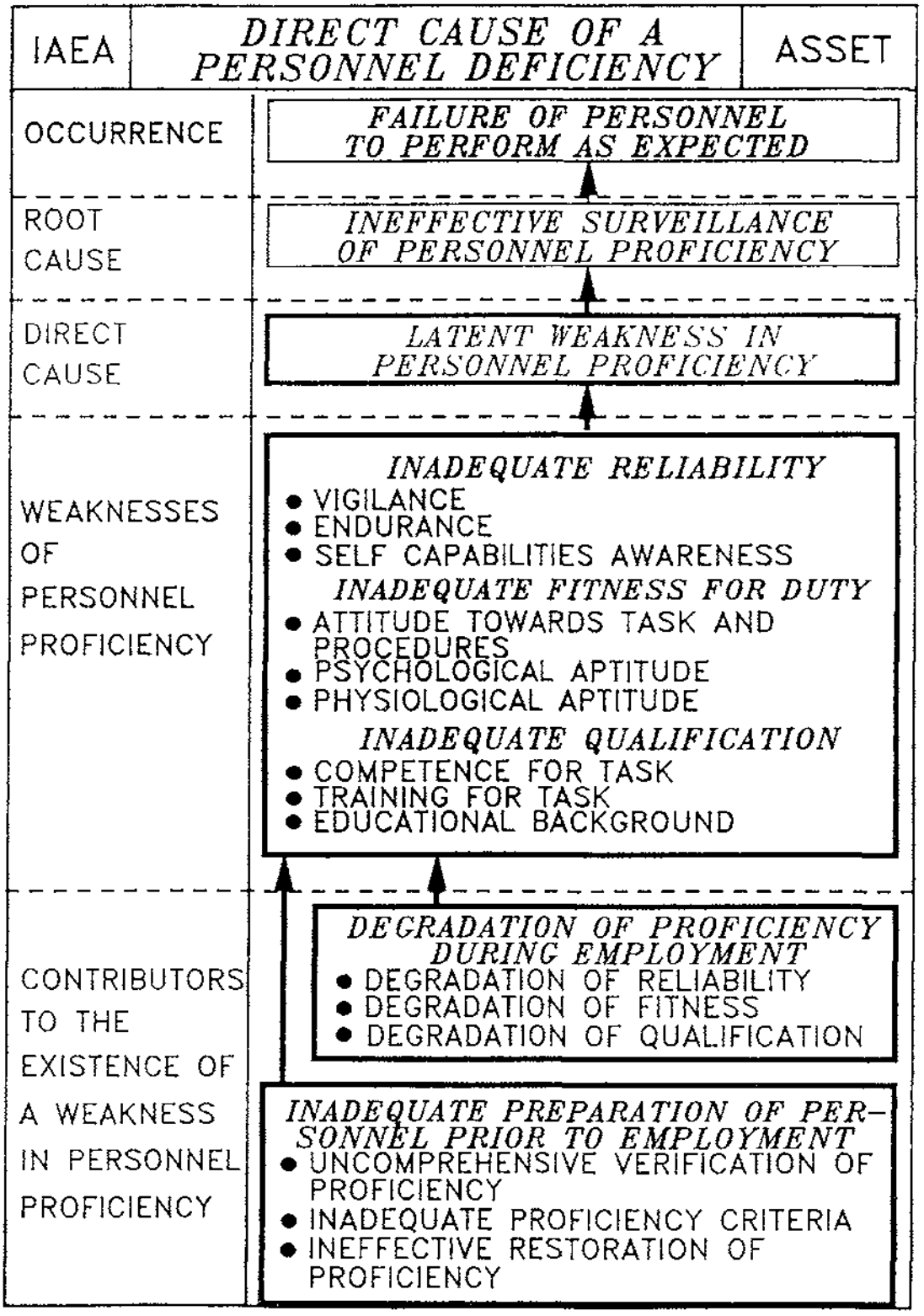
5.3.2 Identification of the direct cause of a personnel deficiency

When it is considered (in accordance with section 5.3.0) that the occurrence involved is a personnel deficiency, the following should be considered in the process of identifying the direct cause of this deficiency:

1) the latent weakness in the proficiency of the individual leading to the inappropriate action.

2) the contributors to the existence of this weakness.

Note: The assessment of the operating organization's process and results of determining the direct cause of the occurrence can be done in parallel with this effort (see section 5.4).



5.3.2.1 Identification of the latent weakness of personnel proficiency

The starting point is the observed inappropriate action for which a lack of personnel proficiency has been determined (or is suspected). From there, proceed to find the true latent weakness that caused the inappropriate action by identifying the weak aspects of the proficiency of the individual(s) involved.

5.3.2.1.1 Basic characteristics of the individual proficiency

For the purpose of the systematic investigation of the individual proficiency at work and the process of identification of the direct and root causes for the evolving inappropriate action taken by the individual, the following basic characteristics of proficiency should be analyzed.

A. Reliability at work

- A1. Vigilance
- A2. Physical and mental fitness
- A3. Self capability awareness

B. External influences

- B1. Communications
- B2. Physical environment
- B3. Safety culture

C. Qualification to perform the task

- C1. Experience
- C2. Training
- C3. Educational background

5.3.2.1.2 Weak aspects of personnel proficiency

Proceed to identify the weak aspects of the proficiency of the individual(s) involved at the time of the inappropriate action. This can be done by reviewing for inadequacies in all aspects related to the basic characteristics as summarized in Section 5.3.2.1.1. For this purpose review documentation and perform interviews of plant staff as specified in Sections

5.2 and 5.3.0.2. Additional guidance is provided by the following instructions.

A. Reliability at work

A1. Vigilance

- Check that appropriate attention was given by the operator to the situation during execution of the task, and that his attention was not distracted by other activities.

- Verify that the operator was conscious of the importance of the task and employed appropriate self-checking practices.

- Check that the individual had plant safety objectives in mind.

- Verify that the operator's vigilance was not impaired by too frequent execution of the same task.

A2. Physical and mental fitness

- Was the individual's ability impaired by any of the following factors?

  o sickness, injury, or drugs/alcohol abuse

  o stress due to personal problems

  o stress created by the job in hand, including fear of inadequate performance

  - Check that the individual's general interest in and attitude towards the task was appropriate.
  - Was the individual's performance affected by work schedule or pattern (e.g. overtime, shifts)?
  - Was the individual given a too high workload?

A3. Self capability awareness

- Verify that quality of task performance was not affected by the individual's

  - o being unconscious of his capabilities or limits
  - o reliance on co-workers and supervision
  - o underestimating complexity of task
  - o preparations to perform the task
  - o being over confident of knowledge of task and procedures
  - o being complacient about procedure usage

B. External influences

B1. Communications

- Was the individual's performance affected by a breakdown in communications, in particular:

  - Check that the initial planning requirements for the job were clearly specified to the supervisor.
  - Verify that adequate information was passed from the supervisor to the individual.
  - Check that communication errors did not occur between different individuals involved in the task.
  - Verify that any communication equipment used was in good working order.
  - Confirm that any equipment involved in providing information to the operator was in good order (e.g. instrumentation, displays, labels).

B2. Physical environment

- Did the physical and environmental condition of the workspace affect the individual's performance? Investigate the following factors:

  - o cramped or untidy area
  - o crowded and/or noisy conditions

- o prolonged exposure to high temperature or humidity
- o requirement to wear protective clothing or respiratory equipment.

- Was the potential for such problems identified and recognised?

B3. Safety culture

- Determine what managerial methods and policies are in place to ensure continued quality of operations and maintenance.

  - o are management goals and objectives clearly established and widely understood?
  - o are policies clearly defined, disseminated and enforced?
  - o does management respond to known problems and take account of input from staff?
  - o is there adequate recognition of the resource required and is this reflected in a satisfactory level of general morale?

C. Qualification to perform the task

C1. Experience

- For how long has the individual been assigned to the job?
- Has the individual performed the task before?
- How often is the individual required to perform the task?

C2. Training

- Check that the basic training provided a good general knowledge of plant, systems and physical phenomena involved.
- Verify that the individual had received training for the specific task.
- Check that this training included assessment and examination of the individual's competence for the task.
- Was the training content appropriate?

C3. Educational background

- Review standards established for selection, training and assignment of the individual to the task.

  - o Are the required standards of basic education and qualifications clearly defined for the individual's assigned post?
  - o Does the individual conform to these defined standards?
  - o Check records relating to the individual's education.

5.3.2.1.3 Conclusions on the latent weakness in personnel proficiency

Note: If no weak aspects were identified in personnel proficiency, please reconsider the nature of the occurrence.

As a result of completing the review according to sections 5.3.0.2 and 5.3.2.1.2, the nature of the inappropriate action can be confirmed and the weak aspects of personnel proficiency can be determined.

- If more than one weak aspect is identified, then consider relative weight (based on engineering judgement) for each weak aspect according to its contribution to the inappropriate action.

- Based on the combination of these weighted weak aspects establish the latent weakness in the proficiency of the individual(s) involved.

5.3.2.2 Identification of the contributors to the latent weakness in personnel proficiency

The starting point of this investigation is the latent weakness identified at the conclusion of the review done in accordance with section 5.3.2.1. The end result of this review will be to establish the direct cause

of the inappropriate action based on the identified latent weakness and the review of the following contributors to the latent weakness:

- o inadequate preparation of personnel prior to job assignment.
- o degradation of the proficiency of personnel during employment.

5.3.2.2.1 Inadequate preparation of personnel prior to job assignment

Review all contributors that affect proficiency of personnel prior to job assignment. Identify inadequacies in the following areas:

- o Verification of proficiency of personnel
- o Detection of discrepancies in the proficiency of personnel
- o Correction of detected discrepancies.

5.3.2.2.1.1 Inadequacies in verification of the proficiency of personnel

- Verify that records are available at the plant demonstrating proficiency of personnel prior to job assignment.
- Review those records and verify that the demonstration of proficiency deals with all basic characteristics of personnel proficiency as specified in section 5.3.2.1.1.
- Review the content of each specific test regarding the weak aspects identified in the proficiency of the individual involved (section 5.3.2.1.2) and verify its adequacy.

5.3.2.2.1.2 Inadequacies in detection of discrepancies in personnel proficiency

- Verify that criteria are available at the plant to detect possible discrepancies in proficiency of personnel prior to job assignment.

- Review the list and definition of the criteria related to the weak aspects of the proficiency of the individual involved as identified in section 5.3.2.1.2.

  o Are the criteria adequate to ensure sufficient proficiency before assignment to the tasks under consideration.

  o Were any discrepancies detected in the proficiency of the individual(s) involved? If so, were they forwarded to the correction process?

5.3.2.2.1.3 Inadequacies in the correction of discrepancies detected in the proficiency of personnel prior to job assignment

- Verify that procedures are available at the plant that provide guidance on correction of discrepancies in the proficiency of personnel.

- Review these procedures and review specifically the proposed actions regarding the weak aspects identified in the proficiency of the individual(s) involved (section 5.3.2.1.2). Verify that those actions are appropriate and complete to ensure proficiency of the individual(s) involved.

5.3.2.2.2 Degradation of the proficiency of personnel during employment

Review unforseen contributors that might have degraded the proficiency of the individual(s) involved. The contributors to be considered should relate to the following areas:

- Reliability at work
- Fitness for duty
- Qualification to perform the task.

Concentrate your effort according to the weak aspects identified in section 5.3.2.1.2.

Note: The intent here is to look for contributing factors which may not have been considered at the time of initial job assignment of the individual involved.

Review staff history records (such as regular medical reports and psychological tests, if available and accessible), retraining programmes and their implementation, work environment measurements. Interview plant staff on this matter.

5.3.2.2.2.1 Degradation of reliability at work

- Verify if there were any factors such as task duration, evolution in the number of tasks assigned to the individual, number of tasks to be performed at the same time, degradation of motivation to meet plant safety objectives, that could have affected the vigilance of the involved individual(s).

- Verify if there were any factors such as continuous fatigue (due to excessive workload or other reasons), change in work organization, task rescheduling or changes in work environment that could have affected the endurance of the individual(s) involved.

- Verify if there were any factors such as buildup of over-confidence, a general tendency to omit to detect alarms or to respond to alarms that could have affected the awareness of limited personal capabilities by the individual(s) involved.

5.3.2.2.2.2 Degradation of fitness for duty

- Verify if there were any factors such as degradation of motivation, duration of the same job assignment, work reorganization or rescheduling, over-confidence buildup, complacency, that could have affected the attitudes of the individual(s) involved toward job, task or procedures.

- Verify if there were any factors such as work reorganization or work rescheduling inducing insecurity (e.g. unsuccessful adaptation to introduced team work) or stress (e.g. due to work overload), communication problems with other shift personnel, appearance of social environment problems, or general loss of self-confidence for any reason, that could have affected the psychological aptitude of the individual involved to the assigned tasks.

- Verify if there were any factors such as changes in physical environment (i.e. illumination, temperature, humidity, noise, vibration, radiation, number of people in the working area; need to use respiratory equipment, anti-contamination clothing, industrial safety equipment), changes in shift - duties cycle, illnesses showing-up after initial job assignment, that could have affected the physiological aptitude of the individual involved to the assigned tasks.

5.3.2.2.2.3 Degradation of qualification to perform the task

- Verify if any factors such as task assignment, reorganization, inadequate frequency of retraining programmes, changes in social behaviour (e.g. use of alcohol, drugs), could have affected the competence of the individual involved.

- Verify that any factors such as changes in equipment, procedures, tools not properly taken into consideration in the updating process of retraining programmes could have affected the efficiency of training and retraining of the individual(s) involved.

- Verify that any factors such as introduction of new technology, lack of retraining in basic knowledge, could have affected the adequacy of the educational background of the individual(s) involved.

5.3.2.2.3 Conclusion on the contributors to the latent weakness in personnel proficiency

As as result of completing the review according to sections 5.3.2.2.1 and 5.3.2.2.2 the contributors to the latent weakness in personnel proficiency can be determined.

- List the contributors to inadequate preparation of personnel prior to job assignment.

- List the contributors to the degradation of the proficiency of personnel during employment.

- Consider a relative weight (based on engineering judgement) to each contributor.

5.3.2.3 Determination of the direct cause of the occurrence

Logically combine the findings of the latent weakness (conclusions in 5.3.2.1.3) and of the contributors to the latent weakness (conclusions in 5.3.2.2.3), to establish the direct cause of the occurrence.

5.3.3 Identification of the direct cause of a procedural guidance deficiency

When it is determined (in accordance with section [5.3.0]) that the occurrence involved is a procedural guidance deficiency, the following should be considered in the process of identifying the direct cause of this deficiency:

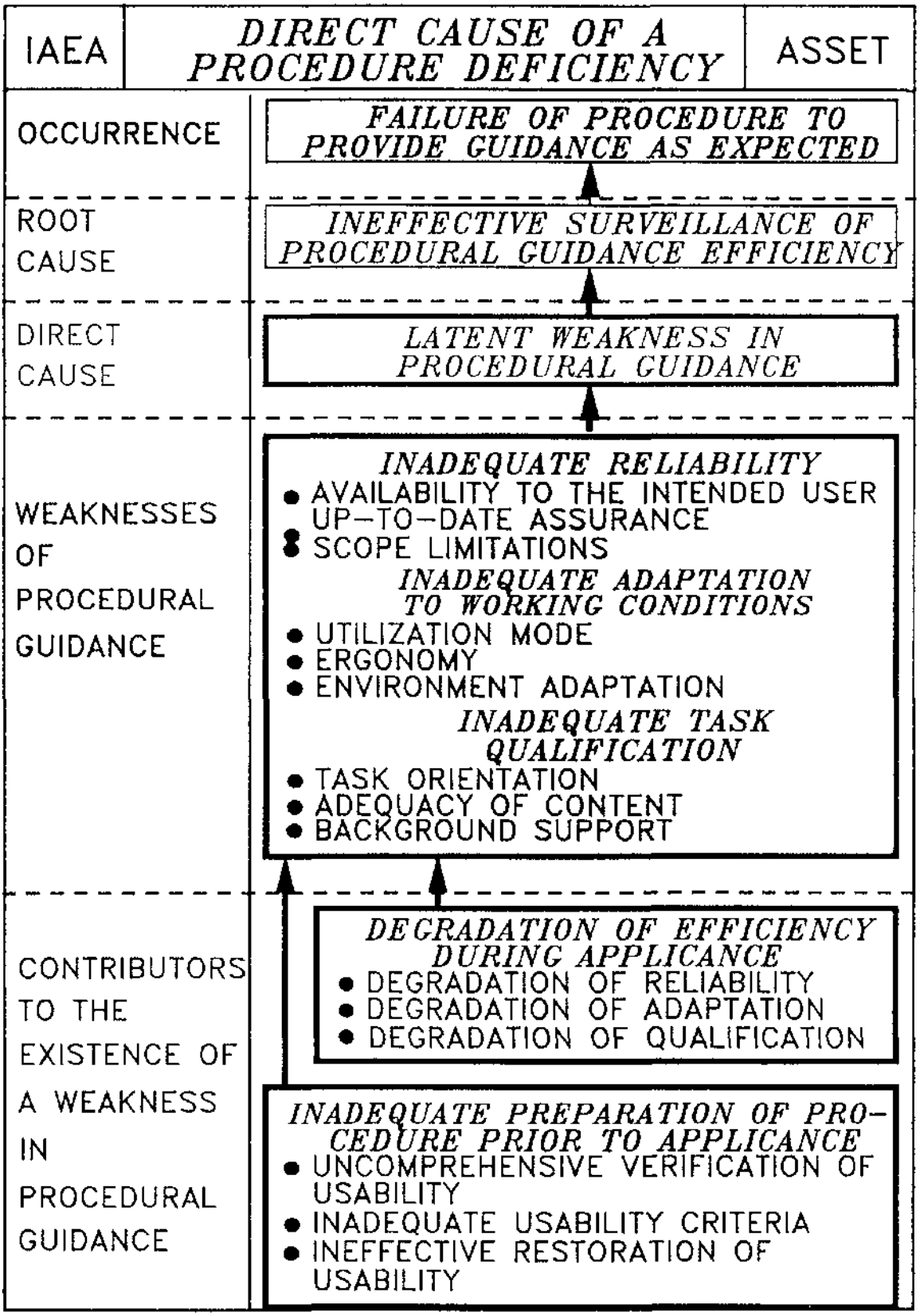
1) the latent weakness of the guidance provided by the procedure leading to the inappropriate action

2) the contributors to the existence of this weakness.

Note: The assessment of the operating organizations process and results of determining the direct cause of the occurrence can be done in parallel with this effort - see section 5.4.

5.3.3.1 Identification of the latent weakness of procedural guidance

The starting point is the observed inappropriate action for which a lack of adequate procedural guidance has been determined (or is suspected). From there, proceed to find the true latent weakness that caused the inappropriate action by identifying the weak aspects of the guidance provided by the applicable procedure(s).


IAEA
DIRECT CAUSE OF A PROCEDURE DEFICIENCY
ASSET
OCCURRENCE
FAILURE OF PROCEDURE TO PROVIDE GUIDANCE AS EXPECTED
ROOT CAUSE
INEFFECTIVE SURVEILLANCE OF PROCEDURAL GUIDANCE EFFICIENCY
DIRECT CAUSE
LATENT WEAKNESS IN PROCEDURAL GUIDANCE
WEAKNESSES OF PROCEDURAL GUIDANCE
INADEQUATE RELIABILITY
AVAILABILITY TO THE INTENDED USER
UP-TO-DATE ASSURANCE
SCOPE LIMITATIONS
INADEQUATE ADAPTATION TO WORKING CONDITIONS
UTILIZATION MODE
ERGONOMY
ENVIRONMENT ADAPTATION
INADEQUATE TASK QUALIFICATION
TASK ORIENTATION
ADEQUACY OF CONTENT
BACKGROUND SUPPORT
CONTRIBUTORS TO THE EXISTENCE OF A WEAKNESS IN PROCEDURAL GUIDANCE
DEGRADATION OF EFFICIENCY DURING APPLICANCE
DEGRADATION OF RELIABILITY
DEGRADATION OF ADAPTATION
DEGRADATION OF QUALIFICATION
INADEQUATE PREPARATION OF PROCEDURE PRIOR TO APPLICANCE
UNCOMPREHENSIVE VERIFICATION OF USABILITY
INADEQUATE USABILITY CRITERIA
INEFFECTIVE RESTORATION OF USABILITY

5.3.3.1.1 **Basic characteristics of the procedural guidance**

For the purpose of the systematic investigation of the procedural guidance efficiency and the process of identification of the direct and root causes for the evolving inappropriate action, the following basic characteristics of procedural guidance efficiency should be analyzed.

A. Reliability in appliance

A1) Availability to the intended user
A2) Up-to-date assurance
A3) Scope limitations

B. Adaptation to working conditions

B1. Utilization mode
B2. Ergonomy
B3. Environment adaptation

C. Task qualification

C1. Task orientation
C2. Adequacy of content
C3. Background support

5.3.3.1.2 **Weak aspects of procedural guidance**

Proceed to identify the weak aspects of the guidance provided by procedures at the time of the inappropriate action. This can be done by reviewing for inadequacies in all aspects related to the basic characteristics as summarized in section 5.3.3.1.1. For this purpose review documentation and perform interviews of plant staff as specified in sections 5.2 and 5.3.0.3. Additional guidance is provided by the following instructions.

A. Reliability in appliance

A1. Availability to the intended user

- Consider the complexity of the task involved and verify the nature of the procedure available to execute this task (written

or verbally communicated instructions). Is this nature in accordance to the observed complexity?

- Verify that the procedure was accessible to the intended user and clearly identified by the work authorization permit or other document.

- Verify that the applicable procedure was effectively used to perform the task.

- Verify appropriate identification information on each page of the procedure and appropriate identification of the last page.

A2. Up-to-date assurance

- Consider the task involved and verify the adequacy of the type of procedure to execute the task (permanent procedure, procedure established specifically for the task or temporary procedure).

- Check that no outdated procedure was used to perform the task. Review document control policies at the plant in this respect (is an up-to-date index of procedures available at the plant?).

- Verify that the procedure was recently reviewed (verified and validated). Check approval status of the procedure.

A3. Scope limitations

- Check presence of a clear statement on the purpose for which the procedure or instruction is intended.

- Verify that the procedure or work order clearly describes the scope of work, the boundaries of the work area, access to the work area and particular safety hazards to be avoided.

- Check presence of a clear statement on the applicability of the procedure (depending on plant status).

- Check presence of indications in the procedure of the personnel qualification needed to perform the task.

Review the document control policies at the plant.

Review the Quality Assurance manual and consistency with Quality Assurance procedures in this respect, if necessary.

Review the concerned procedure(s) with respect to the abovementioned characteristics.

Analyze the tasks to be performed, in which the inappropriate action occurred and interview involved plant personnel to judge on the adequacy of nature and type of the available procedure.

B. Adaptation to working conditions

B.1 Utilization mode

Review the procedure and verify that it was adequately designed to be used in the working conditions at the time of the event:

- Check that the procedure provides the necessary job planning information (prior action or procedures to be executed; plant, system or equipment conditions which must exist prior to use; precautions to be observed; the specific equipment to which the procedure is applicable; special tools and test equipment required; other documents required).

- Check that the procedure and user aids as well as indicated communication equipment, instrumentation and tools were adequate and adapted to the operating conditions encountered at the time of the event.

- Analyze the complexity of the tasks involved and verify if the procedure was written in accordance to this complexity, and adapted to the level of staff training.

- Verify the adequacy of the communication means as specified by the procedure, in order to coordinate the activities if two or more persons are required to perform the procedure or monitor instrumentation or alarms.

- Verify the legibility of the used procedure (poor copy) at the time of the event.

- Verify that graphs, charts, tables and data sheets were adequate for readability and interpolation or extraction of values if applicable.

- Verify that worksheets are designed to facilitate required computations if applicable.

- Verify that proper attention is paid in the procedure to aspects such as operability of redundant safety systems, requalification of affected safety related systems when returned to service, proper permission from shift supervisor to defeat or test safety systems.

- Verify appropriate procedure identification information (procedure title, revision number, page numbering).

B2. Ergonomy

Review the procedure and verify that its presentation and content is adequate to induce clear understanding and effective performance:

- Verify the adequacy of the format of the procedure (e.g. quick location of desired information, clear mechanism for conveying information and instructions)

- Verify the adequacy of reference and branching (including assessment of risk overlooking important information such as notes and cautions).

- Verify that instructions are written in short, concise, identifiable steps instead of into multiple step paragraphs.

- Verify absence of unclear or complex wording or grammar.

- Verify that presented symbols in the procedure are commonly used and were understandable to the intended user.

- Verify that necessary graphs, charts, tables and illustrations were provided and properly integrated into the procedure.

- Verify the provision of acceptance criteria and necessary formulas for calculation on data and work sheets.

- Verify that the expression of setpoint tolerance did not require performance of mental calculations.

- Verify that when quantitative acceptance criteria are used, they are stated as a range and not as a point value.

B3. Environment adaptation

Check on the material aspects of the concerned procedures, support equipment, instrumentation and tools and verify their appropriateness for the use made of them, taking into consideration all aspects of the environmental condition at the working place. When possible, inspect the location where the inappropriate action took place in order to assimilate the operating surroundings.

C. Task qualification

C1. Task orientation

Review the procedure and analyze the task involved and verify the adequacy of the procedure to guide effectively personnel in performing this task:

- Verify that separate instructions are provided.

- Verify that instructions were presented in the same sequence as the task was to be performed.

- Verify that cautionary and supplemental information was presented prior to applicable instructions.

- Verify that conditional logic words preceded the required action.

- Verify adequacy of alignment instructions when applicable (item specification and identification, position specification and verification).

- Verify the level of specificity of the procedure by reviewing the specificity of required actions, the quantification of limits and verifying that equipment or parts are completely identified.

- Verify that check-off features of successive steps are provided in the procedure.

C2. Adequacy of content

Review the procedure, Technical Specifications and other applicable reference documents and verify if the content of the procedures was technically appropriate:

- Check for inconsistencies with reference documents (other procedures, Technical Specifications, vendor manuals and recommendations, FSAR, etc.).

- Check for presence of technical inaccuracies. Check that acceptance criteria and limits are stated in quantitative terms.

- Check if relevant information was omitted such as references (drawings and other design documents, operational limits and conditions), prerequisites and precautions.

- Check that the procedure was sufficiently detailed so that the intended user could perform the procedure without obtaining additional information from persons or documents not specified by the procedure, or without obtaining direct assistance from persons not specified by the procedure.

- Verify appropriate instructions for follow-on actions upon the completion of this procedure, if applicable.

- Verify that the procedure provides instructions for reasonable contingencies (e.g. actions to take in case of out of range operation of equipment).

C3. Background support

Review the procedure and background documents and verify the consistency of the procedure with those background documents that provide the technical justifications of the process followed in performing the intended task.

5.3.3.1.3 Conclusions on the latent weakness in procedural guidance

Note: If no weak aspects were identified in procedural guidance, please reconsider the nature of the occurrence.

As a result of completing the review according to sections 5.3.0.3 and 5.3.3.1.2, the nature of the inappropriate action can be confirmed and the weak aspects of procedural guidance can be determined.

- If more than one weak aspect is identified, then consider relative weight (based on engineering judgement) for each weak aspect according to its contribution to the inappropriate action.

- Based on the combination of these weighted weak aspects, establish the latent weakness in the procedural guidance.

5.3.3.2 Identification of the contributors to the latent weakness in procedural guidance

The starting point of this investigation is the latent weakness identified at the conclusion of the review done in accordance with section 5.3.3.1. The end result of this review will be to establish the direct cause of the inappropriate action based on the identified latent weakness and the review of the following contributors to the latent weakness:

- o inadequate preparation of the procedure prior to appliance in operation.

- o degradation of procedural guidance during operation.

5.3.3.2.1 Inadequate preparation of the procedure prior to appliance in operation

Review all contributors that affect efficiency of the procedural guidance prior to its operation. Identify inadequacies in the following areas:

- o Verification of the procedural guidance [efficiency]
- o Detection of discrepancies in the procedural guidance efficiency
- o Correction of detected discrepancies.

5.3.3.2.1.1 Inadequacies in verification of the efficiency of the procedural guidance

- Verify that records are available at the plant demonstrating the [efficiency] of the procedure prior to appliance in operation
- Review those records and verify that the demonstration of efficiency deals with all basic characteristics of the procedural guidance as specified in section 5.3.3.1.1
- Review the content of each specific test regarding the weak aspects identified in the procedural guidance (section 5.3.3.1.2) and verify its adequacy.

5.3.3.2.1.2 Inadequacies in detection of discrepancies in procedural guidance efficiency

- Verify that criteria are available at the plant to detect possible discrepancies in procedural guidance efficiency prior to procedure appliance
- Review the list and definition of the criteria related to the weak aspects identified in section 5.3.3.1.2

- o Are the criteria adequate to ensure sufficient readiness for appliance?

- o Were any discrepancies detected in the efficiency of the procedure(s) involved? If so, were they forwarded to the correction process?

5.3.3.2.1.3 **Inadequacies in the correction of discrepancies detected in the efficiency of the procedural guidance prior to appliance**

- Verify that procedures are available at the plant that provide guidance on correction of discrepancies in procedural guidance efficiency

- Review these procedures and review specifically the proposed actions regarding the weak aspects identified in procedural guidance (section 5.3.3.1.2). Verify that those actions are appropriate and complete to ensure efficiency of the procedure.

5.3.3.2.2 **Degradation of efficiency of the procedural guidance during operation**

Review unforseen contributors that might degrade the efficiency of the procedural guidance involved. The contributors to be considered should relate to the following areas.

- Reliability in appliance
- Adaptation to working conditions
- Task qualification of the procedure.

Concentrate your effort according to the weak aspects identified in section 5.3.3.1.2.

Note: The intent here is to look for contributing factors which could not have been considered in the original writing or intended appliance of the procedure [at the time of initial preparation for appliance].

Review equipment history records and applicable modification records, staff history records, (administrative) procedures history records if necessary and available. Review successive procedure versions. Interview plant staff on this matter.

5.3.3.2.2.1 Degradation of reliability in appliance of the procedure

- Verify if there were any factors in operation, document control organization, task organization, procedure manipulation, staff discipline and motivation, staff training, etc, that could have affected the availability of the procedure to the intended user.

- Verify if there were any factors such as change of nature of the task (temporary instruction versus periodical task), breakdown of document control organization, breakdown in verification, validation and formal approval process of procedures, administrative staff proficiency, that could have affected the up-to-date assurance of the involved procedure.

- Verify if there were any factors in task reorganization, procedure reorganization, work area or environment modifications, task rescheduling, staff reorganization, equipment modification that could have affected the appropriateness of the orginally defined scope definition.

5.3.3.2.2.2 Degradation of adaptation to working conditions

- Verify if there were any factors in task rescheduling equipment modification, support equipment, communication equipment or tool modification, reference document modification, task reorganization, staff training that could have affected the [utilization mode] of the involved procedure.

- Verify if the successive reviewing process of the procedure in itself did not contribute to a degradation of the ergonomic aspects of the procedure.

- Verify if there were any changes in the environmental conditions in which the task had to be performed that could have affected the suitability of the procedural hardware aspects as well as the appropriateness of chosen support equipment, instrumentation and tools.

5.3.3.2.2.3 Degradation of qualification for the task

- Verify if factors such as equipment or system modifications, task reorganization or rescheduling, could have affected the adequacy of the initial orientation to the task.

- Were there any modifications in reference documents, equipment, staff training practices, task organization, task scheduling that could have affected the adequacy of the technical content of the procedure.

- Verify if any factors such as design changes, improved technical insight, experience feedback could have affected the technical justification of the procedure.

5.3.3.2.3 Conclusion on the contributors to the latent weakness in procedural guidance

As a result of completing the review according to sections 5.3.3.2.1 and 5.3.3.2.2 the contributors to the latent weakness in the procedural guidance can be determined.

- List the contributors to inadequate preparation of the procedure prior to appliance

- List the contributors to the degradation of procedural guidance efficiency during operation

- Consider a relative weight (based on engineering judgement) to each contributor.

5.3.3.3 Determination of the direct cause of the occurrence

Logically combine the findings of the latent weakness (conclusions in 5.3.3.1.3) and of the contributors to the latent weakness (conclusions in 5.3.3.2.3), to establish the direct cause of the occurrence.

5.4 Conclusions on the process of identification of the direct cause

Provide conclusions on the process followed and the results obtained by the operating organization in identifying the direct cause of an occurrence.

The review of the process was being performed in parallel with the investigation in sections 5.3.1, 5.3.2 or 5.3.3 and the conclusions of sections 5.3.1.3, 5.3.2.3 or 5.3.3.3 are the starting point for this section.

Determine if the direct cause identified by the operating organization is consistent with the conclusions reached by this review.

If discrepancies exist in this area, explain the reasons why and offer suggestions when necessary.

6. IDENTIFICATION OF THE ROOT CAUSES OF AN OCCURRENCE

6.1 Objectives

The objectives of the review are

(1) to provide independent identification of the root causes of the occurrence, and

(2) to assess the adequacy of the process for identifying root causes, as already performed at the nuclear power plant.

6.2 Preparatory work

For each selected occurrence to be investigated:

- collect and review all available documentation at the plant which can help in identifying the root causes of the occurrence (plant surveillance programme, organization and related procedures, quality restoration programme, organization and procedures, surveillance data records, etc).
- collect and review all available plant procedures and analysis reports that deal with the identification of the root causes of the occurrence.

6.3 Investigations

The starting point of the investigation of the root causes of the occurrence is the latent weakness and its contributors, which were identified as the direct cause of the occurrence in sections 5.3.1.3, 5.3.2.3 or 5.3.3.3.

For each latent weakness the following should be identified:

- the deficiency of the surveillance and/or the deficiency in the restoration of the required level of quality
- the contributors to the existence of these deficiencies addressing the management of the surveillance programme and the management of the quality restoration activities.

According to the determination of the nature of the occurrence, as established in section 5.3.0 and further confirmed by the identification of the latent weakness in that particular area in sections 5.3.1 to 5.3.3, use the methodology described in the following sections:

6.3.1 Equipment deficiency

6.3.2 Personnel deficiency

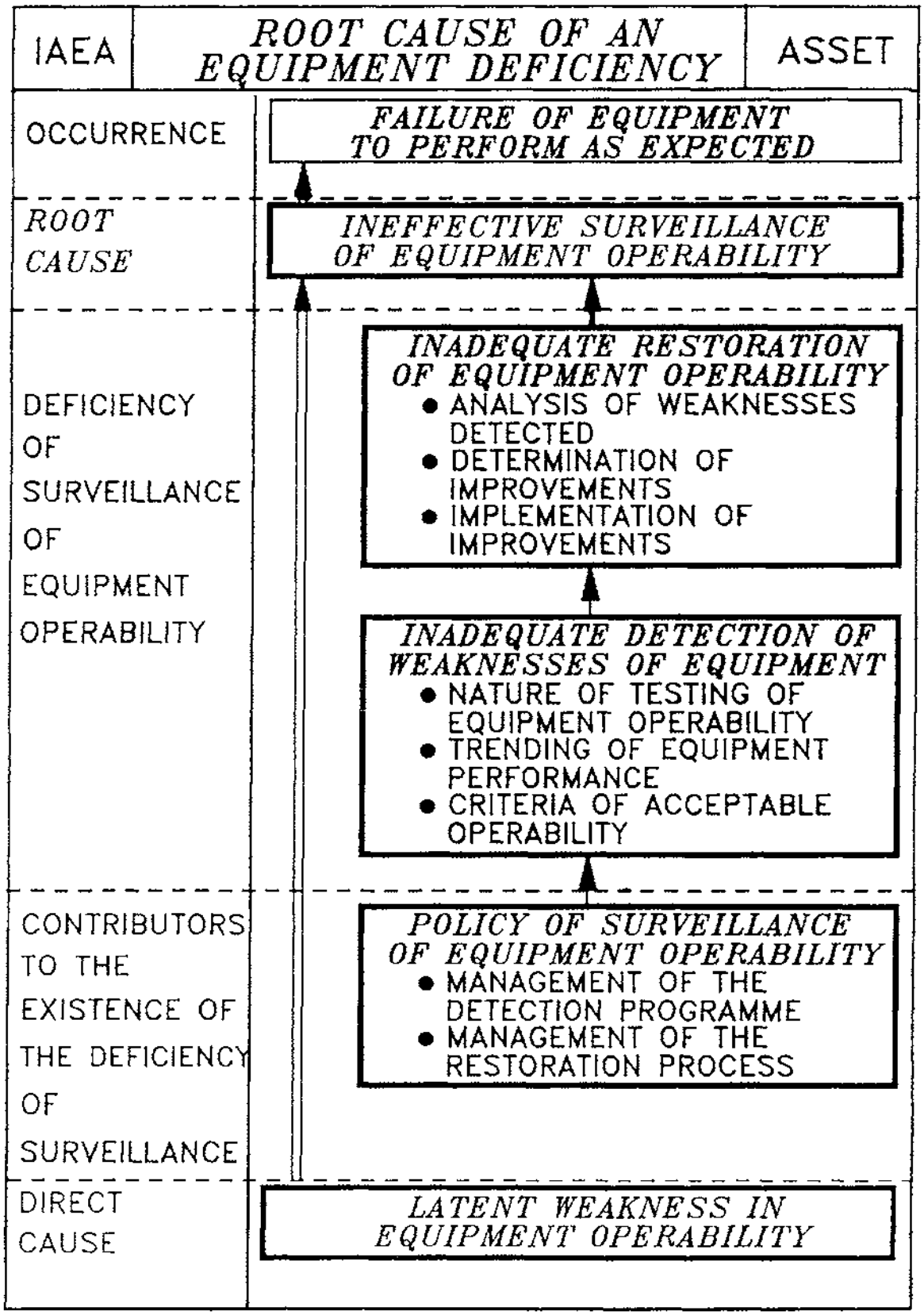
6.3.3 Procedural guidance deficiency

6.3.1 Identification of the root cause of an equipment deficiency

The starting point for this review is the latent weakness in equipment operability and its contributors identified as the direct cause of the occurrence (section 5.3.1).

This section is to guide in determining the root cause of this direct cause. The root cause is directly correlated to deficiencies in the plant equipment surveillance programme which includes the equipment, personnel, and procedures associated with equipment surveillance. The root cause gives an answer to the question why the identified latent weakness was not eliminated earlier by this surveillance programme. The root cause also includes the potential contributors to these deficiencies. Potential contributors are inadequacies in the management of the surveillance (detection) and quality restoration (correction) programmes.

Note: The assessment of the operating organization's process and results of determing the root cause of the occurrence can be done in parallel with this effort (see section 6.4).


IAEA
ROOT CAUSE OF AN EQUIPMENT DEFICIENCY
ASSET
OCCURRENCE
FAILURE OF EQUIPMENT TO PERFORM AS EXPECTED
ROOT CAUSE
INEFFECTIVE SURVEILLANCE OF EQUIPMENT OPERABILITY
DEFICIENCY OF SURVEILLANCE OF EQUIPMENT OPERABILITY
INADEQUATE RESTORATION OF EQUIPMENT OPERABILITY
• ANALYSIS OF WEAKNESSES DETECTED
• DETERMINATION OF IMPROVEMENTS
• IMPLEMENTATION OF IMPROVEMENTS
INADEQUATE DETECTION OF WEAKNESSES OF EQUIPMENT
• NATURE OF TESTING OF EQUIPMENT OPERABILITY
• TRENDING OF EQUIPMENT PERFORMANCE
• CRITERIA OF ACCEPTABLE OPERABILITY
CONTRIBUTORS TO THE EXISTENCE OF THE DEFICIENCY OF SURVEILLANCE
POLICY OF SURVEILLANCE OF EQUIPMENT OPERABILITY
• MANAGEMENT OF THE DETECTION PROGRAMME
• MANAGEMENT OF THE RESTORATION PROCESS
DIRECT CAUSE
LATENT WEAKNESS IN EQUIPMENT OPERABILITY

6.3.1.1 Weak aspects of the programme for Detection of the weaknesses in equipment operability

Review the plant equipment surveillance programme, data, procedures and practices for the detection of the identified equipment latent weaknesses.

The following items should be reviewed:

- Nature of testing of equipment operability or status.

- Trending of equipment performance.

- Acceptance criteria for operability.

6.3.1.1.1 Nature of testing of equipment operability

- Review the means used at the plant for periodic surveillance of the basic aspects of equipment operability as defined in section 5.3.1.1.1 (i.e., the complete programme, including recent test data, for monitoring equipment reliability, working conditions, and function qualification). Determine the adequacy of test frequency, parameters monitored, data accuracies, etc.

- Review the qualification of personnel in charge of the programme.

- Review if the periodic test data are properly analyzed, documented, updated and transmitted to heirarchy.

- Review methods of feedback and coordination of test results and findings.

- Determine the inadequacies in any of these above areas of review, which can be directly linked to the identified latent weakness in equipment operability.

6.3.1.1.2 Trending of equipment performance

- Review the techniques used at the plant to detect slow degradation of equipment performance in the areas of equipment reliability, working conditions, and function qualifications.

- Review if trends are used to trigger improvements in equipment performance.

- Verify the usefulness and adequacy of the program (use a set of recent trend data of the equipment under review), with special attention to the identified weak aspects in equipment operability.

6.3.1.1.3 Acceptance critera for equipment operability

- Review all acceptance criteria used in the equipment surveillance programme.

- Verify the completeness of the criteria against the equipment performance requirements of section 5.3.1.1.1.

- Verify the adequacy of the criteria corresponding to the equipment latent weakness under consideration.

6.3.1.2 Weak aspects of the programme for correction of the equipment operability

Review the plant equipment surveillance programme, procedures, and data with respect to weakness analysis, determination and implementation of corrective actions, all related to the field of equipment operability.

- Identify that provision exists for analysis of weaknesses and their contributing factors, detected by the surveillance program.

- Review the methods used for determination and implementation of corrective actions to restore the desired equipment performance.

- Verify that provision exists for testing the equipment after implementation of corrective actions.

- Verify that for the identified weakness in equipment operability and its contributors, the programme includes the above provisions of determination, implementation and testing of the corrective actions.

- Determine if the corrective actions implemented on this equipment have been adequate to prevent the possibility of recurrence of the same latent weakness (i.e.: Has the equipment experienced repeated failures of the same type?).

6.3.1.3 Conclusions on the deficiency in the equipment surveillance programme

As a result of the reviews performed according to the guidance in sections 6.3.1.1 and 6.3.1.2, the weak aspects of the detection and/or correction programmes related to equipment operability are identified.

Consider a relative weight (using engineering judgement) to each weak aspect identified.

Combine these weighted aspects to establish the deficiency of the equipment surveillance programme.

6.3.1.4 Identification of contributors to the deficiency in the surveillance of equipment operability

The starting point of this section are the findings of section 6.3.1.3 which identified the deficiency of the equipment surveillance programme.

The objective of this review is to identify those contributors (if any) that could combine with the identified surveillance deficiency, and thus provide the root cause of the equipment problem.

The contributors are related to the management of the surveillance program for detection and correction of inadequacies in equipment operability.

Both these programmes have already been reviewed for identification of weak aspects of plant surveillance for equipment operability (sections 6.3.1.1 and 6.3.1.2). Therefore, possible contributors which are under plant management control could be identified from the conclusions of those reviews. Review specifically the organizational aspects of the considered surveillance programme. Review related procedures and interview plant management in this respect. The contributors should address some major weaknesses such as:

- inadequate attention by plant-management towards the equipment surveillance programmes.

- inadequate available resources (financial, staff,...) to establish a sufficiently performing surveillance programme.

- inadequate system for coordination of the various elements of the program and between the various plant disciplines.

When the contributors are identified, consider a relative weight to each of them (based on engineering judgement).

6.3.1.5 Determination of the root cause of the occurrence

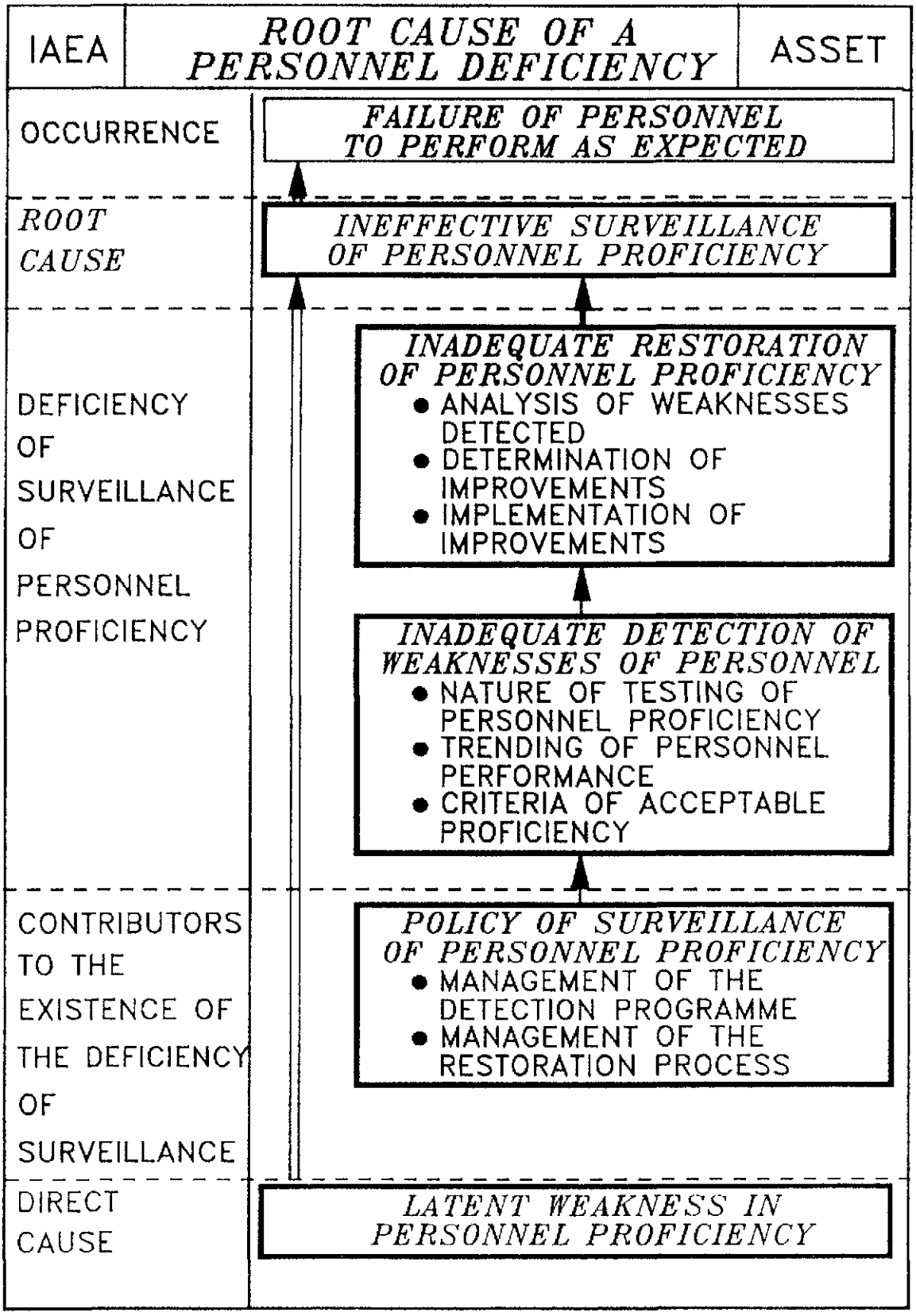
Combine the findings of 6.3.1.3 and 6.3.1.4 by establishing a logical combination of the identified deficiencies in the equipment surveillance program and any identified contributors to obtain the root cause of the latent weakness of the equipment operability under consideration.

6.3.2 Identification of the root cause of a personnel deficiency

The starting point for this review is the latent weakness in the proficiency of the individual(s) involved and its contributors, identified as the direct cause of the occurrence (section 5.3.2).

This section is to guide in determining the root cause of this direct cause. This root cause is directly correlated to deficiencies in the plant personnel proficiency surveillance programme and gives an answer to the question why the identified latent weakness was not eliminated earlier by this surveillance programme (including detection and proficiency restoration). The root cause also include the potential contributors to these deficiencies. Potential contributors are inadequacies in the management of the surveillance (detection) and proficiency restoration (correction) programmes.

Note: The assessment of the operating organization's process and results of determining the root cause of the occurrence can be done in parallel with this effort (see section 6.4).


IAEA
ROOT CAUSE OF A PERSONNEL DEFICIENCY
ASSET
OCCURRENCE
FAILURE OF PERSONNEL TO PERFORM AS EXPECTED
ROOT CAUSE
INEFFECTIVE SURVEILLANCE OF PERSONNEL PROFICIENCY
DEFICIENCY OF SURVEILLANCE OF PERSONNEL PROFICIENCY
INADEQUATE RESTORATION OF PERSONNEL PROFICIENCY
ANALYSIS OF WEAKNESSES DETECTED
DETERMINATION OF IMPROVEMENTS
IMPLEMENTATION OF IMPROVEMENTS
INADEQUATE DETECTION OF WEAKNESSES OF PERSONNEL
NATURE OF TESTING OF PERSONNEL PROFICIENCY
TRENDING OF PERSONNEL PERFORMANCE
CRITERIA OF ACCEPTABLE PROFICIENCY
CONTRIBUTORS TO THE EXISTENCE OF THE DEFICIENCY OF SURVEILLANCE
POLICY OF SURVEILLANCE OF PERSONNEL PROFICIENCY
MANAGEMENT OF THE DETECTION PROGRAMME
MANAGEMENT OF THE RESTORATION PROCESS
DIRECT CAUSE
LATENT WEAKNESS IN PERSONNEL PROFICIENCY

6.3.2.1 Weak aspects of the programme for detection of weaknesses in personnel proficiency

Review the plant surveillance programme, procedures and practices for the detection of latent weaknesses in personnel proficiency.

The following items should be reviewed:

- Nature of personnel proficiency testing
- Trending of personnel performance
- Acceptance criteria for personnel proficiency

6.3.2.1.1 Nature of personnel proficiency testing

- Check that a programme exists to monitor personnel proficiency (e.g. training record, medical checks, maintenance reports).
- Check that the programme adequately defines content, frequency of tests, qualification of examiners and a system for reporting deficiencies to management.
- Determine how the programme itself is implemented, monitored and reviewed.

6.3.2.1.2 Trending of personnel performance

- Check that the monitoring programme referred to above is also used to monitor trends.
- Review if trends are adequately brought to the attention of management.
- Check if analysis of anomalies, near-miss incidents, etc. is used to highlight degradation of personnel proficiency.

6.3.2.1.3 Acceptance criteria for personnel proficiency

- Check that a list of acceptance criteria exists for all designated duties.
- Compare these criteria with normal industry standards.

6.3.2.2 Weak aspects in restoration of personnel proficiency

- Determine if:

  - o Detected weaknesses were analyzed properly.
  - o Improvements were correctly determined.
  - o Identified improvements were implemented in a timely and effective fashion.

6.3.2.3 Conclusions on the deficiency in the personnel proficiency surveillance programme

As a result of the review performed according to the guidance in sections 6.3.2.1 and 6.3.2.2, the weak aspects of the detection and/or correction programmes related to personnel proficiency are identified.

Consider a relative weight (using engineering judgement) to each weak aspect identified.

Combine these weighted aspects to establish the deficiency of the personnel proficiency surveillance programme.

6.3.2.4 Identification of contributors to the deficiency in the surveillance of personnel proficiency

The starting point of this section are the findings of section 6.3.2.3 which identified the deficiency of the personnel proficiency surveillance programme.

The objective of this review is to identify those contributors (if any) that could combine with the identified surveillance deficiency and thus provide the root cause of the proficiency problem of the individual(s) involved.

The contributors are related to the management of the surveillance programme with respect to detection and correction of inadequacies in personnel proficiency.

Both these programmes have already been reviewed for identification of weak aspects of plant surveillance for personnel proficiency (sections 6.3.2.1 and 6.3.2.2). Therefore, possible contributors which are under plant

management control could be identified from the conclusions of these reviews. Review specifically the organizational aspects of the considered surveillance programme. Review related procedures and interview plant management in this respect.

The contributors should address some major weaknesses such as:

- inadequate attention of plant management towards the personnel proficiency surveillance programmes.

- inadequate available resources (financial, staff...) to establish a sufficiently performing surveillance programme.

- inadequate system for coordination of the various elements of the programme (documentation, reporting and experience feedback).

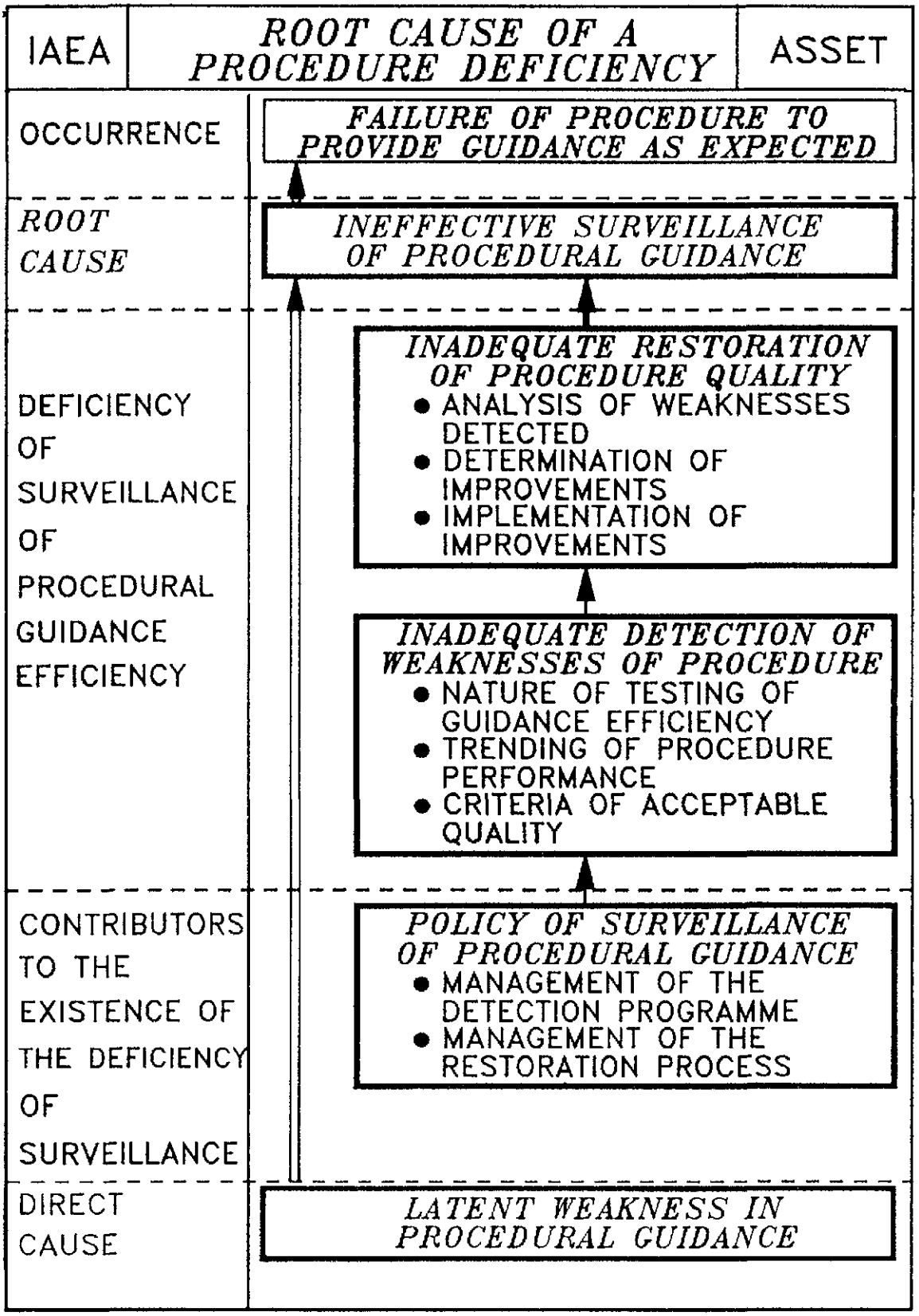
When the contributors are identified, consider a relative weight to each of them (based on engineering judgement).

6.3.2.5 Determination of the root cause of the occurrences

Combine the findings of sections 6.3.2.3 and 6.3.2.4 by establishing a logical combination of the identified deficiencies in the personnel proficiency surveillance programme and any identified contributors to obtain the root cause of the latent weakness of the proficiency of the individual(s) involved, which is under consideration.

6.3.3 Identification of the root cause of the procedural guidance deficiency

The starting point for this review is the latent weakness in procedural guidance and its contributors, identified as the direct cause of the occurrence (section 5.3.3).


IAEA
ROOT CAUSE OF A PROCEDURE DEFICIENCY
ASSET
OCCURRENCE
FAILURE OF PROCEDURE TO PROVIDE GUIDANCE AS EXPECTED
ROOT CAUSE
INEFFECTIVE SURVEILLANCE OF PROCEDURAL GUIDANCE
DEFICIENCY OF SURVEILLANCE OF PROCEDURAL GUIDANCE EFFICIENCY
INADEQUATE RESTORATION OF PROCEDURE QUALITY
• ANALYSIS OF WEAKNESSES DETECTED
• DETERMINATION OF IMPROVEMENTS
• IMPLEMENTATION OF IMPROVEMENTS
INADEQUATE DETECTION OF WEAKNESSES OF PROCEDURE
• NATURE OF TESTING OF GUIDANCE EFFICIENCY
• TRENDING OF PROCEDURE PERFORMANCE
• CRITERIA OF ACCEPTABLE QUALITY
CONTRIBUTORS TO THE EXISTENCE OF THE DEFICIENCY OF SURVEILLANCE
POLICY OF SURVEILLANCE OF PROCEDURAL GUIDANCE
• MANAGEMENT OF THE DETECTION PROGRAMME
• MANAGEMENT OF THE RESTORATION PROCESS
DIRECT CAUSE
LATENT WEAKNESS IN PROCEDURAL GUIDANCE

This section is to guide in determining the root cause of this direct cause. This root cause is directly correlated to deficiencies in the plant procedure surveillance programme and gives an answer to the question why the identified latent weakness was not eliminated earlier by this surveillance programme (including detection and quality restoration). The root cause also includes the potential contributors to these deficiencies. Potential contributors are inadequacies in the management of the surveillance (detection) and quality restoration (correction) programmes.

Note: The assessment of the operating organization's process and results of determining the root cause of the occurrence can be done in parallel with this effort (see section 6.4).

6.3.3.1 Weak aspects of the programme for detection of weaknesses in procedural guidance

Review the plant procedure surveillance programme, procedures and practices for the detection of latent weaknesses in procedural guidance.

The following items should be reviewed:

- Nature of testing (verification) of the efficiency of procedural guidance
- Trending of procedural guidance performance
- Acceptance criteria for procedural guidance efficiency.

6.3.3.1.1 Nature of testing the efficiency of procedural guidance

- Review the means used and the approach at the plant for periodic surveillance of the basic characteristics of procedural guidance as defined in section 5.3.3.1.1 (i.e. the complete programme, including test records, for monitoring procedural guidance reliability in appliance, adaptation to working conditions and task qualification).
- Determine the adequacy of test (verification) frequency.

- Assess the adequacy of support tools (including simulators) and of personnel, used to perform the tasks as described in the procedure, in this verification process.

- Review the qualification of personnel in charge of the programme.

- Review if the findings of periodic procedure verifications are properly checked, documented and transmitted to hierarchy.

- Review methods of feedback and coordination of verification findings.

- Determine the inadequacies in any of these above areas of review, which can be directly linked to the identified latent weakness in the procedural guidance.

6.3.3.1.2 **Trending of procedural guidance performance**

- Review the techniques used at the plant to detect slow degradation of procedural guidance performance in the areas of procedural guidance reliability, adaptation to working conditions and task qualification.

- Review if trends are used to trigger improvements in procedural guidance performance.

- Verify the usefulness and adequacy of the trending programme with special attention to the identified weak aspects in procedural guidance.

6.3.3.1.3 **Acceptance criteria for procedural guidance efficiency**

- Review all acceptance criteria used in the procedural guidance surveillance programme.

- Verify the completeness of the criteria against the procedural guidance performance requirements of section 5.3.3.1.1.

- Verify the adequacy of the criteria corresponding to the procedural guidance latent weakness under consideration.

6.3.3.2 Weak aspects of the programme for restoration of the quality level of procedural guidance

Review the plant procedure quality restoration programme, procedures and practices with respect to weakness analysis, determination and implementation of corrective actions, all related to the field of procedural guidance.

- Identify that provision exists for analysis of weaknesses and their contributing factors, detected by the plant surveillance programme.

- Review the available means and methods used for the determination and implementation of corrective actions to restore the desired level of quality of procedural guidance.

- Verify that provision exists for testing the procedures after implementation of corrective actions (validation process).

- Verify that for the identified weakness and its contributors in procedural guidance, the programme includes the above provisions of determination, implementation and validation of the corrective actions.

- Determine if the corrective actions implemented into the considered procedures have been adequate to prevent the possibility of recurrence of the same or similar inappropriate actions.

6.3.3.3 Conclusions on the deficiency in the procedural guidance efficiency surveillance programme

As a result of the review performed according to the guidance in sections 6.3.3.1 and 6.3.3.2, the weak aspects of the detection and/or correction programmes related to procedural guidance efficiency are identified.

Consider a relative weight (using engineering judgement) to each weak aspect identified.

Combine these weighted aspects to establish the deficiency of the surveillance programme for procedural guidance efficiency.

6.3.3.4 Identification of contributors to the deficiency in the surveillance of procedural guidance efficiency

The starting point of this section are the findings of section 6.3.3.3 which identified the deficiency of the procedural guidance efficiency surveillance programme.

The objective of this review is to identify those contributors (if any) that could combine with the identified surveillance deficiency and thus provide the root cause of the procedural guidance problem.

The contributors are related to the management of the surveillance programme with respect to timely detection and correction of inadequacies in procedural guidance.

Both these programmes have already been reviewed for identification of weak aspects of plant surveillance related to procedural guidance (sections 6.3.3.1 and 6.3.3.2). Therefore possible contributors which are under plant management control could be identified from the conclusions of these reviews. Review specifically the organizational aspects of the considered surveillance programme. Review related procedures and interview plant management in this respect.

The contributors should address some major weaknesses such as:

- inadequate attention by plant management towards the procedural guidance efficiency surveillance programme (lack of safety culture).

- inadequate available resources (financial, staff, ...) to establish a sufficiently performing surveillance programme (including detection and correction of weaknesses).

- inadequate system for coordination of the various elements of the programme (documentation, reporting and experience feedback).

When the contributors are identified, consider a relative weight to each of them (based on engineering judgement).

6.3.3.5 Determination of the root cause of the occurrence

Combine the findings of sections 6.3.3.3 and 6.3.3.4 by establishing a logical combination of the identified deficiencies in the procedural guidance surveillance programme and any identified contributors to obtain the root cause of the latent weakness of the procedural guidance under consideration.

6.4 Conclusions on the process of identification of the root cause

Provide conclusions on the process followed and the results found by the operating organization in identifying the root cause of the occurrence.

The review of the process and results were being done in parallel with sections 6.3.1 to 6.3.3 and the conclusions in sections 6.3.1.5 to 6.3.3.5 are the starting point of this section.

Determine if the root cause obtained by the operating organizations review is consistent with the conclusions of this investigation (sections 6.3.1.5, 6.3.2.5 or 6.3.3.5).

If discrepancies are identified explain the reasons for them and offer suggestions as necessary.

7. DETERMINATION OF CORRECTIVE ACTIONS

7.1 Objectives

The objectives of this review are:

(1) to provide independent identification of the needed corrective actions, and

(2) to assess the adequacy of corrective actions, as already performed at the nuclear power plant.

7.2 Preparatory work

Review direct and root causes, as identified in accordance to sections 5 and 6, for the selected occurrences under investigation.

Review the sections of the analysis report of the event under investigation dealing with corrective actions.

7.3 Investigations

The starting point of the determination of the necessary corrective actions is

(a) the latent weaknesses and their contributors, which were identified as the direct causes of the selected occurrences in accordance to sections 5.3.1.3, 5.3.2.3 and 5.3.3.3.

(b) the deficiencies in the surveillance programmes and their contributors, which were identified as the root causes of the selected occurrences in accordance to sections 6.3.1.5, 6.3.2.5 and 6.3.3.5.

The purpose of this investigation is threefold:

(1) to eliminate the actual consequences of the event.

(2) to restore the level of quality required for the deficient basic elements involved (i.e. equipment operability, personnel proficiency and procedural guidance).

(3) to prevent that any degradation of this level of quality will result in future recurrence of the occurrences under investigation or similar occurrences.

Note: The assessment of the operating organization's process and results of determining corrective actions can be done in parallel with this effort (see section 7.4).

7.3.1 Elimination of the actual consequences of the event

The starting point is the determination of the observed actual consequences of the event under investigation. Review the narrative description of the event in this respect and interview plant personnel.

Review and assess immediate actions taken by plant staff to restore the plant operating conditions during or shortly after the reported event, addressing the actual consequences.

7.3.2 Restoration of the level of quality of the deficient basic elements

The starting point is the latent weakness and their contributors which were identified as direct causes of the set of occurrences, selected for in-depth investigation.

The purpose of this investigation is twofold:

(1) to determine corrective actions that remove the latent weakness of the basic elements (equipment, personnel, procedures) which failed.

(2) to determine corrective actions that address or consider the identified contributors to the existence of those latent weaknesses.

By implementing these corrective actions, the required level of quality of the basic elements under consideration (equipment operability, personnel proficiency, procedural guidance) is restored in the short term.

Review the corrective actions planned or implemented at the power plant to eliminate the identified latent weakness of each basic element which failed to perform as expected during the event.

Verify that corrective actions (planned or implmeneted) take all identified contributors to the latent weakness into consideration:

- verify that any inadequacy of preparation prior to equipment operation, job assignment of personnel or procedure field appliance is corrected.

- verify that any reason for degradation of equipment operability during operation, of personnel proficiency during employment or of procedural guidance during in field appliance is appropriately identified and corrected.

Review the implemented corrective actions in retrospect, in order to assess their efficiency in restoring the required level of quality of the basic elements involved.

Make suggestions for further improvements if this quality is not restored to full satisfaction.

7.3.3 Prevention of recurrence

The starting point is the deficiencies of the surveillance programmes and their contributors which were identified as root causes of the set of occurrences, selected for in-depth investigation.

The purpose of this investigation is twofold:

(1) to determine corrective actions that remove the deficiencies of the plant surveillance programmes which failed to detect and/or restore in a timely manner the latent weakness of the basic elements involved (equipment, personnel, procedures).

(2) to determine corrective actions that address the identified contributors to the existence of those deficiencies.

By implementating these corrective actions, the required level of quality of the basic elements under investigation (equipment operability, personnel proficiency and procedural guidance) is maintained in the long term. By detecting and restoring in a timely manner any minor degradation in

quality, major degradations can be avoided resulting in a prevention of recurrence of the observed or similar occurrences.

Review the corrective actions planned or implemented at the power plant to eliminate the identified deficiencies of the plant surveillance programmes for each basic element which failed to perform as expected during the event (detection programmes and restoration process).

Verify corrective actions planned and implemented that address the contributing factors to the existence of those deficiencies. Verify if aspects of management of the plant surveillance programme (including management of the detection programme and the restoration process) were considered and that corrective actions were taken to improve management control.

Review implemented corrective actions in retrospect in order to assess their efficiency in maintaining the required level of quality of the basic elements involved.

Make suggestions for further improvements if this quality was not maintained to full satisfaction.

7.4 Conclusions on implemented corrective actions

Provide conclusions on the process followed and the solutions found by the operating organization in determining the necessary corrective actions to:

- eliminate the actual consequences of the event.
- restore the level of quality required for the deficient basic elements involved.
- maintain that quality and prevent any degradation resulting in recurrences.

Assess the appropriateness and completeness of these corrective actions planned and implemented.

Review of the process and solutions was being performed in parallel with the investigations in section 7.3.

8. GENERIC LESSONS AND SUGGESTIONS FOR THE ENHANCEMENT OF THE POLICY OF PREVENTION OF INCIDENTS

8.1 Objectives

The objectives of this review are:

(1) to draw generic lessons and identify good practices from the review of the population of events under investigation, and

(2) to assess the policy of prevention of incidents at the nuclear power plant.

8.2 Preparatory work

Review corrective actions implemented at the nuclear power plant following the events under investigation, as identified in accordance to section 7.

Review actions undertaken by the regulatory body as a result of the events under investigation.

Review suggestions made in accordance to sections 7.3.2 and 7.3.3 for all events under investigation.

Collect and review the documents available at the plant related to the policy of prevention of incidents.

8.3 Generic lessons and good practices

The starting point is the result of the review of

(a) the corrective actions implemented at the nuclear power plant as a result of an analysis of direct and root causes of the events under investigation.

(b) the actions taken by the regulatory as a follow up on those events.

(c) additional corrective actions suggested in section 7.

Draw generic lesson and identify good practices that are of interest to the nuclear community from the actions undertaken by both the operating organization and the regulatory body.

These generic lessons should address the following fields:

- actions of improvement of preparation prior to equipment operation, personnel job assignment and procedure field appliance.

- actions of mitigating degradation of quality of equipment, personnel and procedures.

- actions to improvement of detection capabilities of any quality degradation.

- actions to improve timely restoration of the level of quality of each of the basic elements (equipment, personnel, procedures).

- any other action taken by the operating organization or the regulatory body of general interest.

8.4 Suggestions for further enhancement of the policy of prevention of incidents

The starting point is the result of the review of suggestions made to improve the level of quality of deficient basic elements and to maintain that level of quality during future operation of the nuclear power plant. These suggestions were the result of the assessment of corrective actions planned or implemented by the operating organization following the events under investigation.

Determine the weak points of the plant policy of prevention of incidents and offer suggestions for enhancement of this policy in view of achieving the required level of quality for all basic

elements involved in nuclear power plant operation (i.e. equipment, personnel and procedures):

- by adequate preparation prior to operation, assignment or appliance of those basic elements (quality assurance programme).

- by mitigation of all contributors susceptible of leading to degradation of the level of quality reached prior to operation (quality maintenance programme).

- by establishing a powerful detection programme capable of detecting in a timely manner any potential degradation of the level of quality.

- by establishing an accurate restoration programme capable of prompt correction of any latent weakness detected.

9. OUTLINES OF THE FINAL ASSET REPORT

NENS/ASSET 90/
ORIGINAL: ENGLISH

INTERNATIONAL ATOMIC ENERGY AGENCY

REPORT OF THE

A S S E T

(ASSESSMENT OF SAFETY SIGNIFICANT EVENTS TEAM)

MISSION

AT THE

(NAME) NUCLEAR POWER PLANT

COUNTRY?

DATE?

IAEA-NENS/ASSET/ /

PREAMBLE

This ASSET Report presents the results of the IAEA Assessment of Safety Significant Events Team (ASSET) investigations carried out on the operational events reported on (PLANT) during (YEARS) at the (NAMES) nuclear power plant located in (COUNTRY). The results, conclusions and suggestions presented herein reflect the views of the experts carrying out the investigation. They are provided for consideration by the responsible (COUNTRY) authorities. The ASSET views contained in this report are based on the documentation made available by the operating organization concerned, on oral communical with plant personnel, and promote enhancement of (PLANT) operational safety by addressing the policy of prevention of incidents.

Distribution of the ASSET report is left to the discretion of the Government of (COUNTRY); this includes the removal of any initial restriction. The IAEA makes the report available only with the express permission of the Government of (COUNTRY).

Any use of or reference to the views expressed in this report that may be made by the competent (COUNTRY) organizations is solely their responsiblity.

Foreword by the Director General

The IAEA Assessment of Safety Significant Events Team (ASSET) programme assists Member States by advising them on ways of enhancing operational safety through an effective policy of prevention of incidents at nuclear plants. Although good design, manufacture and construction are pre-requisites, safety ultimately depends on the ability of operating personnel and the attitude and conscientiousness with which they carry out their responsibilities. ASSET missions focus on these aspects when assessing the policy of prevention of incidents in comparison with those used successfully in other countries and when exchanging, at the working level, ideas for improving its effectiveness.

An ASSET mission is undertaken on request of operating or regulatory organizations of a Member State and is not a regulatory type of inspection to determine compliance with national requirements. However, an ASSET review can complement national efforts by providing an independent, international assessment that may identify areas for potential improvement which may have been overlooked.

An ASSET mission affords an opportunity for ASSET members and operating personnel to exchange knowledge and experience, to update the knowledge of regulatory personnel of the host country assigned to follow the ASSET review, and to train personnel through observation of the experts involved in the ASSET review process. This can contribute to the attainment of an international standard of excellence for the prevention of incidents, not through regulatory requirements, but through an exchange of information on, and voluntary acceptance of, successful efficient practices.

The IAEA Safety Series document, including the Nuclear Safety Standards (NUSS) for nuclear power plants and the Basic Safety Principles for Nuclear Power Plant (Safety Series No.75-INSAG-3) and the expertise of the ASSET members themselves, form the point of departure for an ASSET review. The ASSET review is performed according to a detailed and systematic methodology which ensures thoroughness of the analysis for identification of the root causes and determination of appropriate corrective actions.

The scope of an ASSET review is tailored to the specific needs of the particular facility. Depending on individual needs, the ASSET review concentrates on areas of special interest for the development of the plant management policy related to the prevention of incidents at Plants.

In formulating their views, the ASSET members discuss their observations with their utility counterparts and consider further comments made by the other team members. They record their observations and conclusions to prepare for their oral presentation at the concluding meeting with utility and regulatory management. These notes are also input to the ASSET Report highlighting the more significant matters for utility response, which is prepared after completion of the ASSET mission and submitted to the hosting organization through official channels.

The ASSET Report conveys the conclusions of the mission and the proposals for improvement to the operating organization, which review and analyses them in order to determine what further actions may be appropriate. The proposals made may carry different weights. Their substance rather than their number determines their contribution to the operational safety improvement process. Response priorities may be indicated by the operating organizations. No assessment of the plant's overall safety status is made, however.

WORKING SESSION OF THE IAEA
ASSESSMENT OF SAFETY SIGNIFICANT EVENTS TEAM
AT THE NUCLEAR POWER PLANT

DATES

CONTENT OF THE REPORT

I. INTRODUCTION

At the invitation of the Government of (COUNTRY) [the operating organization (COMPANY)] the IAEA Assessment of Safety Significant Events Team (ASSET) held its (COUNTING NUMBER) working session at the (NAME) Nuclear Power Plant, (COUNTRY) from to 19 .

The objective of this session was to provide an assessment of plant operational safety regarding policy of prevention of incidents at (PLANT).

The scope of the ASSET mission was defined as follows:

+ To review the operational events reported in (DATES) in Units and to provide conclusions on significance, causes, implemented corrective actions and generic lessons.

+ To deeply analyze (NUMBER) events significant to safety and to provide conclusions on the appropriateness and completeness of corrective actions:

  1) EVENT TITLE

  2) EVENT TITLE

  3) EVENT TITLE

The task was carried out jointly by (PLANT) staff and external experts members of the ASSET according to the systematic analysis methodology developed by the IAEA for the ASSET programme. The IAEA team was composed of (NUMBER) participants specifically recruited for their long experience of nuclear power plant operation in different countries, their knowledge of analytical techniques and their sensitivity to the importance of human contribution to incidents.

The Company

Owner of the Plant?

Operator?

Number of plants operated by the company?
(Type, power, etc....)?

The Nuclear Power Plant

Location?

Situation of the plant in the local environment?

History of Operation

- Diagram of operation?

- Total production and capacity factor?

- Main problems encountered and corrective actions implemented?

- Present situation of plant?

The ASSET Approach

The ASSET approach is based on the following:

EVENTS (PROBLEMS, INCIDENTS OR ACCIDENTS) occur always because of a

FAILURE (OCCURRENCE) to perform as expected due to a

LATENT WEAKNESS (DIRECT CAUSE) [preparation and maintenance] which was not promptly eliminated due to

SURVEILLANCE DEFICIENCIES (ROOT CAUSE) [Detection and Restoration] on quality of equipment, personnel or procedures.

As the primary goal of any operating organization is to strive for safe and reliable operation, the main concern of the ASSET approach is therefore the effectiveness of the incident prevention policy at nuclear power plants visited.

The ASSET approach is based on commonly shared principles, as outlined for example in Safety Series document No.75-INSAG-3 Basic Safety Principles. Safe operation and good performance at nuclear power plants require basic elements of high standard: proficient personnel, operable equipment and useable procedural guidance.

The ASSET recognises that personnel, equipment or procedures should not necessarily be held responsible for not performing as expected during on-line operation. Incidents may demonstrate only that these basic elements were poorly prepared, maintained or restored to ensure safe and reliable operation. Plant management control is decisive, and human performance is crucial in the carrying out of important off line activities such as:

- Careful preparation of personnel, equipment and procedures prior to plant operation, through an effective plant quality assurance programme.
- Prevention of any degradation of the level of quality of personnel, equipment and procedures during plant operation through an effective plant maintenance programme.
- Timely identification of any latent weakness or degradation of quality of any of these three elements, by use of an effective detection programme; and
- Prompt correction of weaknesses detected through an effective restoration process.

The ASSET systematic analytical methodology

The events selected are reviewed according to the ASSET guidelines and the ASSET operating instructions provide both, practical guidance for dismantling the mechanism of events and consistent basis for conclusions on a population of events.

The ASSET investigation is carried out according to the 7 following steps:

1. **Description and significance of the event:**

   How was the event detected? What were the consequences and the actions taken? What is the actual and potential significance of the event?

2. **Selection of the occurrences to be analysed:**

What is the occurrence or the combination of occurences most significant to safety in the sequence of the event?

3. **Identification of the direct cause:**

What was the latent weakness which was affecting the element (personnel, equipment or procedure) that failed to perform as expected?

4. **Identification of the root cause:**

Why was the latent weakness (of the element which failed to perform as expected) not eliminated earlier by the plant surveillance (detection or restoration) programme?

5. **Determination of the corrective actions:**

What are the areas of improvements and the corrective actions needed to enhance both, quality and surveillance of quality, of the element which failed to perform as expected?

6. **Generic lessons:**

What are the generic lessons learned for further enhancement of prevention of incidents?

7. **Suggested actions plan:**

What are the specific actions that are suggested for implementation to enhance safe operation? What are the alternatives and the schedule for implementation?

II. REVIEW OF THE OPERATIONAL EVENTS REPORTED IN 19 , 19 IN UNITS

2.1 Description and conclusions on significance of the events

2.1.1 Conclusions on the reporting criteria

- o Nature and requirements of the operating and regulatory organizations

2.1.2 Description of the population of events

- o Nature of events
- o Number of events
- o Recurrence of events

2.1.3 Conclusions on the significance to safety of the operational events selected

- o use the international severity scale for this assessment (see definitions)
- o conclusions on events below or out of scale
- o conclusions on event categorized in scale (to be selected for the review)

2.1.4 Conclusions on consequences of the operational events selected

- o off-site impact
- o on-site impact
- o in-depth defence degradation

2.1.5 Conclusions on immediate actions taken related to the operational events selected

- o immediate actions taken
  - + to interrupt the sequence of the event
  - + to restore safety
- o final status of the plant

2.2 Conclusions on the occurrences (failures) that led to the safety significant events selected

2.2.1 Conclusions on Equipment failures

2.2.2 Conclusions on Personnel failures

2.2.3 Conclusions on Procedure failures

2.3 Conclusions on the direct causes of the significant events selected

2.3.1 Conclusions on the latent weakness which were affecting personnel, equipment or procedure when they failed to perform as expected.

- + Were the latent weaknesses identified in all cases?
- + Were they related to a problem:
  of reliability in operation?
  of fitness to specific working conditions?
  of qualification for the task?

2.3.2 Conclusions on the contributors to the existence of these latent weaknesses

- + Was it due to inadequate preparation prior to operation (quality assurance)?
- + Was it due to degradation during operation (maintenance)?

2.4 Conclusions on the root causes of the significant events selected

2.4.1 Conclusions on the deficiency of the plant surveillance programme that did not eliminate the latent weakness before the event occurs.

- + Was it due to a inadequate detection programme?
- + Was it due to a inadequate restoration process once the latent weakness was detected?

2.4.2 Conclusions on the contributors to the deficiency of the plant surveillance programme.

+ Was the plant surveillance policy appropriate?

+ Was management of the plant surveillance programme adequate for timely detection and prompt restoration?

2.5 Conclusions on corrective actions related to the significant events selected

2.5.1 Conclusions on immediate actions taken to eliminate the actual consequences of the event.

2.5.2 Conclusions on actions taken to eliminate the latent weakness of the elements that failed to perform as expected

+ to restore the level of quality of the elements that failed

+ to mitigate the contributors to existence of the latent weakness.

2.5.3 Conclusions on actions taken to eliminate the deficiency of the plant surveillance programme

+ to improve the plant detection programme

+ to improve the plant restoration process

+ to mitigate the contributors to deficiency of the plant surveillance programme (policy and management)

2.5.4 Conclusions on appropriateness and completeness of corrective actions implemented by the operating organization

2.6 Conclusions on generic lessons and policy of prevention of incidents

2.6.1 Conclusions on generic lessons and good practices

2.6.2 Conclusions on plant quality assurance programme to qualify equipment, personnel and procedure prior to operation

2.6.3 Conclusions on plant maintenance programme to prevent degradation of quality of equipment, personnel and procedure during operation

2.6.4 Conclusions on plant surveillance programme to detect and restore any degradation of quality of equipment, personnel and procedure during operation

2.7 Suggested actions plan

2.7.1 Short term and long term actions

2.7.2 Improvement of quality of equipment

- design, manufacturing, installation
- qualification tests
- periodic testing

2.7.3 Improvement of quality of personnel

- recruiting criteria
- training, retraining, licensing
- periodic testing

2.7.4 Improvement of quality of procedures

- content and format
- validation
- periodic review

2.7.5 Improvement of management of

* quality assurance programme on activities directed to the achievement of the required level of quality for equipment, personnel, procedures

* maintenance programme to keep at the level required quality of equipment, personnel and procedures

* surveillance programme to timely detect and promptly restore any degradation of the level of quality of equipment, personnel and procedures

III. ANALYSIS OF A SPECIFIC EVENT: (TITLE?)

3.1 Description and significance of the event

3.1.1 Initital status of the plant

3.1.2 Detection of the event

3.1.3 Brief description of the event

3.1.4 Final status of the plant

3.1.5 Actual consequences of the event

(A) Off-site impact

+ Impact on the public	- deaths - injuries - irradiation - etc.
+ Impact on the environment	- contamination of soil and water - etc.
+ Radioactive releases without impact on public and environment	- noble gases - I 131 - aerosols - liquids - solids - etc.

(B) On-site impact

+ Impact on plant personnel	- deaths - injuries - irradiation - contamination - etc.
+ Impact on plant safety functions performance	- safety functions (barrier, protection, supply) did not perform as expected when requested - etc.
+ Impact on plant structures	- irradiation fields - surface or atmospheric contamination - fires on safety related features - etc.

(C) Degradation of in-depth defence

+ Degradation of the safety function "BARRIER" (passive features)	- fuel cladding - primary envelop - containment
+ Degradation of the safety function "PROTECTION" (active features)	- reactor shutdown - cooling of fuel - confinement of radioactive products
+ Degradation of the safety function "SUPPLY"	- electrical power (off-site and on-site) - cooling water - instrument air

3.1.6 Immediate actions taken

- o to interrupt the event sequence
- o to restore safety

3.1.7 Assessment of the severity of the event based on actual consequences

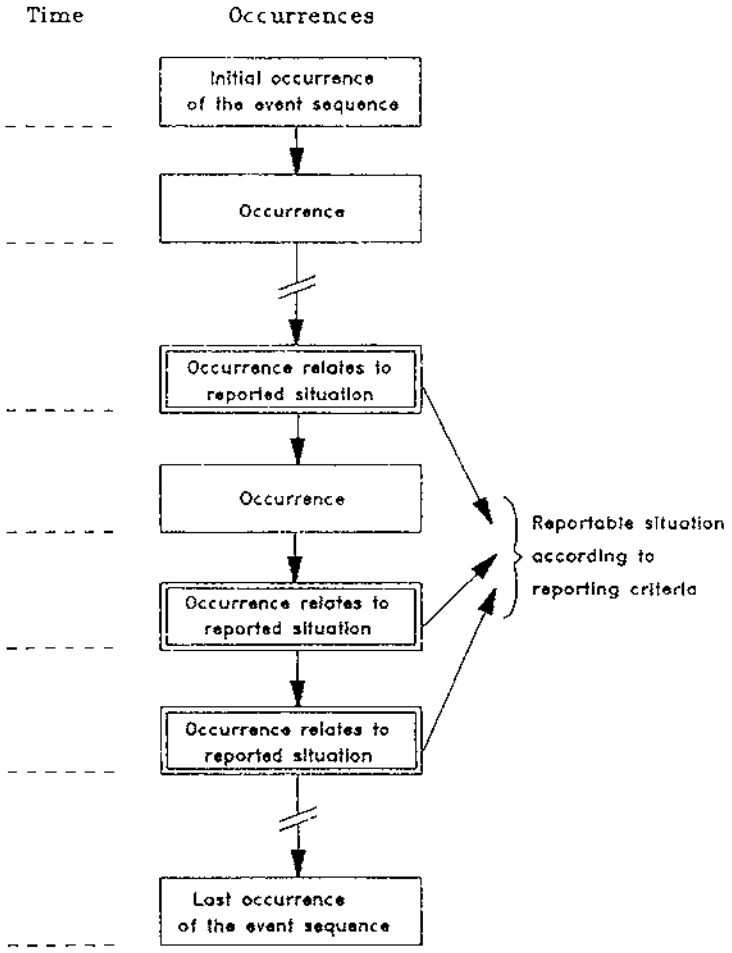
- o according to the international severity scale
- o comments on severity of the off-site impact (actual significance)
- o comments on severity of the on-site impact (potential significance regarding possible off-site impact)
- o comment on severity of degradation of the in-depth defence of the plant (potential significance regarding possible on-site and off-site impact)

3.2 Selection of the occurrences to be analyzed

3.2.1 Establishment of the chronologic sequence of occurrences related to the reported event

EVENT (INCIDENT OR ACCIDENT)

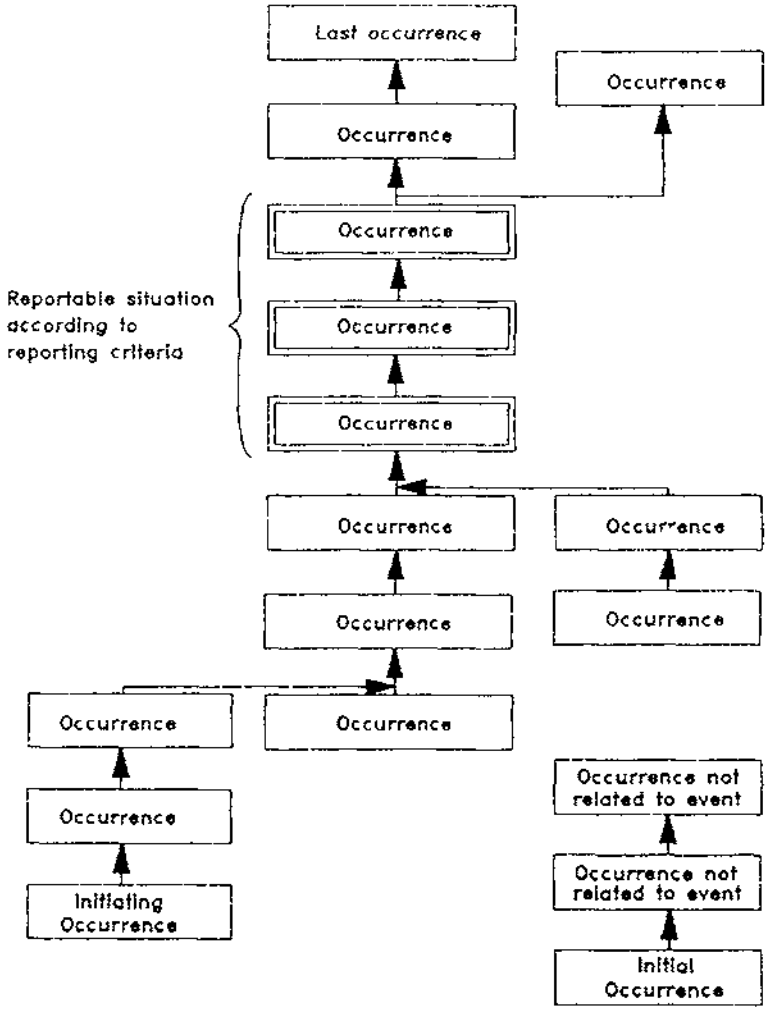
EXAMPLE OF CHRONOLOGICAL SEQUENCE OF OCCURRENCES



3.2.2 Establishment of the logic tree of occurrences

EVENT (INCIDENT OR ACCIDENT)

EXAMPLE OF LOGIC TREE OF OCCURRENCES



3.2.3 Assessment of the safety significance of each occurrence

3.2.4 Selection of the occurrences to be analyzed

3.3 <u>Identification of the direct cause of each occurrence</u>

3.3.1 Identification of the nature of the occurrence (personnel, equipment, procedure failure)

3.3.2 Identification of the latent weakness which was affecting personnel, equipment or procedures when they failed to perform as expected due to poor:

* reliability in operation?
* fitness to working conditions?
* qualification for task?

3.3.3 Identification of the contributors to the existence of this latent weakness.

* Inadequate preparation prior to operation (quality assurance)?
* Degradation during operation (inadequate preventive maintenance)?

3.3.4 Conclusions on the direct cause identified by the operating organization

3.4 **Identification of the root cause of each occurrence**

3.4.1 Identification of the deficiency of the plant surveillance programme that did not eliminate the latent weakness before incident

* Inadequate detection programme?

* Inadequate restoration process following detection of weakness?

3.4.2 Identification of the contributors to the deficiency of the plant surveillance programme

* Surveillance policy appropriate?

* Management of surveillance programme adequate for timely detection and prompt restoration

3.4.3 Conclusions on the root cause identified by the operating organization

3.5 **Determination of corrective actions**

3.5.1 Elimination of the actual consequences of the event

3.5.2 Repair: Elimination of the latent weakness (direct cause) of the elements that failed to perform as expected

- by restoring the level of quality of the elements that failed

- by mitigating the contributors to the existence of the latent weakness

3.5.3 Remedy: Elimination of the deficiency of the plant surveillance programme (root cause) that did not eliminate the latent weakness

- by enhancement of the plant detection programme

- by enhancement of the plant restoration programme

- by mitigation of the contributors to the deficiency of the plant surveillance programme (policy and management)

3.5.4 Conclusions on the appropriateness and completeness of the corrective actions implemented by the operating organization.

3.6 **Generic lessons on prevention of incidents at the plant**

3.6.1 Conclusions on generic lessons and good practices

3.6.2 Conclusions on plant quality assurance programme to qualify equipment, personnel and procedure prior to operation

3.6.3 Conclusions on plant maintenance programme to prevent degradation of quality of equipment, personnel and procedure during operation

3.6.4 Conclusions on plant surveillance programme to detect and restore any degradation of quality of equipment, personnel and procedure during operation

3.7 **Suggested actions plan**

3.7.1 Short term and long term actions

3.7.2 Improvement of quality of equipment

- design, manufacturing, installation
- qualification tests
- periodic testing

3.7.3 Improvement of quality of personnel

- recruiting criteria
- training, retraining, licensing
- periodic testing

3.7.4 Improvement of quality of procedures

- content and format
- validation
- periodic review

3.7.5 Improvement of management of

* quality assurance programme on activities directed to the achievement of the required level of quality for equipment, personnel, procedures
* maintenance programme to keep at the level required quality of equipment, personnel and procedures
* surveillance programme to timely detect and promptly restore any degradation of the level of quality of equipment, personnel, and procedures

IV. GENERAL CONCLUSIONS OF THE ASSET MISSION

4.1 Plant performance

- capacity factor
- operational events
- significance to safety

4.2 Restoration of quality following events

- achieving the required quality level
- maintaining the required quality level

4.3 Prevention of incidents

- Detection of degradation of quality
- Restoration of quality when degradation detected

4.4 Generic lessons

4.5 Summarized actions plan

V. RESPONSE OF THE OPERATING ORGANIZATION

This section is provided by

the operating organization

on the basis of the

conclusions and suggestions of the ASSET team

ACKNOWLEDGEMENTS

The operating organization and its (NAME) nuclear power plant provided valuable support to the ASSET. The traditionally close co-operation of (COUNTRY) with the IAEA in all nuclear safety activities, had already established many personal contacts and a common basis for continuing work. In accordance with the discussions at a preparatory meeting, well selected and prepared information was made available in advance to familiarize the ASSET members with their assignments. Throughout the whole mission, plant counterparts were open-minded, cooperative and helpful in locating persons and information. They were instrumental in establishing a highly effective working relationship with the ASSET members. It extended occasionally beyond working hours and will not be terminated with the submission of the report. The efforts of the liaison officer and the secretarial support were outstanding. The (PLANT) ASSET wishes to express its gratitude to all concerned for the prior efforts and for the excellent working conditions during the review.

ANNEX 1

LIST OF PARTICIPANTS

(NAME) Nuclear Power Plant (Address, phone, telex, fax)

Names	Position

Regulatory Body (Address, phone, telex, fax)

Names	Position

Assessment of Safety Significant Events Team

Names	Country	Company	(Address, phone, telex, fax)

ANNEX 2

SCHEDULE OF ACTIVITIES

		DATES
1.	Official request of the Government of (COUNTRY)	.....
2.	Preparatory meeting with regulatory body and plant management	.....
3.	Recruitment of external experts	.....
4.	Technical preparation of the ASSET mission	.....
5.	Meeting for final preparation	.....
6.	ASSET investigation at the (NAME) nuclear power plant	.....
7.	Submission of the final report	.....

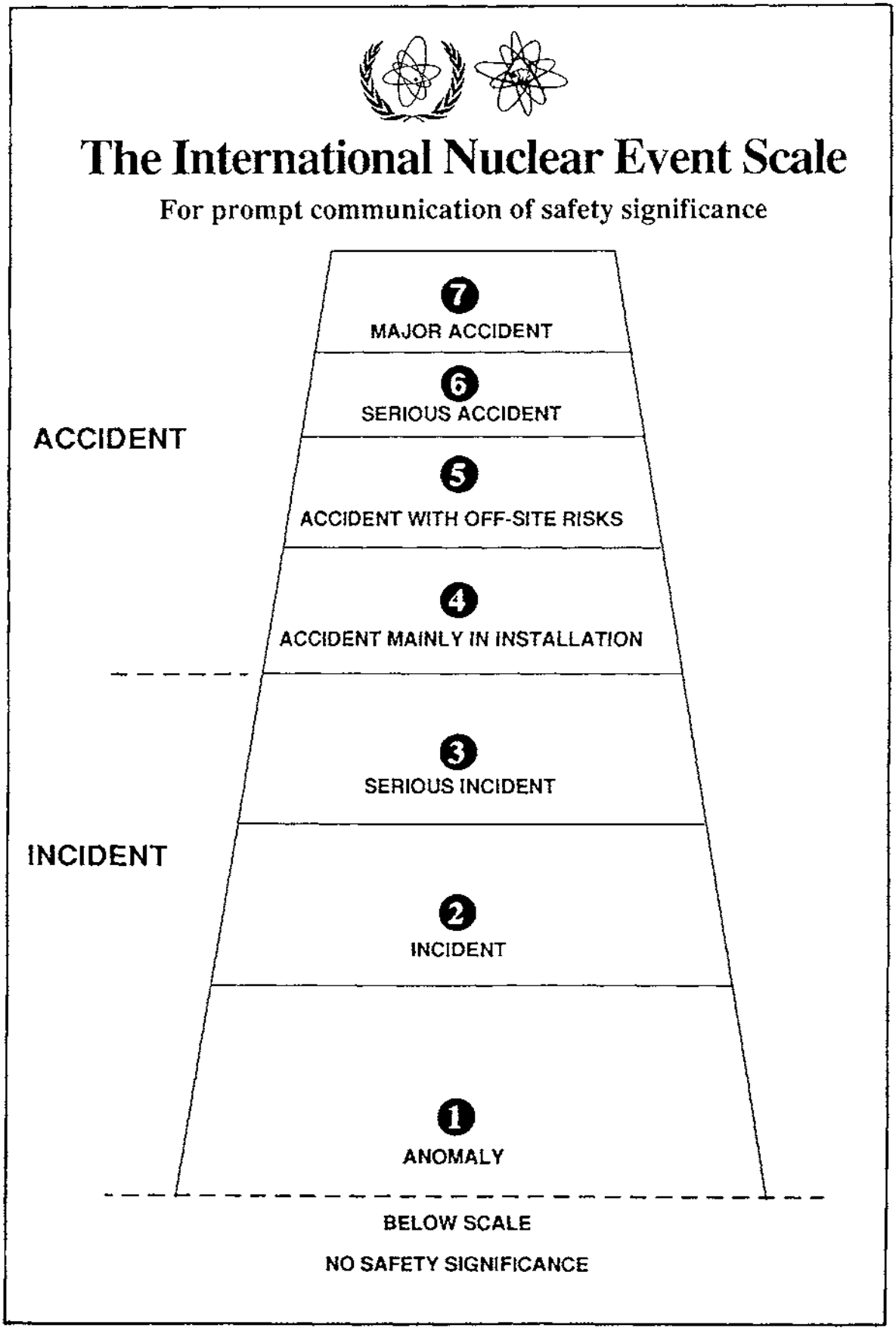
Appendix 1

ASSET GLOSSARY

EVENT:	Problem, issue, abnormality, incident, accident that is reported according to reporting criteria.
OCCURRENCE:	Failure to perform as expected of equipment of personnel, of procedure. Several occurrences may usually be identified in the sequence of an event.
DIRECT CAUSE OF AN OCCURRENCE	It is the latent weakness which was pre-existing in the element that failed to perform as expected under adverse circumstances.
LATENT WEAKNESS:	It is the potential for an occurrence.
CONTRIBUTORS TO EXISTENCE OF A LATENT WEAKNESS:	Weaknesses among equipment, personnel, procedure are due to 2 main contributors: + The level of quality required for operation was not achieved prior to operation due to poor quality assurance programme. + The level of quality achieved for operation was not maintained during operation due to poor maintenance programme.
ROOT CAUSE OF AN OCCURRENCE:	It is the deficiency of the plant surveillance programme that did not timely eliminate the latent weakness (detection and restoration).
SURVEILLANCE DEFICIENCY:	It is the incapacity of the plant surveillance to play its role of ultimate barrier of the in-depth defence system such as: + Degradation of the level of quality required was not detected due to poor detection programme. + Restoration of the level of quality when degraded was not effective due to poor restoration process.
CONTRIBUTORS TO DEFICIENCY OF SURVEILLANCE:	Deficiencies of the plant surveillance programme on equipment, personnel and procedures are due to 2 main contributors: + Plant surveillance policy is inappropriate. + Management of the plant surveillance programme is inadequate.

Appendix 2

THE INTERNATIONAL NUCLEAR EVENT SCALE



Background

The International Nuclear Event Scale is a means for promptly communicating to the public in consistent terms the safety significance of events reported at nuclear power plants. By putting events into proper perspective, the Scale can facilitate a common understanding between the nuclear community, the media, and the public.

The Scale was designed by an international group of experts convened jointly by the International Atomic Energy Agency and the Nuclear Energy Agency of the Organisation for Economic Co-operation and Development. The group was guided in its work by the findings from a series of international meetings held to discuss general principles underlying such a scale. The Scale also reflects the experience gained from the use of similar scales in France and Japan and from considerations of possible scales in several other countries.

The Scale is being applied initially for a trial period of about one year, during which the international agencies and user countries will monitor its progress. It would be revised, as necessary, based on user experience and feedback from the nuclear community, the media, and the public. The Scale is designed for use initially at nuclear power plants, but its application to events at other nuclear installations is desirable. To that end, the international agencies and user countries will consider what modifications might be needed to encompass the wider range of conditions which can prevail at other nuclear installations.

The Scale is designed for prompt assessment following an event. Internationally agreed guidance is available to assist those classifying events, but engineering judgement must play a role in fixing the appropriate level. Those using the Scale can also draw on validation experience gained by classifying events previously reported in several countries for different types of nuclear power reactors. Where necessary, justification for classifying an event at a particular level can be given. An event can be reclassified at a later date based on further analysis or developments, but reclassification should be kept to a minimum.

The Scale does not replace criteria adopted nationally and internationally for the reporting, description, definition, and technical analysis of nuclear events. Nor should it be used to compare safety performance in different countries. If a radiological emergency occurs in the vicinity of a nuclear power plant, existing national emergency planning will take precedence over the use of the Scale.

Although broadly comparable, detailed nuclear safety criteria and the associated terminology may vary from country to country. Although the Scale is designed to allow for this variance, a user country may wish to clarify it in the national context.

Using the scale

Events classified on the Scale (see back page) relate only to nuclear or radiological safety. These are classified at seven levels. The levels, their descriptors and detailed criteria are shown opposite, together with examples of classified nuclear events which have occurred at nuclear power plants. The lower levels (1–3) are termed incidents, and the upper levels (4–7) accidents. Events which have no safety significance are classified as Below Scale/Level Zero. Industrial accidents or other events which are not related to nuclear plant operations are not classified on the scale; these are termed Out of Scale.

As a rough guide, it might be expected that about ten times fewer events would be classified at each successively higher level of the Scale.

The matrix opposite explains the underlying logic of the Scale. Key words indicate generally the safety significance and are not intended to be precise or definitive. Events are considered in terms of three broad criteria represented by each of the columns: off-site impact, on-site impact, and defence-in-depth degradation.

The first criterion applies to events resulting in releases of radioactivity off-site. Understandably, the public is most concerned with such external releases. Level 7, the highest in this column, corresponds to a major nuclear accident with widespread health and environmental consequences. Level 3, the lowest point in this column, represents a very small release that would result in a radiation dose to the most exposed members of the public equivalent to a fraction of the prescribed annual dose limit for the public. Such a dose is typically about a tenth of the average annual dose from exposure to natural background radiation.

The second criterion considers the on-site impact of the event. The range is from Level 5, typically representing a situation of severe damage to the nuclear reactor core, down to Level 3 at which there is major contamination and/or overexposure of workers.

The third criterion applies to events involving the degradation of a plant's defence-in-depth. All plants are designed such that a succession of safety systems act to prevent major on-site and off-site impacts. The defence-in-depth considerations classify events as Levels 3 through 1.

An event which has characteristics represented by more than one criterion is always classified at the highest level according to any one criterion.

Examples of classified nuclear events

• The 1986 accident at the Chernobyl nuclear power plant in the Soviet Union had widespread environmental and human health effects. It is thus classified as Level 7.

• The 1957 accident at the air-cooled graphite reactor at Windscale (now Sellafield) facility in the United Kingdom involved an external release of radioactive fission products. Based on the off-site impact of this event, it is classified as Level 5.

• The 1979 accident at the Three Mile Island nuclear power plant in the United States resulted in a severely damaged reactor core. The off-site release of radioactivity was very limited. The event is classified as Level 5, based on the on-site impact.

• The 1980 accident at the Saint-Laurent nuclear power plant in France resulted in partial damage to the reactor core, but there was no external release of radioactivity. It is classified as Level 4, based on the on-site impact.

• The 1989 incident at the Vandellos nuclear power plant in Spain did not result in an external release of radioactivity, nor was there damage to the reactor core or contamination on site. However, the damage to the plant's safety systems degraded the defence-in-depth significantly. The event is classified as Level 3, based on the defence-in-depth criterion.

• From experience in validating the Scale, the majority of reported events were found to be below Level 3. Although no examples of these events are given here, countries using the Scale may wish to provide examples of events at these lower levels.

Underlying logic of the scale

(Criteria given in matrix are broad indicators only)

LEVEL/ DESCRIPTOR	CRITERIA		
	OFF-SITE IMPACT	ON-SITE IMPACT	DEFENCE-IN-DEPTH DEGRADATION
7 MAJOR ACCIDENT	MAJOR RELEASE: WIDESPREAD HEALTH AND ENVIRONMENTAL EFFECTS		
6 SERIOUS ACCIDENT	SIGNIFICANT RELEASE: FULL IMPLEMENTATION OF LOCAL EMERGENCY PLANS		
5 ACCIDENT WITH OFF-SITE RISKS	LIMITED RELEASE: PARTIAL IMPLEMENTATION OF LOCAL EMERGENCY PLANS	SEVERE CORE DAMAGE	
4 ACCIDENT MAINLY IN INSTALLATION	MINOR RELEASE: PUBLIC EXPOSURE OF THE ORDER OF PRESCRIBED LIMITS	PARTIAL CORE DAMAGE ACUTE HEALTH EFFECTS TO WORKERS	
3 SERIOUS INCIDENT	VERY SMALL RELEASE: PUBLIC EXPOSURE AT A FRACTION OF PRESCRIBED LIMITS	MAJOR CONTAMINATION OVEREXPOSURE OF WORKERS	NEAR ACCIDENT — LOSS OF DEFENCE-IN-DEPTH PROVISIONS
2 INCIDENT			INCIDENTS WITH POTENTIAL SAFETY CONSEQUENCES
1 ANOMALY			DEVIATIONS FROM AUTHORIZED FUNCTIONAL DOMAINS
0 /BELOW SCALE			NO SAFETY SIGNIFICANCE

The International Nuclear Event Scale

for prompt communication of safety significance

LEVEL	DESCRIPTOR	CRITERIA	EXAMPLES
ACCIDENTS 7	MAJOR ACCIDENT	• External release of a large fraction of the reactor core inventory typically involving a mixture of short and long-lived radioactive fission products (in quantities radiologically equivalent to more than tens of thousands terabecquerels of iodine-131) Possibility of acute health effects Delayed health effects over a wide area, possibly involving more than one country Long-term environmental consequences	Chernobyl, USSR 1986
6	SERIOUS ACCIDENT	• External release of fission products (in quantities radiologically equivalent to the order of thousands to tens of thousands of terabecquerels of iodine-131) Full implementation of local emergency plans most likely needed to limit serious health effects	
5	ACCIDENT WITH OFF-SITE RISKS	• External release of fission products (in quantities radiologically equivalent to the order of hundreds to thousands of terabecquerels of iodine-131) Partial implementation of emergency plans (e g local sheltering and/or evacuation) required in some cases to lessen the likelihood of health effects • Severe damage to large fraction of the core due to mechanical effects and/or melting	Windscale, UK 1957 Three Mile Island, USA, 1979
4	ACCIDENT MAINLY IN INSTALLATION	• External release of radioactivity resulting in a dose to the most exposed individual off-site of the order of a few millisieverts * Need for off-site protective actions generally unlikely except possibly for local food control • Some damage to reactor core due to mechanical effects and/or melting • Worker doses that can lead to acute health effects (of the order of 1 Sievert) **	Saint-Laurent, France, 1980
INCIDENTS 3	SERIOUS INCIDENT	• External release of radioactivity above authorized limits, resulting in a dose to the most exposed individual off site of the order of tenths of a millisievert * Off-site protective measures not needed • High radiation levels and/or contamination on-site due to equipment failures or operational incidents Overexposure of workers (individual doses exceeding 50 millisieverts) ** • Incidents in which a further failure of safety systems could lead to accident conditions, or a situation in which safety systems would be unable to prevent an accident if certain initiators were to occur	Vandellos, Spain 1989
2	INCIDENT	• Technical incidents or anomalies which, although not directly or immediately affecting plant safety, are liable to lead to subsequent re-evaluation of safety provisions	
1	ANOMALY	• Functional or operational anomalies which do not pose a risk but which indicate a lack of safety provisions This may be due to equipment failure, human error or procedural inadequacies (Such anomalies should be distinguished from situations where operational limits and conditions are not exceeded and which are properly managed in accordance with adequate procedures These are typically "below scale")	
BELOW SCALE/ZERO	NO SAFETY SIGNIFICANCE		

April 1990

** The doses are expressed in terms of effective dose equivalent (whole body dose) Those criteria where appropriate also can be expressed in terms of corresponding annual effluent discharge limits authorized by National authorities*

*** These doses are also expressed, for simplicity, in terms of effective dose equivalents (sieverts) although the doses in the range involving acute health effects should be expressed in terms of absorbed dose (grays)*

International Atomic Energy Agency
Wagramerstrasse 5
A-1400 Vienna, Austria

OECD Nuclear Energy Agency
38, Boulevard Suchet
75016 Paris, France

Appendix 3

'SUMMARY OF THE EVENT ROOT CAUSE ANALYSIS' FORM

ASSET FORM

IAEA	"SUMMARY OF THE EVENT ROOT CAUSE ANALYSIS"	ASSET

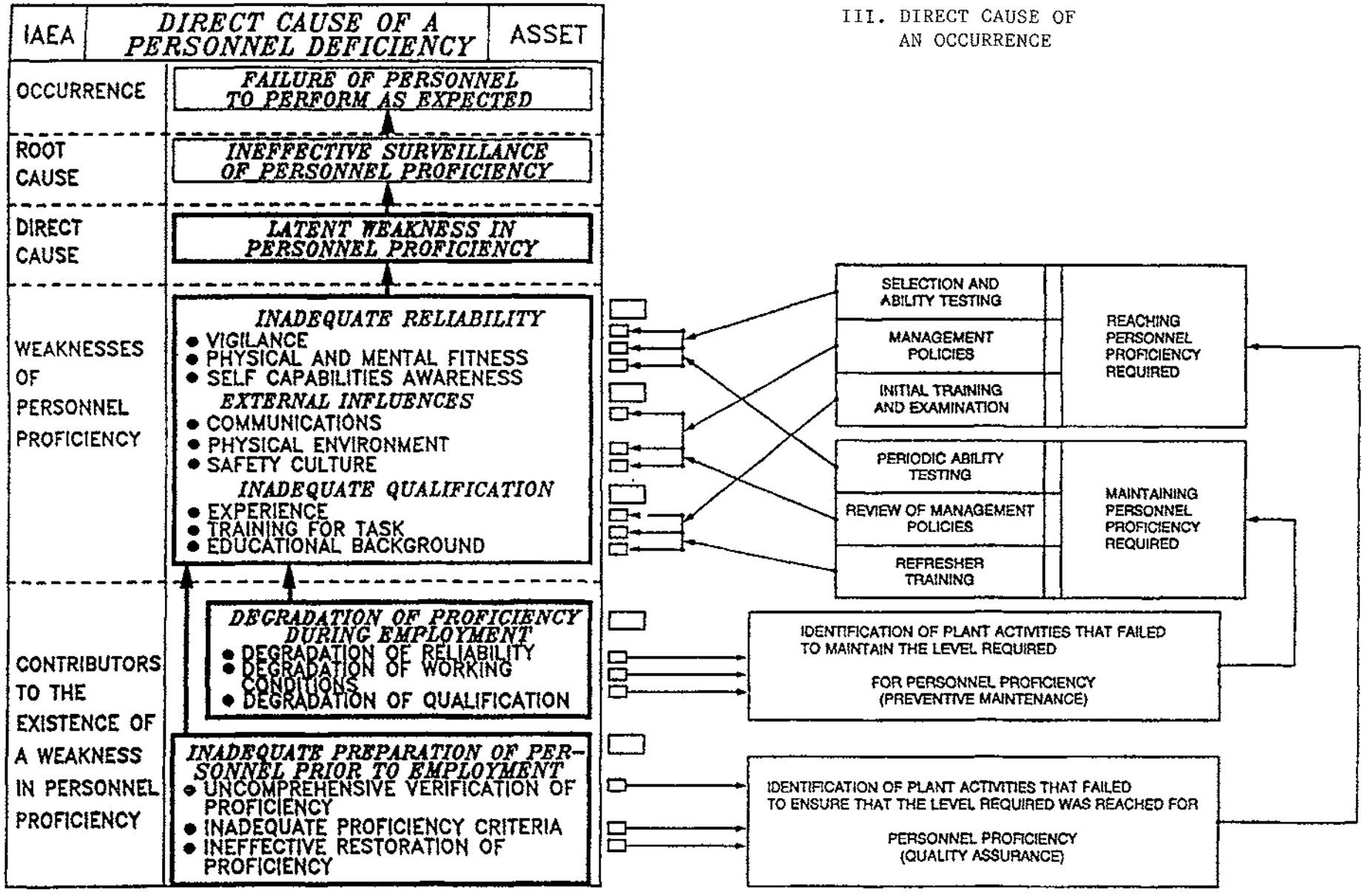
NUCLEAR POWER PLANT :	DATE OF THE EVENT:

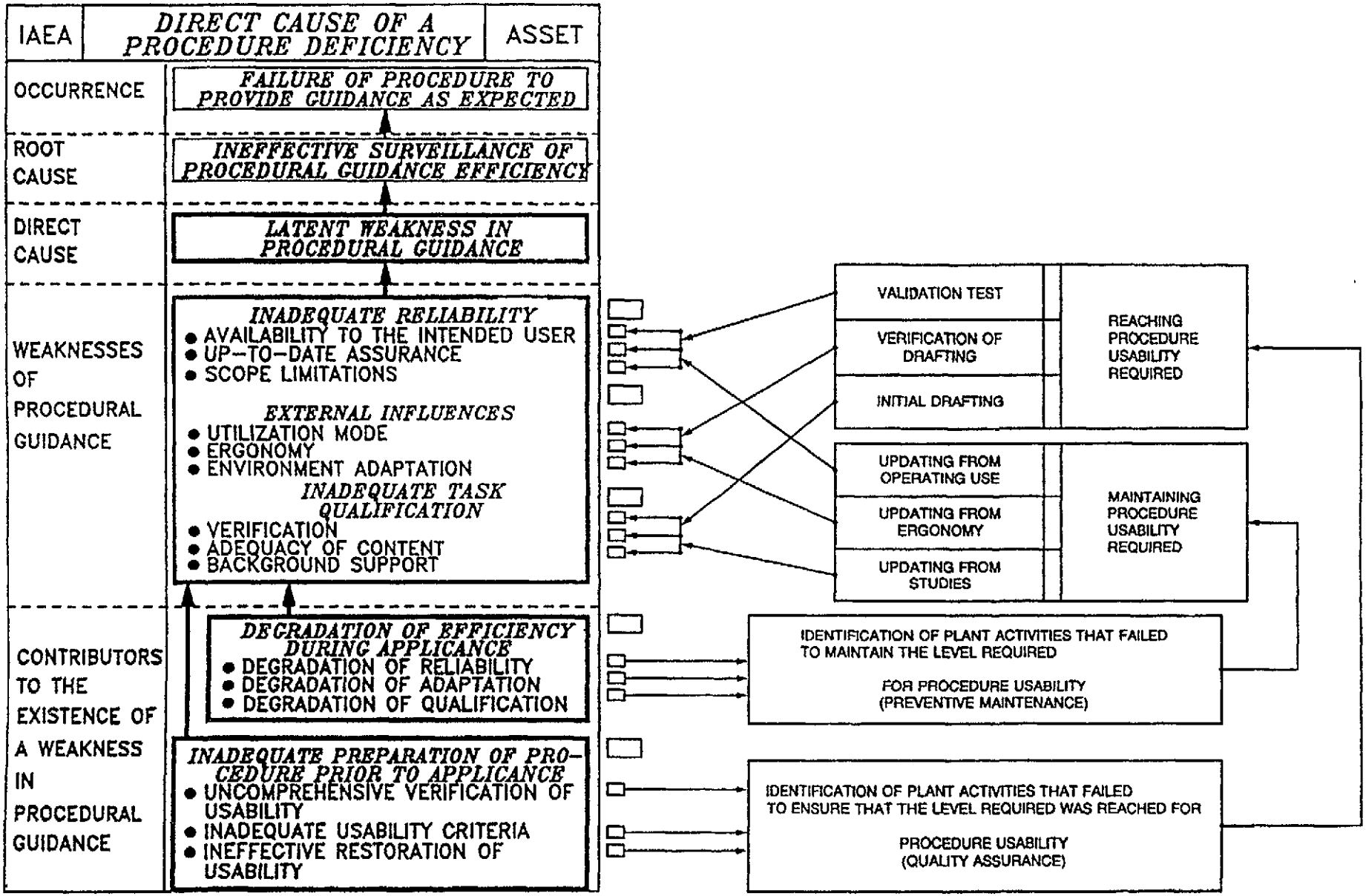
Ø. EVENT TITLE :

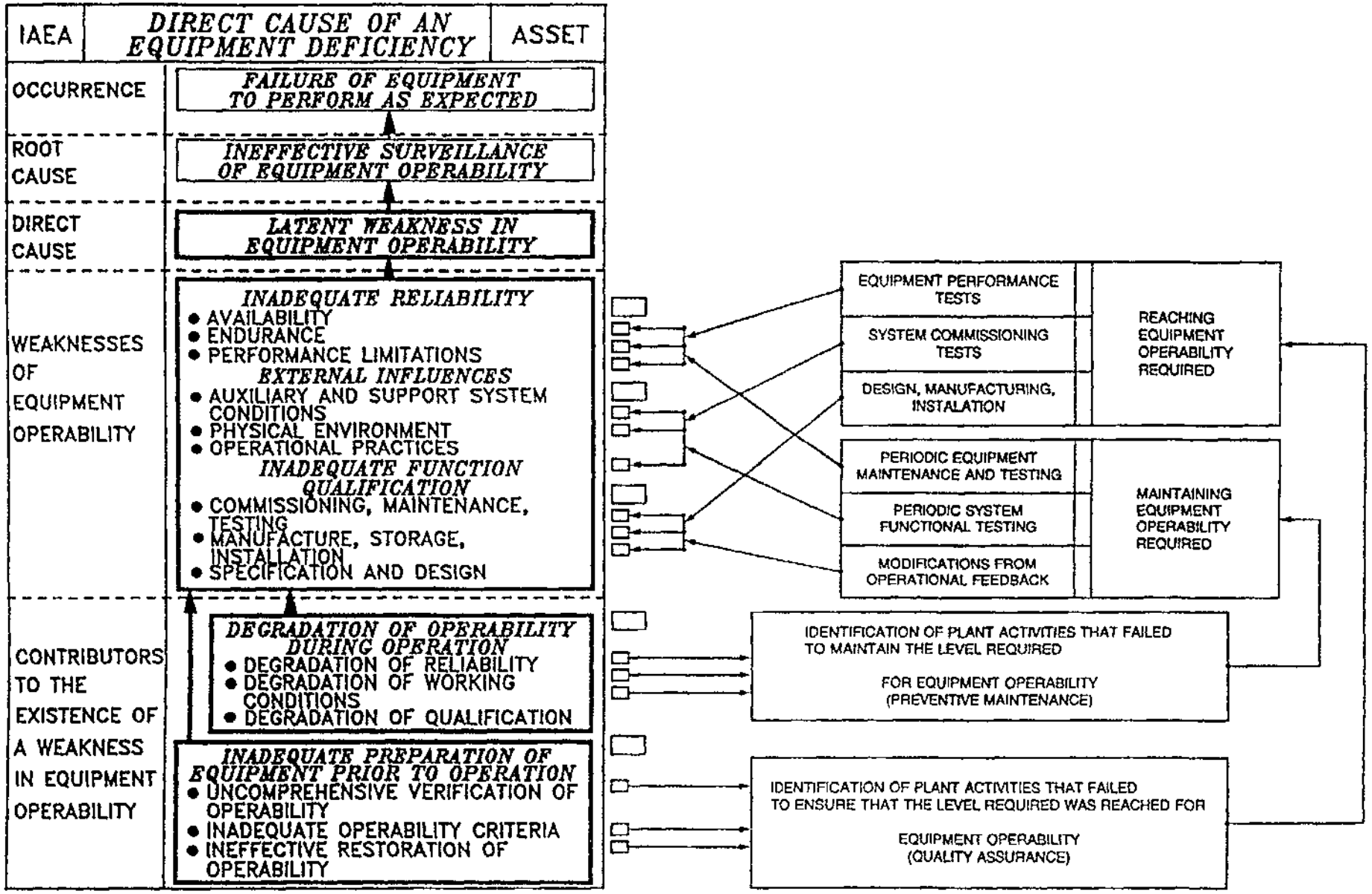
I. SIGNIFICANCE OF THE EVENT JUSTIFICATION OF RATING INES:	LEVEL OF SEVERITY ACCORDING TO INTERNATIONAL SCALE			
	OFF-SITE IMPACT	7	MAJOR RELEASE - WIDE SPREAD HEALTH AND ENVIRONMENTAL EFFECTS	
		6	SIGNIFICANT RELEASE - FULL IMPLEMENTATION OF LOCAL EMERGENCY PLANS	
		5	LIMITED RELEASE - PARTIAL IMPLEMENTATION OF LOCAL EMERGENCY PLANS	
		4	MINOR RELEASE - PUBLIC EXPOSURE OF THE ORDER OF PRESCRIBED LIMITS	
		3	VERY SMALL RELEASE - PUBLIC EXPOSURE AT A FRACTION OF PRESCRIBED LIMITS	
	ON-SITE IMPACT	5	SEVERE CORE DAMAGE	
		4	PARTIAL CORE DAMAGE ACUTE HEALTH EFFECTS TO WORKERS	
		3	MAJOR CONTAMINATION OVEREXPOSURE OF WORKERS	
	DEGRADATION OF IN-DEPTH DEFENCE	3	NEAR ACCIDENT - LOSS OF DEFENCE IN-DEPTH PROVISIONS	
		2	INCIDENT WITH POTENTIAL CONSEQUENCES TO SAFETY	
		1	DEVIATION FROM AUTHORIZED FUNCTIONAL DOMAINS	
	BELOW/OUT SCALE	0	NO SAFETY SIGNIFICANCE	
II. OCCURRENCES SELECTED FOR ANALYSIS	PERSONNEL FAILURE		DID NOT ACT	
			DID ACT BUT WRONGLY	
			DID ACT RIGHTLY BUT NOT TIMELY	
	PROCEDURE FAILURE		NO GUIDANCE FOR TASK	
			WRONG GUIDANCE FOR TASK	
			WRONG SEQUENCE FOR TASK	
	EQUIPMENT FAILURE		DID NOT WORK	
			DID WORK BUT NOT PERFORM AS EXPECTED	
			DID WORK BUT NOT WHEN REQUESTED	

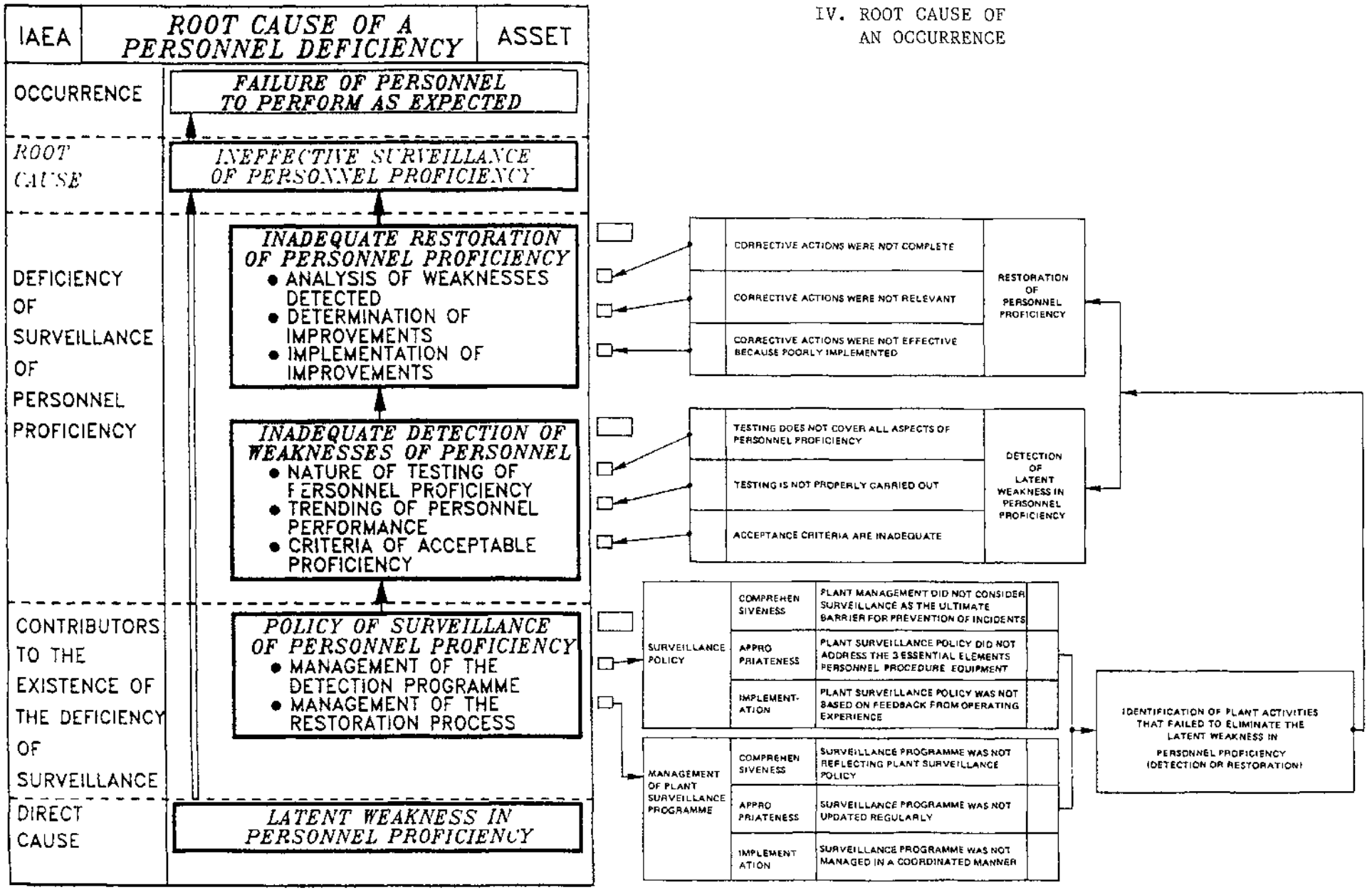
N.B.: For each occurrence selected, please fill in the 4 following sheets (Direct Cause, Root Cause and Corrective Actions) to record the conclusions of your investigation.

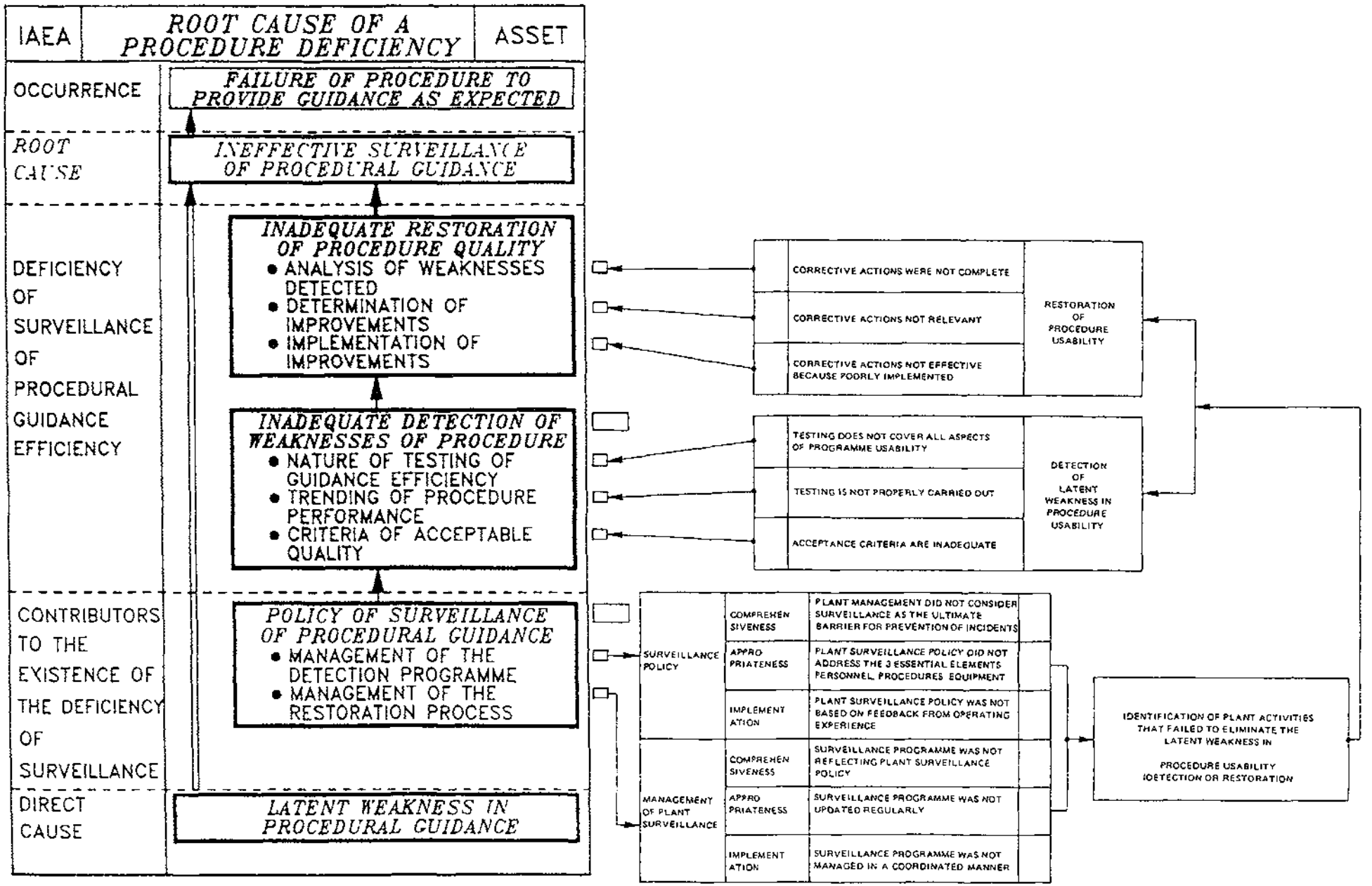
III. DIRECT CAUSE OF AN OCCURRENCE

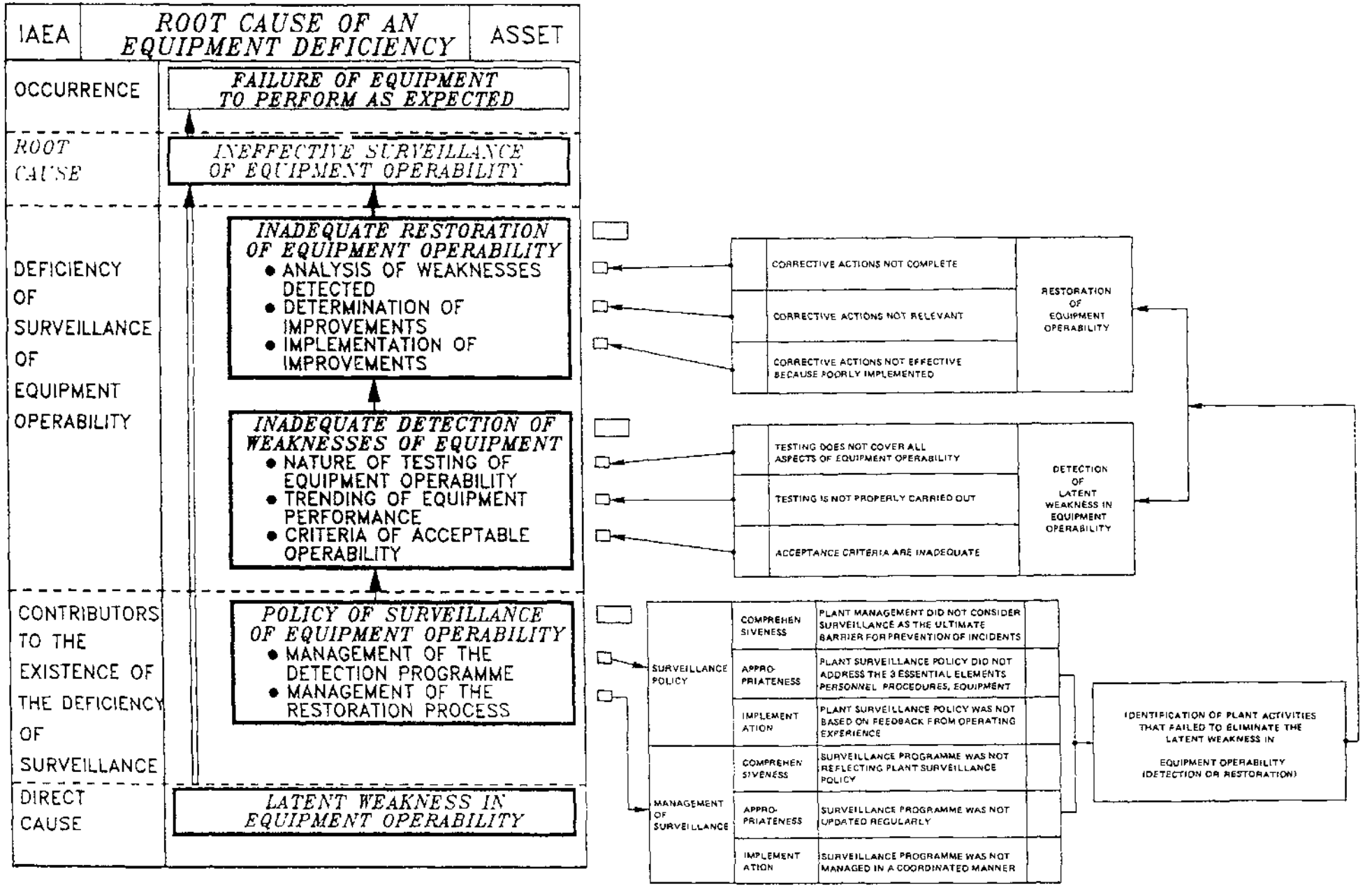



IAEA
DIRECT CAUSE OF A PROCEDURE DEFICIENCY
ASSET
OCCURRENCE
FAILURE OF PROCEDURE TO PROVIDE GUIDANCE AS EXPECTED
ROOT CAUSE
INEFFECTIVE SURVEILLANCE OF PROCEDURAL GUIDANCE EFFICIENCY
DIRECT CAUSE
LATENT WEAKNESS IN PROCEDURAL GUIDANCE
WEAKNESSES OF PROCEDURAL GUIDANCE
INADEQUATE RELIABILITY
AVAILABILITY TO THE INTENDED USER
UP-TO-DATE ASSURANCE
SCOPE LIMITATIONS
EXTERNAL INFLUENCES
UTILIZATION MODE
ERGONOMY
ENVIRONMENT ADAPTATION
INADEQUATE TASK QUALIFICATION
VERIFICATION
ADEQUACY OF CONTENT
BACKGROUND SUPPORT
CONTRIBUTORS TO THE EXISTENCE OF A WEAKNESS IN PROCEDURAL GUIDANCE
DEGRADATION OF EFFICIENCY DURING APPLICANCE
DEGRADATION OF RELIABILITY
DEGRADATION OF ADAPTATION
DEGRADATION OF QUALIFICATION
INADEQUATE PREPARATION OF PROCEDURE PRIOR TO APPLICANCE
UNCOMPREHENSIVE VERIFICATION OF USABILITY
INADEQUATE USABILITY CRITERIA
INEFFECTIVE RESTORATION OF USABILITY
VALIDATION TEST
VERIFICATION OF DRAFTING
INITIAL DRAFTING
REACHING PROCEDURE USABILITY REQUIRED
UPDATING FROM OPERATING USE
UPDATING FROM ERGONOMY
UPDATING FROM STUDIES
MAINTAINING PROCEDURE USABILITY REQUIRED
IDENTIFICATION OF PLANT ACTIVITIES THAT FAILED TO MAINTAIN THE LEVEL REQUIRED
FOR PROCEDURE USABILITY (PREVENTIVE MAINTENANCE)
IDENTIFICATION OF PLANT ACTIVITIES THAT FAILED TO ENSURE THAT THE LEVEL REQUIRED WAS REACHED FOR
PROCEDURE USABILITY (QUALITY ASSURANCE)


IAEA
DIRECT CAUSE OF AN EQUIPMENT DEFICIENCY
ASSET
OCCURRENCE
FAILURE OF EQUIPMENT TO PERFORM AS EXPECTED
ROOT CAUSE
INEFFECTIVE SURVEILLANCE OF EQUIPMENT OPERABILITY
DIRECT CAUSE
LATENT WEAKNESS IN EQUIPMENT OPERABILITY
WEAKNESSES OF EQUIPMENT OPERABILITY
INADEQUATE RELIABILITY
AVAILABILITY
ENDURANCE
PERFORMANCE LIMITATIONS
EXTERNAL INFLUENCES
AUXILIARY AND SUPPORT SYSTEM CONDITIONS
PHYSICAL ENVIRONMENT
OPERATIONAL PRACTICES
INADEQUATE FUNCTION QUALIFICATION
COMMISSIONING, MAINTENANCE, TESTING
MANUFACTURE, STORAGE, INSTALLATION
SPECIFICATION AND DESIGN
CONTRIBUTORS TO THE EXISTENCE OF A WEAKNESS IN EQUIPMENT OPERABILITY
DEGRADATION OF OPERABILITY DURING OPERATION
DEGRADATION OF RELIABILITY
DEGRADATION OF WORKING CONDITIONS
DEGRADATION OF QUALIFICATION
INADEQUATE PREPARATION OF EQUIPMENT PRIOR TO OPERATION
UNCOMPREHENSIVE VERIFICATION OF OPERABILITY
INADEQUATE OPERABILITY CRITERIA
INEFFECTIVE RESTORATION OF OPERABILITY
EQUIPMENT PERFORMANCE TESTS
SYSTEM COMMISSIONING TESTS
DESIGN, MANUFACTURING, INSTALATION
REACHING EQUIPMENT OPERABILITY REQUIRED
PERIODIC EQUIPMENT MAINTENANCE AND TESTING
PERIODIC SYSTEM FUNCTIONAL TESTING
MODIFICATIONS FROM OPERATIONAL FEEDBACK
MAINTAINING EQUIPMENT OPERABILITY REQUIRED
IDENTIFICATION OF PLANT ACTIVITIES THAT FAILED TO MAINTAIN THE LEVEL REQUIRED
FOR EQUIPMENT OPERABILITY (PREVENTIVE MAINTENANCE)
IDENTIFICATION OF PLANT ACTIVITIES THAT FAILED TO ENSURE THAT THE LEVEL REQUIRED WAS REACHED FOR
EQUIPMENT OPERABILITY (QUALITY ASSURANCE)


IAEA
ROOT CAUSE OF A PERSONNEL DEFICIENCY
ASSET
OCCURRENCE
FAILURE OF PERSONNEL TO PERFORM AS EXPECTED
ROOT CAUSE
INEFFECTIVE SURVEILLANCE OF PERSONNEL PROFICIENCY
DEFICIENCY OF SURVEILLANCE OF PERSONNEL PROFICIENCY
INADEQUATE RESTORATION OF PERSONNEL PROFICIENCY
• ANALYSIS OF WEAKNESSES DETECTED
• DETERMINATION OF IMPROVEMENTS
• IMPLEMENTATION OF IMPROVEMENTS
INADEQUATE DETECTION OF WEAKNESSES OF PERSONNEL
• NATURE OF TESTING OF PERSONNEL PROFICIENCY
• TRENDING OF PERSONNEL PERFORMANCE
• CRITERIA OF ACCEPTABLE PROFICIENCY
CONTRIBUTORS TO THE EXISTENCE OF THE DEFICIENCY OF SURVEILLANCE
POLICY OF SURVEILLANCE OF PERSONNEL PROFICIENCY
• MANAGEMENT OF THE DETECTION PROGRAMME
• MANAGEMENT OF THE RESTORATION PROCESS
DIRECT CAUSE
LATENT WEAKNESS IN PERSONNEL PROFICIENCY
CORRECTIVE ACTIONS WERE NOT COMPLETE
CORRECTIVE ACTIONS WERE NOT RELEVANT
CORRECTIVE ACTIONS WERE NOT EFFECTIVE BECAUSE POORLY IMPLEMENTED
RESTORATION OF PERSONNEL PROFICIENCY
TESTING DOES NOT COVER ALL ASPECTS OF PERSONNEL PROFICIENCY
TESTING IS NOT PROPERLY CARRIED OUT
ACCEPTANCE CRITERIA ARE INADEQUATE
DETECTION OF LATENT WEAKNESS IN PERSONNEL PROFICIENCY
SURVEILLANCE POLICY
COMPREHENSIVENESS
PLANT MANAGEMENT DID NOT CONSIDER SURVEILLANCE AS THE ULTIMATE BARRIER FOR PREVENTION OF INCIDENTS
APPROPRIATENESS
PLANT SURVEILLANCE POLICY DID NOT ADDRESS THE 3 ESSENTIAL ELEMENTS PERSONNEL PROCEDURE EQUIPMENT
IMPLEMENTATION
PLANT SURVEILLANCE POLICY WAS NOT BASED ON FEEDBACK FROM OPERATING EXPERIENCE
MANAGEMENT OF PLANT SURVEILLANCE PROGRAMME
COMPREHENSIVENESS
SURVEILLANCE PROGRAMME WAS NOT REFLECTING PLANT SURVEILLANCE POLICY
APPROPRIATENESS
SURVEILLANCE PROGRAMME WAS NOT UPDATED REGULARLY
IMPLEMENTATION
SURVEILLANCE PROGRAMME WAS NOT MANAGED IN A COORDINATED MANNER
IDENTIFICATION OF PLANT ACTIVITIES THAT FAILED TO ELIMINATE THE LATENT WEAKNESS IN PERSONNEL PROFICIENCY (DETECTION OR RESTORATION)


IAEA
ROOT CAUSE OF A PROCEDURE DEFICIENCY
ASSET
OCCURRENCE
FAILURE OF PROCEDURE TO PROVIDE GUIDANCE AS EXPECTED
ROOT CAUSE
INEFFECTIVE SURVEILLANCE OF PROCEDURAL GUIDANCE
DEFICIENCY OF SURVEILLANCE OF PROCEDURAL GUIDANCE EFFICIENCY
INADEQUATE RESTORATION OF PROCEDURE QUALITY
• ANALYSIS OF WEAKNESSES DETECTED
• DETERMINATION OF IMPROVEMENTS
• IMPLEMENTATION OF IMPROVEMENTS
INADEQUATE DETECTION OF WEAKNESSES OF PROCEDURE
• NATURE OF TESTING OF GUIDANCE EFFICIENCY
• TRENDING OF PROCEDURE PERFORMANCE
• CRITERIA OF ACCEPTABLE QUALITY
CONTRIBUTORS TO THE EXISTENCE OF THE DEFICIENCY OF SURVEILLANCE
POLICY OF SURVEILLANCE OF PROCEDURAL GUIDANCE
• MANAGEMENT OF THE DETECTION PROGRAMME
• MANAGEMENT OF THE RESTORATION PROCESS
DIRECT CAUSE
LATENT WEAKNESS IN PROCEDURAL GUIDANCE
CORRECTIVE ACTIONS WERE NOT COMPLETE
CORRECTIVE ACTIONS NOT RELEVANT
CORRECTIVE ACTIONS NOT EFFECTIVE BECAUSE POORLY IMPLEMENTED
RESTORATION OF PROCEDURE USABILITY
TESTING DOES NOT COVER ALL ASPECTS OF PROGRAMME USABILITY
TESTING IS NOT PROPERLY CARRIED OUT
ACCEPTANCE CRITERIA ARE INADEQUATE
DETECTION OF LATENT WEAKNESS IN PROCEDURE USABILITY
SURVEILLANCE POLICY
COMPREHENSIVENESS
PLANT MANAGEMENT DID NOT CONSIDER SURVEILLANCE AS THE ULTIMATE BARRIER FOR PREVENTION OF INCIDENTS
APPROPRIATENESS
PLANT SURVEILLANCE POLICY DID NOT ADDRESS THE 3 ESSENTIAL ELEMENTS PERSONNEL, PROCEDURES EQUIPMENT
IMPLEMENTATION
PLANT SURVEILLANCE POLICY WAS NOT BASED ON FEEDBACK FROM OPERATING EXPERIENCE
MANAGEMENT OF PLANT SURVEILLANCE
COMPREHENSIVENESS
SURVEILLANCE PROGRAMME WAS NOT REFLECTING PLANT SURVEILLANCE POLICY
APPROPRIATENESS
SURVEILLANCE PROGRAMME WAS NOT UPDATED REGULARLY
IMPLEMENTATION
SURVEILLANCE PROGRAMME WAS NOT MANAGED IN A COORDINATED MANNER
IDENTIFICATION OF PLANT ACTIVITIES THAT FAILED TO ELIMINATE THE LATENT WEAKNESS IN
PROCEDURE USABILITY
DETECTION OR RESTORATION


IAEA
ROOT CAUSE OF AN EQUIPMENT DEFICIENCY
ASSET
OCCURRENCE
FAILURE OF EQUIPMENT TO PERFORM AS EXPECTED
ROOT CAUSE
INEFFECTIVE SURVEILLANCE OF EQUIPMENT OPERABILITY
DEFICIENCY OF SURVEILLANCE OF EQUIPMENT OPERABILITY
INADEQUATE RESTORATION OF EQUIPMENT OPERABILITY
• ANALYSIS OF WEAKNESSES DETECTED
• DETERMINATION OF IMPROVEMENTS
• IMPLEMENTATION OF IMPROVEMENTS
INADEQUATE DETECTION OF WEAKNESSES OF EQUIPMENT
• NATURE OF TESTING OF EQUIPMENT OPERABILITY
• TRENDING OF EQUIPMENT PERFORMANCE
• CRITERIA OF ACCEPTABLE OPERABILITY
CONTRIBUTORS TO THE EXISTENCE OF THE DEFICIENCY OF SURVEILLANCE
POLICY OF SURVEILLANCE OF EQUIPMENT OPERABILITY
• MANAGEMENT OF THE DETECTION PROGRAMME
• MANAGEMENT OF THE RESTORATION PROCESS
DIRECT CAUSE
LATENT WEAKNESS IN EQUIPMENT OPERABILITY
CORRECTIVE ACTIONS NOT COMPLETE
CORRECTIVE ACTIONS NOT RELEVANT
CORRECTIVE ACTIONS NOT EFFECTIVE BECAUSE POORLY IMPLEMENTED
RESTORATION OF EQUIPMENT OPERABILITY
TESTING DOES NOT COVER ALL ASPECTS OF EQUIPMENT OPERABILITY
TESTING IS NOT PROPERLY CARRIED OUT
ACCEPTANCE CRITERIA ARE INADEQUATE
DETECTION OF LATENT WEAKNESS IN EQUIPMENT OPERABILITY
SURVEILLANCE POLICY
COMPREHENSIVENESS
PLANT MANAGEMENT DID NOT CONSIDER SURVEILLANCE AS THE ULTIMATE BARRIER FOR PREVENTION OF INCIDENTS
APPROPRIATENESS
PLANT SURVEILLANCE POLICY DID NOT ADDRESS THE 3 ESSENTIAL ELEMENTS PERSONNEL PROCEDURES, EQUIPMENT
IMPLEMENTATION
PLANT SURVEILLANCE POLICY WAS NOT BASED ON FEEDBACK FROM OPERATING EXPERIENCE
MANAGEMENT OF SURVEILLANCE
COMPREHENSIVENESS
SURVEILLANCE PROGRAMME WAS NOT REFLECTING PLANT SURVEILLANCE POLICY
APPROPRIATENESS
SURVEILLANCE PROGRAMME WAS NOT UPDATED REGULARLY
IMPLEMENTATION
SURVEILLANCE PROGRAMME WAS NOT MANAGED IN A COORDINATED MANNER
IDENTIFICATION OF PLANT ACTIVITIES THAT FAILED TO ELIMINATE THE LATENT WEAKNESS IN
EQUIPMENT OPERABILITY (DETECTION OR RESTORATION)

OCCURRENCE TITLE:	
V. CORREC- TIVE ACTIONS	ELIMINATION OF THE DIRECT CAUSE: I. ELIMINATION OF THE LATENT WEAKNESS: II. ELIMINATION OF THE CONTRIBUTORS TO LATENT WEAKNESS: - CONTRIBUTOR NO. 1: - CONTRIBUTOR NO. 2:
	ELIMINATION OF THE ROOT CAUSE: III. ELIMINATION OF THE SURVEILLANCE DEFICIENCY: IV. ELIMINATION OF THE CONTRIBUTORS TO SURVEILLANCE DEFICIENCY: - CONTRIBUTOR NO. 1: - CONTRIBUTOR NO. 2:

CONCLUSIONS ON
APPROPRIATENESS AND COMPLETENESS OF
CORRECTIVE ACTIONS IMPLEMENTED

OCCURRENCE TITLE:

	NEEDED	APPROPRIATE	COMPLETE
REPAIRS (DIRECT CAUSE) I) CORRECTIVE ACTIONS TO ELIMINATE LATENT WEAKNESS(ES) OF ELEMENT(S) THAT FAILED TO WORK AS EXPECTED			
II) CORRECTIVE ACTIONS TO MITIGATE CONTRIBUTING FACTORS TO LATENT WEAKNESS(ES) (Quality control and/or preventive maintenance)			
REMEDIES (ROOT CAUSE) III) CORRECTIVE ACTIONS TO ELIMINATE DEFICIENCY OF PLANT SURVEILLANCE PROGRAMME (DETECTION PROGRAMME OR RESTORATION PROCESS)			
IV) CORRECTIVE ACTIONS TO MITIGATE CONTRIBUTING FACTORS TO DEFICIENCY OF PLANT SURVEILLANCE (Surveillance policy and/or management of plant surveillance programme)			

VI. GENERIC LESSONS ON PLANT POLICY FOR PREVENTION OF INCIDENTS

6.1 GOOD PRACTICES

6.2 EFFECTIVENESS OF PLANT QUALITY ASSURANCE PROGRAMME (PREPARATION PRIOR TO OPERATION)

6.3 EFFECTIVENESS OF PLANT MAINTENANCE PROGRAMME (PREVENTION OF DEGRADATION DURING OPERATION)

6.4 EFFECTIVENESS OF PLANT SURVEILLANCE PROGRAMME

6.4.1 PLANT DETECTION PROGRAMME

6.4.2 PLANT RESTORATION PROCESS

VII. SUGGESTED ACTION PLANT FOR ENHANCING PREVENTION OF INCIDENTS

7.1 IMPROVEMENT OF OPERABILITY OF EQUIPMENT

7.2 IMPROVEMENT OF PROFICIENCY OF PERSONNEL

7.3 IMPROVEMENT OF PROCEDURAL GUIDANCE

7.4 IMPROVEMENT OF MANAGEMENT

7.4.1 QUALITY ASSURANCE PROGRAMME

7.4.2 PREVENTIVE MAINTENANCE PROGRAMME

7.4.3 SURVEILLANCE PROGRAMME

CONTRIBUTORS TO DRAFTING AND REVIEW

CONSULTANTS MEETING 1987

Y. Van den Berghe	Vincotte Brussels Belgium
J. Libmann	IPSN Fontenay-aux-Roses France
K. Kotthoff	Ges. f. Reaktorsicherheit (GRS) Köln Federal Republic of Germany
G. Grimaldi	Directorate for Nuclear Safety Rome Italy
S. Curcuruto	-"-
W. Lanning	US NRC Washington DC USA
J. Dular	Nuclearna Elektrarna Krsko Yugoslavia
M. Gabrovsek	-"-
M. Dusic	Republiski Energetski Inspectorat Ljubljana Yugoslavia

IAEA:

B. Thomas	Scientific Secretary Division of Nuclear Safety
E. Swaton	Division of Nuclear Safety
V. Tolstykh	Division of Nuclear Safety

CONSULTANTS MEETING 27 February - 3 March 1989

Y. Van den Berghe	Association Vincotte ASBL Brussels Belgium
W. Poroykov	Ministry of Nuclear Power Moscow USSR
E. Pozdyshev	State Committee for Utilization of Atomic Energy Moscow USSR

IAEA:

B. Thomas	Scientific Secretary Division of Nuclear Safety
M. Dusic	-"-
B. Tomic	-"-
V. Tolstykh	-"-
J. van Daatselaar	-"-

CONSULTANTS MEETING 3-6 July 1989

P. Kafka	Ges. f. Reaktorsicherheit (GRS) mbH Forschungsgelände D-8056 Garching Federal Republic of Germany

IAEA:

B. Thomas	Scientific Secretary Division of Nuclear Safety

CONSULTANTS MEETING 3-7 July 1989

Z. Gabrovsek	Nuclear Power Plant Krsko Vrbina 12 68270 Krsko Yugoslavia

IAEA:

M. Dusic	Scientific Secretary Division of Nuclear Safety

CONSULTANTS MEETING 3-7 July 1989

M. Chiramal — US NRC, Washington D.C. 20555, U.S.A.

IAEA:

B. Tomic — Scientific Secretary, Division of Nuclear Safety

CONSULTANTS MEETING 18-29 September 1989

Y. Van den Berghe — Association Vincotte ASBL, Brussels, Belgium

IAEA:

L. Carlsson — Scientific Secretary, Division of Nuclear Safety

CONSULTANTS MEETING 18-19 December 1989

Y. van den Berghe — Association Vincotte ASBL, Brussels, Belgium

IAEA:

M. Dusic — Scientific Secretary, Division of Nuclear Safety

CONSULTANTS MEETING 3-7 December 1990

S.J. Price — Sizewell Electric plc, Nr. Leiston, Suffolk, IP16 4 UE, United Kingdom

T. Wadell — INPO, 1100 Circle 75 Parkway, Atlanta, Georgia 30 339, USA

Z. Gabrousek — Krsko NPP, Vrbina 12, 68 270 Krsko, Yugoslavia

IAEA:

M. Dusic	Scientific Secretary Division of Nuclear Safety
V. Tolstykh	Division of Nuclear Safety
B. Thomas	Division of Nuclear Safety
B. Tomic	Division of Nuclear Safety

This section contain information on four Root Cause Analysis methodologies:

1. **Japanese Human Performance Enhancement System (J-HPES)**
2. **Systematic Approach For Error Reduction (SAFER)**
3. **Japanese Nuclear Energy Safety Organization (JNES) * Organizational Factors List (JOFL)**

* JNES ceased to exist in March 2014 as a result of integration into Nuclear Regulation Authority.

1. Japanese Human Performance Enhancement System (J-HPES)

Introduction

The Central Research Institute of Electric Power Industry (CRIEPI) in Japan developed a human error analysis method, J-HPES (a Japanese version of the human performance enhancement system), in 1990 (Takano, Sawayanagi, & Kabetani, 1994), and has also been conducting analysis of human error events at nuclear power plants. Moreover, the basic framework for human error event has been developed and incorporated into the analytic procedure of J-HPES.

In the following, a basic framework for human error event analysis is first introduced. Then, the modified J-HPES, an analysis method for human error events, is described. Next, a method for identifying the commonalities among analysis results of human error events is explained.

Basic Framework for Event Analysis

This section introduces a framework to assist event investigators in their examination of various causal factors of human error events. The J-HPES was developed by fully modifying the HPES method devised by the U.S. Institute of Nuclear Power Operations, so that it was adapted to a Japanese environment (Takano, Sawayanagi, & Kabetani, 1994). Developed as a remedy-oriented system for systematically analyzing and evaluating human-related events occurring at nuclear power plants, this method aims in particular at identifying causal factors and deriving proposals for specific hierarchical countermeasures. The procedure of the J-HPES comprises four stages:

1. Correct understanding of events
2. Circumstantial analysis (gathering human factor data)
3. Causal analysis
4. Proposing countermeasures

The causal analysis step (Step 3) is applied to each trigger action (defined as a human action contributing directly to an abnormal change of machinery state in an event). The approach applies the modified fault tree method to initiate a search reaching down to the ultimate underlying causal factors. This causal relation chart (Figure 1) clarifies the direct causal factors that have induced the trigger action, indirect causes that have contributed to the direct causal factors, and latent causes that have contributed to the indirect causes. The procedure of J-HPES is similar to the "why–because analysis" (Paul-Stuve, 2005). The J-HPES, however, especially focuses on the human actions that trigger an event and places emphasis on human factors when searching for the underlying causes of the actions.

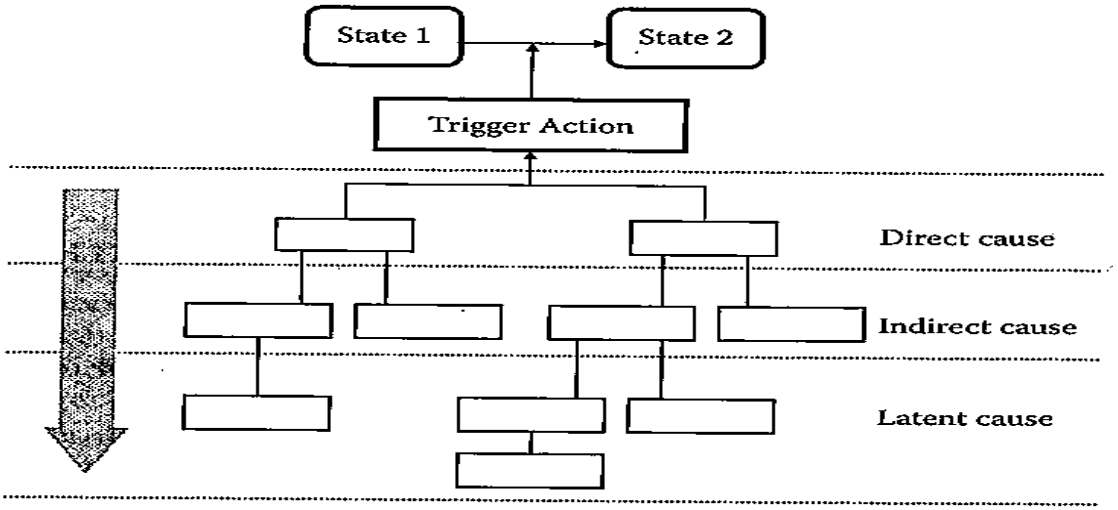


Figure 1 Causal relation chart (J-HPES).

The basic idea of the causal analysis is to ask the question "why" repeatedly, starting from "why does the trigger action occur." Thirteen categories of causal factors, such as work practice and work verification, are given as references for examining possible causal factors. An advantage of this method is that there are only a few rules and conventions so that investigators can propose causal factors on their own. However, there is a concern that analysis results may vary too much because the choice of potential factors to examine and the decision of when to stop asking the "why" questions are influenced by the investigator's knowledge about facilities and human factors. Particularly, when it comes to finding commonalities among human error event data accumulated in an organization, reliable and useful results do not appear unless the analysis of individual human error event is based on the unified mindset. Hence, in 2006, CRIEPI developed a framework (see Figure 2) for exploring causal factors of trigger actions (Hirotsu et al., 2006).

This framework was developed based on the model of accident investigation (stages in the development and investigation of an organizational accident) described by Reason (1997), as well as CRIEPI's experiences in event analysis. Each item of this framework was defined while considering work in a nuclear power plant. Moreover, the causal factors reference list (Figure 3) was summarized based on this framework, in order to assist investigators who do not have sufficient knowledge about human factors in identifying causal factors.

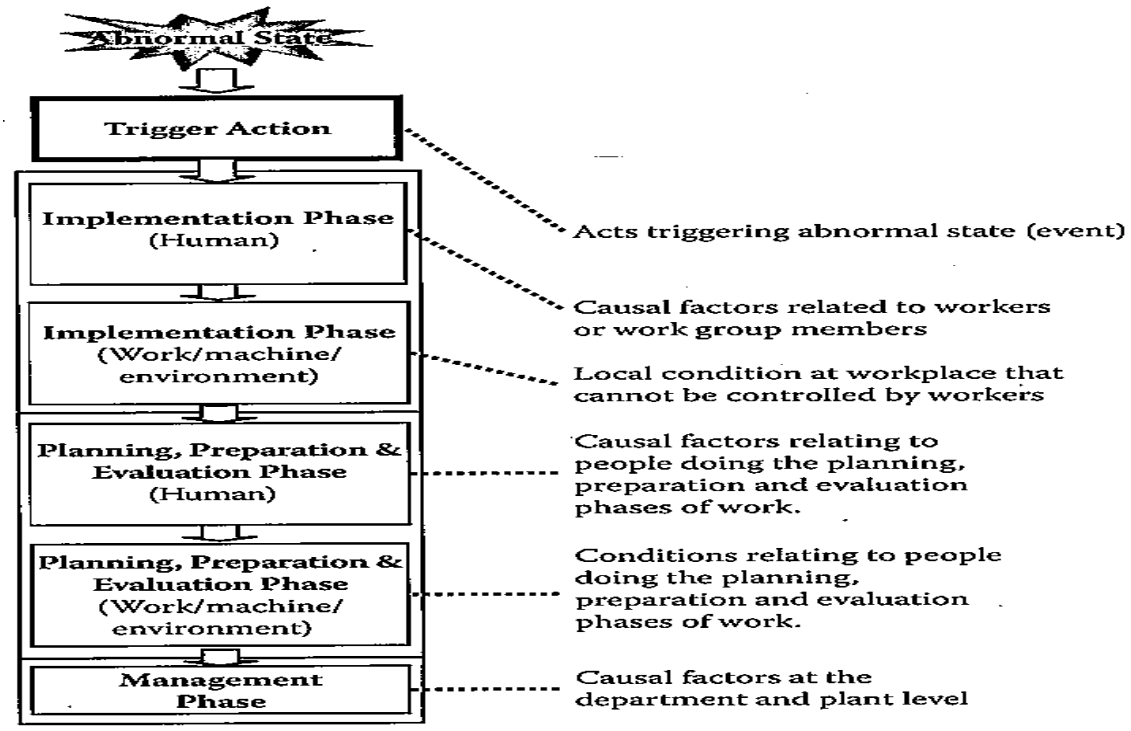


Figure 2 Basic framework for human error event analysis.

This framework is applied to a causal analysis (Step 3 above) after identifying trigger actions. First, one examines the factors concerning personnel involved at implementation phase, which is the working level. These factors concern workers or work group members. Next, one examines local workplace factors such as task demands and work environment. After that, one examines work control such as preparing procedures and work packages. Finally, one discusses management factors such as training, quality control, and safety culture. Figure 2 shows that the scope of the factors discussed is gradually broadened. Thus, analyzing various factors, ranging from those directly related to errors to management, leads to identification of problems in the whole organization.

The Procedure of HINT /J-HPES

In order to permit investigators who do not have sufficient knowledge concerning human factors and analysis experience to identify causal factors and to develop countermeasures, CRIEPI reviewed the analytic procedure of the J-HPES (Takano, Sawayanagi, & Kabetani, 1994) by reflecting the basic framework of Figure 2 (Hirotsu et al., 2006). The revised procedure, named HINT/J-HPES, comprises four stages. ("HINT" is not an acronym, but was added to the name of the method because the revised version includes enhanced hints, in the form of the basic framework, for causal analysis.) Stages 1 and 4 have not changed from those of the original J-HPES. Gathering information for Stage 2 has been enhanced by using the causal factor reference list (Figure 3), with the basic framework (Figure 2) as a reference. The framework

(Figure 2) has also been applied to the causal analysis (Stage 3) to guide the search down to the management factors.

Work Phase	Types	Categories	Subcategories (example)
Imple-mentation phase	Human	Communication	Pre-job briefing (Work direction etc.) Communication during work (Reporting, communicating, counseling etc.) Turnover (Coordination, turnover etc.)
		Work practice	Execution (Procedure use, self checking, housekeeping etc.) Check (Hold point etc.) Cleanup (Cleanup of workplace etc.)
		Psychological	Memory (Memory lapse, preoccupation etc.)
Manage-ment phase		Rules (Department/Plant)	Rules & regulation, guidelines, etc.

Figure 3 Causal factors reference list.

Stage 1: Understanding of events

A timeline of what happened before the event is consolidated in the form of an event sequential table (see Figure 4). In the second column of this table, abnormal machinery states are described. Next, each abnormal state is examined to see whether it was due to a human activity. If so, the activity is defined as a trigger action. Then, a series of activities of the workers who were associated with the trigger action is described. Finally, actions or communications that either induced the trigger action or led to it being overlooked are specified as contributing actions.

Date/ Time	Abnormal State	Work Phase	Acts & Communications				Problems	
			Planning manager	Job supervisor	Worker A	Worker B	Trigger Actions	Contributing Actions
5/14		Planning	Work permit	Prepare procedure				Compiled procedure based on examples of maintenance during power outage
5/18 10:30		Implementa-tion		Supervise other job	Check terminal number ↔	Inspect controller A		Worker B used un-insulated screwdrivers
14:00				Supervise other job	Check terminal number ↔	Inspect controller B		Worker B held two screwdrivers in one hand
14:30	Blown fuse					Survey controller B	Made the terminals short-circuit	

Figure 4 Event sequential table (with examples).

Stage 2: Gathering and Classifying Information on Causal Factors

In this stage, interviews and field investigations concerning trigger actions and contributing actions clarified in Stage 1 are carried out in reference to the causal factor categories listed in the

form for causal factor data (Figure 5). This form is based on the causal factors reference list (Figure 3). Any collected information is classified and filled into the form. Contributing actions identified in Stage 1 are classified as causal factors of "communication" or "work practice" of "implementation phase [human]" or "planning, preparation, & evaluation phase [human]." After the gathered information is filled into the form, possible contributions to the trigger actions of each column are evaluated in discussions among investigators, and the result is recorded in the evaluation column. If the description seems to have contributed directly or indirectly to the occurrence of trigger actions, a Y will be placed in the evaluation column. If not, an N will be placed in the evaluation column. Neglecting the human factors viewpoint in data gathering is prevented by confirming that information corresponding to each category of this form is present.

Work Phase	Types	Categories	Factors	Evaluation
Implementation Phase	Human	Communication	Worker A failed to warn worker B about improper handling of tools	Y
		Work Practice	Worker B held two screwdrivers in one hand	Y
			Worker B used an un-insulated screwdriver	Y
		Psychological Factors	Work group members were not made aware of short circuit danger during pre-job briefing	Y
		Physical, Physiological Factors	Work group members had no problem in their health	N
		Knowledge, Skill	Worker B had no experience in handling live circuits	Y
	Work	Work Characteristic	The task was monotonous and repetitive	Y
		Work Hour	The schedule was tight	Y
Planning Phase	Human	Communication	Supervisor had not told workers about short circuit danger	Y
		Work Practice	Supervisor compiled the procedure based on examples	Y
Management Phase				
		Organizational Culture		
		Rules (Department/Plant)		

Figure 5 Form for causal factor data (with examples).

Stage 3: Causal Analysis

In this stage, the conceivable causal factors are analyzed to draw up a causal relation chart in the format shown in Figure 6. The basic idea of the analysis is to ask the question "why" repeatedly and to use the basic framework of Figure 2 to deepen the analysis. For each trigger action, a fault tree-style causal relation chart is created to examine the causal factors listed in Stage 2. At this point in time, causal factors that form the basis of each trigger action are explored as far as possible in accordance with the five levels of the basic framework shown in Figure 2. The part

where the examination is insufficient (dotted line frame in Figure 6) can be clarified by associating a classification framework to the causal relation chart.

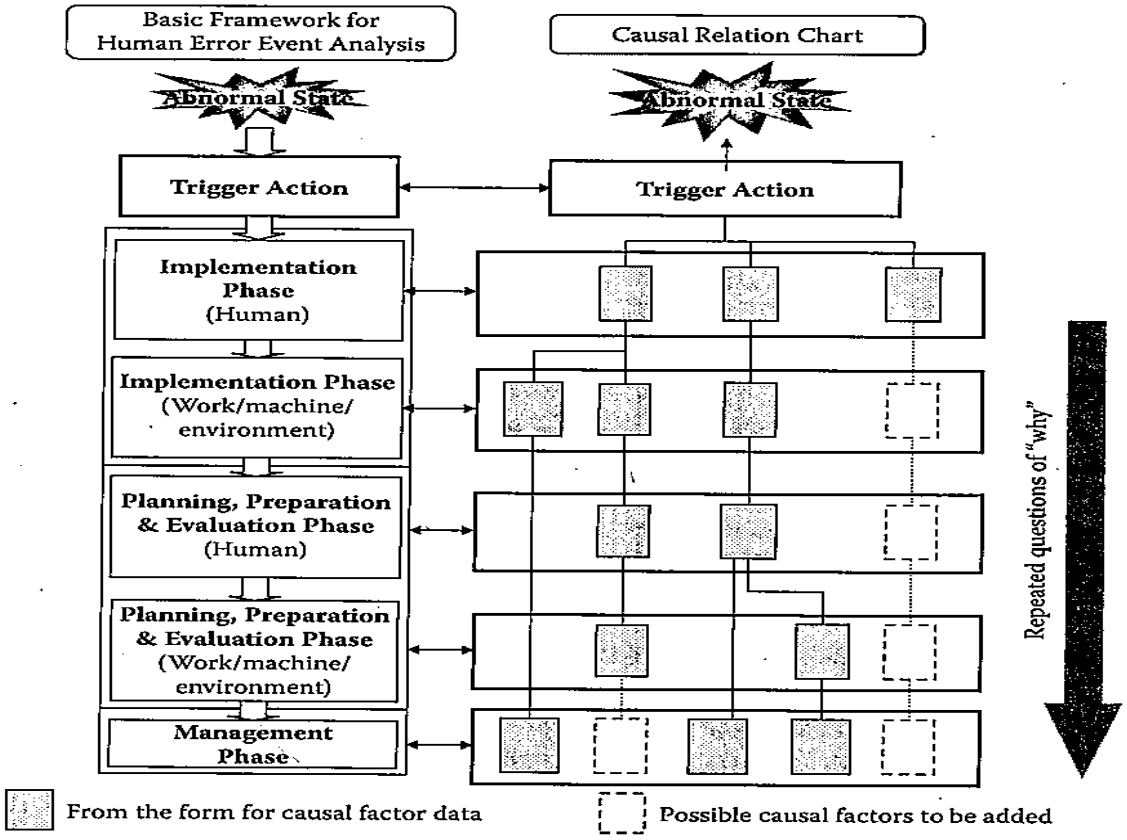


Figure 6 Causal relation chart (HINT/J-HPES).

The analysis result can be fulfilled by supplementing such shortages with additional data collections. Through this procedure, investigators will become aware of causal factors they did not take notice of in the previous J-HPES procedure and will thereby be able to obtain more satisfying results. In most cases, latent problems in the management phase are not mentioned, particularly during the interview of Stage 2. By referring to the basic framework, investigators try to find out the latent factors in management that may have contributed to the causal factors listed in Stage 2 and linked in the causal relation chart. An example of a causal relation chart can be found in Figure 7.

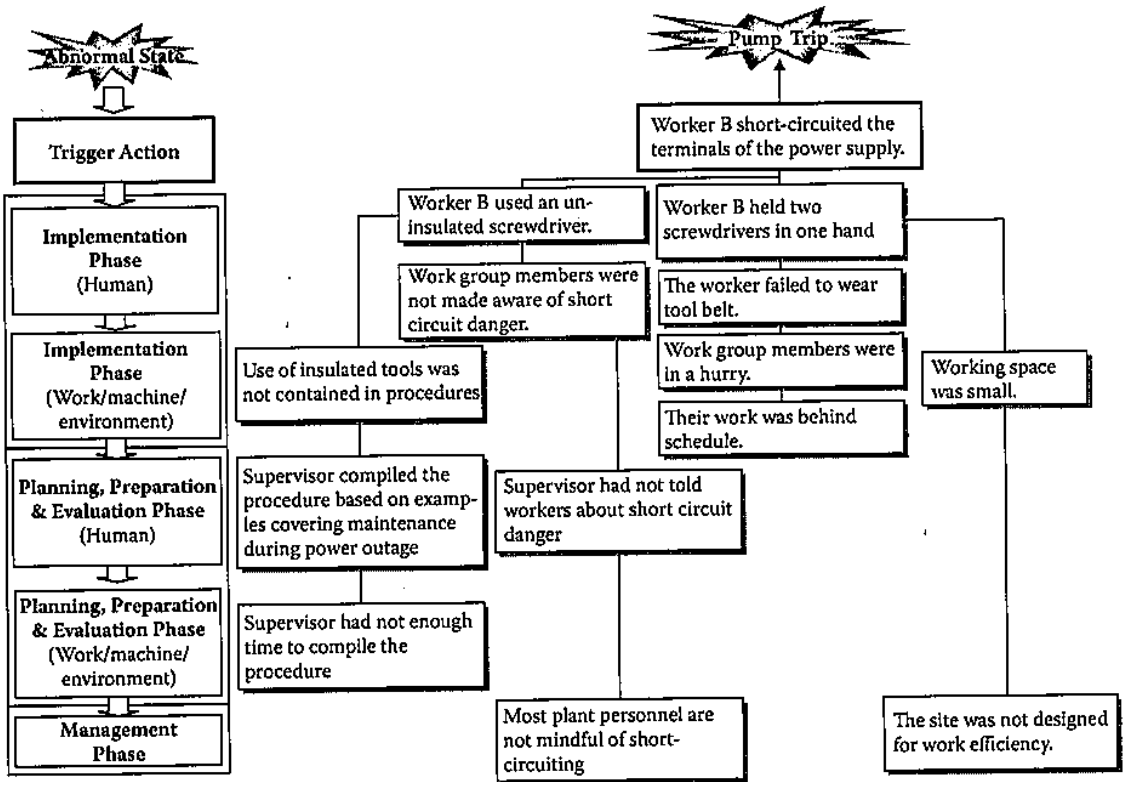


Figure 7 An example of causal relation chart (part).

Stage 4: Proposing Countermeasures

The fourth and final phase in HINT/J-HPES is to develop countermeasures for the purpose of correcting problems identified in Stage 3. Table 1 presents a form for countermeasure proposal.

First, specific countermeasures are developed for the trigger action. The countermeasures are selected based on the following criteria:

- Providing a means of averting an abnormal state being caused by a trigger action
- Providing a means of preventing the occurrence of a trigger action

Next, specific countermeasures are developed for each causal factor identified in Stage 3. The countermeasures are selected based on the following criteria:

- Providing a means of averting a harmful effect of a causal factor
- Providing a means of preventing the occurrence of a causal factor

In addition, the following four categories of countermeasures are shown on the form for countermeasure proposal, in the order of the effect of the prevention of recurrence:

1. Equipment improvement (improvement of the machinery, fail-safe, etc.)
2. Working environment improvement (indication bill, the improvement of the tool for operation, etc.)
3. Improvement of procedures and work management method (improvement of work management method, revising procedures, etc.)

4. Training/familiarizing (training for safety work, provision of information, calling for attention, etc.)

These categories can assist investigators in coming up with various countermeasures. An example of a countermeasure proposal can be found in Figure 8. It looks as if many countermeasures could be proposed by following this procedure. However, because each countermeasure can address several causal factors, the number of countermeasures will not be proportional to the number of causal factors. Countermeasures selected for implementation can be prioritized if the resources are limited.

Table 1 Form for Countermeasure Proposal

Level	Description of Countermeasures	
	Equipment Improvement	
	Working Environment Improvement	
	Improvement of Procedures and Work Management Method	
	Training/Familiarizing	
Level 1 [Trigger Action]	Equipment Improvement	
	Working Environment Improvement	
	Improvement of Procedures and Work Management Method	
Level 2 [Implementation Phase]	Training/Familiarizing	
Level 3 [Planning, Preparation and Evaluation Phase]	Equipment Improvement	
	Working Environment Improvement	
	Improvement of Procedures and Work Management Method	
	Training/Familiarizing	
Level 4 [Management Phase]		

Level	Description of Countermeasures	
Level 1 (Trigger Action)	**Equipment Improvement**	–
	Working Environment Improvement	(1) Have all bare wiring in control cubicles covered by insulation.
	Improvement of Procedures & Work Management Method	(2) Stipulate by rule to have this kind of job done with power cut out.
	Training/Familiarizing	–
Level 2 (Implementation Phase)	**Equipment Improvement**	–
	Working Environment Improvement	Same as (1) above in Level 1
	Improvement of Procedures & Work Management Method	Same as (2) above in Level 1 (3) Add provision in textbooks for preventing electrical accidents: Avoid work on live circuit in so far as possible. When indispensable, only use insulated tools. (4)
Level 4 (Management Phase)		(13) Include considerations of maintainability in the design of cubicles. Same as (3)(4)(9)(10) above in Level 2

Figure 8 An example of countermeasure proposal (incomplete).

Looking for Commonalities among Human Error Events

Because serious events are rare, it is essential to be able to recognize latent weakness by looking for commonalities among minor human error events (i.e., events where the outcomes are not significant), and from this to address the problems with the entire organization. CRIEPI therefore developed a procedure for finding commonalities among accumulated analysis results of human error events (Hirotsu et al., 2006). Using the basic framework introduced in Figure 2, CRIEPI created a diagram that shows the procedure for finding commonalities among events (Figure 9).

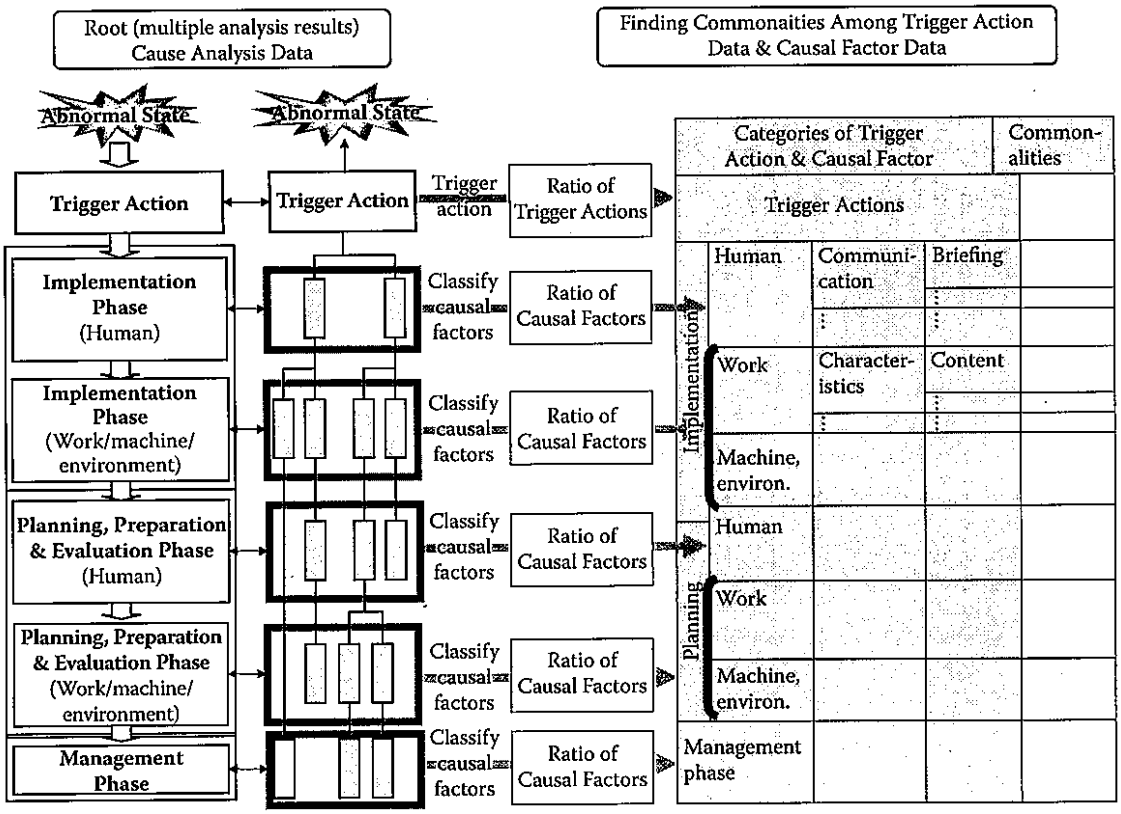


Figure 9 An image of finding commonalities among event databased on the basic framework.

Regarding trigger actions, trigger action data of analysis results of multiple events within a certain time frame (e.g., in the past year) are classified according to the trigger action categories (Figure 10), which were obtained by classifying trigger action data of human error events at Japanese nuclear power plants. The most prevalent trigger action categories are determined on the basis of the ratio of each category occupying the total number of error occurrence. This means that if three of ten trigger actions are classified in a category called "skip of an operation step," then the category occupies 30% of the total trigger actions; this should be recognized as a characteristic error type.

As to the causal factors, the data from the analysis results of multiple human error events can be classified according to the subcategories of causal factors (Figure 3). The most prevalent causal

factor subcategories are determined on the basis of frequency of occurrence of each subcategory against the total number of error occurrence. In other words, the finding that the factors concerning "communication during work" are related to seven of ten trigger actions should be interpreted to mean that "it is a characteristic of the organization that is common to 70% of the total number of trigger actions there." By this method, the analysis result can avoid being affected by just a few events with many causal factors involved.

Moreover, in terms of the characteristic trigger action categories and causal factor subcategories identified above, commonalities are extracted on the basis of description of each concerning action and causal factor. Take the case of "communication during work," where there are possibilities such as inadequate reporting and the vague instructions of the boss. You therefore further examine the descriptions of causal factors related to seven trigger actions classified as "communication during work" in order to extract concretely commonalities of inappropriate communication.

This method is effective because the trigger actions and causal factors affecting multiple events will be recognized as problems, even if they are perceived as having little significance for an individual event. For example, a causal factor such as "using inappropriate tool" of a minor event might be addressed by the workgroup performing similar work activities. However, if the recurrence of similar problems (factors) is identified by analyzing multiple events, the basis for managing tools or instruction for selecting them will be fundamentally reviewed. Thus, identifying problems as the characteristics of an organization and actively coping with them will improve the resilience of the entire organization against human errors.

Trigger Action Mode of J-HPES	Categories for Operations	Categories for Maintenance
Omission	• Overlooking abnormal condition • Skip of an operation step	• Overlooking abnormal condition • Skip of a maintenance step • Omission of preventive maintenance and monitoring
Drop, contingence, falling, intrusion	• Hit/knock together	• Hit/knock together • Contacting bare live part • Fall • Foreign material intrusion
Wrong object	• Wrong unit/train/component	• Misconnetion and miswiring of terminal • Wrong unit/train/component
Improper manipulation/ work amount	• Insufficient manipulation of valve	• Insufficient tightening of terminals • Insufficient torque of bolts

Figure 10 Categories of trigger action (for nuclear power plant).

Acknowledgments

The contents of this section are quoted from the following reference:
Yuko Hirotsu (2009). A Management Process for Strategic Error Prevention, Safer Complex Industrial Environments: A Human Factors Approach, pp93-111, CRC Press.

References

Center for Chemical Process Safety of the American Institute of Chemical Engineers (CCPS) (1994). *Guidelines for preventing human error in process safety*. New York: American Institute of Chemical Engineers.

Hirotsu, Y., Ebisu, M., Aikawa, T. & Matsubara, K. (2006). *A trend analysis of human error events for proactive prevention of accidents — Methodology development and effective utilization*, CRIEPI Rep. Y05010 (in Japanese).

Paul-Stuve, T. (2005). *A practical guide to the why–because analysis method — Performing a why–because analysis*. (http://www.rvs.uni-bielefeld.de/research/WBA/WBA-Guide. pdf, accessed August 11, 2008).]

Reason, J. (1997). Managing the risks of organizational accidents. Aldershot, UK: Ashgate.

Takano, K., Sawayanagi, K. & Kabetani. T. (1994). System for analyzing and evaluating human-related nuclear power plant incidents. *Journal of Nuclear Science Technology*, 31, 894–913.

2. Systematic Approach For Error Reduction (SAFER)

Outline of the Incident/Accident Analysis Method-SAFER

This section presents an outline of SAFER, an incident/accident analysis method based on human factors engineering principles described previously. The name SAFER, meaning Systematic Approach For Error Reduction, was originally developed in 1997 as H^2-SAFER by the TEPCO HFG (see Yoshizawa, 1999). (H^2 stands for Hiyari-Hatto, which is the Japanese term for near misses.) It was considerably improved in 2003 and renamed SAFER. Refinements are still continuing in an effort to provide a better and more usable method.

Background and Features of SAFER

H^2-SAFER was a product of field-oriented or fact-oriented thinking. Because a number of error-inducing factors were found by the analysis of real accidents, it led to the idea that analyzing an accident should reveal the whole set of background factors. Effective analysis and corrective activities are usually performed by people on the site rather than by external method specialists. There is therefore a need for a handy analysis method that is easy for the on-site people to use and that helps them reveal the whole set of background factors for an incident or accident. This motivation for developing H^2-SAFER remained unchanged during the revision that changed it to SAFER.

The main features of SAFER can be summarized by the following points:

- It is convenient for everybody to use: Once the basic notions and the steps of analysis have been learned, persons on-site as well as the specialists in methodology can use it easily.
- It is applicable to various events: The target events cover everything from serious accidents to near-miss incidents and are not restricted to human errors but include problems in facilities and organizational matters.
- It is useful for developing a common way of thinking: The basic notion of human factors engineering, and the knowledge about how surroundings can lead to accidents, is far more important than procedures and formats. The use of SAFER can help a person acquire the underlying notion, the viewpoints, and the way of thinking, and to share them on-site or in the office.

Three Stages in the Framework of SAFER

Neither a good analysis of accidents nor effective means of correction can be produced if one looks only at the moment when the erroneous actions and/or accidents happened. What happened, the errors or accidents, is the result of something else. In analyzing an event TEPCO therefore have to trace the history of how a trigger was induced and how it developed into the final consequences. TEPCO have to reveal the whole set of background factors related to the history, and this should be the grounds for effective countermeasures. To realize this idea, TEPCO proposed that the following three stages, which constitute the framework of SAFER:

1. Fact-finding: Develop the right understanding of what happened during the event and find the related facts.

A first step is to arrange information and make an event flow chart, both to correctly understand the details of the event and to share them among participants. One way is to align the persons and facilities concerned along the horizontal axis of the chart and to show the flow of time on the vertical axis. The next step is to enter every piece of information onto the chart using simple phrases, and then to connect each piece with arrows to clearly show the flow and development of the event.

2. Logical investigation: Use multi-sided analyses to find the causality among the various background factors behind the event.

Based on the information in the chart, one should logically investigate the background factors behind the event in order to produce a background factors causality diagram, which represents the causal relations among the factors. This diagram is similar to the fault tree that is generally used in describing the failure analysis of mechanical systems. Based on the notion of human factors engineering, it provides a complete view of the background factors and shows how various factors are linked or interrelated and how they finally resulted in the event. It is necessary to make a proper diagram (i.e. to represent all factors and their causal relations as correctly as possible) in order to develop effective countermeasures. On the basis of their on-site experience, TEPCO have therefore prepared considerable guidance, some of which will be mentioned in the following sections.

3. Preventive measures against background factors: Consider how to cut off the causality in order to prevent the event from recurring.

As the last step, try to develop preventive measures to cut off the causality among the background factors that caused the event, according to the background factors in the diagram. Then decide on the order of priority to implement preventive measures based on the evaluation of their effect, residual risk, and difficulty of execution, such as cost and lead time. A proper diagram logically shows the candidate factors that can be used to take preventive measures. Together with the evaluation of their effect and residual risk, this provides a comprehensive viewpoint that enables us to decide efficiently on useful preventive measures. TEPCO have also at this stage prepared considerable guidance to serve as a help to think about effective preventive measures, as well as a method to evaluate them. All of this is based on the notion of human factors engineering.

The importance of these three stages derives from the purpose of analysis, which is to prevent the undesirable event from recurring. In order to prevent an event from recurring, countermeasures are needed to cut off the causality relations among the background factors that

induced the event. This demands a comprehensive and correct representation of the factors and causality relations, which in turn requires grasping a wide range of facts related to the event.

The SAFER procedure embodies these three stages and further splits them into eight steps, as shown in Figure 1. The first step, understanding the notion of human factors engineering, occurs before the first step. The first stage corresponds to Step 2, the second stage to Steps 3 and 4, and the third stage to Steps 5 and 6, respectively. Steps 7 and 8 lie beyond the SAFER desktop analysis and are not easy to generalize as method; therefore, TEPCO provide only a few remarks for their implementation. Note that in the actual incident/accident analysis, Steps 2-4 (or sometimes Steps 2-6) are not necessarily sequential but may be repetitive, because not all information about the event is ready in advance.

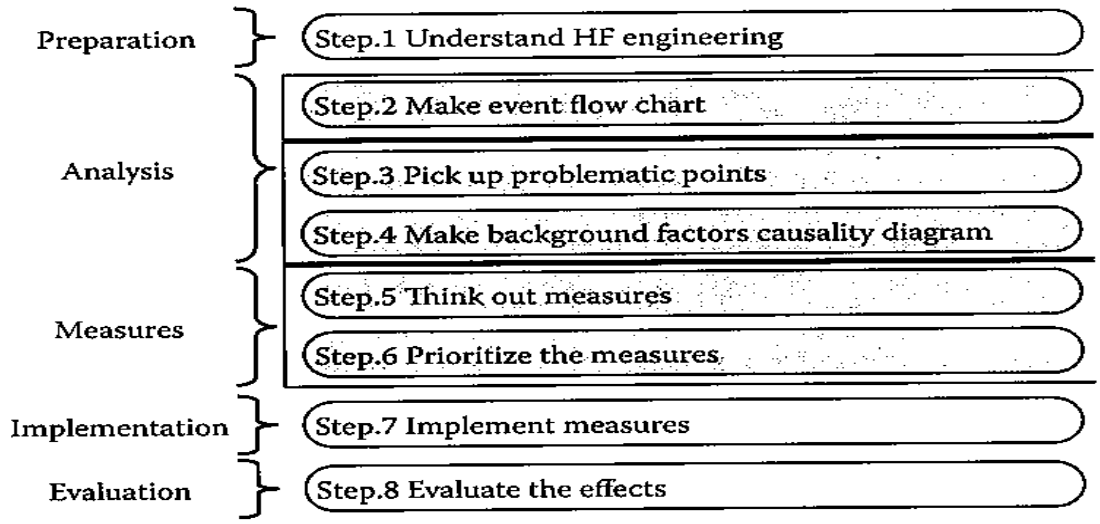


Figure 1 Procedure of SAFER.

Improvement of SAFER based on Experiences On-Site

In order to contribute to reducing incidents and accidents related to human erroneous action, the Human Factors Group has promoted SAFER within TEPCO. Through this activity TEPCO have found many cases where background factors were not properly investigated and/or where preventive measures seemed ineffective, even though the persons doing the analysis followed the SAFER procedure. The following briefly describes some typical issues that were found, together with the corresponding improvements that have been made to SAFER during the last few years:

Issue 1.Place more emphasis on procedure and mode and less consideration on why errors or accidents were induced.

This issue relates to Steps 2-6 in the SAFER procedure represented in Figure 1. One typical misuse of SAFER is that background factors are classified by the m-SHEL model. Although the use of the m-SHEL model or the classification of background factors is not bad in itself, neither of them is essential for using SAFER. It is more important to make a logical

investigation of the background factors that induced the errors or accidents than to classify them. The m-SHEL model is furthermore not a strict model that can be used to prescribe viewpoints but more like a loose framework of reference that can be used to bring out multiple viewpoints in investigation.

Preventing an over-adherence to procedure and a misuse of model is a difficult issue in performing an event analysis, and a simple improvement of the procedure or the guidance will not be sufficient. TEPCO therefore first tried to improve the procedure by adding as a first step the idea of understanding the notion of human factors engineering (Figure 1). Because the problem was an outcome of persistently following the procedure, TEPCO explicitly built in the basic notion as the first step. Besides this improvement, TEPCO prepared some guidance for how to make a background factors causality diagram, such as "Do not stop searching for background factors when you find a factor related to a person's action or consciousness." This continuation rule encourages the analyst to pay more attention to surroundings and to the context that induced the consequences.

Issue 2. Unclear causality between consequences and background factors, or poor grounds to show the effectiveness of preventive measures.

This issue is mainly related to Steps 4 and 5 in the SAFER procedure (Figure 1). An example of unclear causality is, for instance, to ascribe an outcome (e.g., a worker received a burn) to an arbitrary operation of the injured worker. Although this sometimes might be a reasonable guess, it does not explain why the arbitrary operation led to the outcome (the burn). The uncertainty of such a cause-effect relation weakens the basis for claiming that countermeasures taken to prevent the operation in question will be effective to prevent future instances of burns.

This issue of unclear causality has long been recognized as important, and TEPCO have used their experience to prepare advice on how to appropriately investigate causality, as mentioned in the following sections. This underlines that the basic principle of SAFER is to reveal the causality among background factors, and to produce preventive measures to cut off the causality. Although this in some ways is similar to a fault tree analysis, as mentioned previously, the uncertainty of human actions means that it does not require the same detailed and strict procedure. In order to explain this principle in an easily understandable way, TEPCO prepared some illustrative materials, as shown in Figure 2. This shows the difference between their background factors causality diagram and a cause-and-effect diagram that often is used in quality control activities.

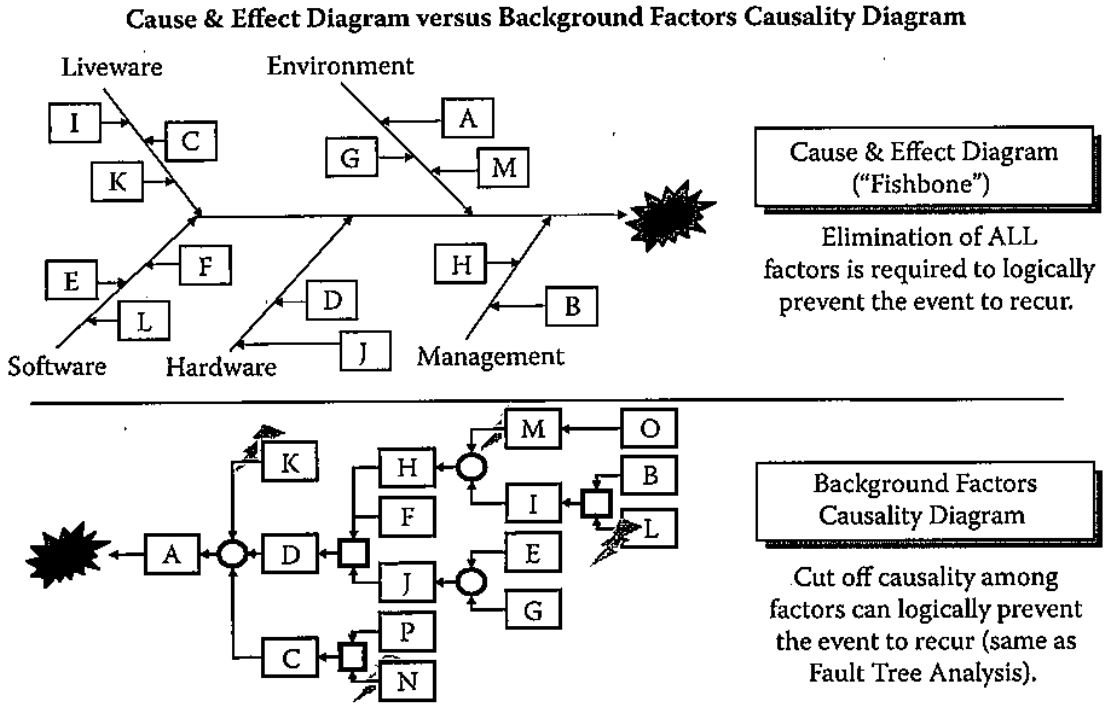


Figure 2 An example of illustrative material to explain the basic principle of SAFER.

Issue 3. Logical jumps in investigating the causality between background factors.

This issue relates to Step 4 in the SAFER procedure. It is important that the logical investigation of background factors (i.e., an investigation of the underlying causality) is free of logical jumps, because otherwise the effectiveness of a proposed measure to cut off the causality cannot be justified. Basically, the investigation is performed by asking why this result or factor is induced, but it is difficult to think in this way without sometimes making logical jumps. TEPCO therefore prepared some guiding principles on how to support a logical investigation, as illustrated in Figure 3. For instance, subdivide what happened and observe it physically or verify the logic of causality by backtrack; in other words, if it is found that A is caused by B, then verify whether B really causes A. By using the guiding principles, the determination of a direct cause of, for example, a burn accident should not point to the worker's arbitrary operation, as mentioned previously, but instead point to the coexistence of "something being hot" and "that something is touched." This is a more appropriate explanation of how the burn physically occurred. It also verifies the causality, because touching something hot is certain to result in or cause a burn, whereas an arbitrary operation is not.

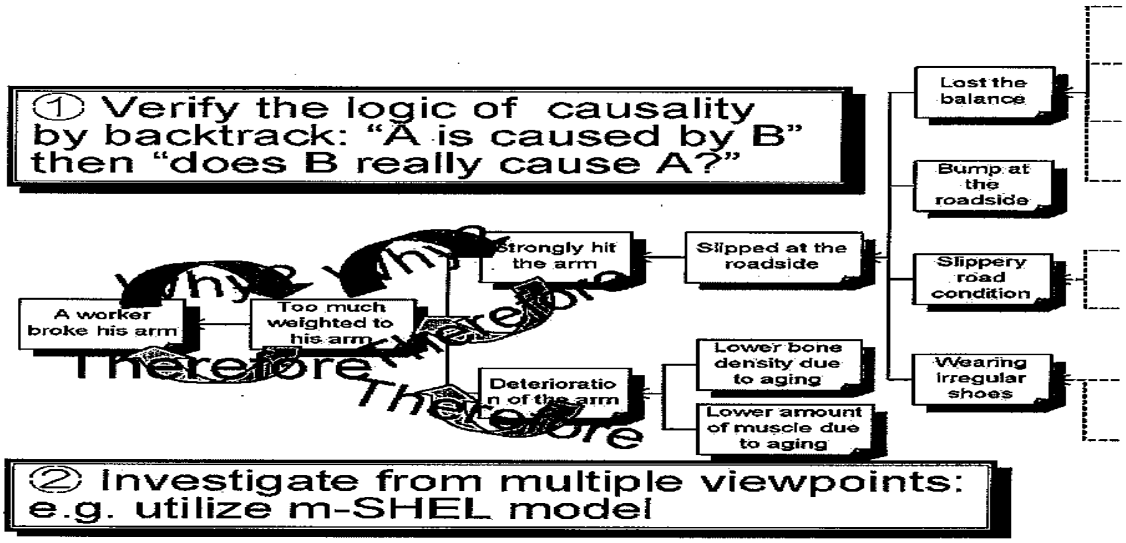


Figure 3 An example of know-how to make a proper causality diagram.

Issue 4. Many requests for a comprehensive guide on how to think out preventive measures.

This issue relates to Steps 4 and 5 in the SAFER procedure. A guideline named H²-GUIDE was given in H²-SAFER. This guideline covered a wide range of ideas for preventive measures, from "elimination" to "preparation," based on the notion of an error-proof technique (i.e., trying to make sure something is error proof). Although the H²-GUIDE was still very useful, TEPCO improved it to make it more comprehensive. It is now an easy-to-use guide that consists of eleven steps, as shown in Figure 4. At the same time, TEPCO also renamed it simply "GUIDE." The improvements came about in the following way. TEPCO first specified that the object of countermeasures is to prevent or minimize damage resulting from accidents related to human erroneous action. TEPCO then introduced a distinction between two phases, prevention of errors and mitigation of effects, and two approaches, improvement of surrounding factors and improvement of individual abilities (individualistic countermeasures). This altogether resulted in the eleven steps shown in Figure 4. A detailed explanation of this solution is provided in Kawano (2006). (The individualistic countermeasures do not refer to individual psychological issues, but rather to established human factors principles and cognitive models of human behavior.)

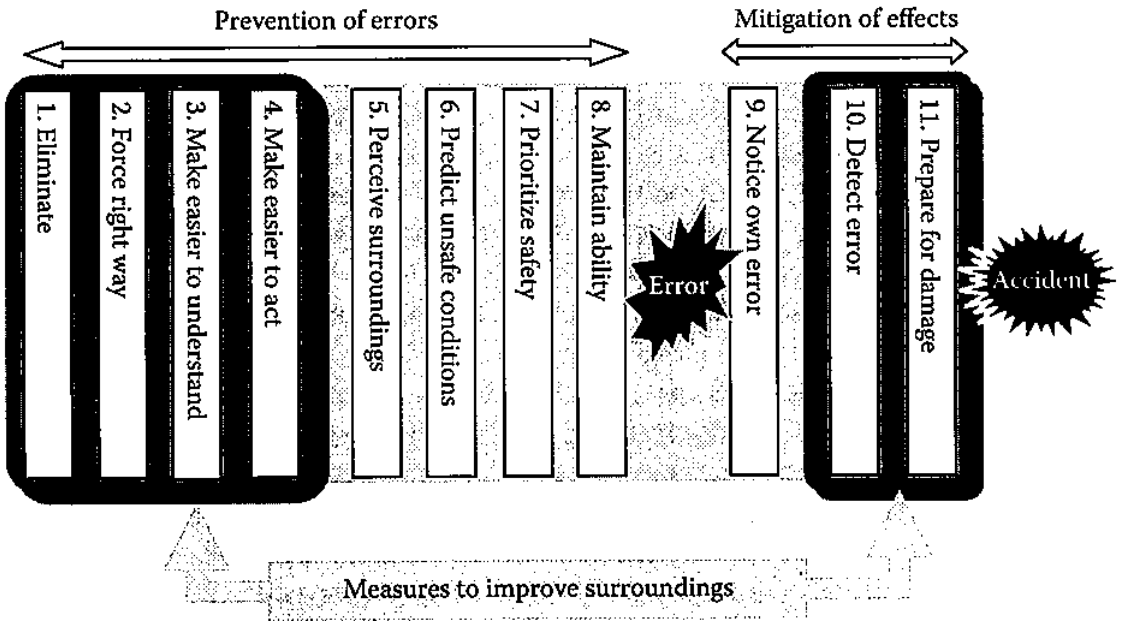


Figure 4 A guideline to think out measures "GUIDE".

Issue 5. Inadequate examination of candidate preventive measures may lead to a preference for individualistic countermeasures.

This issue relates to Step 6 in the SAFER procedure. When the candidate preventive measures are evaluated, individualistic countermeasures are often chosen even when countermeasures to improve the surroundings are present. This may be because it is common to examine preventive measures using their cost rather than their effectiveness as a criterion. One reason is that the true effectiveness of a measure generally is difficult to evaluate quantitatively. Another reason is that the thinking often seems to focus on the binary choice between taking some measure to prevent a recurrent and taking no measure.

In order to overcome this, TEPCO proposed a quasi-quantitative evaluation of the effectiveness of a measure, with GUIDE (Figure 4) as a basis, grading each on a scale from one to ten points. Residual risks and side effects of a measure are also introduced in order to promote a risk-oriented evaluation, for instance, to consider how much a measure decreases the risk of occurrence of an accident and/or damage. A combination of these evaluations, with the difficulty of execution, such as cost and lead time, enables a realistic examination of countermeasures, while putting stress on their effect.

Description and Usage of SAFER

Besides the improvements described above, TEPCO continuously evaluate and refine their experience in a detailed manner and continue to develop instructional materials to improve SAFER, while keeping the basic notion and the overall framework unchanged.

The following sections briefly describe the eight steps in the SAFER procedure and its usage as of July 2008.

Step 1: Understand HumanFfactors Engineering

The first step of SAFER is to understand the notion of human factors engineering, because this is the very basis for the other seven steps. This step is actually not an analysis activity as such but a preparation phase, and usually it is provided by an off-the-job course or lecture. TEPCO have developed some instructional materials, such as "e-learning contents," a reference book (Kawano, 2006), and presentation sheets. A standard set contains approximately sixty presentation sheets and is used for a one-hour course. This standard course consists of three parts; (1) providing arguments against the conventional view of human errors, (2) illustration of human characteristics and surrounding factors that affect human behavior, and (3) explanation of the notion of human factors engineering. In all three parts TEPCO include many small exercises and refer to many real incident/accident cases. Their experience has shown them that in order for persons to gain a clear understanding of human factors engineering and to utilize it as the basis of analysis activities, they must also be exposed to practice and case studies in addition to general knowledge. Their original "counting up game," which is a simple mental calculation in a context that induces the person to forget a figure carried, is an exercise in which people can experience their susceptibility to context.

Step 2: Make Event Flow Chart

This step is actually the first step of the event analysis work. The aim of this step is to understand properly what happened in the event and to share the information among participants. The process by which to make the event flow chart is very simple, as described in a previous section: line up the persons, facilities, etc., on the horizontal axis and show the flow of time on the vertical axis. After that, enter all pieces of information (actions, events) in the chart and draw arrows among them to show the information flow and the development of the overall event. It is useful to combine different sources of information to make the chart, such as evidence from an inspection of the scene, record of interviews with the persons concerned, documents about the task where the event occurred, etc. However, it is not necessary to have the complete information in advance, because the flexibility of the chart makes it possible to make additions and changes latter on.

The experience of how to perform a good analysis is also included in this simple step. Some of this experience may appear very common or even trivial, but TEPCO have found that it is worthwhile to provide such guidance explicitly:

- Information should be traced into the past to a certain depth so that potential background factors can be considered. Examples are planning of tasks, alterations of design, and change of team members. It is important that the analysis is not limited to the scene of the event.

• It is recommended to include all types of information, supplementary explanations, and even presumptions in the chart, although a strict discrimination should be made between facts and other kinds of information.

• Each piece of information should be written briefly, possibly by using a simple phrase. This is good not only for the easy understanding and sharing of information, but also for maintaining a neutral attitude towards the facts.

In most cases, this step is performed using many tags on big sheets of paper. TEPCO have also developed a simple support tool for this step using Microsoft Excel.

Step 3: Pick Up Problematic Points

Before beginning the investigation of background factors in order to make the causality diagram, one should pick up all possible problematic points from the event flow chart. This step is useful to make a thorough extraction of problems from the beginning to the end of the event. Some of these problems might not be obvious from the background factors found for the final consequences.

The possible problematic points not only include human actions but also deviations, unusual occurrences, and circumstances that might not be bad or problematic in themselves. As part of the work, it is possible to select pieces of information from the chart and transcribe them to other tags. For the convenience of the following analysis phase, it is recommended to add the subject of an action or a condition in this transcription. Each piece of information in the event flow chart need not refer to a different subject; several pieces in the same column may refer to the same subject.

Step 4: Make A Background Factors Causality Diagram

The aim of this step is to provide an overall view or set of background factors that logically shows how a combination of these factors can lead to the event. The first step is to select one problematic point as the target for which a recurrence should be prevented. This is usually the final consequences, such as the damage to a facility or a violation of a regulation. Other problematic points, such as an unusual triggering action, can also be the target, depending on the purpose of analysis. The second step is to investigate the background factors in order to make a causality diagram based on the information in the event flow chart, using the target as the starting point. Most of the problematic points picked up in Step 3 are generally incorporated into the diagram as background factors. If some points remain, it means that heterogeneous problems have been left untouched; these may possibly become other targets to be the subject of new causality diagrams.

It is necessary to make a proper background factors causality diagram in order to consider effective preventive measures, and this is therefore an essential step in the SAFER analysis. The key issues in the investigation are logical thinking and the use of multiple viewpoints based on

human factors engineering. As mentioned in the previous section, considerable experience is brought to bear on these issues, such as the verification of logic by backtracking causality, physical observations of what happened, continuation rules to prevent a premature stop of the analysis, and a reference to the m-SHEL model. Besides such basic guidance, TEPCO have also prepared advanced guidance, illustrated as follows:

•*Consideration of logical gates(i.e. AND and OR combinations of background factors).* If, for instance, there is an AND gate between factors that lead to an event, it is not necessary to develop countermeasures for every factor in order to prevent the event. This will in turn lead to an effective reduction in the number of preventive measures.

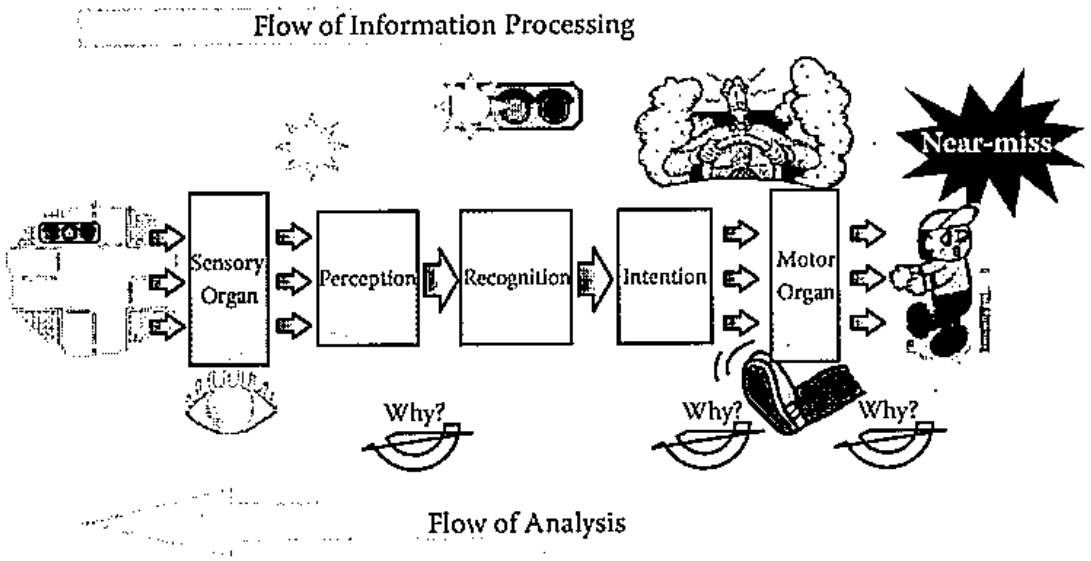


Figure 5 A reference to information processing model of human.

• *The use of a reference human information processing model to investigate background factors behind a person's actions.* Generally an action should be the product of a certain intention that depends on the person's knowledge, attention, recognition, and perception of information, all of which interact with the circumstances and the context. (see Figure 5).

• *Investigation using multiple perspectives and positions, not only for the persons concerned but also for partners, witnesses, and victims of the event*. Although background factors for these other persons often are not considered, because they are beyond the range of preventive measures, they often provide good hints for what TEPCO should do as effective preventive measures.

In most cases, this step is also performed using many tags and large sheets of paper. The support tool mentioned previously is also available here.

Step 5: Think out Preventive Measures

After describing the overall set of background factors with the causality diagram, the next step is to think out preventive measures by which to cut off the causal relations that lead to the event. A

typical misunderstanding is that preventive measures should be found for all factors at the very end of each chain of causalities. This solution certainly cuts off every chain leading to the event, so it is not entirely wrong. Yet it is neither essential nor efficient. It is instead important to cut off the chains anywhere possible in the diagram. If it is possible, for instance, to take concrete and effective countermeasures against a background factor close to the event, they will be both more efficient and more effective. It may often be difficult to take such countermeasures because background factors near the event are consequences rather than causes. In performing this step, it is important to show explicitly the correspondence between each measure and background factors, in order to clarify the aim of each measure.

Flexible and diverse ideas for preventive measures that differ from conventional examples or immediate restrictions are important at this step. To find these, TEPCO recommend the style of brainstorming, in order to make good use of other persons' ideas without criticizing them. In brainstorming, even wild ideas are welcome. Their comprehensive GUIDE (see also Figure 3) can help one think out effective and diverse countermeasures. TEPCO have also prepared a set of instructional material with many examples. Based on the notion of human factors engineering, the improvement of surrounding factors should precede the improvement of individual abilities; elimination-oriented ideas are also recommended as effective and reliable preventive measures. This view of priority is the base for the evaluation of effectiveness, as described in the next step.

Step 6: Prioritize the Countermeasures

Each measure proposed in Step 5 is prioritized by evaluating its effect, residual risk, side effect, and difficulty in execution. The effectiveness of a measure is graded on a scale from one to ten points according to the classification used in GUIDE (see Table 1). The numerical value of a point has no strict meaning, because this scale is mainly a numerical expression of the notions of GUIDE. These notions are that preventive measures are more effective if they depend less on an individual's ability or sense, and that the prevention of errors should precede the mitigation of effects. Note that the same preventive measures can differ in grading depending on their means. For instance, ensuring the proper execution of actions by means of a sensor and interlock system will correspond to eight points ("force the right way of doing things"), whereas it will be given only one point if done by self-check ("notice own error"). Difficulty in execution typically contains cost, leading time, and applicability. This should be considered before deciding on a measure, whereas residual risks and side effects should be considered afterwards. Examination of these topics encourages a risk-oriented and comprehensive evaluation of preventive measures.

This kind of evaluation can be used to decide the priority among preventive measures to be implemented. Some comments on this decision are illustrated in the following:

- Basically, a measure with a higher number of points for effectiveness gets a higher priority for implementation. This decision should ensure that the measure effectively cuts off

causality relations among the events. If only one measure with a small number of points for effectiveness is proposed, it is recommended to look for another measure with a higher number of points, or to combine the proposal with other preventive measures.

• For cases in which a measure with a smaller number of points for effectiveness is implemented, the residual risk should be made as clear as possible, and its effect should periodically be verified.

• Many preventive measures produce only a small effect. An effective and simple prevention of the recurrence of events can be ensured by making a proper background factors causality diagram and by taking preventive measures with a high score of effectiveness against the causality relations found by the analysis.

Table 1 Effectiveness Point by Classification Used in GUIDE

Elimination	10
Force the right way of doing things	8
Make things easier to understand; make things easier to do	4
Direct errors; prepare for damages	2
Perceive surroundings; predict unsafe conditions; prioritize safety; maintain ability; notice own error	1

Step 7: Implement Preventive Measures

In step 7, you implement the preventive measures that were prioritized in Step 6 by first building a concrete and detailed plan and then carrying it out. It is important to be clear about who is responsible for planning, preparation, and execution. The effects of step 7 are evaluated in step 8. Steps 7 and 8 go beyond a desk analysis, and the particular manner in which they should be carried out has not yet been established.

Step 8: Evaluate the Effects

Finally, the actual effects of the preventive measures taken should be evaluated after their implementation. Before the evaluation, you should verify that the preventive measures were definitely and properly executed. This evaluation will be performed by considering two sets of consequences: those related to the prevention of a recurrence of events and those related to the side effects. The former can be both quantitative and qualitative, such as a decrease in the number of events or a subjective improvement of the easiness of work, for instance. There will always be both good and bad side effects. Some examples are synergy from the improvement of surroundings, increasing busyness, or new types of problems such as automation-induced surprise. Quantitative effects of event prevention may be difficult to evaluate statistically because of the low rate of occurrences, and qualitative evaluations are therefore important.

Acknowledgments

The contents of this section are quoted from the following reference:

Yutaka Furuhama (2009). Beyond Procedures Development and Use of the SAFER Methods, Safer Complex Industrial Environments: A Human Factors Approach, pp113-131, CRC Press.

References

Kawano, R., & TEPCO Human Factors Group (2006) *Human Error wo Fusegu Gijutsu*. *Human Error wo Fusegu Gijutsu* is the original published titled in Japanese. An English translation would be "Techniques to prevent human errors."

Yoshizawa, Y., (1999) Activities for on-site application performed in Human Factors Group. *Proceedings of the 3rd International Conference on Human Factor Research in Nuclear Power Operation (ICNPO-III), Mihama, Japan*

3. Japanese Nuclear Energy Safety Organization (JNES)

Organizational Factors List (JOFL)

INTRODUCTION

The Japan Nuclear Energy Safety Organization (JNES) is working very hard to ensure the safety and reliability of the Japanese nuclear power operation and technically to support the Nuclear and Industrial Safety Agency (NISA). To be specific, the JNES is collecting, organizing and reviewing various information about nuclear incident and accident cases both inside and outside of Japan, looking particularly for factors that are harmful to human and organizational safety and reliability, in order to develop guidelines for judgment that appropriately match the current situation in Japan.

This section presents a regulatory perspective on analysis practices and trends in causes, and it describes the intention behind an enacted "Guideline for Regulatory Agencies in Evaluating Contents of Root Cause Analysis by Licensees". The objective is to provide a guideline on how to verify the appropriateness of the corrective actions and proactive measures implemented by licensees, based on a root cause analysis of events. This guideline takes four points into special consideration for adequate application. They are:

1 Encouragement of further activities of the licensees
2 Flexible interpretation of the intention
3 Versatility of the analysis methods
4 Concepts and consideration of no blame culture

Moreover, as a perspective for regulatory agencies, the guideline places special emphasis on ensuring the neutrality of the investigation team, the objectivity of analysis results, and the logic of the analysis method.

Approach to establishment a guideline and a standard for a root cause analysis

Up to the present, root cause analysis has been enforced by licensees as part of the self-controlled operational safety activities comprising corrective actions and proactive measures provided by the rules of quality assurance. However, the licensees' efforts have not been sufficient to rectify the shortcomings of the conventional method. Often, the licensees' approach to correcting non-conformance has been superficial; that is, it has been directed at the improvement of manifest events only, whereas the activities to analyze and improve the root cause, centered on organizational causes such as an inappropriateness of the management system, have not been adequately performed so far. Because of this, there have been frequent accidents and problems partly associated with organizational causes, the root causes of which have remained unaddressed.

Although the nuclear industry seems to have attained its maturity, the developments mentioned here make it clear that the industry should take thorough corrective actions and proactive

measures. The basis for this should be the root cause analysis, through which the latent organizational factors for each event are made clear, in order to make sure that they do not recur.

As a consequence, the process and the system for implementation of a root cause analysis have been defined in the regulatory rules, as provisions of quality assurance in the operational safety program, and the licensees have been forced to include them in their quality assurance program. In addition to this, NISA has provided regulatory requirements for the evaluation of how a root cause analysis is implemented by a licensee, as well as the requirements for the process of a root cause analysis in the rules. All licensees have been notified of these developments.

The regulatory requirements comprise the following four items:

1. The implementation of root cause analysis shall ensure the neutrality of the analysis, the objectivity of the analysis result, and the logic or consistency of the analysis method.
2. For events that have a significant impact on safety, appropriate corrective actions and proactive measures shall be carried out, and a root cause analysis for each event shall be implemented to ensure prevention of a recurrence.
3. Concerning other events that do not have a significant impact on safety, analysis of the accumulated data related to non-conformance shall be conducted after taking corrective actions, and a root cause analysis shall be implemented depending on the necessity to implement proactive measures.
4. Corrective actions and proactive measures should be based firmly on the result of the root cause analysis, and a specific implementation plan should be clarified and conducted without fail.

The implementation procedure of root cause analysis is shown in Figure 1.

Based on these requirements, the regulatory guideline for inspectors to evaluate the results of a root cause analysis implemented by a licensee was established in December of 2007. The regulatory guideline was developed via discussion by a subcommittee on a draft of a guideline worked out by NISA and JNES（Nuclear and Industrial Safety Agency, 2007）. The guideline is named Guideline for Regulatory Agencies in Evaluating Contents of Root Cause Analysis by Licensees. The Japan Electric Association (JEA) established the association standards (JEA, 2007) relating to a guide for implementation of a root cause analysis. These standards provide an adequate system, methods, screening, reporting, measures, effect evaluation of measures etc., relating to implementation of a root cause analysis. NISA has evaluated this and approved it as the standard to meet the regulatory requirements.

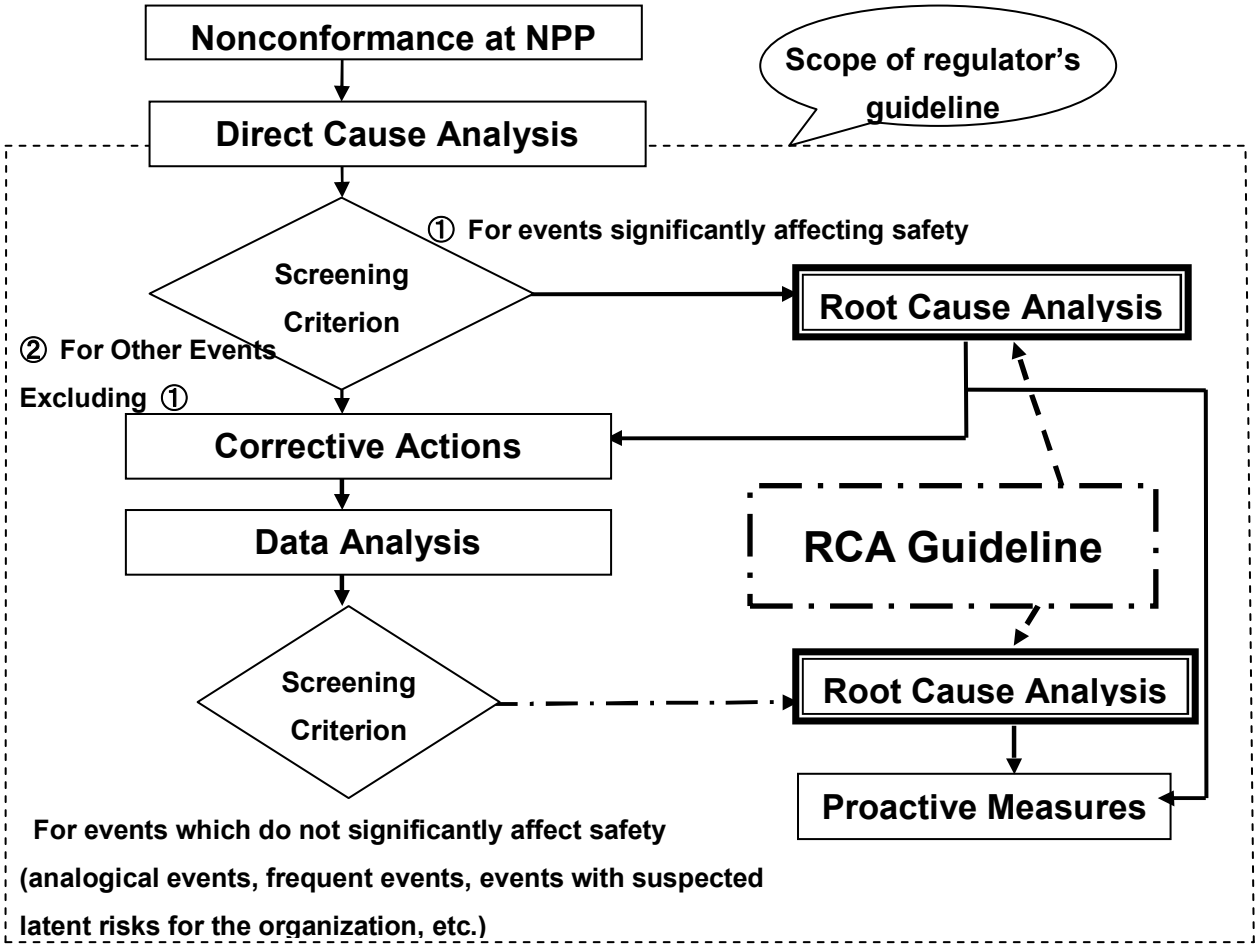


Figure 1 Process flow for enforcement of root cause analysis.

The enforcement of this regulatory guideline is expected to encourage the prevention of incidents stemming from organizational systems, due to thorough implementation of corrective actions and proactive measures. The following effects are expected from the enactment of this guideline:

・The definition of terms such as "root cause analysis," and "organizational factors," etc., will promote a common understanding between regulators and licensees.

・The provision of minimum requirements for events subject to implementation of a root cause analysis will encourage positive investment of resource in a root cause analysis and stimulates adequate common information for proactive measures among licensees.

・The provision of a requirement to ensure the neutrality of a setup for a root cause analysis is expected to ensure the reliability of results.

・The provision of a requirement to ensure objectivity in implementing a process of root cause analysis is expected to help identify or extract adequately organizational factors that are latent in a target event and to draw up adequate and substantial measures for the extracted organizational factors.

・The provision of a requirement to ensure the logic of the analysis method will lead to a more systematic account of organizational factors.

・The provision of a guide for evaluating the appropriateness of corrective actions and proactive measures is expected to help ensure checks on the status of implementation and effectiveness of actions.

Contents of the Regulatory Guideline

The regulatory guideline (hereafter referred to as just "guideline") provides the guidance to verify that the corrective actions and proactive measures implemented by a licensee, based on the results a root cause analysis, and are appropriate. The guideline takes four points into special consideration for adequate application:

1. In addition to the judgment of whether or not the root cause analysis satisfies the government requirements, an evaluation should be made with the aim to encourage further activities of the licensees to improve methodology, process and results of the root cause analysis.
2. In the event of any doubt about descriptions in the guideline, a flexible interpretation of the intention of the root cause analysis should be implemented rather than adhering to the specific wording.
3. When verifying the licensees' approach, positive discussion should be held with licensees on a continuous basis. Versatility of the analysis methods and concepts adopted by licensees should be allowed.
4. The regulators concerned should have sufficient awareness of the fact that there are various factors in the behaviors of the personnel involved in a non-conformance: In addition to the negative factors, such as misunderstanding, wrong judgment, and insufficient confirmation, there may be negative effects (influences) caused by excessive implementation of actions based on the expectation for positive effects, such as improvement of working environment, efficiency improvement, and the pursuit of cost reduction.

Guides to verify process and results of root cause analysis implemented by licensees

Based on the regulatory requirements for root cause analysis, three additional guidelines were developed to confirm the process and the result of root cause analysis:

1. The guideline to confirm that the investigation team is neutral
2. The guideline to confirm that the analysis results are objective
3. The guideline to confirm that the methodology used for analysis is logical

It has further been made clear that:

When applying the contents of the following descriptions, the guide for application and its depth should be judged based on the importance of each item seen from the analysis results and licensee's management system, instead of applying all the items in a uniform manner.

In other words, the guideline should be applied carefully and not in a routine or rule-based manner. An overview of each guideline is given in the following.

The guideline to confirm that the investigation team is neutral

For an accurate analysis implementation, the neutrality of the investigation team and non-suffering disadvantage in personnel evaluation must be assured. Also, to extract organizational factors, the interview with the senior manager is indispensable.

This leads to the following four guidelines:

1. The investigation team shall comprise other personnel that are not related to the area under investigation. The investigation team may include personnel that are related to the area under investigation, but the investigation team cannot include him in case of the serious events such as an event for which involvement of an organizational problem is suspected and an event with falsification of data or intentional fraud.
2. Access to the essential data shall be authorized. Further, implementation of research, including interviews with senior managers and the related functions, shall be ensured.
3. The individual who implemented the root cause analysis shall be protected from potential disadvantageous treatment associated with the analysis and its results.
4. The team leader or sub-leader who is in charge of the root cause analysis shall have experience in safety preservation activities in power plants, or shall understand such practice in addition to experience of education / training related to the root cause analysis.

The guideline to confirm that the analysis results are objective

To elaborate this guideline, the following five precise guidelines are introduced:

1. In the contents of events and problems, the concerned functions and individuals shall be kept anonymous and the behaviors concerned shall be described in details.

   Note: “Identification based on the anonymous basis” refers to the identification based on one’s responsibility, authority, and role in an organization. If multiple individuals have an identical responsibility, authority, and role, they shall be identified with symbols such as A and B.
2. Problems shall be clarified and described quantitatively as much as possible.
3. Organizational factors corresponding to the problem shall be clarified and described in details.
4. Actions corresponding to organizational factors shall be clarified and described in details.
5. For improved understandability, the specific example of each guideline is specified in the guideline.

The guideline to confirm that the methodology used for analysis is logical

For this guideline, the following six precise guidelines are introduced:

1. The root cause analysis shall systematically consider the perspectives of organizational factors and their causal relationship depending on the reported events. As a reference list of organizational factors, the JNES Organizational Factors List (JOFL) is provided.

   Note: Systematic analysis refers to the identification of the factors based on a specific framework and the narrowing of the targeted factors depending on the magnitude of impact on the results. This is done to prevent omission of any important factor to prevent recurrence of accidents caused by similar factors.
2. Trans-sectional analysis of events, data, and research results from various perspectives shall be conducted as necessary to explore common factors.
3. The analysis shall have sufficient dept to be able to improve inappropriateness of the management system.
4. Depending on the need, the possible inappropriateness of the past corrective actions and proactive measures shall be reviewed.
6. Depending on the need, difference factors caused by change and modification before and after the event concerned shall be analyzed.
7. Depending on the need, an analysis shall be conducted of whether or not a barrier was present to prevent event occurrence or human error, whether or not such a barrier was lost or dysfunctional.

The guideline to verify appropriateness of corrective actions and proactive measures

It is possible that some of the present reports for incidents do not include an actual plan or process of evaluation activities for corrective actions and proactive measures. To improve this situation, the following six guidelines are introduced:

1. Corrective actions and proactive measures corresponding to the root cause analysis shall be formulated.
2. If no action is taken, the reason for this shall be indicated clearly.
3. An effectiveness review of corrective actions and proactive measures shall be conducted and the extent of their ability to prevent events caused by a similar direct factor shall be indicated clearly.
4. An effectiveness review shall be conducted on the side effects associated with the corrective actions and proactive measures.
5. A specific implementation program of corrective actions and proactive measures (system, schedule, resources, follow-up method, method of evaluating efficacy, priority etc.) shall be identified clearly, accepted by the staffs concerned, and feasible.

6. The necessity and applicable range for cross-cutting development of corrective actions and proactive measures shall be reviewed.

Review of the guideline based on feedback from operational experience

Only two cases have been practically implemented by licensees under the new root cause analysis system that came into force in December 2007. They have been evaluated by NISA in accordance with this new established guideline. Obviously, additional actual use of this guideline will provide both licensees and the regulatory body with valuable lessons about root cause analysis. This will also provide essential feedback to the guideline. It is the intension to review the guideline continuously in the future.

Development of JOFL

The method used by a licensee for a root cause analysis should not be restricted by the regulatory body. A licensee should use a method that is recommended by an association standard (JEA, 2007). But the regulatory body expects licensees to adopt an adequate method and implement it correctly. It is also important that the essential organizational factors from various root causes analyses are considered together so that they can possibly be combined. In order to facilitate this, the JNES has prepared the JNES Organizational Factors List (JOFL) as a reference list for regulatory body to confirm the appropriateness of organizational factors found by the licensees' root cause analyses.

The JNES has developed a safety culture evaluation support tool, called SCEST, to characterize the fragility of safety culture (Makino, Sakaue, & Inoue, 2005; Safety Standard Division, 2006). The JNES has also developed an organizational reliability model (OR model) to identify organizational factors that may be disincentive of safety culture (Institute of Human Factors, 2003). The JOFL integrated these evaluation items with the readjusted organizational factors evaluation items to create a new original list (Safety Standard Division, 2007).

Reflecting the results of the application to the specific cases for which NISA implemented special audits, an original list was processed to produce the JOFL. This reference list is composed of six key factors structured that refer to a structure of 33 intermediate classifications (total 63 by adding small classification) and 137 perspectives, as well as questions for the confirmation of each perspective (Status report of activity,2008). The six key factors are external environmental factors, organizational psychological factors, corporate governance factors, senior management factors, group factors, and individual psychological factors, as shown in Table 1. They are referred to in the guideline as perspectives for organizational factors.

Perspectives for organizational factors in root cause analysis

The following examples of perspectives can be used to decide whether or not causal relationships of organizational factors associated with senior management factors of the power plant shall be analyzed:

1. Whether or not senior management factors that caused inappropriate behaviors have been analyzed.
2. Whether or not corporate governance factors that caused the senior management factors have been analyzed.
3. Whether or not the association of inappropriate behaviors, senior management factors, and corporate governance factors has been analyzed in a logical manner.
4. Whether or not the association of individual psychological factor, workplace psychological factor (group factors), and organizational psychological factor have been analyzed, depending on the necessity.

External Environmental Factor

The factors related to the external environment of the organization concerned can be included among the set of organizational factor if the impact of economic status, regulatory response policy, external communication, general reputation and so forth are important for the issue concerned.

Organization Psychological Factor

These are the factors related to the common sense of value among organization members as a mode of thinking or behavior, formed during a long period in the organization (each collective level such as corporate level, power plant level, function level, group level and team level). They can be expressed in a form of consciousness, awareness, and behavior. They can be included in the set of organizational factor if they are important for the issue concerned. They are called "organizational culture".

Corporate Governance Factor

The factors related to the corporate governance of the head office can be included in the set of organizational factor if the following factors are important for the issue concerned. These factors are illustrative of inappropriateness or lack of specificity or effectiveness of top management commitment, organizational administration (operation status, organizational structure, organizational objectives and strategies, decision-making of head office etc.), human resource management, corporate policies and compliance criteria and standards, communication between the head office and power station, and self-assessment (or third party assessment).

Senior Management Factor

The factors related to the senior management of the power plant can be included in the set of organizational factor if the following factors are important for the issue concerned. These factors are illustrative of inappropriateness or lack of specificity or effectiveness of senior-manager level organization administration (objectives and strategies, establishment of a Quality Management System, improvement of manuals, etc.), conformance to rules, continuous education of the organization (handing down of skills, reflection of operation experience), personnel management,

communication, procurement management (communication and control with cooperative companies), human resources management related to organizational structure (role and responsibility, selection and arrangement, performance, education, and training), engineering control, work control, change control (control at modification of the organization, control at change of work etc.), non-conformance control, corrective action, and documentation control.

Group Factor

These are the factors related to the groups at each level of the organization (e.g., management, division, section, team on shift, job team, etc.). They can be included in the set of organizational factors if their negative impacts of inter- or intra-party communication, knowledge/ education, groupthink and decision-making based on principle of individuality, etc., are important for the issue concerned.

Individual Psychological Factor

The factors related to the individuals (employees or senior managers) in the organization or groups can be included in the set of organizational factors if their impacts, such as lack of knowledge or skill, leadership, eagerness/ prudent for safety, eagerness for management, concern about field staffs, motivations, stress, etc., are important for the issue concerned.

Table 1 Key factors and intermediate classifications of JOFL

No	Key factors	No.	Intermedeate classifications
1	External Environmental Factor	1-1	economic status
		1-2	regulatory response policy
		1-3	external communication
		1-4	general reputation
2	Organizational Psychological Factor	2-1	organizational culture
3	Corporate Govenance Factor	3-1	top management commitment
		3-2	organizational administratin
		3-3	human resource management
		3-4	corporate policies and compliance criteria and standards
		3-5	communication between the head office and power station
		3-6	self-assessment (or the third party assessment)
4	Senior Management Factor	4-1	senior manager level organization administration
		4-2	conformance to rules
		4-3	continuous education of the organization
		4-4	personnel management
		4-5	communication
		4-6	procurement management
		4-7	human resources management related to organizational structure
		4-8	engineering control
		4-9	work control
		4-10	change control
		4-11	non-conformance control
		4-12	corrective action
		4-13	documentation control
5	Group Factor	5-1	inter/intra-party communication
		5-2	knowledge / education
		5-3	groupthink and decision-making based on principle of individuality
6	Individual Psychological Factor	6-1	knowledge or skill
		6-2	leadership
		6-3	eagerness / prudent for safety
		6-4	eagerness for management
		6-5	concern about field staffs
		6-6	motivations, stress

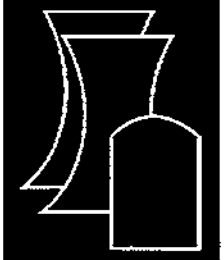
References

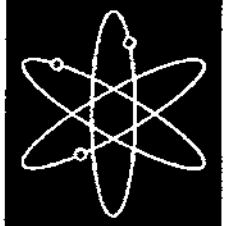
Institute of Human Factors (2003). Making of guideline of understanding and enforcement of safety culture. Annual report on human factors research project, 2002. Report No.IHF/0301.Tokyo: Nuclear Power Engineering Corporation.

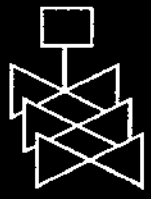
JEA(2007). Application guide to quality assurance code for safety in nuclear power plants (JEAC4111-2003)-Operation phase of nuclear power plants. JEAG4121-2005[2007 Suppl.2]. Tokyo: Japan Electric Association.

Makino,M., Sakaue,T. & Inoue,S.(2005). Toward a safety culture evaluation tool. In N. Itoigawa, B. Wilpert & B. Fahlbruch (Eds.), Emerging demands for the safety of nuclear power operations (pp. 73-84). Boca Raton, FL: CRC Press.
Nuclear and Industrial Safety Agency (2007).Guideline for regulatory agencies in evaluating contents of root cause analysis by licensees (NISA Document No.NISA-166c-07-10).Tokyo:NISA
Safety Standard Division. (2006).The safety culture assessment method (The implementation manual).JNES-SS report No. JNES-SS-0616.Tokyo:Incorporated Administrative Agency, Japan Nuclear Energy Safety Organization.
Safety Standard Division. (2007).Preparation of regulatory requirements for cultivation and infiltration of nuclear safety culture in organizations. Annual report No. 07-KIHI-HOU-0003.Tokyo: Incorporated Administrative Agency, Japan Nuclear Energy Safety Organization.
Status report of activity (2008). Guideline and Training Materials for Regulatory Agencies in Evaluating Contents of Root Cause Analysis by Licensees, Japan Nuclear Energy Safety Organization (JNES) Home page, Attachment 2 [On line Document].
URL http://www.jnes.go.jp/content/000008245.pdf

NUREG/CR-6751







The Human Performance Evaluation Process: A Resource for Reviewing the Identification and Resolution of Human Performance Problems

Performance, Safety and Health Associates, Inc.

U.S. Nuclear Regulatory Commission
Office of Nuclear Regulatory Research
Washington, DC 20555-0001

AVAILABILITY OF REFERENCE MATERIALS IN NRC PUBLICATIONS

NRC Reference Material

As of November 1999, you may electronically access NUREG-series publications and other NRC records at NRC's Public Electronic Reading Room at www.nrc.gov/NRC/ADAMS/index.html.
Publicly released records include, to name a few, NUREG-series publications; *Federal Register* notices; applicant, licensee, and vendor documents and correspondence; NRC correspondence and internal memoranda; bulletins and information notices; inspection and investigative reports; licensee event reports; and Commission papers and their attachments.

NRC publications in the NUREG series, NRC regulations, and *Title 10, Energy*, in the Code of *Federal Regulations* may also be purchased from one of these two sources.

1. The Superintendent of Documents
   U.S. Government Printing Office
   Mail Stop SSOP
   Washington, DC 20402–0001
   Internet: bookstore.gpo.gov
   Telephone: 202-512-1800
   Fax: 202-512-2250
2. The National Technical Information Service
   Springfield, VA 22161–0002
   www.ntis.gov
   1–800–553–6847 or, locally, 703–605–6000

A single copy of each NRC draft report for comment is available free, to the extent of supply, upon written request as follows:

Address: Office of the Chief Information Officer,
Reproduction and Distribution
Services Section
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001
E-mail: DISTRIBUTION@nrc.gov
Facsimile: 301–415–2289

Some publications in the NUREG series that are posted at NRC's Web site address www.nrc.gov/NRC/NUREGS/indexnum.html are updated periodically and may differ from the last printed version. Although references to material found on a Web site bear the date the material was accessed, the material available on the date cited may subsequently be removed from the site.

Non-NRC Reference Material

Documents available from public and special technical libraries include all open literature items, such as books, journal articles, and transactions, *Federal Register* notices, Federal and State legislation, and congressional reports. Such documents as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings may be purchased from their sponsoring organization.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at—

The NRC Technical Library
Two White Flint North
11545 Rockville Pike
Rockville, MD 20852–2738

These standards are available in the library for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from—

American National Standards Institute
11 West 42nd Street
New York, NY 10036–8002
www.ansi.org
212–642–4900

Legally binding regulatory requirements are stated only in laws; NRC regulations; licenses, including technical specifications; or orders, not in NUREG-series publications. The views expressed in contractor-prepared publications in this series are not necessarily those of the NRC.

The NUREG series comprises (1) technical and administrative reports and books prepared by the staff (NUREG–XXXX) or agency contractors (NUREG/CR–XXXX), (2) proceedings of conferences (NUREG/CP–XXXX), (3) reports resulting from international agreements (NUREG/IA–XXXX), (4) brochures (NUREG/BR–XXXX), and (5) compilations of legal decisions and orders of the Commission and Atomic and Safety Licensing Boards and of Directors' decisions under Section 2.206 of NRC's regulations (NUREG–0750).

NUREG/CR-6751

The Human Performance Evaluation Process: A Resource for Reviewing the Identification and Resolution of Human Performance Problems

Manuscript Completed: September 2001
Date Published: March 2002

Prepared by
V. Barnes, B. Haagensen[1]

Contributing Author:
J. O'Hara[2]

[1]Performance, Safety and Health Associates, Inc.
P.O. Box 30
Boalsburg, PA 16827

[2]Brookhaven National Laboratory
Energy Sciences and Technology Department
Upton, NY 11973

I. Schoenfeld, E. Trager, NRC Project Managers

Prepared for
Division of Engineering Technology
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001
NRC Job Code W6528

ABSTRACT

The Human Performance Evaluation Process (HPEP) is a resource for U.S. Nuclear Regulatory Commission inspectors to use when reviewing licensee problem identification and resolution programs with regard to human performance. Part I provides a step-by-step process for reviewing licensee effectiveness in identifying, analyzing and resolving human performance problems. Part I also addresses the challenges in identifying and investigating human performance problems, describes three root cause analysis techniques, and discusses characteristics of effective corrective action plans. Part II is comprised of the HPEP Cause Tree and Modules. The Cause Tree is a screening tool for identifying the range of possible causes for a human performance problem. The Modules describe frequently identified causes for human performance problems and provide examples. Part II is intended to support the evaluation of licensee root cause analyses for human performance problems identified in Part I.

Contents

Contents (continued)

Contents (continued)

Contents (continued)

Contents (continued)

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGEMENTS

The authors wish to express their sincere gratitude to Isabelle Schoenfeld, Julius Persensky, Eugene Trager and Clare Goodman of the U.S. Nuclear Regulatory Commission for their technical guidance, knowledge and support of this project. We also wish to recognize John Kauffman and Robert Spence of the U.S. Nuclear Regulatory Commission, and Calvin Walbert of the U.S. Chemical Safety and Hazard Investigation Board, for their reviews of the report. These reviewers provided insightful comments on the issues addressed in the report, and their perspectives as experienced inspectors and investigators were invaluable. The primary author also wishes to thank Dennis Vernon, Program Manager of the U.S. Department of Energy's Environment, Safety and Health Office of Oversight Accident Investigation Program, for his tutelage.

PART I:

THE HUMAN PERFORMANCE REVIEW PROCESS

1 OVERVIEW OF THE HUMAN PERFORMANCE EVALUATION PROCESS (HPEP)

1.1 INTRODUCTION

Reliable human performance is a requirement for safe operations in many settings, including operations of commercial nuclear power and nuclear materials licensees. Among the industries regulated by the U.S. Nuclear Regulatory Commission (NRC), **human error** has played an important role in numerous events. Researchers for the Electric Power Research Institute note:

> Ever since the systematic study of human performance and accidents began, it has been clear that human errors (i.e., inappropriate or inadequate human actions) contribute to a large portion of accidents and incidents. This has been found true for vehicle operation (aircraft, cars, motorcycles, bicycles), for industry (commercial aviation maintenance, manufacturing, chemical processing, mining), and for electric power generation. In nuclear power generation, the portion of events or mishaps attributed at least in part to human error has ranged from 40% to 80%, depending on the study and the specific measures used, but it is consistently reported as having a major role (Gross and Ayres, 1998).

Human errors may play several different roles in an event sequence. An error may

- directly cause an event,
- contribute to an event by setting up the conditions that, in combination with other events or conditions, allowed the event to occur (e.g., leaving a valve open that should be closed),
- make the consequences of an event more severe, or
- delay recovery from an event.

Human errors typically contribute to events rather than directly cause them. In fact, a single human error directly causes very few significant events because most systems that involve nuclear processes are designed to be fault-tolerant; that is, designed to prevent a single human action (or failure to act) from causing an event with important consequences.

More often, a risk-significant event involves several system deficiencies, some of which may have happened long before the event takes place. For example, errors in the original installation of a system may set the stage for another human error to initiate an event months or years later. The value of investigating the human errors involved in an event is to understand what caused them so that **corrective actions** can be developed to minimize the likelihood of recurrence.

It is also important to detect and correct patterns of errors before they result in an event. **Human performance trends** are a pattern of related errors resulting from the same causal factors.

Although most errors that are made day-to-day have no immediate impact on safe operations, an adverse human performance trend may contribute to an overall increase in risk to the public. For example, a pattern of related errors may systematically degrade the reliability of a class of components (e.g., miscalibration errors) or the errors may be committed in the wrong combination of circumstances and cause an event.

In most cases, the causes of errors that occur in an event or as part of a trend (collectively referred to here as **human performance problems**) can be traced to weaknesses in the programs, policies and practices that NRC licensees use to increase the reliability of human performance in their operations. Examples of these programs include training and qualification programs; the fitness-for-duty program; programs to develop and validate procedures; work planning and control processes; overtime policies; and structured methods for communicating important information, such as shift turnover. Programmatic weaknesses are often found to be the root causes of human performance problems.

In the course of implementing NRC Inspection Procedure 71152, Identification and Resolution of Problems, inspectors may be called upon to validate licensees' investigations of events involving human performance problems. For significant conditions adverse to quality, inspectors will evaluate licensees' detection and characterization of human performance problems as well as the effectiveness of licensee root cause analyses and corrective actions. The Human Performance Evaluation Process (HPEP) is intended to help NRC inspectors in performing these tasks.

1.2 OBJECTIVES

The HPEP is not intended to replace existing NRC inspection procedures. The purpose of the HPEP is to support NRC staff reviews of the effectiveness of licensee problem identification and resolution programs in detecting and resolving human performance problems. Methods are presented for evaluating licensee investigations of human performance problems, root cause analyses and corrective actions. It is recognized that the approach described in Part II of the HPEP is different from that used in NRC inspection procedures, such as Inspection Procedure 71841, Human Performance.

1.3 ORGANIZATION

The HPEP is presented in two parts. Part I is a step-by-step process to help a reviewer evaluate a licensee's problem identification, investigation, causal analyses and corrective actions for human performance problems. Part II is comprised of the HPEP Cause Tree and Modules. The modules provide background information on frequently identified causes of human performance problems and specific examples to assist in the evaluation of a licensee's causal analyses.

A glossary of terms and concepts that are central to understanding and applying the review guidance is presented in Appendix A. Terms that are defined in the glossary are presented in bold in the text.

Appendix B presents a bibliography of sources used to develop this document. References are not cited in the text in order to increase the usability of the document.

2 HUMAN PERFORMANCE PROBLEM REVIEW

2.1 OVERVIEW OF THE REVIEW PROCESS

In this section, a systematic method is presented for evaluating the effectiveness of a licensee's identification and resolution program with regard to human performance problems. The HPEP review process is organized as a series of tables that ask the inspector to answer evaluation questions in four areas. These areas are:

- The licensee's identification and characterization of human performance problems (Table 2.1 Problem Identification and Characterization)
- Methods and information used to investigate human performance (Table 2.2 Investigation Methods)
- The analyses used to determine the causes of the human performance problems (Table 2.3 Causal Analyses)
- The likely effectiveness of corrective action plans (Table 2.4 Corrective Actions).

Table 2.5, Summary Review Table, is provided to assist in summarizing the results of the review. Blank tables are presented at the end of this section and in Appendix C for copying.

More detailed background information on each of the evaluation areas is provided in Sections 3-6 of this document, as follows:

- Challenges in identifying human performance problems and the theoretical framework underlying the HPEP are discussed in Section 3.
- Information and detailed guidance regarding appropriate investigation methods for human performance problems are presented in Section 4.
- An overview of root cause analysis is presented in Section 5. Three root cause analysis techniques are also described: events and causal factors analysis, barrier analysis and change analysis.
- Information regarding corrective actions for human performance problems is presented in Section 6. This section discusses alternative methods of correcting human performance problems and determining the appropriate scope of a corrective action plan.

The HPEP Cause Tree and Modules are presented in Part II of this document to assist in answering the questions in Table 2.3, Causal Analyses. This additional information on typical causes of human performance problems is presented because determining the causes for human performance problems is often difficult.

2.2 PROBLEM IDENTIFICATION AND CHARACTERIZATION

The review questions in Table 2.1 (p. 2-9) may be used in evaluating the extent to which licensees appropriately identify and characterize human performance problems. Human performance problems are sometimes difficult to identify in the documents that describe problems at licensee facilities or may not be identified at all. Licensee documentation may focus on system or equipment performance without discussion of the human actions and decisions that contributed to the event or condition.

There are a number of reasons that human performance problems may not be well documented in either internal licensee problem reports or in reports to the NRC. For example, human errors may not be reported and documented as such to avoid embarrassment to personnel or possible disciplinary action. A more complete discussion of the challenges in identifying human performance problems is presented in Section 3.

For some problems that the licensee has identified, human actions and decisions may not be important contributors to the problem. In others, human behavior may have been central to creating the problem, and an understanding of the nature and causes of the behavior was necessary to develop effective corrective actions. In the latter case, it is important that the human performance problem was characterized in sufficient detail to support problem resolution.

If the licensee did not identify the human performance problem(s) in the documents available for review, it may be necessary to request additional documents or to interview licensee personnel. Often, the human performance problem(s) in an event, for example, were identified and investigated, but the information may not have been included in a formal report.

2.3 INVESTIGATION METHODS

The review questions in Table 2.2 (p. 2-10) may be used to guide the evaluation of a licensee's investigation of a human performance problem. A thorough and systematic investigation is necessary to provide the information needed to perform causal analyses and develop effective corrective actions.

In general, the extent to which licensee personnel will investigate a human performance problem depends upon the perceived significance of the problem. For example, an error that caused a reportable event will likely receive more attention than an error that resulted in an event that was not reportable. Many licensees have established criteria for determining the types of problems that must be investigated and the degree of thoroughness required in the investigation. These criteria may include risk, cost, or regulatory implications, for example. If a human performance problem falls below the licensee's threshold for conducting an investigation and the inspector agrees with the licensee's determination, many of the questions in Table 2.2 will be marked as NA for the problem.

A discussion of methods for investigating human performance problems can be found in Section 4.

2.4 CAUSAL ANALYSES

The review questions in Table 2.3 (p. 2-12) may be used in evaluating the licensee's causal analyses of human performance problems. The purpose of analyzing the causes of human performance problems is to guide the development of effective corrective actions. Standard **root cause analysis** techniques, such as events and causal factors charting and analysis, change analysis and barrier analysis, are resource-intensive and time-consuming to apply, but yield reliable and useful results when performed properly. Use of the standard techniques may not always be warranted, however, and licensees apply these techniques only to the more significant problems. When standard root cause analysis techniques are used, more than one cause is typically identified for a human performance problem. An overview of root cause analysis, and a discussion of the different types of causes that will be identified by using root cause analysis techniques, can be found in Section 5.

More detailed information about frequently identified causes of human performance problems is presented in the HPEP Cause Modules in Part II. The HPEP Cause Tree and Modules are intended to assist inspectors in verifying the causal factors a licensee has identified as an aid in answering the questions in Table 2.3.

2.5 CORRECTIVE ACTIONS

The review questions in Table 2.4 (p. 2-14) may be used in evaluating the licensee's corrective actions for human performance problems. An effective corrective action for a human performance problem is one that will decrease the likelihood that it, and similar problems, will happen again. In an ideal world, an effective corrective action would prevent recurrence of the human performance problem. As discussed in Section 3, however, the causes of human behavior are difficult to identify and, as a result, measures to improve human performance often yield inconsistent results.

Developing effective corrective actions typically requires a thorough root cause analysis and an understanding of available methods for enhancing human performance. Depending upon the significance and scope of the cause(s) identified, corrective action plans may vary in scope from correcting a single cause, such as a missing tag on a valve, to a general organizational improvement plan. As a minimum, corrective actions must address each of the causal factors identified from the investigation.

Corrective action plans that have an appropriate scope still may be ineffective, however. Corrective action plans may be ineffective because, for example, the steps for achieving the plan's objectives were not defined in detail; responsibility was not assigned to specific individuals for accomplishing the actions; or measures for determining the success of the corrective actions were not defined or used to refine the plan when necessary. Other management initiatives and events may arise that take precedence over implementing the corrective actions. Without a method for monitoring the on-going effectiveness of the corrective action plan, human performance problems may reoccur.

More detailed background information about corrective action plans can be found in Section 6.

2.6 USING THE REVIEW TABLES

Follow these steps to use the review tables:

1. Assemble the reports that describe the human performance problems to be evaluated. These may consist of Licensee Event Reports, self-assessments, problem reports entered into a licensee's corrective action tracking system(s), licensee responses to inspection findings, or others. Request that the licensee also provide any related background or supporting documentation that may contain more information than what is available in the reports.

2. Identify each human error or trend that is described in the documents and develop a brief, shorthand description of the human performance problem. Focus on describing the human behavior or action, to the extent that information is available. For example, "procedure step skipped," "alarm disabled," "jumper not removed," and so on. Record the brief description in the top row of each table, along with the date it occurred, if that information is available. (If you will be reviewing multiple human performance problems, make additional copies of the tables. Space is provided on each table to review two problems.)

3. In the row labeled "Document Identifier" at the top of Table 2.1, you may also want to record information about the source document in which you found the human performance problem discussed for later reference.

4. Begin the review of each human performance problem with Table 2.1 and continue through Table 2.4. Answer the questions in all of the tables for each problem. If a question is not applicable to the problem, mark it as NA. Space is provided in each table for recording notes.

5. When you have completed answering the questions on the page, count up and record the total number of Yes answers you circled and the total number of NA answers you circled on that page. Record these totals in the spaces provided in the lower right-hand corner of the page. The questions in each table are designed so that a Yes answer suggests problem identification and resolution program effectiveness. There is no threshold percentage of Yes answers that would show that a licensee's problem identification and resolution program was ineffective with regard to human performance. However, these percentages provide an indication of program sensitivity to human performance problems.

6. When you have completed Tables 2.1-2.4 for each human performance problem under review, summarize the results of your evaluations in Table 2.5. By following the procedure described below, calculate the percentage of Yes answers you circled to the applicable evaluation questions in each area addressed by the tables. Figure 2.1 shows an example of Table 2.5 that has been completed for a hypothetical inspection.

a. Record the total number of human performance problems you reviewed in the space provided at the top left of the table.
b. Multiply the number of problems you reviewed by the number of questions in each table (the latter number is provided in the summary table).
c. Add up the total number of Yes answers you circled in each table and record those totals in Row C. For example, if you used six copies of Table 2.1 (to review twelve human performance problems), you would add up the Yes answers on all of the six pages to arrive at the total number of Yes answers you circled in Table 2.1. Record this total in Row C in the column titled "2.1 Problem Identification and Characterization" on Table 2.5, the "Summary Review Table."
d. Add up the total number of NA answers you circled in each table and record those totals in Row D.
e. Subtract the total number of NA answers (Row D) from the total calculated in Row B. The difference represents the number of applicable questions that could have been answered Yes.
f. Divide the number of Yes answers in each table (as recorded in Row C) by the number of applicable questions that could have been answered Yes (as recorded in Row E).
g. Multiply the result in Row F by 100 to arrive at the percentage of Yes answers you circled out of the total number of applicable questions that could have been answered Yes.
h. Adding up your answers to each question in Tables 2.1-2.4 may also be useful in developing insights regarding any specific areas of weakness in the licensee's problem identification and resolution program with regard to human performance. For example, question 2.2.3 in Table 2.2 asks, " Did the licensee validate the information gathered about the problem by seeking information from more than one source?" If you find that you circled No for 11 out of 12 problems reviewed, your answers may suggest that further assessment of the licensee's investigation methods is warranted. Copies of the tables may also be used to record the tallies for each question.

2.7 ASSESSING RISK IMPACT

There are a number of methods available for assessing the risk importance of the human performance problems reviewed. The problem identification reports that are reviewed may be screened prior to the HPEP evaluation to ensure that only risk-important events or trends are evaluated. Or, as the HPEP evaluation progresses, the inspector may identify human performance problems that should be evaluated for risk-significance. Guidance for assessing the risk impact of weaknesses in the licensee's problem identification and resolution processes with regard to human performance problems may also be consulted.

2.8 INCORPORATING HPEP FINDINGS IN AN INSPECTION REPORT

The results of an HPEP review, taken together with other information from inspection activities, should assist NRC personnel in drawing conclusions regarding the effectiveness of a licensee's problem identification and resolution program for human performance. For example, if an HPEP

review indicated that a licensee identified and appropriately characterized the human performance problems in only 10% of the issues reviewed (as indicated by the percentage of Yes answers calculated in Row G of Table 2.5), inspectors may question the sensitivity of the program to human performance problems. Or, if a low percentage of Yes answers were given to the questions in Table 2.3 regarding the licensee's causal analyses, inspectors may question the likely effectiveness of corrective actions based upon those analyses. Taken together with additional information that shows a pattern of undetected human performance trends, a low percentage of Yes answers to the HPEP review questions could support a finding that the licensee's program is weak in the identification and resolution of human performance problems.

Table 2.5 Summary Review Table				
A. Number of human performance problems reviewed = 10	**Tables**			
	2.1 Problem Identification and Characterization	**2.2 Investigation Methods**	**2.3 Causal Analyses**	**2.4 Corrective Actions**
Number of questions in each table	6	10	13	12
B. Multiply the number of questions in each table by the total number of problems reviewed	6 X 10=(B)60	10 X 10=(B)100	13 X 10=(B)130	12 X 10=(B)120
C. Record the total number of Yes answers circled from each table	(C) = 40	(C) = 65	(C) = 110	(C) = 87
D. Record the total number of NA answers circled from each table	(D) = 7	(D) = 5	(D) = 0	(D) = 3
E. Subtract the total from Row D from the total in Row B	(B)60 - (D)7=(E)53	(B)100 - (D)5=(E)95	(B)130 - (D)0=(E)130	(B)120 - (D)3=(E)127
F. Divide the answer in Row C by the answer in Row E	(C)40 /(E)53=(F).75	(C)65 /(E)95=(F).68	(C)110 /(E)130=(F).85	(C)87/ (E)127=(F).69
G. Multiply the answer in Row F by 100 to obtain the percentage of Yes answers	(F).75 X 100 = 75%	(F).68 X 100 = 68%	(F).85X 100 = 85%	(F).69 X 100 = 69%

Figure 2.1 An Example of Table 2.5 Completed for a Hypothetical Inspection

HPEP REVIEW TABLES

Table 2.1 Problem Identification and Characterization

Document Identifier:		Problem Number: __		Problem Number: __	
Question Number	Brief description of the problem and date(s) of occurrence:				
2.1.1	Was the human performance problem identified?	Yes No NA	Notes:	Yes No NA	Notes:
2.1.2	If not, was the human performance problem tangential to understanding and resolving the issue under review?	Yes No NA		Yes No NA	
2.1.3	Were the individuals involved in the problem identified (by job role)?	Yes No NA		Yes No NA	
2.1.4	Were the actions and decisions or failures to act that comprised the problem described?	Yes No NA		Yes No NA	
2.1.5	Were precursor errors or earlier evidence of a developing trend identified?	Yes No NA		Yes No NA	
2.1.6	Was the problem described in enough detail to support causal analyses and the development of corrective actions?	Yes No NA		Yes No NA	

Notes:

Total number of Yes's: ____

Total number of NA's: ____

Table 2.2 Investigation Methods

Question Number	Problem description:	Problem Number: __		Problem Number: __	
2.2.1	Was the extent of the investigation consistent with the importance of the problem?	Yes No NA	Notes:	Yes No NA	Notes:
2.2.2	Were licensee criteria for determining which issues require an investigation appropriately applied to this problem?	Yes No NA		Yes No NA	
2.2.3	Did the licensee validate the information gathered about the problem by seeking information from more than one source?	Yes No NA		Yes No NA	
2.2.4	Did the licensee seek the appropriate type(s) of evidence for investigating the problem?	Yes No NA		Yes No NA	
2.2.5	Did the licensee gather enough information to understand the sequence of events and conditions leading up to the problem?	Yes No NA		Yes No NA	

Notes:

Total number of Yes's: ____

Total number of NA's: ____

Table 2.2 Investigation Methods (continued)

Question Number	Problem description:	Problem Number: __		Problem Number: __	
2.2.6	Did the licensee check plant records to identify other problems that occurred during the same work activity?	Yes No NA	Notes:	Yes No NA	Notes:
2.2.7	Did the licensee identify the programs that applied to the job(s) during which the human performance problem arose?	Yes No NA		Yes No NA	
2.2.8	If the licensee found weaknesses in the applicable programs, were the weaknesses investigated in sufficient detail to understand their scope and likely effects, if not corrected?	Yes No NA		Yes No NA	
2.2.9	Were the licensee's conclusions clearly supported by the results of the investigation?	Yes No NA		Yes No NA	
2.2.10	Was there a basis documented for stopping the investigation?	Yes No NA		Yes No NA	

Notes:

Total number of Yes's: ____

Total number of NA's: ____

Table 2.3 Causal Analyses

Question Number	Problem description:	Problem number: __		Problem Number: __	
2.3.1	Were causal factors identified for this human performance problem?	Yes No NA	Notes:	Yes No NA	Notes:
2.3.2	Was more than one causal factor identified for the problem?	Yes No NA		Yes No NA	
2.3.3	Was the type of causal analysis of this problem consistent with its importance?	Yes No NA		Yes No NA	
2.3.4	Was there enough information provided to verify the accuracy of the causal factors identified?	Yes No NA		Yes No NA	
2.3.5	Were several possible causes for the problem investigated?	Yes No NA		Yes No NA	
2.3.6	Did the evidence support the licensee's choice of causes?	Yes No NA		Yes No NA	
2.3.7	Were the bases for rejecting possible causes for the problem documented?	Yes No NA		Yes No NA	

Notes:

Total number of Yes's: ____

Total number of NA's: ____

Table 2.3 Causal Analyses (continued)

Question Number	Problem description:	Problem Number: __		Problem Number: __	
2.3.8	Did the licensee analyze programmatic weaknesses to determine if they could account for more than one human performance problem?	Yes No NA	Notes:	Yes No NA	Notes:
2.3.9	Did the licensee perform and document a root cause analysis using systematic root cause analysis techniques?	Yes No NA		Yes No NA	
2.3.10	Was more than one root cause analysis technique used?	Yes No NA		Yes No NA	
2.3.11	Was the rationale for terminating the root cause analysis sufficient and documented?	Yes No NA		Yes No NA	
2.3.12	Were the root causes identified under management control?	Yes No NA		Yes No NA	
2.3.13	If corrected, would the causes identified reduce the likelihood of the same and similar problems from happening again?	Yes No NA		Yes No NA	

Notes:

Total number of Yes's: ____

Total number of NA's: ____

Table 2.4 Corrective Actions

Question Number	Problem description:	Problem Number: __		Problem Number: __	
2.4.1	Were corrective actions for the human performance problem identified?	Yes No NA	Notes:	Yes No NA	Notes:
2.4.2	Were the corrective actions effective, or appear likely to be effective, even if no causal analysis was performed and/or documented?	Yes No NA		Yes No NA	
2.4.3	If a causal analysis was performed, were the links between the causal factors and the corrective actions clear?	Yes No NA		Yes No NA	
2.4.4	Was there a corrective action for every causal factor? (a one-to-one correspondence is not required)	Yes No NA		Yes No NA	
2.4.5	Was the scope of the corrective action plan appropriate?	Yes No NA		Yes No NA	
2.4.6	Were the desired condition(s) that the corrective actions are intended to create clearly described?	Yes No NA		Yes No NA	

Notes:

Total number of Yes's: ____

Total number of NA's: ____

Table 2.4 Corrective Actions (continued)

Question Number	Problem description:	Problem Number: __		Problem Number: __	
2.4.7	Did the licensee define measurable objectives to be achieved from the corrective actions?	Yes No NA	Notes:	Yes No NA	Notes:
2.4.8	Did the licensee define evaluation and acceptance criteria for assessing corrective action effectiveness?	Yes No NA		Yes No NA	
2.4.9	Did the licensee define an implementation process for the corrective actions and specific performance indicators for evaluating success?	Yes No NA		Yes No NA	
2.4.10	Did the licensee assign responsibility to specific, qualified individuals for implementing the corrective actions?	Yes No NA		Yes No NA	
2.4.11	Did the licensee develop a plan for on-going monitoring of continued acceptable performance?	Yes No NA		Yes No NA	
2.4.12	Did the licensee review the corrective actions before implementation to ensure that they will not cause unintended negative consequences?	Yes No NA		Yes No NA	

Notes:

Total number of Yes's: ____

Total number of NA's: ____

Table 2.5 Summary Review Table

A. Number of human performance problems reviewed = ____	Tables			
	2.1 Problem Identification and Characterization	2.2 Investigation Methods	2.3 Causal Analyses	2.4 Corrective Actions
Number of questions in each table	6	10	13	12
B. Multiply the number of questions in each table by the total number of problems reviewed	6 X ___=(B)____	10 X ___=(B)____	13 X ___=(B)____	12 X ___=(B)____
C. Record the total number of Yes answers circled from each table	(C) = ____	(C) = ____	(C) = ____	(C) = ____
D. Record the total number of NA answers circled from each table	(D) = ____	(D) = ____	(D) = ____	(D) = ____
E. Subtract the total in Row D from the total in Row B	(B)____-(D)____=(E)____	(B)____-(D)____=(E)____	(B)____-(D)____=(E)____	(B)____-(D)____=(E)____
F. Divide the answer in Row C by the answer in Row E	(C)____/(E) ____=(F)____	(C)____/(E) ____=(F)____	(C)____/(E)____=(F)____	(C)____/ (E)____=(F)____
G. Multiply the answer in Row F by 100 to obtain the percentage of Yes answers circled in each review table	(F)____X 100 = ____%	(F)____X 100 = ____%	(F)____X 100 = ____%	(F)____X 100 = ____%
Notes:				

3 IDENTIFYING HUMAN PERFORMANCE PROBLEMS AND THEIR CAUSES

3.1 INTRODUCTION

Identifying human performance problems and their causes is often difficult. Further, the simple identification of "human error" as a root or contributing cause of events provides little information about how to prevent similar problems from recurring. Recognizing human performance problems when they occur and accurately identifying their causes are necessary first steps to developing effective corrective actions.

In this section, the term, "**human error,**" is discussed and the challenges to identifying human performance problems are discussed. Common difficulties in identifying the causes of error are also discussed. Finally, the framework for investigating human errors that underlies the design of the HPEP is presented.

3.2 CHALLENGES IN IDENTIFYING HUMAN PERFORMANCE PROBLEMS

The term, "human error," refers to an interaction between human behavior and the context in which it occurs.[1] The concept of an interaction is important because it is the context in which a human action takes place that determines whether or not it is an error. In most cases, a particular human action only becomes an "error" when it deviates from what was planned or expected in a given task environment. This definition of error is important because it directs attention both to the behavior and to the characteristics of the task environment that allowed the behavior to cause or contribute to an event.

The human behaviors of greatest concern in a nuclear power plant are those in which personnel interact with plant equipment and systems (i.e., human-system interactions), such as manipulating valves, operating controls, placing or removing jumpers, locating and reading gauges, or making and implementing decisions. Human-system interactions affect plant performance.

Human performance trends, defined as a pattern of related errors resulting from the same causal factors, may be difficult to identify for several reasons. First, humans commit errors

[1] The term, "human error," has become somewhat controversial. Some practitioners and researchers have argued that it inappropriately focuses attention on workers as the cause of an event and carries a connotation of blame (NUREG-1624, 2000; Reason, 1997). The term is used in this document, however, because "error" accurately implies that the very large majority of actions (or failures to act) that cause or contribute to events are unintentional. For blame to accrue to an individual worker, it would be necessary to establish that the worker had both knowledge of the correct actions to take in the given context and took the incorrect actions with intent (i.e., despite the knowledge that the actions were proscribed). If both knowledge and intent were established, but the intent did not involve causing harm, then the more accurate term for the worker's behavior would be a "violation." If harm was intended, which we are certain is rarely the case, then the more accurate term would be "sabotage." Both violations and sabotage fall outside the scope of this document.

relatively frequently but the errors often are not detected and reported as such. Most are not detected for two primary reasons: (1) they have no impact on equipment or system performance, or (2) they are caught and corrected before they have an impact. Errors are so common, in fact, that people often do not notice an error has been committed unless it results in observable consequences, such as degraded equipment, injuries, or equipment failures.

Second, personnel are often reluctant to report their own or co-workers' errors for many different reasons. These may include the desire to avoid embarrassment or the potential for disciplinary action; "chilling effects" from management that discourage workers from reporting problems; a fear of retaliation or social ostracism from peers; the simple burden of filling out paperwork; or there may be no systematic and impersonal method available to report errors and their causes. As a result, a pattern of repeated errors may not be detected until they have a noticeable impact on hardware performance. An accepted practice of deviating from the steps in a poorly written procedure, rather than ensuring that the procedure is revised, is an example of an error that may not be reported, but could result in adverse consequences if, for example, the deviations had undetected effects on equipment, such as accelerated aging.

Third, some licensee's corrective action item tracking systems may not be designed to support the aggregation of human performance data to identify trends. In some cases, problems are coded and tracked by the system, component or part, and human errors that occurred to cause the problem may be buried in the problem descriptions and not coded in a manner that is retrievable for analysis. As a result, different errors that result from the same cause may not be identified as symptoms of an underlying problem.

Finally, management and regulators may also affect the human performance information that is reported and tracked. For example, some managers may edit or influence the writing of problem reports to ensure that their departments are not blamed for the problems or to address economic considerations. Regulatory interest in some types of human performance problems may influence the types of problems that are reported and how they are characterized. The results might be that some problems are under-reported while others may be over-reported.

A number of classification schemes have been developed to categorize human errors into different types. For example, Kirwan (1994) identifies four types of errors, including (1) errors of commission, in which incorrect actions were taken, (2) errors of omission, in which required actions were not taken, (3) extraneous acts, in which an action that was not required was taken, and (4) missed error-recovery opportunities, comprised of actions which could have corrected previous errors. Other schemes divide errors into motor (e.g., a slip) and cognitive (e.g., a mental lapse) categories that may be further divided into subtypes.

Error classification schemes that focus on behaviors provide a language for describing the different ways in which human behavior in a nuclear licensee's workplace can go wrong. But, as will be discussed below, they are not particularly useful for understanding the causes of errors that lead to events or to on-going human performance problems.

3.3 CHALLENGES IN IDENTIFYING THE CAUSES OF ERRORS

Establishing the causes of errors is necessary to detect and correct human performance problems, but is often more difficult than establishing the causes for hardware failures. The challenge arises from the flexibility and adaptability of human behavior as well as from the post hoc nature of problem or event investigations.

There are few simple, one-to-one relationships between causal factors and specific human errors. For example, a single causal factor, such as fatigue, may cause a variety of different types of errors, such as skipping a step in a procedure, dropping tools, performing maintenance on the wrong valve or failing to detect a sudden change in temperature or pressure on a gauge. Further, humans are highly adaptable and the presence of a potential causal factor does not guarantee that it will cause an error to be committed. Even a deeply fatigued person may be able to sustain high levels of accurate performance in some circumstances, such as in combat or the operating room. Although human factors research provides rules-of-thumb for designing human-system interfaces to reduce the likelihood of errors, and guidelines for the design of tasks and organizations, the person who is investigating an error cannot be sure that the research results apply to the specific situation under investigation.

Establishing causes for human error in an event sequence can be further complicated by weaknesses in the evidence available. For example, although interview data yield reliable information about some **lines of inquiry**, people are notably limited in their ability to know what has influenced their behavior. The social psychological research literature provides numerous examples of how people create explanations for their decisions and actions that bear little or no relationship to what can be objectively demonstrated to have caused them to behave in a particular way. In addition, interview data are subject to various predictable biases and memory distortions that reduce their reliability. For example, some research has shown that the accuracy of people's memories for events decreases by about 50% within two days after the event occurred. Moreover, in contrast to the equipment or materials involved in an event, licensee investigation personnel or NRC inspectors typically do not have the option of sending the humans involved off to the laboratory for additional testing to confirm a causal hypothesis.

The consequence of the lack of a one-to-one correspondence between different types of errors and specific causes is that there is no reliable road map to guide the identification of an error's causes. Any single error may be caused by a variety of factors, and the "true" cause of the error may be unknowable after the fact. Of course, there are cases in which an error's cause can be determined unambiguously. For example, if a procedure step provides an incorrect instruction, personnel report that they followed the step, and the consequences of their actions are consistent with what should have occurred from following the incorrect step, the investigator can be fairly confident that the "true" cause of the error was in the procedure. However, those cases are rare.

Identifying causes for human error is further complicated by many possible sources of bias or limitations in the investigation process itself. The choice of potential causes to investigate for a human error may be influenced, for example, by the investigator's greater knowledge of and comfort level with some causal factors over others as well as by a lack of knowledge in some

areas. Or, the investigation and selection of causal factors may be influenced by the anticipated costs of implementing subsequent corrective actions; institutional biases and mindsets; the time and resources available to conduct the investigation; the investigators' perceptions of what will be acceptable to management; and, sometimes, communications from management regarding acceptable or unacceptable lines of inquiry to pursue and the "right" answers to the investigations' questions.

Inherent biases in how humans process information and come to conclusions about causes may also affect an investigation. For example, research into the event investigation process identified the following ways in which human information-processing biases can affect investigations:

- There is a general tendency to start an investigation with a few ideas about possible causes, and then restrict the investigation to seeking information related to those causes. It is also common to end the investigation before alternative causes have been fully explored.
- People are subject to what has been termed the "confirmation bias," in which they only seek out information that is consistent with an explanation and ignore disconfirming evidence.
- Investigators may base their ideas of possible causes on the most immediately available and visible information and neglect information that is less obvious.
- There is a general human tendency to attribute the cause of an event to the dispositions, motivations or traits of persons rather than to situational factors, so the characteristics of the "actors" involved in an event may be given more weight as causal factors than the characteristics of the work environment.

Because the task of conclusively identifying the cause(s) for an error in an event sequence is so difficult, a comprehensive and systematic approach to investigating human errors is necessary. The barrier analysis framework described below is an approach to investigating human error that has been shown to be useful in practice and to lead to reliable results.

3.4 A BARRIER ANALYSIS FRAMEWORK FOR INVESTIGATING HUMAN ERRORS

The fact that human performance is fallible is one of the bases for the "defense-in-depth" approach to nuclear power plant operations in which multiple barriers to human error are implemented. Research and industry experience have identified both the most common causes of human error and the barriers to error that are effective in addressing these common causes. Those responsible for safe operations implement programs, policies and processes to ensure that these barriers are in-place and functioning, commensurate with the risks posed by the activities involved.

The barriers can be grouped into four basic categories, as follows:

- **Personnel** attributes required for successful task performance, including fitness for duty, knowledge and skills, and attention and motivation

- The **resources** provided to support task performance, such as complete, technically accurate and usable procedures, accurate and complete reference documentation, appropriate tools and equipment, supervision and the appropriate number of staff to accomplish the work
- A **physical work environment** compatible with human capabilities, including the design of human-system interfaces and appropriate controls on environmental factors, such as noise, vibration, and temperature
- An **organizational work environment** that facilitates task performance, including effective verbal and written communications, inter-group and intra-group coordination, an established safety culture, and planning and scheduling of work activities.

When these barriers are in-place and functioning, plant operations are controlled and the likelihood of errors is reduced.

Missing barriers, such as the failure to hold a pre-job briefing for important work on a safety system, or deficiencies in existing barriers, such as a poorly designed display, are often found to be the direct causes of errors. Direct causes of errors are also known as **performance-shaping factors**.

Once an error has been identified and characterized, the initial lines of inquiry into the cause(s) of the error determine what barriers to the error existed and how they failed, and what barriers could have been implemented to prevent the error from occurring, but were missing. The HPEP Cause Modules in Part II (e.g., Procedures, Communications, Supervision) represent the most common barriers implemented at plants to prevent errors. The modules also include examples of the types of direct causes that lead to errors when the barriers fail or are missing.

3.5 ANALYZING THE PROGRAMS THAT CREATE AND MAINTAIN BARRIERS

Although the identification of missing or failed barriers to human error is more useful than simply identifying "human error" as one of an event's causes, stopping the investigation at this level may not provide sufficient information to develop effective corrective actions. When failed or missing barriers to human error are encountered, it is also important to determine whether the failed or missing barriers represent isolated conditions or are symptoms of underlying flaws in the plant programs intended to ensure that the barriers are in-place and effective.

The **root cause** of an error is often found in programmatic weaknesses. **Programs** are comprised of policies (both formal and informal), organizational processes and procedures that define management expectations for how work is to be performed. Some are solely focused on ensuring safe operations (e.g., the ALARA program or the process for developing emergency operating procedures), while others perform a dual role (e.g., human resources and training programs) or have little direct impact on safety (e.g., the accounting system). If there is a flaw in one of the programs responsible for maintaining safe operations, that flaw will create conditions that may not only allow the error under investigation to reoccur, but may represent a vulnerability to additional events caused by the same programmatic flaw. Programmatic weaknesses are often found to be the cause of human performance trends.

As a simple example, an incorrect step in a procedure that is found to have caused an error may represent an isolated problem in a single procedure. Or, there may be a weakness in the program responsible for developing and maintaining procedures that allowed not only the one incorrect step to be published, but was ineffective in ensuring that procedures overall were technically accurate. If the investigation were to stop with the identification of the single incorrect step, and a corrective action was taken to fix that one step in the single procedure, the underlying flaw in the procedures program would not be detected. The consequence of failing to detect and correct the programmatic flaw would be that other inaccuracies in procedures would remain. Further, any new procedures that were developed under the same program could also include technical inaccuracies, thus setting the stage for further errors that could result in future hardware failures and other events.

Tracing the root causes of human error to the programmatic level can be resource intensive, however. Licensee problem identification and resolution programs may not require this type of extensive investigation and analysis until a human error is implicated in a significant problem or event, although definitions of "significance" vary among licensees. Databases that allow the tracking of human errors and their direct causes may pinpoint an emerging human performance trend, however, and could also lead to an investigation of programmatic causes. For this reason, the HPEP includes guidance for assessing a licensee's investigation of programmatic weaknesses that may be causing an adverse human performance trend or that played a causal or contributory role in a significant event.

3.6 SUMMARY

Figure 3-1 illustrates the HPEP framework described in this section. A hypothetical event sequence is shown across the bottom of the figure. Possible direct causes of the human error (barriers that failed or were missing) are shown above the event sequence. Possible programmatic causes that may have been responsible for the barrier failure are shown above the direct causes, demonstrating the loss of operational control that is evident from a human performance problem or significant event. In this hypothetical event, a person who was not qualified to perform the task committed the error, and both the training and work control programs were implicated as root causes.

The HPEP, then, may be used when evaluating a licensee's problem identification and resolution program to determine whether it (1) is effective in identifying the causes of human performance problems that play a causal or contributory role in significant events, and (2) results in corrective actions that target the causes of the problem(s) and result in effective problem resolution.

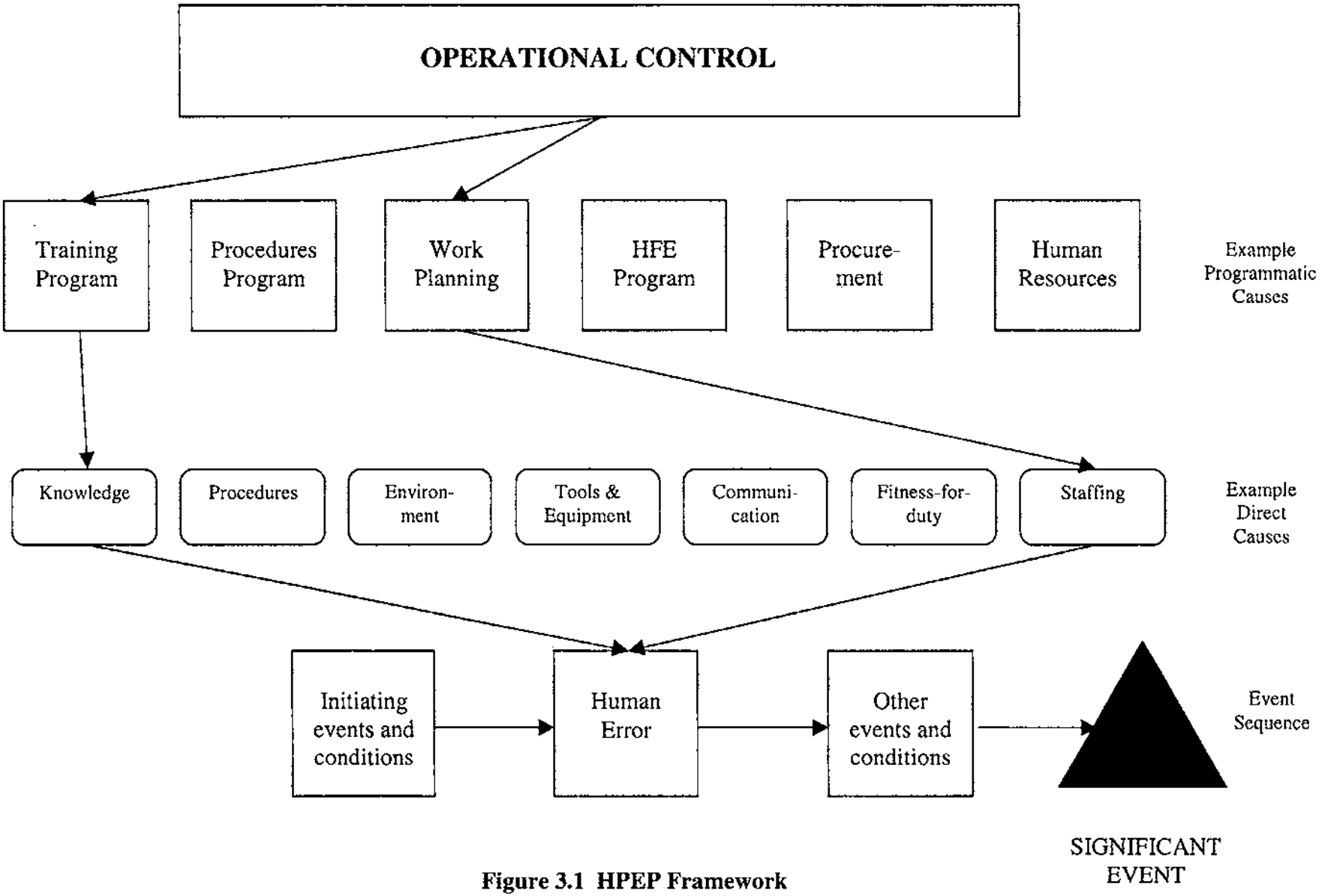


Figure 3.1 HPEP Framework

4 INVESTIGATION METHODS FOR HUMAN PERFORMANCE

4.1 INTRODUCTION

The purpose of investigating human performance problems is to gather the information necessary to identify their causes and develop effective corrective actions. An investigation should establish the "Who, What, When, Where and How?" of the human performance issue. The causal analysis of the information gathered in the investigation establishes the "Why."

In general, the thoroughness with which an error or a human performance problem will be investigated and analyzed depends upon the perceived significance (e.g., safety, potential economic impact) of the event sequence in which the error occurred or the potential for harm that an adverse human performance trend presents. In addition, the role of the error in an event sequence will also influence the extent to which an error is investigated. For example, an error that was the root cause of an event will likely receive more attention than an error that only contributed to the event.

Although licensees will not thoroughly investigate every human performance problem that arises, a systematic investigation of significant problems provides the basis for developing corrective actions to decrease the likelihood of recurrence. The investigation should be systematic to overcome the many challenges to investigating human performance that were discussed in Section 3. A **systematic investigation** process assures that the evidence gathered is complete, valid and reliable. **Evidence validity** refers to the accuracy of the information. **Evidence reliability** refers to whether or not different investigators would find the same information and reach the same conclusions from it. A **complete investigation** identifies the direct, contributing and root causes of the human performance problem so that corrective actions can be developed to minimize recurrence of the same and similar problems. In this section, methods for systematically investigating human performance problems are presented.

4.2 LINES OF INQUIRY

At the beginning of an investigation, investigators focus is on establishing the basic facts surrounding the human performance problem. As the investigation progresses, the lines of inquiry expand to investigate possible causes for the human performance problem and the scope of any problems that are identified.

The initial lines of inquiry in an investigation help characterize the human performance problem. Questions to be answered may include:

- What were the specific actions (or failures to act) that occurred in the event or that comprise the human performance trend?
- What were the conditions under which the actions occurred?
- What work activities, if any, were going on at the time of the error, or that are linked to

the human performance problem?

- What systems or equipment were involved or affected by the actions?
- When and where did the problem occur?
- Who was involved in the work activity and who was supervising?

Developing an event chronology (i.e., a timeline), or an events and causal factors chart, organizes the information gathered and is useful for showing gaps and conflicts in the information that has been collected. **Events and causal factors charting** is discussed in Section 5.

At times, the information required to develop the event chronology leads rapidly to identification of the direct cause of the human error under investigation. For example, the evidence may show that personnel were working in a very noisy environment, wearing hearing protection, and were unable to communicate effectively -- with the result that a communication error occurred. The noisy environment would be the direct cause of the error, in this case.

At other times, the direct cause of the error will not be obvious and more investigation and analysis may be required. Direct causes that are commonly implicated in human performance issues are described in detail in the HPEP Cause Modules in Part II of this document. The Cause Modules may suggest possible lines of inquiry to follow to establish the direct cause of an error. In addition, special tests or analyses may be required. For example, interview data may suggest that the worker who committed the error had been drinking. A blood or breath sample, if available, may be necessary to determine the validity of the interview data and to assess the likelihood that the worker was impaired.

Once the basic facts surrounding the human performance problem have been established, the lines of inquiry expand to begin identifying root and contributing causes for the error. The investigator will analyze the events and conditions leading up to the error and may use standard causal analysis techniques, such as those discussed in Section 5, to identify possible causal factors. **Programmatic causes** are investigated to determine whether a deficiency in a program, policy or practices for managing work activities at a site allowed barriers to error, established by management, to fail. As discussed in Section 3, barriers may fail because they are missing altogether or there is a weakness in how they are implemented.

The **extent of the conditions** that caused the human performance problem is also investigated. The investigator gathers evidence to determine whether the problem has occurred before, how frequently, and whether the conditions that led to this problem could cause other, similar human performance problems if not corrected. Further, the potential consequences of a recurrence of this error under different circumstances should also be evaluated.

For an error that was directly caused by a miscommunication in a noisy work environment, the lines of inquiry to identify programmatic causes and the extent of the conditions that caused the communication error might include: "What were the communication practices, if any, that personnel were trained to use in noisy environments? Did they follow those practices? If not, why not? Were there additional communication practices or devices that would have allowed the

operators to communicate more effectively in the noisy work environment? How many times in the past year have communication errors occurred in this and other noisy environments? Are there circumstances in which an inability to communicate could increase plant risk to unacceptable levels?"

For an error that was directly caused by fatigue from excessive hours worked over several months, the investigator could ask, "What are the work scheduling and overtime practices at this site? How many times in the past year have hours in excess of administrative limits been approved and for how many workers? How many extra work hours were approved for individuals, for certain job positions, within departments? Is there any evidence that error rates increased during the periods in which other personnel were working excess hours? What kinds of tasks were they performing and could errors on those tasks increase plant risk to unacceptable levels?"

The process of establishing the event chronology and gathering the information needed for conducting the causal analyses and to identify the needed corrective actions is described sequentially here. In most investigations, however, the investigation process is iterative. That is, the answers to one set of questions generate new questions for which information must be gathered. In general, the more thorough the investigation, the more likely that the causal analyses will identify the correct causal factors for the problem and that the corrective actions will be effective.

4.3 COLLECTING EVIDENCE

The evidence that can be used to investigate human performance problems falls into three general types. These are defined here as physical evidence, documentary evidence and human evidence. A thorough discussion of evidence collection and preservation methods is outside the scope of this document. Some of the methods for and challenges in collecting and preserving evidence are discussed here, however, to facilitate review of the licensee's investigation.

Physical evidence is any matter (e.g., solids, liquids, gases) related to the error or human performance problem, such as equipment, parts, debris, contaminated water, hardware or tools. Physical evidence may be used to establish the state or condition of equipment and the work environment prior to an event as well as to determine what happened in the course of the event. For example, examination of the personal protective equipment worn by the individuals involved may show that their ability to see through a faceplate or to make fine manual adjustments in gloves was limited and could have contributed to an error. At times, physical evidence regarding the state or condition of the individuals involved in an event may also be collected, such as collecting urine or blood samples to test for the presence of drug metabolites. Assuring that perishable physical evidence is analyzed before it degrades, and that non-perishable evidence is controlled so that it is available for further analysis, if necessary, are two important challenges in gathering physical evidence.

Documentary evidence is also useful in understanding human performance problems, and particularly any programmatic causes for an error. Documents regarding the work activity in

which the human performance problem occurred help to establish what happened, who was involved and the conditions under which the problem arose. Examples of documentary evidence include:

- Event recordings (e.g., event history, computer printouts, automatic and manual plots of plant variables as a function of time showing the occurrence of alarms, system activations, and other conditions during the event). These documents may show, for example, the actions that were taken, when they were taken and any unusual conditions that existed at the time.
- Design drawings, specifications, design and installation procedures, modification packages. These documents may be useful in identifying discrepancies between how a system was designed and how it was functioning at the time an error occurred, for example. This information might allow the investigator to determine whether personnel were trained appropriately and whether the instructions and supporting information they had available during task performance were accurate.
- Maintenance records for affected systems, including vendor manuals. Maintenance records may be useful in determining, for example, the point in time at which an error during maintenance first occurred and, perhaps, how often it was repeated. Vendor manuals can be used to verify that procedures are up-to-date.
- Procedures and work orders used during or relevant to the event. These documents are very useful in establishing what happened in the event and in identifying discrepancies between what was planned versus what was implemented.
- Plant technical specifications and associated safety analyses. These documents are often useful in identifying discrepancies between what should have occurred versus what actually happened.
- Operations logs. Similar to event recordings, these documents may be helpful in establishing what happened and when.
- Correspondence, such as e-mails, letters, memoranda. These documents may also contain information that is useful in establishing the event timeline, but also often contain important information about the organizational work environment.
- Records of similar events, including root causes and corrective actions. These documents assist investigators in assessing the scope of the human performance problem as well as the effectiveness of previous corrective actions for similar human performance problems.
- Descriptions of programs, processes, and practices addressing plant operations and maintenance, personnel performance, and procedure development. These documents often clarify programmatic weaknesses, such as missing or weak barriers to error.

Human evidence is typically the primary source of information about human performance problems, and may include written statements, the results of interviews, recordings of human actions during the event or similar work activities, and the results of event reconstruction activities. For example, audio or videotapes of the situation that preceded or occurred during the event can be particularly useful for analyzing an error, but are usually not recorded. Tapes of similar work activities, such as those made of control room crews for training purposes, can be used to assess general work practices and may demonstrate an on-going human performance problem, or help to determine whether the particular error that occurred in an event is common.

Human evidence may also include demonstrations of critical actions, such as manipulations of the equipment involved in the event; walk through exercises, in which personnel act out important actions as the stages of a scenario are described or are directed by procedure steps; and dynamic exercises, in which scenarios are reenacted under more realistic conditions, such as in a training simulator. These evidence collection activities may provide information about possible task overload, for example, or deficiencies in the human-system interface, coordination and communication problems, knowledge or skill deficiencies, and so on.

The participants in an event are often available to the investigator and are typically able to provide the most detailed information about the error that occurred or the human performance problem. As discussed in Section 3, however, individuals' memories for events may be limited, if they are not interviewed immediately after the event. Further, they may not possess complete information about the event, because what they remember will be limited to the aspects of the event on which they were focused at the time. Or, memory for the event may be distorted from strong emotion, the passage of time and intervening thoughts, by hearing others' descriptions of what occurred or discussing it with them, the kinds of questions that are asked during the interview, and other factors. Licensee investigators should interview eyewitnesses who observed the event but did not participate in it as well as the event participants as soon as possible after the event.

The information obtained from different sources is often conflicting. Further evidence collection may resolve some conflicts. As a simple example, an operator may report in an interview that he entered a room at a particular time, but the entry records for that room show that he keyed in about 15 minutes later than he reported. Additional evidence regarding the accuracy and reliability of the clock used when recording entries may allow the investigator to conclude that the entry log is the more accurate information source. In other instances, it may not be possible to collect additional evidence to resolve conflicts. In these cases, investigators will have to weigh the evidence and use judgment to reach a conclusion. For example, if five eyewitnesses' descriptions of an event are consistent, but vary from the description given by the individual who committed the error, the investigator might conclude that the eyewitnesses' accounts were more valid.

It is often the case, however, that the evidence an investigator needs to conclusively establish what happened or why an error occurred does not exist or is unavailable. In these cases, investigators may have to assume that certain events occurred or conditions existed to explain the error, or may develop and analyze plausible alternative scenarios. Given that human performance is often so difficult to explain post hoc, it may be possible to derive some lessons learned from the investigation but not to develop corrective actions that will be effective in minimizing the likelihood that a similar error will reoccur.

As noted above, collecting evidence about a human performance problem is an iterative process. As answers to one question are found, other questions arise that require follow-up. In addition, new information may shed a different light on information collected earlier in the investigation or conflict with it, so that additional information collection is necessary.

In general, the evidence gathered about a human performance problem should enable licensee staff to identify several possible causes for the problem. Plausible causes should be documented and the licensee should gather further evidence to confirm or rule out the possibilities. The most plausible causes that were not confirmed by the evidence and the basis for rejecting them should also be documented.

4.4 TERMINATING THE INVESTIGATION

The licensee's basis for terminating the investigation of a human performance problem should also be documented. Theoretically, an investigation could continue until every question is fully resolved. Time and resources for conducting an investigation this thoroughly are usually not available, however. Therefore, other criteria may be applied to determine when an investigation should be terminated. These could include, for example, a pre-set deadline for completing the investigation, reaching a dead-end due to the unavailability of further evidence, or a decision that the problem under investigation is minor and does not warrant the expenditure of further resources. For events that the licensee has classified as significant, the investigation is typically not terminated until the investigator and licensee management concur that sufficient evidence has been gathered to support the determination of the causes of the human performance problem and to develop specific and effective corrective actions.

5 EVALUATING THE LICENSEE'S ROOT CAUSE ANALYSIS

5.1 INTRODUCTION

Root cause analysis is a systematic method for analyzing the evidence collected about a hardware failure or human performance problem. The purpose of root cause analysis is to identify the basic set of conditions that, if eliminated or modified, would minimize the likelihood of the same and similar problems from happening again. Performing a systematic root cause analysis and identifying the direct, contributing and root causes for human performance problems aids in ensuring that the problem is understood with sufficient depth to support the development of effective correction actions.

In this section, background information for evaluating licensees' root cause analyses of human performance problems is presented. The different types of causes that may be identified as a result of using root cause analysis techniques are discussed, and detailed information about three commonly used root cause analysis techniques is presented. These techniques are events and causal factors charting and analysis, change analysis and barrier analysis.

5.2 CAUSAL FACTORS

A **causal factor** is any action or condition that occurred or existed prior to an error without which the error is less likely have occurred. There are three types of causal factors that a root cause analysis will typically identify. These are the direct cause, contributing causes and root causes. Programmatic weaknesses are also often identified using root cause analysis techniques, and may be determined to be either contributing or root causes of a human performance problem. Apparent causes for an error may be identified by a licensee in problem reports for tracking and trending purposes, but are not derived from applying a formal root cause analysis technique.

A **direct cause** is the action or condition immediately preceding an error in an event sequence that caused or allowed the error to occur. For example, consider a situation in which an operator silenced what he thought was a nuisance high radiation alarm from an air monitor that had a history of spurious activations. Within a few minutes, however, it was discovered that the alarm was valid when several other air monitors in the same area also alarmed. The error here was failing to confirm whether the alarm was valid before silencing it. The investigation and analysis in this example showed that the direct cause of the error (i.e., the reason that the operator did not confirm the alarm's validity before silencing it) was the operator's belief that the alarm was invalid, based on its history of spurious activations. (Many other examples of typical direct causes for human errors can be found in Part II of this document, the HPEP Cause Modules.)

A **contributing cause** is the actions or conditions that set the stage for a human performance problem to occur, but, alone, were not sufficient to cause it. A contributing cause may be a long-standing condition or a series of prior events and problems that, while unimportant in themselves, increased the probability of error. For example, consider again the operator who silenced the high radiation alarm. In this case, the alarm's history of spurious activation would

be a contributing cause for the error, because it set the stage for the error, but, alone, did not cause it. Other operators at the site or at other plants might have assessed conditions in the area monitored before silencing the alarm, so the alarm's history contributed to the operator's action of silencing the alarm, but did not fully explain it.

A **root cause** of a human performance problem is the set of conditions that, if eliminated or modified, would minimize the likelihood that the problem would reoccur as well as prevent similar problems from occurring. A root cause is often responsible for multiple human errors or hardware failures, rather than single problems. Root causes are more fundamental causes than direct causes, affect a wider scope of work activities, are both necessary and sufficient to cause the problem, and are often the results of programmatic weaknesses. In the case of the alarm error, a deficiency in alarm response procedures, supervision or training may have allowed a practice to develop of silencing alarms without verifying conditions. If so, weaknesses in the procedures or training programs could be a root cause of the error and some other operators at the plant, who use the same procedures or have received the same training, may be likely to commit the same error. Weaknesses in immediate supervision, such as the failure to communicate and enforce management expectations regarding alarm verification before silencing, could also be a root cause of the error.

A **programmatic cause** is a deficiency in one of the licensee's programs for managing work activities at a site that allows human errors to occur and may be the root cause of a single error as well as an adverse human performance trend. Licensee programs, such as the procedures and training programs, overtime policies and practices, or the fitness-for-duty program, are implemented by management to create and maintain barriers to errors. When weaknesses exist in these programs, or their implementation is flawed, the barriers to error they are intended to maintain may be ineffective. In the alarm example discussed above, a failure to emphasize alarm verification, even of nuisance alarms, in the operator training program would be a programmatic cause of the operators error, as well as a possible root cause. Other examples of common programmatic causes for human performance problems can be found in Part II of this document, the HPEP Cause Modules.

Many licensees also identify apparent causes for human performance problems that are perceived as having little individual significance but that will be tracked to enable monitoring of developing trends. An **apparent cause** is typically an estimate of the direct cause of an event or problem, based upon a limited investigation. An apparent cause is identified without using standard root cause analysis techniques.

Using standard root cause analysis techniques is not a regulatory requirement. The licensee is required under 10 CFR 50 Appendix B Criteria XVI to prevent the recurrence of "significant conditions adverse to quality," however, and many licensees have concluded that the use of standard root cause analysis techniques is beneficial in understanding and correcting these significant conditions. Licensees specify the criteria for determining significance, which may include issues of risk, regulatory requirements and economic considerations. Other conditions that are "adverse to quality," but do not meet the licensee's significance criteria, may be assigned an apparent cause on the basis of a cursory investigation and without a formal root

cause analysis. In some cases, the licensee may elect to track these low-risk conditions and monitor adverse trends for a larger number of similar conditions. If the trending indicates a common or related cause for these conditions, then a root cause determination may be required by the licensee's policy or administrative procedures.

5.3 OVERVIEW OF ROOT CAUSE ANALYSIS TECHNIQUES

Root cause analysis relies to some extent on judgment. However, structured root cause analysis techniques provide step-by-step procedures that can be repeated and verified. Clear documentation of the analysis allows a reviewer to check its accuracy and completeness.

Several root cause analysis methods that may be used in licensee facilities are listed below:

- Events and causal factors analysis (to identify the events and conditions that led up to the human performance issue)
- Change analysis (to identify changes in the work environment since the job was last performed successfully that may have caused or contributed to the problem)
- Barrier analysis (to identify the barriers that, if present or strengthened, would have prevented the human performance issue from occurring)
- Management Oversight and Risk Tree (MORT) analysis (to systematically check that all possible causes of problems have been considered)
- Critical incident techniques (to identify critical actions that, if performed correctly, would have prevented the event from occurring or would have significantly reduced its consequences)
- Fault tree analysis (to identify relationships among events and the probability of event occurrence)

In general, a root cause analysis repeatedly asks the question "Why?" about the events and conditions that caused or contributed to the human performance problem.

Once the evidence has been gathered and the important causes for the human performance problem have been identified, the root cause analysis then looks for any relationships among the causes. The root cause analysis determines whether the causal factors demonstrate any order or precedence, either in terms of time or scope of effect. If one causal factor preceded another in time and affected it, or if a causal factor accounted for more than one of the human errors that occurred in an event sequence or among those comprising an adverse human performance trend, it is a candidate root cause. The goal of the analysis is to determine which causal factor(s), if corrected, would prevent the recurrence of the same and similar errors. Events and causal factors charting and analysis, change analysis and barrier analysis work well together to ensure that all causal factors are identified.

5.4 EVENTS AND CAUSAL FACTORS CHARTING AND ANALYSIS

Events and causal factors charting and analysis is a method for organizing and analyzing the evidence gathered during an investigation. An events and causal factors (ECF) chart graphically

displays the events and conditions associated with an occurrence (e.g., an error, a significant event, a human performance problem) the user wishes to understand. In an ECF analysis, the chart is used to identify the causal factors associated with the hardware failure or human performance problem.

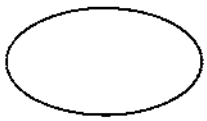
5.4.1 Events and Causal Factors Charting

An ECF chart is comprised of symbols that represent the important events and conditions that led up to the hardware failure or human performance problem under investigation. An **event** in an ECF chart is any action or occurrence that happened at a specific point in time relative to the hardware failure or human performance problem under investigation. A **condition** is a state or circumstance that affected the sequence of events in the ECF chart.

Some of the symbols that may be used for ECF charting are as follows[2]:

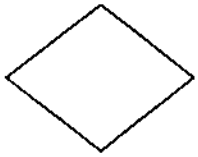
A rectangle is typically used to indicate an event. A brief description of the event is written within the symbol as well as the date and time at which the event occurred. Events are arranged in a line in chronological order from left to right.

Events that are assumed to have occurred, but for which no validated evidence exists or has yet been collected, may be indicated by a rectangle outlined with dashed lines.



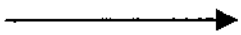
An oval is typically used to indicate a condition. A brief description of the condition is written within the oval and the condition is placed above the event it affected on the chart.

A condition that is assumed to have existed, but for which no validated evidence exists or has yet been collected, is indicated by an oval outlined with dashed lines.

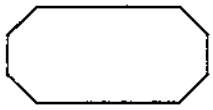


A diamond is used to indicate the occurrence of interest, such as a significant event.

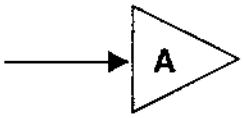
[2] The symbols used for charting are unimportant. Any symbol set or other method to differentiate among events, conditions, causes and their inter-relationship, such as color-coding, may be used in the chart.



Arrows are used to connect events, and to connect conditions to events.



An octagon may be used to indicate a causal factor and is placed above the events or conditions it caused.



Triangles are used to connect event lines that must be broken when, for example, the entire sequence of events will not fit on a page.

An example of an ECF chart can be found in Figure 5-1. This example depicts a partially completed ECF chart for an operational event in which the residual heat removal (RHR) system was overpressurized during initial pressurization of the reactor coolant system (RCS) following a refueling outage (NUREG/CR-5953, 1992).

Events and causal factors charting was developed to support the investigation of a single event. It can also be used to identify human performance problems. Developing ECF charts for the different errors that may represent an adverse trend and comparing them allows the detection of patterns and similarities in the events and conditions associated with the different errors.

5.4.2 Events and Causal Factors Analysis

Analysis of the ECF chart begins after the investigation is completed, although the analysis itself may raise additional questions that require further investigation. The analysis is performed to identify direct, contributing and root causes for the hardware failure or human performance problem of interest. The analysis consists of first identifying the significant events in the timeline and then evaluating them by asking a number of questions about each one.

An ECF chart will often contain events that did not play a causal role in the human performance problem under investigation, but must be included to "tell the story," so that others can understand what happened. These other events may be retained in the chart, but only the significant events will be analyzed.

Identifying the **significant events in the ECF chart** starts with the event that came immediately before the hardware failure or human performance problem of interest. To determine whether this event is significant or not, the question is asked, "If this event had not occurred, would the

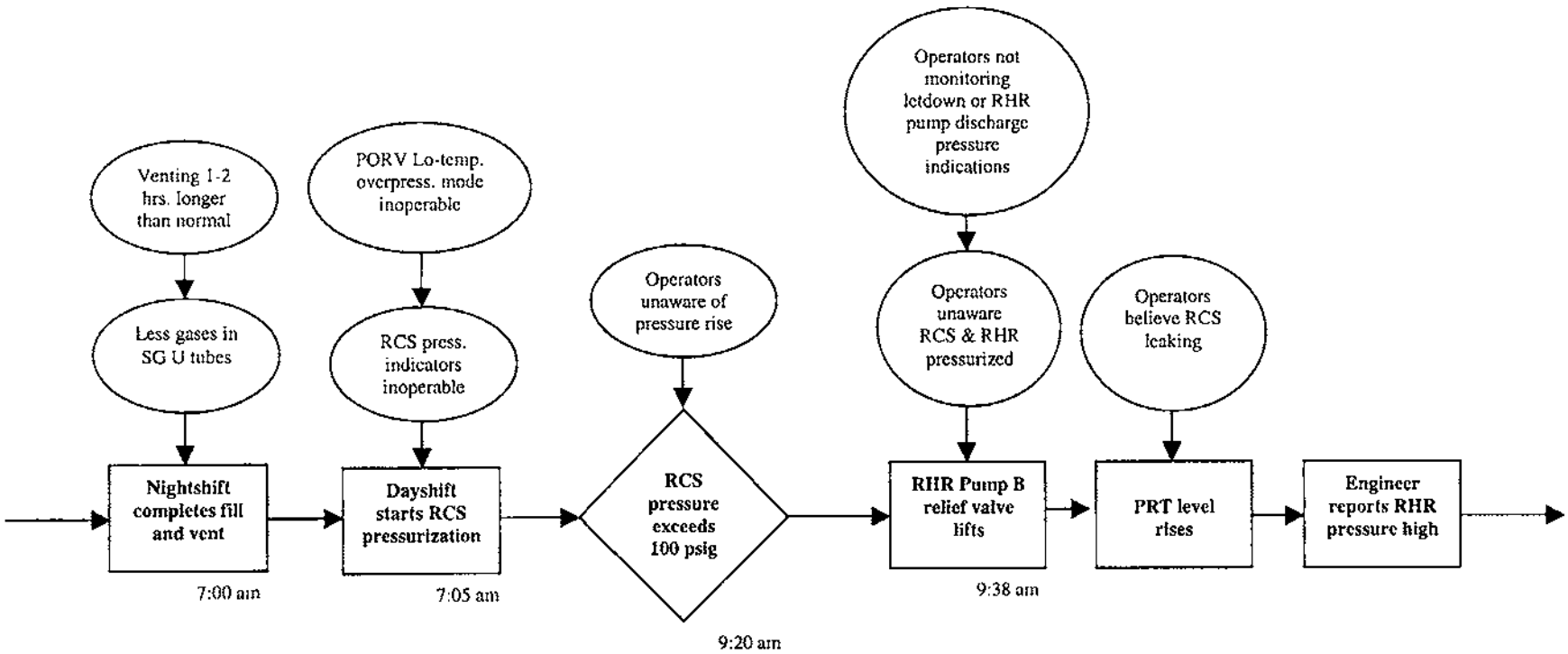


Figure 5-1. Partial ECF Chart from March, 1990 RHR Overpressurization Event

failure have occurred?" If the answer to this question is, "Yes," then the question is asked whether the event represented a normal activity with the expected outcomes. If it was a normal activity with the expected outcomes (e.g., the maintenance technician arrived at work, control rods were inserted and the reactor scrammed), then it is not a significant event in the chart. If the event had unplanned or unwanted consequences, then it is a significant event in the chart and should be further analyzed by asking the following additional questions:

- What were the other events and conditions that led to the significant event?
- What went wrong that allowed the event to occur?
- Why did those conditions exist?
- Were other significant events necessary for the failure or problem to occur or would the recurrent of this event alone lead to another failure or problem?
- Is the significant event linked to other events or conditions that may indicate a more general or larger deficiency, such as a programmatic weakness?

For example, in Figure 5-1, the event in the chart that precedes the overpressurization was the control room crew initiating system pressurization. Starting RCS pressurization is a significant event in this timeline, because, obviously, RCS could not have overpressurized without it and because initiating pressurization had unplanned and unwanted consequences.

The significant events in an ECF chart, and the events and conditions that were responsible for them, are causal factors. A brief statement that summarizes the relevant characteristics of the causal factor is added to the ECF chart above the significant event to which it applies. Figure 5-2 shows the ECF chart for the overpressurization event with one causal factor added above the conditions and event in the chart to which it applies.

When each significant event in the chart has been analyzed, relationships among the causal factors may be revealed. For example, in some situations, several examples of training weaknesses may be identified or the failure of one piece of equipment or system is found to have caused several of the events in the chart. When common causes are found, they may indicate the root cause of the problem under investigation.

5.5 CHANGE ANALYSIS

Changes in the work environment often result in unanticipated and unwanted consequences. **Change analysis** involves systematically identifying and analyzing any changes that may have affected the problem under investigation.

Many types of changes may lead to unwanted consequences. These could include, for example, changes in

- the characteristics or number of workers involved in the task
- other work activities going on concurrently with the work activity of interest
- equipment condition or status
- the work location or the environmental conditions in which the work was performed

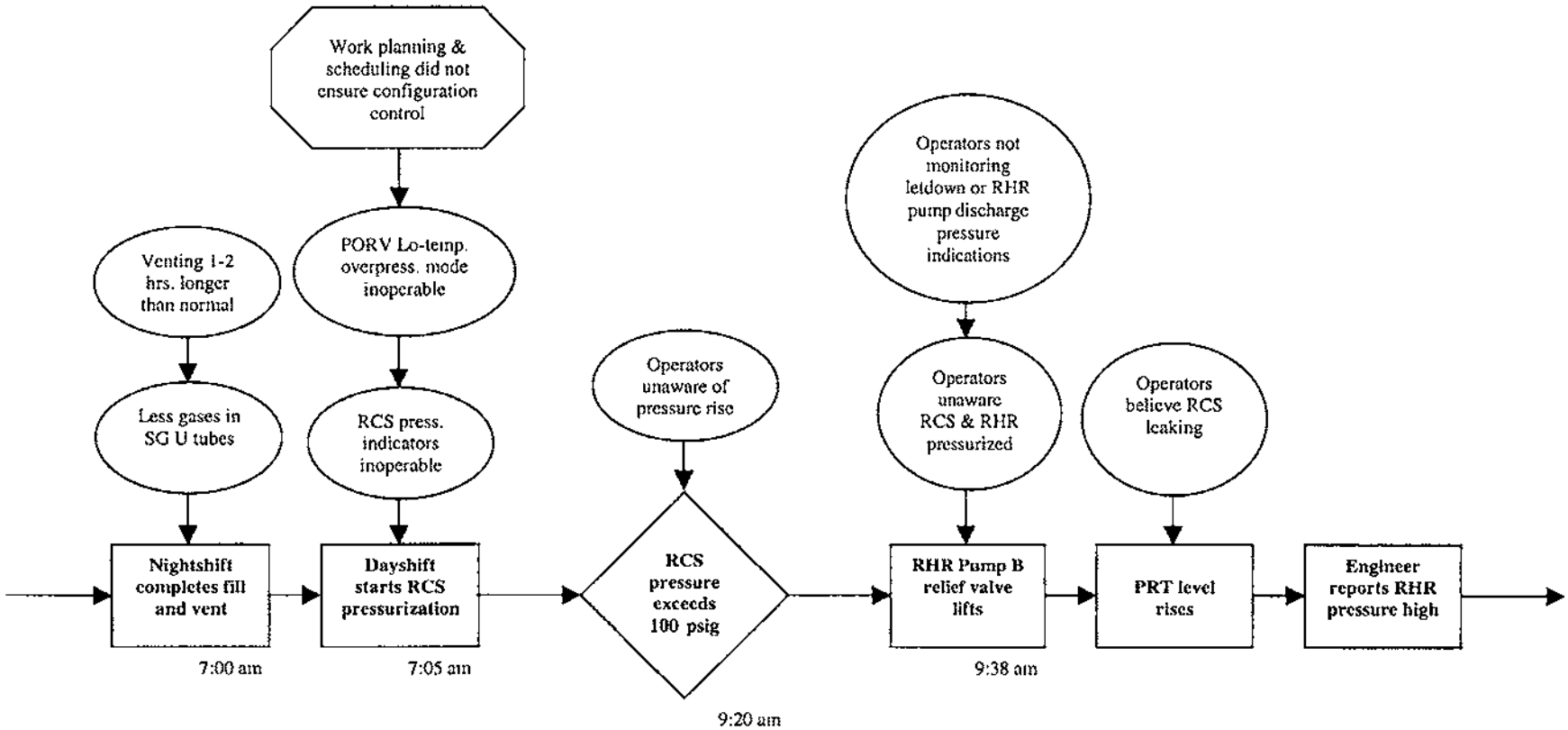


Figure 5-2. Partial ECF Chart from March, 1990 RHR Overpressurization Event with One Causal Factor Added

- supervision
- management expectations for the work.

Changes that may lead to an unwanted occurrence can be difficult to detect in advance because change is pervasive. Change control processes, such as reviewing the safety implications of planned changes, are one method to ensure that changes do not have a negative impact on safe operations. Formal reviews or risk analyses sometimes miss important conditions, however. There also are many avenues for introducing changes to the work environment that do not appear to be sufficiently risky to warrant formal review.

Change analysis for human performance problems is most effective when the same work activity has been performed successfully in the past, when the work activity and conditions under which it was performed were documented or can be reconstructed, and when procedures for performing the work are available. Change analysis can also be performed by comparing the work activity under investigation to how the work activity is successfully performed at other sites, or to "ideal" situations as documented in standards and regulations.

The first step of a change analysis is to define the "event-free situation" and compare it to the situation in which the "event" under investigation occurred. The "event" may be any hardware failure, human error or human performance problem. The "event-free" situation is a comparable situation in which the hardware did not fail or the work activity was performed successfully.

Once the "event" and "event-free" situations have been identified, they are analyzed to determine the specific differences between them. The impact of each difference on the event is then evaluated to determine whether the change was unimportant or was a direct, contributing, root and/or programmatic cause of the problem.

Table 5.1 shows an example of a change analysis worksheet for the overpressurization event discussed previously. The human error of interest is the operators' failure to detect and control the rapid rise in RCS pressure. As can be seen in Table 5.1, four changes from previous occasions on which RCS pressurization activities were performed successfully were identified.

Evaluating the causal roles of these changes involves asking, for each change, whether or not it meets the definition of a direct, contributing, root and/or programmatic cause, or did not play a causal role in the error. In this example, the inoperability of the RCS pressure transmitters was the direct cause of the error, because it was "the action or condition immediately preceding the error in the event sequence that caused or allowed the error to occur." If the RCS pressure transmitters were operable, the crew would have detected the rapid pressure increase in time to control it and prevent the transient. Evaluation of the roles of the other four changes, based on the evidence available, indicates that they were contributing causes. That is, each of the changes, alone, did not cause the error, but rather set the stage for it. It was the combination of these additional changes with the inoperability of the RCS pressure indications that allowed the event to occur.

Table 5.1 Example Change Analysis Worksheet for an RCS Overpressurization Event

Event Situation	Event-Free Situation	Difference	Effect on Event
RCS pressure instrument transmitters isolated for maintenance	RCS pressure indicators operable	No accurate indications of RCS pressure were available	Operators were unable to monitor RCS pressure
Fill and venting of reactor head extended	Fill and vent evolution completed within normal time limits	Venting continued 1-2 hours longer than normally	The longer vent and fill evolution decreased the volume of gases in the steam generator (SG) U tubes
Reduced volume of gases in SG U tubes caused by longer vent time	Greater volume of gases in SG U tubes	Reduced amount of non-condensable gases caused RCS pressure to increase sooner than in previous refill operations	RCS pressure rose sooner then expected and approached 100 psig within 2.5 hours of initiating pressurization
Operators were monitoring the inoperable RCS pressure gauges, but not all available pressure indications (e.g., letdown and RHR discharge pump pressure gauges)	Operators monitored all available pressure indications	Operators did not detect indications of the rapid pressure increases on the letdown and RHR discharge pump pressure gauges	An opportunity to detect the pressure rise and prevent the overpressurization was missed

5.6 BARRIER ANALYSIS

The **barrier analysis** technique can also be used to identify causes for human performance problems. The purpose of a barrier analysis is to identify the barriers to error that were missing, bypassed or failed and their causal roles. Barrier analysis also shows the barriers that succeeded and prevented the problem from having more serious consequences.

Barrier analysis is based on the concept that **hazards** represent potentially harmful energy flows or environmental conditions from which **targets** (i.e., personnel and equipment) must be protected. Hazards to personnel may include, for example, radiation, electrical energy, chemical and biological agents or adverse environmental conditions. Hazards to equipment may include human error, damage from wear and tear or natural phenomena.

A **barrier** is any means used to protect targets from hazards. There are two basic types: physical and management barriers. Examples of typical physical barriers used in industrial settings to protect personnel are fences, guardrails around moving equipment, protective clothing and safety devices. Management barriers used to protect equipment in nuclear licensee facilities

include preventative and corrective maintenance as well as supervision, training, the design of the human-system interface or procedures to reduce the likelihood of damage from human error. The barriers that could or should have been in-place and how they should have functioned can be identified from subject matter expertise, knowledge of industry good practices, licensee policies and procedures, design basis documents and regulations.

A barrier analysis is performed in five steps. The first step is to identify the hazard and target. The second step is to identify all of the barriers that could have protected the target from the hazard. The third step is to evaluate how each barrier performed. That is, did the barrier succeed or fail? For barriers that failed, the fourth step is to determine why they failed. Finally, the causal role of each barrier is evaluated to determine whether it was a direct, contributing, root and/or programmatic cause.

This technique is particularly useful in providing the basis for developing corrective actions to prevent the same or a similar problem from happening again. Corrective actions can strengthen existing barriers that failed or erect barriers where they are missing.

Table 5.2 shows an example of a barrier analysis worksheet for the RCS overpressurization event. In this example, the hazard would be pressure and the target would be the catastrophic failure of the reactor coolant or residual heat removal system piping.

Evaluating the causal role of each failed barrier involves asking whether or not it meets the definition of a direct, contributing or root cause, or did not play a causal role in the error. In this example, the inoperability of the RCS pressure transmitters again meets the criterion for the direct cause of the error, because it was "the action or condition immediately preceding the error in the event sequence that caused or allowed the error to occur." Further, if the RCS pressure transmitters were operable, two additional physical barriers would not have failed: the power-operated relief valves (PORVs) low-temperature overpressure protection and the computer alarm. Because the failure of these barriers was dependent upon the RCS pressure transmitters being inoperable, they are contributing causes of this event.

As can be seen from this example, barrier analysis is an effective method to begin identifying programmatic causes as well as potential corrective actions. For example, had the RCS pressure indicators been tagged out-of-service, it is unlikely that the operators would have started RCS pressurization activities until these indications were available. The station's policy of excluding control room instrumentation from the tagout program indicates that the scope of the tagout program may have been a programmatic weakness that, if corrected, could have prevented this event and other, similar events. However, responsibility for configuration control lies with the work management program. Had the work planners (or an independent review) recognized that the RCS indicators were not available for initial RCS pressurization and ensured that they were, the rate of the pressure rise and the operators' focus on the three RCS indicators would not have mattered because accurate pressure indications would have been available to detect and control pressure. Therefore, the startup procedure and the operators' status monitoring were contributing causes to the event, but not root causes. Further investigation of the work management program

Table 5.2 Example Barrier Analysis Worksheet for Overpressurization Event

Hazard: Pressure		**Target:** Catastrophic failure of system piping	
Physical Barriers	**Performance**	**Why Did it Fail?**	**Effect on Event**
RCS pressure instrument transmitters	Failed	Out of service for maintenance	RCS pressure indicators inoperable so operators could not detect rapid pressure rise
Power-operated relief valves (PORVs) low-temperature overpressure protection	Failed	The two wide-range RCS pressure instruments were the sensors for the PORV low-temperature over-pressure protection mode	PORV low-temperature over-pressure protection unavailable
RHR Pump B suction relief valve	Succeeded in stopping uncontrolled pressure rise		Maintained pressure below limits – prevented catastrophic failure of RHR piping
Pressurizer relief tank (PRT) level indication	PRT level increased when RHR suction relief valve opened		Succeeded in alerting operators to problem situation
Annunciators	Missing	RHR pressure did not reach alarm actuation setpoint and computer alarm came off the inoperable pressure transmitters	No audible indications of pressure rise
Management Barriers	**Performance**	**Why Did it Fail?**	**Effect on Event**
Startup procedures	Did not control RCS vent evolution	Fill and vent procedure did not specify a time limit for venting gases from reactor head	Night shift extended the RCS vent evolution 1-2 hours longer than normal, reducing the volume of gases remaining in the SG U tubes
Work management (planning and scheduling)	Failed	Work planners overlooked the need for the RCS pressure instruments to be operable before initial pressurization of the RCS	Pressurization was initiated without RCS pressure indications operable
Independent review	Missing	Not performed or required	Failed to identify the RCS pressure instrument isolation
Tagging out-of-service control room instruments	Missing	Tagging of out-of-service instruments in control room not required by tagout program	There was no visual cue that the three RCS pressure indicators were inoperable
Systems monitoring	Inadequate	Operators were focused on the RCS pressure indicators and were not monitoring all pressure indications available	Operators did not notice other indications of the pressure rise that indicated RHR, CVCS and RCS were pressurized

would be necessary to identify the specific weaknesses that allowed this event to occur, as well as the corrective actions necessary to strengthen the program. However, flaws in the work management program appear to have been the root cause of the operators' error in this event.

5.7 COMBINING TECHNIQUES

Practical experience has shown that different root cause analysis techniques provide different perspectives on an event. As a result, using a combination of methods ensures that a more complete set of causal factors is identified.

Because different root cause analysis techniques ask different questions about a human performance or hardware problem, the causes that are identified may differ. Compare, for example, the differences in the causal factors above that resulted from the change and barrier analyses for the overpressurization event. For the overpressurization event, the barrier analysis yielded a larger number of causal factors and led to the identification of the root causes of the event. For other events, changes may be the key causal factors and barrier analysis used alone may not identify them.

No matter which root cause analysis techniques are used by a licensee, the purpose of the analysis is to identify the causal factors that, if corrected, would minimize the likelihood that the same and similar "significant conditions adverse to quality" will occur again. The effectiveness of a problem identification and resolution program rests less on the root cause analysis techniques used than on the thoroughness of the investigation conducted, assurance that the key causal factors have been identified, and the development and implementation of the corrective actions suggested by the analysis.

6 EVALUATING CORRECTIVE ACTION PLANS

6.1 INTRODUCTION

An effective **corrective action** for a human performance problem is one that will minimize the likelihood of the problem happening again. Developing effective corrective actions for human performance problems requires a thorough root cause analysis and an understanding of methods for enhancing human performance.

In this section, background information for evaluating corrective actions plans is presented. The different types of corrective action plans and issues in implementing them are discussed.

6.2 CORRECTIVE ACTION PLAN SCOPE

Corrective action plans, which incorporate corrective actions for human performance problems, vary in scope. The scope of the plan is determined by the significance of the error or adverse trend as well as the extent of the conditions created by the causal factors identified. Three types are described below.

The broadest type is a **general organizational improvement plan**. This type of plan usually involves all or a large number of the work groups at a site and, sometimes, corporate headquarters. Its purpose is to make significant changes in how work is done and how it is managed in order to improve operational performance and to reverse declining performance trends. Corrective actions may address problems in any aspect of plant operations, such as

- changing the organizational structure
- changing managers' spans of control
- improving manager capabilities and competence
- improving worker training and qualification programs
- revising the hierarchical family of vision, goals, objectives, policies, programs, processes, procedures and practices.

General organizational improvement plans are typically required to correct a safety culture problem in an organization.

An **intermediate scope corrective action plan** focuses on adding to or strengthening the programs that are responsible for maintaining barriers to human performance problems. Typical programs that are implemented to maintain barriers to error are:

- programs for developing procedures, keeping them updated and requiring their use for certain jobs
- human resources programs for selecting and promoting personnel
- behavioral safety programs such as STAR (Stop, Think, Act, Review)

- human-system interface design programs, such as the program responsible for ensuring that labels on parts and equipment are accurate and legible
- management systems for defining and organizing work flow
- quality control programs.

Limited scope corrective action plans focus on fixing the direct cause of an error. These plans add or strengthen specific barriers.

Corrective actions to add new barriers might include:

- writing a procedure for a task that previously depended on "skill of the craft"
- moving personnel with operations experience into the work planning group
- developing a new training module for maintenance workers, or
- replacing an analog display with a new digital display that is more accurate and easier to read.

Corrective actions to strengthen existing barriers could be redesigning an existing training module or adding a requirement for a supervisor to be present when a particular job is performed. Most limited corrective action plans use a combination of adding new and strengthening existing barriers.

Sometimes correcting the direct cause of an error will prevent that specific error from recurring but fail to prevent similar errors. For example, if the direct cause of an error was an ambiguous procedure step, fixing that one step may stop others from making the same error when performing that step. But fixing that step in the procedure will not correct other ambiguous steps in the same procedure or in other procedures. If the ambiguous steps have the same root cause, such as a procedure writer in need of additional training, the root cause must be corrected to prevent future errors due to poorly written procedure steps.

Corrective action plans must also address any adverse conditions that were created by a human performance problem, based upon the assessment done of the extent of the conditions created by a causal factor. For example, if an instrument is miscalibrated and the cause is determined to be an error in a miscalibration procedure, the corrective action plan must include actions not only to ensure that the instrument is re-calibrated correctly, but also that other instruments governed by the same procedure are also calibrated correctly.

The appropriate scope of a corrective action plan depends upon the nature of the causal factors identified in the root cause analysis, their scope and the risks they pose. Licensees may use probabilistic risk assessment or human reliability analysis methods to choose among corrective action alternatives.

6.3 ACCOUNTABILITY FOR HUMAN PERFORMANCE

Some corrective actions in a corrective action plan may focus on the individual worker who committed an error. These corrective actions may include, for example, remedial training, participation in the investigation and root cause analysis, loss of qualification for a period of time and/or time off work.

Corrective actions that focus on the individual worker are often ineffective. Routinely placing responsibility for errors on the individual workers adversely impacts a licensee's safety culture and may discourage personnel from reporting errors or raising concerns. A "blame the worker" approach to human performance may result in adversarial relations between workers and supervisors, which will hinder effective communication and teamwork. On the other hand, it may be appropriate to hold workers accountable for errors if they have been provided with the necessary resources to perform their tasks correctly. These resources include relevant training, usable and technically accurate procedures, well-designed tools and equipment, accurate drawings, labels on equipment and other operator aids, and clearly defined and specific management expectations for performing each task. Industry experience has shown that improving human performance requires balancing the organization's responsibility for providing personnel with the tools and resources they need to accomplish their tasks with individual accountability for performance to reasonable standards.

6.4 CORRECTIVE ACTION PLAN COMPLETENESS

An important requirement for corrective action plan effectiveness is completeness. A complete corrective action plan addresses each of the causal factors that were identified from the root cause analysis. In some cases, a single corrective action may address more than one causal factor. For example, if a root cause analysis has identified several weaknesses in work planning and scheduling, the licensee may decide to re-engineer the entire work management program. Often, several corrective actions may be developed to address one causal factor. More than one corrective action may be required because the causal factor is complex or the licensee wishes to ensure there is "defense-in-depth" against a recurrence of the human performance problem.

6.5 PLAN IMPLEMENTATION AND EFFECTIVENESS

Corrective action plans that appear to have an appropriate scope and to be complete may be ineffective when they are implemented. Corrective action plan implementation may be ineffective for several reasons.

A common reason that corrective action plans fail is that detailed information from the problem investigation and root cause analysis is not communicated to those who are assigned responsibility for developing and implementing the corrective actions. The detailed information about the human performance problem that has been collected is usually not recorded in the investigation report or presented in a briefing. Further, information collected about human performance problem may include sensitive personnel matters that are not documented. A

detailed understanding of the human performance problem is necessary for corrective action effectiveness, however, because these problems are typically complex with multiple, interacting causes. Ensuring that the individuals involved in investigating and analyzing human performance problems work closely with the personnel responsible for the corrective action plans improves the likelihood that the plans will be effective.

Other commonly identified reasons for ineffective corrective action plans are:

- **Responsibility not assigned**. Responsibility for developing, implementing and monitoring the effectiveness of corrective actions may not be assigned to specific individuals who are held accountable for them. Responsibility for corrective actions may be assigned to a department or to "management," rather than to individuals who have the expertise, authority and resources to ensure they are implemented.

- **Staffing changes.** Personnel change jobs and the individuals who developed and began implementing a corrective action plan may move on to other positions. The information they had about the basis for a corrective action plan may not be communicated to their successors.

- The steps for achieving the plan's **objectives are not defined**. Some corrective action plans define the goals to be achieved, but not the steps required to achieve them. Corrective action implementation is typically most effective when project management techniques are used, such as defining milestones and deliverables, a project schedule, the resources required, and so on.

- **Competition for resources**. Other management initiatives and events arise that take precedence over implementing the corrective actions.

- **Measurement.** Corrective action plans may fail because measures for determining the success of the corrective actions were not defined and used to refine the plan when necessary.

- **Unintended consequences.** Corrective actions may have unforeseen, unintended consequences that cause them to fail.

For human performance problems that have a relatively high risk significance, the licensee may schedule effectiveness reviews for the corrective action plan that was implemented. **Corrective action effectiveness reviews** are analyses of whether the corrective actions in a plan have worked as intended. They are typically scheduled weeks or months after a corrective action has been implemented and has had time to demonstrate an effect. The schedule for conducting effectiveness reviews and the measures of effectiveness that will be used may be included in the initial corrective action plan.

6.6 CONCLUSION

The most important test of a corrective action plan is whether it succeeds in minimizing recurrence of the human performance problem it is designed to address. As discussed in Section 3, however, the recurrence of a problem behavior does not necessarily indicate that a corrective action plan is ineffective because the same behavior can result from many different causal factors. The corrective action plan may have been effective in controlling one cause for a particular behavior, but other causes may still exist. These other causes could not have been identified in the investigation and analysis because they did not play a role in the original problem. Investigation and causal analysis of the recurrent problem behavior would be necessary to determine whether the corrective action plan for the initial problem was ineffective or whether the recurrent problem is due to other causes that would then need to be addressed.

THE HUMAN PERFORMANCE EVALUATION PROCESS

Part II: The HPEP Cause Tree and Modules

7 OVERVIEW OF THE HPEP CAUSE TREE AND MODULES

7.1 INTRODUCTION

Part II of the Human Performance Evaluation Process (HPEP) is comprised of the HPEP Cause Tree and Modules. The HPEP Cause Tree is a screening tool for identifying the range of possible causes for a human performance problem. The Cause Modules discuss typical causes of human performance problems in nuclear licensee facilities and provide examples of frequently identified direct and programmatic causes, based upon the research literature and industry experience.

The Cause Tree and Modules are not a complete list of all possible causes for human errors. In practice, the evidence that is collected in an investigation and the results of causal analyses are necessary to determine an error's actual cause(s). The primary value of a list of possible causes, such as those presented here, is that it prompts consideration of a range of causes. Used as a checklist, the Cause Tree and Modules assist in overcoming the tendency to arrive at conclusions too early in an investigation or to only investigate the possibilities that are initially suggested when an error is committed. Thus, the Cause Tree and Modules are intended to be used heuristically, but the possible causes that are investigated must be derived from the evidence.

7.2 USING THE CAUSE TREE AND MODULES

Part II is for use by inspectors to verify the causes that a licensee has identified for human performance problems in order to complete Table 2.3, Causal Analyses, in Part I. The HPEP Cause Tree and Cause Modules may also be used as guidance in conducting an event investigation and to identify a human performance trend.

7.2.1 Verification

The HPEP Cause Tree and Modules are intended to assist in evaluating a licensee's causal analyses of human performance problems. In general, a causal analysis that is complete and valid will also be reliable. That is, it will yield similar results when repeated by another individual or team, although the specific terminology used to describe the cause(s) will likely differ. By answering the questions in the Cause Tree and reviewing the information in the appropriate Cause Modules, the inspector could verify that the evidence the licensee has gathered supports the causes identified and that other plausible causes can be ruled out.

To verify the licensee's conclusions, the inspector may (1) use the information available in the licensee's documentation of the investigation or collect evidence independently, (2) answer the questions in the Cause Tree and then (3) review the information in the appropriate Cause Modules to determine whether or not the licensee correctly identified the causes of a human performance problem. If the inspector arrives at direct and programmatic causes that are similar to those documented by the licensee, based upon the same evidence, it is likely that the licensee has accurately identified the causes for the human performance problem. If the inspector arrives at different direct and programmatic causes, then the Cause Modules may be used to identify additional information to request from the licensee. Or, the inspector may use the Cause

Modules to determine the lines of inquiry for an independent investigation. In most cases, discrepancies between the inspectors' cause(s) and the licensee's will be resolved on the basis of the evidence.

7.2.2 Conducting an Independent Event Investigation

If an inspector or NRC inspection team is conducting an independent event investigation, the Cause Tree and Modules can be used to understand the human errors that occurred in the event. The Cause Tree and Modules may be used to identify promising lines of inquiry to explore in the investigation. They may also serve as a checklist to ensure that possible causes for the error(s) have not been overlooked.

The Cause Tree will streamline an investigation by directing inspectors to the most likely causes of an error. Further evidence can then be collected regarding a specific cause to support the causal analysis. The lists of possible direct and programmatic causes within the Modules may be used to develop the specific lines of inquiry. For example, the Cause Tree would prompt inspectors to ask, "Were there weaknesses in the procedures used to perform the task?" If the answer were "yes," then the Procedures Module in Section 11 would prompt the investigators to further ask, "What were the procedural weaknesses and did they cause or contribute to the error? Were there systematic weaknesses in the procedures or another program that allowed these flaws in the procedure to exist? Are other licensee procedures similarly affected?"

As the investigation matures, the Cause Tree and Modules can be reviewed again to verify that potential causes have not been overlooked. Often the evidence that is gathered indicates that different causes than originally identified should be investigated. Repeated reference to the Cause Tree and Modules during the course of an investigation may help to assure that the investigation is complete and that sufficient evidence has been gathered to support the team's conclusions.

7.2.3 Identifying a Human Performance Trend

The Cause Tree and Modules may also be helpful in identifying a human performance trend. A human performance trend may be indicated if one cause category, such a procedures or supervision, is repeatedly identified by the licensee in a sample of problem reports, or appears to the inspector to be implicated in numerous problem reports.

To verify that a human performance trend has developed, however, it is important that the human errors are investigated and analyzed sufficiently to identify the direct and programmatic causes with some confidence. By definition, a human performance trend is a pattern of related errors resulting from the same causal factor. Therefore, licensee reports of the apparent causes of an error may be suggestive, but even a large number of reports citing a particular cause category do not establish the existence of a human performance trend unless the direct and programmatic causes of the errors are known.

7.3 ORGANIZATION

The HPEP Cause Tree is presented in Figure 7-1. The HPEP Cause Modules are presented in Sections 8 through 18. The Cause Tree asks a series of questions about the conditions surrounding a human error of interest. Based upon the answers to those questions, the inspector is referred to the appropriate Cause Modules. Each Cause Module is comprised of causal factors that have been found to affect human performance in the workplace as follows:

Personnel – These Cause Modules discuss characteristics that individual workers bring to the job that may affect task performance, such as

Section 8:	Fitness for Duty
Section 9:	Knowledge, Skills and Abilities
Section 10:	Attention and Motivation

Resources – These Cause Modules discuss characteristics of the resources available to personnel to assist in performing their tasks, such as

Section 11:	Procedures and Reference Documentation
Section 12:	Tools and Equipment
Section 13:	Staffing
Section 14:	Supervision

Work Environment – These Cause Modules discuss characteristics of the work environments in which personnel perform tasks, such as

Section 15:	Human-System Interface
Section 16:	Task Environment

Communication and Coordination – These Cause Modules discuss characteristics of the human interactions required to perform a task correctly, such as

Section 17:	Communication
Section 18:	Coordination and Control

Within each Cause Module, background information is presented regarding the effects of each causal factor on human performance and examples of typical direct and programmatic causes for errors are listed.

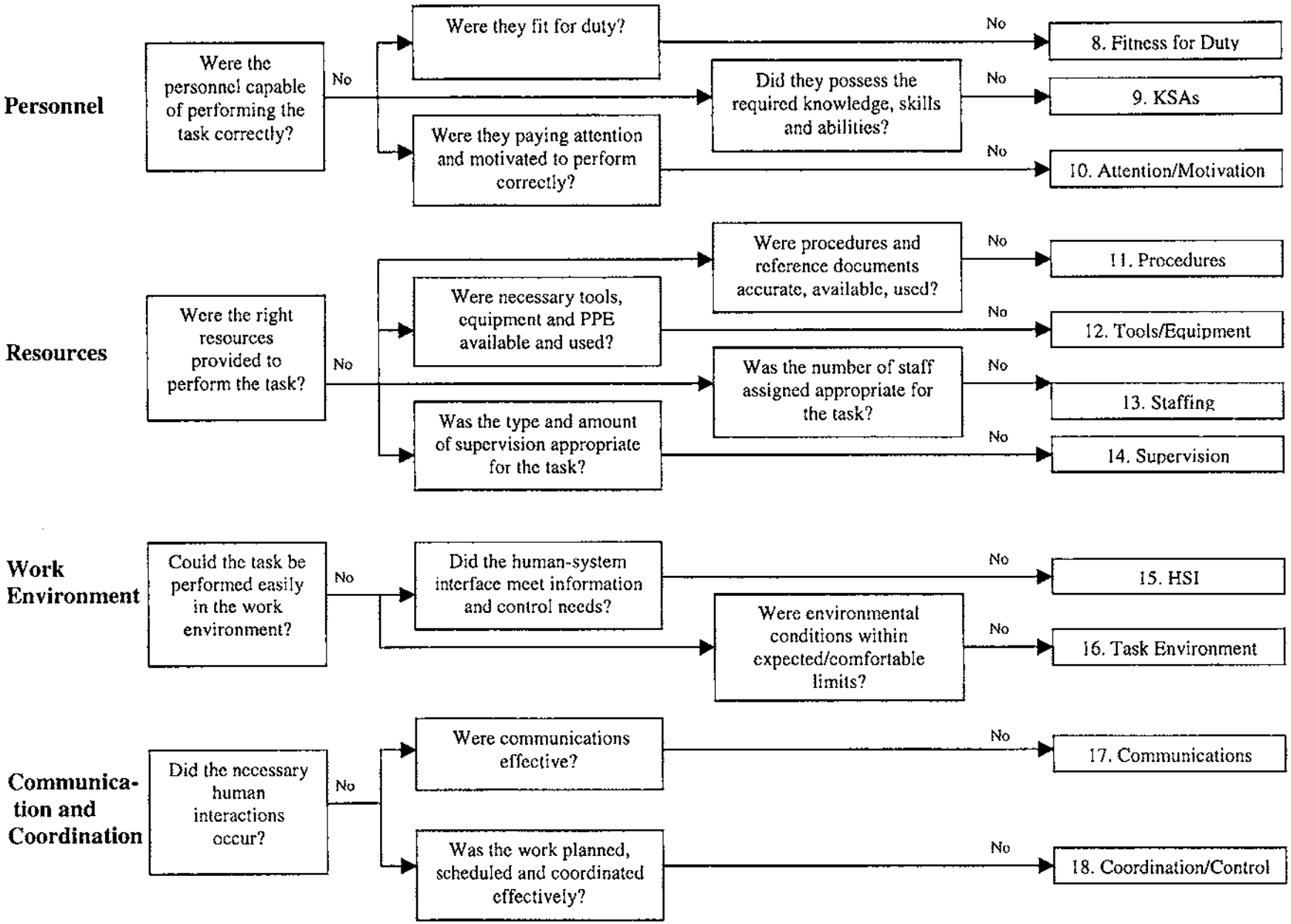


Figure 7-1 The HPEP Cause Tree

8 FITNESS FOR DUTY

8.1 ERRORS RELATED TO FITNESS FOR DUTY

Successful task performance requires that the capabilities workers bring to the task fall within an expected range. **Impairment**, or a reduction in an individual's mental or physical capabilities due to substance abuse, fatigue, illness or stress, increases the likelihood of errors. Types of possible impairments and their likely consequences for task performance are discussed below.

8.1.1 Drug and Alcohol Use

The use of some drugs and alcohol on the job or within several hours of reporting to work may adversely impact human performance. Extensive information about the effects of different drugs on task performance, including prescription and over-the-counter (OTC) drugs, has been published elsewhere (see Section 8.4 of this Module below). This information is briefly summarized here.

8.1.1.1 Marijuana

The use of marijuana has several effects that may adversely impact task performance. Marijuana use decreases the ability to process both auditory and visual stimuli, so may affect, for example, an individual's ability to read and follow procedures correctly or to correctly process verbal instructions. It also reduces an individual's attention span. Other effects include impaired social behavior and reduced retention and recall of information. Marijuana use also affects motor performance. It slows reaction time, decreases motor steadiness and manual dexterity, and reduces eye-hand coordination.

8.1.1.2 Stimulants

Drugs that are stimulants include caffeine, cocaine and amphetamines. Some OTC medications also contain stimulants, such as pseudophedrine, which is commonly used in cold and allergy medications. In small amounts, stimulants generally improve both cognitive and motor performance. For example, attention span is increased, vigilance is improved and reaction time is faster. Larger doses or chronic use adversely affect performance in all areas.

8.1.1.3 Depressants

Central nervous system depressants include the opiates, barbiturates, sedatives, the minor tranquilizers and alcohol. In general, higher doses are associated with significant cognitive and motor performance impairments. At lower doses, the effects depend upon the specific drug used, body weight and the extent to which the user has become habituated to it. For example, eye-hand coordination and performance of complex tasks will be adversely affected by barbiturate use, but typically are not affected by the minor tranquilizers. Use of drugs in this class will often cause drowsiness when they are first taken, but this effect decreases with continued use. Depressants cause disruptions in auditory and visual information processing, impair learning and recall, and reduce attention span.

8.1.1.4 Hallucinogens

Hallucinogens, by definition, are drugs that distort sensory perception, thought processes and behavior. There are four subclasses: anticholinergics (these are rare), catechols (e.g., peyote, mescaline, MDA), indoles (e.g., LSD, psilocybin), and anaesthetics (e.g., PCP). The anticholinergics are highly toxic and not of concern in the workplace. The catechols distort perception of light, color, space and shapes, and increase alertness. They are not associated with memory loss, but may cause muscle spasms in large doses. The indoles primarily cause mood and sensory perception changes leading to altered senses of time, space, touch and color. Vision and hearing are impaired and motor functions decline. At higher doses of indoles, the user may experience euphoria, fear, hostility and confusion. Anaesthetics cause confusion, distorted spatial awareness, aggression, trouble breathing and numbed nerves.

8.1.2 Fatigue

Fatigue has been shown to impair both cognitive and motor performance with an important adverse effect on alertness. Fatigue decreases the ability to process complex information such as that presented by unusual plant conditions. In addition, fatigue may increase reaction time, and impair recall and decision-making. As fatigue increases, performance is increasingly impaired and shows greater variability.

There are many factors that may cause fatigue. These include the amount of time spent working on a single task, sleep disorders and deprivation, and the effects of circadian rhythms or their disruption. For example, long periods of time performing a single physical task will cause muscles to become fatigued so that they are less easily controlled and errors are more likely.

Sleep disorders and sleep schedules that do not allow sufficient deep sleep will adversely affect cognitive and motor performance and, over time, individuals will accumulate a "sleep debt." That is, most working-age adults require about eight hours of sleep on a regular schedule to maintain optimum alertness, mood and performance levels. If sleep is ineffective or insufficient, impairments will be seen during the next waking period. If sleep is ineffective or insufficient for an extended period, the impairments will be cumulative.

Task performance and alertness are also affected by circadian rhythms. **Circadian rhythms** are also known as "biological clocks" and are patterns in physiological functioning over the course of a day. Sleepiness, for example, typically is at a peak between 3 a.m. and 5 a.m. with another increase occurring between 3 p.m. and 5 p.m. When an individual's daily schedule is changed by a change in shift schedule or travel to a different time zone, circadian rhythms are disrupted and performance decrements will occur until a new pattern is established.

8.1.3 Emotional Stress

Stress is an internal psychological and physiological response to threatening events or conditions that require unusual changes in behavior or adaptation. The amount of stress an individual experiences in any given context increases when the individual perceives that the demands of the situation are perceived as exceeding his or her capabilities to cope.

Because a stress response depends upon the individual's appraisal of his or her ability to cope with the situation, individuals will differ in the events and conditions that they experience as stressful. Common sources of potential emotional stress include interpersonal conflicts at home or on the job, grief and loss, unpredictability in one's personal or work life, and any events at home or at work that reduce self-esteem.

Stress may impair task performance in several ways. Personnel may become distracted and unable to focus on the task and so commit errors. Or, stress may cause a worker to become too focused on one aspect of a task to the exclusion of others or have difficulty determining when and how to act. Physiological stress responses may also reduce fine motor coordination. If stress persists over a long period of time, it can cause physical and mental illnesses.

Stress may also adversely affect team performance. Team members typically communicate less under stressful conditions and may fail to exchange information needed to succeed at a task. Or, team members may lose sight of team goals and focus instead on their personal goals and needs.

Experience with a stressor reduces the stress response. Successful past experiences in surviving stressful events and conditions increase an individual's confidence in his or her ability to cope, so that less stress is experienced when similar situations are encountered again.

8.1.4 Illness

Physical and mental illnesses may also cause errors. The effects of physical illness on cognitive and motor performance depend upon the nature of the illness itself. Most physical illnesses are accompanied by fatigue. Some may cause stress. Similarly, the effects of mental illnesses depend upon the nature of the illness and the extent to which symptoms are controllable (and are controlled) with medication.

8.1.5 Combinations of Factors

The effects on performance of combinations of these impairment-causing factors may be synergistic and they may also interact with other conditions in the workplace. For example, fatigue may increase the experience of emotional stress. Or, physical illness may reduce an individual's tolerance for environmental conditions, such as heat or noise.

8.2 DIRECT CAUSES OF FITNESS-FOR-DUTY-RELATED ERRORS

A direct cause of an error resulting from personnel impairment describes characteristics of the impairment that caused task performance to fail. There are a number of ways in which impairment may cause or contribute to an error. These include:

> Substance use – Personnel capabilities were reduced by the use of drugs or alcohol prior to or during working hours, resulting in errors.
>
> Excessive consecutive work hours – Personnel became fatigued because of working too many consecutive hours or working too long on the same task. As a result, for example, mental fatigue due to long hours performing a repetitious task without rest breaks caused

a momentary lapse in monitoring of indications with the result that a safety parameter was exceeded.

Inadequate rest – Excessive overtime with insufficient time off-duty created a "sleep debt." As a result, for example, personnel vigilance was reduced and changes to parameters were not detected.

Circadian rhythms – An individual's circadian rhythms were disrupted by scheduled changes, such as shift rotation or jet lag. Or, capabilities were reduced because task performance occurred during a natural "trough" in physiological functioning. As a result, for example, steps were performed incorrectly during a task because the worker did not recall the correct action sequence.

Emotional stress – Events or conditions in an individual's personal or work life affected the individual's task focus or motor coordination.

Illness – Worker capabilities to perform a task were reduced by the symptoms of physical or mental illness that were not controlled by medication. For example, judgment and decision making may be impaired, leading to errors.

Combination of impairments – Combinations of impairing factors reduced worker capabilities, leading to errors.

8.3 PROGRAMMATIC CAUSES OF FITNESS-FOR-DUTY ERRORS

Barriers to fitness-for-duty-related errors include licensee programs for the detection and prevention of potential or actual impairment, as well as the individual responsibility of workers to decline assignments if they are impaired for any reason. The latter barrier is a weak one, however, because humans are generally over-confident of their capabilities when under the influence of drugs or alcohol, or are stressed, fatigued or ill. Other factors that may discourage self-reporting include the fear of losing access authorization, an operating license or extra income from overtime. Licensee programs that may be implicated in errors caused by personnel impairment include:

Access Authorization – This program is responsible for assuring that individuals with access to special nuclear materials are reliable and trustworthy. Psychological examinations and background investigations are two of the techniques used. Weaknesses in this program may allow impaired individuals to have unescorted access to vital areas in a plant.

Fitness-for-Duty – Licensee fitness-for-duty programs are primarily responsible for detecting and preventing impaired personnel from performing tasks that may affect public health and safety. Medical evaluations of personnel, behavioral observation programs, employee assistance programs and drug and alcohol testing are used to detect impairment. Weaknesses in this program may allow impaired personnel to have access to vital areas in a plant where they could commit errors.

Operator Licensing – NRC requirements for obtaining and maintaining an operating license also include medical and psychological examinations to screen for potential health conditions. Weaknesses in this program may set the stage for health conditions to adversely affect an operator's ability to perform his or her tasks.

Overtime Policies and Practices – The NRC issued Generic Letter 82-12 that provides guidance for limiting work hours to reduce on-the-job fatigue and the potential consequences for task performance. Licensee Technical Specifications and administrative procedures also define work-hour limitations. Routine authorization for work hours in excess of those recommended may result in fatigued workers. Further, a practice of excluding training or meetings that occur outside of an individual's normal work schedule from work-hour limitations will also contribute to fatigue.

Shift Scheduling – Shift scheduling may also affect the likelihood that personnel will show performance decrements due to fatigue. A change in the assigned shift or a rotating shift schedule will disrupt circadian rhythms and may increase the likelihood of errors.

Safety Culture – The effectiveness of self-reporting and behavioral observation programs depends greatly upon the safety culture at a site. For example, if self-reporting of impairment or reporting an impairment concern about another staff member consistently results in disciplinary action, then supervisors and workers may be reluctant to report other staff members who appear to be impaired. On the other hand, if individuals who have come to work under some form of stress are treated fairly and with concern, personnel will report more frequently. If the licensee's culture emphasizes safety over other goals, personnel may be willing to turn down overtime and monitor their own fatigue levels, even if turning down the opportunity results in a loss of income.

8.4 ADDITIONAL RESOURCES ON FITNESS FOR DUTY

- *U.S. Code of Federal Regulations*, Part 11, Criteria and procedures for determining eligibility for access to or control over special nuclear material, Title 10, Energy (revised periodically). Washington, DC: U.S. Government Printing Office.

- *U.S. Code of Federal Regulations,* Part 26, Fitness for duty programs, Title 10, Energy (revised periodically). Washington, DC: U.S. Government Printing Office.

- *U.S. Code of Federal Regulations,* Part 55, Operators licenses, Title 10, Energy (revised periodically). Washington, DC: U.S. Government Printing Office.

- *U.S. Code of Federal Regulations,* Part 73, Physical protection of plants and materials, Title 10, Energy (revised periodically). Washington, DC: U.S. Government Printing Office.

- U.S. Nuclear Regulatory Commission (1982). *Nuclear power plant staff working hours* (Generic Letter 82-12). Washington, DC: U.S. Nuclear Regulatory Commission.

- U.S. Nuclear Regulatory Commission (1989). *Fitness for duty in the nuclear power industry: Responses to public comments* (NUREG-1354). Washington, DC: U.S. Nuclear Regulatory Commission.

- U.S. Nuclear Regulatory Commission (1989). *Fitness for duty in the nuclear power industry: Responses to implementation questions* (NUREG-1385). Washington, DC: U.S. Nuclear Regulatory Commission.

- U.S. Nuclear Regulatory Commission (1991). *Nuclear plant staff working hours* (Information Notice 91-36). Washington, DC: U.S. Nuclear Regulatory Commission.

- U.S. Nuclear Regulatory Commission (1998). *Medical evaluation of licensed personnel at nuclear power plants* (Regulatory Guide 1.134, Rev. 3). Washington, DC: U.S. Nuclear Regulatory Commission.

- Baker, T. (1995). *Alertness, performance and off-duty sleep on 8-hour and 12-hour night shifts in a simulated continuous operations control room setting* (NUREG/CR-6046). Washington, DC: U.S. Nuclear Regulatory Commission.

- Barnes, V.E., Fleming, I., Grant, T., Hauth, J., Hendrickson, I., Kono, B., Moore, C., Olson, J. Saari, L., Toquam, J., Wieringa, D., Yost, P., Hendrickson,P., Moon, D and Scott, W. (1988). *Fitness for duty in the nuclear power industry: A review of technical issues* (NUREG/CR-5227). Washington, DC: U.S. Nuclear Regulatory Commission.

- Durbin, N., Moore, C. Grant, T., Fleming, T., Hunt, P., Martin, R. Murphy, S., Hauth, J. Wilson, R., Bittner, A., Bramwell, A., Macauley, J., Olson, J., Terrill, E. and Toquam, J. (1991). *Fitness for duty in the nuclear power industry: A review of the first year of program performance and an update of the technical issues* (NUREG/CR-5784, PNL-7795, BHARC-700/91/025). Washington, DC: U.S. Nuclear Regulatory Commission.

- Durbin, N. and Grant, T. (1996). *Fitness for duty in the nuclear industry: Update of the technical issues 1996* (NUREG/CR-6470, BSRC-700/96/004, PNNL-11134). Washington, DC: U.S. Nuclear Regulatory Commission.

- Moore, C., Barnes, V., Hauth, J., Wilson, R., Fawcett-Long, J., Toquam, J., Baker, K., Wieringa, D., Olson, J., & Christensen, J. (1989). *Fitness for duty in the nuclear power industry: A review of technical issues* (NUREG/CR-5227, Supplement 1, PNL-6652, BHARC-700/88/018). Washington, DC: U.S. Nuclear Regulatory Commission.

9 KNOWLEDGE, SKILLS AND ABILITIES

9.1 KNOWLEDGE, SKILLS AND ABILITIES IN HUMAN PERFORMANCE

Many of the job positions at licensee sites require extensive and specialized KSAs for correct task performance. **Knowledge** is a set of facts, factual information, a method of analysis or the application of methods and facts to successfully perform a task. A **skill** is a motor or mental capability such as the ability to open a valve or operate a controller. **Ability** is the combination of knowledge and skills required to perform a task. **Mastery** is the process of achieving the requisite KSAs to perform a job or task safely and competently.

A KSA deficiency is one of the more frequently identified causes for human error. There are four basic ways in which an error may occur as a result of KSA deficiencies. These are:

- The worker did not receive training and so did not master the requisite KSA(s)
- The worker was trained, but the training did not result in KSA mastery
- The worker was trained and mastered the KSA, but did not retain it over time
- The worker mastered the requisite KSA, but did not apply it to the task.

The potential risk impacts of personnel performing tasks without the requisite KSAs are the basis for NRC and industry efforts to improve training programs. Not all KSA errors are caused by training deficiencies, however. As will be discussed below, a mental lapse or a momentary loss of situational awareness may also cause KSA-related errors. In addition, for some jobs, a certain level of proficiency is expected when personnel are hired into the position or the services of contractors are obtained. In these cases, human resources screening and selection processes or procurement processes for contractor services may play a role in preventing KSA errors.

9.1.1 Systems Approach to Training

Licensee training programs are presently conducted in accordance with the principles of the **systems approach to training** (SAT), which is also called **performance-based training** (PBT). The NRC assures that training is conducted in accordance with 10 CFR 50.120, "Training and Qualification of Nuclear Power Plant Personnel" and 10 CFR 55.4, "Operators Licenses (Definitions)." The systems approach to training means that a training program includes the following five elements:

- Systematic analysis of the jobs to be performed
- Learning objectives derived from the analysis, which describe desired performance after training
- Training design and implementation based on the learning objectives
- Evaluation of trainee mastery of the objectives during training
- Evaluation and revision of the training based on the performance of trained personnel in the job setting.

As noted in the Statements of Consideration for the 1987 amendment to 10 CFR 55.4, a licensee's training program is considered NRC-approved when it is accredited by the National Nuclear Accrediting Board.

There are currently nine licensee training programs subject to accreditation, as follows:

1. Licensed and non-licensed operators
2. Shift supervisor
3. Shift technical advisor
4. Instrument and control technician
5. Electrical maintenance personnel
6. Mechanical maintenance personnel
7. Radiological protection technician
8. Chemistry technician
9. Engineering support personnel

These training programs identify the required KSAs to successfully function in a job. A job is defined by a set of tasks to be mastered by the worker. These tasks are analyzed to identify the KSAs they require. The KSAs are then consolidated into a master taxonomy of KSAs for each job. Learning objectives for training are prepared from the taxonomies. Mastery of the learning objectives equates to mastery of the KSAs and a successful training program assures that each worker is qualified to perform the various tasks that comprise his or her job.

Performance-based training programs were implemented and first accredited during the late 1980s. Most nuclear power plant personnel have been trained under these programs.

9.1.2 Identifying KSAs with Job and Task Analysis

Job and task analysis (JTA) is a systematic method for identifying the KSAs that are required for successful performance of the tasks associated with a job. The JTA is used to identify the tasks for which training is necessary and may be used to identify requirements for personnel screening and selection.

Tasks are analyzed in the JTA based upon their importance, frequency and difficulty.

- An important task is one that is critical to successful job performance. For example, the operator actions that are modeled in plant probabilistic risk assessments are important, so training for mastery is required.
- An infrequently performed task is one that may not be performed often enough for personnel to maintain mastery.
- A difficult task is one that is complex. For example, the task may involve multiple decisions based upon dynamic plant states.

The KSAs required for these tasks are affected by the quality of the procedures that are available and the characteristics of the **human-system interface** (HSI). For example, if controls are easily manipulated and displays easy to understand, then the operator may not need to master a large

body of detailed information to operate the system. Similarly, if the procedures for a task are clearly written and easily understood, then the worker might not need to memorize the exact sequence of actions required to repair a particular component, because the procedure steps will guide the worker through the task.

Changes to equipment, the HSI and the as-written procedures may require an update to the JTA. When equipment design or procedures are changed, training program personnel will reassess the adequacy of the existing KSAs to determine if additional training is required, or whether current training should be revised or deleted. Revisions to existing training programs and new training may also be required as operating experience provides lessons learned. Personnel screening and selection criteria or contractor requirements may also be impacted.

9.1.3 Training

Training to master the KSAs required for a job may be obtained from a variety of sources. Whether the licensee provides the training or it is obtained from other sources (e.g., trade schools, universities, contractor organizations), there are several factors that may result in personnel not mastering the required KSAs for a job. These include course design and delivery methods, course completion, and training frequency.

Course design begins when the learning objectives have been identified. The design process consists of determining the delivery methods (e.g., classroom, simulator, on-the-job training), number of hours required to cover the materials, instructor qualifications and so on. Although some methods, materials and instructors may be more effective or efficient than others, the important issue is that the course content is complete and addresses all of the relevant KSAs, so that the learning objectives are met and the KSAs mastered.

Another determinant of KSA mastery is course completion. Although this factor appears obvious, there are often competing demands on personnel that may pull them out of training at times. As a result, they may miss the instruction related to specific KSAs. Testing may not identify the KSA deficiency because it is impossible to test mastery of all KSAs. Sampling techniques are used to generate examinations. If attendance and participation are not controlled, some personnel may miss training on specific KSAs and testing may not identify the deficiencies before an error is committed.

9.1.4 Testing

Testing is the primary means used to evaluate KSA mastery. In order to assure that personnel are competent to perform their jobs, the testing requirements should be valid for the job. There are three kinds of validity that are important for a mastery test:

- Content validity – the test items are directly related to job performance by ensuring they match the learning objectives and are appropriately weighted
- Operational validity – the test items address the mental and psychomotor activities that are performed on the job

- Discriminate validity – the test items differentiate between workers who have mastered KSAs required to perform the job and those who have not.

Most training programs do not require perfect performance on test items for all KSAs to demonstrate mastery of the subject. As an example, a score of 80% on most components of the test is required in the operator licensing examination process. A score of 100% is not required, in part, because the validity and reliability of test items vary.

The examination process should identify critical tasks, however. For operators, critical tasks are those actions that are so important to safety that a competent operator is expected to correctly perform these tasks every time to demonstrate mastery. Critical tasks typically form a small subset of the overall group of tasks to be mastered for any job. Emphasis on critical tasks and their associated KSAs in training and testing is important to reduce the likelihood of error.

9.1.5 Proficiency Training

Another factor affecting KSA mastery is forgetting. An individual's ability to perform a task will degrade over time unless the relevant KSAs are refreshed. Proficiency training (i.e., refresher) will be required for some tasks to maintain the level of mastery that was demonstrated following initial training. One function of training programs is to identify those tasks that require proficiency training.

If certain tasks are performed frequently, proficiency training may be unnecessary. By performing a task, personnel practice the task and obtain feedback regarding successful task mastery. Task performance refreshes the KSAs and successful task performance verifies that proficiency has been maintained.

"Just-in-time" training may be used for infrequently performed and difficult tasks. "Just-in-time" training techniques may include a comprehensive pre-job briefing, practice runs on a mock-up or a simulator familiarization session. Determination of the periodicity required to refresh KSAs is part of the design of the training and requalification program, although actual "just-in-time" training may be triggered and administered by a different process, such as work planning and control.

9.1.6 Training Evaluation and Revision

An important aspect of a performance-based training system is the constant evaluation and revision of the training program. This mechanism assures that changes in plant configuration, equipment modifications, procedural changes and lessons learned from operating experience are included in learning objectives and addressed in training program design. An effective training program is dynamic as the plant organization changes and learns. If the training program ceases to capture changes in the plant and industry, training will not provide the necessary KSAs to assure successful task performance.

9.1.7 Cognitive Errors: Loss of Situational Awareness and Mental Lapses

Two fundamental sources of human error that are not associated with KSA mastery are a loss of situational awareness and a mental lapse. A loss of situational awareness or a mental lapse occurs when personnel have previously demonstrated mastery of a KSA but cannot recall it at the required time to prevent an error. An example would be failure to trip a pump when pressure reached a certain value. If the operator did not recognize that pressure had reached that value, the problem was caused by a loss of situational awareness. If the operator recognized that pressure had reached the pump trip criterion but still did not trip the pump, the problem would be a mental lapse. In each case, if the operator had been directly asked when he or she needed to trip the pump, the operator would have correctly responded, "when pressure reached the trip criterion."

9.1.7.1 Loss of Situational Awareness

Loss of situational awareness occurs when a worker does not recognize that a certain KSA applies to the task that he or she is performing. The worker has mastered the KSA and, if asked in a different setting, would be able to demonstrate this mastery. There are four elements required for a finding of a loss of situational awareness:

1. The KSA was essential for satisfactory task performance
2. The individual received training to adequately complete the task
3. The individual mastered the KSA required for task performance
4. The individual did not recognize that the KSA was applicable to the task.

There are several methods available to prevent the likelihood of errors due to a loss of situational awareness. Situational awareness can be improved through "just-in-time training" that focuses on "what-if" scenarios for events that are pre-planned. This allows the individual to think through the various situations that may be encountered during the work activity. Emphasizing rule-based precautions during training may also be helpful (e.g., "Always check Tech Specs whenever any component is declared inoperable"), but will not prevent all losses of situational awareness. Placing the staff member into the situation in which a KSA will be applied, such as a simulator, is also useful in preventing a loss of situational awareness. However, there are so many potential event paths in a nuclear power plant that it is unlikely that simulator-based training can address every possible situation.

The most effective corrective actions to enhance situational awareness for unplanned events are to ensure that prompts or reminders are included in job performance aids. This type of support may include:

- Adding notes or cautions to procedures
- Adding annunciators and alarms that call attention to equipment conditions
- Eliminating or conditionally suppressing unnecessary annunciators that may overwhelm operators during events
- Improving the human-system interface.

9.1.7.2 Mental Lapse

Another source of error is the **mental lapse**, or a momentary lapse in recall for the correct KSA when it is required. Lapses may be random, or may be related to performance shaping factors, such as fatigue, environmental conditions or stress. Often, the lapse occurs because the individual becomes distracted or unfocused. For example, an individual may have been working through one procedure when the task was interrupted by the need to implement a higher priority procedure. The staff member may have intended to complete the initial procedure, but was distracted by the other, higher priority activities and did not remember to return to the first procedure.

Mental lapses are identified when the following four conditions are met:

1. The KSA was essential for satisfactory task performance
2. The individual received training to adequately complete the task
3. The individual previously demonstrated mastery of the KSA(s) required to complete the task
4. The individual did not recall the KSA(s) when required.

Although training programs cannot prevent mental lapses, personnel can be trained to recognize the warning signs of conditions that may increase the likelihood of a lapse and use various strategies to minimize their occurrence. These strategies may include self-checking programs or stress management techniques.

Reducing or eliminating the performance-shaping factors that momentarily distract or overload cognitive processes may also reduce the likelihood of mental lapses. Corrective actions to minimize or eliminate the performance-shaping factors that caused a lapse will be more effective than remedial training on the KSA, given that the individual has already mastered it.

9.1.8 Personnel Selection and Contracting

Licensees often hire new staff, promote staff to new positions, or augment the existing staff with contractor personnel. Personnel selection processes identify the best-qualified individual for a job using several different methods, which typically include an evaluation of previous job experience, education and training. Personality, ability and proficiency tests may also be administered. These methods are intended to ensure that new hires and the staff who are promoted either possess the KSAs required for the job or have the ability to benefit from training for the job. Procurement processes specify the qualifications that contractor personnel are required to have, although licensees may also provide site-specific training to contractor personnel. Weaknesses in the personnel selection and procurement processes may result in work being performed by individuals who have not mastered the necessary KSAs for the task and so lead to errors.

9.2 DIRECT CAUSES OF KSA-RELATED ERRORS

A direct cause of a KSA error describes the reason that the requisite KSA was not applied to task performance. The direct cause of the error may be:

No KSA – The worker did not possess the KSA required for successful task performance. For example, certain skills were required to use a particular type of self-contained breathing apparatus (SCBA) but the worker did not possess those skills. As a result, the individual was exposed to airborne contamination because the SCBA did not fit properly.

Inadequate mastery - The individual had not mastered the KSA. In this case, the individual had received some form of training, but it was inadequate. For example, a maintenance technician was required to review a new revision to a procedure on her own time. She completed the review, but when it was time to use the procedure, she found that certain steps in the procedure did not make sense to her and she was unable to follow it. As a result, she took incorrect actions.

Inadequate retention – The individual had mastered the KSA but had forgotten how to perform important components of the task, and so, for example, performed steps out of sequence.

Loss of situational awareness - The individual had mastered the KSA but did not recognize the KSA applied to the current situation and so committed an error. For example, a unit supervisor had mastered knowledge regarding the conditions under which it is necessary to post a fire watch, but failed to recognize that a fire watch was required for a particular welding job. As a result, sparks from the welding task caused a small fire.

Mental lapse – The individual had mastered the KSA but failed to recall it and so did not apply it to performing the task. For example, a security guard became distracted by an incident that was being discussed over the radio and so failed to check that a door was securely locked.

9.3 PROGRAMMATIC CAUSES OF KSA-RELATED ERRORS

The training program is responsible for assuring that personnel master the necessary KSAs to perform their tasks. NUREG-1220, Training Review Criteria and Procedures, provides detailed review criteria for assessing training program effectiveness. Several key training program weaknesses are also described here. In addition, other licensee programs or processes that may cause or contribute to KSA-related errors are also listed.

9.3.1 Training Program Weaknesses

Job and Task Analysis – The JTA did not identify and characterize all of the important KSAs for a job position. As a result, training did not address them and workers were not prepared to perform some tasks correctly. For example, operators violated Technical

Specifications because they had not been trained to understand their applicability to the current situation.

Training Design and Delivery – Training was provided but the design and delivery did not assure KSA mastery. For example, the course content may not have addressed all of the important KSAs for the job, course delivery methods may have been inappropriate for the KSA (e.g., classroom lectures to teach a skill with no opportunity to practice), or the instructors were not qualified to teach the course.

Training Completion – Student attendance and participation were not managed. As a result, an individual or group of workers missed instruction related to important KSAs, did not master them and could not perform the task correctly when required.

Testing – KSA mastery was not evaluated or testing was invalid. As a result, students who had not mastered important KSAs were not detected and so were allowed to perform tasks for which they were not qualified.

Frequency – Proficiency training was not provided or was not provided with sufficient frequency. As a result, KSA mastery degraded and personnel could no longer perform some tasks correctly.

Evaluation and Revision – Lessons learned related to training weaknesses were not communicated or tracked and so training was not revised to address them. Or, changes in plant equipment, work practices and requirements did not result in training revisions. As a result, some staff's KSAs were incomplete or inaccurate.

9.3.2 Other Programmatic Weaknesses

Human Resources – Personnel selection processes did not ensure that new hires or newly promoted individuals had mastered the KSAs required for the job. As a result, some staff did not possess the KSAs to perform effectively.

Procurement – Licensee processes for bringing contractor personnel on-site did not assure that the contractors had mastered the KSAs required for the job.

Work Planning and Control – The work planning and control process did not assign qualified individuals to the task. As a result, personnel who had not mastered the KSAs required performed a task and committed errors.

Shift Staffing – An inadequate number of qualified personnel were assigned to each shift. As a result, planned work could not be executed or unplanned conditions or events could not be managed.

Human Factors Engineering – Procedures, equipment labeling, and human-system interfaces were inadequate to assist personnel in maintaining situational awareness. As a result, workers were unable to complete a repair task because the combination of

inadequate training with poor procedures and labeling prevented them from locating the component on which the task was to be performed.

Industrial Hygiene and Radiation Protection – Weaknesses in these programs may result in workers performing tasks under environmental conditions that promote errors. For example, excessive noise distracted staff from performing their tasks, leading to a mental lapse.

9.4 ADDITIONAL RESOURCES ON KSAs AND TRAINING

- *U.S. Code of Federal Regulations,* Part 50.120, Training and qualification of nuclear power plant personnel, Title 10, Energy (revised periodically). Washington, DC: U.S. Government Printing Office.

- *U.S. Code of Federal Regulations,* Part 55.4, Operators licenses (definitions), Title 10, Energy (revised periodically). Washington, DC: U.S. Government Printing Office.

- U.S. Nuclear Regulatory Commission (2000). *Qualification and training of personnel for nuclear power plants* (Regulatory Guide 1.8, Rev. 3). Washington, DC: U.S. Nuclear Regulatory Commission.

- U.S. Nuclear Regulatory Commission (1999). *Operator licensing examination standards for power reactors* (NUREG-1021). Washington, DC: U.S. Nuclear Regulatory Commission.

- U.S. Nuclear Regulatory Commission (1998). *Knowledge and abilities catalog for nuclear power plant operators: Pressurized water reactors* (NUREG-1122, Rev. 2). Washington, DC: U.S. Nuclear Regulatory Commission.

- U.S. Nuclear Regulatory Commission (1998). *Knowledge and abilities catalog for nuclear power plant operators: Boiling water reactors* (NUREG-1123, Rev. 2). Washington, DC: U.S. Nuclear Regulatory Commission.

- U.S. Nuclear Regulatory Commission (1996). *Nuclear power plant simulation facilities for use in operator license examinations* (Regulatory Guide 1.149, Rev. 2). Washington, DC: U.S. Nuclear Regulatory Commission.

- U.S. Nuclear Regulatory Commission (1993). *Training review criteria and procedures* (NUREG-1220, Rev.1). Washington, DC: U.S. Nuclear Regulatory Commission.

10 ATTENTION AND MOTIVATON

10.1 ATTENTION AND MOTIVATION IN HUMAN PERFORMANCE

Attention and motivation are often identified as causes for error. "Inattention to detail" and "complacency," for example, are frequently cited as causal factors in licensee problem reports. The evidence supporting these conclusions is often weak, however.

Determining the role of attention or motivation in a human error is difficult outside of a laboratory or simulator setting. Attention and motivation are internal states that cannot be measured directly. In the laboratory, the experimenter can use sensitive instruments to track eye movements and record focus times as measures of attention, for example, or can establish control over the incentives presented to subjects to manipulate motivation levels. Recordings of workers "thinking aloud" as they perform tasks also provide insights into attention and motivation. In an investigation, however, real-time, objective measures of attention or motivation cannot be obtained because the investigation necessarily occurs after the fact. As a result, the investigator must rely on self-reports and inference, which are subject to the biases and inaccuracies discussed in Section 3.

Attributing causality to workers' attention, attitudes, motivations or traits may be common because it is consistent with the "fundamental attribution error." As mentioned in Section 3, this "error" is a natural human tendency in how we explain another's behavior and appears to be "hard-wired" into the human perceptual system. In the absence of compelling evidence that some characteristic of the work environment affected the workers' actions, investigators may resort to this "default" explanation and conclude that the workers were not paying attention or lacked the motivation to perform their work correctly. In reviewing a licensee problem report that cites attention and motivation as causal factors, it may be necessary for NRC inspectors to carefully assess the evidence provided to ensure that it supports the conclusions.

10.1.1 Attention

The term, "**cognition**," refers to how people attend to and process information in making decisions and performing tasks. A useful description of the cognitive processes involved in task performance can be found in NUREG/CR-6126, "Cognitive Skill Training for Nuclear Power Plant Operational Decision Making," and is summarized here.

The information processing required for task performance can be broken down into four stages. These are (1) detection and monitoring, (2) situation assessment, (3) planning, and (4) execution.

In the detection and monitoring stage, the individual seeks out information that is relevant to the task, such as reading gauges, or receives it from signals and cues in the environment that draw attention to salient information, such as alarms activating. The information that is sought is determined by the individual's knowledge of what information is needed or by procedures and

other task demands. The signals and cues provided by the environment may be relevant to the task, such as alarms, or irrelevant, such as a thunderclap.

Numerous errors are possible at this first processing stage. For example, an individual may only seek some information and ignore other relevant information. Or, the worker may be distracted and fail to monitor important indications. Or, there may be too many signals received from the environment at one time and the individual misses important information.

In the situation assessment stage, the individual uses the information gathered from detection and monitoring and his or her knowledge to develop a coherent explanation of the information received. This explanation is formed into a **mental representation** of plant state, in the case of operators, or equipment status, for maintenance or instrumentation and control technicians. This mental representation is used to generate expectations about other plant or equipment parameters, expectations about future consequences, and explanations of what has been observed, as well as to identify unusual conditions and anticipate potential problems.

Errors during the situation assessment stage arise due to inaccuracies in the mental representation that is formed. For example, the representation may be incomplete, if relevant information was not detected during the initial stage. Or, the information received may be interpreted incorrectly. Or, the knowledge that is incorporated into the representation may be incomplete or inaccurate. In some cases, a situation may be too complex for an operator to be able to form an accurate mental representation.

In the response planning stage, the individual chooses a course of action based upon the situation assessment. Response planning involves establishing goals, generating an action plan, monitoring the effectiveness of the plan in achieving the goals, filling in gaps in the plan and adapting it as the situation changes or feedback is received on its effectiveness.

Errors may also occur during any of the response-planning activities. For example, the goals that are established may be incorrect because the situation assessment was inaccurate. The procedure selected for use may be the wrong one for the situation. Or, unexpected events may occur that are not detected, so the plan is not corrected.

Finally, in the execution phase, plans are implemented to achieve the task goals. Plan execution will typically require prioritization of actions, and the allocation of personnel resources and coordination, whenever more than one individual is involved in the task. During the execution phase, the achievement of subgoals is monitored and adjustments may be required.

Errors also occur during plan execution. For example, an individual may forget to take a required action or fail to detect and correct an error that is made.

A key contributor to information-processing errors is the limited capacity of working memory. Long-term memory, where knowledge is stored, is virtually unlimited. But research has shown that working memory can hold and manipulate only about seven items at one time. As a result, information that exceeds working memory capacity may be displaced or lost.

Another contributor to information-processing errors is habit. When a behavior has been practiced or executed many times, it becomes automatic. That is, the need to pay attention to executing the behavior and to exert conscious control over actions is reduced. The benefit of habits is that they reduce the burden on working memory. The disadvantage is that a habit may intrude on performing a new or different task where the habitual behavior is unwanted.

10.1.2 Motivation

Work motivation has been defined as "the conditions responsible for variations in the intensity, quality, and direction of ongoing behavior." Intensity refers to how hard personnel work and how productively work hours are used. Quality refers to both the manner in which work is performed (e.g., safely, conscientiously) and the extent to which work products meet expectations. The direction of work behavior is determined by the values, needs and expectations that personnel bring to the job and the individual's interpretation of the organization's values, reward structures and the goals that are communicated.

Personnel generally require more than a paycheck from their jobs to sustain motivation. Other job characteristics, such as opportunities to maintain and enhance self-esteem, to meet social needs and to grow professionally, have also been shown to be important. In fact, the highest levels of work motivation are found when the organization's and individual's values, needs, expectations and goals are congruent, so that the organization fosters the individual's ability to meet personal needs and goals on the job.

It is important to note, however, that high levels of motivation do not always translate into error-free performance. There are many prerequisites that must be met in a work environment before motivation has much effect. For example, motivation to perform a task correctly is of little value without the knowledge of how to do it. Motivation to perform work safely will not ensure safe performance if the potential risks associated with the work activity and methods to minimize or avoid them are not known. Motivation to perform work in accordance with procedures will be stymied if the procedures for a task are out-of-date, do not apply to current plant status, or cannot be used in the work environment. Motivation to use the required **personal protective equipment** (PPE) or tools and equipment for a job will not ensure safe performance if the necessary PPE, tools and equipment are not available. A key issue for NRC inspectors who are reviewing an investigation in which motivation has been cited as a cause, then, is to rule out other causes for error that may have made worker motivation irrelevant.

One way in which high levels of motivation may reduce errors is that motivated personnel may be more likely to take responsibility for bringing attention to any barriers to correct task performance that they encounter and to fixing those that are within their span of control. But, if the problems identified are not within the workers' span of control and are not addressed by the organization, high levels of motivation may also lead personnel to develop workarounds to get work done despite the barriers. Or, motivation may be decreased and workers become disaffected, if concerns and problems are repeatedly raised but not addressed.

An important source of motivational errors is in defining the goals to be accomplished in task performance. Supervision plays a key role in establishing and communicating the goals to be

met in a work activity. Section 14 discusses the effects of supervisory direction, oversight and leadership on motivation.

Peers may also influence motivation. Crosschecking may detect and correct errors that occur. Peer group norms as they apply to work intensity and quality may also affect individual motivation. Behavior-based safety programs include peer observation and feedback to reduce unsafe acts, although these programs are controversial because of their perceived emphasis on "fixing the worker" rather than "fixing the work environment."

10.2 DIRECT CAUSES OF ATTENTION AND MOTIVATION ERRORS

A direct cause of an attention and motivation error describes the characteristics of a worker's internal state that caused or contributed to an error. Specific examples of errors that may be due to attention and motivation are presented below.

10.2.1 Detection and Monitoring

Information not detected – Task-relevant information was available, but it was not detected. For example, a conversation between an operator and a security guard distracted the operator on her rounds and she failed to detect that a pipe was leaking.

Information discounted – Task-relevant information was available, but it was ignored or interpreted incorrectly. For example, an operator may mentally adjust a reading from an instrument that typically reads high, when the instrument was recently re-calibrated and is reading correctly.

Information lost – Task-relevant information was detected, but was not recalled when needed. For example, an operator may have taken a reading on an instrument, but did not write it down, and so did not remember the earlier reading when he or she checked it again, and failed to detect a trend.

10.2.2 Situation Assessment

Assessment incomplete – Errors were committed because the situation was assessed incompletely due, for example, to incomplete information or the inability to interpret and analyze the information available because of time constraints. As a result, for example, the crew did not recognize that they had entered a Limiting Condition for Operation.

Assessment inaccurate – Errors were committed because the situation assessment was incorrect. The information on which the assessment was based may have been inaccurate, for example, or personnel may have misinterpreted the information received. Or, personnel may not have possessed the knowledge required to assess the situation accurately (refer to Section 9, Knowledge, Skills and Abilities).

10.2.3 Response Planning

Plan incorrect – Errors were committed because, for example, the plan was incomplete or could not be implemented as intended under current plant conditions. For example, workers assigned to a preventative maintenance task were unable to complete it because a control room operator recognized that taking the component out of service would have conflicted with other plant activities.

Plan not modified – Errors occurred because circumstances changed and the plan was no longer appropriate for the circumstances. For example, a construction task could not be completed when an electrical conduit that was not on the drawings was discovered.

10.2.4 Execution

Slip – An error occurred because an unintended action was taken. For example, a technician placed a switch in the OFF position when he had intended to place it in AUTO.

Lapse – An error occurred because the required action was momentarily lost from working memory. As a result, the action was not performed or was performed incorrectly.

Intrusion – An error occurred because an overlearned sequence of actions was performed without conscious control and the habit was inappropriate for the circumstances. For example, personnel risked exposure to hazardous fumes when they followed their usual path to the break room, which required them to pass through a locked door. When they unlocked the door, the fumes reminded them that the room they were about to enter was the site of a recent chemical spill that had not yet been contained.

10.2.5 Motivation

Expectations – Management expectations regarding productivity, quality workmanship and safety were not effectively communicated to personnel and examples of the desired behaviors were not provided. As a result, personnel may have been confused or misinterpreted expectations so that their decisions and actions deviated from what was desired.

Reward structure – The desired behaviors with regard to productivity, quality workmanship and safety were not appropriately rewarded. As a result, individuals' motivation to perform to expectations was decreased, leading to errors.

Feedback – Personnel did not raise concerns or identify barriers to effective performance with the result that errors occurred. Concerns were not raised, for example, due to a perception that nothing would be done to correct the problems or that personnel would be punished for raising concerns.

Workarounds – Concerns were raised and barriers to effective performance were identified, but not corrected. As a result, personnel developed unauthorized and unanalyzed work practices to accomplish tasks and the workarounds resulted in errors. Or, management authorized the workaround because a repair would be too expensive, leading to errors.

Peers – Errors were committed because crosschecking was not performed or peer influence adversely affected productivity, quality workmanship or safety behavior. For example, a staff member who consistently wore hearing protection where required was ridiculed by other staff for doing so.

10.3 PROGRAMMATIC CAUSES OF ATTENTION AND MOTIVATION ERRORS

Many licensee programs, policies and practices are intended to reduce errors associated with attention and motivation. Some programs directly focus on these potential causes and contributors to error, such as the **human factors engineering** program at a site or a behavior-based safety program. Others may indirectly affect attention and motivation during task performance. Licensee programs that may be implicated in errors caused by attention or motivation include:

Human Factors Engineering – Weaknesses in the design of human-system interfaces, for example, may make it difficult for personnel to detect changes in important parameters or to interpret the information displayed correctly. Difficult-to-use human-system interfaces also may frustrate personnel and inadvertently communicate a management message that accurate, timely human performance is not important.

Procedures – Accurate, accessible and usable procedures also play an important role in directing attention, assisting in the development of an accurate situation assessment and in developing and executing response plans. For example, the entry conditions to operating procedures assist personnel to assess the situation accurately. If entry conditions and prerequisites are not provided, personnel are more likely to miss relevant information about the situation and execute an incorrect response plan.

Training – Because knowledge guides information processing at every stage, weaknesses in the training program may have a key effect on the likelihood of attention-related errors. A programmatic weakness in ensuring proficiency training, for example, may prevent personnel from maintaining mastery of the knowledge required to develop an accurate situation assessment or develop effective response plans for tasks that are infrequently performed.

Human Resources – Personnel selection processes play a role in ensuring that staff is qualified (i.e., possess the KSAs required for the job). Weaknesses in the personnel job performance evaluation and reward systems also may fail to communicate management expectations or may reward behavior that does not meets those expectations. If

disciplinary actions are not perceived as being administered lawfully and fairly, employee motivation to work productively and safely may be reduced.

Supervision – Supervision communicates and reinforces management expectations and establishes goals and requirements for task performance. Supervisory oversight may increase motivation to perform in accordance with expectations as well as detect and correct any errors that occur. Weaknesses in supervision, for example, may cause staff to choose production over safety goals in their work or to tolerate workarounds that may lead to errors.

Problem Identification/Resolution – Licensee programs for reporting, documenting and resolving barriers to effective performance maintain staff motivation levels when problem reports result in elimination or mitigation of the barriers. Weaknesses in these programs may not only frustrate personnel, but also encourage the development of workarounds that may lead to errors.

Employee Concerns – Employee concerns programs provide another avenue for personnel to raise safety issues. Weaknesses in the employee concerns program will discourage personnel from raising problems when they fear adverse consequences and will call stated management expectations into question, resulting in lower compliance.

Behavioral Safety – Behavioral safety programs focus on identifying and correcting work behaviors that may result in adverse consequences through behavioral observation and feedback from supervisors and peers. Some programs also emphasize self-checking, such as the Institute for Nuclear Power Operations' STAR program (stop-think-act-review). Focusing on potentially unsafe acts appears to improve human performance at some sites.

10.4 ADDITIONAL RESOURCES ON ATTENTION AND MOTIVATION

- *U.S. Code of Federal Regulations,* Part 19.20, Employee protection, Title 10, Energy (revised periodically). Washington, DC: U.S. Government Printing Office.

- Mumaw, R.J. (1994). *The effects of stress on nuclear power plant operational decision making and training approaches to reduce stress effects* (NUREG/CR-6127). Washington, DC: U.S. Nuclear Regulatory Commission.

- Mumaw, R., Swatzler, D., Roth, E. and Thomas, W. (1994). *Cognitive Skill Training for Nuclear Power Plant Operational Decision Making* (NUREG/CR-6126). Washington, D.C.: U.S. Nuclear Regulatory Commission.

- Roth, E., Mumaw, R. and Lewis, P. (1994). *An Empirical Investigation of Operator Performance in Cognitively Demanding Simulated Emergencies* (NUREG/CR-6208). Washington, D.C.: U.S. Nuclear Regulatory Commission.

- Woods, D., Pople, H.E. and Roth, E.M. (1990). The Cognitive Environment Simulation as a Tool for Modeling Human Performance and Reliability (NUREG/CR-5213, Vols. 1 and 2). Washington DC: U.S. Nuclear Regulatory Commission.

11 PROCEDURES

11.1 PROCEDURE-RELATED ERRORS AND THEIR CAUSES

Procedures are instructions for performing a task. The instructions may be provided in formal written procedures or as hand-written information included in a work package. Procedure-related errors are errors that occur because some characteristic of the procedure caused task performance to fail.

The primary purpose of procedures is to ensure that tasks are performed correctly. Procedures also can document the best way to perform a task, so work is performed more efficiently. Procedures may also serve a record-keeping function to document when and how a task was performed.

Procedures reduce the likelihood of human errors under several conditions. When a task is complex or performed infrequently, even the most experienced workers may forget the steps required or the order in which certain steps must be performed. Procedures can also fill gaps in a worker's knowledge about a task, component or system. Procedures are particularly helpful when plant systems are in an unusual configuration and routine actions that may normally be performed without a procedure can result in adverse consequences.

For procedures to be effective in ensuring that tasks are performed correctly, they must be used. There are a number of reasons that workers may not use procedures:

- Procedures are inaccurate
- Procedures are out of date
- No procedure has been written for the task
- Users cannot find the procedure they want to use
- Users don't need a procedure because the task is simple
- Users need more information than the procedures contain
- Users see procedures as an affront to their skill
- Procedures are difficult to use in the work environment
- Procedures are difficult to understand.

It is important to note that using a procedure introduces an additional task to the work being performed. Using a procedure in a step-by-step manner, and checking off each step as it is performed, may ensure that tasks are performed deliberately and correctly. However, there are many circumstances in a plant in which the physical demands of using a procedure in this way complicates the job and can contribute to the likelihood of errors rather than reducing them. Using a procedure also increases mental demands by requiring that the users read the procedure, comprehend it and then act on what they have understood. When this read-comprehend-act loop is added to the primary tasks that operators must perform during upset conditions (e.g., monitoring and detection, situation assessment, response planning and response implementation), it is particularly important that the procedures are easy to understand and use.

The list of reasons for not using procedures also points out some of the ways in which errors can occur when they are used. For example, if a procedure contains inaccurate instructions or a drawing is out-of-date because a system or component has been modified since the document was written, personnel who use the procedure may take incorrect actions. Or, if a procedure step is written in an ambiguous and confusing manner, workers may try to follow it, but take incorrect actions because they misinterpret a step.

Human performance problems are often erroneously attributed to procedures or a failure to follow procedures. Procedures are frequently identified as a cause for human performance problems because they describe the standards and requirements for task performance, and when task performance fails, there is likely some procedure or policy that appears to have been violated. It may not be the case, however, that an attribute of the procedure, or the lack of a procedure, or the failure to use a procedure or reference document caused the error. Rather, what appears to be a failure to follow the procedure may be a symptom of another underlying cause, such as a training need or inadequate labeling, rather than the result of the procedure's characteristics. It is important, therefore, that the licensee provides evidence linking the human error specifically to characteristics of the document or weaknesses in how it was used when identifying a procedure-related error.

11.2 DIRECT CAUSES OF PROCEDURE-RELATED ERRORS

A direct cause of a procedure-related error describes characteristics of the procedures that caused task performance to fail or how the procedure was used or not used that caused task performance to fail. There are a number of ways in which procedures may cause, contribute to or fail to prevent an error. These include:

11.2.1 No Procedure Used

No procedure - Task performance failed because no procedure was written for the task and the workers' reliance on memory or "skill of the craft" resulted in, for example, forgetting important steps, performing steps out of sequence or taking incorrect actions.

Procedure not available - A procedure for the task existed, but was not used and should have been. For example, a procedure may not be available for a task because it was not included in the work package or the workers were not aware that the document existed and so did not find and use it.

Procedure inconvenient to use - Task performance failed because using a procedure was difficult in the work environment. For example, procedure use may be inconvenient in confined spaces, in contamination zones or when wearing protective equipment.

Procedure too difficult to use - Task performance failed because workers considered the procedure too difficult to use and so did not use it. For example, workers may avoid using procedures that are written in excessive detail or that include what they consider to be unnecessary steps that interfere with performing the task. Or, a procedure may be

written with too little detail for the knowledge levels of the workers, so that they do not understand the procedure or misinterpret it.

Procedure use not required - Task performance failed because an existing procedure was not used. For example, licensee policy may have required that the procedure be reviewed before use or that it be available at the work site, but did not require that the procedure be in-hand and followed step-by-step during task performance.

11.2.2 Wrong Procedure Used

Wrong unit, train, component - Task performance failed because the procedure was not intended for use with the equipment that was being operated or maintained. The wrong procedure may be included in the work package or workers may select the wrong document for use. Or, a procedure may not clearly indicate the equipment to which it applies. In some cases, the wrong procedure may be used because labeling is deficient and the workers cannot verify that the procedure applies.

Wrong revision - Task performance failed because the most recent revision to the procedure was not used. If modifications were made to equipment, but the affected documents were not updated, incorrect instructions in the procedure may cause an error. Or, workers may inadvertently access and use an earlier revision.

Wrong procedure for plant/equipment state - Task performance failed because prerequisites for using the procedure were not met by current equipment or system configuration.

11.2.3 Procedure Used, But Wrong or Incomplete

Typographical error - An error was made because information presented in the procedure was incorrect due to a typographical error. For example, the numbers or letters in equipment identifiers, such as valve names, or required values for instrument readings may be transposed or incomplete.

Facts incorrect - Task performance failed because the instructions or the information presented in procedure steps was incorrect. For example, the procedure may include improper set points or describe actions that cannot be taken under normal conditions of use.

Incomplete - Task performance failed because facts or useful information were omitted from the procedure. For example, the procedure writer may have assumed that workers would know the steps required to prepare for conducting a maintenance activity and so did not include them in the procedure. Or, important cautionary information about how to perform a step was not included in the procedure.

Sequence wrong - Task performance failed because the sequence in which the steps were presented in the procedure was incorrect.

Second checker needed, but absent - Task performance failed because the task was important enough to warrant independent verification that the objective of a task or series of actions was achieved, but verification was not required. As a result, errors were committed during task performance, but not detected and corrected.

No placekeeping - Task performance failed because the procedure did not provide a method for placekeeping. Sign-off spaces next to critical steps or other methods for assisting the user to track progress through the procedure were not used. Omitting a procedure step is the most common consequence of not providing placekeeping aids.

11.2.4 Procedure Used, But Followed Incorrectly

Format confusing - The layout of procedure elements on the page was confusing to workers. For example, cautions or notes were not separated from action steps and highlighted with distinctive formatting. Or, the relationship of steps to substeps or lists was unclear because no indenting was used.

Content confusing - The information presented in the procedure or reference document was confusing to workers. For example, the abbreviations or acronyms used were unfamiliar to the users. Or, short, simple action steps in the imperative voice were not used. Conditional statements (i.e., logic steps used to present decision points in procedures) can be particularly confusing if formal Boolean logic statements are not used. Cross-references to other procedures, to reference documents or to other steps within the same procedure may be confusing and can cause workers to lose track of the sequence in which they are to perform steps.

Graphics confusing - Graphics used in the procedures were confusing to workers. Tables or figures were difficult to read and understand. Or, too many emphasis techniques were used in the procedure text so that unimportant information was highlighted, while important information was not.

11.3 PROGRAMMATIC CAUSES OF PROCEDURE-RELATED ERRORS

Programmatic causes of procedure-related errors are typically found in the licensee's processes for managing the development, use and control of procedures. A number of good practices have been identified to assure that procedures will be effective in preventing errors, many of which are documented in NRC guidance for emergency operating procedures programs. Other programs may also contribute to procedure-related errors.

11.3.1 Procedures Program

The following weaknesses in procedures programs have been shown to result in ineffective procedures:

Multidisciplinary team not used - Development of technically accurate and usable procedures is enhanced by the involvement of a multidisciplinary team. Procedure development teams should include specially trained procedure writers working with

subject matter experts, such as a representative of the intended users and engineers with specific expertise regarding the equipment to be operated or maintained. A single procedure writer working alone may miss important technical information, may use terminology that is unfamiliar to the intended users, or sequence the procedure steps inefficiently. As a result, the procedure may be inaccurate or difficult to comprehend, increasing the likelihood of errors.

Writer's guide - Writers' guides provide information to procedure writers regarding techniques for formatting procedures, presenting different types of content (e.g., action and decision steps) and for developing usable graphics. If a writer's guide is not followed or it is incomplete, the resulting procedures may be difficult to comprehend and follow.

Verification - Procedure verification is a process that provides a final check on the technical accuracy of the procedure steps and on the procedure's compliance with writers' guide requirements. In most plants, an individual who was not involved in authoring the procedure typically verifies that the procedure correctly incorporates information from the technical basis documents and meets the writer's guide requirements. Verification may also involve walking down the procedure at the work site to ensure that equipment identifiers in the procedure match the labels and tags on the equipment, that the procedure can be used under the expected conditions at the work site, that the steps are sequenced correctly and efficiently considering the layout of the worksite, and that the tools list is complete. Procedures that have not been verified are often incomplete, inaccurate and difficult to use.

Validation - Procedure validation is a process to check that the procedure can be used as written. Validation exercises in a control room simulator with crews of operators may be used to validate operating procedures. Maintenance simulators or mock-ups may be used to validate maintenance procedures. Procedures that have not been validated may result in unintended consequences or may not be usable under actual work conditions.

Review and approval - The procedure review and approval process ensures that personnel in all other departments whose work may be affected by the procedure have the opportunity to review it to assure that activities in their departments are not adversely affected. Review and approval should also assure that any other procedures affected by the procedure are identified and modified, if necessary. Out-dated cross-references between procedures are a common source of error. Management reviews of procedures or procedure revisions will ensure that the procedure is consistent with management goals and policies.

Procedure revisions - The procedure program should include a process for reviewing and revising procedures when changes occur at the plant that may affect the technical accuracy or usability of the procedures. For example, if plant equipment is modified, the procedures and drawings that apply to the equipment may require revision. Or, if the knowledge and skills of the workforce change due to new hires, layoffs, an aging and retiring workforce, then the level of detail in the procedures may need to be increased to

better accommodate the new users. Changes in management goals and policies may also require procedures to be revised to ensure they are consistent with new directives. And, if other documents change that are referenced in the procedure, the procedure should be reviewed to determine whether any revisions are required.

11.3.2 Other Programmatic Weaknesses

Training – Coordination between the training and procedures programs is necessary to ensure that user training needs are assessed for a new or revised procedure. Changes to existing training may be necessary to ensure that the users are, at a minimum, familiar with the new or revised procedure and are qualified to use it before the procedure is implemented. Weaknesses in training on a new or revised procedure may

Operating Experience – Lessons learned from users' experiences with the procedures is necessary to ensure that any problems or limitations in procedures are detected and corrected. If operating experience does not lead to timely procedure revisions, personnel may avoid using the procedures or develop workarounds.

Information Management - Technically accurate procedures depend on the availability of up-to-date reference documents, such as vendor manuals, engineering analyses, and drawings. If the reference documents used to develop procedures are incomplete or contain errors, those omissions and errors may be translated into the procedures. A document control process is also necessary to ensure that workers have access to a complete and the most recent revision of the procedure.

Maintenance – Procedures are written on the basis of assumptions about the operability and condition of the equipment to which they apply. If the equipment has not been maintained and is inoperable or in a degraded condition, errors may occur if the procedure is not revised to reflect actual equipment conditions.

11.4 ADDITIONAL RESOURCES ON PROCEDURES

- *U.S. Code of Federal Regulations,* Appendix B to Part 50, *Quality assurance criteria for nuclear power plants and fuel reprocessing plants*, Criterion V, Instructions, procedures and drawings, Title 10, Energy (revised periodically). Washington, DC: U.S. Government Printing Office.

- U.S. Nuclear Regulatory Commission (1978). *Quality assurance program requirements (Operation)* (Regulatory Guide 1.33, Rev. 2). Washington, DC: U.S. Nuclear Regulatory Commission.

- U.S. Nuclear Regulatory Commission (1982). *Guidelines for the preparation of emergency operating procedures* (NUREG-0899). Washington, DC: U.S. Nuclear Regulatory Commission.

- U.S. Nuclear Regulatory Commission (1989). *Lessons learned from the special inspection program for emergency operating procedures* (NUREG-1358). Washington, DC: U.S. Nuclear Regulatory Commission.

- O'Hara, J.M., Higgins, J.C., Stubler, W.F. and Kramer, J. (2000). *Computer-based procedure systems: Technical basis and human factors review guidance* (NUREG/CR-6634). Washington, DC: U.S. Nuclear Regulatory Commission.

- Barnes, V.E., Moore, C.J. Wieringa, D.R., Isakson, C.S., Kono, B.K. and Gruel, R.L. (1989). *Techniques for preparing flowchart-format emergency operating procedures: Vol.s 1 and 2* (NUREG/CR-5228, PNL-6653, BHARC-700/88/017). Washington, DC: U.S. Nuclear Regulatory Commission.

- Morgenstern, M., Barnes, V., McGuire, M., Radford, L. and Wheeler, W. (1985) *Operating procedures in nuclear power plants: Practices and problems* (NUREG/CR-3968, PNL-5648). Washington, DC: U.S. Nuclear Regulatory Commission.

- Morgenstern, M., Barnes, V., Radford, L., Wheeler, W. and Badalamente, R. (1984). *The development, use and control of maintenance procedures in nuclear power plants: Problems and recommendations* (NUREG/CR-3817, PNL-5121). Washington, DC: U.S. Nuclear Regulatory Commission.

12 TOOLS AND EQUIPMENT

12.1 EFFECTS OF TOOLS AND EQUIPMENT ON HUMAN PERFORMANCE

The design and use of tools, equipment and **personal protective equipment** (PPE) in the workplace are typically considered industrial safety and health issues. But, tools, equipment or PPE may impact risk if they cause or allow personnel to make errors that may affect safety systems.

12.1.1 Tool Design and Use

Tool use is often necessary for work activities at licensee sites. Numerous checklists containing evaluation criteria for tools have been published as a result of increased public concern over workplace injuries, particularly those resulting from repetitive motion (e.g., carpal tunnel syndrome). In general, any tool characteristic that increases the risk of worker injuries will also increase the risk of errors during task performance.

The proper tools for a task depend upon the characteristics of the workplace, the individual workers and the task demands. For example, in confined areas, tools must be small enough to be usable in the workspace available while retaining their functionality. Errors may result if tools do not fit a user's hand size or handedness (i.e., use of a right-handed tool by a left-handed worker), skill levels or strength. Errors are also more likely if the task requires the use of force or repetitive motion in using the tool.

Poorly designed tools, tools that are inappropriate for the workplace, worker or task, or tools that are not maintained may affect human performance in several ways. The primary effect of poorly designed tools is on motor performance. Poorly designed tools may be dropped, cause physical slips and erroneous actions, or lead to fatigued or injured muscles that are more difficult to control. Some tools may interfere with visibility or increase discomfort and cause workers to rush through jobs. Tools that are not maintained will not function as intended and may cause errors when they are used.

12.1.2 Equipment

The use of various types of equipment and machinery necessary to perform some work activities may also cause or contribute to errors. Equipment may be temporary or permanently staged at a worksite. Ladders, scaffolds or lifts may be used for aboveground work. Cranes, trucks, forklifts, loaders, or robots, for example, may be brought to a worksite for some tasks. Some tasks require the temporary deployment of additional lighting, parts, and the electrical cabling to energize necessary machinery. The introduction of equipment and machinery to a worksite may complicate task performance and represents a change. Equipment and machinery may also affect task performance if personnel expect it to be available and it is not, such as a missing ladder that was pre-staged for emergency operations but was removed and used for other purposes.

Aboveground work is particularly hazardous and may have adverse effects on some workers. For example, personnel may experience dizziness, instability or vertigo when working at heights.

These responses may be intensified if the surface on which they are standing moves. Work at any height also introduces the potential for tools and other materials to be dropped, which may damage equipment or personnel below, or create foreign material issues.

Extensive regulations and guidance have been published by the Occupational Safety and Health Administration and other government agencies regarding the safe work practices and design characteristics of equipment that prevent worker injuries and other workplace hazards. In general, the practices and equipment designs necessary to prevent injuries also serve to prevent errors that may impact safe operations.

12.1.3 Personal Protective Equipment

Personal protective equipment is necessary to perform many tasks at licensee sites. Depending upon the type of hazard to which workers may be exposed, PPE may include eye, hand, ear and foot protection, aprons or full suits, such as anti-contamination clothing. Protection from heat stress and cold may be necessary at times, as well as respiratory protection or protection from open flames for hot work. Aboveground work may require safety harnesses.

The design and use of PPE may cause or contribute to errors in several ways. The most important concerns are that PPE may reduce sensory input, limit feedback and impair motor capabilities. For example, darkly tinted safety glasses may hinder vision if used indoors. Gloves reduce fine motor control. Hearing protection may prevent personnel from hearing alarms or verbal communications. Personnel may become entangled in fall protection gear. Some forms of protective clothing may contribute to heat stress, which may affect both cognitive and motor functioning, leading to errors. Combinations of PPE may interact and interfere with performance. Wearing PPE is also often uncomfortable and may distract workers or cause them to hurry through tasks, increasing the potential for errors.

Personal protective equipment that is not maintained properly may also lead to errors. For example, safety glasses and face shields that have become scratched distort or interfere with vision. In general, the use of PPE is the least preferred alternative for protecting workers because of the impacts on performance most types of PPE will have.

12.2 DIRECT CAUSES OF ERRORS RELATED TO TOOLS AND EQUIPMENT

A direct cause of an error related to tools and equipment describes the characteristics of the tools or equipment that caused task performance to fail. There are a number of ways in which the design and use of tools and equipment may impair performance. Examples of these are presented below.

12.2.1 Tools

Tool mismatched to task environment – The tool used for the task was too large, too small or otherwise inappropriate for the work environment. It may have obscured the parts or equipment on which work was being performed, causing errors, or created discomfort.

Tool mismatched to worker – The tool was too large, too small or inappropriate for the worker's physical characteristics, such as hand-size, strength or agility. Some tools require skills to be used. If a worker has not been trained to use the tool or the tool is mismatched to the individual's characteristics, he or she may commit errors by using it improperly, break equipment or become injured.

Tool poorly designed - Poorly designed tools may increase discomfort. Tools that are uncomfortable to use may cause personnel to rush through a task and commit errors. Tools that are poorly designed may also impair motor control and cause errors, such as breaking equipment or applying excessive torque on a screw.

Tool degraded - Tools that are not maintained may not function as intended or in accordance with the workers' expectations. Miscalibrated or broken tools may cause personnel to take incorrect actions or may damage other equipment.

Correct tools not available or used - When special tools have been designed for performing a task, an administrative challenge is created to ensure that they are available at the worksite when needed. If other tools are substituted for the special tool, task performance may be delayed by the workaround or it may not be possible to accomplish the task to specifications.

12.2.2 Equipment

Deployment wrong – Errors occurred because the equipment or machinery was deployed incorrectly. For example, the ground underneath a ladder or scaffolding was uneven, angled or could not support the weight. Or, machinery was deployed too near electrical power lines, possibly resulting in an electrical, or too near overhead obstructions, possibly causing damage to other equipment or injuries to personnel.

Design or construction wrong – Errors occurred because the equipment or machinery was poorly designed or constructed. For example, toeboards were not provided on platforms erected in areas where dropping tools or material could cause harm. Or, the scaffolding materials used were insufficiently sturdy for the weight placed on them.

Used improperly – The equipment or machinery was used in a manner for which it was not designed or not authorized. For example, a load contained too much weight or a crane was used to lift personnel without following proper procedures, increasing the likelihood of equipment damage or injuries.

Not available - Equipment or machinery required to perform a task was not available when needed. Errors may occur if task performance is delayed while personnel search for the required equipment and if other equipment or machinery is substituted for the missing equipment.

12.2.3 Personal Protective Equipment (PPE)

Mismatched to task – Task performance failed because the design or use of the PPE made it more difficult than necessary. For example, work was performed in a high temperature environment with multiple layers of anti-contamination clothing and other PPE, resulting in cognitive impairment due to heat stress. Or, the use of tinted safety glasses indoors impaired vision and prevented a worker from correctly reading a tag.

Mismatched to worker – Task performance failed because ill-fitting PPE caused discomfort and interfered with task performance. For example, gloves that were too large further reduced fine motor control and tactile feedback, leading to errors. Workers were uncomfortable and rushed through tasks, with the result that post-maintenance testing was not completed.

Poorly designed – Task performance failed because required PPE was poorly designed and so was ineffective, allowing workers to be exposed to hazards that cause errors. For example, a poorly designed respirator may allow a worker to be overcome by caustic fumes.

Not used – Task performance failed because PPE was not used when required, with the result that personnel were exposed to hazards that caused injuries and errors. For example, an instrumentation and control technician received an electrical shock, which also destroyed some wiring in the electrical panel.

Not available – Task performance failed because PPE was not available when required. As a result, personnel were unable to complete a surveillance timely and Technical Specifications were violated. Or, respirators were not readily available for emergency use and workers were unable to enter an area to respond.

Used incorrectly – Task performance failed because personnel used the incorrect PPE for a task or used PPE incorrectly. For example, a worker allowed his safety glasses to slide down the bridge of his nose and spilled a caustic chemical when fluid splashed into his eyes.

Degraded – Task performance failed because PPE was not maintained and failed to protect workers from hazards. For example, a degraded respirator allowed an uptake.

Combined – Task performance failed because combinations of PPE were required for a task and interacted to interfere with performance. For example, safety glasses worn under a face shield distorted vision, causing errors.

12.3 PROGRAMMATIC CAUSES FOR ERRORS RELATED TO TOOLS AND EQUIPMENT

Programmatic causes of errors related to tools and equipment are typically found in the licensee's procurement processes, and industrial hygiene, radiation protection and

maintenance programs. Other programs may also be implicated. Common programmatic causes of errors related to tools and equipment include:

Work Planning and Control - Work planning and control processes may fail to identify the tools and equipment needed at the work site. For example, working in a high temperature environment with multiple layers of anti-contamination clothing and other PPE, without assuring adequate body cooling or personnel rotation, may cause cognitive impairment due to heat stress.

Procurement – The licensee's procurement program ensures that the tools, equipment or PPE that are required to perform a work activity have been purchased and meet specifications. For mobile equipment that may be brought to the site, such as cranes, the procurement program is also typically responsible for ensuring that contractor equipment meets requirements and that contractor personnel are qualified to operate the equipment. Weaknesses in the procurement program may lead to the use of inappropriate, uncomfortable or ineffective tools, equipment or PPE.

Industrial Hygiene and Radiation Protection – These licensee programs are responsible for ensuring that the hazards associated with a work activity have been identified, communicated to the workers, and that proper hazard controls are implemented. These programs are also typically responsible for ensuring that PPE is fitted to individual workers. Weaknesses in these programs may not only result in the unnecessary exposure of workers to hazards, but may also set the stage for errors.

Procedures - As part of the licensee's procedure development process, the tools, equipment and PPE required for a work activity should be considered when designing the procedures and defining how they will be used. For example, effective procedures are designed so that their use is compatible with the use of tools, equipment and PPE. Procedures that do not specify the tools, equipment and PPE required to perform a task may cause delays or errors if incorrect tools and equipment are used.

Training – Personnel often need specialized training to use some types of tools, equipment and PPE. If these training needs have not been met, workers may use incorrect tools, equipment or PPE or use them improperly, resulting in errors.

Human Factors Engineering – Requirements for special tools, equipment and PPE should be considered whenever new equipment or systems are installed. As a general rule, engineering controls for hazards are more effective than PPE. The need for special tools or equipment creates an administrative burden and can often be avoided if the potential impacts on human performance are considered during the design stage. Reducing the need for special tools, equipment and PPE reduces opportunities for delays and errors in task performance.

Operating Experience - Reviews of relevant operating experiences from the plant and other facilities with similar work activities may reveal problems associated with tools and equipment as well as solutions to those problems. Weaknesses in the operating experience

program may Personnel may have reported problems with tools and equipment that previously interfered with performance, and further issues may be avoided if the problems are corrected.

Maintenance – Maintenance of tools, equipment and PPE is necessary to ensure that they are in working condition when needed. Inadequate maintenance will allow tools, equipment and PPE to degrade so that they are difficult to use, ineffective or cannot be used.

12.4 ADDITIONAL RESOURCES ON TOOLS AND EQUIPMENT

- U.S. Nuclear Regulatory Commission (1988). *Memorandum of understanding between NRC and OSHA relating to NRC-licensed facilities* (Information Notice 88-100). Washington, DC: U.S. Nuclear Regulatory Commission.

- U.S. Nuclear Regulatory Commission (1998). *Potential for degradation of the emergency core cooling system and the containment spray system after a loss-of-coolant accident because of construction and protective coating deficiencies and foreign material containment* (Generic Letter 98-04). Washington, DC: U.S. Nuclear Regulatory Commission.

- U.S. Nuclear Regulatory Commission (1999). *Acceptable programs for respiratory protection* (Regulatory Guide 8.15, Rev. 1). Washington, DC: U.S. Nuclear Regulatory Commission.

- U.S. Nuclear Regulatory Commission (1996). *Human-system interface design review guideline* (NUREG-0700, Rev. 1, Vol.s 1-3). Washington, DC: U.S. Nuclear Regulatory Commission.

13 STAFFING

13.1 EFFECTS OF STAFFING ON HUMAN PERFORMANCE

Staffing is the process of accessing, maintaining and scheduling personnel resources to accomplish work. An adequately staffed organization ensures that personnel are available with the proper qualifications for both planned and foreseeable unplanned activities. Staffing is a dynamic process in which plant management monitors personnel performance to ensure that overall organizational performance goals are met or exceeded. The result of an effective staffing process is a balance between personnel costs and the achievement of broader organizational goals.

13.1.1 Staffing Requirements

The NRC has established several regulations regarding the staffing of nuclear power plants. Title 10 CFR 50.54(m) establishes the regulatory minimum crew composition for licensed operators. Title 10 CFR 50 Appendix R establishes the requirements for a Fire Brigade. NUREG 0737, "Clarification of TMI Action Plan Requirements," sets the requirement for a Shift Technical Advisor (STA). Each licensee has further established requirements in Technical Specifications or Site Licensee Commitments for a minimum level of shift staffing as well as a general description of the site organization. The regulatory requirements are often lower than the licensee's administrative requirements for minimum shift staffing levels.

NRC Information Notices 91-77 (Shift Staffing at Nuclear Power Plants) and 95-48 (Results of Shift Staffing Study) both stated in part:

> "The number of staff on each shift is expected to be sufficient to accomplish all necessary actions to ensure a safe shutdown of the reactor following an event. Those actions include implementing emergency operating procedures, performing required notifications, establishing and maintaining communications with the NRC and plant management, and any additional duties assigned by the licensee's administrative controls...."

13.1.2 Staffing Decision-Making

Personnel costs comprise a significant proportion of an organization's operating budget. Managing staff size to manage costs is a necessity for any business. There are a number of issues to be addressed when staffing decisions are made. These include the range of expertise required, the number of personnel needed, and the anticipated workload, so that the necessary staff and expertise are available when needed.

13.1.2.1 Range of Expertise

Each organization requires the proper amount and type of expertise to safely and competently operate the plant under a variety of conditions. The term "expertise" includes the attributes of

talent, effectiveness, knowledge, skills, abilities and experience necessary to operate and maintain plant systems, structures and components.

Organizations balance the costs of maintaining full-time expertise on staff with the probability that the expertise can be obtained from outside the organization when the need arises. For example, it may be cost-effective to hire three junior engineers in a discipline for the same costs as two senior engineers, if the normal engineering workload requires three full-time staff. However, complex issues may occasionally arise that junior staff cannot resolve effectively. A lack of access to the expertise of senior personnel could increase the workload, costs, or the likelihood of human errors if, for example, a corrective action developed by junior staff was not the optimum approach.

Another factor that may impact access to expertise is the aging workforce in the nuclear power industry. Many of the individuals who were involved in plant construction and start-up activities are reaching retirement age. As they leave the workforce, these individuals often take with them extensive and irretrievable information about the design, construction, operation and maintenance of the specific systems and components with which they worked over the years. Efforts to document their knowledge and extended turnovers to the junior staff may capture some of the knowledge they have accumulated. It has been the case at times, however, that the knowledge was simply lost, with the result that errors have occurred as junior staff "learn the ropes."

13.1.2.2 Staff Size

The number of individuals who are available to support planned and unplanned activities is a key staffing issue. Organizations must ensure that adequate numbers of personnel are available to accomplish on-going work activities timely and to address the unplanned activities, or plant events, that may occur. On the other hand, too many staff may hamper performance on some tasks. Manpower planning and analyses ensure that the staff size supports human performance.

Surges in workload, such as outages at nuclear power plants, typically require staff augmentation as well as longer work hours for permanent staff. The introduction of contractor personnel or licensee personnel from other sites may increase the likelihood of errors due to unfamiliarity with the plant, its procedures and hardware, for example. Longer work hours have the potential to increase fatigue, which also contributes to the likelihood of error.

A key consideration in establishing the shift schedule is the staff size and composition that would be required to respond to an event during the period in which the Emergency Response Organization is recalled. This period generally lasts for the first hour of the event due to activation and personnel transit time to the site, especially on the back shift. The occurrence of an event typically involves a substantial increase in workload. Insufficient staff to meet the increased demands will exacerbate the **stress** naturally experienced by personnel on-shift at the time an event occurs and increase the potential for errors, as discussed below.

Workload may also be increased by organizational changes. For example, in order to reduce costs, some organizations reorganize and re-assign job responsibilities. Others may implement a local or across-the-board hiring freeze and attractive early retirement packages, to reduce staff

size through attrition. In the absence of careful planning and workload analysis, these efforts to reduce personnel costs may result in an increase in human performance problems. Morale may suffer if personnel are "required to do more with less" and are unable to complete their assigned work on schedule. Or, staff may feel constant pressure to "do more" and so take shortcuts or rush through their tasks, leading to errors. Personnel may find themselves working longer hours over the long-term, which may result in increased fatigue and an increase in the likelihood of errors. And, if the potential loss of expertise associated with buy-out packages for senior staff is not considered, errors may increase as junior staff members assume new responsibilities.

Maintaining a larger staff or assigning more staff to a task does not always improve performance. Organizations can become "bloated" and develop inefficient, bureaucratic work methods if the number of personnel available is greater than the workload. In addition, the assignment of multiple staff to a task may increase task complexity by increasing the amount of communication and coordination required among personnel. For example, some maintenance tasks may require expertise in both mechanical and electrical maintenance. If two specialists are used to perform the task, it is likely that they will need to communicate about the work and coordinate their activities. These ancillary tasks of coordinating and communicating introduce increased opportunities for error. One individual who is qualified in both specialties may be able to perform the task more effectively.

13.1.3 Task Overload

The primary consequence of inadequate shift staffing is **task overload**. Task overload exists when the number of tasks that must be accomplished in a given period of time exceeds the available personnel resources. There are various work management strategies for responding to task overload including:

- task prioritization and deferral or slippage
- increasing the work pace
- task delegation.

These strategies may lead to errors in some circumstances. For example, tasks may be inappropriately deferred so that systems or components are unavailable when needed. Increasing the work pace may lead to shortcuts or errors due to rushing. Task delegation may result in tasks being performed by individuals who do not have the expertise to perform them correctly. Task overload may increase stress, leading to errors.

13.2 DIRECT CAUSES OF STAFFING-RELATED ERRORS

A direct cause of a staffing-related error describes the characteristics of staffing practices that caused or contributed to the error. Examples of direct causes for staffing-related errors are presented below.

> Expertise Not Available – The correct mix of qualified personnel was not available on staff to perform the work. For example, a lack of available expertise resulted in delaying

task performance until a qualified person could be called in, or the task was assigned to a less qualified person who committed an error.

Insufficient Staff Available – Task performance failed because adequate numbers of personnel were not available to perform the work. As a result, work management strategies were employed and the level of stress increased, leading to errors.

Too Many Staff – Task performance failed because too many workers were assigned to the job. As a result, communication and coordination burdens were increased, which increased the opportunity for errors.

13.3 PROGRAMMATIC CAUSES FOR STAFFING-RELATED ERRORS

Programmatic causes of errors related to staffing are typically found in the licensee's business planning and work scheduling programs. Other programs may also be implicated. Common programmatic causes of errors related to staffing include:

Human Resources – Most licensees develop some form of a business plan that defines organizational goals and objectives. Business plans are often used to estimate the resources required to achieve the goals and run the business. Business plans may be used to determine staffing levels for the various parts of the corporate organization, sometimes without manpower planning and analyses of anticipated workload levels. As a result, there may be insufficient staff or staff may not have the required expertise.

Work Planning and Control - The work planning and control system is often used as an integrated scheduling tool to match the workers to support specific jobs. Weaknesses in the work planning and control system may result in the assignment of too few or too many personnel for a job or fail to ensure that only qualified personnel are assigned.

Shift Staffing - All licensees establish a shift staffing policy that defines the minimum required levels of shift personnel. This policy is often integrated with the scheduling of individuals to shifts and overtime management. If these policies are not clearly defined, the lack of clarity can cause staffing deficits that set the stage for human errors.

Training – The training program ensures that personnel are qualified for their jobs and that managers are trained to implement shift staffing and overtime policies. Sometimes, these policies may be difficult to understand. Weaknesses in the training program may fail to assure that supervisory personnel understand staffing requirements, for example.

Human Factors Engineering – The human factors engineering program ensures that the number of personnel required and the expertise they will need are considered whenever new equipment or systems are installed. Weaknesses in this program may result in too few or too many personnel assigned to a job or in the installation of systems that staff cannot operate with their existing KSAs.

13.4 ADDITIONAL RESOURCES ON STAFFING

- *U.S. Code of Federal Regulations,* Part 50.54(m), Conditions of licenses, Title 10, Energy (revised periodically). Washington, DC: U.S. Government Printing Office.

- *U.S. Code of Federal Regulations,* Appendix R to Part 50, *Quality assurance criteria for nuclear power plants and fuel reprocessing plants,* Criterion III (H), Fire brigade, Title 10, Energy (revised periodically). Washington, DC: U.S. Government Printing Office.

- U.S. Nuclear Regulatory Commission (1995). *Results of shift staffing study* (Information Notice 95-48). Washington, DC: U.S. Nuclear Regulatory Commission.

- U.S. Nuclear Regulatory Commission (1991). *Shift staffing at nuclear power plants* (Information Notice 91-77). Washington, DC: U.S. Nuclear Regulatory Commission.

- U.S. Nuclear Regulatory Commission (1983). *NUREG-0737 technical specifications* (Generic Letter 83-02). Washington, DC: U.S. Nuclear Regulatory Commission.

- U.S. Nuclear Regulatory Commission (1983). *Clarification of TMI action plan requirements* (NUREG-0737, Supplement 1). Washington, DC: U.S. Nuclear Regulatory Commission.

- U.S. Nuclear Regulatory Commission (1982). *NUREG-0737 technical specifications* (Generic Letter 82-16). Washington, DC: U.S. Nuclear Regulatory Commission.

- U.S. Nuclear Regulatory Commission (1981). *Standard review plan,* (NUREG-0800), Chapter 13, Conduct of operations, Sections 13.1.1-13.1.3. Washington, DC: U.S. Nuclear Regulatory Commission.

- U.S. Nuclear Regulatory Commission (1980). *TMI action plan* (NUREG-0737). Washington, DC: U.S. Nuclear Regulatory Commission.

- Hallbert, B.P., Sebok, A. and Morisseau, D. (2000). *A study of control room staffing levels for advanced reactors* (NUREG/IA-0137). Washington, DC: U.S. Nuclear Regulatory Commission.

14 SUPERVISION

14.1 SUPERVISION AND HUMAN PERFORMANCE

Supervision is the process by which work is directed and overseen by first-line management. Successful supervision requires a combination of leadership skills and technical competence. Supervision differs from peer checking or quality control because a supervisor has line management responsibility for the worker(s) as well as responsibility for the work activity.

Supervision is more than the moment-to-moment direction of a work activity. Successful supervision requires the assessment and shaping of worker attitudes and motivation, communication and implementation of management expectations for performing work, the assignment of the best-qualified workers to various tasks, as well as the technical competence to identify incorrect actions and stop improper activities before an error is committed. Effective supervision involves directing the work, overseeing how it is performed and leadership.

14.1.1 Direction

Directing work activities includes defining desired outcomes, planning, organizing and controlling work, and problem solving. Direction occurs during preparation for a task and during task performance.

The role of supervision during work preparation is to assure that the personnel who will be performing the task have the information and resources required to perform effectively. These resources include knowledge of the goal(s) of the work activity as well as management expectations for how the work is to be performed. Goals and expectations are often communicated during pre-job walkthroughs of the task environment and in pre-job briefings. Supervisors may also be required to ensure that the personnel assigned to perform the task are qualified, that the necessary tools and equipment are available, and that procedures and other instructions for performing the task, such as those included in a work package, are complete and understood by the workers. Supervisors may be responsible for verifying that the prerequisite conditions for tagging equipment out-of-service are met before the work begins and for obtaining authorization to start the task.

Supervisors act as a resource during performance of the work activity. Workers may call on them to answer questions, provide instructions in ambiguous or unanticipated situations and problem-solve. Supervisors also are the interface between the work group performing the task and other parts of the organization, including more senior management. Interface responsibilities may include requesting additional resources to complete the task, obtaining authorization to change the work plan or stopping work if unexpected conditions arise.
Personnel generally respond well to a supervisor when they have confidence in his or her technical background. Conversely, a supervisor with inadequate technical qualifications can foster resentment and degrade team performance because the supervisor cannot fulfill some of his or her responsibilities to the team. A first-line supervisor who is not technically competent may direct the work incorrectly.

Errors due to poor supervisory direction may arise when any of the supervisor's responsibilities for directing the work are not met. For example, on a task that will be repeated several times on different components, a supervisor may decide that a walkthrough and the pre-job briefing need only be done once before the task is performed the first time. If the same task is performed over several weeks or days, system configurations may change between jobs or the personnel who are on-shift and assigned to perform the work may change. Without the walkthrough and briefing before the task is performed each time, personnel may commit errors because they are unaware of changed plant conditions or newly assigned personnel may not have a full understanding of the task requirements.

14.1.2 Oversight

In addition to directing work activities, first-line supervisors typically are responsible for overseeing performance of the work. Supervisory oversight entails monitoring the work activity to ensure it is performed in accordance with the work plan, procedures and management expectations.

Effective supervisors are technically qualified to independently detect and correct errors, with the same or a superior level of technical knowledge as the worker performing the task. Although this is not always possible, it is important for high risk, complex activities. The best supervisor for a particular task is not always a higher-level manager who may be less familiar with the details of the task. A worker who was recently promoted to the ranks of first-line supervisors may provide more effective oversight if he or she has recent technical knowledge of the activity and has mastered the necessary supervisory skills.

The supervisor may or may not participate in the work assignment, but if he or she participates, the ability to concurrently provide oversight may be momentarily lost or reduced. The key element of supervisory oversight is that it provides a "second pair of eyes" not involved in the work activity that can detect errors and act promptly to correct them.

14.1.3 Leadership

Leadership involves motivating personnel, building trust, maintaining accountability and empowering action. As the first level of line management, the supervisor plays a key role in establishing and maintaining the work group's norms, values and safety culture. In addition, the supervisor's leadership style will affect the team's performance.

Supervisors translate and apply general organizational goals and management expectations to the specific activities of the work group. This process occurs both overtly, with explicit communications about goals and expectations, as well as indirectly. Goals and expectations, for example, may be communicated indirectly by the example the supervisor sets with his or her work behavior, such as the extent to which he or she takes short-cuts when performing tasks. Expectations may also be indirectly communicated through tacit behaviors, such as a failure to correct worker actions that achieve production goals while circumventing safe work practices. Supervisors also communicate goals and enforce management expectations through the worker behaviors that they reward with recommendations for promotions, merit raises and/or bonuses, desirable work assignments, training opportunities and overtime allocations, and even with such

subtle rewards as individual attention for some subordinates. Supervisors may overtly or covertly discourage a questioning attitude among workers, for example, by not taking time to fully answer questions during meetings, or, at an extreme, by ridiculing staff members who raise questions and concerns.

In addition to communicating organizational goals and management expectations, the supervisor's leadership style affects team performance. The research literature shows that leadership styles generally range from participative, with a focus on establishing and maintaining good interpersonal relations, to authoritarian and task-focused. The most effective leadership style in a given work situation depends upon the characteristics of the work situation and of the team members.

A participative leadership style is effective when team members are experienced, the task is moderately structured, and time pressure is absent. For example, a brainstorming session for the development of an improved work control process will benefit from participative leadership where the formal operational lines of authority are suppressed and the participants interact as equals.

A more authoritarian leadership style is effective when team members are new to the task, the work is either unstructured or is highly structured, or the work must be completed under time pressure. In a nuclear power plant control room, for example, authoritarian leadership would be critical during emergency operations if a crew were faced with new and unanticipated circumstances and had to respond rapidly.

An effective supervisor adapts his or her personal style to the requirements of the task at hand. This flexibility does not come naturally to many people and supervisory training may be required to modify an individual's leadership style. For example, an experienced first-line supervisor with a strong authoritarian personality that served him or her well in the maintenance department may have to adopt a more participative, coaching style of leadership when he or she is promoted to a management position. Supervisors who are able to change leadership style to adapt to the demands of the situation lead consistently high performing teams.

Mismatches between the leadership style applied in a given work situation and the task demands may cause or contribute to errors in several ways. For example, team members may attempt to debate a verbal instruction from a supervisor who has been consistently participative at a time when it is necessary to implement an order promptly. A consistently authoritarian leadership style may discourage team members from offering ideas that could solve a problem or from raising valid concerns when their input could prevent an unwanted outcome.

14.2 DIRECT CAUSES OF SUPERVISION ERRORS

A direct cause of a supervision error describes the characteristics of supervision that either caused the human error or failed to prevent a human error when prevention was possible. Supervision may play a role in errors through weaknesses in direction, oversight or leadership. Specific examples of direct supervisory causes for errors are presented below.

14.2.1 Direction

Task goals not defined – Task performance failed because personnel were not informed of the goals of the task by supervision prior to starting the job. As a result, for example, the job may be performed on the wrong system or equipment or performed incorrectly.

Task methods not defined – Task performance failed because personnel did not receive necessary guidance from supervision regarding management expectations for how the task was to be performed. The supervisor may not have provided a pre-job briefing or ensured that the work package was complete and included the necessary drawings or procedures.

Unusual or hazardous conditions not identified – Task performance failed because unusual or hazardous conditions at the worksite were unknown to the workers. Supervision may not have walked down the job in advance with the workers to identify any unusual equipment or environmental conditions that could require special tools or equipment or a change to the planned work methods. As a result, errors may occur when the workers encounter unexpected conditions.

Prerequisites not met – Task performance failed because supervision did not ensure that all of the prerequisite conditions were met prior to allowing the job to start. As a result, for example, necessary tools and equipment were not available to perform the work timely, or the equipment was not tagged out and ready for the work to be performed.

Authorization not obtained – Task performance failed because supervision did not ensure that authorization was received before the job was started, or, if the work was delayed, that the authorization continued to be valid. As a result, for example, the job may have conflicted with other work being performed or safety systems may have been taken out of service without the control room's knowledge.

Resources not provided – Task performance failed because supervision did not ensure that workers had the resources required to perform the task. These resources could include information, procedures, guidance or assistance in solving problems that arise.

Qualifications not assured – Task performance failed because supervision assigned workers to tasks for which they were not qualified. As a result, errors were committed and the task was performed incorrectly or incompletely.

Decisions/guidance incorrect – Task performance failed because supervision was not technically competent to direct the work activity and so made decisions or provided guidance that was technically incorrect.

14.2.2 Oversight

No oversight – Task performance failed because supervision was not present during the performance of important tasks or critical portions of a job, with the result that errors were not detected, corrected or prevented.

Oversight unqualified – Task performance failed because supervisory oversight was present, but was not sufficiently familiar with the work to detect and correct or prevent errors.

Oversight distracted – Task performance failed because supervision was involved in performing the job or attending to other matters.

14.2.3 Leadership

Wrong goals – Task performance failed because supervision communicated, directly or indirectly, an emphasis on production or cost goals over safety. As a result, for example, workers may have skipped steps or used alternate methods to those prescribed in the procedures or work package to complete the job quickly.

Questioning attitude discouraged – Task performance failed because supervision, directly or indirectly, discouraged workers from questioning work practices or instructions. As a result, workers may have taken actions that they believed were incorrect or possibly unsafe, or started work without fully understand the task.

Mismatched leadership style – Task performance failed because there was a mismatch between the supervisor's leadership style and the task demands. As a result, teamwork or morale were adversely affected and led to errors.

14.3 PROGRAMMATIC CAUSES OF SUPERVISION ERRORS

Programmatic causes for supervision errors are typically found in the licensee's human resources and training programs. Licensee human resources programs are responsible for ensuring that personnel selected and promoted to supervisory positions are qualified to supervise. Selection and promotion processes screen for technical qualifications and often also assess candidates' decision-making capabilities, leadership skills and other attributes that predict success in the position. Technical training and training in supervisory skills assure that supervisors can fulfill their functions. Other programs may also be implicated.

14.4 ADDITIONAL RESOURCES ON SUPERVISION

- U.S. Nuclear Regulatory Commission (2000). *Qualification and training of personnel for nuclear power* plants (Regulatory Guide 1.8, Rev. 3). Washington, DC: U.S. Nuclear Regulatory Commission

- U.S. Nuclear Regulatory Commission (2000). *Medical misadministrations caused by human errors involving gamma stereotactic radiosurgery (gamma knife)* (Information Notice 2000-22). Washington, DC: U.S. Nuclear Regulatory Commission.

- U.S. Nuclear Regulatory Commission (1981). *Standard review plan*, (NUREG-0800), Chapter 13, Conduct of operations, Sections 13.1.1-13.1.3. Washington, DC: U.S. Nuclear Regulatory Commission.

15 HUMAN-SYSTEM INTERFACE

15.1 THE HUMAN-SYSTEM INTERFACE AND HUMAN PERFORMANCE

In NUREG-0711, " Human Factors Engineering Program review Model," the **human-system interface** (HSI) is defined as the technology through which personnel interact with plant systems to perform their functions and tasks. The major types of HSIs include alarms, information systems, and control systems. Each type of HSI is made up of hardware and software components that provide information displays, which are the means for user-system interaction, and controls for executing these interactions. Personnel use of HSIs is influenced directly by (1) the organization of HSIs into workstations (e.g., consoles and panels); (2) the arrangement of workstations and supporting equipment into facilities, such as a main control room, remote shutdown station, local control station, technical support center, and emergency operations facility; and (3) the environmental conditions in which the HSIs are used, including temperature, humidity, ventilation, illumination, and noise.

Use of the HSI is also affected indirectly by other aspects of plant design and operation, including training (Section 9), supervision (Section 13), staffing (Section 14), and communications (Section 17), which are addressed in other modules. Plant procedures also are considered part of the HSI, as defined by NUREG-0711. However, in the HPEP, a separate module (Section 11) addresses the information content and design of procedures, while this section addresses the user-system interface considerations of computer-based procedure systems as part of the HSI.

In determining the causes of a human performance problem, the licensee may identify specific characteristics of the HSI that led to error. Methods for evaluating HSI characteristics and detailed review guidelines are available in NUREG-0700, "Human System Interface Design Review Guideline." The major topics to consider in evaluating the HSI and determining whether HSI characteristics had an impact on an error are summarized below.

15.1.1 HSI Design Process

Licensees are responsible for the original design of an HSI and any subsequent upgrades and modifications, whether the licensee, a contractor or vendor did the work. A central concern of the design process is ensuring that the HSI will support correct human performance.

There are three important goals to be achieved in the design and implementation of an HSI. These are:

- **Design for operability** refers to designing the HSI to be consistent with the abilities and limitations of the personnel who will be operating it. Weaknesses in the design processes can result in an HSI that is not well suited to the tasks that personnel must perform to ensure plant safety, resulting in increased workload, decreased performance by personnel, and an increased likelihood of errors.

- **Design for maintainability** refers to designing the HSI and associated plant equipment to ensure that personnel are able to perform necessary maintenance activities efficiently. Weaknesses in the design process can result in systems that impose excessive demands on personnel for maintenance and, therefore, are prone to maintenance errors or problems with reliability and availability.

- **Design for implementation** refers to the way that changes, such as upgrades to the HSI, are planned and put into use. A new HSI component may require the user to perform functions and tasks in new ways. Skills that the user developed for managing workload when using the former design, such as ways for scanning information or executing control actions, may no longer be compatible with the new design. The new HSIs must also be compatible with the remaining HSIs so that operators can use them together with limited possibilities for human error. Also, HSI modifications may not be installed or put into service all at one time, causing the user to adapt to temporary configurations that are different from both the original and final configurations. Weaknesses in HSI implementation can increase operator workload and the likelihood of errors.

15.1.2 HSI Characteristics

The characteristics of HSIs that have been found to affect human performance are discussed below. In this section, each HSI characteristic is introduced and defined, and the potential impacts of HSI weaknesses on performance are briefly discussed.

15.1.2.1 Information Display

Information **display** refers to the way that information is presented to personnel. Both the **display devices** and the displays contained in the devices are addressed by this topic. Display device considerations include their location in the work environment and factors that affect legibility, such as brightness and flicker. Display considerations include how information is organized and presented within the display device. A **display page** is a set of information that is presented at one time by a display device. **Display formats** refer to standard groupings of information within pages, including text, tables, graphs, and mimics. **Display elements** refer to the items that make-up the formats, such as characters, numbers, symbols, and icons. Other considerations include whether needed information is present and available, and the quality (i.e., reliability) of the plant data provided to the user. Weaknesses in information display can affect the ability of personnel to promptly and correctly detect, read, and understand information needed to perform their tasks.

15.1.2.2 User-System Interaction

User-system interaction is the set of methods provided in a computer system through which personnel and the computer communicate with each other. The following topics are included. User input formats refers to the type of dialogue between the user and the computer. **Cursors** are pointers that indicate the position of the user's operation on a display screen. **System response** refers to the manner in which the computer system behaves after receiving inputs from the user. **Managing displays** refers to the actions performed by a user to control the way that individual displays are presented on a device. **Managing information** refers to capabilities that

allow the user to create, change, store, and retrieve documents via the computer. **Managing errors** refers to features that support the prevention, detection, and correction of errors. **Help** refers to features that provide guidance to the user (e.g., describes how the user interface works). **System security** includes features that restrict personnel access to aspects of the computer system to prevent accidental or deliberate damage. Weaknesses in user-system interaction can increase the amount of effort for the user to find and arrange needed information. These weaknesses can also inhibit the user's ability to prevent, detect, correct, and recover from errors.

15.1.2.3 Controls

Controls are devices that personnel use to interact with the HSI and the plant. They may be conventional, hardwired control devices or computer-based input devices. Weaknesses in the design of control devices, whether conventional or computer-based, can interfere with the ability of users to perform control or input actions promptly and without errors.

15.1.2.4 Alarm Systems

Alarm systems are automated systems consisting of processing and display hardware and software, which analyze signals from plant sensors and alert the operator via visual or auditory displays (i.e., when the monitored parameters deviate from specified limits). Important characteristics include processing functions; information display; user-system interaction; controls; reliability; test and maintenance capabilities; failure indications; alarm response procedures; control-display coordination; and its integration with the rest of the HSI. Alarm system weaknesses can increase personnel workload associated with finding and assessing plant information and decrease operator awareness of plant status.

15.1.2.5 Soft Control Systems

These are computer-based systems that provide operators with control interfaces that are mediated by software rather than direct physical connects, as in hard-wired knobs and buttons. **Soft controls** can be used to control plant equipment, such as a pump, or the HSI, such as in selecting a display. Important characteristics of soft control systems include the information display, user-system interaction, controls, and integration with the rest of the HSI. Weaknesses in the design of soft control systems can increase the likelihood of human performance problems, such as unintentional actuation, incorrect inputs (i.e., wrong control, wrong input value), and delayed completion of control actions.

15.1.2.6 Computer-Based Procedure Systems

These systems present plant procedures in computer-based rather than paper-based formats. **Computer-based procedures** (CBP) systems can present procedures steps and plant status information in ways that better support decision-making. They can also include capabilities for managing multiple procedures and procedure steps. Important characteristics include processing capabilities (automation for procedure functions), information display, user-system interaction, controls, and integration with the rest of the HSI. Weaknesses in the design of CBP systems can increase workload associated with assessing plant status and selecting appropriate responses and decrease operator awareness of plant status.

15.1.2.7 Computerized Operator Support Systems

These systems use computer technology to support operators or maintenance personnel in situation assessment and response planning. They can monitor status and provide recommendations or warnings. Example applications include: fault detection and diagnosis, safety function monitoring, plant performance monitoring, core monitoring, maintenance advising, and operator support for plant control. Important characteristics include processing capabilities, information display, user-system interaction, controls, and integration with the rest of the HSI. Weaknesses in the design of **computerized operator support systems** can increase workload associated with assessing plant status and selecting appropriate responses and decrease operator awareness of plant status.

15.1.2.8 Workstations

Control, display, and alarm devices of the HSI are often organized into **workstations** where crew functions and tasks are performed. Examples include sit-stand workstations, stand-up consoles, sit-down consoles, vertical panels, and desks. Workstation characteristics affect reach, vision, comfort, the ability to gather and compare information across display devices, and the ability to use control and display devices in a coordinated fashion. Weaknesses in workstation design can interfere with the ability of personnel to detect important information or accurately perform control and computer input actions.

15.1.2.9 Control Room

A control room is a facility in which controls and displays of the HSI are centralized (e.g., the main control room and the technical support center). Two important aspects of a control room are its configuration (i.e., its arrangement of workstations and other equipment) and its environment (i.e., the adequacy of lighting, temperature, humidity, and ventilation for normal and emergency conditions). Weaknesses in control room layout may interfere with the ability of personnel to detect and monitor information and interact with each other. Weaknesses in lighting may affect the ability of personnel to accurately read displays, procedures, and other information sources. Weaknesses in lighting, temperature, humidity, or ventilation may also affect personnel alertness, comfort, and health.

15.1.2.10 Local Control Stations

Local control stations are places outside of the main control room, where operators interact with the plant. They may include multifunction workstations and panels, as well as individual interfaces, such as controls (e.g., valves, switches, and breakers) and displays (e.g., meters and VDUs). When implemented in environments that are not as carefully controlled as the main control room, local control stations may have special considerations such as high levels of background noise and severe environmental conditions. Weaknesses in control station layout may interfere with the ability of personnel to detect and monitor information, perform control actions, and interact with other personnel. Weaknesses in lighting may affect the ability of personnel to accurately read displays, procedures, and other information sources. Weaknesses in temperature, humidity, or ventilation may affect personnel performance, comfort, health, and safety.

15.1.2.11 Maintainability Features

All plant equipment, including the HSI, must be periodically maintained. The design of the maintenance interfaces of plant equipment and the tools used in maintenance tasks can affect personnel performance for these tasks. **Maintainability** refers to the design of features and capabilities that support personnel in detecting equipment failures and performing necessary preventive, routine, and corrective maintenance. This includes the layout of components that must be maintained, labels and markers, controls for adjusting equipment, **test points**, service points, and test equipment (e.g., the user interfaces and capabilities of diagnostic devices). An area that is posing increasing human performance challenges in NPPs is the maintenance of digital systems, due to the complexity of these systems and their susceptibility to incorrect actions. Some maintainability considerations for digital systems include the design of: instrument cabinets and racks, equipment packaging within these enclosures, and fuses and circuit breakers. Weaknesses in the design of maintenance interfaces and tools can increase the likelihood of maintenance errors and the amount of time needed to complete maintenance tasks. This may increase the occurrence of plant transients or decrease the availability of plant equipment needed to ensure plant safety.

15.2 DIRECT CAUSES OF HSI-RELATED ERRORS

A direct cause of an HSI-related error describes characteristics of the HSI that caused task performance to fail. There are a number of ways in which the HSI may cause, contribute to or fail to prevent an error. These include:

15.2.1 Information Display

No display or information not available – Needed information was not displayed or the information that a display was intended to provide was not available. As a result, the user did not have access to the information needed to perform the task.

Display formats, elements or pages unsuitable – The display was formatted (e.g., text, tables, graphs, mimics, speech output) or display elements (e.g., characters, numbers, symbols, icons) were presented in a manner that made them difficult to read, understand or use. As a result, personnel did not or could not use the information displayed when performing the task.

Data quality and update rate inadequate – The display did not provide useful indications of the quality of the data that was provided or the update rate of the data was too slow to be useful. As a result, users were unable to depend on and use the information displayed to guide task performance.

Display equipment inadequate – The equipment used to display information (e.g., VDUs, printers, plotters, meters, light indicators, numerical readouts, and audio devices) did not work or was unsuitable for performing the task. As a result, users did not have access to necessary information.

15.2.2 User-System Interaction

User input formats unsuitable – The format provided by which personnel interacted with the system (e.g., command language, menus, function keys, response entry forms, direct manipulation, query language) was unsuitable for the task. As a result, user inputs were delayed or input errors occurred.

Cursor inadequate – The type of cursor provided was too small or otherwise difficult to see on the screen, or was difficult to manipulate and understand. As a result, task performance was delayed or input errors were committed.

System response inadequate – The HSI did not provide adequate feedback to the user or response times were too slow. For example, prompts regarding the expected input were not provided, no feedback was given when the user entered an input, or the time between an input and the system's response to it was too slow to maintain control.

Display management difficult – Methods for managing displays (e.g., selection, navigation, freeze/update, scroll, page, pan and zoom) were not provided or difficult to use. As a result, personnel could not access needed information or could not access it timely.

Information management inadequate – Means to create, change, store and retrieve documents were not provided or were difficult to use. As a result, needed information was lost.

Errors difficult to detect and correct – The HSI did not provide means to catch input errors or provide easy means to correct them. As a result, errors were made and neither detected nor corrected.

Help function missing or inadequate – Assistance in using the system was not provided or was difficult to access. As a result, personnel could not use the system to perform their tasks.

System not secure – Security features were missing. As a result, personnel caused accidental or deliberate damage.

15.2.3 Controls and Soft Control Systems

Controls not available – The HSI did not provide all the controls necessary to perform the task. For example, controls were not available for selecting plant variables to view or to act upon or means were not provided for monitoring feedback.

Controls not integrated – Control actions or control devices were inconsistent or incompatible with other aspects of the HSI. As a result, personnel took incorrect actions when operating the controls.

Computer-based input devices inadequate – The input devices (e.g., keyboards, trackballs, joysticks, mice, touch screens, light pens, graphic tables and speech input devices) did not work or were unsuitable for the task. As a result, user inputs were delayed or errors committed.

Conventional control devices inadequate – The hardwired control devices (e.g., push buttons, rotary controls, thumbwheels and switches) did not work or were unsuitable for the task. As a result, control actions were delayed or errors occurred.

No backups – Alternate means for taking control actions on critical tasks were not provided should the controls fail. For example, no hardwired backups for soft controls were available, if the soft controls failed.

15.2.4 Alarm Systems

Alarm functions missing – Alarms to alert, inform, guide or assist personnel were not provided. As a result, personnel did not detect important changes in system state or did not have access to needed information to perform their tasks.

Alarm display inadequate – Necessary information was not presented in either an auditory or visual format that was effective in drawing attention and conveying detailed information. As a result, personnel had difficulty detecting and diagnosing system states, leading to errors.

User-alarm interactions inadequate – Silence, acknowledge, reset and test controls were not provided or did not function correctly. As a result, the user was unable to interact effectively with the alarm.

Failure indications missing – The alarm system did not indicate when it was not functioning or it was difficult to determine whether the alarm was operable. As a result, personnel were not aware that alarms were not operable and so did not detect important changes in plant state.

Alarm response guidance missing – Detailed information about alarm conditions and appropriate actions to take in response to alarms (e.g., alarm response procedures) was not available to personnel. As a result, response was delayed or incorrect.

Alarms not integrated – Display and control arrangements for the alarm system were difficult to use or were inconsistent or incompatible with the rest of the HSI. As a result, incorrect actions were taking when interacting with the alarms or use of the alarm system interfered with actions required by other aspects of the HSI.

15.2.5 Computer-based Procedures and Operator Support Systems

Information missing or inadequate – The computer-based procedures or computerized operator support systems did not provide the information users required or it was not

presented in a format that supported performance. For example, the level of detail was insufficient to assist personnel in decision-making.

User-system interactions inadequate – The computer-based procedures or computerized operator support system displays and controls were difficult to understand or manipulate. As a result, personnel responses were delayed or incorrect.

Not integrated – The computer-based procedures or computerized operator support systems were inconsistent or incompatible with the rest of the HSI. For example, control and display devices operated differently from those used for other systems leading to errors.

No backups – No alternate hard-copy procedures or hardwired systems were provided in case of computer-based procedures or computerized operator support system failures. As a result, if the systems failed, personnel had no procedural guidance for performing their tasks.

15.2.6 Workstations

Configuration inadequate – The workstation design did not support user reach, vision or comfort. As a result, for example, personnel became fatigued, could not see important information or were delayed in taking control actions.

Layout inadequate – The layout of controls and displays on the workstation did not support control actions. As a result, personnel became fatigued or made errors when using the controls.

Labeling and demarcation inadequate – Labels and markings did not assist users in finding and identifying controls, displays and other equipment. As a result, for example, personnel used the wrong controls for the intended action or read the wrong display.

15.2.7 Control Room

Space and layout inadequate – Sufficient space was not available or equipment was laid out in ways that it was difficult for personnel to view or access information, communicate or walk around. Or, there was inadequate space available to store needed procedures, other documents, spare parts, expendables, tools, protective equipment and personal items. As a result, for example, procedures could not be laid out so that placekeeping was difficult or needed items were lost and prevented task completion.

Supervisor inaccessible – Access to the shift supervisor's office via walking or communication links was difficult. As a result, the supervisor was unavailable when needed or was unable to maintain awareness of control room activities.

Multi-units not distinguishable – Features to distinguish between controls and displays for different units, or mirror-image control rooms, caused personnel to incorrectly monitor plant parameters or take control actions on the wrong unit.

15.2.8 Local Control Stations

No display or information not available – Needed information was not displayed or the information that a display was intended to provide was not available. As a result, the user did not have access to the information needed to perform the task.

No controls or controls not available - The controls necessary to perform the task were either missing or not working at the local control station. As a result, necessary control actions could not be performed.

Layout inadequate – The layout of controls and displays at the local control station did not support control actions. As a result, personnel could not accurately determine system status and made incorrect operational decisions.

Labeling and demarcation inadequate – Labels and markings did not assist users in finding and identifying controls, displays and other equipment. As a result, for example, personnel used the wrong controls for the intended action or read the wrong display.

15.2.9 Maintainability

Equipment inaccessible – The arrangement of components and access to them for inspection, testing, replacement and repair was inadequate. As a result, maintenance activities were delayed or errors were committed.

Labeling and demarcation inadequate – Labels or markings did not support proper identification of equipment and components. As a result, task performance was delayed while personnel attempted to identify the correct piping.

Adjustment controls missing or inadequate – Control devices for performing adjustments on equipment were not provided or were inconvenient to use. As a result, setpoints could not be accurately maintained.

Test and service points missing or inadequate – Test and service points were not provided or were inconvenient to access and use. As a result, personnel skipped a surveillance rather than attempt to access a test point.

Test equipment inadequate – Equipment needed for testing was not available, was difficult to use, was miscalibrated or was otherwise not properly configured for the maintenance task. As a result, the maintenance task was not completed or equipment operability following maintenance could not be verified.

15.3 PROGRAMMATIC CAUSES FOR HSI-RELATED ERRORS

Licensees may have many programs, processes, and practices to ensure that human factors engineering considerations are properly addressed in the design and installation of the HSI and other plant equipment, and that human performance considerations continue to be met in on-going operations after installation. There are three primary programs or processes that may set the stage for HSI weaknesses that cause errors. These are the HSI design and implementation process, and maintenance and housekeeping activities. If the display system is not fully operational, contains outdated information, or has labels that are either illegible due to accumulated dirt or missing, the licensee should consider programmatic causes related to its repair, maintenance, and general housekeeping.

HSI Design – The HSI design and implementation process assures that original HSI designs and upgrades fully meet the needs of operations and maintenance personnel and that problems are avoided when the new design is put into service. If design and implementation processes are deficient, weaknesses will exist in the HSI. For example, a poorly designed display system or controls that are difficult to use may result from an inadequate design process.

Maintenance – A licensee may have a variety of programs for ensuring that the HSI and plant equipment are in working order and available for use. These include preventative, routine, and corrective maintenance programs for both hardware and software components. An important concern for software maintenance is ensuring that the computer system is updated with the most current and correct set of instructions and data. Another maintenance concern is the replacement of missing or degraded labels throughout the plant. Weaknesses in these programs can result in the HSI being inadequately or incorrectly serviced, resulting in problems with reliability and availability.

Housekeeping – Housekeeping includes activities performed to maintain a clean and orderly work environment. Examples include cleaning labels and displays so they can be easily read, cleaning input devices so they can be used properly, removing trash and used materials to eliminate unnecessary clutter, and storing documents so they can be readily accessed when needed. Housekeeping practices refers to the way these tasks are performed on an ongoing basis to maintain a productive work environment. Weaknesses in housekeeping practices can increase operator response time and the likelihood of errors.

15.4 ADDITIONAL RESOURCES ON THE HSI

- U.S. Nuclear Regulatory Commission (1996). *Standard review plan for the review of safety analysis reports for nuclear power plants* (NUREG-0800). Washington, D.C.: U.S. Nuclear Regulatory Commission.

- U.S. Nuclear Regulatory Commission (1996). *Human System Interface Design Review Guideline* (NUREG-0700, Rev 1.). Washington, DC: U.S. Nuclear Regulatory Commission.

- U.S. Nuclear Regulatory Commission (1994). *Human factors engineering program review model* (NUREG-0711). Washington, DC: U.S. Nuclear Regulatory Commission.

- U.S. Nuclear Regulatory Commission (1994). *Human Factors Engineering Guidance for the Review of Advanced Alarm Systems* (NUREG/CR-6105). Washington, DC: U.S. Nuclear Regulatory Commission.

- Brown, W.S., O'Hara, J.M. and Higgins, J.C. (2000). *Advanced alarm systems: Revision of guidance and its technical basis* (NUREG/CR-6684). Washington, DC: U.S. Nuclear Regulatory Commission.

- O'Hara, J.M., Higgins, J.C., Stubler, W.C. and Kramer, J. (2000). *Advanced information systems design: Technical basis and human factors review guidance* (NUREG/CR-6633). Washington, DC: U.S. Nuclear Regulatory Commission.

- O'Hara, J.M., Higgins, J.C., Stubler, W.F. and Kramer, J. (2000). *Computer-based procedure systems: Technical basis and human factors review guidance* (NUREG/CR-6634). Washington, DC: U.S. Nuclear Regulatory Commission.

- Stubler, W.F., O'Hara, J.M., and Kramer, J. (2000). *Soft controls: Technical basis and human factors review guidance* (NUREG/CR-6635). Washington, DC: U.S. Nuclear Regulatory Commission.

- Stubler, W.F., Higgins, J.C. and Kramer, J. (2000). *Maintainability of digital systems: Technical basis and human factors review guidance* (NUREG/CR-6636). Washington, DC: U.S. Nuclear Regulatory Commission.

- Stubler, W.F., O'Hara, J.M., Higgins, J.C. and Kramer, J. (2000). *Human Systems Interface and Plant Modernization Process: Technical Basis and Human Factors Review Guidance* (NUREG/CR-6637). Washington, DC: U.S. Nuclear Regulatory Commission.

- Higgins, J. and Nasta, K. (1997). *Human factors engineering (HFE) insights for advanced reactors based upon operating experience* (NUREG/CR-6400). Washington, DC: U.S. Nuclear Regulatory Commission.

- Brown, W., Higgins, J., and O'Hara, J. (1994). *Local Control Stations: Human Engineering Issues and Insights* (NUREG/CR-6146, BNL-NUREG-52400). Washington, D.C.: U.S. Nuclear Regulatory Commission.

- O'Hara, J.M., Brown, W.S., Baker, C.C., Welch, D.L., Granda, T.M. and Vingelis, J.P. (1994). *Advanced human-system interface design review guideline: Evaluation procedures and guidelines for human factors engineering reviews* (NUREG/CR-5908, Vol. 2). Washington, DC: U.S. Nuclear Regulatory Commission.

16 TASK ENVIRONMENT

16.1 EFFECTS OF ENVIRONMENTAL FACTORS ON HUMAN PERFORMANCE

The **task environment** refers to the physical conditions in which work is performed. Environmental conditions that can affect performance include excessive vibration and noise, temperature extremes and insufficient lighting. These adverse environmental conditions can stress personnel, interfere with performance and increase the likelihood that they will commit errors while performing a task. Work conditions that require protective gear, such as high radiation or some confined space environments, or that require unusual physical postures, also can interfere with task performance, as may poor housekeeping.

16.1.1 Vibration

There are two types of vibration that may cause errors. The first is **whole-body vibration**, in which vibration is transferred to the worker from standing or sitting on a vibrating surface. The second is **object vibration**, in which a stationary worker interacts with a vibrating object in some fashion. The effects of vibration depend upon its frequency and acceleration. **Frequency** is the number of oscillations (cycles) that occur in one second. **Acceleration** is the force, or intensity, of the vibration.

Whole-body vibration affects personnel comfort levels. As discomfort increases, errors may occur. Personnel are most uncomfortable when the frequency of the vibration approaches the resonance point of the human body (5 Hz) and can tolerate only short exposures. Discomfort also increases as acceleration increases. Discomfort may induce errors by causing personnel to rush through their work or by distracting them.

Whole-body vibration also affects the ability to control fine hand and arm movements. Vibration will induce errors in tasks that require accurate hand and arm movement, such as writing, placing and tightening screws, or attaching jumpers.

Vibration also blurs vision. Errors may occur from vibration on tasks that require accurate vision, such as reading instruments, procedures or drawings.

Object vibration may also adversely affect performance. For example, errors may occur when making fine adjustments or in reading instruments, if equipment is vibrating.

16.1.2 Noise

Noise is unwanted sound. Noise can cause errors in several ways. It may disrupt communications, affect the ability to perform tasks and annoy personnel.

The effects of noise on communications are complex. Even relatively low levels of noise can mask speech, but only under some circumstances. For example, speakers naturally raise their voices when there is background noise and may be able to overcome some of its effects on

communication. Being able to see the speaker's face or using standardized phrases also improves communication in a noisy environment. The type of background noise also affects communication. It is easier to communicate over noise that is steady and uniform than noise that includes sharp tonal peaks, such as background speech.

Noise has been shown to affect decision-making, memory, vigilance, attention and motor skills. Whether noise will cause errors depends upon (1) the degree of familiarity with the noise, (2) the complexity of the task the worker is performing and (3) the frequency and intensity of the noise, measured in decibels.

Familiar noises are usually continuous, such as the sound of freeway traffic or the hum of a motor. Even high levels of familiar noise typically do not impair performance on simple tasks and will cause only minor effects on complex tasks, such as reading or decision-making.

Unfamiliar noise is more disruptive. Unfamiliar noise includes speech, alarms and some kinds of music. Loud and unfamiliar noise may cause only minor performance effects on simple tasks, but will disrupt performance of complex tasks. Multiple alarms sounding simultaneously in a control room, for example, could interfere with performance of complex tasks.

Unfamiliar, loud noise is also annoying. Annoyance may cause workers to rush through their tasks or disrupt teamwork. Unexpected and unfamiliar loud noise, such as sonic booms from line breaks, may startle personnel.

16.1.3 Heat

Heat exposure is a common problem in many areas of a plant, such as the turbine building when the plant is operating. The extent to which workers will be affected by heat depends on many factors. These include physical characteristics, such as age, weight, acclimation to heat, physical fitness and dehydration. Other factors that determine the effects of heat on performance include airflow, humidity, clothing and level of physical activity.

As **whole-body temperature** (a measure of internal body temperature that is estimated externally by wet-bulb globe temperature - WBGT) increases, first the workers' comfort levels are affected, then task performance is affected, followed by the onset of heat stress. Performance of perceptual/motor tasks, such as tracking, monitoring, and manipulating objects, is affected even at relatively low temperatures (69°F WBGT). Performance on perceptual/motor tasks degrades over the first two hours of exposure, and then levels off. Performance of mental tasks, such as arithmetic computations, logical reasoning, and recalling information from memory, begins to degrade sharply after about 30 minutes of exposure to temperatures above 90°F WBGT, but then levels off. When workers begin to experience heat stress, they may become confused and disoriented, in addition to experiencing physical symptoms, and are very likely to commit errors if they attempt to continue working.

16.1.4 Cold

Exposure to cold affects the performance of manual tasks. Decreases in the ability to control hand movements begin at an air temperature of approximately 54° F. The fingers may become

numb to pain at this temperature and touch sensitivity is reduced. Performance of gross manual tasks, such as those involving the arms and legs is also degraded at 54° F. The speed at which manual tasks can be performed is affected by the rate of cooling. Slow temperature drops have a greater negative impact on manual dexterity than rapid temperature decreases, during the initial exposure period.

Hypothermia occurs when a worker can no longer maintain an adequate deep-body temperature. In the early stages, individuals experience lethargy, clumsiness, confusion and irritability. As the hypothermia deepens, hallucinations or arrested breathing will occur.

The effects of cold temperatures on performance are affected by clothing, whether exposed skin and clothing are wet or dry, air movement (wind chill) and the length of exposure. Performance impairments may be experienced at higher air temperatures than those discussed above if workers are not dressed warmly, their skin or clothing is wet, or they are exposed to air movement or to cold temperatures for extended periods of time.

16.1.5 Lighting

Adequate lighting is required for accurate performance of nearly every task in a nuclear power plant. Visibility depends upon several factors:

- The intensity of the light radiated by a light source, measured by **candle power**
- The amount of light striking an object from a light source, known as its **illuminance**
- The perceived brightness of an object, known as its **luminance**, which depends upon the object's reflectance
- The difference between an object's luminance compared to the luminance of the object's background, or **contrast**
- The object's size
- The individual worker's age and visual acuity.

Visibility is also affected by changes in light levels as the eyes adapt. Individuals have particular difficulty seeing while their eyes are adapting to a different level of illuminance, such as entering a darkened room from full sunlight.

The ability to accurately perceive colors (**color discrimination**) is also affected by lighting. Color discrimination may be reduced by the characteristics of the light source. For example, high-pressure sodium discharge lamps reduce the ability to discriminate colors, while artificial daylight fluorescent lamps maintain it. Very low lighting levels also adversely affect color discrimination.

Glare and flicker will also reduce visual performance. **Glare** occurs when the luminance level (the amount of light reflected from an object) is annoying. It may reduce contrast, interfere with reading and inspection tasks and cause visual fatigue. **Flicker** causes discomfort and eye fatigue when reading.

16.1.6 Other Adverse Task Conditions

Other adverse environmental conditions may also affect task performance. In general, any physical conditions that require the use of PPE or devices complicate task performance, may be stressful and so may increase the likelihood of errors (see Section 12, Tools and Equipment.) For example, working in confined or elevated spaces may encourage personnel to hurry through their tasks and so commit errors. Working in high radiation environments may require that task performance be repeatedly interrupted to minimize exposures. Poor housekeeping may increase the likelihood of trips and falls, or obscure displays and controls. Working on ladders or platforms, or in cramped working conditions that require unusual physical postures may cause discomfort, can be distracting and may increase the likelihood of errors.

16.1.7 Combinations of Conditions

Most of the research that has examined the effects of environmental factors on human performance has been done in the laboratory or in other highly controlled settings. In most industrial settings, environmental factors are not as rigidly controlled and often fluctuate. Further, in industry, adverse environmental conditions often occur together, such as high noise levels and excessive heat when high-energy equipment is operating. Large fluctuations in conditions and combinations of conditions have not been as thoroughly studied. There is some evidence to suggest, however, that performance degradations are more severe under fluctuating and/or combined conditions.

16.2 DIRECT CAUSES OF TASK ENVIRONMENT-RELATED ERRORS

A direct cause of a task environment error describes the physical conditions that caused task performance to fail. There are a number of ways in which characteristics of the task environment may impair performance. These include:

Vibration - Task performance failed because high levels of whole-body or object vibration made displays, instruments or documents difficult to read or caused discomfort. For example, vibration prevented a worker from accurately reading a piping and instrumentation diagram.

Noise - Task performance failed because high noise levels interfered with communications, caused discomfort, or impaired mental or physical performance.

Heat - Task performance failed because excessive exposure to heat caused discomfort or impaired mental or physical performance. Or, the need for frequent work breaks delayed task completion or increased the communication burden on personnel due to rotations.

Cold - Task performance failed because excessive exposure to cold caused discomfort or impaired motor performance. For example, workers dropped tools or were unable to manipulate controls.

Lighting - Task performance failed because lighting was excessive, insufficient, the wrong type for discriminating color, or produced annoyance from glare or flicker. For example, a computer screen was difficult to read due to glare.

Poor housekeeping - Task performance failed because displays or controls were obscured by trash or equipment that should have been stored. Workers tripped over or were required to walk out of their way to avoid tools or equipment that should have been removed.

Workspace - Task performance failed because the worker had insufficient space to perform the task or had to assume uncomfortable positions.

High radiation – Task performance failed because workers were hurried or their activities were repeatedly interrupted to avoid excessive exposures.

Combinations of factors - Task performance failed because a combination of environmental factors impaired performance. For example, a job in the turbine building involved exposure to heat, noise and low lighting, none of which individually exceeded levels at which performance is affected, but the combination of conditions distracted the workers and caused errors.

16.3 PROGRAMMATIC CAUSES OF TASK ENVIRONMENT ERRORS

Programmatic causes of task environment errors are typically found in the licensee's processes for designing human-system interfaces or in managing maintenance activities. Other programs may also be implicated. Common programmatic causes of task environment errors include:

Industrial Hygiene and Radiation Protection – These programs are responsible for ensuring that task environments have been evaluated to identify hazards and that needed controls are implemented to minimize exposures. Weaknesses in these programs may result in personnel working in task environments that are conducive to errors.

Work Planning and Control - Weaknesses in the work planning and control system may allow work to be planned without consideration of adverse environmental conditions and performed without the necessary compensatory measures. For example, communication devices may not be provided in noisy environments to support task performance. For tasks that involve unusual physical positions or cramped workspace, additional time to complete the task may not be scheduled. Rest breaks for hot and cold environments may not be planned into the work, or additional temporary lighting may not be provided if the work site is not adequately lighted.

Procedures - Weaknesses in the licensee's procedure development process may result in the design of procedures that are inappropriate for the conditions in which they will be used. For example, procedures that may be used at night, outside and in the rain should

be laminated and the type size should be larger to ensure the procedure can be read. Procedures that will be used in vibration conditions may also require larger type size than procedures read in the stationary environment of the control room, for example.

Human Factors Engineering - Weaknesses in the human factors engineering program may result in the installation of new equipment or systems without consideration of task environment characteristics. For example, the impact of control room lighting on the visibility of digital displays or effects of vibration on the legibility of dials or gauges at local control stations should be considered before installation.

Operating Experience - Reviews of relevant operating experiences of the plant and other facilities with similar environmental conditions should be conducted to identify and analyze task environment problems and successful mitigation efforts. Personnel may have reported task environment conditions that interfered with performance that are recorded in the licensee's corrective action database, and corrective actions should have been implemented. Weaknesses in this program will result in repeated errors.

Labeling - Weaknesses in this program may result in tags and plaques that are illegible in the task environment, if low lighting levels or vibration are present.

16.4 ADDITIONAL RESOURCES ON TASK ENVIRONMENTS

- U.S. Nuclear Regulatory Commission (1992). *Shutdown and low-power operation at commercial nuclear power plants in the United States* (NUREG-1449). Washington, DC: U.S. Nuclear Regulatory Commission.

- U.S. Nuclear Regulatory Commission (1996). *Human-system interface design review guideline* (NUREG-0700, Rev. 1, Vol.s 1-3). Washington, DC: U.S. Nuclear Regulatory Commission.

- Echeverria, D., Barnes, V., Bittner, A., Durbin, N., Fawcett-Long, J., Moore, C., Slavich, A. Terrill, B., Westra, C., Wieringa, D., Wilson, R., Draper, D., Morisseau, D. and Persensky, J. (1994). *The impact of environmental conditions on human performance: A handbook of environmental exposures* (NUREG/CR-5680, Vol.s 1 and 2). Washington, DC: U.S. Nuclear Regulatory Commission.

17 COMMUNICATIONS

17.1 COMMUNICATIONS IN ORGANIZATIONS

Communication is the exchange of information while preparing for or performing work. Verbal communication occurs face-to-face, by telephone, sound-powered phones or walkie-talkies, as well as over public address systems. Written communication occurs, for example, through policies, standards, work packages, training materials, and e-mail.

Communication involves two sets of behaviors: (1) creating and sending messages and (2) receiving and interpreting them. Communication always involves at least two individuals, the sender and the receiver, and occurs:

- Between individuals
- Within and among work groups
- In meetings
- In pre-job or pre-evolution briefings
- During shift turnover

Successful communication requires several steps. The sender first develops the intention to communicate either verbally or in writing. The sender then composes a message that presents the meaning as clearly as possible. The receiver must pay attention to the message and then interpret its meaning. If the communication is successful, the receiver interprets the message consistently with the sender's intended meaning.

The similarity of the meanings given to the message by the sender and receiver can be verified through feedback. An example of feedback verification in verbal communication is when the receiver "repeats back" the message and the sender either agrees with the receiver's repeat back or corrects it. Verification feedback serves an important error-checking function in the communication process. It also allows supervisory oversight of communications to catch errors before they have consequences.

A sender and receiver must both be active for communication to be effective. The sender and receiver share responsibility for ensuring successful communication. However, when licensees analyze the causes of events, errors in sending messages are more often identified than errors in receiving. The reasons for the difference are unclear. A licensee's investigation should consider sending and receiving errors and corrective actions should address both to be effective.

17.2 DIRECT CAUSES OF COMMUNICATIONS-RELATED ERRORS

A direct cause of a communication error describes the characteristics of the communication that caused it to fail. The direct cause of the error may be characteristics of how the message was sent or how it was received and interpreted. In some cases, a communication error will be compounded by failures in verification feedback or supervisory oversight.

There are a number of ways in which communication can fail. Research regarding communication errors in nuclear licensee facilities identified eleven direct causes of sending and five direct causes of errors in receiving:

17.2.1 Sending Errors

Content wrong - Communication failed because the information contained in the message was incorrect. For example, an operator in the control room refers to the wrong unit when giving instructions to an operator in the field.

Content inconsistent -Communication failed because, although the information in a message was correct, it was partially or completely inconsistent with other information available to the receiver. For example, a required surveillance test appears on a maintenance worker's schedule but his supervisor assigns him to another job and the surveillance is missed.

Content inappropriate for the job - Communication failed because the information in a message was irrelevant or inappropriate for the job at-hand. For example, a work order references a procedure that contains prerequisite conditions that cannot be met during at-power operations, but the maintenance worker attempts to perform the procedure anyway.

Content inappropriate for the receiver - Communication failed because the message was not tailored to the receiver's background, training or level of technical knowledge. For example, a non-licensed operator is instructed to perform a task on an unfamiliar system and cannot find it.

Standard terminology not used - Communication failed because complete identification information was not provided in the message. For example, a maintenance supervisor refers to a valve using a generic pronoun (e.g., "it"), rather than using the valve's proper name and number, and the maintenance crew works on the wrong valve.

Familiar terminology not used - Communication failed because unfamiliar terms were used in the message. For example, the formal name of a building, rather than the site-specific nickname, is used in a pre-job briefing and the crew is confused about which building is being discussed.

Message production inadequate - Communication failed because the message was not produced adequately. For example, a message is garbled when transmitted over the public address system or cannot be heard against background noise. A written communication contains typographical errors or copies are illegible.

Necessary information not sent - Communication failed because the information needed to perform a task was not provided to the worker. For example, a work order omits an instruction to obtain control room authorization before taking the component out of service.

Wrong place or person - Communication failed because necessary information did not reach the intended receiver. For example, a sender dials the wrong phone number or incorrectly addresses an e-mail message.

Wrong time - Communication failed because the message was sent too early or too late to be used by the receiver. For example, a maintenance worker finishes one job early and starts on the next before her supervisor has the opportunity to communicate that the job has been rescheduled.

Sending verification failure - Communication failed because the sender did not ensure that the receiver accepted and accurately interpreted the message. For example, a non-licensed operator calls the control room to report a leak and can tell that the control room operator is busy and distracted, so does not request that the control room operator repeat back the location and rate of the leak.

17.2.2 Receiving Errors

Information not sought - Communication failed because a receiver did not seek the information necessary to perform a task. For example, a work order references drawings needed to verify the location of a component, but the planner does not include them in the work package and maintenance technicians do not obtain and review them before starting work.

Information not found - Communication failed because the receiver, intentionally or unintentionally, did not find necessary information for performing a task. For example, an identification tag on a cable is hidden and the crew decides to perform the task without positively identifying the cable referenced in the work package, resulting in errors.

Information not used - Communication failed because the information necessary to perform a task was not used. For example, the need to wear electrical safety PPE is discussed at a pre-job briefing, but the instrumentation and control technician is in a hurry and performs the task without it.

Message misunderstood - Communication failed because the receiver misunderstood the message. For example, a control room supervisor and an operator discuss two related jobs, one of which requires establishing a fire watch. In the course of the discussion, the operator becomes confused about which job requires the fire watch and establishes the watch for the wrong job.

Receiving verification failure - Communication failed because the receiver did not take actions to test his or her understanding of the message received. For example, the control room operator in the fire watch example failed to repeat back or paraphrase the supervisor's message to check concurrence and to identify any gaps in the message or in his understanding of it.

17.3 PROGRAMMATIC CAUSES OF COMMUNICATIONS-RELATED ERRORS

Most work activities in organizations require coordination within and among work groups. Coordination requires effective verbal and written communication. Communication is necessary to define the work to be done and how to do it, so communication errors are frequently found to be causal factors in events. But, because so many work activities depend on effective communication, a wider variety of programmatic causes are associated with communication errors than with other types of human errors.

Programmatic causes that have been shown to cause or contribute to communication errors at nuclear licensee facilities are described below. Weaknesses in other programs at a licensee's site may also cause communication errors.

Information management - Flaws in programs for developing and managing technical documentation are a common source of communication errors. Omissions and technical inaccuracies in vendor manuals, engineering analyses, design basis or other reference documents may be translated into inaccuracies in procedures and work orders that are used to perform jobs. Failures to update drawings and procedures when new hardware is installed or existing hardware is modified can result in communication errors.

Work Planning and Control - Planning and scheduling maintenance activities is a complex task. Weaknesses in work planning and control programs may result in both written and verbal communication errors associated with, for example, inadequate work orders, inadequate pre-job briefings, or communication failures during job performance.

Shift Staffing - Insufficient staffing can increase the workload for those performing a job, and so interfere with required communications. Increased workload during plant outages and the increased numbers of workers on-site, or increased workload during off-normal events, can tax the supervisory abilities of those responsible for coordinating the work, resulting in incomplete or too few communications. Too many staff involved in performing a job can increase the communication burden on all involved and result in communication failures.

Training - Effective communication requires some degree of shared understanding of the work to be performed. Inadequate job knowledge, resulting from deficient training or qualifications, can lead to both sending and receiving errors. Effective communication also depends upon an understanding of the information needs of those involved in performing a job. Communication across organizational boundaries (e.g., between individuals in different departments, in different job roles, or on different shifts) can cause problems because senders and receivers may not understand one another's terminology or the contexts and constraints of the other's job.

Procurement and Maintenance – Some communications occur across physical distances through communication devices. Procurement and maintenance programs ensure that communication devices are suitable for their intended uses and are working properly. Communication errors can arise here, for example, when there is too much background

noise for a receiver to hear a public address announcement or what is being said on the radio or over the telephone. An insufficient number of radio frequencies to support communication needs may also cause or contribute to communication errors.

Supervision - Some communication failures occur as a result of human errors in job performance. These errors can often be caught and corrected through independent observation and supervisory oversight of the work being done. Weaknesses in plant programs for deciding which jobs require independent oversight or for ensuring that appropriate supervision is available to watch for errors can allow communication errors to occur.

Procedures - Lack of communication skills or failure to apply standard verbal and written communication practices are often associated with communication errors. A lack of training in standard communication techniques and the absence of procedures to prescribe the circumstances in which standard communication techniques will be used often contribute to the occurrence of errors.

17.4 ADDITIONAL RESOURCES ON COMMUNICATIONS

- U.S. Nuclear Regulatory Commission (1996). *Human-system interface design review guideline* (NUREG-0700, Rev. 1, Vol.s 1-3). Washington, DC: U.S. Nuclear Regulatory Commission.

- U.S. Nuclear Regulatory Commission (1997). *Evaluation criteria for communications-related corrective action plans* (NUREG-1545). Washington, DC: U.S. Nuclear Regulatory Commission.

18 COORDINATION AND CONTROL

Note that the structure of this module differs from the others and does not include a section discussing direct causes of errors associated with coordination and control. Errors do not typically result directly from weaknesses in coordination and control at licensee sites. Rather, coordination and control processes, along with other programs, policies and processes, are responsible for establishing and maintaining a licensee's barriers to error. Therefore, in most events, there will be elements of coordination and control processes that failed to prevent the error from occurring. However, the element of coordination and control that failed is typically insufficient to cause the error by itself and so serves as a contributing, rather than direct cause of an error.

18.1 COORDINATION AND CONTROL: SETTING THE STAGE FOR ERRORS

Control can be defined as ensuring that work activities at a site have the intended results and no others. Maintaining control requires that:

- The desired consequences of a work activity are known in advance
- The risks and hazards inherent in the activity are known and addressed
- The external conditions that increase the risks/hazards of the activity are known and can be controlled, and
- The activity is coordinated with other work activities so that they do not interfere with one another and the combination of activities does not create an unexpected plant state.

Operations are controlled at a licensee facility when work activities are routinely conducted without surprises.

There are three elements necessary to maintain operational control:

- Administrative processes that formalize activities commensurate with their risk impact and complexity.
- Effective methods of coordinating the activities of diverse work groups within the organization as well as the activities of individuals within work groups.
- Information management to capture, communicate and retain important information over time and changes in equipment and personnel.

These elements ensure that an organization has the tools required to establish and maintain control over maintenance, engineering and plant operational activities. They are also the hallmark of a reliable organization.

18.1.1 Work Control

The first element of control includes the administrative processes by which work is conceptualized, reviewed, approved, authorized and performed. Licensees have adopted a variety of programs to structure the manner in which work is to be performed. Often the names

and terminology of the processes are different at different sites. However, there are some fundamental characteristics of effective administrative work control processes that should be incorporated into the individual programs.

The control process involves a series of steps that define how work activities in maintenance, engineering and operations are accomplished to ensure that management expectations are met. These steps include:

1. Requirement determination – the decision to perform the activity
2. Development – work design and preparation of the procedures or work package
3. Approval – supervisory review of the work plan
4. Authorization – approval to perform the work after consideration of conditions
5. Implementation – performing the work or activity
6. Oversight – supervisory review of the work or activity including QA/QC
7. Closeout – review of documentation and acceptance of quality of work

Effective work control requires the selection of an appropriate level of formality, deliberateness and precision for each step in the process. The level of formality must be commensurate with the risk, complexity and importance of the activity. Greater degrees of formality ensure higher levels of performance and quality at the cost of additional time and resources. Typically, the greater potential risk, complexity or economic importance of an activity, the greater the formality in planning and implementing the work. For more complex or important jobs, licensee administrative processes may require more extensive reviews of work plans, higher levels of management involved in approving the plans and authorizing the start of work, increased oversight of the work as it is being performed and more thorough testing and evaluation prior to job close-out.

Another significant aspect of operational control is the preplanning that must be accomplished in order to allow simple evolutions to be performed with a reasonable level of effort and to allow rapid and correct action to be taken when off-normal or emergency conditions occur. An example of this preplanning may be observed in the control room when an operator must respond to an annunciator. In this case, plant management has predetermined that the operator can invoke the annunciator response procedure and take the necessary actions without further planning or control steps. The operator has achieved a level of mastery that qualified him or her to respond to the annunciator without further management involvement. The annunciator response procedure has been verified and validated in advance to ensure that the procedure will address the alarm condition. However, each of the seven steps in the control process is still applicable and invoked by management decisions, many of which were made long before the annunciator alarmed and the operator took action to respond to the condition.

Administrative processes are also required to address unanticipated conditions. Even with extensive preplanning, conditions often arise that deviate from those specified or assumed in a work plan when it is implemented. Clear delineation of roles, responsibilities and authorities is necessary for personnel to understand the types of unexpected situations in which they are authorized to make decisions, resolve problems or to change work plans to address existing conditions. Clear assignment of authority to stop work when unexpected conditions arise is also necessary to maintain control. Changes to work plans that have not been analyzed and approved

by individuals who are qualified to evaluate the implications of the changes are a common cause of errors at licensee facilities.

18.1.2 Coordination

Coordination is the process by which resources (people, equipment, tools, procedures, parts, facilities) are identified, scheduled and assigned to a work activity. The scope of work activities may range from station-wide projects (such as steam generator replacements) to individual tasks (such as drafting a work order) and the time frames in which the work occurs may range from minutes to years.

Effective performance requires coordination at two organizational levels. The activities of different organizational units (e.g., maintenance, operations, engineering, and subgroups within those departments) must be coordinated, and the activities of individuals within work groups (e.g., control room or maintenance crews) must be coordinated when more than one individual is assigned to a task. In general, the licensee's managers and work planning and scheduling processes coordinate work activities between organizational units. First-line supervision is typically responsible for coordinating the activities of individuals and teams within a department.

In general, the goals of coordination are to ensure that:

- work activities are planned and scheduled so that they do not interfere with one another
- the combination of activities occurring concurrently does not create unexpected, unknown or unanalyzed conditions
- the necessary resources required to perform a task are available to perform the task when required (e.g., necessary tools, parts and equipment, procedures, sufficient numbers of qualified personnel)
- the work will be completed on time.

Coordination methods range from highly complex, detailed and formalized interactive software planning tools to simple "to do" lists. The licensee will often require the use of several different scheduling tools or methods in station administrative procedures for different types of work activities. For example, most licensees typically use interactive, real time, critical path planning software to coordinate outage work activities. However, they often use less formalized planning and scheduling tools for the daily, at-power operations and other internal departmental activities. In each case, the elements of a successful coordination process are consistent with the complexity and the risk significance of the activity.

Work planning determines the specific human performance elements that are necessary for each work package or job and ensure that they are available and integrated. Human performance elements required to conduct a specific job may include requirements for communication, procedures, skilled personnel, documentation, supervisory oversight, quality assurance, special tools and equipment or other resources.

An example of a coordination error would be a fuel rod placed into the wrong position because the refueling operator did not obtain independent verification of correct grid position prior to lowering the assembly into the core. Clearly, an error of this type could also result from the

operator's inability to select the correct grid position in the core or skipping the step in the procedure that required independent verification. However, if the refueling procedure did not require independent verification of the grid position prior to lowering the assembly, or no one was available to perform the verification even though the operator might otherwise have waited for it to be verified before proceeding, the cause of the error would lie in coordination.

The most common consequences of weaknesses in coordination are that work is delayed. For example, a maintenance crew may have to stop a job for two hours while waiting for a quality control (QC) inspector to be available. Or, work on a piece of equipment cannot start on time because the tags were not hung by the previous shift. Delays typically affect productivity rather than cause errors. However, the likelihood of errors increases if plant conditions change during the delay so that the work plan can no longer be implemented as written, or if the job must be extended over more than one shift and important information is not communicated during shift change.

18.1.3 Information Management

The third element necessary to effective control is the information management systems that capture, communicate and maintain important information that is required to conduct work activities safely. The organization identifies information that will be required to safely and effectively operate or repair the plant, disseminates it and maintains this information to assure that it can be accessed when required. The type of information to be managed includes such diverse areas as operations configuration control of equipment alignments, engineering design control of systems and components, quality assurance of spare parts, and quality control of nondestructive testing. In each case, the information required to safely operate or maintain the equipment must be identified, captured, retained and made readily available as the plant personnel change over time. This process includes configuration management of short-term equipment alignments to ensure compliance with technical specifications as well as long-term engineering design control changes that may impact the plant safety envelope over the life of the reactor.

Identification of important information is a dynamic process. As new conditions and events occur, information requirements will change. For example, industry codes and standards may be updated. Information may become available from Significant Operational Events Reviews (SOERs), licensee reports to the NRC and lessons learned from NRC inspection activities that should be disseminated and retained. Changes in the workforce at a site may also require that more or different types of information be made available to new personnel.

An example of a human error related to information management would be if a vendor determined that a certain preventive maintenance action was required and the plant maintenance staff did not have an active vendor manual program to identify the change and incorporate this preventive maintenance item into the plant's schedule. The result was a component that failed because a process had not been adequately established to update the vendor manuals.

18.2 EFFECTS OF COORDINATION AND CONTROL WEAKNESSES

The following are examples of ways in which coordination and control may set the stage for other performance shaping factors to cause errors.

18.2.1 Work Control

Requirements not identified or incomplete – The risks and hazards associated with the work activity were not identified or were identified incompletely. For example, applicable standards and codes were not reviewed or the job site was not walked down prior to developing the work plan. As a result, controls for the risks/hazards were not incorporated into the work plan.

Work planning informal – The degree of deliberateness, formality and thoroughness in work planning and preparation was not commensurate with the risks/hazards the work entailed. For example, a work package was not developed for the job or was incomplete, resource requirements were not analyzed in advance, or timing requirements were not identified. As a result, the resources required to complete the work on time and safely were not available.

Approval process inadequate – Review and approval of the work plan was weak. For example, personnel not qualified to evaluate it reviewed the work plan, not all of the affected work groups reviewed the plan, or approval was not obtained or was obtained from an individual without the authority to do so. As a result, missing or conflicting elements in the work plan were not identified or risk implications of the work were not identified and addressed.

Authorization inadequate – Authorization to begin the work was not obtained or was obtained on the basis of conditions that had changed or ceased to exist by the time the job started. For example, despite requirements documented in procedures, taught in training and communicated as management expectations, an instrumentation and control technician did not call the control room for permission to power down a controller for testing. Or, a control room operator determined that another emergency operating procedure was applicable to the circumstances and began implementing it without authorization from the unit supervisor.

Implementation not controlled – The work was planned, approved and authorized, but was not performed in accordance with the work plan. For example, individuals without the proper authority changed the plan to accommodate unexpected circumstances.

Oversight inadequate – The amount or type of oversight of the work, including management, supervision or QA/QC, was less than the risks and hazards of the work warranted. As a result, for example, decisions were made without adequate authorization or errors were not caught and corrected.

Closeout inadequate – Documentation of the job was not completed or was completed incorrectly, required tests were not performed, lessons learned were not identified and communicated. As a result, for example, equipment was left in an inoperable condition following maintenance.

18.2.2 Coordination

Job conflicts – Work activities were scheduled in a manner that caused them to interfere with one another. For example, due to schedule slippage, two jobs were scheduled to work on the same component on the same shift.

Job combinations – Work activities that were scheduled concurrently had unanticipated and adverse consequences. For example, a component was taken out of service that operators needed to complete a scheduled tech spec surveillance. Or, all trains of safety system were inadvertently disabled at the same time.

Resources unavailable – The resources required to perform a job were not scheduled to be available when needed. For example, the same health physics technician was assigned to monitor two jobs concurrently on different units. Or, tools and equipment required for a job were in use on another job when needed.

Work untimely – Work activities or work products were not available when needed. For example, new drawings that were required to finish planning a construction job were three weeks late in being delivered from the engineering department.

18.2.3 Information Management

Documentation missing – Required information was not obtained or was not accessible when needed. For example, reference documentation needed to develop a new procedure had not been purchased from the vendor or could not be located.

Documentation inaccurate – Information about equipment, drawings, valve lists, or design basis documents, for example, was out-of-date or wrong. As a result, work packages were incomplete, procedures were incomplete or inaccurate, or training did not address required KSAs.

18.3 ADDITIONAL RESOURCES ON COORDINATION AND CONTROL

- *U.S. Code of Federal Regulations,* Part 50.65, Requirements for monitoring the effectiveness of maintenance at nuclear power plants, Title 10, Energy (revised periodically). Washington, DC: U.S. Government Printing Office.

- *U.S. Code of Federal Regulations,* Appendix B to Part 50, Quality assurance criteria for nuclear power plants and fuel reprocessing plants, Title 10, Energy (revised periodically). Washington, DC: U.S. Government Printing Office.

- U.S. Nuclear Regulatory Commission (1978). *Quality assurance program requirements (Operation)* (Regulatory Guide 1.33, Rev. 2). Washington, DC: U.S. Nuclear Regulatory Commission.

- U.S. Nuclear Regulatory Commission (1997). *Monitoring the effectiveness of maintenance at nuclear power plants* (Regulatory Guide 1.160, Rev. 2). Washington, DC: U.S. Nuclear Regulatory Commission.

- U.S. Nuclear Regulatory Commission (1985). *Quality assurance program requirements for nuclear power plants* (Regulatory Guide 1.28, Rev. 3). Washington, DC: U.S. Nuclear Regulatory Commission.

- U.S. Nuclear Regulatory Commission (2000). *Assessing and managing risk before maintenance activities at nuclear power plants* (Regulatory Guide 1.182). Washington, DC: U.S. Nuclear Regulatory Commission.

Appendix A

Glossary

Glossary of Terms

An **ability** is the combination of knowledge and skill required to perform a task correctly.

An **alarm system** is an automated system consisting of processing and display hardware and software, which processes or analyzes signals from plant sensors and alerts the operator via visual and/or auditory displays when monitored parameters deviate from specified limits (setpoints).

A **barrier** is any means used to protect personnel and equipment from hazards. There are two types: physical and management barriers. Examples of physical barriers are fences, guard rails around moving equipment, protective clothing and safety devices, or shields. Examples of management barriers are risk and hazard analyses, supervision, training, or procedures.

Barrier analysis is a root cause analysis method. It is performed once the basic facts of an event or human performance problem are understood and asks the question, "What physical or management barriers could have prevented this event or problem from occurring?"

A **causal factor** is any action or condition that occurred or existed prior to the initiation of an event and without which the event may not have occurred. The term "causal factor" is synonymous with the term "cause," and may refer to direct, contributing, programmatic or root causes.

Circadian rhythms are also known as "biological clocks" and are patterns in physiological functioning over the course of a day.

Cognitive performance refers to mental activities and includes perception, interpretation, judgment and decision-making.

A **communication error** is a failure in the exchange of information between a sender and receiver, in which the receiver fails to receive or interpret a message consistently with the sender's intended meaning. The failure can occur in creating and sending messages or in receiving and interpreting them.

Communication systems are physical systems that support communications, such as between personnel in the main control room, between the main control room and local sites within the plant, and across sites within the plant. The broad variety of communication media may be generally categorized as speech-based and computer-based systems.

Computer-based procedure system present plant procedures in computer-based, rather than paper-based, formats.

Computerized operator support systems use computer technology to support operators or maintenance personnel in situation assessment and response planning. They can monitor status and provide recommendations or warnings.

A test has **content validity** if the test items are directly related to job performance by ensuring they match the instructional objectives and are appropriately weighted.

A **control** is a mechanism used to regulate, and/or guide the operation of a component, equipment, subsystem, or system.

A **contributing cause** is an action or condition that sets the stage for the event to occur. A contributing cause may be a long-standing condition or a series of prior events that, while unimportant in themselves, increase the probability that the event would occur.

A **corrective action** is an action authorized by and under the control of management intended to solve problems identified as the result of an event investigation. Effective corrective actions for an event prevent the recurrence of the same or a similar event.

A **causal analysis** is a systematic method for evaluating the evidence gathered about an event from an event investigation. The purpose of a causal analysis is to identify the basic set of actions and conditions that, if eliminated or modified, would prevent the same event and similar events from happening again.

A **cursor** is a display graphic that is used to indicate the position of the user's operation on the display (such as an arrow or flashing bar).

A **direct cause of an event** is the actions or conditions immediately preceding the event that caused or allowed it to occur.

The **direct cause of an error** is the actions or conditions immediately preceding the error that caused or allowed the error to occur. Direct causes of errors are also known as **performance-shaping factors.**

A test has **discriminate validity** if it differentiates between workers who have mastered KSAs required to perform the job and those who have not.

A **display** is a specific integrated, organized set of information. A display can include several display formats (such as a system mimic which includes bar charts, trend graphs, and data fields).

A **display device** is the hardware used to present the display to users. Examples include video display units and speakers for system messages.

Display elements are the basic components used to make up display formats, such as abbreviations, labels, icons, symbols, coding, and highlighting.

Display format refers to the general class of information presentation. Examples of general classes are continuous text (such as a procedure display), mimics and piping and instrumentation diagram (P&ID) displays, trend graphs, and flowcharts.

A **display network** is a group of display pages within an information system and their organizational structure.

A **display page** is a defined set of information that is intended to be displayed as a single unit. Typical display pages in a nuclear power plant may combine several different formats on a single VDU screen, such as putting bar charts and digital displays in a graphic P&ID format. Display pages typically have a label and designation within the computer system so operators can assess them as a single display.

Documentary evidence includes paper and electronic information, such as records, reports, procedures, work orders, memoranda, and vendor manuals.

Evidence reliability refers to whether or not different investigators would be able to find the same information and reach the same conclusions from it. Conflicting stories from different interviewees is an example of unreliable evidence that requires further validation.

Evidence validity refers to the accuracy of the information gathered in the course of an investigation. Valid evidence is information gathered from more than one source that supports the "truth" of an assertion.

Functional requirements analysis and allocation is an analysis for identifying the plant's safety functional requirements and ensuring that the functions have been allocated to support an acceptable role for plant personnel.

A **general organizational improvement plan** is developed by plant or corporate senior management and is intended to make significant changes in how work is done and how it is managed in order to improve operational performance and to reverse declining performance trends.

The **Help** function in a software program refers to features that provide guidance to the user (e.g., describes how the user interface works).

HFE program is a plan for ensuring that HFE considerations will be integrated into the development, design, evaluation, and implementation of the HSI.

Housekeeping refers to activities performed to maintain a clean and orderly work environment.

HSI design is the systematic application of HFE principles and criteria to translate the user's function and task requirements into the details of the HSI design. It includes the

use of HFE tests, evaluations, guidelines, and design documentation in the development of the HSI design.

Human errors are inappropriate or inadequate human actions, including failures to take action when required.

Human factors is a body of scientific facts about human characteristics. The term covers all biomedical, psychological, and psychosocial considerations; it includes, but is not limited to, principles and applications in the areas of human factors engineering, personnel selection, training, job performance aids, and human performance evaluation.

Human factors engineering (HFE) is the application of knowledge about human capabilities and limitations to the design of a plant, system, and equipment. HFE ensures that such designs, human tasks, and work environment are compatible with the sensory, perceptual, cognitive, and physical attributes of the personnel who operate, maintain, and support them (See human factors).

A **human performance problem** is a term used to collectively refer to human errors and human performance trends.

A **human performance trend** is a pattern of related errors resulting from the same causal factor(s).

Human reliability analysis is an analysis of the human error mechanisms relevant to the design of the HSI, procedures, staffing, and training to reduce their likelihood and consequences.

Human-system interface (HSI) is the means through which personnel interact with the plant, including the alarms, displays, controls, and job-performance aids. Generically, this also includes maintenance, test, and inspection interfaces.

Impairment refers to decrements in cognitive and physical capabilities that are usually the result of substance abuse, fatigue, illness, stress or other factors that temporarily affect an individual's ability to perform tasks.

Information is organized data that users need to successfully perform their tasks. Information can include (a) a representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or automatic means; and (b) any representations, such as characters or analog quantities, to which meaning is, or might be, assigned.

Integrated system validation entails performance-based evaluations conducted to ensure that the integration of the HSI, procedures, and training adequately supports plant personnel in the safe operation of the plant.

An **intermediate corrective action plan** is more limited in scope than a general organizational improvement plan and focuses on erecting or strengthening barriers to human performance problems.

Investigation methods are the techniques used to gather evidence about an event. Investigation methods include establishing and pursuing lines of inquiry about the event by gathering physical, documentary and testamentary evidence.

A **job and task analysis (JTA)** is the process used to systematically determine the jobs that are assigned to workers and the tasks that must be performed in order to satisfactorily complete the job.

Just-in-time training is training that is provided to workers immediately prior to performing the job.

Knowledge is a set of facts, factual information, a method of analysis or the application of methods and facts to successfully perform a task.

KSAs are the knowledge, skills and abilities required for a job incumbent to safely and competently perform a job.

Labeling and marking refer to the use of labels and demarcations to identify units of equipment, modules, components, and parts.

Learning objectives provide a brief description of the training course material that must be taught by the training program to ensure mastery of all KSAs required to perform a certain job, task or to meet a training requirement.

Limited scope corrective action plans focus on fixing the direct cause of an error. For example, a limited scope corrective action for an ambiguous step in a procedure that confused a worker and caused her to commit an error would be to revise that step in the procedure.

A **local control station (LCS)** is an operator interface related to nuclear power plant process control that is not located in the main control room. This includes multifunction panels, as well as single-function LCSs, such as controls (e.g., valves, switches, and breakers) and displays (e.g., meters) that are operated or consulted during normal, abnormal, or emergency operations.

Maintainability refers to the design of equipment to support effective and efficient maintenance activities.

Managing displays refers to actions performed by a user to control the way that individual displays are presented on a device.

Managing errors refers to actions performed by a user to prevent, detect, or correct errors.

Managing information refers to the capabilities of software that allow the user to create, change, store, and retrieve documents via the computer.

Mastery is the process of achieving the requisite knowledge, skills and abilities to perform a job or task safely and competently.

A **mental lapse** is a momentary gap in recall for the correct knowledge or ability when it is required to perform a job.

National Nuclear Accrediting Board is a body of experts chartered by the Institute of Nuclear Power Operations (INPO) to review, accept and accredit the training programs at every nuclear power station.

An **operating experience review** is a review of relevant operating history from the plant's on-going collection, analysis, and documentation of operating experiences.

Operational validity ensures that test items address the mental and psychomotor activities that are performed on the job.

Performance-based training (PBT), also called the **Systematic Approach to Training**, includes the following five elements:

1. Systematic analysis of the jobs to be performed
2. Learning objectives derived from the analysis, which describe desired performance after training
3. Training design and implementation based on the learning objectives
4. Evaluation of trainee mastery of the objectives during training
5. Evaluation and revision of the training based on the performance of trained personnel in the job setting.

Personal protective equipment (PPE) is equipment worn by a worker to minimize exposure to specific occupational hazards. Examples of PPE are respirators, gloves, aprons, fall protection, and full body suits, as well as head, eye and foot protection.

Physical evidence is matter related to the event, such as equipment, parts, debris, liquids, hardware or tools.

Procedures development refers to the integration of HFE principles and criteria in a procedure development program to ensure that the resulting procedures: (1) support and guide human interaction with plant systems and plant-related events and activities, and (2) are technically accurate, comprehensive, explicit, easy to use, and validated.

A **programmatic cause** is a deficiency in one of the licensee's policies, programs and processes for managing work activities at a site that allows human errors to occur. For

example, a deficiency in a licensee's training program could set the stage for errors because workers may not have the knowledge or required skills to perform a job correctly.

The **root cause** of an event is the actions or set of conditions that, if eliminated or modified, would keep the event from recurring as well as prevent similar events from occurring. A root cause is often responsible for multiple human errors or hardware failures, rather than single problems or faults. Root causes are more fundamental causes than direct causes, and are typically programmatic or management weaknesses.

Root cause analysis is a structured, repeatable, systematic method for synthesizing information about an event and its causal factors to identify the critical set of conditions that, if eliminated or modified, would prevent the same event and similar events from recurring.

Service points are equipment locations used for performing routine maintenance tasks, such as adjusting, cleaning, or replacing components.

A loss of **situational awareness** occurs when a worker has mastered the relevant knowledge, but fails to recognize that the knowledge applies to the task at time of performance.

A **skill** is a motor or mental capability such as the ability to open a valve or operate a controller.

A **soft control** is a control device that has connections with the control or display system mediated by software rather than direct physical connections. As a result, the functions of a soft control may be variable and context-dependent rather than statically defined. Also, the location of a soft control may be virtual (e.g., within the display system structure) rather than spatially dedicated. Soft controls include devices activated from display devices (e.g., buttons and sliders on touch screens), multi-function control devices (e.g., knobs, buttons, keyboard keys, and switches that perform different functions depending upon the current condition of the plant, the control system, or the HSI), and devices activated via voice input.

Span of control refers to the personnel and functions for which a job incumbent has responsibility and authority. Higher management positions within an organization have broader spans of control.

Staffing is the process of accessing, maintaining and scheduling the personnel resources needed to accomplish work under normal and foreseeable off-normal conditions. Staffing decisions consider regulatory requirements, operating costs, the range of expertise required, the number of staff needed and scheduling.

A **staffing analysis** is a systematic analysis of the requirements for the number and qualifications of personnel based on an understanding of task and applicable regulatory requirements.

Stress is a psychological and physiological response to a threatening situation. A threatening situation is one that an individual has appraised as exceeding his or her capabilities to cope. Stressful situations, or **stressors**, may be emotional, cognitive, environmental or physiological.

System response refers to the manner in which the computer system behaves after receiving inputs from the user.

System security refers to features that restrict personnel access to aspects of the computer system to prevent accidental or deliberate damage.

Systematic Approach to Training (SAT) – See performance-based training.

Task analysis is a method of detailing the components of a task in terms of the demands placed upon the human operator, the information required by the operator, the extent to which the task requires reliance on or coordination with other personnel, and the relation of the task to other tasks.

The **task environment** refers to the physical conditions in which work is performed, such a noise and illumination levels, temperature, or radiation.

Task overload occurs when the number of tasks to be performed in a given period of time exceeds the available personnel resources. Task overload may increase stress and often results in the application of various work management strategies. These strategies may include task deferral, delegation or increasing the work pace, all of which may result in errors.

Testamentary evidence includes witness statements and the results of interviews.

Test equipment refers to diagnostic tools used to assess the status of equipment and locate faults that may be present.

Test points are equipment locations used for conducting tests to determine the operational status of equipment and for isolating malfunctions. Test equipment may be connected at these points.

Training development refers to the use of a systematic approach in the development of personnel training.

User-system interaction refers to the set of methods provided in a computer system through which personnel and the computer communicate with each other.

Validation is: (1) The process of determining whether the design of machine elements and the organizational design of human elements of a human-machine system are adequate to support effective integrated performance of established functions. (2) The capability of a system to check information entry items for correct content of format as defined by software logic.

Verification is the process of determining whether procedures, instrumentation, controls, and other equipment meet the specific requirements of the tasks performed by personnel. The term is used in the following contexts:

> **HSI task support verification**: The individual HSI components (e.g., control and display devices) and characteristics (range, accuracy, and safety grade) needed for the task are compared to those actually provided in the work environment.
>
> **HFE design verification**: The characteristics of the HSI, workplace, and HSI support functions are reviewed by the licensee to determine whether their design is consistent with accepted HFE principles, guidelines, and standards.
>
> **Human factors issue resolution verification**: A check to ensure that the HFE issues identified during the design process have been acceptably addressed and resolved.

A **workstation** is the physical console at which a user performs tasks.

Appendix B

Bibliography

BIBLIOGRAPHY

ABS Consulting, Inc. (2001). *Root cause leader.* http://www.jbfa.com/rootcauseleader.html.

Apollo Associated Services (2001). *Apollo method of root cause analysis.* http://www.apollo-as.com.

Baker, K., Olson, J. and Morisseau, D. (1994). Work practices, fatigue, and nuclear power plant safety performance. *Human Factors, 36,* 244-257.

Baker, T. (1995). *Alertness, performance and off-duty sleep on 8-hour and 12-hour night shifts in a simulated continuous operations control room setting* (NUREG/CR-6046). Washington, DC: U.S. Nuclear Regulatory Commission.

Barnes, V.E., Fleming, I., Grant, T., Hauth, J., Hendrickson, J., Kono, B., Moore, C., Olson, J. Saari, L., Toquam, J., Wieringa, D., Yost, P., Hendrickson,P., Moon, D and Scott, W. (1988). *Fitness for duty in the nuclear power industry: A review of technical issues* (NUREG/CR-5227). Washington, DC: U.S. Nuclear Regulatory Commission.

Barnes, V.E., Moore, C.J. Wieringa, D.R., Isakson, C.S., Kono, B.K. and Gruel, R.L. (1989) *Techniques for preparing flowchart-format emergency operating procedures: Vol.s 1 and 2* (NUREG/CR-5228, PNL-6653, BHARC-700/88/017). Washington, DC: U.S. Nuclear Regulatory Commission.

Barnes, V. E., Mumaw, R. J. and Schoenfeld, I. (1996). Communication errors in nuclear power plants. In *Proceedings of the 1996 American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies.* American Nuclear Society: La Grange Park, IL, 671-678.

Beedle, Wayne. (1996). Accident investigation: The ergonomic eye. *Occupational Health and Safety Canada, 12,* 36-38.

Benner, L., Jr. (1985). Rating accident models and investigation methodologies. *Journal of Safety Research, 16,* 105-126.

Bird, F. E. and Germain, G. L. (1985, revised 1990). *Practical loss control leadership.* Loganville, Georgia: International Loss Control Institute/DeNorske Veratis).

Bowers, C.A., Jentsch, F., Salas E. and Braun, C.C. (1998). Analyzing communication sequences for team training needs assessment. *Human Factors, 40,* 672-679.

Brown, W.S., Higgins, J.C., O'Hara, J.M. (1994). *Local control stations: Human engineering issues and insights* (NUREG/CR-6146). Washington, DC: U.S. Nuclear Regulatory Commission.

Brown, W.S., O'Hara, J.M. and Higgins, J.C. (2000). *Advanced alarm systems: Revision of guidance and its technical basis* (NUREG/CR-6684). Washington, DC: U.S. Nuclear Regulatory Commission.

Byers, J.C., Hill, S.G and Rothblum, A.M. (1994). *U.S. Coast Guard marine casualty investigation and reporting: Analysis and recommendations for improvement, interim report.* (Report No. CG-D-13-95). National Technical Information Service: Springfield, Virginia.

Cantarella, A. (1997). Incident investigations: Critical to the safety effort. *Professional Safety, 42,* 10.

Corcoran, W.R. (1999). *The thirteen steps of a world class corrective action program.* Windsor, CT: Nuclear Safety Review Concepts.

Decision Systems, Inc. (2001). *REASON root cause analysis.* http://www.rootause.com

Dew, J.R. (1991). In search of the root cause. *Quality Progress, 24,* 97-102.

Durbin, N. and Grant, T. (1996). *Fitness for duty in the nuclear industry: Update of the technical issues 1996* (NUREG/CR-6470, BSRC-700/96/004, PNNL-11134). Washington, DC: U.S. Nuclear Regulatory Commission.

Durbin, N., Moore, C. Grant, T., Fleming, T., Hunt, P., Martin, R. Murphy, S., Hauth, J. Wilson, R., Bittner, A., Bramwell, A., Macauley, J., Olson, J., Terrill, E. and Toquam, J. (1991). *Fitness for duty in the nuclear power industry: A review of the first year of program performance and an update of the technical issues* (NUREG/CR-5784, PNL-7795, BHARC-700/91/025). Washington, DC: U.S. Nuclear Regulatory Commission.

Echeverria, D., Barnes, V., Bittner, A., Durbin, N., Fawcett-Long, J., Moore, C., Slavich, A. Terrill, B., Westra, C., Wieringa, D., Wilson, R., Draper, D., Morisseau, D. and Persensky, J. (1994). *The impact of environmental conditions on human performance: A handbook of environmental exposures* (NUREG/CR-5680, Vol.s 1 and 2). Washington, DC: U.S. Nuclear Regulatory Commission.

Enconet Consulting, Inc. (2001). *ERCAP.* http://www.enconet.com/pages/ercap.htm

Failsafe Network, Inc. (2001). *Root cause discovery.* http://www.failsafe-network.com

Ferry, T. S. (1990). *Modern accident investigation and analysis.* New York: John Wiley and Sons, Inc.

Fiedler, F.E. (1967). *A theory of leadership effectiveness.* New York: McGraw-Hill, 1967.

Fullwood, R. (2000). *Probabilistic safety assessment in the chemical and nuclear industries.* Boston, MA: Butterworth-Heinemann.

Gross, M. & Ayres, T. (1998). Research initiative for human performance management of nuclear power. Paper presented at the *IEEE Workshop: R&D for Cost Reduction.* Fukuoka, Japan: September 30-October 1.

Haber et al. (1995). *Nuclear Power Plant Shift Staffing Levels: Site Data Collection Report* (Accession No. 9510030160). Upton, NY: Brookhaven National Laboratory.

Hallbert, B.P., Sebok, A. and Morisseau, D. (2000). *A study of control room staffing levels for advanced reactors* (NUREG/IA-0137). Washington, DC: U.S. Nuclear Regulatory Commission.

Hendrick, H. and Kleiner, B. (2001). *Macroergonomics: An introduction to work system design.* Santa Monica, CA: Human Factors and Ergonomics Society.

Howlett, H.C. (1995). *The industrial operator□s handbook: A systematic approach to industrial operations*. Pocatello, ID: Techstar.

Higgins, J. and Nasta, K. (1997). *Human factors engineering (HFE) insights for advanced reactors based upon operating experience (*NUREG/CR-6400). Washington, DC: U.S. Nuclear Regulatory Commission.

Institute of Electrical and Electronics Engineers (1999). *IEEE guide for the evaluation of human-system performance in nuclear power generating stations (*IEEE Standard 845-1999). New York: Institute of Electrical and Electronics Engineers

Joint Commission on Accreditation of Healthcare Organizations (1996). *Conducting a root cause analysis in response to a sentinel event.* Oakbrook Terrace, IL: Joint Commission on Accreditation of Healthcare Organizations.

Joint Commission on Accreditation of Healthcare Organizations (2001). *Sentinel events.* http://www.jcaho.org/sentinel/sentevnt_frm.html

Jorgensen, Ernest B. (1990). Accident investigations for simple people like me. *Professional Safety, 35*, 31.

Kirwan, B. (1994). *A guide to practical human reliability assessment.* Bristol, PA: Taylor & Francis.

Klein G., Orasanu J., Calderwood R. and Zsambok, E. (Ed.s) (1993). *Decision making in action: Models and methods.* Norwood, New Jersey: Ablex Publishing.

Landy, F. and Trumbo, D. (1976). *Psychology of work behavior.* Homewood, IL: The Dorsey Press .

Loftus, E. (1996). *Eyewitness testimony.* Harvard University Press.

Loftus, E.F., Miller, D.G. and Burns H.J. (1978). Semantic integration of verbal information into a visual memory. *Journal of Experimental Psychology: Human Learning and Memory, 4*, 19-31.

Managerial Technology Corporation (2001). *Risk Management Internet Services*, http://www.rmis.com

Marx, D. (2001). *The causation trainer.* http://www.causationtrainer.com

McCallum, M.C., Raby, M. and Roghblum, A. (1996). *Procedures for investigating and reporting human factors and fatigue contributions to marine casualties*. (Report No. CG-D-09-97). National Technical Information Service: Springfield, Virginia.

Medical Risk Management Associates, LLC (2001). *Sentinel events and root cause analysis in healthcare.* http://www.rootcauseanalyst.com

Merritt, A.C. and Helmreich, R.L. (1996). Creating and sustaining a safety culture. *CRM Advocate, 1*, 8-12.

Meyer, O., Hill, S. and Steinke, W. (1993). *Studies of human performance during operating events, 1990-1992* (NUREG/CR-5953). Washington, DC: U.S. Nuclear Regulatory Commission.

Miller, M.C. (1992). *Root Cause Analysis Methodology* (NTIS ID No. AD-A256 855, Report No. CRDEC-SP-053). National Technical Information Service: Springfield, VA.

Moore, C., Barnes, V., Hauth, J., Wilson, R., Fawcett-Long, J., Toquam, J., Baker, K., Wieringa, D., Olson, J., & Christensen, J. (1989). *Fitness for duty in the nuclear power industry: A review of technical issues* (NUREG/CR-5227, Supplement 1, PNL-6652, BHARC-700/88/018). Washington, DC: U.S. Nuclear Regulatory Commission.

Morgenstern, M., Barnes, V., McGuire, M., Radford, L. and Wheeler, W. (1985) *Operating procedures in nuclear power plants: Practices and problems* (NUREG/CR-3968, PNL-5648). Washington, DC: U.S. Nuclear Regulatory Commission.

Morgenstern, M., Barnes, V., Radford, L., Wheeler, W. and Badalamente, R. (1984). *The development, use and control of maintenance procedures in nuclear power plants: Problems and recommendations* (NUREG/CR-3817, PNL-5121). Washington, DC: U.S. Nuclear Regulatory Commission.

Mumaw, R.J. (1994). *The effects of stress on nuclear power plant operational decision making and training approaches to reduce stress effects* (NUREG/CR-6127). Washington, DC: U.S. Nuclear Regulatory Commission.

Mumaw, R., Swatzler, D., Roth, E. and Thomas, W. (1994). *Cognitive skill training for nuclear power plant operational decision making* (NUREG/CR-6126). Washington, D.C.: U.S. Nuclear Regulatory Commission.

Muschara, T. (2000). INPO Human Performance Evaluations and Other Developments. In *Proceedings of the 2000 Human Performance Root Cause Trending Workshop*. Philadelphia, PA: June 12-15, 2000.

Nelms, R. (2001). *Root cause live.* http://www.rootcauselive.com

Norman, D. (1981). Categorization of action slips. *Psychological Review, 88,* 1-15.

O'Hara et al. (1999). The development of guidance for the review of plant modifications involving risk-important human actions (BNL Letter Report W6022-T2-1-11/99). Upton, New York: Brookhaven National Laboratory.

O'Hara, J.M., Brown, W.S., Baker, C.C., Welch, D.L., Granda, T.M. and Vingelis, J.P. (1994). *Advanced human-system interface design review guideline: Evaluation procedures and guidelines for human factors engineering reviews* (NUREG/CR-5908, Vol. 2). Washington, DC: U.S. Nuclear Regulatory Commission.

O'Hara, J.M., Brown, W.S., Higgins, J.C. and Stubler, W.F. (1994). *Human Factors Engineering Guidance for the Review of Advanced Alarm Systems* (NUREG/CR-6105). Washington, DC: U.S. Nuclear Regulatory Commission.

O'Hara, J., Higgins, J., Stubler, W., Goodman, C., Eckenrode, R., Bongarra, J., and Galletti, G. (1994). *Human factors engineering program review model* (NUREG-0711). Washington, DC: U.S. Nuclear Regulatory Commission.

O'Hara, J.M., Higgins, J.C., Stubler, W.C. and Kramer, J. (2000). *Advanced information systems design: Technical basis and human factors review guidance* (NUREG/CR-6633). Washington, DC: U.S. Nuclear Regulatory Commission.

O'Hara, J.M., Higgins, J.C., Stubler, W.F. and Kramer, J. (2000). *Computer-based procedure systems: Technical basis and human factors review guidance* (NUREG/CR-6634). Washington, DC: U.S. Nuclear Regulatory Commission.

Orion Healthcare Technologies, Inc. (2001). *Root cause analyst.* http://www.rcasoftware.com

Paradies, M., Unger, L., Haas, P. and Terranova, M. (1993). *The NRC's human performance investigation process* (NUREG/CR-5455, Vol.s 1-3). Washington, DC: U.S. Nuclear Regulatory Commission.

Pedrali, M. and Cojazzi, G. (1994). A methodological framework for root cause analysis of human errors. In *Proceedings of the 21st Conference on Aviation Psychology: Developing Theory and Extending Practice*, Dublin (IE), March 28-31, 1994.

Peters, V. (May 24, 1995). Personal communication.

Reliability Center, Inc. (2001). *PROACT root cause analysis software.* http://www.reliability.com/proact.htm

Reason, J.T. (1990). *Human error.* Cambridge: Cambridge University Press.

Reason, J.T. (1997). *Managing risks of organizational accidents.* Burlington, VT: Ashgate Publishing.

Roth, E.M., Mumaw, R.J. and Lewis, P.M. (1994). *An empirical investigation of operator performance in cognitively demanding simulated emergencies* (NUREG/CR-6208). Washington, DC: U.S. Nuclear Regulatory Commission.

Sayers, D. (1994). Accident investigations. *Occupational Health and Safety Canada, 10,* S12-S15.

Schacter, D. (Ed.) (1997). *Memory distortion: how minds, brains, and societies reconstruct the past.* Harvard University Press.

Senecal, P. (1994). Root cause analysis: What took us so long? *Occupational Hazards, 56,* 63-65.

Shurberg, D et al. (1994). *Identification of Issues Associated with Nuclear Power Plant Shift Staffing Levels, Task 1 Letter Report* (Accession No. 951003074). Upton, NY: Brookhaven National Laboratory.

Steinmeyer, P. (2001). *Manual of respiratory protection against airborne radioactive material* (NUREG/CR-0041, Rev. 1). Washington, DC: U.S. Nuclear Regulatory Commission.

Stephenson, J. (1991). *System safety 2000: A practical guide for planning, managing, and conducting system safety programs.* New York: Van Nostrand Reinhold.

Stubler, W.F., Higgins, J.C. and Kramer, J. (2000). *Maintainability of digital systems: Technical basis and human factors review guidance* (NUREG/CR-6636). Washington, DC: U.S. Nuclear Regulatory Commission.

Stubler, W.F., O'Hara, J.M., and Kramer, J. (2000). *Soft controls: Technical basis and human factors review guidance* (NUREG/CR-6635). Washington, DC: U.S. Nuclear Regulatory Commission.

Stubler, W.F., O'Hara, J.M., Higgins, J.C. and Kramer, J. (2000). *Human Systems Interface and Plant Modernization Process: Technical Basis and Human Factors Review Guidance* (NUREG/CR-6637). Washington, DC: U.S. Nuclear Regulatory Commission.

Svenson, O. and Maule, A. J. (Ed.s) (1993). *Time pressure and stress in human judgment and decision making.* New York: Plenum Press.

Swartz, G. (1993). Incident report: A vital part of quality safety programs. *Professional Safety, 38*, 32-34.

System Improvements, Inc. (2001). *TapRoot - Changing the way the world solves problems.* http://www.taproot.com

Texaco, Inc. (1994). Root cause analysis in practice. *Environmental Manager, 6*, 8-10.

ThinkReliability, Inc. (2001). *Cause mapping.* http://www.causemapping.com

Thomen, J. (1996). Root cause: Holy grail or fatal trap? *Professional Safety, 41*, 31.

Tritsch, S. (1992). Accident investigations: How to ask why. *Safety and Health, 146*, 40-43.

Unwin Company (2001). *Root cause analysis and incident investigation.* http://www.unwin-co.com/IncidentInv.cfm

Urian, R. (2000). Organizational unlearning: Detrimental behaviors present in chemical process incident investigation teams. In *Proceedings of Process Industry Incidents: Investigation Protocols, Case Histories, Lessons Learned.* New York: American Institute of Chemical Engineers, 341-362.

U.S. Code of Federal Regulations, Part 11, Criteria and procedures for determining eligibility for access to or control over special nuclear material, Title 10, Energy (revised periodically). Washington, DC: U.S. Government Printing Office.

U.S. Code of Federal Regulations, Part 19.20, Employee protection, Title 10, Energy (revised periodically). Washington, DC: U.S. Government Printing Office.

U.S. Code of Federal Regulations, Part 26, Fitness for duty programs, Title 10, Energy (revised periodically). Washington, DC: U.S. Government Printing Office.

U.S. Code of Federal Regulations, Part 50.54(m), Conditions of licenses, Title 10, Energy (revised periodically). Washington, DC: U.S. Government Printing Office.

U.S. Code of Federal Regulations, Part 50.65, Requirements for monitoring the effectiveness of maintenance at nuclear power plants, Title 10, Energy (revised periodically). Washington, DC: U.S. Government Printing Office.

U.S. Code of Federal Regulations, Part 50.120, Training and qualification of nuclear power plant personnel, Title 10, Energy (revised periodically). Washington, DC: U.S. Government Printing Office.

U.S. Code of Federal Regulations, Appendix B to Part 50, *Quality assurance criteria for nuclear power plants and fuel reprocessing plants*, Criterion V, Instructions, procedures and drawings, Title 10, Energy (revised periodically). Washington, DC: U.S. Government Printing Office.

U.S. Code of Federal Regulations, Appendix R to Part 50, *Quality assurance criteria for nuclear power plants and fuel reprocessing plants,* Criterion III (H), Fire brigade, Title 10, Energy (revised periodically). Washington, DC: U.S. Government Printing Office.

U.S. Code of Federal Regulations, Part 55.4, Operators licenses (definitions), Title 10, Energy (revised periodically). Washington, DC: U.S. Government Printing Office.

U.S. Department of Energy (1998). *Conducting accident investigations, Revision 2, a DOE Workbook*. Germantown, MD: U.S. Department of Energy. http://tis.eh.doe.gov/oversight/missions/air/air_overview.html

U.S. Nuclear Regulatory Commission (1978). *Quality assurance program requirements (Operation)* (Regulatory Guide 1.33, Rev. 2). Washington, DC: U.S. Nuclear Regulatory Commission.

--- (1980). *TMI action plan* (NUREG-0737). Washington, DC: U.S. Nuclear Regulatory Commission.

--- (1982). *Nuclear power plant staff working hours* (Generic Letter 82-12). Washington, DC: U.S. Nuclear Regulatory Commission.

--- (1982). *NUREG-0737 technical specifications* (Generic Letter 82-16). Washington, DC: U.S. Nuclear Regulatory Commission.

--- (1982). *Guidelines for the preparation of emergency operating procedures* (NUREG-0899). Washington, DC: U.S. Nuclear Regulatory Commission.

--- (1983). *NUREG-0737 technical specifications* (Generic Letter 83-02). Washington, DC: U.S. Nuclear Regulatory Commission.

--- (1983). *Clarification of TMI action plan requirements* (NUREG-0737, Supplement 1). Washington, DC: U.S. Nuclear Regulatory Commission.

--- (1985). *Quality assurance program requirements for nuclear power plants* (Regulatory Guide 1.28, Rev. 3). Washington, DC: U.S. Nuclear Regulatory Commission.

--- (1988). *Memorandum of understanding between NRC and OSHA relating to NRC-licensed facilities* (Information Notice 88-100). Washington, DC: U.S. Nuclear Regulatory Commission.

--- (1989). *Fitness for duty in the nuclear power industry: Responses to public comments* (NUREG-1354). Washington, DC: U.S. Nuclear Regulatory Commission.

--- (1989). *Lessons learned from the special inspection program for emergency operating procedures* (NUREG-1358). Washington, DC: U.S. Nuclear Regulatory Commission.

--- (1989). *Fitness for duty in the nuclear power industry: Responses to implementation questions* (NUREG-1385). Washington, DC: U.S. Nuclear Regulatory Commission.

--- (1991). *Nuclear plant staff working hours* (Information Notice 91-36). Washington, DC: U.S. Nuclear Regulatory Commission.

--- (1991). *Shift staffing at nuclear power plants* (Information Notice 91-77). Washington, DC: U.S. Nuclear Regulatory Commission.

--- (1992). *Shutdown and low-power operation at commercial nuclear power plants in the United States* (NUREG-1449). Washington, DC: U.S. Nuclear Regulatory Commission.

--- (1993). *Training review criteria and procedures* (NUREG-1220, Rev.1). Washington, DC: U.S. Nuclear Regulatory Commission.

--- (1994). *Human factors engineering program review model* (NUREG-0711). Washington, DC: U.S. Nuclear Regulatory Commission.

--- (1995). *Results of shift staffing study* (Information Notice 95-48). Washington, DC: U.S. Nuclear Regulatory Commission.

--- (1996). *Nuclear power plant simulation facilities for use in operator license examinations* (Regulatory Guide 1.149, Rev. 2). Washington, DC: U.S. Nuclear Regulatory Commission.

--- (1996). *Suggested guidance relating to development and implementation of corrective action programs* (Information Notice 96-28). Washington, DC: U.S. Nuclear Regulatory Commission.

--- (1996). *Human-system interface design review guideline* (NUREG-0700, Rev. 1, Vol.s 1-3). Washington, DC: U.S. Nuclear Regulatory Commission.

--- (1996). *Standard review plan for the review of safety analysis reports for nuclear power plants* (NUREG-0800). Washington, DC: U.S. Nuclear Regulatory Commission.

--- (1997). *Monitoring the effectiveness of maintenance at nuclear power plants* (Regulatory Guide 1.160, Rev. 2). Washington, DC: U.S. Nuclear Regulatory Commission.

--- (1997). *Evaluation criteria for communications-related corrective action plans* (NUREG-1545). Washington, DC: U.S. Nuclear Regulatory Commission.

--- (1998). *Medical evaluation of licensed personnel at nuclear power plants* (Regulatory Guide 1.134, Rev. 3). Washington, DC: U.S. Nuclear Regulatory Commission.

--- (1998). *Potential for degradation of the emergency core cooling system and the containment spray system after a loss-of-coolant accident because of construction and protective coating deficiencies and foreign material containment* (Generic Letter 98-04). Washington, DC: U.S. Nuclear Regulatory Commission.

--- (1998). *Knowledge and abilities catalog for nuclear power plant operators: Pressurized water reactors* (NUREG-1122, Rev. 2). Washington, DC: U.S. Nuclear Regulatory Commission.

--- (1998). *Knowledge and abilities catalog for nuclear power plant operators: Boiling water reactors* (NUREG-1123, Rev. 2). Washington, DC: U.S. Nuclear Regulatory Commission.

--- (1999). *Acceptable programs for respiratory protection* (Regulatory Guide 8.15, Rev. 1). Washington, DC: U.S. Nuclear Regulatory Commission.

--- (1999). *Operator licensing examination standards for power reactors* (NUREG-1021). Washington, DC: U.S. Nuclear Regulatory Commission.

--- (2000). *Medical misadministrations caused by human errors involving gamma stereotactic radiosurgey (gamma knife)* (Information Notice 2000-22). Washington, DC: U.S. Nuclear Regulatory Commission.

--- (2000). *Qualification and training of personnel for nuclear power plants* (Regulatory Guide 1.8, Rev. 3). Washington, DC: U.S. Nuclear Regulatory Commission.

--- (2000). *Assessing and managing risk before maintenance activities at nuclear power plants* (Regulatory Guide 1.182). Washington, DC: U.S. Nuclear Regulatory Commission.

--- (2000). *Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA)* (NUREG-1624, Rev. 1). Washington, DC: U.S. Nuclear Regulatory Commission.

--- (2001). *Fitness for duty.* http://www.nrc.gov/NRC/REACTOR/FFD

--- (2001). *Human factors information system (HFIS) database reports homepage.* *http://www.nrc.gov/NRR/HFIS/index.htm*

--- (2001). *Operator licensing program.* http://www.nrc.gov/NRC/REACTOR/OL/OLhome.html

West, S. and Wicklund, R. (1980). *A primer of social psychological theories.* Monterey, CA: Brooks/Cole Publishing Company.

Wieringa, D., Moore, C. and Barnes, V. (1998). *Procedure writing: Principles and practices, second edition.* Columbus, OH: Battelle Press.

Wilpert, B., Uth, H.J., Miller, R. and Ninov, E. (2000). Safety management through learning from experience in the chemical industry: Example of a new incident analysis methodology. In *Proceedings of Process Industry Incidents: Investigation Protocols, Case Histories, Lessons Learned*. New York: American Institute of Chemical Engineers, 303-312.

Woods, D.D., Pople, H.E., Jr. and Roth, E.M. (1990). *The cognitive environment simulation as a tool for modeling human performance and reliability* (NUREG/CR-5213, Vols. 1 and 2). Washington, DC: U.S. Nuclear Regulatory Commission.

APPENDIX C

BLANK REVIEW TABLES

Table 2.1 Problem Identification and Characterization

Document Identifier:		Problem Number: __		Problem Number: __	
Question Number	Brief description of the problem and date(s) of occurrence:				
2.1.1	Was the human performance problem identified?	Yes No NA	Notes:	Yes No NA	Notes:
2.1.2	If not, was the human performance problem tangential to understanding and resolving the issue under review?	Yes No NA		Yes No NA	
2.1.3	Were the individuals involved in the problem identified (by job role)?	Yes No NA		Yes No NA	
2.1.4	Were the actions and decisions or failures to act that comprised the problem described?	Yes No NA		Yes No NA	
2.1.5	Were precursor errors or earlier evidence of a developing trend identified?	Yes No NA		Yes No NA	
2.1.6	Was the problem described in enough detail to support causal analyses and the development of corrective actions?	Yes No NA		Yes No NA	

Notes:

Total number of Yes's: ____

Total number of NA's: ____

Table 2.2 Investigation Methods

Question Number	Problem description:	Problem Number: __		Problem Number: __	
2.2.1	Was the extent of the investigation consistent with the importance of the problem?	Yes No NA	Notes:	Yes No NA	Notes:
2.2.2	Were licensee criteria for determining which issues require an investigation appropriately applied to this problem?	Yes No NA		Yes No NA	
2.2.3	Did the licensee validate the information gathered about the problem by seeking information from more than one source?	Yes No NA		Yes No NA	
2.2.4	Did the licensee seek the appropriate type(s) of evidence for investigating the problem?	Yes No NA		Yes No NA	
2.2.5	Did the licensee gather enough information to understand the sequence of events and conditions leading up to the problem?	Yes No NA		Yes No NA	

Notes:

Total number of Yes's: ____

Total number of NA's: ____

Table 2.2 Investigation Methods (continued)

Question Number	Problem description:	Problem Number: __		Problem Number: ___	
2.2.6	Did the licensee check plant records to identify other problems that occurred during the same work activity?	Yes No NA	Notes:	Yes No NA	Notes:
2.2.7	Did the licensee identify the programs that applied to the job(s) during which the human performance problem arose?	Yes No NA		Yes No NA	
2.2.8	If the licensee found weaknesses in the applicable programs, were the weaknesses investigated in sufficient detail to understand their scope and likely effects, if not corrected?	Yes No NA		Yes No NA	
2.2.9	Were the licensee's conclusions clearly supported by the results of the investigation?	Yes No NA		Yes No NA	
2.2.10	Was there a basis documented for stopping the investigation?	Yes No NA		Yes No NA	

Notes:

Total number of Yes's: ____

Total number of NA's: ____

Table 2.3 Causal Analyses

Question Number	Problem description:	Problem number: __		Problem Number: __	
2.3.1	Were causal factors identified for this human performance problem?	Yes No NA	Notes:	Yes No NA	Notes:
2.3.2	Was more than one causal factor identified for the problem?	Yes No NA		Yes No NA	
2.3.3	Was the type of causal analysis of this problem consistent with its importance?	Yes No NA		Yes No NA	
2.3.4	Was there enough information provided to verify the accuracy of the causal factors identified?	Yes No NA		Yes No NA	
2.3.5	Were several possible causes for the problem investigated?	Yes No NA		Yes No NA	
2.3.6	Did the evidence support the licensee's choice of causes?	Yes No NA		Yes No NA	
2.3.7	Were the bases for rejecting possible causes for the problem documented?	Yes No NA		Yes No NA	

Notes:

Total number of Yes's: ____

Total number of NA's: ____

Table 2.3 Causal Analyses (continued)

Question Number	Problem description:	Problem Number: __		Problem Number: __	
2.3.8	Did the licensee analyze programmatic weaknesses to determine if they could account for more than one human performance problem?	Yes No NA	Notes:	Yes No NA	Notes:
2.3.9	Did the licensee perform and document a root cause analysis using systematic root cause analysis techniques?	Yes No NA		Yes No NA	
2.3.10	Was more than one root cause analysis technique used?	Yes No NA		Yes No NA	
2.3.11	Was the rationale for terminating the root cause analysis sufficient and documented?	Yes No NA		Yes No NA	
2.3.12	Were the root causes identified under management control?	Yes No NA		Yes No NA	
2.3.13	If corrected, would the causes identified reduce the likelihood of the same and similar problems from happening again?	Yes No NA		Yes No NA	

Notes:

Total number of Yes's: ____

Total number of NA's: ____

Table 2.4 Corrective Actions

Question Number	Problem description:	Problem Number: __		Problem Number: __	
2.4.1	Were corrective actions for the human performance problem identified?	Yes No NA	Notes:	Yes No NA	Notes:
2.4.2	Were the corrective actions effective, or appear likely to be effective, even if no causal analysis was performed and/or documented?	Yes No NA		Yes No NA	
2.4.3	If a causal analysis was performed, were the links between the causal factors and the corrective actions clear?	Yes No NA		Yes No NA	
2.4.4	Was there a corrective action for every causal factor? (a one-to-one correspondence is not required)	Yes No NA		Yes No NA	
2.4.5	Was the scope of the corrective action plan appropriate?	Yes No NA		Yes No NA	
2.4.6	Were the desired condition(s) that the corrective actions are intended to create clearly described?	Yes No NA		Yes No NA	

Notes:

Total number of Yes's: ____

Total number of NA's: ____

Table 2.4 Corrective Actions (continued)

Question Number	Problem description:	Problem Number: __		Problem Number: __	
2.4.7	Did the licensee define measurable objectives to be achieved from the corrective actions?	Yes No NA	Notes:	Yes No NA	Notes:
2.4.8	Did the licensee define evaluation and acceptance criteria for assessing corrective action effectiveness?	Yes No NA		Yes No NA	
2.4.9	Did the licensee define an implementation process for the corrective actions and specific performance indicators for evaluating success?	Yes No NA		Yes No NA	
2.4.10	Did the licensee assign responsibility to specific, qualified individuals for implementing the corrective actions?	Yes No NA		Yes No NA	
2.4.11	Did the licensee develop a plan for on-going monitoring of continued acceptable performance?	Yes No NA		Yes No NA	
2.4.12	Did the licensee review the corrective actions before implementation to ensure that they will not cause unintended negative consequences?	Yes No NA		Yes No NA	

Notes:

Total number of Yes's: ____

Total number of NA's: ____

Table 2.5 Summary Review Table				
A. Number of human performance problems reviewed = ____	**Tables**			
	2.1 Problem Identification and Characterization	**2.2 Investigation Methods**	**2.3 Causal Analyses**	**2.4 Corrective Actions**
Number of questions in each table	6	10	13	12
B. Multiply the number of questions in each table by the total number of problems reviewed	6 X ___=(B)____	10 X ___=(B)____	13 X ___=(B)____	12 X ___=(B)____
C. Record the total number of Yes answers circled from each table	(C) = ____	(C) = ____	(C) = ____	(C) = ____
D. Record the total number of NA answers circled from each table	(D) = ____	(D) = ____	(D) = ____	(D) = ____
E. Subtract the total in Row D from the total in Row B	(B)____-(D)____=(E)____	(B)____-(D)____=(E)____	(B)____-(D)____=(E)____	(B)____-(D)____=(E)____
F. Divide the answer in Row C by the answer in Row E	(C)____/(E) ____=(F)____	(C)____/(E) ____=(F)____	(C)____/(E)____=(F)____	(C)____/ (E)____=(F)____
G. Multiply the answer in Row F by 100 to obtain the percentage of Yes answers circled in each review table	(F)____X 100 = ____%	(F)____X 100 = ____%	(F)____X 100 = ____%	(F)____X 100 = ____%
Notes:				

NRC FORM 335 (2-89) NRCM 1102, 3201, 3202

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

(See instructions on the reverse)

1. REPORT NUMBER (Assigned by NRC, Add Vol., Supp., Rev., and Addendum Numbers, if any.)

NUREG/CR-6751

2. TITLE AND SUBTITLE

THE HUMAN PERFORMANCE EVALUATION PROCESS: A Resource for Reviewing the Identification and Resolution of Human Performance Problems

3. DATE REPORT PUBLISHED

MONTH: March YEAR: 2002

4. FIN OR GRANT NUMBER

W6528

5. AUTHOR(S)

V. E. Barnes, B. C. Haagensen, J. M. O'Hara

6. TYPE OF REPORT

Technical

7. PERIOD COVERED *(Inclusive Dates)*

6-23-97 to 11-30-01

8. PERFORMING ORGANIZATION - NAME AND ADDRESS *(If NRC, provide Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address; if contractor, provide name and mailing address.)*

Performance, Safety and Health Associates, Inc.
P.O. Box 30
Boalsburg, PA 16827

9. SPONSORING ORGANIZATION - NAME AND ADDRESS *(If NRC, type "Same as above"; if contractor, provide NRC Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address.)*

Division of Systems Analysis and Regulatory Effectiveness
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

10. SUPPLEMENTARY NOTES

E. A. Trager, I. Schoenfeld, NRC Project Managers

11. ABSTRACT *(200 words or less)*

The Human Performance Evaluation Process (HPEP) is a resource for U.S. Nuclear Regulatory Commission inspectors to use when reviewing licensee problem identification and resolution programs with regard to human performance. Part I provides a step-by-step process for reviewing licensee effectiveness in identifying, analyzing and resolving human performance problems. Part I also addresses the challenges in identifying and investigating human performance problems, describes three root cause analysis techniques, and discusses characteristics of effective corrective action plans. Part II is comprised of the HPEP Cause Tree and Modules. The Cause Tree is a screening tool for identifying the range of possible causes for a human performance problem. The Modules describe frequently identified causes for human performance problems and provide examples. Part II is intended to support the evaluation of licensee root cause analyses for human performance problems identified in Part I.

12. KEY WORDS/DESCRIPTORS *(List words or phrases that will assist researchers in locating the report.)*

Human performance, human error, root cause analysis, corrective action plans, events and causal factors, barrier analysis, change analysis, performance shaping factors, event investigations

13. AVAILABILITY STATEMENT

unlimited

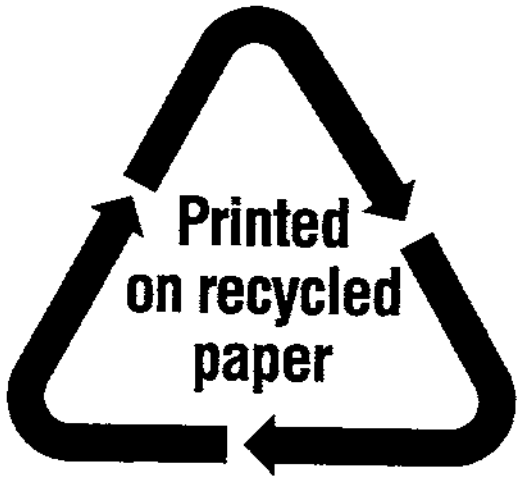
14. SECURITY CLASSIFICATION

(This Page) unclassified

(This Report) unclassified

15. NUMBER OF PAGES

16. PRICE



Federal Recycling Program

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, DC 20555-0001

NRI-4 (2014)

ECFA+

Events and Conditional Factors Analysis Manual

Second Edition

Produced by

The Noordwijk Risk Initiative Foundation

Published and distributed by:

The Noordwijk Risk Initiative Foundation
P.O. Box 286,
2600 AG Delft,
The Netherlands.

Email: Info@nri.eu.com
Website: www.nri.eu.com

ISBN 978-90-77284-00-1

NRI-4 (2014)

ECFA+

Events and Conditional Factors Analysis Manual

Second Edition

June 2014

This edition prepared by

J. Kingston (UK)
F. Koornneef (NL)

on behalf of the Noordwijk Risk Initiative Foundation,
P.O. Box 286, 2600 AG Delft, The Netherlands.
www.nri.eu.com

In memory of Dr Robert J. Nertney,
our friend and colleague.

6 September 1923 – 13 July 2004

Preface

The NRI Foundation conserves the knowledge created by the MORT programme. Between 1968 and 2002, the programme accumulated a wealth of material to support the U.S. nuclear industry's management of safety, health and environmental protection. Some materials are in the public domain, but paper-based for the most part. The NRI Foundation exists to publish an archive of the written material, and to supplement it where it will help to keep the knowledge relevant.

Purpose of this document

The Noordwijk Risk Initiative Foundation has written this manual and will maintain it in the public domain. The manual is intended to:

- help investigators produce accounts of incidents that are robust with regard to evidence and completeness;
- encourage stakeholders to share information about incidents;
- provide a reference point for practitioners (of investigation), tool developers, researchers and students.

This manual describes a method that is based on "Events and Causal Factors Analysis", ECFA (Buys and Clark, 1995). It includes rules found by experience as well as those derived from published sources (see the bibliography). In order to distinguish this method from its predecessor, it is called ECFA+, Events and Conditional Factors Analysis.

Structure of this document

ECFA+ is explained in three complementary ways. First, the ideas and conventions are introduced (pages 9-18). Second, with the novice user in mind, ECFA+ is described as a set of procedural steps (pages 20-25). Third, to support the more experienced ECFA+ user, summary instructions for ECFA+ are provided in a single-page aide memoire (Appendix 1, page 27).

Status of this document

This is the second edition of the ECFA+ manual. It contains the insights gained by the authors during the last seven years of applying, reviewing and teaching ECFA+. NRI published the first edition of the ECFA+ manual (2007) as a new method based on the procedure described in the 1995 ECFA manual (Buys and Clark).

Acknowledgements

Particular thanks go to the academics and practitioners who reviewed and suggested improvements to this 2014 edition of the ECFA+ manual. We gratefully acknowledge: Dr MJ Cooper, formerly of the European Institute of Health & Medical Studies, University of Surrey, UK; Mark Dixon; Dr Celeste Jacinto of the Universidade Nova de Lisboa; Dr Paul Lindhout; Phil Parry (former Principal Inspector, Health and Safety Executive), and Chris Peace, Risk Management Ltd, Wellington, New Zealand.

The present authors also thank those who helped put together the 2007 version of this manual: Jan Jager; Prof. Germund Hesslow (Emeritus, Lund University), Cedric Gilson; Jane Paul; Mauro Iacobacci; Cara Dawson; Prof. Peter Waterhouse; Ludwig Benner, and; the late Robert J. Nertney.

We remain most grateful to the 3M United Kingdom plc for their permission to use the term "Post-it Note" (a registered trademark of the 3M Company).

[This page is intentionally left blank]

Contents

Appendices

[This page is intentionally left blank]

1 Introduction

ECFA+ is a way to produce an account of an incident[1] from the available evidence. This account focuses on the events that comprise the incident. These events are put into the order in which they occurred and then linked using the causal relationships between them. The links are tested to ensure that each event is accounted for. When needed, conditions—passive circumstances that affect the course of events—are included to make sure that the account is complete.

An ECFA+ analysis is built-up iteratively. An early analysis is done to help the investigator identify lines of enquiry. These enquiries might be to fill gaps in detail, or to better prove the facts. Thereafter, new information is added to the evolving ECF chart[2] and this often raises new topics for further enquiries. Usually, each iteration of the analysis will take between one and two hours, depending on skill and the quality of data.

To allow the whole analysis to be read at a glance, ECFA+ is done using paper and pencil. This needs enough space in which to do the work: a blind wall, four metres wide is adequate for most analyses. If confidentiality is an issue, you will need a secure space. At the end of the analysis, it is normal to record the ECF chart. This can be done by hand, or by taking photographs. If report quality materials are needed, the ECFA+ chart can be drawn-up using a flow-charting package or other vector graphics software application such as Microsoft Visio. You will find Visio templates for this purpose on the NRI Foundation website.

1.1 Team Approach

In most cases, working in a pair is better than working on your own. Working with someone else encourages progress and can help in other ways too. If the people working on the ECFA+ have complementary knowledge, they can help each other to spot relevant facts and opportunities for further enquiries.

In a larger investigation—involving three or more people, say—you might consider using a facilitator. A facilitator can keep the analysis moving in a disciplined way, freeing the other team members to concentrate on the content.

It is ideal to have the analysis reviewed by someone else. Although the ECFA+ rule set will help you to be objective, a fresh pair of eyes provides useful challenge and review.

1.2 Benefits of ECFA+ to investigation

You can use ECFA+ analysis to:

- produce a simple, evidence-based description of an incident;
- identify gaps in evidence and to suggest further lines of enquiry;
- close off some lines of enquiry which are not relevant to the incident (especially where a large number of potential witnesses or events/conditions are being considered).

ECFA+ can be applied to any incident, but you will have to judge on the merits of each case whether it is worthwhile. In larger investigations there is generally more appetite to invest time in fact finding and analysis. On the other hand, even in simple occupational accidents, a detailed look at the timeline can produce insights for prevention that would not be visible from a superficial glance. Like all tools, ECFA+ should be your servant not your master, so only use it when you believe that it is worthwhile. The main benefits of using ECFA+ are:

- to support subsequent root cause analysis. Methods like 3CA (Kingston, 2008) rely on clear, robust descriptions of incidents;
- to make it easier to write a clear, evidence-based description in the investigation report;
- to keep an overview of what is known about the incident and the key areas of uncertainty;
- to assist briefing new investigators joining the investigating team, or for briefing those with responsibility for the progress of the investigation.

[1] *Throughout this text the authors will use 'incident' to include all unwanted events.*
[2] *The phrase 'ECF chart'(Events and Conditional Factors Chart) refers to any specific instance of applying ECFA+ rules to analyse an incident.*

Note that ECFA+ is just one tool in the 'investigator's toolkit'. ECFA+ can help to establish a clear sequence of events, but other tools will be needed to analyse the barriers, controls and root causes of those events. This is discussed fully in Frei et al. (2003).

2 The parts used in an ECFA+

ECFA+ is a set of rules about how to make a time sequenced model of an incident. Like any model, it is a simplification of the real thing. An ECF model is made from three types of parts: Events, Conditions and Arrows. You will also see Queries and dashed lines: two ways of showing gaps and uncertainties in an ECF model. All of these features are explained in detail in the subsections that follow.

The analysis includes some attributes, but not others. ECFA+ represents an incident as a set of actions that move a situation from a controlled state to an uncontrolled state, and then back again. In the real situation, many other things may be happening, but ECFA+ includes only those actions that are relevant to control.

The analysis tries to keep things as simple as possible. In the real world, events flow smoothly, but in an ECF analysis they are treated as moments of change. Like a silent movie of the 1920's, the action in an ECFA+ is jerky. However, there should be enough continuity to allow the viewer to make sense of what is going on.

2.1 Events

The main task in ECFA+ is to identify changes of activity and to transcribe them as simple phrases, referred to as "events". In ECFA+, events have three attributes:

- the "*actor*" effecting the change; *(e.g. Mr. Bloggs)*
- the "*action*" of the *actor* on the *object; and,* *(e.g. moves)*
- what is being changed – the *object;* *(e.g. a valve handle)*

Vague language, especially *passive voice* phrases such as "the pump failed", can hide the causal 'mechanisms' at work in an incident. Making actor, action and object visible helps the investigator to create a concrete description of the incident. Using the active voice[3] helps investigators to spot gaps in the evidence—such as unknown actors or ambiguous actions.

The general rule in ECFA+ is that an event should have only one actor and one action. Sometimes the actor is composed of several parts (e.g. a team) but it must work as a unit to produce the action.

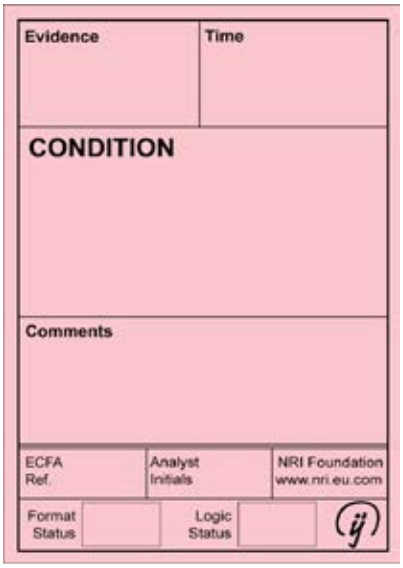
When doing ECF analysis using paper and pencil, it is usual to write events onto yellow post-it notes. This allows them to be moved around as the analysis develops, and to see at a glance which items are events. Blank post-it notes are fine, but some investigators use a pre-printed version (an example shown, right). Pre-printed post-it notes remind users about the information needed when stating an event. This, and the desire for a standard approach across several teams, is why the artwork was drawn-up for the investigation of the disaster at Enschede (see page 35). Figure 2 (page 14) describes the artwork and its use.

[3] *Active and passive voice are explained in Appendix 8 on page 3636*

2.2 Conditions

When accounting for the sequence of events—for why events unfolded as they did—events alone are not enough. Investigators need to identify ***conditions*** which, had they been different, would have altered the course of events. A match struck in an explosive atmosphere gives a very different result to one struck in normal conditions. In ECFA+, the main distinction between events and conditions is that events are active, whereas conditions are passive; conditions persist until acted upon.

ECFA+ analysis begins by identifying events. Conditions are included into the analysis *only* when they are needed to explain those events. This is one way of keeping the analysis as simple[4] as possible. It also helps to avoid force-fitting conditions that are not strictly relevant.



Although more difficult to prove than objective facts, investigators may want to include decisions, thoughts and feelings in the analysis. ECFA+ uses conditions to describe subjective states like those. This is because it is difficult or impossible to state subjective states in a way that can satisfy the criteria for events. Specifically, subjective states cannot be visualised, nor can they be described mechanistically.

When doing ECF analysis using paper and pencil, it is usual to write conditions onto pink post-it notes. This allows them to be moved around as the analysis develops, and to see at a glance which items are conditions and which are events. As explained earlier, blank post-it notes are fine, but some investigators use a pre-printed version (an example shown, right). Figure 3 (page 15) describes the artwork and its use.

Sometimes, investigators want to include *omissions* in an analysis. An example of the general form is “Actor does NOT do action”. In ECFA+, these omissions are called *non-events*, and are discussed in the next section.

2.3 Non-Events

A *non-event* is a special type of condition. You can use it to describe something expected to occur given the circumstances, but which did not happen in the incident. For example, if omitting an action leads to an accident, you might view that non-event as an essential part of the story[5].

Non-events are passive, and that is why they are treated as conditions. However, unlike other conditions, non-events are negative; they define a condition by what is not happening. ECF analysis includes only the conditions that are needed to account for the sequence of events. This test of relevance applies to non-events, as it does to any other condition. The breaking of a workplace rule might be relevant to your investigation, but it might not be relevant in the ECF analysis.

When describing a condition as a non-event, you need to state your basis for judging it to be relevant to the incident. You do this by stating the standard against which you are comparing the conditions and events in the incident. This means the procedure, good-practice or expert opinion that justifies the behaviour implied by the non-event. If, for example, work was being

[4] *In ECF analysis, the aim is to arrive at the simplest explanation that fits the facts of the incident. This is an application of Occam’s razor: the principle that entities must not be multiplied beyond what is necessary.*

[5] *Appendix 5 contains a discussion of this issue; item (e) is of particular relevance.*

done without a permit, the non-event must specify the standard that required a permit. This allows other people to verify the analysis.

Although ECFA+ allows non-events, you should consider whether the facts would be better expressed in another way. Bear in mind that you should only include items that are necessary, and without which the sequence of events would have been different. The risk of including non-events is that they tend to exaggerate the responsibility of individuals and may obscure other facts about the context.

In summary, a non-event is a negative condition. Before putting a non-event into your analysis, make sure that it:

- applies in the specific case: you need it to account for an event;
- applies in the general case: the standard used to justify the non-event is valid in the context of the incident;
- can be stated accurately only as a non-event. If you can say the same thing in positive terms, it is simpler to use a regular condition.

2.4 Arrows in ECFA+

In ECFA+, an arrow drawn between two items means that the earlier item—an event or condition—directly causes the later item. To keep their meaning clear, arrows must only be used to mean direct cause.

2.5 Dashed lines

All events, conditions and direct causal relationships (shown by arrows) must be supported by some evidence. However, ECFA+ uses dashed lines to mark where the facts cannot be proved conclusively. Dashes are used as follows:

- a dashed arrow means that there is some evidence for a direct causal relationship, but not conclusive[6] proof;
- an event (or condition) enclosed by dashes means there is adequate evidence to justify its presence in the analysis, but not enough to treat it as a proven fact.

When enclosed by dashes, events and conditions are called *presumptive*. Usually, investigators accept events and conditions as presumptive only when it is clear that further enquiries would not be able to prove the facts[7]. Before then, while the investigation is still live, it is normal to use the format status box on the post-it notes to show gaps in the evidence. Section 3.3 describes how to use the format status box.

3 How to construct an ECFA+

This section introduces the rules for describing an incident using ECFA+. Before you read the rules in detail, please reflect for a moment on these three points. ECFA+ analysis is:

- iterative, and is usually built-up in two or more sittings;
- best started early in the investigation and added-to as facts come to hand;
- an evidence-based description of the incident, which although useful is a simplification of a more complex reality.

---

[6] Conclusive, that is, at whichever standard of proof the investigator needs to satisfy. This might be 'more likely than not' in civil matters, or beyond reasonable doubt in the context of criminal proceedings. You can find a more detailed discussion of evidence in Appendix 6 on page 34).

[7] Although not part of the ECFA+ rule-set, lines-of-enquiry need to be managed actively. This includes making and recording decisions to curtail further enquiries..

3.1 ECFA+ start and end points

The decision about where to start and end depends on the purposes of the investigation. It is up to you what you model. Be aware, however, that other stakeholders to an incident will have their own point of view and may see things differently. As a result, their ECF analysis may differ from yours.

It is usual for the ECF chart to include the event that compromises control and the event that makes the situation safe again. For example, the events shown in Figure 1 have created conditions that are not under control. By default, the investigators would continue the time-line forward and include in the analysis the events and conditions that show how control was restored and the situation made safe. In the case of Figure 1, how the car fire was extinguished, and the casualties (including the injured Officer-in-Charge, OiC) were stabilised.

Beginning and ending points are not always clear-cut, because control is generally a matter of degree rather than absolute. The point is to reflect on whether the analysis has made it adequately clear how control was lost and regained.

Conditions are sometimes created by earlier events. When these earlier events (and their associated conditions) fall outside of the time frame of the incident, they are called *secondary* event lines. Where it fits within the scope of your investigation, you may need to include secondary events in your analysis. However, bear in mind the practicalities and consider whether a secondary event line should be made the subject—*the primary event line*—of a separate ECF analysis.

The answer to "how far back in time an investigator may need to reach" depends on whether we are discussing the primary or secondary events. Primary events are generally close in time to the unplanned outcomes which are the focus of the investigation; in the order of minutes, hours, or days. Secondary events are included to explain the coming into existence of conditions; and these may reach back days, weeks, or years.

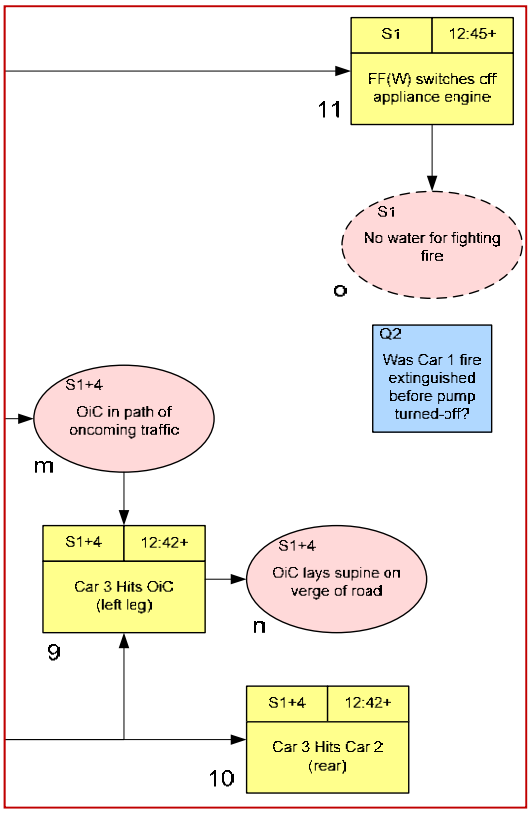


Figure 1. Excerpt from an ECF chart (more at Appendix 2)

3.2 Iterative approach

Usually, investigators begin the ECF analysis early and build it up in two or more sittings. ECFA+, like many forms of analysis, help to structure what is known and unknown. Spotting the unknowns early in the investigation helps to steer further enquiries while the evidence is most easily collected.

There is no limit to how many events and conditions you include in a completed ECFA+. The rule is that all of them should be necessary. However, to make progress at the start of the analysis, you should include no more than 12 events. The first logic check (see section 3.4) of this small set of events will reveal the need to include conditions and more events.

There are exceptions to this rule. Firstly, in large investigations, rather than building the analysis in deliberate iterations, ECFA+ might be a continuous effort done in parallel with other investigative activities. Secondly, when reviewing a completed investigation, or when taking-over a nearly complete investigation, the analysis might be done in one sitting. In all of

these situations, ECFA+ is being used to structure and confirm the facts about how the incident happened.

3.3 Format checking

Analysis involves manipulating data according to a set of rules. Without the rules, the analysis becomes unsystematic and unreliable. This means that the analyst has to keep in mind both the facts of the incident and the ECFA+ process rules. ECFA+ works well when it is done rapidly with the focus on the content. To ensure that rapid progress results in a rigorous analysis, two types of check are done at intervals: format checking and logic checking.

Format checking has two aspects:

1. Check for gaps in evidence;
2. Check for conformity with ECFA+ rules for the format of events and conditions.

In each iteration you will add some events and conditions to the analysis. In the first iteration, you will go from a blank sheet to a set of up to 12 events with, perhaps, one or two conditions. At this point you should check the format of every event and condition in the ECF chart. In later iterations, the format check is performed on each item as it is added into the ECF chart.

Figure 2 summarises what you need to look for when checking the format of an event, and how to record it. Sometimes, you might find that a condition is stated on an event post-it, or vice versa. If so, decide which is appropriate and re-write if necessary.

The format check can have two outcomes. The first—shown by a tick in the "Format Status" box—is satisfactory. The tick means that there is sufficient evidence to treat the event as a fact, and all the needed details are included in the format specified in section 2. The second outcome—shown by a Q*n*—is that you decide that more evidence is needed to corroborate or to fill in missing details. The '*n*' is the reference number of the relevant item on the further enquiries list (see Appendix 4).

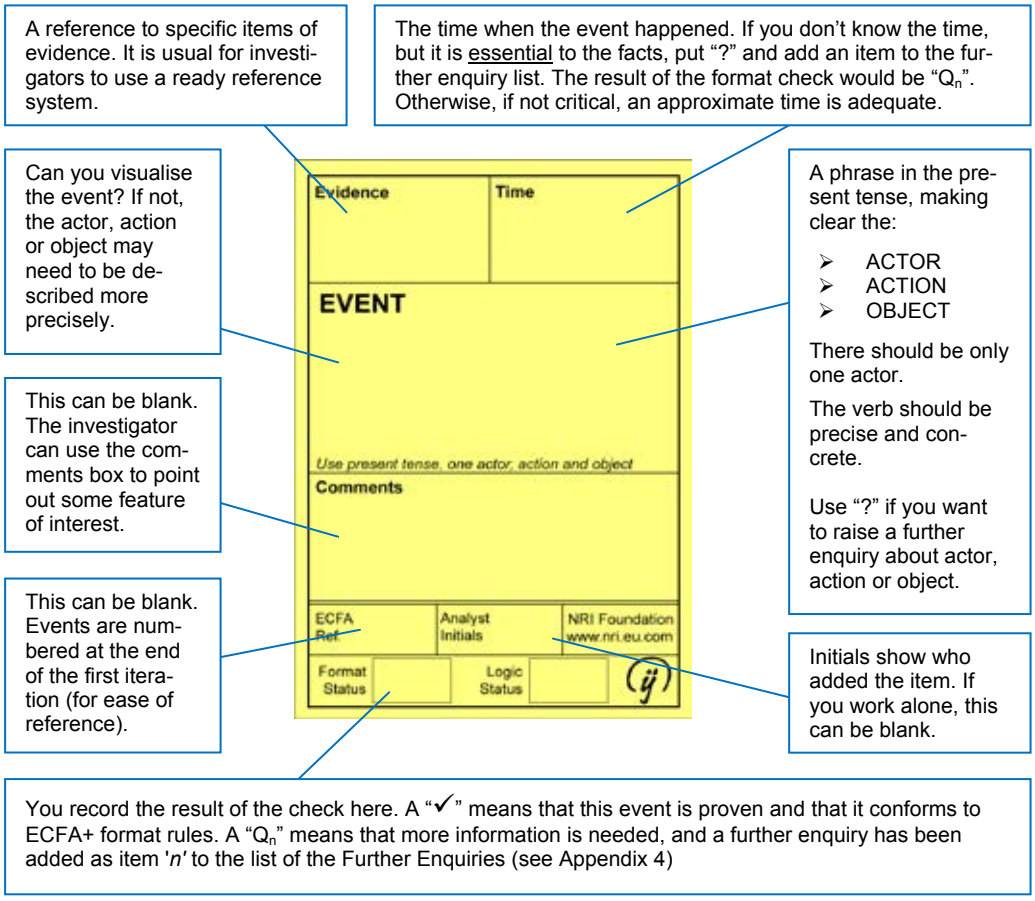


Figure 2. What to look for when checking the format of an event

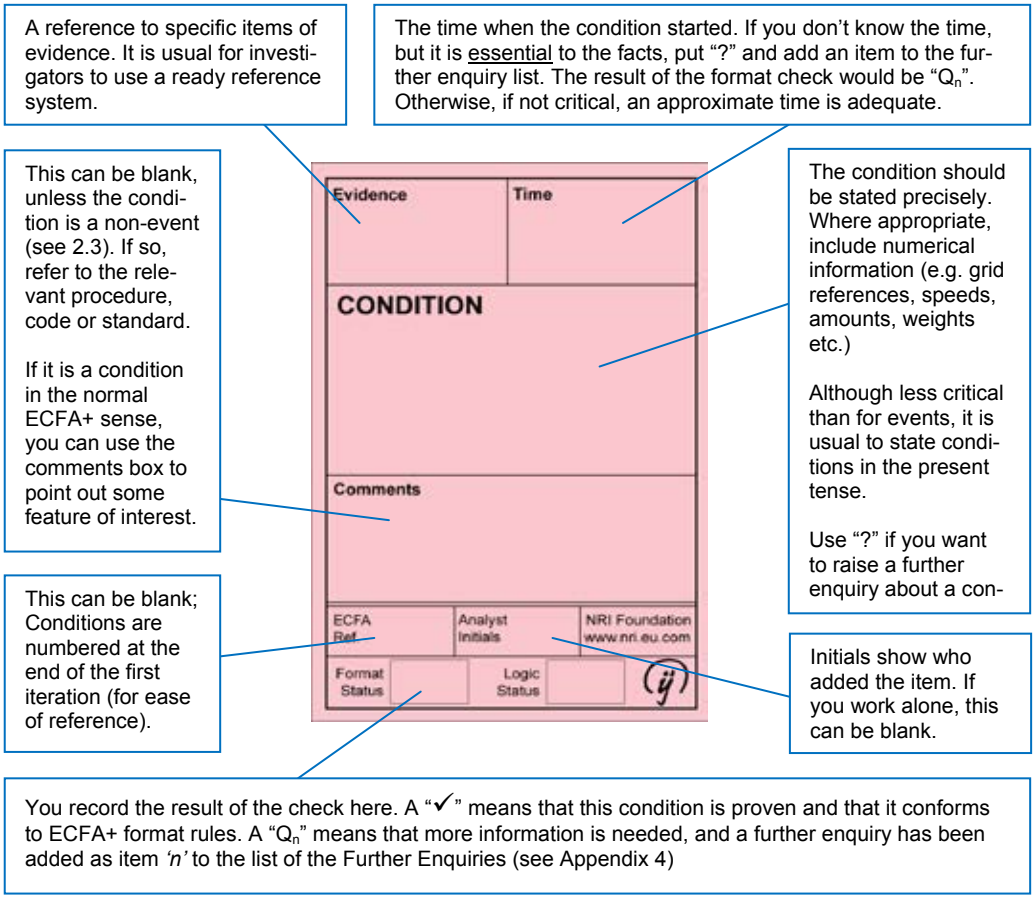


Figure 3. What to look for when checking the format of a condition

Normally, fresh evidence allows you to revise 'format status' from 'Q' (needs more evidence) to '✓' (satisfactory). However, two situations can make it happen the other way around. Firstly, new evidence can force you to review items that you had thought satisfactory. Secondly, a reviewer may disagree with your interpretation.

Format checking is a critical routine in ECFA+. Events and conditions stated poorly or with inadequate evidence can complicate or undermine the analysis. Furthermore, early checking will give you the best chance of filling any gaps you find. Knowing which rules can be broken, and under what circumstances, is part of being an expert. However, even if you are a supremely confident ECF analyst, always do the format checking!

3.4 Logic checking

The logic check finds the events and conditions that directly cause an item. The aim is to make connections between the item being checked and those that happened earlier in the timeline.

Checking the logic moves forward the analysis in three ways. It:

- finds gaps in the account of the incident;
- adds needed events and conditions;
- adds structure to the ECF chart of the incident.

Starting with the last item—the post-it note to the far right—you will need to check the logic of every event and condition in the analysis. Each item is checked using a six-step routine:

1) Select an item to account for.
2) Find the earlier events and conditions that directly cause the item.
3) If these earlier events and conditions occur, would the item in question always result?
4) If the item would not always result, add post-its with the missing facts to the ECF chart:
   a) add events or conditions, if the evidence allows;
   b) check the format of any new events or conditions that you add;
   c) If wanted, reposition all the related items;
   d) draw arrows (solid or dashed) from the earlier events and conditions to the item;
   e) add a Query note, if more evidence is needed;
   f) add to your 'further enquiries list' the question asked in the Query note;
   g) place any Query notes near the item, without drawing arrows (but a dashed line can be used to connect the query with the item it relates to).
5) If the item would always result:
   a) draw solid arrows from the earlier events and conditions to the item;
   b) If wanted, reposition all the related items.
6) Record the outcome of the check (a tick or 'Qn') in the logic status box.

3.5 Dashed or Solid Arrows

When drawing an arrow, you need to decide whether to use a dashed line or a solid one. The reasons were given in section 2.5 (page 12). As well as reflecting on the strength of evidence, you will also need to make a note of any further enquiries that might be needed. The decisions, bulleted below, amplify step 4(d) of the six–step logic check routine.

- If the evidence proves the logical relationship, the lines should be solid.
- If the evidence is not strong enough,
  - use a dashed line to show a presumed relationship, and;
  - write a '?' next to the arrow to show that there is a line of further enquiry aimed at strengthening the evidence for a dashed arrow;
  - there should already be a query note asking a question about the subject; if not, add one and make a corresponding entry on the further enquiries list.
- If sufficient evidence is forthcoming, the dashed line can be redrawn as solid.

3.6 Query Notes

Blue 'Query notes' are place markers that show the gaps in the ECFA+ account of an incident. Arguably, a 'Qn' in the logic status box would be enough to record a gap, but the query note makes it easier to review this aspect of an ECF analysis.

Every time you add a query note, you should make a corresponding entry in the further enquiries list. The further enquiries list belongs to the investigation as a whole, and it needs to be a complete register of all the uncertainties in it.

Usually, query notes are used only to show the more important gaps in the analysis. This is why most query notes are added during logic checking. If every small question of detail was written on a query note, the ECF chart would be overcomplicated by blue post-it notes.

3.7 Arranging events and conditions

In the early stages of the analysis, you might have grouped actors into horizontal rows. This approach helps to organise the early part of the analysis and makes it easier to spot gaps in the action. However, once each actor's actions are accounted for in the first iteration of the analysis, separate actor rows become less valuable.

Usually, the logic check is the time to move items; but it is optional. If you are content with actor rows, the arrows between logically related events and conditions might have to dodge around intervening items. The arrow between events (2) and (6) in Figure 4 is an example.

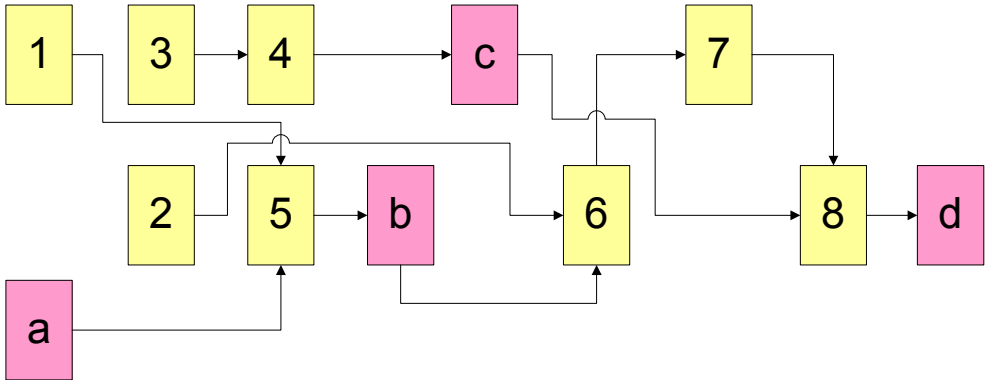


Figure 4. Schematic of an ECFA+ in which items are aligned by actor

So long as the arrows only link items that have direct causal relations, and the time order is preserved, the analyst can suit themselves. However, some analysts find it more intuitive to align causally connected items into horizontal rows, while keeping the time order of the items. This is illustrated in Figure 5.

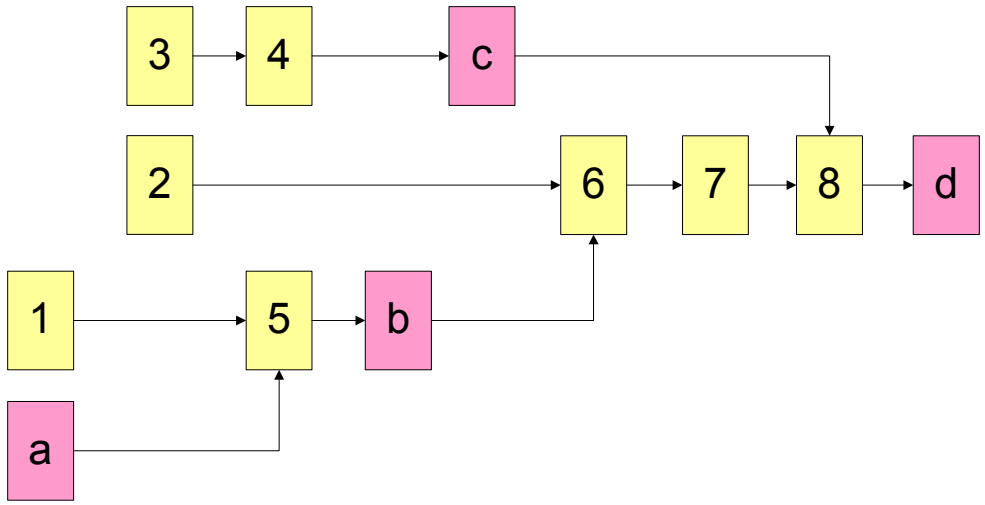


Figure 5. Schematic of an ECFA+ in which items are aligned by causal relationship

4 Finalising the analysis

At the end of the first iteration of the analysis, every format and logic status box should contain either a tick, or a 'Qn' cross-reference to the list of further enquiries. There should be no blank boxes. After the first iteration, keep the analysis updated and available for review until the investigation is closed.

Even in its final form, an ECF chart will still have some dashed lines, query notes and 'Qn' references in the check boxes. An analysis is finished not when all uncertainties have been removed, but when the investigator has no further use for it. Some gaps will remain no matter how much effort is invested in fact finding.

4.1 Independent Review

You should not accept an analysis as final until it has been reviewed. Even when sticking close to the rules set out in this manual, there is still room for differences of interpretation and for error.

You will need to consider how formal a review needs to be. Given the role of ECFA+ in finding new lines of enquiry, rapid reviews done at intervals can add a lot of value.

Another factor is the independence needed by the reviewer. At the minimum, the reviewer needs to bring a fresh pair of eyes, and this means someone who has not been involved in the analysis. You might judge it best to involve someone who has not been involved in the investigation. In either case, to engage critically, the individual will need enough technical knowledge of the content to understand the items and relationships in the analysis. As well as content knowledge, the reviewer will need to be able to verify the format and logic of all items in the analysis. To ensure thoroughness, the reviewer should know how to do these checks before they start the review.

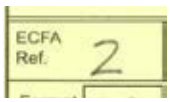
4.2 Recording ECF Charts

You might want to make a record of a paper and pencil ECF chart for a number of reasons:

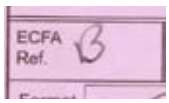
- to remove the chart and to put it up again later or somewhere else;
- to make a formal record of the ECF chart at the end of the investigation;
- to prepare the ECF chart to be drawn-up for a report or as a prop for briefings.

If you have little time, a series of photographs can capture the ECF chart. To make sense of the analysis, you will need to be able to both read the detail and see enough of the chart at a glance. This might require hard copies of the photographs.

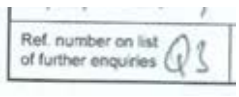
Another option is to make a sketch of the analysis. This is surprisingly quick to do for even a 40-item ECF analyses. The first step is to make sure that every item in the analysis has a unique reference:



Use numbers for events



Use letters for conditions



Queries use the 'Qn' format

Figure 6. Reference system for ECFA+ items

Next, write the references in the pattern they appear in the ECF chart. Then draw the arrows between the references, being careful to reproduce dashed and solid lines. Similarly, dashes enclosing events or conditions should be added to the sketch. The original post-it notes should be kept with the sketch.

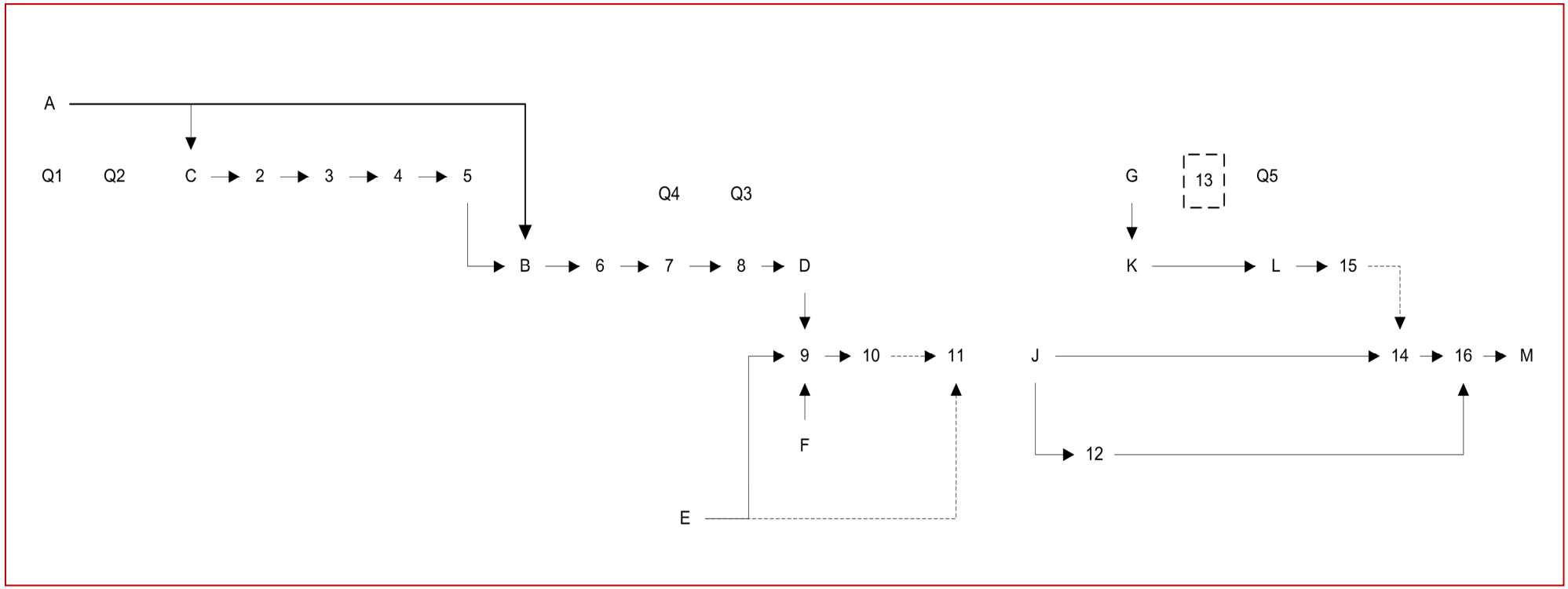


Figure 7. Example sketch of an ECF chart
(allows the final state of the analysis to be recreated using the original post-it notes)

If report quality materials are needed, the ECFA+ chart can be drawn-up using a flow-charting package or other vector graphics software application. You will find Visio templates for this purpose on the NRI Foundation website.

5 Procedure for ECFA+

This procedure is written with the new user in mind: detailed steps are provided together with guidance. Once familiar with this procedure, the one-page aide-memoire (Appendix 1) should be enough to remind users of the key steps.

Task Steps	Description & Criteria	Guidance
1. Study all available information about the incident		Start the analysis early. Applying ECFA+ helps to find gaps in information. It is easy to update the ECF chart in the light of new evidence. Work in pencil (easier to amend).
2. Write out information about actions onto 'Event' Post-it Notes (yellow).	(a) At the start of the analysis, write out no more than 12 events.	To make progress at the very beginning of an ECF analysis, include no more than 12 events. There is no limit to how many events and conditions you can include when you reach step 5, although all must be necessary. You can ignore this rule if using ECFA+ to review a completed investigation, or when taking-over a nearly complete investigation.
	(b) Describe each event as a single moment of change.	If you wish to transcribe an action that continues for some time, consider breaking it down into its constituent actions (separate Post-it Notes for each) or transcribe as a condition.
	(c) Describe the event using just one actor and one action.	An actor can be a person or a thing. If the actor has more than one part or member (e.g. "crew leave site") these parts must be acting as a single unit. If not, consider transcribing events for each distinct actor.

Task Steps	Description & Criteria	Guidance
2. (Continued) *Transcribe information about actions onto 'Event' Post-it Notes (yellow).*	(d) Phrase the event using the present tense and active voice (actor does action)	Use the active voice: make the actor the subject of the sentence stating the event (e.g. Bloggs undoes the clip). Use verbs that describe easily visualised, concrete actions. The thing or person acted on (the object) must be obvious in the event. If you find yourself needing to use the progressive form of a verb (e.g. with an '–ing' ending) either identify the constituent events or consider transcribing the activity as a condition.
	(e) Avoid non-events. An example of a non-event is "Bloggs did not close exit valve";	Non-events are things that did not happen but which, according to some ideal way of carrying-out a task, ought to have. Transcribe non-events as conditions, using (pink) Post-it Notes. State the standard you are relying on to make the judgment (e.g. a specific written procedure, code, or standard). If you do not know the specific standard that applies, make an entry on your list of further enquiries to find out.
	(f) State the evidence for the event occurring (if you lack proof, put a "?" in the evidence box and make a note on your list of further enquiries;	It is essential that all events and conditions either cite evidence or are connected explicitly to a further enquiry. Cross-references to specific items of evidence can be speeded up by using a systematic referencing system.
	(g) State the time, if known;	Knowing the time helps to correlate different sources of evidence for a given event or condition. If you do not know the precise time the event occurred, use a question mark. For example, if after 12:50, but before 13:00; use "12:5?". If wholly unknown; put "?". Consider adding a corresponding entry to the list of further enquiries.

Task Steps	Description & Criteria	Guidance
3. Put event Post-it Notes onto a wall and position them using these rules-of-thumb:	*(a) vertically* – it can be helpful for each actor to have his/her/its own row, but it is optional.	It is not essential to have a separate row for each actor but it can be helpful if there is a lot going-on in the incident you are analysing. Later in the ECFA+ process, you will probably re-arrange events to emphasise certain sequences.
	(b) horizontally – put events in time order, so that later events are always to the right of earlier events.	ECFA+ does not use a fixed base for time (meaning equal intervals of time marked on the horizontal axis of the ECF chart).
4(a) Check the format of every event.	(a) Is the event stated in the simple present tense? (b) Is the event stated in the active voice? (c) Are the actor, action and object clearly identified? (d) Is the event a moment of change? (e) Can the event be visualised? (f) Is evidence cited? (g) Is the time stated? (h) Has it been initialled by the analyst?	Format checks are essential to ECFA+. Poorly stated events can complicate or undermine the analysis. Also, finding gaps allows further evidence to be collected. Sometimes the object and the actor are the same ("Bloggs walks to the door", "the tank explodes"). If the time is not stated, but it is essential to the facts, put "?" and add an item to the further enquiry list. The result of the format check would be 'Q_n'. Visualisation: you should be able to form a mental image of every event. If you cannot, there is either a problem with how the event is stated or with your understanding of the action described.
4(b) Check the format of every condition.	(a) Is it stated precisely? (b) Is numerical data given where needed? (c) Is evidence cited? (d) Is the time stated? (e) Has it been initialled by the analyst? (f) If a non-event, is the standard stated?	Anything you include in your analysis implies "after this, therefore because of this". Because non-events can exaggerate the role played by individuals, check these points: • Is it really needed? If not, remove. • Is a non-event the only way to state the facts accurately? If not, use a regular condition. • Does the explicit standard (e.g. a procedure) stated in the "Comment box" apply in the context of the incident?

Task Steps	Description & Criteria	Guidance
4(c) Record the result of the format check in the "Format Status" box.	(a) Tick the box if all details are present and correct. (b) If any data are missing, or the evidence is inadequate, add a numbered entry to the further enquiries list. Record this number in the Format Status box as 'Qn' (where 'n' is the number of the entry on the further enquiries list)	A tick in the "format status" box means that the analyst is satisfied that the event is an accurate factual representation of the action described. An example format for a further enquiries list is provided in Appendix 4.
5. Check the logic of cause and effect for every item (event and condition).	Start with the last item. Focus on the item (event or condition) to be checked for logic: a) identify the earlier events (or conditions) that directly cause the item in question; b) if these earlier events and conditions occur would the item in question always result?	The 'logic checking' process identifies the chain of cause and effect that links together the various events and conditions. The logic check of an item looks for relationships with other items, whereas the format check focuses on an item in isolation.
	c) If the item can be explained by earlier events and conditions i) draw linking arrows from the relevant events and conditions to the event in question;	A linking arrow between two Post-it Notes means that the earlier "causes" the later to occur. You need to consider the strength of evidence for this causal relationship.
	ii) reposition the Post-it Notes to achieve the simplest arrangement (but preserve time order);	When repositioning, try to avoid crossing lines. This is not always possible, but the idea is to make the ECF chart as clear as possible.
	iii) tick the "logic status" box.	A tick in the 'logic status' box means that the event is explained.

Task Steps	Description & Criteria	Guidance
5. (Continued) *Check the logic of cause and effect for every item (event and condition).*	d) If the item <u>cannot</u> be explained by the events and conditions present in the ECF analysis: i) add needed events or conditions, if the evidence allows; ii) check the format of any new events or conditions that you add; iii) if wanted, reposition all the related items; iv) draw (solid or dashed) arrows from the earlier events and conditions to the item; v) add a Query note, if more evidence is needed; vi) add to your 'further enquiries list' the question asked in the Query note; vii) place any Query notes near the item, without drawing arrows; viii) write 'Qn' in the logic status box (where 'n' is the number of the entry on the further enquiries list).	The logic check will often trigger you to recognise the relevance of events or conditions that need to be added to the ECFA+ chart. This is especially true of conditions. Arrows should be drawn from events and conditions to the item in question, even when the item cannot be fully explained. If the item cannot be explained, each arrow still represents a 'necessary cause". However, all of the arrows taken together are 'insufficient' to explain the item. When drawing an arrow, you need to decide whether to use a dashed line or a solid one. The arrows represent direct causal relationships and must be supported by some evidence. Dashed lines show relationships that cannot be proved conclusively. As well as reflecting on the strength of evidence, you will also need to make a note of any further enquiries that might be needed. Query notes are blue and provide a way of "parking" an uncertainty that needs to be kept visible in your analysis, but without trying to resolve the issue there and then. This allows you to keep making progress with the analysis. Further enquiries should be numbered sequentially. A proforma for recording these is provided in Appendix 4.
6. As new events and conditions are added to the analysis, apply the format and logic checking rules.	(a) Add new events and conditions in the light of fresh information. (b) Consider obtaining an independent review of the analysis.	ECFA+ is usually done in two or more sittings. At each sitting, new events and conditions are integrated into the ECF chart using the format and logic checking rules.

Task Steps	Description & Criteria	Guidance
7. Perform final revision	Challenge any events left in the analysis that do not satisfy format or logic criteria:	When all evidence collection is finished, the ECF chart needs to be finalised to show the final state of information, including remaining uncertainties. Most investigations leave some uncertainty. It adds to the value and credibility of your analysis to be explicit about what was not explained by your investigation.
	a) If any event or condition has a **blank box** (format or logic status): i) If you judge that the event or condition is not critical to the analysis, remove it. ii) If the item is essential, decide what the status should be and write it in.	'Dashed' events and conditions should be used sparingly in ECFA+. Ensure that all dashed items are based on some evidence and reasoned hypothesis (and not just unqualified opinions).
	b) Remove, or outline with dashed lines, events or conditions that have '**Qn**' in their **format** status box: i) If you judge that the event or condition is <u>not</u> critical to the analysis, remove it. ii) If the item is essential, but lacking detail or evidence, enclose it in dashes.	
8. Record the analysis	c) Make a suitable record of the analysis (e.g. by sketch, storage of original materials, or photographs).	Investigations happen in many different settings, and what is a suitable record in one situation might not be adequate or convenient in another. Consider the following: • Is the ECF chart to be taken down and put up again? • Is a permanent record of the analysis needed? • Is a paper and pencil analysis to be drawn-up using software? You might seek advice about what is needed in your particular situation.

Bibliography

Benner, L., and Rimson, I. (1991) Quality Management for Accident Investigations – Part 1, ISASI *forum*, Oct 1991 (24:3). Available via internet: http://www.iprr.org/LIB/QMA_P1.html

Benner, L., and Rimson, I. (1992) Quality Management for Accident Investigations – Part 2, ISASI *forum*, March 1992 (25:2). Available via internet: http://www.iprr.org/LIB/QMA_P2.html

Buys, J.R. and Clark, J.L. (1995), "*Events & Causal Factors Analysis*". US Dept. of Energy. Ref. DOE 76-45/14, SSDC-14. http://tis.eh.doe.gov/analysis/trac/14/trac14.pdf

Chambers (1996) "Guide to Grammar and Usage". Compiled by George Davidson. Larousse. Edinburgh.

Frei, R., Kingston, J., Koornneef, F., and Schallier, P. (2003), "Investigation Tools in Context". JRC/ESReDA Seminar on "Safety Investigation of Accidents" in Petten, The Netherlands, 12-13 May 2003. Available via internet: www.nri.eu.com.

Giannelli, P.C. (2003) "Understanding Evidence". LexisNexis.

Hayakawa, S.I., and Hayakawa, A.R. (1990) "Language in Thought and Action". 5th edition. Harcourt Brace & Company.

Hesslow, G. (1988) "The Problem of Causal Selection". In Contemporary Science and Natural Explanation: Commonsense Conceptions of Causality. D. Hilton (ed.), Brighton, Harvester Press. Full text at: http://www.hesslow.com/germund/philosophy/Problemselection.htm.

Hendrick, K. and Benner, L. (1987), "*Investigating accidents with STEP*". Marcel Dekker.

Kingston, J. (2008) "*3CA – Control Change Cause Analysis Manual*, Form B". NRI-5 (2008), Noordwijk Risk Initiative Foundation, The Netherlands. Available via internet: www.nri.eu.com.NRI5.pdf

Tapper, C. (2003). "Cross & Tapper on Evidence". 10th Edition. LexisNexis.

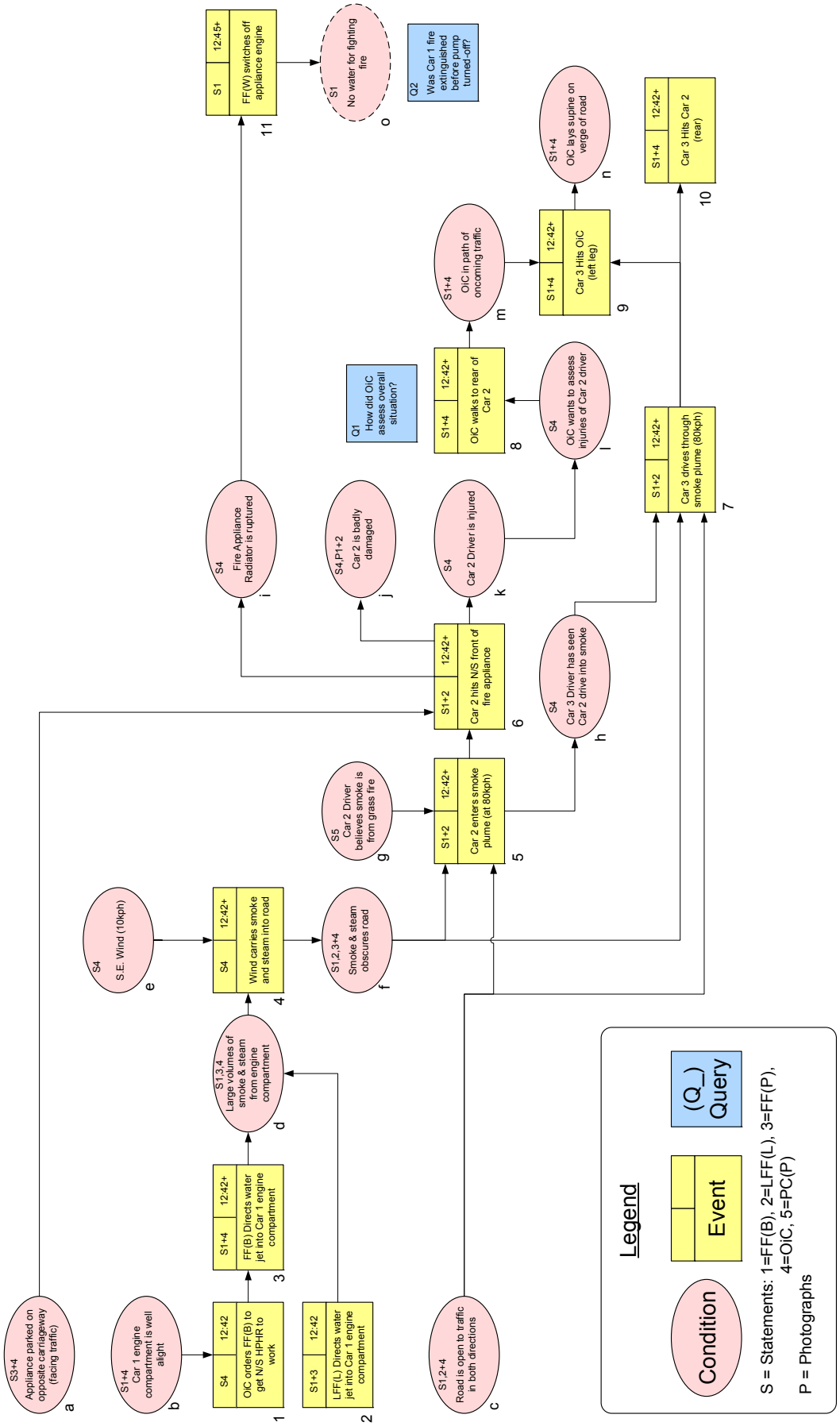
Trost, W.A. and Nertney, R.J. (1995), "*Barrier Analysis*". US Department of Energy Ref. DOE 76-45/29, SSDC-29.

Appendix 1: Aide Memoire

1. Familiarise yourself with available information (including the site, if accessible).
2. Write up to 12 actions into Event (yellow) Post-it Notes.
3. An event (e.g. 'Smith opens valve 2') should conform to the following criteria:
   - It describes a moment of change.
   - It identifies the actor, action and object.
   - It describes the action simply, concretely and precisely.
   - It is written in the present tense using the active voice (sentence starts with the actor)
   - The event can be visualised.
   - A source of evidence (e.g. statement, photograph) is stated in the "Evidence box".
   - The time (and date, if needed for clarity) is given in the "Time" box.
   - It is initialled by the analyst who put the event into the ECF chart.
4. Most conditions (e.g. 'Solvent flows from the open flange of valve 2') will be written at step 8, but some will appear as a by-product of identifying events. Unlike events, conditions endure and are passive. Conditions may be started and stopped by Events. A condition (written using pink Post-it Notes), should conform to the following criteria:
   - It is described precisely.
   - A source of evidence (e.g. statement, photograph) is stated in the "Evidence box".
   - If a non-event, is it justified?
   - All relevant quantitative data are given.
   - It is initialled by the analyst who put into the ECF chart.
5. "Park" queries on your list of further enquiries. Keep the analysis moving.
6. Put items (events and conditions) into chronological order.
7. Verify that all items conform to ECFA+ criteria. Note items requiring further enquiries. Use the 'format status box' to record the result of the check.
8. Question causation item-by-item (more conditions are produced by this stage)
   - Can you prove that there is a direct causal connection between the item in question and earlier items? If yes, draw arrows from the precursor items to the item in question. If no, make a note of the further enquiries required on a blue Query Post-it Note and cross refer with the list of further enquiries.
   - Are the precursor events and conditions stated sufficient to explain the event? Would these precursors always produce this event – if not, note further enquiries, add-in and connect the necessary events and conditions.
9. Review the analysis. Ideally, ask a colleague who hasn't been involved to review the analysis and try to visualise the event line. If they have trouble, there may be gaps.
10. Correlate with other techniques. Root cause methods often produce conditions, some of which may be relevant in the ECF analysis. When integrating these into the ECFA chart, ensure that the conditions meet ECFA criteria (for evidence and precision in particular).
11. Record the Chart: number all Post-it Notes
    - Events: Numbers (1, 2, 3…)
    - Conditions: Letters (A,B,C…)
    - Queries: Prefix "Q" plus the relevant entry in the further enquiries sheet (e.g. Q1)

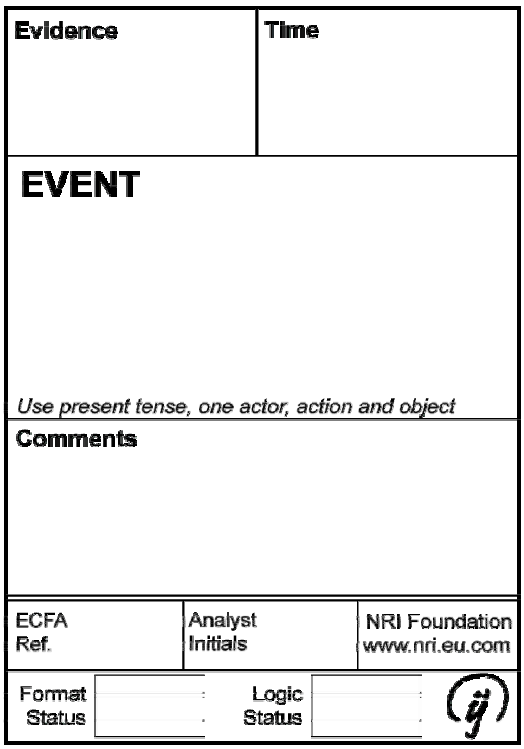
    Either photograph the analysis or make a sketch of the pattern of numbers and arrows on a piece of paper. Remove and store the Post-it Notes.

Appendix 2: Excerpt from an ECFA+ analysis.

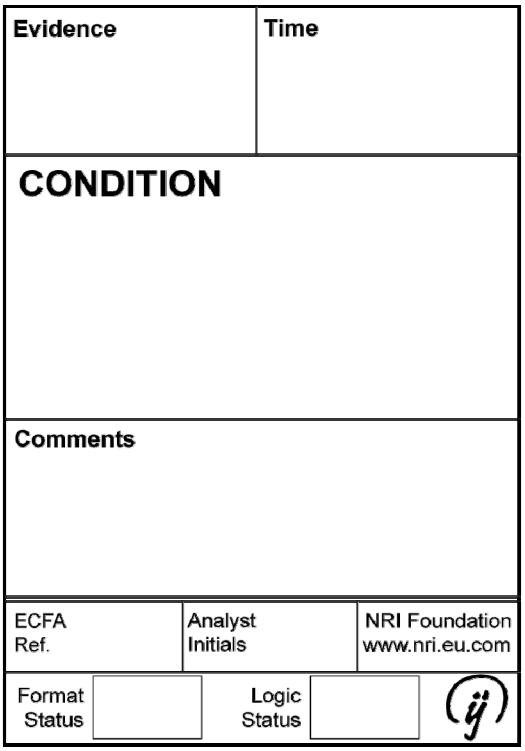


Appendix 3: ECFA+ Artwork for printed Post-it® Notes†.

EVENT: Print onto yellow



CONDITION: Print onto pink



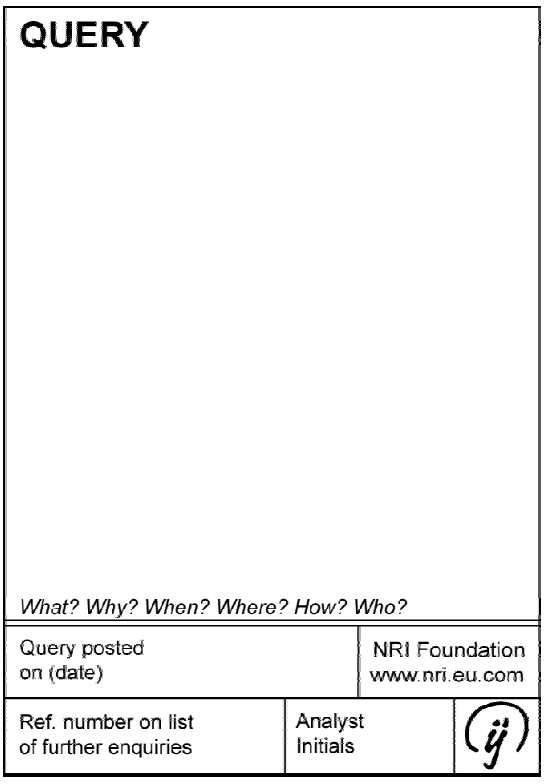
CONDITIONS OF USE

This artwork is produced by the Noordwijk Risk Initiative Foundation. It is provided free of charge subject to the following conditions:

- you may copy, print, or distribute these images but only if you acknowledge the NRI Foundation's authorship;
- these images are subject to continuous revision – you are asked not to put copies of them on the internet without the prior permission of the Foundation - please use a link and not a copy;
- this artwork, and any other content from this document, must not be sold for profit or given out in any way other than as stated above.

† *Post-it is a registered trademark of 3M Company.*

QUERY: Print onto blue



Appendix 4: Pro-forma for Further Enquiries List

Ref.	Information required	Source of Info	Priority

Appendix 5: Note on Causal Selection

This note is a condensed version of the chapter written by Germund Hesslow and published in "Contemporary Science and Natural Explanation: Commonsense Conceptions of Causality". D. Hilton (ed.), 1988, Brighton, Harvester Press.

The full text, which contains many examples, extensive discussion of the issues and a full attribution of sources, can be obtained from:
http://www.hesslow.com/germund/philosophy/Problemselection.htm.

THE PROBLEM OF CAUSAL SELECTION

Introduction: the plurality of causes

Events, facts, states or properties have infinitely many causes. There are three reasons for this:

1. an event will normally depend on the immediately preceding occurrence of several different events;
2. it will usually be possible to trace a causal chain backwards in time;
3. it is generally possible to conceptualise the causes in infinitely many different ways.

Selecting one or more causes from a set of conditions is a special case of the weighting of causes according to their relative importance. For instance, although we might explain someone's alcohol problems by their biochemical susceptibility to alcohol dependence, we might also concede that other factors, such as personal problems, were contributory. When the selection criterion unequivocally picks out one condition we call this the cause, but when other conditions come close to satisfying the criterion these are termed contributory, and the condition which best fits the criterion is considered more important than the others.

Two basic distinctions: "selection versus connection", "individual versus generic"

The selection problem has two interrelated aspects:

- the "connection problem" – the existence of a causal relation between two events. The connection problem is the problem of understanding the process by which we determine that, say, the presence of oxygen, combustible material and a source of ignition are all *necessary* conditions for houses catching fire.

- the "selection problem" – the relative importance of causes. The selection problem is the problem of deciding which of the necessary conditions was the most important, in a concrete individual case. We do not say that a fire was caused by oxygen, in spite of the fact that we know that there is a causal connection between oxygen and fire. Instead, we mention only the combustible material and the source of ignition.

There are two kinds of causal relationship, individual and generic:

- Individual causal relationships are those which obtain between concrete individual occurrences of events, such as the house's catching fire at 9.05 p.m. yesterday because of the explosion in the television set a moment earlier or the fact that Smith's recent death was caused by a heart attack.

- Generic causal relationships are those which obtain between kinds of events (generic events) or between properties, such as the general propensity of explosions to cause fires, or the fact that heart attacks cause death.

One view of the relationship between these two kinds of causal relation is that we arrive at generic causal relations by generalising from individual cases of co-occurrence and then apply this general knowledge to other individual occurrences. Thus, since a large proportion of

those who have heart attacks die, we conclude that the disease is deadly. If Smith has an infarction and dies, we use our knowledge of the general causal relation to justify the belief that his death was caused by the infarction. *Note, however, that a general causal statement can be true while a corresponding individual statement is not.* Smith's heart attack may not have killed him and he may have been killed by something else.

Criteria which govern causal selections and weightings

There are many different criteria that can be applied to the task of selecting a relevant subset of causes from the infinitely large set of causes that can be argued to precede any event or state. It is not self-evident that any of the criteria described below, are "true" or "correct". Most people, when confronted with this list of selection criteria, would probably find some truth in each of them. To those of us who like compromises, it is tempting to conclude that all, or at least most, of the criteria are true but that different criteria are used in different contexts.

(a) Unexpected conditions. According to Mill, *"If we do not... enumerate all the conditions, it is only because some of them will in most cases be understood without being expressed, or because for the purpose in view they may without detriment be overlooked. For example, when we say, the cause of man's death was that his foot slipped in climbing a ladder, we omit as a thing unnecessary to be stated the circumstance of his weight, though quite as indispensable a condition of the effect which took place"*.

On this basis, some conditions are not mentioned because they are presumed to be already known to the listener, and stating them explicitly would be superfluous. Consequently, we select as causes only such conditions that are unknown or unexpected.

We do not generally require explanations when things behave normally; we ask "why" mainly when something unexpected happens. A relevant explanation will state events which were both unexpected and would have enabled us to predict the surprising event if we had known about them.

(b) Precipitating causes. It is often possible to divide the complete cause into more-or-less permanent states and instantaneous changes or events. We usually select the events immediately preceding the effect which we are trying to explain. In such cases, we explicitly use the distinction between permanent conditions and the instantaneous event which came last into existence.

(c) Abnormal conditions. This selects factors on the basis of making the difference between an accident and normal functioning. In a railway accident there are conditions such as the normal speed, weight of the train and routine stopping and acceleration. These conditions are true both in the case where such accidents occur and in the normal cases where they do not, and so we reject them as the cause of the accident, *even though it is true that accident would not have occurred without them*. It is this consideration that leads us to conclude that to cite factors which are present both in the case of disaster and normal functioning, would explain nothing: such factors do not 'make the difference' as would a bent rail.

There is substantial difference between unexpected and abnormal conditions: abnormality refers to objective facts; things are normal or abnormal independently of our knowledge of them, while unexpectedness refers to a subjective state.

(d) Variability refers to the selection of those conditions which are variable in contrast to more permanent conditions. This is a blend of the first three criteria discussed.

(e) Deviation from theoretical ideal. Theoretical concepts often guide causal selections. For instance, in explaining a deviation we select causes which are also deviations from an ideal model of the system in question.

(f) Responsibility. Causal statements may have an evaluative component. Indeed, the Greek word for cause, *aitia*, also means guilt. The ancient Greeks modelled their idea of causation in nature by analogy using ideas about social organisation. A *cause* was thought of as some-

thing that brings about a disturbance in state of harmonious equilibrium in nature, and the *effect* as something that restores this equilibrium, much as a punishment restores the social harmony after a crime. In general, we identify the cause of a tragedy before assigning blame. However, it may be claimed that in selecting among the causal conditions we pick out those events or actions which deviate, not from what is normal, but from what is good, reasonable or appropriate. A cause will often be an omission which coincides with what is reprehensible by established norms of conduct. Thus, when we say that a fire was caused by negligence of the authorities (who failed to notice the special dangers in the building), we are not denying that oxygen, a heat source etc. had something to do with it. Neither are we saying that negligence is abnormal. We are, rather, specifying what went wrong.

(g) Predictive value. This holds that an explanation for a certain event consists of information that, had we had access to it before the event to be explained occurred, would have enabled us to predict it. In view of this, a natural and intuitively compelling selection criterion would be that we select as the most important causes those that most effectively predict the effect.

(h) Replaceability and necessity. Most of us think about certain historical figures like Napoleon, Gandhi or Lenin as being important causal factors in history. Historians sometimes take a different view and argue against the role of the individual in history – that even if the person X had not done this or that, someone else would have done it instead, and therefore history would not have been much different. This argument does not deny that X did bring about certain things, only that X was not necessary. However, if there were other people with similar characters, motives etc., they could have achieved the same effects, hypothetically speaking. X was, we might say, replaceable, and therefore not as important a cause for historical developments as causes which were irreplaceable.

There are similarities between the replaceability criterion and the criterion of predictive value: a condition which could be replaced is also a bad predictor of the effect. However, predictive value focuses on the probability that the effect occurs, whereas replaceability focuses on the probability that the effect does not occur in the absence of the causal candidates.

(i) Instrumental efficacy. It is possible to consider causes as levers by means of which we can produce or prevent certain effects. If causality is viewed in this way, it is very natural to think that we select those conditions which enable us to manipulate effects. If we want to bring about something, we will select conditions which come as close as possible to being sufficient for a desired end, and if we want to prevent something, we select conditions which come as close as possible to being necessary for whatever it is we wish to avoid.

(j) Interest. This holds that causal selections are governed by the particular interests of the person giving an explanation. For example, explaining a road accident, a road engineer might point out that the road had a poor surface and that the cause of the accident was the slippery highway. A policeman might instead pick out some other factor, like the excessive speed of the car, and a psychologist yet another factor such as the driver's disturbed state of mind. Each person looks at the situation from a special point of view and singles out that factor that interests him or her most.

Appendix 6: Standards of Evidence

ECFA+ has three levels of confidence, these are denoted by: solid lines (established as fact); dashed lines (presumptions with some evidence, but not proof); and queries (queries need to be justified by some reasoning). It is essential that the analyst ensures that all items and connections shown in an ECF chart are supported by adequate evidence. What constitutes *adequate* is a complex matter that needs to be decided in context. This paper highlights principles for the reader to keep in mind during ECFA+; it does not advocate a particular standard of proof or any particular methodology for acquiring and handling evidence[8].

Reliability and validity

Reliability and validity are two qualities often associated with matters of measurement and which provide insight into the more general topic of evidence. *Validity* is the extent to which a quantity measures what it purports to. *Reliability* is the extent to which measurements of a given phenomenon give consistent results and are uninfluenced by other factors. Applied to evidence, *reliability* is about the way that the evidence was created, collected and relayed; whereas validity is about the extent to which evidence is a true indicator of the fact asserted. The two qualities are connected: evidence cannot be valid without being reliable; but reliable evidence can be invalid. In practice, validity often implies interpretation on the part of the person receiving the evidence.

Promoting reliability

Evidence can be seen as the link between a person such as an investigator and the specific condition or event from the past that they are considering. In this perspective, evidence can be seen as a process of communication between a particular historical state or action and the investigator. Error and distortion can affect any stage of this communication, which can be considered as a five stage process:

- Create – the change created in the witness plate[9] by the action or state in question;
- Collect – the collection of data from the witness plate;
- Conserve – the preservation of the data in or acquired from the witness plate;
- Convey – the transfer of the data to the investigator or other interested party;
- Consider – the examination of the data as evidence for the action or state in question.

Reliability is a necessary but not sufficient condition to consider when evaluating evidence. However, highly reliable tests and assessments can give the impression of scientific credibility which may seduce investigators into assuming that the data so produced are valid evidence about the matter question.

Assuring Validity

Assessing the validity of evidence is a matter of gauging the extent to which the evidence supports the assertion as fact of the event, condition or causal connection in question. The following questions may be useful in stimulating critical assessment if the validity of evidence:

- Could the same evidence support another interpretation?
- What other evidence would we expect to find given the fact in question?
- What is the justification for asserting a relationship between the evidence and the fact in question?

---

[8] For readers interested in the consideration of evidence within systems of law, texts such as Tapper (2003) and Giannelli (2003) are helpful guides. However, the detailed conventions developed in legal systems do not constitute a complete solution for the complex issues of evidence.

[9] Witness plates, which can be people or things, "provide data about the events that changed them" … "One investigative task is to identify the people and things who or which were the witness plates to an accident. Obtain the accident data, the signals, that the witness plates have captured, and then read the data to reconstruct the events that produced the data. The witness plate idea helps locate and evaluate sources of data recorded during an accident." (Hendrick and Benner, page 73-74, 1987).

Appendix 7: **ECFA+ criteria developed to assist the investigation of the emergency service response to the fire and explosion at Enschede, the Netherlands, 13 May 2000**

On 13 May 2000, there was a large explosion in the town of Enschede in the Netherlands. To advance the subsequent investigation, the emergency services needed to process substantial quantities of data collected by several teams of investigators from a variety of sources. To assist with this task, NRI worked with the investigators to develop criteria for identifying relevant events and conditions. The criteria are listed below:

A. Communication

1. inter-agency (e.g. between Fire Brigade and Police)
2. intra-agency
3. external

B. Decision making

1. assessing the situation (to inform decision making)
2. to deploy resources
3. to disseminate information
4. to enact a plan or procedure

C. Operation

1. actual deployment of resources (following decision making)
2. a planned change
3. unplanned change (positive)
4. unplanned change (negative)

The criteria have different bases: category “A” is needed to integrate data provided by the various agencies and to bring into focus command and control; category “B” makes decision-making visible to analysis, and; category “C” is an important catch-all that helps to identify differences between theory and practice of disaster management.

The criteria were used to filter the data obtained by the various investigation teams. When applied to reports, the investigators noted which criterion was relevant to each datum. This ensured that the transformation of source reports and other material into ECF charts was transparent. It also provided traceability between each item in the ECF chart and the evidence that corresponded to it.

Lastly, when applying criteria to select-in relevant data, it is prudent for the analyst to watch for instances where seemingly pertinent data are filtered-out. This “sense” check was applied by investigators in the Enschede analysis to develop and refine the criteria as well as to ensure that relevant data were included.

Appendix 8: Glossary of Terms

Action: The means by which an actor changes the state of an object. In ECFA+ actions are described using transitive verbs.

Active Voice: Chambers (1996) states that "A verb is said to be in the active voice when the subject of the verb is performing the action or is in the state described by the verb. 'Voice' is simply the technical word for that aspect of the grammar of verbs that is covered by the terms 'active' and 'passive'. For example, in *The boy stroked the cat,* the *boy* is the subject of the verb *stroked* and it is the boy who is performing the action of stroking; *stroked* is therefore in the active voice." … "The opposite of an active verb is a passive verb, as in *The cat was stroked by the boy*…".

As well as a clearly identified actor, each event need to be described using an accurate, clear-cut verb. The verb should make it easy to visualise the action, like a frame from a video. The active voice makes it clear who or what is acting; choosing an accurate action also needs to be clear. the rule is to be sure that the event is stated in a way that makes it clear what is acting, how it is acting and the object affected.

Actor: A person or thing that acts on an object.

Condition: A passive state that endures for some period of time. E.g. "40kph SE wind", "Valve shut", "Road open to traffic". Written onto pink Post-it Notes, if available.

Dashes** and **dashed-lines are used to denote uncertainty in ECF charts and can be applied to both connecting arrows and to the outlines of events and conditions.

ECFA+ is the acronym of the title "Events and Conditional Factors Analysis". The "+" character is used to distinguish this method from its predecessor "Events and Causal Factors Analysis" (Buys and Clark, 1995).

ECF chart: Any diagram produced by applying the ECFA+ procedure.

Event: A moment, generally of short duration, characterised by a change of state. In ECFA+, an event is described by the action of an actor on an object (e.g. "Car enters smoke plume", "Smith moves PTO lever to 'on' position"). Written on yellow Post-it Notes, if available.

List of Further Enquiries: an open-ended table in which questions and uncertainties can be noted as they arise during the investigation. An example is provided in Appendix 4.

Non-event: an event that would be expected to occur given the circumstances, but which in fact did not happen. In ECFA+, non-events are treated as conditions and the analyst is required to identify the standard of judgement that they are using – such as a procedure, custom or practice, or theory). This approach enables other stakeholders to challenge the judgement of the analyst and reminds the analyst of the need to justify their reasoning in such instances.

Object: The person or thing receiving the action of an actor.

Occam's razor refers to the principle of minimising the number of items in an explanation to only those needed. It is also sometimes called *the principle of economy*.

Primary Events/Conditions are generally close in time (i.e. minutes, hours, or days) to the unplanned outcomes in question. Primary is defined in relation to Secondary (see *Secondary Events/Conditions,* below*).*

Query: The third type of item that can be used in ECFA+ (the others are events and conditions). Queries are used to denote areas of uncertainty, especially where this has causal relevance. Written on blue Post-it Notes, if available.

Secondary Events/Conditions: Secondary events are included to explain the coming into existence of primary conditions; these may reach days, weeks, or years back in time from the unplanned outcomes which are the focus of investigation.

Simple Present tense: Chambers (1996) states that "The present tense of a verb is the tense which refers, among other things, to actions going on or states existing at the present time or in general". This is in contrast to the progressive or continuous form of the present tense which "…consists of the *-ing* form of the verb in combination with the auxiliary Verb *to be*".

Appendix 9: Changes (2014 ECFA+ manual compared to the 2007 version)

1. No blank check boxes

This version introduces a new way to manage further enquiries. In the previous version, the format and logic checking boxes would be ticked to show completeness, or else left blank. After further enquiries, the analyst would review these blank items. However, blank boxes can have several meanings, leaving the status of an analysis unclear. Blank boxes could mean that the item:

- has not been checked;
- has been checked and a problem found (e.g. missing data or lacking evidence);
- has been checked and found satisfactory, but the decision was not recorded.

2. Artwork has changed

The artwork of events and conditions has been changed to encourage analysts to record the results of checking format and logic. The boxes have been enlarged and the labels changed.

The labels of the boxes now read:

- “Format Status” (previously, “Format Check Passed”)
- “Logic Status” (previously, “Logic Check Passed”)

The enlarged boxes allow the analyst space to write a cross reference to a further enquiry. This takes the form ‘Qn’, where ‘n’ is the reference number of the entry on the further enquiry list.

3. First iteration: Maximum 12 events

Previously, the analyst was free to write out an unlimited number of events and conditions. This remains true, but an arbitrary maximum of 12 has been set on the number of events that can be written at the start of the analysis. As soon as the analyst reaches the stage of checking the logic, they are free to add more events and conditions.

This rule prevents the process being overwhelmed by too many items at the start of the analysis. Limiting the number avoids the following problems:

- slow progress, which discourages the investigator and costs time;
- unreliable format and logic checks, which allow errors and miss gaps;
- overcomplicated ECF charts, which limits their value to the investigation;
- stating events at a level of description that is unnecessarily low, which creates long chains of events where just one would be enough;
- analysis that is disconnected from the terms-of-reference of the investigation, in essence becoming the master rather than the servant of the investigator.

4. Readability

The main body of the text (i.e. pages 9-24 of the 2014 version) was re-written to bring it up-to-date and to improve readability. The authors checked the effect on readability using specialist software (Readability Studio). The software uses several measures, including the ‘Flesch Reading Ease’ which measures readability on a scale of 0-100, where 100 is the easiest. The main body of the 2007 ECFA manual scored 46, whereas the new manual scored 57.

The software estimated how easy the text would be for 'English as a second/foreign language' (ESL/EFL) readers. Using the McAlpine EFLAW test (McAlpine, 2006), the software predicts that ESL/EFL readers would find the 2007 manual “very confusing to read”. In contrast, the software predicts that these readers should find the 2014 manual “very easy to read”.

At the time of writing, NRI plans to release a Dutch version of the revised manual by 2015.

[This page is intentionally left blank]

NRI Document Improvement Proposal

1. Document reference	2. Version date	3. Document title
NRI-4 Rev 1	30 June 2014	ECFA+ Manual

4. Recommended improvement (identify page, paragraph and include modified text or graphic, attach pages as necessary)

5. Reason for recommendation

6. Originator of recommendation

Name:	Organisation:	
Address:	Phone: Fax: E-mail:	**7. Date of submission**

8. Send to NRI Secretariat

Name:	***Address:***	
Dr Rudolf Frei	NRI Foundation P.O. Box 286 2600 AG Delft The Netherlands	Phone: +44 (0)121 288 3206 email: info@nri.eu.com

NRI-1 (2009)

NRI MORT User's Manual

For use with the Management Oversight & Risk Tree analytical logic diagram

Second Edition

Produced by

The Noordwijk Risk Initiative Foundation

In Partnership with

Royal Dutch Navy
Koninklijke Marine

Published and distributed by:

The Noordwijk Risk Initiative Foundation
P.O. Box 286,
2600 AG Delft,
The Netherlands.

Email: Info@nri.eu.com
Website: www.nri.eu.com

ISBN 978-90-77284-08-7

NRI-1 (2009)

NRI MORT User's Manual

2nd Edition

for use with the
Management Oversight & Risk Tree
analytical logic diagram

20th December 2009

Based on the original manual (three revisions 1978-1992) prepared by Norm W. Knox and Robert W. Eicher on behalf of the System Safety Development Centre, EG&G Idaho, Inc. Idaho Falls, Idaho 83415 for the US Department of Energy.

This edition prepared by

J. Kingston, F. Koornneef, J. van den Ruit, R. Frei, & P. Schallier

on behalf of the Noordwijk Risk Initiative Foundation,
P.O. Box 286, 2600 AG Delft, The Netherlands.
www.nri.eu.com

Intended for use with the
MORT chart NRI-2 (2009), ISBN 978-90-77284-4

[This page is intentionally left blank]

Preface to the first edition

In 1971, William G. Johnson and I started the "trials at Aerojet": proving and further developing ideas that would eventually comprise the MORT Safety Assurance System. These trials were part of a project headed by Bill, which aimed to improve safety management in the US nuclear industry. We produced a system of ideas that sought to draw together Bill's lifetime of experience and the best practices of organisations such as those in the National Safety Council (NSC) network, a web in which Bill was richly connected. Using the expertise of our team and the test-bench of the Aerojet trials, we wove this into a coherent model of safety management. Bill wrote the result up in a report entitled "MORT: The Management Oversight and Risk Tree"[1]. This document succeeded in capturing much of the content of the project but only a little of the dynamism that animated the ideas. Nonetheless, it was enough to establish the organisation – the Safety System Development Centre (SSDC) – that served as the platform for our subsequent work in the industry and beyond. Initially, the mission of SSDC was the subject of a contract with the Atomic Energy Commission (AEC) and continued with ERDA, the Energy Research and Development Agency, and ultimately, DOE – the US Department of Energy.

The contract from the AEC is worthy of comment, it placed on us a requirement to make available in the public domain the knowledge developed within the project; this was a visionary step. It created a motor that drove innovation, in which success bred success. Through our tools, documents, training and consultancy, we established a reputation beyond the nuclear industry and attracted opportunities to help solve new problems through collaboration with the Military, World Bank and others. The experience we gained and the ideas that we jointly developed, were fed back directly into our mission and this was reflected in our public domain output. We used "MORT" as the collective term for this canon of work on risk management, to which the MORT diagram is the index.

From an early stage, MORT, the investigation method, developed a life of its own. During the original project (1969 to 1972), both senior line management and safety specialists warmly welcomed the investigation method. The public domain orientation of the SSDC meant that people outside the nuclear industry got to hear of MORT. In 1975, when the AEC was replaced by ERDA, and the mission broadened from nuclear to strategic energy (including oil and gas reserves), the international networks of these industries brought many new people to our door and several fruitful collaborations.

My connection to NRI has a number of strands. In 1975, I met Rudolf Frei at the Los Alamos National Laboratory. His PhD was the first connected to MORT, another was produced by John Kingston ten years later; both of these gentlemen later joining the board of the NRI Foundation. These two examples of collaboration are drawn from a pool of similar instances that affirm my view that intellectual generosity is in fact a wise investment! Since its inception in 1998, I have been pleased to advise the Foundation and to continue the dialogue about risk management. I am delighted that these investments are still showing a good return and look forward to the reading the ensuing chapters of the MORT book of knowledge that myself, Bill Johnson and our colleagues started penning some thirty years ago.

Dr Robert J. Nertney
December 2002

[1] MORT - The Management Oversight and Risk Tree, Prepared For The U.S. Atomic Energy Commission, Division of Operational Safety, Under Contract No. AT(04-3)-821, Submitted to AEC February 12, 1973 (San 821-2). Downloadable from www.nri.eu.com

Contents

Preface to the Second Edition

When NRI published the first edition of MORT User's Manual and Chart in 2002, the only version of the manual then available in the public domain was that written for the United States Department of Energy. Understandably, the DoE edition of the manual was written in American English and referred to documents and organisations that were relatively unknown to people outside of the intended readership. The manual was also ten years old.

The first edition of the NRI MORT User's Manual provided European users of MORT with a question set in British English. The revisers kept to the structure of the 1992 version of the MORT Chart and stayed close to the concepts of the original (1973) MORT text. The publication of the first edition also meant that the MORT method stayed available in the public domain and accessible via the internet.

This second edition arose from a project to translate the MORT user's manual and MORT chart into Dutch. This project was undertaken by the NRI Foundation in partnership with the Royal Dutch Navy. Early on in the project, the members of translation team realised that they were investing considerable effort to clarify – in English – the concepts behind some of the questions posed in the manual. In effect, the team were revising the English manual as a necessary prelude to producing a Dutch text. Furthermore, some of these clarifications suggested that changes were needed to the structure of the MORT Tree. To consider these structural changes, the Foundation formed a second team. Over a period of two years, these two teams have reviewed each other's ideas until consensus was reached about the changes to the MORT tree and the phrasing of the questions in the manual. In this way, a translation became a revision with a scope wide enough to justify the result as a second edition rather than as a minor revision.

The Board,
Noordwijk Risk Initiative Foundation
1st October 2009

Users Manual Part 1:
MORT and its Application

1 Introduction

The Management Oversight and Risk Tree (MORT) method is an analytical procedure for inquiring into causes and contributing factors of accidents and incidents. The MORT method reflects the key ideas of a 34-year programme run by the US Government to ensure high levels of safety and quality assurance in its energy industry. The MORT programme started with a project documented in SAN 821-2, W.G. Johnson, February 1973[2].

The MORT method is a logical expression of the functions needed by an organisation to manage its risks effectively. These functions have been described generically; the emphasis is on "what" rather than "how", and this allows MORT to be applied to different industries. MORT reflects a philosophy which holds that the most effective way of managing safety is to make it an integral part of business management and operational control.

This document describes how to apply MORT to incident and accident investigation. It is intended for use with the NRI MORT diagram, dated August 2009 available from "www.nri.eu.com". This manual is provided as a general guide to the investigative use of MORT, but it is in no way a replacement for a proper training in accident investigation. It is published to encourage the use of MORT and to promote the discussion of root cause analysis.

[2] SAN 821-2 can be downloaded from www.nri.eu.com

1.1 What is MORT

The acronym MORT is used to refer to four things:

1. a safety-assurance programme which ran between 1968 and 2002;
2. the body of written material which documented the programme;
3. a logic tree diagram: the Management Oversight and Risk TREE;
4. a method for helping investigators probe into the systemic causes of accidents and incidents.

This manual describes the item 4, the MORT Method, and is designed to be used with the MORT TREE (which can be found on the internet at www.nri.eu.com/NRI2EN.pdf).

The connection between these various senses of the term MORT is as follows. The project which started the MORT programme was documented in a report written by W.G. Johnson in 1973 (it is often referred to by its reference code, SAN 821-2; it is available from the NRI website). In the report, Johnson sets out the ideas that were incorporated into the MORT programme after a very wide survey of risk management practices in different industries around the world. Historically, the MORT diagram served as a graphical index to that report, arranging the ideas hierarchically in functional groups. This diagram was used by investigators and quality assurance specialists to systematically review a work activity or process. They were expected to know the material in SAN 821-2, and the body of documentation that accrued during the lifespan of the MORT programme, to which the chart was a ready-reference.

To help investigators, especially novices, the 500+ pages of the original report were distilled into question set of 40 pages. The questions are the main component of the MORT User's Manual. MORT as a method is now independent of MORT as a programme, certainly in Europe. In practice, the MORT programme documents (especially, SAN 821-2) have become disassociated from the MORT chart, leaving the MORT User's Manual as the most common reference for applying the MORT tree.

1.2 How is MORT applied to accidents and incidents

The MORT method consists of three steps:

Step 1: define the events to be analysed;

Step 2: characterise each event in terms of unwanted transfers of energy;

Step 3: evaluate the hypothesis that the unwanted transfers of energy were the result of how risks were being managed in the activity in which the accident occurred.

Step 1 is supported using a procedure called *Energy Trace and Barrier Analysis*, which you will find described on page xix. In this step the analyst is trying to identify a complete set of events comprising the incident or accident, and to define each event clearly. It is very difficult to use MORT, even in a superficial way, without first performing an Energy Trace and Barrier Analysis.

In Step 2, the analyst looks at how the energy was exchanged with the person or asset. This way of characterising accidents – as a series of 'energy exchanges' –was proposed by William Haddon[3] as a means of analysing accidents scientifically. There may be several different energy transfers that need to be considered in the same investigation. In this step, the analyst aims to understand how the harm, damage or danger occurred.

In Step 3, the analyst considers how the activity was managed. This step involves the analyst looking at the 'local' management specific to the activity and resources. The analyst also looks "upstream" to find management and design decisions about people, equipment, processes and procedures that are relevant to the accident. To help make this analysis systematic, the analyst uses the MORT chart; this lists the topics and allows an analyst to keep track of his/her progress.

Each topic on the MORT chart has a corresponding question in Part 2 of this manual. The questions in MORT are asked in a particular sequence, one that is designed to help the user clarify the facts surrounding an incident. The analyst, focussed on the context of the accident, identifies which topics are relevant and uses the questions in the manual as a resource to frame his/her own inquiries.

Like most forms of analysis applied in investigations, MORT helps the analyst structure what they know and identify what they need to find out; mostly the latter. The accent in MORT analysis is on inquiry and reflection by the analyst.

[3] This was reprinted in: Injury Prevention 1999;5:231–236.

2 Description of the MORT Tree

The MORT tree shares some of the conventions of Fault Tree Analysis, but other symbols and systems are also used.

2.1 Inputs, outputs and logic gates

Fault Trees are composed of *inputs* connected to *outputs* through *logic gates*. These inputs and outputs are generally called *events*. For example, in Figure 1, the output event, "Fire" is connected to the three input events, "Fuel Present", "Source of Ignition", and "Oxygen present".

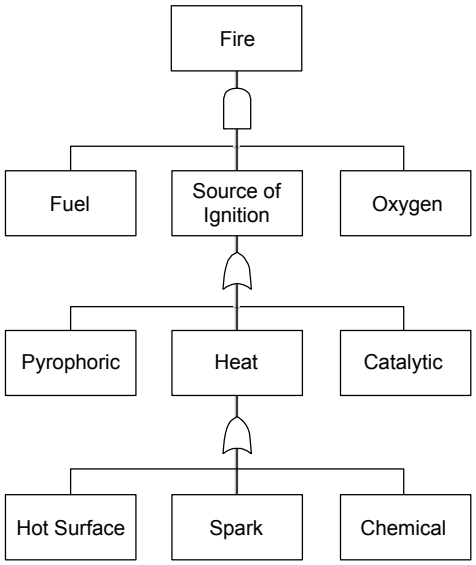


Figure 1. Example of Hierarchical Logic

The MORT chart uses logic gates. However, when using MORT in an investigative setting, the logic gates make little contribution to the analysis: they can safely be ignored.

In a theoretical setting, the logic gates have more significance. There are 93 logic gates in the MORT chart[6], only two of these are AND gates. The first of these AND gates remind the reader that although accidents are often produced by "Oversights and Omissions" these problems arise not just in the specific control of the activity, but also in the relevant management systems. This is illustrated in Figure 2.

[6] Not counting gates that are repeated by transfers (which account for another 180 or so)

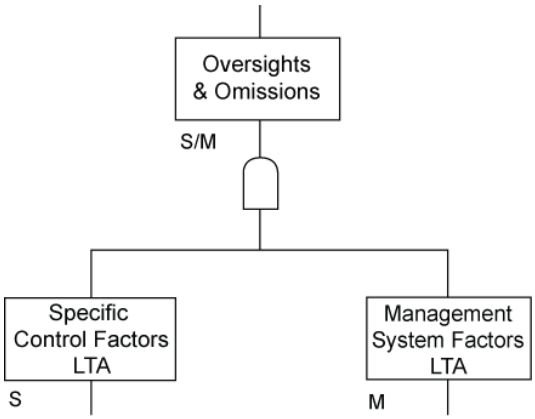


Figure 2: Oversights & Omissions arise from Specific Control Factors AND Management System Factors.

2.2 Sequences of energy exchanges

The second AND gate in the MORT tree comes from Haddon's energy exchange model of accidents, introduced earlier (page x).

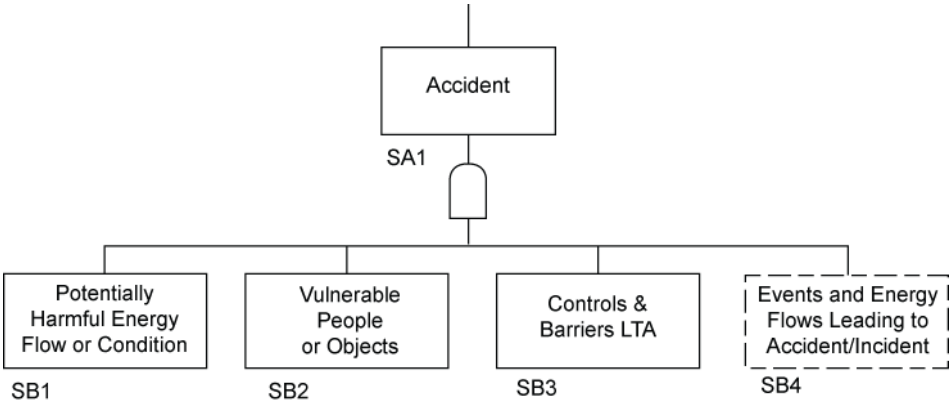


Figure 3. The elements of accident causation

In Figure 3, the AND gate is used to emphasise the point that an accident will occur only if certain elements are present; the accident would not happen were any one of these elements absent. Haddon's concept of "energy exchange" is shown as a triad in which

a potentially harmful energy flow is present, when
vulnerable people or objects are exposed, and
barriers and controls are not adequate to achieve protection.

Energy exchanges, Haddon argued[3], occur in sequences. This requirement is included as the fourth event input: *Events and Energy Flows Leading to Accident/incident*. Figure 3 shows this text enclosed within a dashed rectangle. These dashes symbolise two points for the analyst: first, that this input event is not analysed as part of the

MORT tree, but that; second, all of the events and energy flows need to be identified. This identification is done using Energy Trace and Barrier Analysis; described in in sub-section 3 (page xviii).

2.3 Systems of reference

The MORT chart uses several types of referencing: to link one part of the chart to another; to refer to the questions in Part 2 of this manual, and; to allow every item in the chart to be identified uniquely. All of these types of references are illustrated in Figure 4.

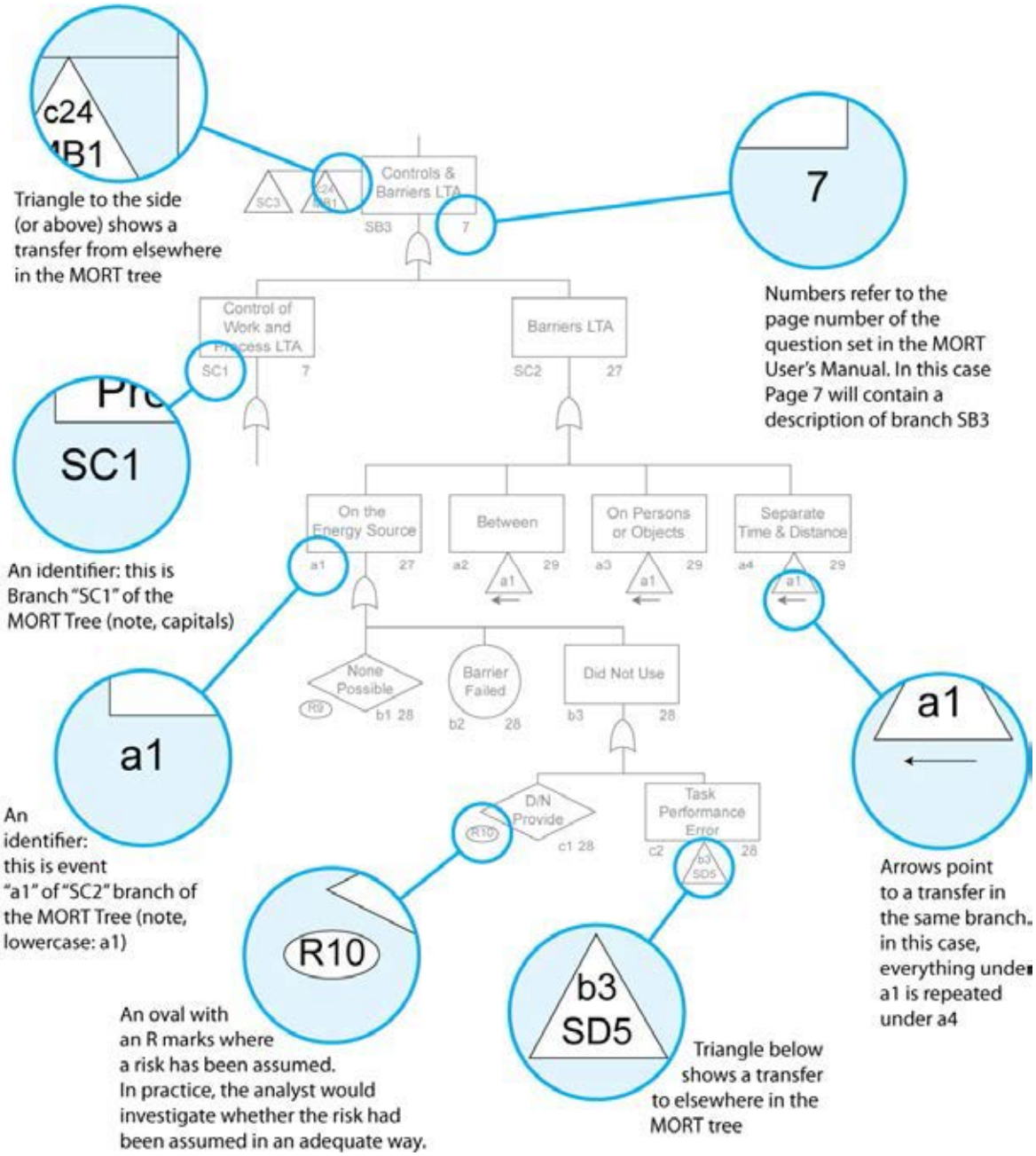
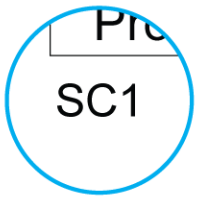
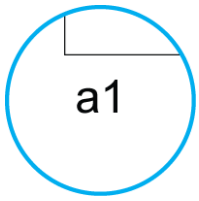


Figure 4. Examples of different reference types



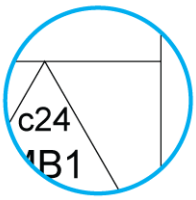
Every item on the MORT diagram has two references, an identifier (e.g. "SC2" is the identity of the MORT branch "Barriers LTA") and a reference to the relevant page of this manual. MORT identifiers follow a hierarchical scheme, reflecting the structure of the chart. The MORT chart can be divided into halves, "Specific Control" and "Management System". Identifiers use capital letters to show that the item is the top of a main branch. A main branch is one that can be regarded as having a distinctive theme, its own identity as it were. For these branches, a two-letter code is used. The first letter will be an 'S' or 'M' depending on whether it is the 'Specific Control' or the 'Management System' half of the MORT tree. The second letter will be an A, B, C or D, these letters corresponding to the tier, or level, of the branch in the tree. 'A' denotes a branch that is one tier down, 'B' a branch that is two tiers down, and so on. For example, in the case of MORT branch SC2, these conventions mean that it is a main branch that is three tiers down in the 'Specific Control' half of the MORT tree. The number 2 (of SC2) means that it the branch starts second from the left at the C-tier of the 'Specific Control 'half of the MORT tree. The numbering is methodical, and reflects the sequence in which the branches should be considered by the analyst. The main branches of the MORT tree are shown in Figure 5 on page xvii.



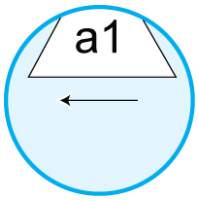
Within the branches of the MORT tree, the twigs or leaves are distinguished using lower case letters, 'a', 'b', 'c', and so on. As before, the choice of letter reflects the level in a hierarchy: 'a' identifies items at the first tier of a main branch, 'b' the next, and so on. The identifiers also have a number which reflects the sequence in which the analyst should work through the branch. For example, in Figure 4, 'b3' "Barrier Failed" is the third item in its tier. Most of the identifiers at the 'twig and leaf' level of the MORT tree are used many times in the tree as a whole. For instance, there are twelve instances of items called 'b3'. However, each instance is unique to its main branch. Hence, to refer to a specific 'twig or leaf', the identifier of the main branch is also given. In the case of leaf 'b3' "Barrier failed", this would be referred to as b3-SC2.

Transfers are another important type of reference system used in the MORT tree. In common with Fault Trees, the MORT tree contains branches that are repeated several times. Rather than draw the repeated branches in full, it is the convention to draw the branch just once and indicate where it is repeated with a triangle. The triangle is used because it resembles the shape of a fault tree. Figure 4, contains a number of transfers; item 'c2' (Task Performance Errors) serves as an example. Item 'c2' deals

with the possibility that people did not use a barrier, even though it was provided. There may be many explanations for this, and the analyst needs to look into the relevant possibilities. To help the analyst, a set of questions has been developed; these correspond to the 'twigs and leaves' of the tree referred to as b3-SD5 (a different branch of the Tree from c2). The triangle below 'c2' is labelled "b3-SD5"; this means that the 'twigs and leaves' below c2 can be found at b3-SD5.



Triangles below an item like c2, are called "transfers-out" and every transfer-out to another part of the MORT tree has a corresponding "transfer-in". In Figure 4, two transfers-in are shown by the triangles connected by lines to 'SB3', "Controls & Barriers LTA".



A variation on the use of triangles-to-show-transfers occurs when the repeated part of the tree is within the same branch as the transfer-out. In Figure 4, there is a triangle below 'a4', "Separate Time and Distance". This triangle, which is labelled "a1", has a left-pointing arrow drawn underneath it. The arrow is a reminder that the transfer is to another twig in the same branch, in this case 'a1'. Hence, at 'a4' when considering why a "separate time & distance" barrier (e.g. segregation of pedestrians from an area traversed by forklift trucks) did not prevent an incident, the analyst would take into account all the items mentioned below 'a1', namely b1, b2, b3, c1 and c2. Within-branch transfers-out do not have a corresponding triangular symbol showing the transfer-in.

The last type of reference used in the MORT tree is for "assumed risks". These are marked using an oval containing an 'R' plus a number; there is an example at 'c1' in Figure 4. At its highest level, MORT has two hypotheses to explain why loss may have occurred. The first is the "oversights & omissions" hypothesis, in which the analyst investigates whether the system, in its broadest sense, has not controlled its risks adequately. The second is the assumed risk hypothesis, in which the analyst investigates the possibility that the loss is the manifestation of a risk that had been properly managed and controlled, albeit at a probability greater than zero. In MORT tree analysis, the analyst may find one or more instances where an "assumed risk hypothesis" needs to be evaluated. A typical example can be seen at c1-SC2 in Figure 4, which deals with the possibility that a barrier was deliberately not provided. If the analysis reveals that c1-SC2 is relevant, the analyst needs to investigate the adequacy of the relevant decisions (i.e. to not provide the barrier and, probably, to control the

risk in other ways). The analysis of assumed risks is discussed further in the next sub-section.

2.4 Provisional Assumed Risks

In MORT analysis, losses can arise from two distinct sources: risks that have been identified and accepted correctly (called "assumed risks") and risks that have not been managed correctly (so-called "oversights and omissions"). In some accidents, there will be contributions from both of these sources.

MORT contains several referrals to the "Assumed Risk" branch. As you can see in Figure 5 (page xvii), the assumed risk branch occurs at the highest level in the MORT tree. In sub-section 2.3, it was described how the analyst might identify relevant assumed risks and that the decision-making surrounding these needs to be investigated. To avoid interrupting the analysis, the analyst can record assumed risks in the table provided on the MORT chart and follow them up later.

MORT Ref.	Description	Adequacy of Decision-making?
b2-SB1	Corrosive effect of salt water on steel pipework	
c1-a3-SC2	Did not coat outside of pipe with salt-proof layer	
d9-SD5	Did not undertake a job safety analysis because job judged to present only low potential risks	

Table 1. Example of entries in a Provisional Assumed Risk Table

2.4 Structure of the MORT Tree

The MORT tree structure is derived from a fault tree analysis of the event "losses". Note that loss is a very general term can apply to anything of value and any type of risk. The first tier answers the general question, "what types of risk would produce losses"? There are two possibilities: risks that were not adequately managed (Oversights and Omissions) or, risks that were adequately managed. Because the tree structure is explored in a set order – top to bottom, left to right – the next question is, "what would produce oversights and omissions"? The answer is given in the second tier of the tree: oversights and omissions arise from the control of the activity (Specific Control Factors) and how the risks of the activity are managed in general (Management System Factors). The rest of the tree is derived in the same way, with each tier "producing" the tier above it. Figure 5 is an overview of the main structure.

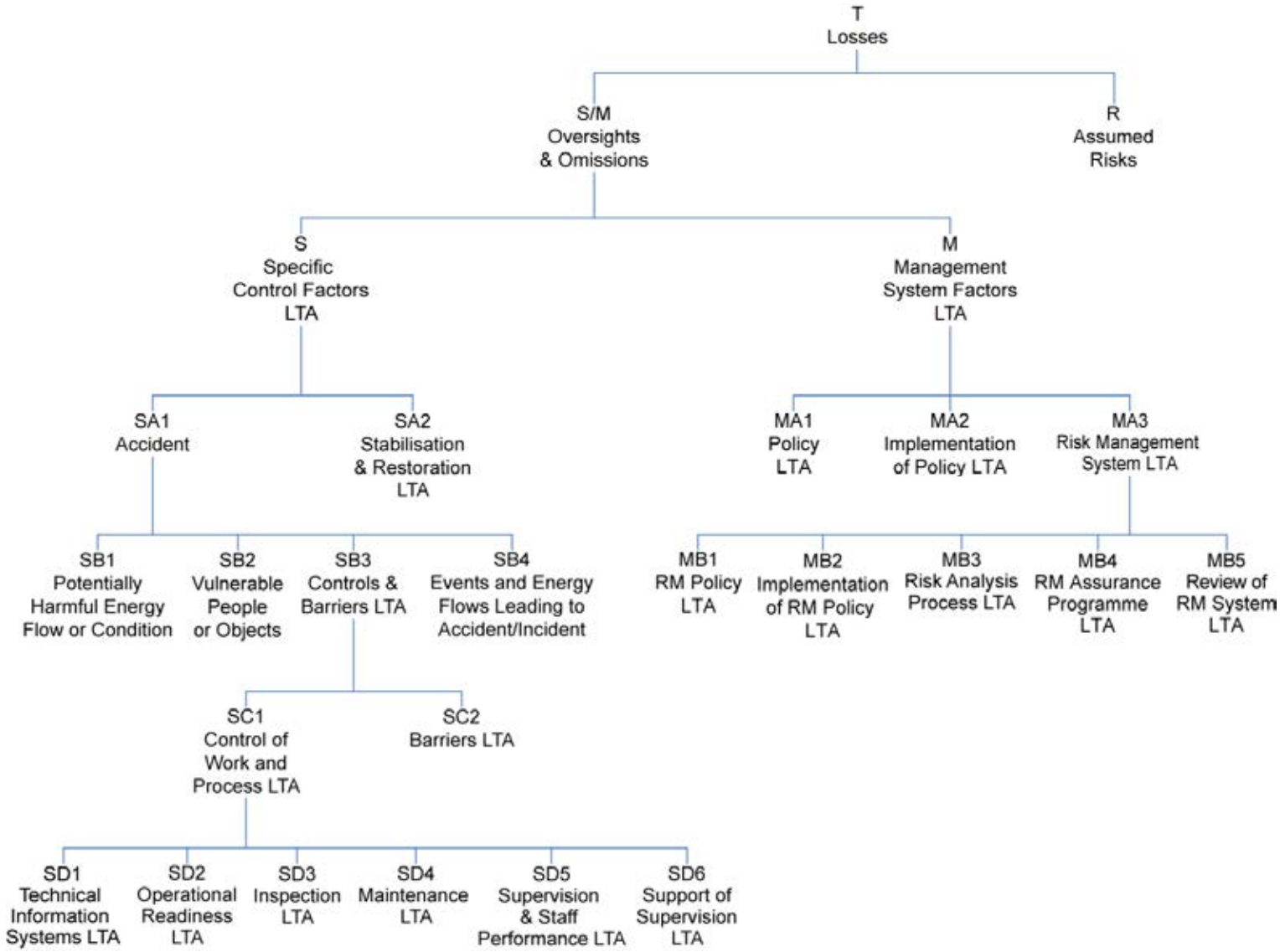


Figure 5.The Main Branches of the MORT Tree

3 Application of MORT to Investigations

Good investigations are built on a secure picture of what happened. MORT analysis needs this as a basis. Analysis using an appropriate "sequencing" method such as Events & Conditional Factors Analysis (ECFA+) can be effective and provides a detailed picture of the events comprising the accident. Using Energy Trace and Barrier Analysis is the way to connect MORT analysis to the events of the accident. Therefore, as soon as the factual picture allows it, carry out an Energy Trace and Barrier Analysis.

3.1 Energy Trace & Barrier Analysis

Energy Trace & Barrier Analysis (ETBA), or "Barrier Analysis" as it is usually called, is used to produce a clear set of episodes, or subjects, for MORT analysis. It is an essential preparation for MORT analysis.

Energy Flow or harmful Agent, adverse environment condition	**Target** Vulnerable person or thing	**Barriers & Controls** to separate Energy and Target

Table 2. Barrier analysis format

"Energy" refers to the harmful agent that threatens or actually damages a "Target" that is exposed to it. Although "Energy" and Energy-Flow are the terms most often used, harmful agents can include environmental conditions (e.g. biohazards, limited oxygen).

"Targets" can be people, things or processes – anything, in fact, that should be protected or would be better not disturbed by the "Energy". MORT defines an accident in terms of loss, so at least one of the targets in the accident sequence has to be valuable. However, incidents (sometimes called near-misses or near-hits) are also of interest.

The "Barrier" part of the title refers to the means by which "Targets" are protected from "Energies". As well as barriers (the nature of which is purely protective), the analysis also focuses on work/process controls as these also provide protection by directing energies (and targets) in a safe manner.

Very often, an accident reveals a number of events where energies met targets in unwanted interactions; Barrier Analysis seeks to trace meticulously all of these interactions and make them available to analysis. This means that a Barrier Analysis table may have have several rows, each row corresponding to a distinct episode of energy interaction with a target.

3.2 Procedure for Barrier Analysis

Requirements: Technical understanding of the system in which the incident occurred and enough information about the sequence of events to allow analysis to begin.

Objective: To account for all unwanted exchanges of energies and to make these available to subsequent analysis within the investigation.

Description:

1) Familiarise yourself with available information (including site if accessible)
2) Determine scope: limit to just those interactions producing harm/damage or include near-misses as well?
3) Create three columns (as shown in table 3)
4) Start in the TARGET column and identify a target that was harmed or damaged (or, if you are looking at near-misses, a target exposed to harm). Identify the energy flow (or harmful agent…) that is acting and describe it simply and with precision in the ENERGY FLOW column.
5) Next, consider the BARRIERS and CONTROLS that should have stopped or limited the interaction between Energy and Target.
6) Repeat this process for another unwanted energy exchange.
7) Review the list of targets for any omissions.
8) Number rows (each row is an episode of energy flow threatening or damaging a target) in chronological order. There should be continuity: do the events follow from one another?
9) Prioritise rows for analysis using MORT (e.g. *** = most important, * = least important)

Energy Flow or harmful Agent, adverse environment condition	**Target** Vulnerable person or thing	**Barriers & Controls** to separate Energy and Target
These may be energies (and harmful agents…) designed to do work in the work process or extraneous energies that act from outside the process. Be meticulous as this stage of the analysis. Energy exchanges can be in the 'reverse direction' (e.g. exposure to cold, loss of pressure). If there are multiple targets for a given energy flow, state each interaction in a separate row.	Targets can be valuable (i.e. a person or asset) or not. The reason for including targets that have no intrinsic value is to ensure the continuity and completeness of the analysis. Try to identify *all* targets involved in the incident (this leads to a clear insight into the state of risk control). Every target mentioned should be accompanied by a word or phrase that identifies the attribute altered. E.g. "Smith (bruised arm)", or "Car (near-side door crumpled)". Note that the object or actor that corresponds to a target at one point in the analysis may also play other roles.	Barriers are means of separation present solely for protective purposes. Controls are means of channelling energy or substances to do work (and provide protection as a by-product). Controls also limit the exposure of targets. It is most effective to identify <u>physical</u> barriers (including time & space barriers) and controls that have their effect at the coal face/shop floor. MORT analysis will tease out the procedural and upstream issues; do not force them. Include *absent* barriers & controls that <u>should</u> have been present according to an explicit standard or justification.

Table 3. Barrier Analysis Headings, annotated with guidance

3.3 Procedure for MORT Analysis

Requirements:

- Two people (ideally)
- Technical Understanding of system in which incident occurred
- Sufficient description of sequence of events to allow analysis to begin
- MORT Charts and coloured pens – Red, Blue, Green
- Means to keep notes of: "blue" items for further enquiry; justification for"red" and "green" items.

Objective: To understand how specific targets were exposed to harm, damage or unwanted change and to explain this in terms of risk management.

Description

1) Choose an event from your Barrier Analysis and write it on the MORT chart above SA1 "Incident"
2) Perform SA1 analysis
   a) Begin at SB1 ("Harmful energy flow…")
   b) Above SB1, state the energy flow
   c) Proceed through chart top to bottom, left to right, as shown in Figure 6
      i) Code RED or GREEN only with evidence and an explicit standard of judgement
      ii) Code BLUE if evidence or required standard is uncertain
      iii) Maintain your list of further enquiries as you go
      iv) Write any provisional Assumed Risks into the table on the MORT Chart
   d) Explore M-branch either
      i) Ad-hoc, during SB3 analysis, or
      ii) When SB3 ("Controls & Barriers LTA") completed
3) If needed, choose another event from your Barrier Analysis
   a) Use fresh MORT chart
   b) Repeat step 2
4) When all required SA1 analyses are complete
   a) Note on the barrier analysis an events that have not been subject to MORT analysis
   b) Move to SA2 – Amelioration
   c) Move to M-Branch and explore (ad hoc or in sequence) in the light of the SA2 analysis
   d) Review Provisional Assumed Risks
5) Review MB4 (Risk Management Assurance Programme) in the light of the analysis so far
6) Review the M-branch issues, taking the overview

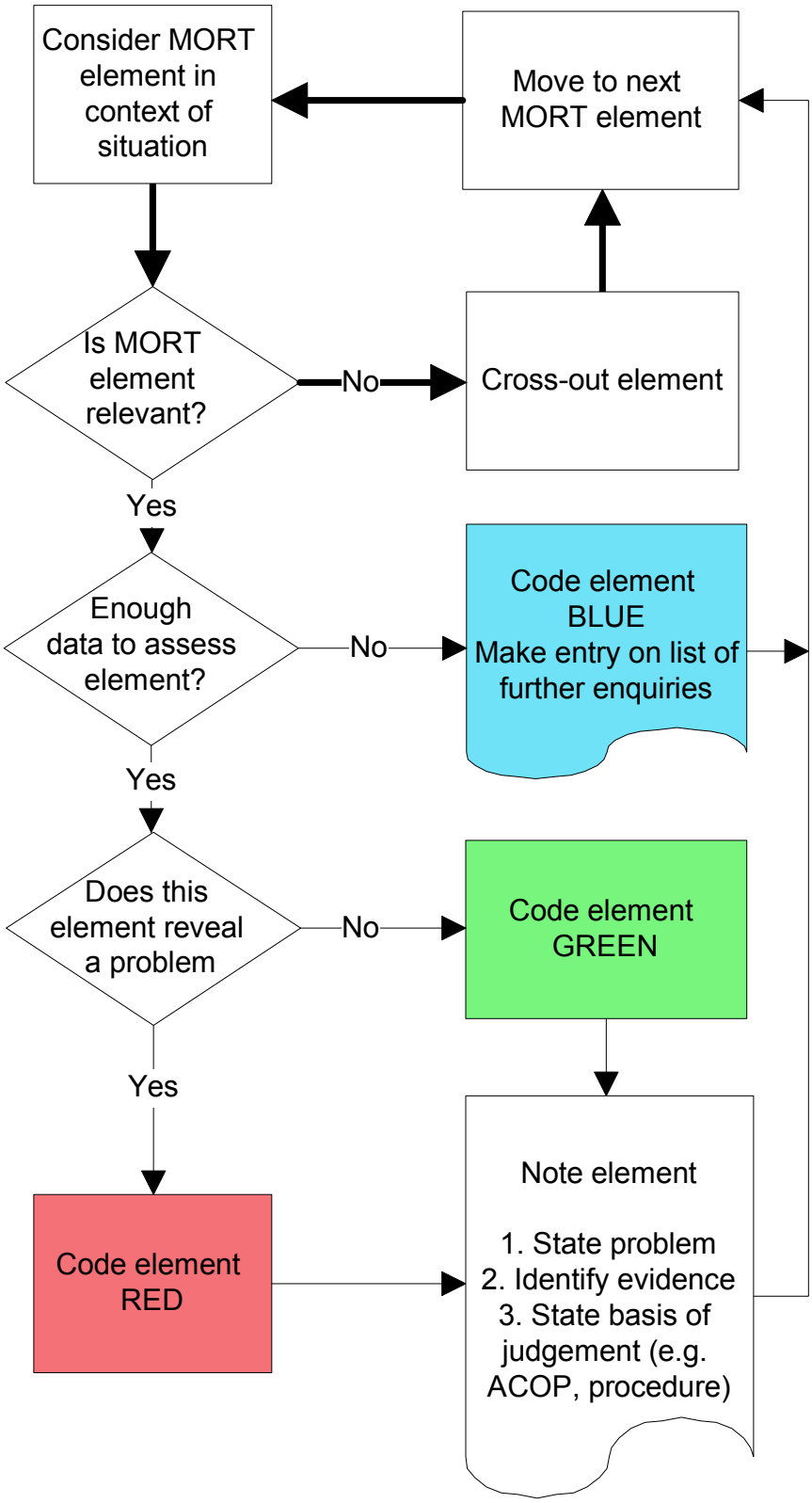


Figure 6. Sequence for work though the MORT Chart

(Note: ACOP, Approved Code of Practice)

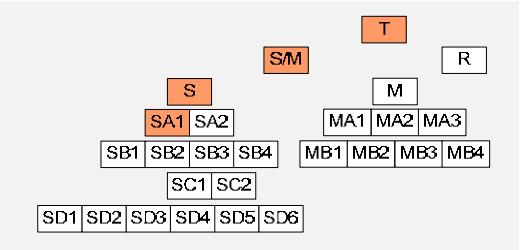
Users Manual Part 2:
MORT Question Set

Intended for use with the
MORT Chart, 2nd Edition, 2009

CONTEXT

T Fundamental questions
S/M Oversights and Omissions
S The Accident

SB1 The potentially harmful energy flow/environmental condition



T Fundamental Questions (the Top event)

- What happened?
- What was the sequence of events including the initiating event that marked the movement of the work/process from adequately controlled to uncontrolled?
- Describe the extent of harm and losses (including intangible assets such as reputation, customer confidence, employee morale).

Subsequent analysis will seek to establish

- *why the harm or loss occurred;*
- *what future undesired events could result from the problems identified.*

S/M. Oversights and Omissions

This tree considers two explanations for the incident. The first explanation to be evaluated is that the incident was due to problems in the planning, design or control of work/process. The second explanation considered in this branch is that the incident was an acceptable outcome of the risk management process – an assumed risk.

S. Specific Control Factors

This half of the MORT tree addresses:

- *the specific controls upon harmful energies*
- *the specific controls upon vulnerable people and assets*
- *the barriers between energies, and people and assets*
- *how emergency actions contributed to the final outcome of the accident.*

As you go through the analysis, consider the future possible effects of the control problems identified. This helps to assess the seriousness of the control problems.

SA1. Accident

MORT analysis may involve more than one sweep through SA1. You are advised to decide at the outset how many energy-flow/target interactions (also called 'energy transfers') you intend to include in your analysis.

SA1 analysis leads naturally to:

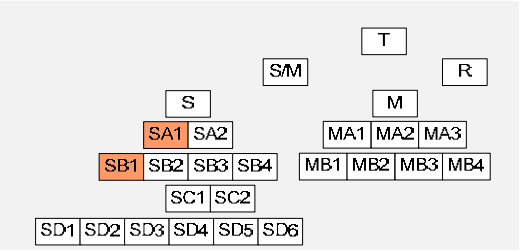
- *consideration of the Management System Factors, and*
- *judgement about whether decisions to accept risks were appropriate or not.*

SB1. Potentially Harmful Energy Flow or Environmental Condition

This branch considers the harmful energy/environmental condition in question. The purpose here is to gain a clear insight into the control issues.

To make this applicable to a wider range of circumstances, 'energy flow' has been extended to include harmful environmental conditions, e. g. a lack of oxygen in a confined space.

SB1 is considered for one energy flow (and associated barrier failures and damage) at a time. The analysis will need to be repeated for other energy flows within the event sequence describing the accident.



CONTEXT

SA1 The Accident

SB1 The potentially harmful energy flow /environmental condition

a1. Non-functional Energy

Consider this branch if the energy flow or environmental condition causing the harm was not a functional part of or product of the system.

A non-functional energy flow is an energy flow which is not meant to be there or did not contribute to the intended purpose or function of the system.

When deciding whether the energy flow was or was not intended, you will need to consider whose perspective to adopt. For example, the intentions of designers, managers, operators and observers may differ.

b1. Control of Non-functional Energy LTA

- Was there adequate control of non-functional energy flows and environmental conditions?

You need to think about what is adequate given the circumstances.

b2. Control Impracticable

- Was such control practicable?

Note that event b2 is flagged with R1 assumed risk symbol. If the control was not used because it was judged impracticable, the decision to leave the risk uncontrolled needs to have been "assumed" correctly. A decision to assume the risk must have been taken by an appropriate person in a suitable manner.

If you are using colours to mark-up a MORT chart, this event should be provisionally coded blue; and an entry made in the "Provisional Assumed Risk" table drawn up for this investigation (see page 56, and section 2.4, page xvi in the introduction).

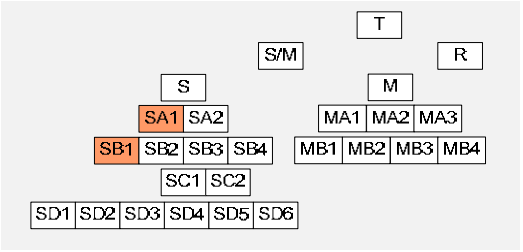
The event cannot be closed until justification for assuming the risk has been evaluated. Justification may be very different in different circumstances.

a2. Functional Energy

Consider this branch if the energy-flow (or environmental condition) was functional, but was used without adequate barriers in place.

Functional energy flow is an energy flow which is meant to be there and contributes to the intended purpose or function of the system.

MORT assumes that energy should only be applied if the barriers are adequate, if the barriers are inadequate, energy should not be applied or used only in reduced amounts.



b3. Control of Use LTA

- Was the energy applied at the right time and in the right amount?
- If not which controls of the energy were less than adequate?

b4. Diversion LTA:

- This branch considers diverting harmful functional energy away from vulnerable people or objects.

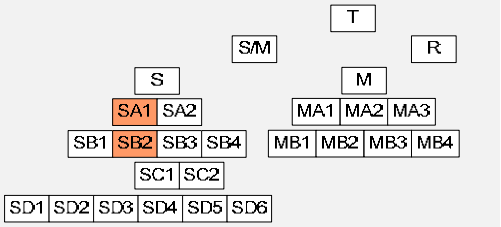
c1. Control of Functional Energy LTA

- Was there adequate diversion of harmful energy flows or environmental conditions?

c2. Diversion of functional Energy LTA

- Was diversion impracticable?

Note that event c2 is flagged with an R2 assumed risk symbol. See page 56, and section 2.4, page xvi in the introduction.



SB2. Vulnerable People or Objects

This branch considers who or what was exposed to the harmful energy flow or environmental condition. The purpose here is to gain a clear insight into the control issues.

SB2 is considered for one energy flow (and associated barrier failures and damage) at a time. The analysis will need to be repeated for other energy flows within the event sequence describing the accident. Section 2.1 in Part 1, discusses the number of energy flows to be considered.

For loss to occur something of value must be damaged or someone must be hurt. However, MORT can also be used to consider incidents where loss does not occur (e. g. near misses) but where energy was out of control.

a1. Non-functional

Consider this branch if the person or object exposed to harm was not a functional part of the system.

A non-functional person or object is one which was not meant to be there. That is, someone or something that did not contribute to the intended purpose or function of the system or is not intended to be part of the system under consideration.

b1. Control LTA

- Was there adequate control of non-functional persons and objects?

b2. Control Impracticable?

- Was such control practicable? (Note that event b2 is flagged with R3 assumed risk symbol)

Example - personnel passing through a worksite to reach an adjacent worksite

a2. Functional

Consider this branch if the person or object was functional, but was exposed without adequate barriers in place.

When deciding whether the presence of the person or object was or was not intended, you will need to consider whose perspective to adopt. For example, the intentions of designers, managers, operators and observers may differ.

b3. Control of exposure LTA

- Were the people or objects in place at the right time?
- If not, what controls to prevent persons or objects from being exposed were less than adequate?

b4. Evasive action LTA

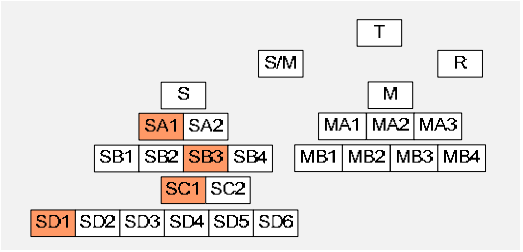
- This branch considers the evasion of harmful energy flows and environmental conditions.

c1. Means of Evasion LTA?

- Given that people and assets could be present, were the means provided to allow people or assets to avoid the harmful energy flow or dangerous conditions adequate?

c2. Evasion Impracticable

- Was evasion impracticable?



SB3. Barriers and Controls LTA

This branch considers whether adequate barriers and controls were in place to prevent vulnerable persons and objects from being exposed to harmful energy flows and/or environmental conditions.

Barriers are purely protective. They need to be designed to fit the characteristics of the energy flows involved and the targets that could be exposed. Examples include machinery guards, PPE, firewalls, blast walls and pipe-work integrity.

SC1. Control of work and process LTA

This branch considers the adequacy of the control system for the work activity or process in question. Six aspects of the control system are considered:

- *Technical information systems [SD1]*
- *Verification of operational readiness [SD2]*
- *Inspection [SD3]*
- *Maintenance [SD4]*
- *Supervision [SD5]*
- *Supervision support [SD6]*

Controls are "controls of work and process" which may also serve to offer protection. Examples include safe operating procedures, toolbox talks, permits to work and isolations.

At this point, you should be able to clearly describe the work activity, equipment or process in question. Diagrams and technical expertise may be needed to support this.

SD1 Technical Information Systems LTA

This branch is about the adequacy of the information system designed to support the work/process in question. This is considered in three ways:

- *Providing information about the technology, activities and materials deployed; Examples – Toolbox talks, formal operator routines, task work pack containing necessary information on codes, standards and safety critical issues.*
- *The monitoring systems that measure the behaviour and efficiency of the "work flow process";*
- *Actions triggered by the results of the monitoring process (e.g. triggering of Risk analysis).*

a1. Technical Information LTA:

This branch considers the contribution of technical information to the control of the work flow process in question.

You need to consider:

- *the timing of information;*
- *the format of information;*
- *the capability for triggering necessary actions;*
- *who will be receiving/exchanging information;*
- *the availability of expertise and technical guidance.*

b1. Knowledge LTA:

This branch is about whether the people making decisions about this work/process were adequately knowledgeable or had access to adequate knowledge.

This includes people managing or supervising the work and people doing the work.

c1. Based upon existing knowledge

This branch considers the application of existing knowledge about the energy flow and/or problem in question.

You will need to find out whether or not there is precedent for the unwanted energy flow.

d1. Application of Codes and Manuals, LTA?

- Were the work/process and related issues adequately addressed by codes and manuals; and,
- Did individuals making decisions adequately apply the knowledge from codes and manuals?

d2. List of Experts LTA

- Was the list of experts (to contact for knowledge) adequate?

d3. Local Knowledge LTA

- Was any relevant but unwritten knowledge about the work flow/process known to the "action" person (the action person is the individual, or individuals, undertaking the work task/process)?

When deciding the adequacy of the list of experts, you need to consider:

- *Accessibility*
- *Availability*
- *Applicability*
- *Any constraints*

d4. Solution Research LTA

- Was there any research directed to the solution of known work flow/process problems and was this adequate?

c2. If there was no known precedent:

- (meaning: no known precedent for the unwanted energy flow and its prevention)

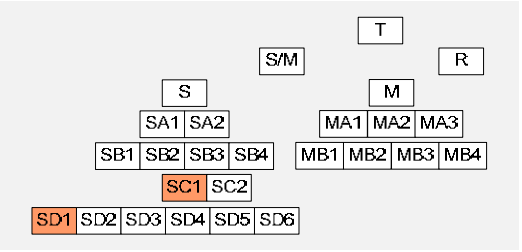
Consider this branch if the problem in question has <u>not</u> been experienced before within the organisation or elsewhere.

d5. Previous investigation and analysis LTA?

- Have there been previous similar accidents or incidents, or risk assessments of this work/process?
- Were these investigations or assessments adequate?

d6. Research LTA?

- Was there any research directed to the identifying and solving work flow process problems? Was this adequate?



b2. Communication LTA:

This branch considers the adequacy of communication of knowledge about the specific problem in question

c3. Internal Communication LTA

This branch considers the adequacy of internal communication of knowledge about the specific problem in question

Consider:

- *the magnitude of hazard involved;*
- *the relevant people, and their different roles in relation to the work/process;*
- *the range of communication channels e.g. procedures, training, supervision, task risk assessment, etc.*

d7. Internal Network Structure LTA

- Was the structure of the internal communication network adequate?

d8. Operation of Internal Network LTA

- Was operation of the internal communication adequate?

Consider:

- *all types of network, formal/informal, including verbal, written and IT*
- *Who needed to know what information and when?*
- *Did people know how to get information if they had a problem?*

c4. Was the external communication LTA?

- This branch is about the adequacy of communication between the organisation and any relevant external sources of knowledge.

d9. External Network Definition LTA?

- How well had the organisation identified external sources of knowledge relevant to the work/process?
- How well was the organisation connected to any relevant external sources of knowledge?

d10. External Network Operation LTA

- Was information obtained from these external sources in an effective way?

a2. Data collection LTA

This branch considers how the organisation captures data about its own operating experience.

The purpose of collecting this data is to provide feedback to improve the work/process.

The focus here is not only data current to the problem under consideration but also the collection of relevant data before the incident to detect problems at an early stage.

b3. Monitoring Plan LTA?

- Was there an adequate plan for monitoring the workprocess and conditions?

b4. Independent Review LTA?

- Did an independent organisation/person review the work/process to identify high potential hazards? Was the review done adequately?
- If no review, should one have been undertaken?

b5. Use of Previous Accident/Incident Information LTA?

- Was information about relevant problems from earlier incidents/accidents used adequately?
- When there are relevant previous incidents:
  - had the work/process been improved in the light of findings and recommendations?
  - were improvements documented?
  - had relevant information been made available to people employed within the work/process?

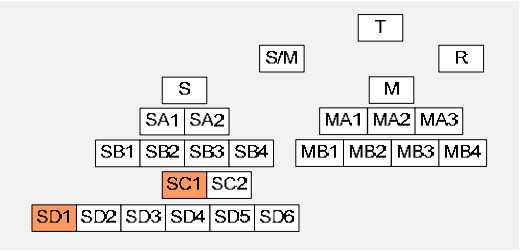
b6. Learning from employee/contractor's personnel experience LTA

- Was there an adequate method for gaining insights into operating experience of the work/process?
- Might it have provided information to identify the problem in question?
- Was there a plan for undertaking research to identify insights? Was it adequate?
- Was there an adequate system for collecting and using employee suggestions?

It is rare that problems are entirely new, but awareness of them may not have reached people in a position to solve them. In view of this, methods such as critical incident studies aim to provide an opportunity to operating personnel to relay their concerns relating to a specific work activities and processes.

b7. Were routine inspections of the work/process LTA?

- Did they adequately consider safety, health and protection of the environment?



b8. "Upstream" process audits LTA

- Was an adequate system in place to assure the quality of the planning and design of the work/process?

"Upstream" work processes include design, construction, selection and training, etc.

b9. Health monitoring

- Was the monitoring of the general health of operational personnel in the work/process LTA?

Audits of planning and design these processes need to include examination of the three basic work ingredients - hardware, procedures, and people.

a3. Data analysis LTA

This branch considers whether data relevant to the work/process had been adequately analysed.

b10. Priority problem list LTA?

- Is the problem in the work/process included on the priority problem list?
- Should it have been?
- Is the absence of the problem in question from the list, an indication that the list is not up-to-date?

A priority problem list (a list of the highest risks) is a statement of the most serious risks assumed within the organisation. These are residual risks that have been accepted for on-going operations after review and reduction measures. The purpose of this list is to maintain awareness of these problems at the appropriate management level.

Each level of management may have its own priority problem list. You should consider whether this is appropriate in the organisation that you are considering.

Data are not informative without analysis. Furthermore, certain forms of analysis can detect patterns not otherwise discernible, for example trend analysis and other forms of projection. Graphical analyses are particularly useful.

Analyses should provide decision-makers with adequate information and interpretation to make appropriate decisions about risk.

Analysis is a continuous process that should aim to provide the best understanding based on the most current and relevant information.

b11. Statistics and Risk projection LTA?

- Were the available status statistics, predictive statistics and projections adequate? Would they have alerted management to the problem in the work/process?

b12. Status Display LTA

- Was there an adequate single information display point for managers to help them keep abreast of current problems, analyses, and results?

a4. Triggers to Risk Analysis LTA

This branch considers whether problems in the work/process should have triggered the risk analysis process before the incident in question.

Triggers are related to change. Planned change will involve pre-set triggers, for example introducing new equipment or new working methods should be informed by risk analysis. Unplanned change needs to be detected by monitoring and analysis, these in turn need to be designed to trigger risk analysis where appropriate. Risk analysis should then initiate appropriate action to reduce risk.

b13. Sensitivity LTA

- Was the technical information system sensitive enough to trigger risk analysis for the individual problem (within the work/process in question)?

b14. Priority Problem Fixes LTA:

- If this was a problem on the Priority Problem List? Did the technical information system trigger the risk analysis process?
- If not, does this indicate less than adequate trigger arrangements?

b15. Planned Change Controls LTA

- If there had been a planned change in the work/process, did the people volved in making that change adequately recognise the need for risk analysis?
- Were the pre-set triggers to initiate risk analysis adequate?
- Was the fact that the risk analysis process was not used, evidence of inadequacies in the change control process?

Planned changes relates both to changes to plant and procedures

b16. Unplanned Change Controls LTA

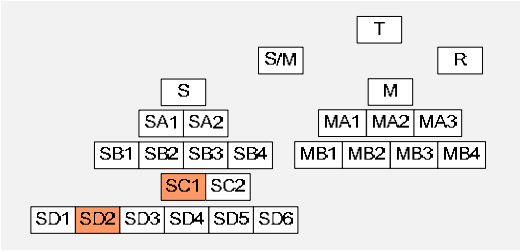
- If there has been unplanned change in the work/process, were the people involved in making that change adequately aware of the need for risk analysis?
- Were there adequate pre-set triggers to initiate risk analysis?
- Was the fact that the risk analysis process was not used, evidence of problems in the change control process?

b17. New Information Use LTA

- Were risk analysis process triggers from research, new standards, etc. , adequately recognised and used?

a5. Independent Audit and Appraisal LTA:

- Was the technical information system subject to adequate review?



SD2. Operational Readiness LTA

This branch considers the adequacy of efforts to ensure that work/process or site was ready to be used or occupied. If operational readiness was not assured, control of the work/process may have been inadequate. Consider readiness in terms of:

- *plant/hardware;*
- *procedures/management controls; and,*
- *personnel.*

This branch deals with "Here & Now Readiness" the purpose of which is to ensure that the requirements specified by planners and designers are met when the work/process or equipment is actually used.

Examples – isolation certificates, hand-over certificates, work permits and inspection of the worksite.

Later in the M-branch (branch b14-MA3), you will consider the second component, "Specification of Operational Readiness". This is the outcome of a task, equipment or process design activity.

a1. Verification of operational readiness LTA

This branch considers whether verification of the operational readiness of the facility and work process was adequate.

b1. Did not Specify Check

- Was an operational readiness check specified for this work/process?
- Would an adequate operational readiness check have identified the problem in question?

b2. Readiness Criteria LTA

- Were the criteria used to check operational readiness, adequately specified?

b3. Verification Procedure LTA

- Was the required procedure for determining operational readiness adequate? Was it followed adequately?

b4. Competence LTA

- Were the personnel who made the decision on operational readiness adequately skilled, competent and experienced?

b5. Follow-up LTA

- Were all actions - identified through operational readiness checks - adequately followed up?
- Were all outstanding actions resolved before start-up of the work/process?

a2. Technical Support LTA:

- Was adequate technical support provided to assuring the readiness of the work/process?

Technical support (e.g. by scientists and engineers) at the work site is particularly important to ensure readiness.

a3. Interface between Operations and Maintenance or Testing Activities LTA:

- Was the interface between operations personnel and testing or maintenance personnel adequate?
- Could procedures have prevented misunderstandings about the state of operational readiness?

a4. Configuration LTA:

- Was the actual physical arrangement or configuration of the work/process identical with that required by latest specifications and procedures?

SD3. INSPECTION LTA

Inspections are done to determine the state of equipment, processes, utilities, operations, etc.

Questions are the same as Maintenance LTA (SD4)

SD4. MAINTENANCE LTA

This branch considers the contribution of maintenance (or inspection) of equipment, processes, utilities, operations, etc relating to the problem in question.

Maintenance or inspections may be carried out by the organisation directly or by agents (e.g. contractors) acting on its behalf.

a1. Planning Process LTA:

This branch considers whether the scope of the (inspection or) maintenance plan adequately considered all the areas relevant to the problem in question.

Was management aware of any aspects relevant to the problem in question not included in the plan?

b1. Specification of Plan LTA:

This branch considers whether the problem in question is related to how the maintenance (or inspection) plan was specified.

c1. Maintainability (Inspectability) LTA:

- Is the problem in question a result of inadequate maintainability (inspectability)?

c2. Completeness of the Plan LTA:

- Is there an adequate inventory of what is to be maintained (or inspected)?

c3. Schedule LTA:

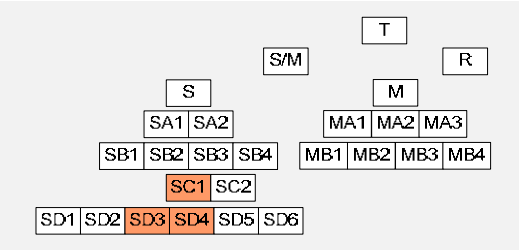
- Did the plan schedule maintenance (inspections) frequently enough to prevent or detect undesired changes?
- Was the schedule readily available to the maintenance (inspection) personnel?

c4. Co-ordination LTA

- Did the (inspection or) maintenance plan adequately address methods for minimising problems with disruption to equipment, processes, utilities, operations, etc. when they are undergoing maintenance (or being inspected)?
- Was the schedule co-ordinated with operations to minimise conflicts?

c5. Competence LTA:

- Was personnel competence adequately specified/developed for the maintenance tasks (inspection tasks) in question?



b2. Analysis of Failures LTA:

- Have previous relevant failures of equipment/process been subject to adequate analysis for cause?
- Were such analyses adequately specified by the plan?
- Did an appropriate individual or group adequately act upon the results of such analysis?

Previous near-miss or incident investigations may also have highlighted the need for maintenance (or inspection) plans to be modified.

a2. Execution LTA:

This branch looks at whether the problem in question is a result of how the maintenance (or inspection) plan was executed.

b3. "Point of Operation" Log LTA:

- Is the problem in question connected to whether a log of maintenance (inspections) was available at the point of operation of the piece of equipment, process, or activity?

A "point of operation log" can be a document that is kept with the equipment concerned to allow ease of examination. Alternatively, the log can be made available using e.g. handheld computing devices that provide local (to the equipment) access to the necessary records.

Logs need to be read out in order to function.

b4. Failure caused by maintenance (inspection) activity:

- Was the problem in question the result of a failure introduced by maintenance (inspection) of the work/process?

b5. Time LTA:

- Was the time specified in the plan's schedule sufficient to adequately perform each task?
- Was the time allocated for personnel adequate to fulfil the schedule? Was the time actually made available?

b6. Task Performance Errors:

- Were the individual tasks (as set out in the plan) performed properly?
- If not, identify who is performing which task and the nature of the errors made. Then refer to further questions in Task performance errors (SD5 , this begin on page 18).

SD5. Supervision and Staff Performance LTA

This branch is about the role of supervision and staff performance in the control of work/process in question.

a1. Time LTA:

- Did the supervisor have sufficient time to thoroughly examine the work/process?

a2. Continuity of Supervision LTA:

- Were there any gaps or confusions in the transfer or hand-over of supervisory tasks related to the problem in question?
- If the supervisor was recently transferred to the job, was there procedure for transfer of risk information from the old to the new supervisor?

Hand-over includes shift changes, new employees and hand-over of responsibility for a location. Examples include:

- *hand-over logs between supervisors back-to-back on shifts*
- *transfer of responsibility on a permit-to-work, or suspension and re-instatement of permits.*

The purpose of supervision is to ensure that an activity or process is working, or will work, smoothly.

It is supervision that is under examination - the emphasis is on what not who. You will need to consider what constitutes supervision, in terms of:

- *Hierarchical levels*
- *Boundaries and interfaces of supervision*
- *Duties and motivations*
- *For any one supervisor, the prevailing circumstances at the time in question. This will often include exploring the supervisor's workload around the time in question*

a3. Detection/Correction of Hazards LTA:

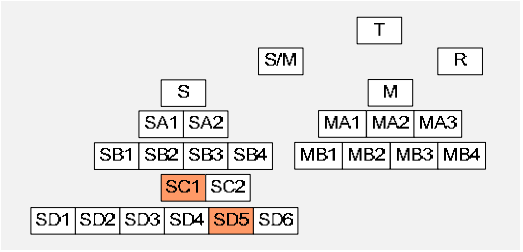
This branch considers whether the supervisor's efforts in detection and correction of hazards were systematic and adequate.

b1. Detection of Hazards LTA:

This branch considers whether the problem in question was related to pre-existing hazardous conditions which went undetected by the supervisor.

c1. Checklists LTA:

- If there was a checklist of hazards in the specific work/process, was it used correctly?
- Did the absence of such a checklist contribute to the problem in question?



c2. Detection Plan LTA:

This branch considers whether there was a systematic approach to uncovering hazardous conditions in the work/process.

d1. Logs, Schematics LTA:

- Was there adequate information available at the point-of-operation to help the supervisor to inform his risk detection?
- Were maintenance and inspection logs available at the equipment concerned adequate?
- Were work diagrams adequate?
- Was the use of labels/tags to signify changed equipment or settings adequate?
- Was the point-of-operation posting of warnings, emergency procedures, etc., provided for?

"Point-of-operation" means the equipment, workstation or area in question.
If relevant, a permit-to-work system should feature the posting of warnings and emergency procedures. Where PTW is not relevant, "General Detection Plan" is the catch-all phrase for ensuring that warnings and emergency information is established and maintained at the point-of-operation.

d2. Supervisor's Monitoring Plan LTA:

- Would the problem in question have been detected by a planned approach to inspecting and monitoring the status of the work/process (i.e. equipment, procedures, and personnel)?

In evaluating this issue you need to consider how the organisation guided and supported the supervisor's efforts. Also consider whether he was given guidance on detection of individual personnel problems, such as alcoholism, drug use, personal problems etc.

d3. Review of Changes LTA:

- Were any changes involved in the work/process, whether planned or unplanned, known to the supervisor? Was his response adequate?
- Was the supervisor's method of detecting and reviewing change adequate?

d4. Did not Relate to Prior Events:

- If there were problems in the work/process before the incident, did the supervisor consider the impact these might have on quality and safety?
- Was the supervisor aware of other signs or warnings that the work/process was moving out of control?

For example, a machine that continuously blocks may provoke users to clear the blockage without turning off the machine.

c3. Time LTA:

- If the problem in question was not identified before the incident, had the supervisor adequate time to detect the hazards?

Consider the supervisor's workload, especially if this is spread over a number of locations. It may be necessary to find out when the supervisor last inspected the area, and if any unsafe condition present in this accident/incident was also present at the time of this inspection.

c4 Workforce Input LTA

- If the workforce already knew about the problem in question, was this information passed on to the supervisor?

Knowledge of hazards is often available from the work force. The supervisor must be receptive, accessible and must act constructively on suggestions. As a rule, it is preferable to involve the people who will be involved or who are already familiar with the work/process in question in task specific risk assessment.

b2. Correction of Hazards LTA:

This branch considers whether the problem in question was related to detected hazards which went uncorrected by the supervisor.

c5. Interdepartmental Co-ordination LTA:

- If the work/process involved two or more departments, was there sufficient and unambiguous co-ordination of activities between the departments?

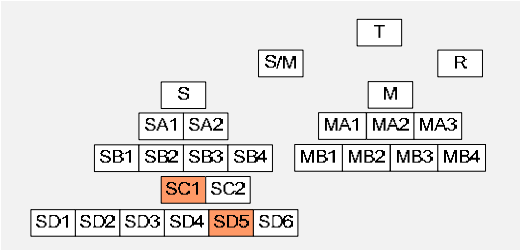
Interdepartmental co-ordination is a key responsibility supervision and line management. It should not be left to work level personnel.

c6 Postpone

- Was the supervisor's decision to accept the risk associated with postponing the correction adequately reached?

Event c6 is flagged with R5 assumed risk symbol. It was an assumed risk only if it was a specific named event, analysed, calculated where possible, evaluated, and subsequently accepted by the supervisor who was properly exercising management-delegated, decision-making authority.

The event cannot be closed until justification for assuming risk has been evaluated. If you are using colours, this event should be provisionally coded blue.



c7. Did not Correct in Time:

This branch considers whether the problem in question could have been corrected if the supervisor had acted in time. The scope of action includes acting directly or referring the problem to an appropriate authority.

d5. Authority LTA

- Was the supervisor's decision to delay hazard correction made on the basis of limited authority to stop the work/process?

d6. Budget LTA

- Was the supervisor's decision to delay hazard correction made on the basis of budget considerations?

d7. Time LTA

- Was the supervisor's decision to delay hazard correction made on the basis of time considerations?

c8. Housekeeping LTA:

- Would adequate housekeeping have prevented the problem in question?
- Was the storage plan for unused equipment adequate?

c9. Supervisory Judgement:

- Was the judgement exercised by the supervisor (not to correct the detected hazard) adequate considering the level of risk involved?
- Has a precedent been established that the supervisor does not act in such circumstances?

Review the supervisor's decision not to act on the hazard. Reasons include perceived ownership, authority to act on hazard, risk perception (underestimating risk, overestimating cost of correction).

a4. Performance Errors:

This branch considers how errors made by front-line personnel contributed to the problem in question.

There are few "unsafe acts" in the sense of blameworthy frontline employee failures. Assignment of "unsafe act" responsibility to a frontline employee should not be made unless or until the following preventive steps have been shown to be adequate:

- *risk analysis;*
- *management of supervisory detection; and*
- *review of procedures for working safely;*
- *Human factors review of*

b3. Task Performance Errors:

When using this branch, you need to have in mind specific errors that contributed to the problem in the work/process.

c10. Task Assignment LTA:

- Was the problem in question a result of how the task was assigned by the supervisor to the member of staff?
- Was the assigned task properly scoped with steps and objectives clearly defined?
- Was the task one an employee should undertake without specific instructions from the supervisor?

c11. Task Specific Risk Assessment Not Performed:

This branch considers whether a task specific risk assessment should have been carried out for the work/process in question. This is of particular concern in situations where a task specific risk assessment has not been applied despite the existence of significant risks.

MORT analysis proceeds on the premise that a task specific risk assessment should always be made for tasks assessed as having high hazard potential. Pre-Job Analysis is an example of how tasks can be surveyed step-by-step to determine hazard potential and therefore the level of risk assessment to be applied to the task/job.

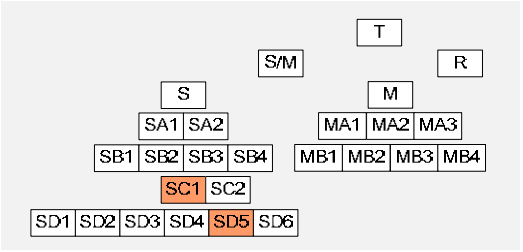
d8. High Potential was not Identified

This branch assumes that a high potential for harm or damage arising from the work/process in question has not been identified by screening.

Ordinarily, MORT assumes that a structured process e. g. Pre-Job-Analysis should be applied to screen the work/process for hazards and identify the need for a risk assessment. The structured process should identify the potential for error, injury, damage, or for encountering an unwanted energy flow.

e1. Task Analysis Not Required

- Did management require a pre-job-analysis to be performed for the work/process in question?



e2. Task Analysis LTA

- If required, was the pre-job-analysis adequate for the work/process in question?

Task Analysis is an example of how tasks can be surveyed step-by-step to determine hazard potential and therefore the level of risk assessment to be applied to the task/job.

e3. Task Analysis Not Made:

- This branch considers the failure to do a pre-job-analysis that was required for the work/process in question.

f1. Authority LTA

- Was the Task analysis not carried out because of lack of authority or because the duty had not been assigned for the work/process in question?

f2. Budget LTA

- Was it because of budget reasons?

f3. Time LTA

- Was it because of time constraints?

f4. Supervisory Judgement LTA

- Was the pre-job analysis not carried out for the work/process in question because of an inappropriate decision by the supervisor?
-

You will need to consider who was in a position to do the analysis and when they could have done it.

d9. Low Potential:

- Was the work/process in question identified as one involving low risk potential? Was this a reasonable assessment?
- Was the supervisor the right person to make this decision?
- Note the event is flagged with R6 assumed risk symbol.

Event d9 is flagged with R6 assumed risk symbol. If the criteria for risk identification and assessment were properly met, this event transfers to the Assumed Risk branch.

The event cannot be closed until justification for assuming risk has been evaluated. If you are using colours, this event should be provisionally coded blue. See page 56, and section 2.4, page xvi in the introduction.

c12. Task Specific Risk Assessment LTA:

This branch considers whether the task specific risk assessment for the work/process in question was adequate and scaled properly for the hazards involved.

The effort that is directed to task specific risk assessment, should be proportionate to the magnitude of the risk posed by the task. In order to determine the magnitude of the risk, some sort of analysis, e.g. pre-job analysis, needs to have been carried out.

d10. Task Specific Risk Analysis LTA:

This branch considers whether the quality of the task specific risk analysis contributed to the problem in question.

e4. Knowledge LTA:

- This branch considers whether there was adequate knowledge available to the task specific risk analysis in question.

f5. Use of Workers' Suggestions and Inputs LTA:

- Were workers' suggestions and inputs adequately used in the task specific risk analysis?

f6. Technical Information Systems LTA:

- This branch considers whether the task specific risk analysis was adequately supported by technical information.
- Analysis of the possible reasons for inadequacy is shown under SD1.

Technical information relevant to risk aspects of the work/process often exists but is not available to the "action" persons carrying out the task specific risk assessment.

Your evaluation of SD1 should be from the perspective of developing a risk assessment.

e5. Execution LTA

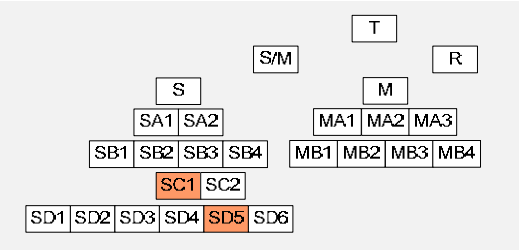
- This branch considers the quality of the task specific risk analysis.

f7. Time LTA:

- Was there sufficient time to adequately perform the task specific risk analysis for the work/process in question?

f8. Budget LTA:

- Was there a sufficient budget?



f9. Scope LTA:

- Were the scope and detail of the task specific risk analysis sufficient to cover all risks related to the work/process in question?

f10. Analytical Skill LTA:

- Were the experience and skill of the supervisor and other participants adequate to accomplish the required task specific risk assessment?

f11. Hazard Selection LTA:

This branch considers the omission of a hazard relevant to the problem in question. Hazard selection is critical to the adequacy of the task specific risk analysis.

g1. Hazard Identification LTA

- Were the criteria used to identify hazards for adequate?

g2. Hazard Prioritisation LTA

- Were the methods used in prioritising the identified hazards adequate?

d11. Recommended Risk Controls LTA:

This branch considers whether the problem in question was related to the adequacy of controls recommended by the task specific risk assessment.

Risk controls in the work/process in question could involve facilities, equipment, procedures and personnel.

e6. Clarity LTA:

- Were the recommendations from the task specific risk assessment sufficiently clear to permit their easy use and understanding?

e7. Compatibility LTA:

- Were the recommended controls compatible with existing controls and requirements that apply to the work/process in question?

e8. Testing of Control LTA:

- Were recommended controls tested in situ for effectiveness before being implemented?

e9. Directive LTA:

- Was the directive for use of the recommended controls adequate?

Was the directive explicit and impossible to misunderstand?

e10. Availability LTA:

- Were the recommended controls available for use by personnel involved?

e11. Adaptability LTA:

- Were the recommended controls designed in a way that allowed them to be adequately adapted to varying situations?

e12. Use Not Mandatory:

- Was use of the recommended controls mandatory?

Event e12 is flagged with the R7 assumed risk symbol. If use of the recommended controls was optional, you need to evaluate whether the failure to use them was a correctly assumed risk or a management system failure.

The event cannot be closed until justification for assuming risk has been evaluated. If you are using colours, this event should be provisionally coded blue; and make an entry made in the "Provisional Assumed Risk" table drawn up for this investigation.

c13. Pre Task Briefing LTA:

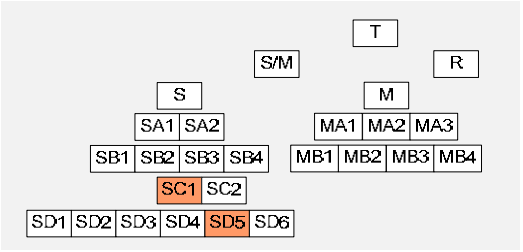
- Was the workforce given an adequate pre-task briefing (prior to performing the task)?

For example, did the briefing include new hazards, the effect of recent changes, such as changes arising through maintenance, new equipment, etc.?

c14. Fit between Task Procedures and actual Situation LTA

- Did the procedure, whether oral or written instruction, fit with the actual requirements or circumstances of the work/process in question?

Aspects of the situation that were not adequately addressed by the procedure should be noted. In practice, you will need to review the relevant procedure.



c15. Personnel Performance Discrepancy:

This branch considers whether the failure of individuals to perform their individual task assignments contributed to the problem in question.

Possible causes of performance discrepancy should be considered for each individual whose performance was judged to vary from correct practice.

d12. Personnel Selection LTA:

This branch considers how selection contributed to the problem in question.

e13. Criteria LTA:

- Did the definition of job requirements result in the selection of an individual who was unable to perform the task in question reliably?

e14. Testing LTA:

- Was an adequate (i.e. valid and reliable) method used to test the candidates against the criteria established for the job.
- Had there been a timely re-examination of the individual against the requirements established for the task?

d13. Training LTA:

This branch considers whether the training of the individual contributed to the performance error.

e15. No Training

- Was the individual trained for the task he or she performed?

Event e15 is relevant if the task required training to achieve reliable performance

e16. Criteria Training LTA:

- Was the individual unable to perform the task in question correctly because of inadequate definition of his or her training needs?

e17. Methods LTA:

- Did the methods used in training adequately prepare the individual to meet the requirements established for the task?

Consider methods such as realistic simulation, programmed self-instruction, and other special training in addition to basic initiation, plant familiarisation, etc.

e18. Trainer Skills LTA:

- Did inadequacies in the professional skills of the trainers compromise the performance of the task in question?

e19. Verification LTA:

- Was the verification of the person's current competence adequate?
- Were re-training and re-qualification requirements of the task adequately defined and enforced?

Did the verification process include initial testing and later assurance of task performance to ensure that the standards established for the task were met?

d14. Consideration of Deviations LTA:

This branch considers whether the supervisor was adequately alert to earlier personnel performance and variability.

e20. Normal Variability:

- Was the individual's performance within the range of normal variability?

Some degree of variability is normal and expected. Normal personnel performance variability is viewed as manageable through appropriate equipment design, good planning, training, and application of human factors.

e21. Changes:

- Did the supervisor detect individual personnel problems, such as alcoholism, drug use, and personal problems?

Consider this question (e21) if the individual's performance in the task in question was significantly different from the performance standard needed for the task.

Some degree of change is normally expected to occur. Significant change may be associated with illness, fatigue, personal problems, etc. These factors may result in individual performance beyond the normal range of variability. MORT assumes that the supervisor will be alert to such changes.

e

e22. Supervisor Observation LTA:

- Did the supervisor observe the individual performing incorrectly (i.e. extreme variability or significant change in the individual)?

e23. Supervisor Correction LTA:

- This branch is concerned with whether the supervisor's actions to correct the individual's performance were adequate.

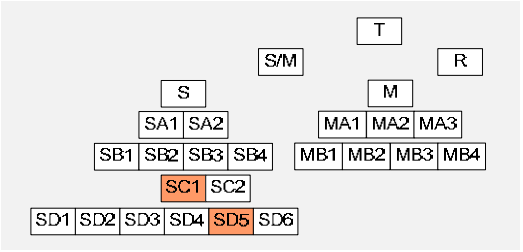
f12. Re-instruction LTA:

- Did the supervisor adequately reinstruct the person as to the correct performance?

Enforcement –You need to consider the work environment. Where rule-breaking has become acceptable, isolated enforcement action by the supervisor may not be either effective or fair.

f13. Enforcement LTA:

- Did the supervisor enforce established correct rules and procedures?
- Were disciplinary measures ordinarily taken against personnel who wilfully and habitually disregarded rules and procedures?



d15. Employee Motivation LTA:

This branch considers whether employee motivation contributed to the incorrect performance of the task in question.

You may better understand how the organisation failed to motivate the individual to perform the work to the required standard by looking at why the individual made the choices he or she made. To do this we need to consider the situation, in particular the rewards and punishments, from the individual's perspective.

e24.Leadership and Example LTA:

- Was the individual poorly led?

e25. Time Pressure:

- Was enough done to limit time pressure and workload to a for the individual acceptable level?

  Consider this question if time pressure was perceived by the individual who made the performance error.

e26. Correct Performance is Punished:

- In the past, was the employee "punished" for performing the task in question correctly?
- Was the supervisor sufficiently alert to this factor?

From the viewpoint of the employee, sometimes there is an undesirable consequence to the person doing a good job.

Punishment does not have to be something intended by supervision, it can be the product of poorly designed work and processes. To understand this, you will need to consider the situation from the individual's perspective.

Leadership and example are difficult to measure but you will need to consider their adequacy, particularly within the line organisation. Aspects of leadership relevant to the task performance issue might include:

- *the consistency through different levels of management;*
- *whether managers decisions and actions match the values they espouse, do they they 'walk the talk'*
- *the visibility of management concern to the individual whose task performance you are considering; and*
- *the vigour with which management expresses its concern.*

e27. Incorrect Performance is Rewarded:

- Did the employee find the consequence of doing the task in question incorrectly more favourable than doing it correctly?
- Was the supervisor sufficiently alert to this factor?

e28. Job Interest Building LTA:

- Does performing the task well really matter to the individual performing it?
- Did management adequately foster the individual's interest in the work?

e29. Group Norms Conflict:

- Did management make adequate efforts to actively engage the individual/group in activities likely to promote agreement about what is important (i.e. policy issues and goals of task performance)?

Consider the question of group norms conflict (e29) if there was disagreement between management and the workforce about the performance of the task

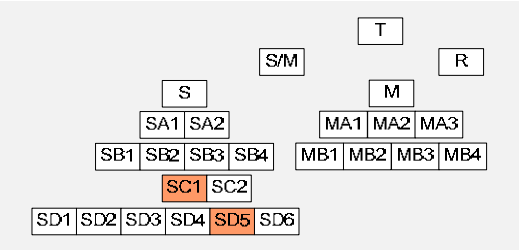
Activities might include participation in implementation of new equipment and working practices, training, projects and investigations.

Attitudes and experiences, particularly those held in common within a peer group (norms), will influence how people interpret task requirements. Performance errors may result from differences in norms between those designing or managing task re-

e30. Obstacles Prevent Performance:

- Were there obstacles that prevented the individual from performing the task to an acceptable level?

Obstacles need to be considered from the individual's perspective. They might be physical or situational in nature.



e31. Personal Conflict:

This branch considers the contribution of individual personal conflicts to the performance error in question.

You will need to explore the work relationships between the individual concerned and co-workers and supervisors.

You will need to consider that there may be a range of people providing supervision to this individual.

f15. [Conflict] with Supervisor:

- Was the relationship between the individual and the supervisor obstructive to adequate performance of the task in question?

f16. [Conflict] with Others:

- Was the relationship between the individual and other workers in the work environment obstructive to adequate performance of the task in question?

f17. Deviant:

- Were the psychological traits exhibited by the individual judged acceptable when considered in the context of the task requirements and related risks?

Event f17 is flagged with the R8 assumed risk symbol. Individuals exhibiting high levels of social maladjustment, emotional instability, and conflict with authority may be more unpredictable and unreliable than others. You need to evaluate whether the decision to employ the individual was a correctly assumed risk or a management system failure. The event cannot be closed until justification for assuming the risk has been evaluated.

If you are using colours, this event should be provisionally coded blue; and an entry made in the "Provisional Assumed Risk" table drawn up for this investigation. See page 56, and section 2.4, page xvi in the introduction.

e32. General Motivation Programme LTA:

- Was there adequate use of motivational programmes to develop desired behavioural change in individuals?

b4. Performance Errors in unrelated tasks:

This branch considers whether the control of the work/process in question was compromised by activities that are not directly part of the task.

c16. Allowed activities:

- Did an allowed activity, unrelated to the work/process in question, contribute to a problem in the control of the work/process?

"Allowed" meaning that the activity was not in conflict with the rules. Examples are going to or from the work area, authorised work break, lunch, etc.

c17. Prohibited activities:

- Did a prohibited activity, unrelated to the work/process in question, contribute to a problem in the control of the work/process?

A prohibited activity is one in violation of rules, such as horseplay. If the prohibited activity been performed in the past without impinging on the control of the work/ process, you will need to consider what was different that made it a problem on this occasion.

b5. Emergency Shutoff Performance Errors:

Use this branch if an emergency was in progress at the time in question. It considers the contribution of errors made during emergency shutdown resulting in:

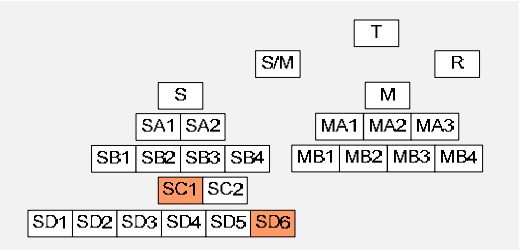
- ❖ failure to restore control of the work/process in question; and/or
- ❖ interference with the control of other work/processes (i.e. shutdown causes a new problem).

c18. Task Performance Errors:

- Did the incorrect execution of an intentional shutdown contribute to the control failure in the work process?
- If the emergency shutdown was not error-free, what were the performance errors? Consider these errors using the questions in branch SD5 b3 (Task Performance Errors). These begin on page 18.

c19. Unrelated Task Errors:

- Did an error in an unrelated activity compromise the execution of a planned shutdown sequence?



SD6. Support of Supervision LTA

This branch considers whether upper level management supported their organisation adequately.

Consider the following questions in the light of any supervisory problems identified through earlier stages of your analysis.

a1. Help and Training Supervisors LTA:

- Is the problem in question connected to the on-going help and assistance given to supervisors to enable them to fulfil their roles?
- Was the feedback to the supervisor about his/her performance adequate?
- Had the supervisor been given adequate training in general supervision?
- Had the supervisor been given adequate training in safety and risk management?

a2. Research and Fact-Finding LTA:

- When needed, was information concerning the control of the work/process researched and provided for the supervisor?

a3. Information Exchange LTA:

- Did a lack of open and frank communication between upper and lower levels contribute to problems in the control of the work/process in question?
- Was communication always verified through feedback?
- Is there a history of shared responsibility (between the supervisor and people providing support) for resolving problems?

a4. Standards and Directives LTA:

- Where codes, standards, and regulations (internal or external) did not cover the control of the work/process in question, did management develop adequate standards and issue appropriate directives?

a5. Resources LTA:

This branch considers whether inadequate resources for supporting the supervisor contributed to the problems in the control of the work/process in question.

b1. Training LTA:

- Was there sufficient training to update and improve needed supervisory skills?

b2. Access to Expertise

- Did supervisors have their own technical staff or access to individuals with technical expertise?
- Was technical support adequate for their needs?

b3. Access to Equipment & Materials LTA:

- Did supervisors have sufficient access to relevant equipment, materials and other services?

b4. Co-ordination of Resources LTA:

- Were resources adequately managed to avoid conflicts between different users and prevent duplication of effort?

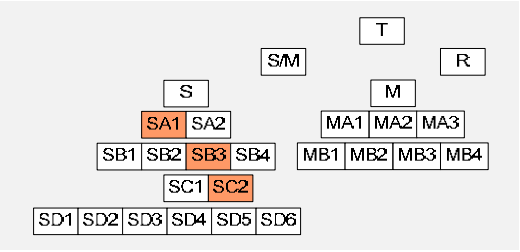
a6. Deployment of Resources LTA:

- Did ineffective use of the available resources contribute to the problems in the control of the work/process in question?
- Was the means of prioritising the use of resources adequate?

Event b21-MB3 (see page 53) considers management arrangements for immediate action on hazardous and otherwise serious problems

a7. Referred Risk Response LTA:

- Was management adequately responsive to problems referred from lower levels?
- Should the issue in question have been dealt with as a matter of urgency?
- Was there a process for dealing with urgent situations or high risks that had been newly recognised? Was the control problem in question already the subject of a referral from lower levels to management?



SC2. Barriers LTA

This branch will prompt you to identify each barrier that was in place, or that should have been. MORT considers four classes of barrier, but you do not need to be overly concerned with the accuracy of your classification, as the classes are just there help you consider the range of barriers that could have been used.

If a barrier was absent or not used you need to state the reference that requires it. References may include a technical standard, a regulation, a risk assessment.

An ETBA (barrier analysis) will facilitate the identification of barriers that you will consider in this branch.

A Barrier is any device or method designed to protect vulnerable "targets" from sources of harm. Targets include people or objects. Vulnerability of a target is specific to the energy or particular environmental condition concerned.

a1. On Energy Source

This branch considers the adequacy of barriers on the energy source.

Barriers of this type are protective devices and systems that were or could be applied to the energy source or environmental condition. The adequacy of the barrier depends upon the nature of the energy and vulnerable target in question.

Note all lower tier development under this event also transfers to events a2, a3, and a4. This means that, if needed, you should ask the questions stated in events b1 to b3, c1 and c2 when evaluating a2, a3 and a4.

Examples – isolations, insulation, fall protection.

b1. Barriers None Possible:

- Was such a barrier impossible?

Event b1 is flagged with R9 assumed risk symbol. This indicates that the appropriate management must assume the risks when they accept work/processes where no barriers were possible.

The event cannot be closed until justification for assuming risk has been evaluated.

If you are using colours, this event should be provisionally coded blue; and an entry made in the "Provisional Assumed Risk" table drawn up for this investigation. see page 56, and section 2.4, page xvi in the introduction.

b2. Barrier Failed:

- Did the barrier function as intended?

If the barrier did fail, you will need to have a clear understanding of how it failed. As well as necessary for your investigation report, this understanding will be necessary for later MORT analysis (especially at MB3, when risk assessment and design will be considered).

b3. Did not Use:

The branch applies to barriers that were possible but were not used.

c1. Did not Provide:

- Were barriers provided where possible?
- Note the event is flagged with R10 assumed risk symbol.

Event b3 is flagged with R10 assumed risk symbol. This indicates that the appropriate management must assume the risks when they accept work/processes where no barriers were possible.

The event cannot be closed until justification for assuming risk has been evaluated. If you are using colours, this event should be provisionally coded blue; and an entry made in the "Provisional Assumed Risk" table drawn up for this investigation. See page 56, and section 2.4, page xvi in the introduction.

c2. Task Performance Errors:

The branch considers errors associated with using provided barriers.

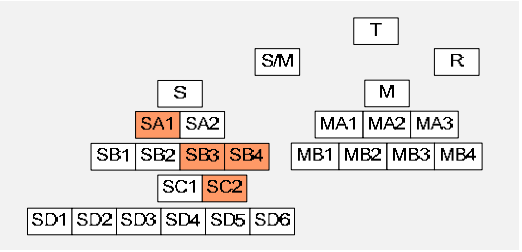
Note that all the lower tier development under event SD5 b3 transfers to this event also. If the barrier failed due to task performance errors, you should ask the questions stated under SD5 b3, these begin on page 18.

a2. Between energy source and target

This branch considers the adequacy of barriers between the energy and the target. The events and questions associated with this branch transfer from a1.

Barriers of this type are protective devices and systems that have been or that could be applied between the energy source or environmental condition and the person/object. The adequacy of the barrier depends upon the nature of the energy and vulnerable target in question.

Examples – handrail, fire wall, machinery guards.



a3. On persons or objects

This branch considers the adequacy of barriers on persons and/or objects.

The events and questions associated with this branch transfer from event a1.

Barriers of this type are protective devices/systems that have been or could be applied to the person or object. The adequacy of the barrier depends upon the nature of the energy and vulnerable target in question.

Examples – PPE, paint, armour.

a4. Separate time and distance

This branch considers the adequacy of "time and space" barriers.

The events and questions associated with this branch transfer from a1.

Barriers of this type work by ensuring the separation of energy and targets in time or space. Obedience to a procedure may accomplish separation by time or space. The adequacy of the barrier depends upon the nature of the energy and vulnerable target in question.

Examples – clearing people from an area for pressure testing, an evacuation, a traffic light.

SB4. Events and Energy Flows Leading to Accident Incident

In analysis of an accident or incident, there are usually several energy/target interactions to analyse. When using MORT, each interaction needs to be analysed separately. The various interactions that could be analysed with MORT are identified via ETBA (barrier analysis). This branch serves as a reminder to the analyst of the need to account for these precursors. At this point in your analysis, you need to decide which (if any) further energy/target interactions you wish to consider next. *See page xxi for help on this subject.*

Whereas branches SB1 to SB3 were concerned with a specific energy flow, branch SB4 refers to any other energy flows which may also need to be analysed.

On the MORT diagram, branch SB4 is shown enclosed in a dotted box. This is because the analysis of each energy flow should be done using a fresh chart.

SC3. Barriers and Controls LTA

Were barriers and controls on energy transfers and other events (leading to conversion of a hazard to an actual accident) less than adequate?
These events need to be identified via ETBA (barrier analysis).

SC4. Energy Transfers

What were the precursor energy transfers that resulted in the conversion of a hazard to an actual accident?
These energy transfers need to be identified via ETBA (barrier analysis).

SA2. Stabilisation and Restoration LTA

This branch is intended to evaluate events following a serious accident.

After an accident, efforts should be directed to limiting the consequences the accident and, whenever possible, to reducing the impact of those consequences.

When evaluating this branch, consider whether actions were pre-planned as opposed to occurring fortuitously at the time of a particular accident.

a1. Prevention of Follow-on Accident LTA:

This branch considers the adequacy of actions to prevent a follow-on accident.

Note all lower tier development under this event also transfers to events a2 and a3.

For example a second person entering an enclosed place without adequate preparation to rescue a first.

b1. Plan LTA:

- Was the plan for stabilisation and restoration adequate?
- Was the performance of people and equipment significantly different from the assumptions made in the plan?

b2. Execution of Plan LTA:

This branch considers whether the plan was executed as intended.

c1. Notification LTA (Trigger):

- Was notification made to relevant services correctly and without delay?
- Were employees adequately instructed on how to notify these services?
- Was there an alternative means of notification and was this pre-planned and trained for?

Consider whether the notification process was easy to do, especially during the stress of an emergency.

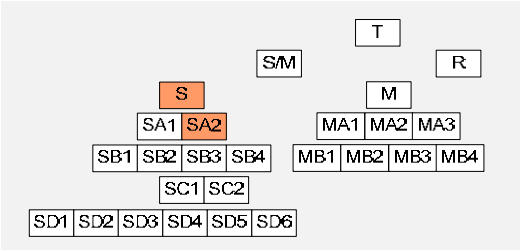
c2. Training & Experience LTA:

- Was there adequate training and experience of the various assignments required by plan?
- Was it realistic?

c3. Personnel and/or Equipment Changes:

- Had adequate counter-changes been considered and introduced to balance any changes in personnel or equipment?

Some degree of change is normally expected to occur. MORT assumes that managers and supervisors will be alert to relevant changes outside the norm.



c4. Logistics LTA:

- Was there adequate availability of transport for services to and from the accident scene (and injured people to medical facilities)?
- Did logistical arrangements worsen the harm suffered by victims of the accident?

You need to consider whether logistics, including the provision of catering and hygiene facilities, was handled adequately.

c5. Task Performance Errors:

This Branch considers errors in the performance of the plan. Consider these errors using the questions in branch SD5 b3 (Task Performance Errors). These questions begin on page 18.

c6. Response delay:

- Was the response time adequate?

Event c6 is flagged with R10 assumed risk symbol. If the response was likely to involve a delay (e.g. because of the form of transport chosen and the distance accepted) the risk involved in this response plan needs to have been "assumed" correctly. A decision to assume the risk must have been taken by an appropriate person in a suitable manner.

The event cannot be closed until justification for assuming risk has been evaluated. If you are using colours, this event should be provisionally coded blue; and an entry made in the "Provisional Assumed Risk" table drawn up for this investigation. See page 56, and section 2.4, page xvi in the introduction.

a2. Emergency Action (Fire-fighting, etc.) LTA:

This branch considers whether the emergency response to the first incident was prompt and adequate. The events associated with this branch transfer from a1; you will need to use those questions to evaluate the adequacy of emergency action.

a3. Rescue and Salvage LTA:

This branch primarily considers whether victims were satisfactorily removed to a safe area. The events associated with this branch transfer from a1; you will need to use those questions to evaluate the adequacy of rescue and salvage after the accident.

You should also consider:

- *the salvage of objects and policy of resolving conflict between rescuing people vs. objects and associated insurance concerns*
- *how rescuers balanced the risk of a follow-on accident against the ability to lessen the severity of injuries to victims, before entering a hazardous area*
- *the evacuation of employees or the public from potentially hazardous areas*

a4. Medical Services LTA:

This branch considers the adequacy of medical assistance and the harm suffered by victims of the accident. The events associated with this branch transfer from a1; use those questions to evaluate the adequacy of medical services.

Medical services include: near-by hospitals, on-site first aid, ambulance services, or general practitioners.

You should consider whether:

- *adequate First Aid was immediately available at the scene*
- *adequate medical treatment was available en route and at the medical facilities*

a5. Dissemination of information LTA:

This branch considers the contribution made by the organisation informing adequately all relevant parties about the accident.

The events associated with this branch transfer from a1; use those questions to evaluate the adequacy of information dissemination.

You should consider in particular whether the following people and groups were adequately informed:

- *Relatives of those injured*
- *Employees*
- *Officials*
- *Customers and Suppliers*
- *Public and Media*
- *Other Stakeholders*

a6. Restoration and Rehabilitation LTA

This branch considers whether people and assets were adequately returned to their pre-accident condition.

b3. Operational Continuity LTA

- Were actions to maintain a basic level of operational continuity adequate?

b4. Rehabilitation LTA

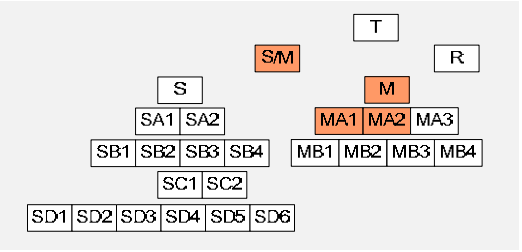
- Were people given adequate support to restore them to full health and employment?
- Were they provided with equivalent employment?

b5. Restoration LTA

- Were assets, including third party, returned to their pre-accident condition or replaced with equivalent alternatives?

b6. Absorb Loss

- Were the losses resulting from the accident accepted before the accident?
- *Note the event is flagged with R12 assumed risk. The event cannot be closed until justification for assuming risk has been evaluated.*



M. Management System Factors LTA

This branch considers the design, planning or policy formulation processes that may have contributed to the incident or accident and its consequences.

Here you will consider, in the light of what you have revealed through S-branch analysis of this accident, which aspects of the management system allowed the S-branch factors to be LTA.

MORT assumes that all issues in the S-branch are tied to issues in the M-Branch. The relationship between these is such that the M-branch designs and governs the S branch. The emphasis here is on processes rather than people. There may be several instances where a function in the "M" branch is the responsibility of a person who does not have "manager" as part of their title or job-description.

MA1. Policy LTA

"Policy" refers to a specific policy subject identified during previous analysis. You will need to bear this subject in mind when considering the questions below.

Concerning a specific policy subject:

- *was the policy clearly stated?*
- *was the policy up-to-date?*
- *was policy formulation adequate?*
- *was the policy of sufficient scope to address the major issues and problems likely to be encountered?*
- *was this policy adequately integrated with other policies?*

Policies are the declared values and intentions of the organisation. The job of policy is to define what is important and what is wanted relative to a particular issue.

Although a policy is specific to a particular issue, it needs to accommodate basic corporate responsibilities (such as duties to staff, the public and the environment, legal compliance, as well as quality and efficiency goals).

Note that Risk Management policy is considered separately at MB1

MA2. Implementation of Policy LTA

This branch considers whether the problem in question is a result of how the relevant policy was implemented.

a1. Planning Process LTA:

This branch considers the relevance of how implementation was planned.

b1. Specification of Plan LTA

This branch considers whether the policy implementation plan was adequately specified.

c1. Methods, Criteria, Analyses LTA:

- Were adequate methods used to plan policy implementation?
- Did accountable management require adequate planning procedures to minimise problems?

Note that in MORT planning is seen as an open-ended process in which plans are adapted in the light of new information gained in the execution phase.

c2. Specification of Responsibilities LTA

This branch considers the adequacy of how responsibilities were assigned for implementing the policy.

d1. Definition of Line Responsibility LTA

- Was there a clear, written statement of duties, derived from the policy, for each person in the line organisation to whom it applied?
- Did each person concerned understand and accept their responsibility?
- Was this verified in an adequate fashion?

Events d1 and d2 make a distinction between line and staff. "Line" refers to the operational part of an organisation, which delivers the service for which the organisation exists. "Staff", refers those parts of the organisation which exist to facilitate the work of the line.

d2. Staff Responsibility LTA

- If the implementation of policy relied upon more than one department, was adequate provision made to assign specific duties to the departments concerned?

d3. Task Assignment LTA

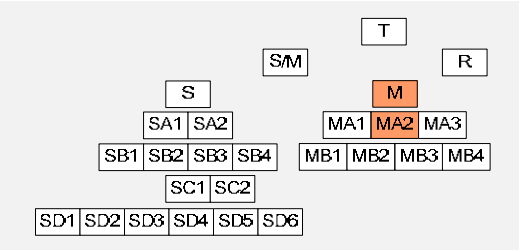
- Was the problem in question a result of how the task was assigned by the supervisor to the member of staff?
- Was the assigned task properly scoped with steps and objectives clearly defined?
- Was the task one an employee should undertake without specific instructions from the supervisor?

c3. Schedule LTA

- Did the plan schedule planning cycles frequently enough to prevent or detect undesired changes?
- Was the schedule readily available to the personnel?

c4. Budgets LTA

- Was the budget adequate to support the planning process in the department or group owning the policy?
- Were the budgets of other departments and groups adequate to support the planning process?



c5. Communication Plan LTA

This branch considers whether implementation of policy may be supported by a planned approach to communication.

d4. Information Flow LTA

- Did management adequately specify the types of information it needed to communicate about policy implementation?
- Did management establish adequate communication arrangements to transmit this information through the organisation?
- Did management support implementation with adequate response to requests for information by lower organisational levels?
- Was adequate provision made for feedback about problems encountered when communicating about policy?

d5. Guidance and Directives LTA

- Did guidance and directives, aimed at communicating the policy, adequately emphasise risk management approaches (such as risk analysis, monitoring, review)?
- Were these directives published in a style conducive to understanding?
- Were the directives constructed to ensure continuity across interfaces between different departments and processes?

b2. Use of Feedback LTA:

- Did the plan encourage people to report problems or better ways of doing things?
- Have previous relevant problems of policy implementation been subject to adequate analysis for cause?
- Were such analyses adequately specified by the plan?
- Did an appropriate individual or group adequately act upon the results of such analysis

a2. Execution of Policy Implementation Plan LTA

This branch looks at whether the problem in question is a result of how the implementation plan was carried out.

b3. Leadership LTA

- Did senior management and other influential people provide adequate leadership?
- Did their behaviour reflect the importance of the implementation of the policy in question?

b4. Capability LTA

This branch considers the organisation's ability to execute the policy implementation plan

c6. Authority LTA

- Were specific duties adequately assigned to named individuals to execute the plan?
- Did the people involved have adequate authority to carry out all aspects of the plan?

c7. Accountability LTA

- Was there adequate accountability of the named individuals involved in carrying out the plan?
- Was there adequate performance feedback to these individuals?

c8. Task Performance LTA

- Were the individual tasks (as set out in the plan) performed adequately?
- *If not, identify who is performing which task and the nature of the inadequacies. Then refer to further questions relating to Task Performance Errors (SD5 b3); these begin on page 18.*

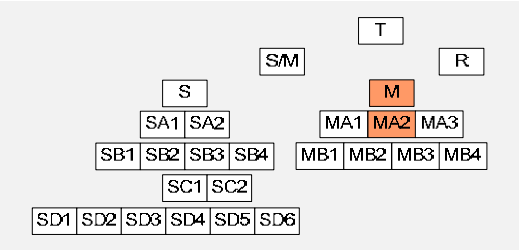
b5. Practical Support LTA

This branch considers whether management supported implementation with adequate services and guidance.

The events associated with this branch follow the same logic as SD6 branch, ask the questions set-out there to evaluate the adequacy of the support

b6. Time and Budget LTA

- Were the time and budget specified in the plan's schedule sufficient to adequately perform each task?
- Were the time and budget allocated for personnel adequate to fulfil the schedule?
- Were the time and budget actually made available?



b7. Delays

- Were solutions to problems of implementation introduced early enough?
- If not, was the delay made known to someone who was able to expedite a solution and assume the risk of continued delay?

Event b7 is flagged with R13 assumed risk symbol. If implementing the policy needed to be delayed, the risk created by the delay needs to have been "assumed" correctly. A decision to assume the risk must have been taken by an appropriate person in a suitable manner.

The event cannot be closed until justification for assuming risk has been evaluated. If you are using colours, this event should be provisionally coded blue; and an entry made in the "Provisional Assumed Risk" table drawn up for this investigation. See page 56, and section 2.4, page xvi in the introduction.

b8. Caused Failure

- Did the implementation of the policy introduce new problems even when the plan was carried out "to the letter"?

a3. Monitoring LTA

Was there adequate monitoring of the implementation process?

MA3. Risk Management System LTA

This branch considers the adequacy of the risk management system.

MB1. Risk Management Policy LTA

This basic event considers the adequacy of the risk management (RM) policy.

- was it clearly stated?
- was it up-to-date?
- was it formulated adequately?
- was it of sufficient scope to address the major issues and problems likely to be encountered?
- was it adequately integrated with other policies?
- was it subject to adequately review?

MB2. Implementation of Risk Management Policy LTA

This branch considers whether the problem in question is a result of how the risk management policy was implemented.

The events associated with this branch follow the same logic as MA2 branch. Ask the questions listed there, pages 37-41,with Implementation of the Risk Management Policy as the subject.

MB3. Risk Analysis Process LTA

This branch considers risk analysis and the design and development of specific work activities and processes.

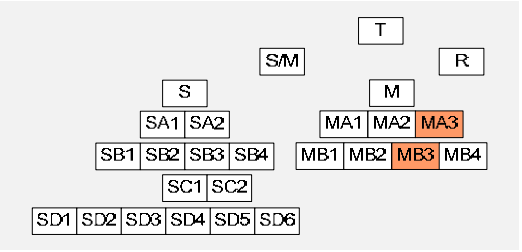
a1. Concepts and Requirements LTA:

This branch considers the adequacy of the risk analysis process and its definition by the organisation.

b1. Technical Information System LTA

This branch considers how the technical information system may have failed to provide adequate support to risk analysis.

Refer to the SD1 branch (p. 5-10) and ask the questions from the perspective of the risk analysis process.



b2. Definition of Goals and Tolerable Risks LTA:

This branch considers the definition of goals and tolerable risks within the organisation

c1. ES&H Goals and Risks not Defined:

- Did the ES&H goals state what level of risk should be attained and when?
- Are tolerable direct and indirect ES&H risks defined and actual risks quantified?

ES&H: Environment, Safety and health.

c2. Performance Goals and Risks Not Defined:

- Have goals been set for performance, efficiency and productivity?
- Have tolerable risks for lost efficiency and productivity been identified and actual risks quantified?

Examples – part of the business plan includes business risk and contractual arrangements with partners

b3. Risk Analysis Criteria LTA:

This branch considers the specification of risk analysis.

c3. Plan LTA:

- Was the plan that describes "who does what and when" in risk analysis, study, and development, adequate?

c4. Change Analysis LTA:

- Was there an adequate method for analysing the effects of planned change? Was it adequately applied?

Whatever method of change analysis was used, it should have:

- *included the impact of the change upon people, procedures and plant/equipment;*
- *been scoped to review arrangements until no change was demonstrated (i.e. the full ramifications should have been identified).*

c5. Other Analytical Methods LTA:

- Was adequate use made of appropriate analytical techniques?
- If not, does this reflect inadequacies in the skills available to the organisation (internally or externally)?

You need to be clear about what methods would have been appropriate to the matter in question.

c6. Scaling Mechanism LTA:

- Was an adequate mechanism established to measure the seriousness/severity of different events?
- Did this mechanism adequately support the evaluation of the work/process in question?

There are several types of scaling mechanisms, for example:

- *Severity x frequency matrices*
- *Ranking by hazard potential*
- *Ranking by amount of energy*

Providing review by experienced people and applying actuarial data may also be relevant here.

c7. Required Alternatives LTA:

- Did management insist on presentation of alternative solutions in its bases for choices and decisions?

Proposals to decision makers tend to state a strong, positive case. Negative aspects may not be emphasised or well presented. A requirement for alternative proposals and/or benchmark analyses, may help to expose problems and obstacles.

c8. Solution Precedence Sequence LTA:

- Was the selection of solutions prioritised by:
  (1) Design,
  (2) Protective Devices,
  (3) Warning Devices,
  (4) Human Factors Review (ergonomics),
  (5) Procedures,
- (6) Personnel, and
  (7) Acceptance of residual risks (after considering the preceding six items)?

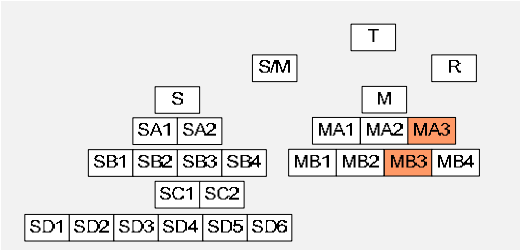
This sequence is in order of effectiveness and reliability. Design can wholly remove a problem, whereas other options attempt to control the effects.

The sequence also reflects the lifecycle and hence cost effectiveness: early solutions are typically less costly and more effective.

b4. Criteria for Procedures LTA:

- Were criteria for writing procedures specified adequately and communicated to staff involved in producing them?
- Were criteria for reviewing new and revised procedures adequately specified and applied?

These criteria should remind engineers and designers of the limitations and issues relevant to writing procedures for operating personnel. Assuring adequate readability and usability is especially important.



b5. Specification of Requirements LTA:

This branch considers the search for and application of criteria relevant to the work system/process or project in question.

c9. Stakeholder/customer requirements.

- Were the requirements from stakeholders or customers taken into account?

'Stakeholders' includes partners, workforce, customers, government agencies, etc.

c10. Statutory codes and regulations

- Were statutory requirements (such as taken into account?

c11. Requirements of other National and International codes and standards

- Were the requirements from national and International codes (*e.g. – ISOs, EN codes and standards)* and standards taken into account?

c12. Local Codes and Bylaws

- Were the requirements from regional and local codes and standards taken into account?

c13. Internal Standards

- Were the requirements from Internal standards taken into account?

b6. Information Search LTA:

This branch considers the adequacy of the information search undertaken in support of risk analysis. This issues can be explored using the lower tier events shown in the MORT diagram under SD1 a1 (Technical Information); the corresponding questions are listed on pages 5-7 of this manual.

b7. Life Cycle Analysis LTA:

- Did risk analysis ensure adequate consideration of all phases of lifecycle?

The lifecycle can be conceived as starting with planning and continuing through design, purchasing, fabrication, construction, operation, maintenance, and disposal.

c14. Scope LTA:

- Did the scope include not only the primary work/process equipment and systems, but also ancillary equipment and systems (e.g. ventilation, waste heat recovery, testing, maintenance, cleaning, etc)?
- Did the analysis adequately include the personnel and procedural components of primary and ancillary systems?

c15. Analysis of Environmental Impact LTA:

- Did the lifecycle analysis adequately address environmental impact?

c16. Requirement for Life Cycle Analysis LTA:

- Did the requirement for Life Cycle Analyses (LCA) assure that a thorough LCA was initiated during the planning stage?

c17. Extended Use Analysis LTA:

- If the facility/operation has been extended beyond its original intended life, was there adequate consideration of special requirements, new problems, and other factors that were or might have been encountered?

a2. Design and Development LTA:

This branch considers the design and implementation of work/process controls and related infrastructure.

b8. Energy Control LTA:

This branch considers options for the use and control of energy. This is done in order of effectiveness and reliability, starting with using the safest form of energy and ending with protective barriers.

According to this principle, the ideal approach is to limit energy to the minimum needed to accomplish the work/process.

c18. Safer Energy LTA:

- Did the design use the safest form of energy that will perform the desired function?

c19. Limitation of Energy LTA:

- Was the amount of available energy limited to that which will perform the operation without any unnecessary excess energy?

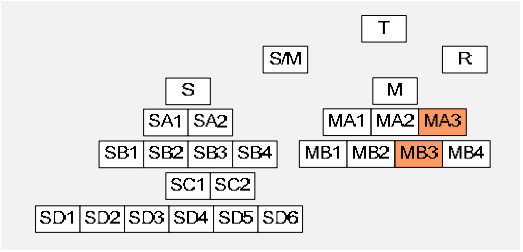
c20. Automatic Controls LTA:

- Were there devices to automatically control the flow of energy and to maintain it in its operating mode? Is use of redundant design adequately employed?

Redundancy should also be a feature of any communication systems linking automatic systems. Examples - parallel and back-up transmitters/receivers, channels, optical and electric cabling etc.

c21. Warnings LTA:

- Were there clear, concise warnings for all situations where persons or objects might unintentionally come into contact with an energy flow?



c22. Manual Controls LTA:

- Were there adequate manually operated controls to maintain the proper energy flow during the normal mode or as a manual override of automatic controls?

c23. Safe Energy Release LTA:

- Had adequate provision been made for safe release of the energy (e.g. electrical earth, pressure relief valve)?

c24. Controls and Barriers LTA:

- Were adequate controls and barriers included as part of the design, plan, or procedure?
- *Refer to the evaluation of controls and barriers analysed through SB3 branch*

b9. Human Factors (Ergonomics) Review LTA:

This branch considers the adequacy of human factors review of the work/process in question.

"Human Factors" is defined here as the application of psychology and physiology to the analysis and improvement of human work performance.

c25. Professional HF Skills LTA:

- Was the minimum level of human factors capability, needed for evaluation of an operation or design, available and was it used?

c26. Task Analysis LTA:

- Was task analysis (TA) adequately applied to the work/process in question.
- Was TA applied early enough in the lifecycle and were the results adequately incorporated into the design?

The preferred HF philosophy is to "fit the task to the person". However, certain tasks require specific characteristics and these must be specifically selected for and/or trained.

c27. Allocation Human/Machine Tasks LTA:

- Did the review adequately ensure the optimum allocation of work/process tasks to people and machines?

Task Allocation: For example, machines excel at tasks requiring high levels of accuracy, strength and repetition. People excel at creative and variable tasks.

c28. Did not Establish Human Task Requirements:

Did the review determine special characteristics or capabilities required of people and machines?

d1. Did not Define Users:

- Was adequate effort made to gain and incorporate knowledge about would be users in the design?
- Was adequate effort made to identify user requirements?

Defining users and their characteristics allows the design to accommodate diversity in the workforce or user population.

d2. Design of Displays LTA:

- Were the work/process displays designed to allow rapid interpretation with high reliability?
- Did the Human Factors review ensure that display stereotypes were used?

Display and Control "Stereotypes" are norms established by design practice: e.g. Red means danger, upward/forward movement indicates increase, etc. Such stereotypes must be adhered to and designers need to be aware of cultural and geographic variations from their own norms.

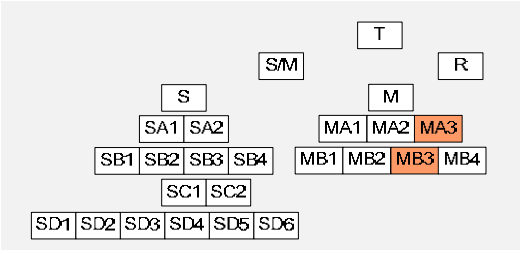
d3. Interpretation LTA:

- Was there adequate review of the likely effects of unreliable interpretation of displays and delays in control actions?

Various psychological and physical factors mediate the interpretation of data available in controls and displays – some degree of error and delay will always be present and this may have consequences.

d4. Design of Controls LTA:

- Were the work/process controls designed to allow rapid use with high reliability?
- Did the Human Factors review ensure that control stereotypes were used and not disregarded?



c29. Did not Predict Errors:

- Was the design process informed by adequate human error prediction and analysis?
- Did the review adequately assess the scope for deliberate errors and other acts of malevolence?

The purpose of such analysis is to predict modes and frequencies with which human errors may occur, and so determine preventive action to reduce the overall error rate.

Examples of general human error types are:

- *incorrect act*
- *act out of sequence*
- *fail to act*

b10. Inspection Plan LTA:

This branch considers the development of an inspection plan for the operation/facility. The issues can be explored using the lower tier events shown in the MORT diagram under SD3 a1 (Inspection Plan); the corresponding questions are listed on pages 12-13 of this manual.

b11. Maintenance Plan LTA:

This branch considers the development of a maintenance plan for the operation/facility. The issues can be explored using the lower tier events shown in the MORT diagram under SD4 a1 (Maintenance Plan); the corresponding questions are listed on pages 12-13 of this manual.

b12. Arrangement LTA:

- Did the design consider problems associated with space, proximity, crowding, convenience, sequence-of-use, freedom from interruption, enclosures, work flow, storage, etc.?

At this point you need to consider the following issues should be considered:

- *How inspectability and maintainability requirements were specified in the design or procurement documents for the operation, facility or equipment in question;*
- *The adequacy with which inspection and maintenance activities were specified in operational plans;*
- *How minimum requirements for inspection and maintenance equipment and staffing were arrived*

b13. Environment LTA:

- Did the design adequately minimise physical stresses upon people and objects?

This might include stresses caused by;

- *the physical conditions of the facility,*
- *conditions generated by the operation, or*
- *interactions of one operation with another?*

b14. Specification of Operational Readiness LTA:

This branch considers the operational specification for all phases of the work/process operation. If the specification is adequate and complied with, the work/process can be described as operationally ready. Whereas event SD2 dealt with the verification of operational readiness, this branch deals with the definition of operational readiness for the work/process in question.

Note that specification of operational readiness is an ongoing effort. It will involve many different types of personnel (e.g. designers, engineers, supervisors) at different times, ranging from the design of plant/process to the ad hoc specification of day-to-day jobs.

c30. Test and Qualification LTA:

- Were new/modified work/processes subject to adequate testing and adjustment before full implementation?
- Did this incorporate plant, people, and procedural aspects of operation and the interfaces between these?

Examples – part of the handover certificate, including service test, testing under operational conditions, formal review of procedures.

c31. [Specification of] Supervision LTA:

- Were there adequate guidelines for the amount of supervision required, minimum supervisory capabilities needed, and responsibilities of supervisors of the work/process?
- Were there adequate guidelines for the supervisory support of JSA and other risk assessment activities associated with the work or process?

c32. Task Procedures LTA

This branch considers the criteria for work/process procedures.

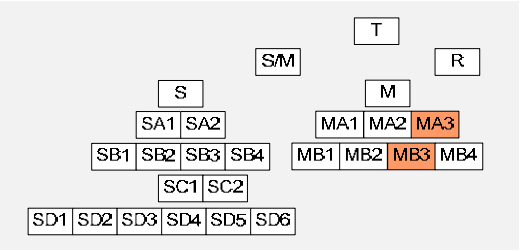
d5. Match to Hardware Change LTA:

- Were procedures revised, if necessary, to correspond with changes in plant or equipment?

d6. Match to Users LTA:

- Were procedures adequately matched to the minimum reading ability and technical competence of the staff who actually used them?

Involving a representative group of users in a structured review of draft procedures can help this.



d7. Match to task/equipment LTA:

- Were procedures adequately checked against applicable criteria and tested under dry run operating conditions?

d8. Emergency Provisions LTA:

- Did procedures give users clear instructions for all anticipated emergency conditions? Are instructions easy to perform under the stress of an emergency?

d9. Cautions and Warnings LTA:

- Were adequate dynamic and static warnings used? Were they located at point of operation as well as in procedures? Was their meaning unambiguous?

Example – advisory/warning signs for non-stereotypical valves or controls.

d10. Task Sequence LTA:

- Did the procedures describe task steps in sequential order where possible?

d11. Lockouts LTA:

- Were lockouts required in the procedure where hazardous situations could be encountered or created by the application of the procedure in question?

Lockouts – physically preventing the use of equipment or access to areas.

d12. Communication Interfaces LTA:

- Where procedures called for communication between users and other individuals, were these interfaces made clear?

d13. Specification of Working Environment LTA:

- Did procedures adequately specify the range of environmental conditions within which the task should be performed? Where a stressful environment is expected, do procedures specify maximum exposure times or other measures to mitigate adverse effects?

c33. Personnel Selection LTA:

- Were adequate criteria and methods for selecting people to undertake the work/process?

Note – consider this, and associated checking/verification, for directly employed staff, contractors and sub-contractors.

Examples – competency standards and assessment, matching the individual to the task in terms of the competence required.

c34. Personnel Training and Qualification LTA:

- Were training methods, qualification criteria and verification process for the people undertaking work/process adequately developed and specified?

Examples – National vocational qualifications, passport systems, verified in-company systems for core staff.

Personnel training and qualification factors are considered in detail under SD5-c15.

c35. Personnel Motivation LTA:

- Was motivation adequately considered in the design of the work/process?

As part of this, consider whether there was an adequate effort to ensure the rewards and "punishments" perceived by work-level staff were consistent with correct task performance.

Personnel motivation factors are considered in detail under SD5-d15

c36. Monitor Points LTA:

- Did written procedures contain adequate prompts to allow monitoring of key steps of the work/process?

b15. Emergency Shutdown Provision LTA:

- Did the design of plant and equipment provide for safe shutdown and safety of persons and objects during all anticipated emergencies?

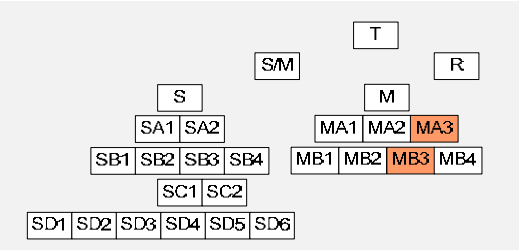
b16 Contingency Planning LTA

- Were all of the emergency functions pre-planned *(rather than left to improvisation)?*
- Did these plans adequately consider the types and severity of accidents to which they applied?
- Were adequate resources allocated to execute the plan properly?
- Were consumable resources subject to an adequate schedule of periodic checks and planned replenishment?

b17. Disposal Planning LTA:

- Did the design adequately minimise disposal problems and hazards associated with the disposal of the plant?

Note that lifecycle analysis is considered at b7.



b18. Independent Review LTA:

- Was there adequate provision of thorough and independent ES&H review at pre-established points in the life cycle?
- Were the risk reduction trade offs documented?
- Was the technical competence of members of the Review Board adequately matched to the level of technology involved?

b19. Configuration Control LTA:

- Was there an adequate programme to assure configuration control throughout the entire life cycle of the facility and/or work process?

The aim of configuration control is to ensure the synchronisation of plant, people and procedural subsystems with each other and to specifications.

b20. Documentation LTA:

- Was there an adequate process to manage, update and authorise documents?
- Were all types of documentation (whether paper or electronic) complete, up to date, and accessible to users?

b21. Fast Action Expedient Cycle LTA:

- Was there an adequate procedure to get an immediate correction of a problem in the work/process?

Fast action cycles should be reserved for high hazard or other problems with significant consequences.

b22. Design Acceptance & Change Control Process LTA:

This branch considers the adequacy of acceptance and control-of-change procedures.

c37. Code Compliance Verification LTA:

- Was there adequate verification that all codes and standards noted as relevant at the conceptual stage were incorporated into the design?

c38. Engineering Studies LTA:

- Were adequate engineering studies conducted to obtain information not available from codes, standards, regulations, and state of the art knowledge?

c39. Standardisation of Parts LTA:

- Was there an adequate attempt to use proven existing standardised parts where possible, and to design so as to encourage their use?

c40. Design Description LTA:

- Did the design description provide all the information needed by its users in a clear and concise manner?

c41. Acceptance Criteria LTA:

- Were acceptance criteria stringent enough to assure operability /maintainability and compliance with the original design?

c42. Development and Qualification Testing LTA:

- Was there adequate testing during development of the new design to demonstrate that it would serve its intended function?
- Did qualification testing assure that non-standard components satisfied the acceptance criteria?

c43. Change Review Procedure LTA:

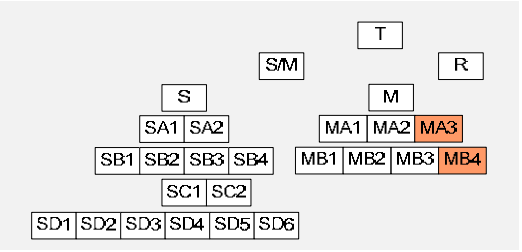
- Was there an adequate procedure for Change Review regarding the work process?
- Did change review include all elements of the system (especially form, fit and function), and continue up to a point where no change was demonstrated?
- Were there change annotations/warnings on drawings and at points of operation?

Change analysis is adequate if the full ramifications of the changes have been found.

c44. Reliability and Quality Assurance (R&QA) LTA:

- Was there an effective reliability and quality assurance programme and was it adequately integrated into the general design process?

In some organisations, the reliability and quality assurance functions are very specifically separated; other organisations combine them. Whether combined or separated, R&QA is a strong complement to HS&E. Close mutual support between HS&E and R&QA should be evident throughout the general design process.



MB4. Risk Management Assurance Programme LTA

This branch considers the adequacy of processes aimed at assuring risk management.

a1. Definition of Aims and Policy LTA:

- Were there adequate assurance policy statements and were the aims of the assurance programme articulated?
- Did this summarise what management should know (and require) of the assurance process?
- Did the aims provide a benchmark against which to measure the risk management programme?
- Were the aims SMART?

This includes ES&H programmes.

SMART – Specific, Measurable, Agreed, Realisable, Time-bound.

a2. Scope LTA:

- Was the scope of the risk management assurance programme set in an adequately forward-looking, future-oriented way? Was the scope adequately informed by best practices?

a3. Documentation LTA:

- Was the risk management assurance process documented adequately?

a4. Assurance Programme Organisation LTA:

This branch considers the organisation of the risk management assurance programme.

b1. Risk Management Assurance Staff Performance LTA:

- Did risk management assurance personnel perform well by both assurance programme and management criteria?
- Were they effective in both technical and behavioural aspects?
- Did they have adequate authority?

b2. Management Committees LTA:

- Were special purpose and permanent committees (or boards) adequate?
- Were these ongoing groups positive, and orientated towards the resolution of real life problems?

b3. Organisation for Improvement LTA:

- Was the assurance programme adequately designed and managed to produce the desired pace of improvement?

Although ownership of problems in the line organisation is crucial, achievement of significant assurance improvement also requires clear definition of goals and effective organisation efforts, particularly by assurance staff.

a5. Assurance Programme Services LTA:

This branch considers the provision of services and guidance needed to support the activities of the assurance programme.

The events associated with this branch follow the same logic as SD6.

a6. Assurance Activities LTA:

- Did the assurance system adequately compare actual performance with assurance programme aims and objectives?

MB5 Review of Risk Management System LTA

Did the organisation ensure that a review of the risk management system was carried out at periodically?
Was the review adequate to ensure suitability and effectiveness of the risk management system?
Were the reviews adequately documented and acted upon?
Was there adequate external review?

R. Assumed Risk

Questions:

- *What were the assumed risks?*
- *Were they specific, named events?*
- *Were they analysed and, where possible, calculated (quantified)?*
- *Was there a specific decision to assume each risk?*
- *Was the decision made by a person who had [management delegated] authority to assume the risk?.*

A loss can be accepted from an assumed risk only if the risk in question was a specific, named event; analysed, calculated where possible, evaluated, and subsequently accepted by a line manager or supervisor who was properly exercising management-delegated, decision-making authority.

To reach your judgement of whether a risk was properly assumed, you will need to consider:

- *The adequacy with which costs were weighed against benefits of risk reduction;*
- *Uncertainty about the risks themselves*
- *Tolerability of risk;*
- *Adequacy of information and interpretation provided to the person making the decision;*

Document Improvement Proposal

1. Document I.D.	2. Document date	3. Document title
NRI-1 EN 2009	20 December 2009	MUM

4. Recommended improvement (identify page, paragraph and include modified text or graphic, attach pages as necessary)

5. Reason for recommendation

6. Originator of recommendation

Name:	Organisation:	
Address:	Phone: Fax: E-mail:	**7. Date**

8. Send to NRI Secretariat

Name:	***Address:***	
J. Kingston@nri.eu.com	Noordwijk Risk Initiative Foundation P.O. Box 286 2600 AG Delft The Netherlands	Tel: +44 (0)121 288 3206 email: info@nri.eu.com

MORT - Management Oversight & Risk Tree

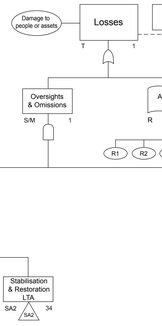
2009 Revision by
The Noordwijk Risk Initiative Foundation

Document Reference: NRI-2 (2009).
For use with the MORT Users' Manual (NRI-1)

Published and distributed by the
Noordwijk Risk Initiative Foundation
P.O. Box 286, 2600 AG Delft,
The Netherlands.

20th December 2009
Email: Info@nri.eu.com
Website: www.nri.eu.com

ISBN 978-90-77284-09-4



An event, usually a fault or oversight, expressed in generic terms.

An event described by a basic component or part failure. It marks the lowest level of development in the tree.

An event where sequence is ended for lack of information or solutions. The event may be transferred to "Assumed Risks".

An event that is satisfactory.

An event that is normally expected to occur.

AND Gate - Requires the coexistence of all gate inputs to produce output.

OR Gate - Requires any one gate input to produce output. If more than one input, the output will still occur.

Conditional gate (either AND or OR) - Inputs produce the output provided the condition is true.

Constraint symbol - Applies conditions to gate or output.

Triangle - Used to transfer sequence to another location on page.

Transfer to Assumed Risk branch - denotes problems for which there is no practicable countermeasure

D/N	Did not
D/NP	Did not provide
ES&H	Environment, Safety & Health
F/T	Failed to
LTA	Less than adequate
W	With
RM	Risk Management

(Provisional) Assumed Risks

MORT Reference	Description of (Provisional) Assumed Risks	Judgement

NRI-2, Second Edition, August 2009. Revised by John Kingston, Floor Koornneef, Jaap v.d. Ruit, Rudolf Frei, and Philippe Schallier. Major revision of MORT 1992, US Department of Energy, drawn by John Kingston.

FOREWORD

Similarly to many other nuclear plants in the world, Paks NPP has applied the root cause analysis (RCA) of its own operational events for many years. The method was used in Paks NPP did not deliver accurate results in the identification of root causes. In order to enhance the operational safety, the management of Paks NPP decided to replace the old method with another RCA method and training the plant staff accordingly. This new method should be workable in the plant environment and should assure that the root causes of any events will be adequately identified, acceptable to the technical experts and convincible to the plant management.

ENCONET Consulting Ges.m.b.H., Austria, committed itself and contracted to supporting the Paks NPP to develop the plant specific RCA method for the purpose of enhancement of nuclear safety and quality management of the Paks NPP. Based on an overview of several RCA methods having been successfully used in the USA and Western European countries, according to the comments provided by the Paks staff at three successive workshops, a concept on an adequate RCA method for Paks NPP was formulated and further advanced.

The first two workshops were conducted at Paks NPP, organized and managed by Mr. Sandor Nagy, Head, Department of Nuclear Safety, Paks NPP Ltd., and supported by his deputy and staff. Mr. Bengt Lydell, RSA Technologies, USA, was invited being a member of the ENCONET team in the preparation and delivery of the lectures. The third workshop was held in the ENCONET office, Vienna.

The Paks specific RCA method is included in the present procedure. This procedure is descriptive specifically developed to meet the needs of safe and reliable operations of the Paks NPP. It was originally an adaptation of the basic structure and contents of the Human Performance Investigation Process (HPIP) of the Nuclear Regulatory Commission (NRC) of the USA and the ideal safety management systems in the Management Oversight & Risk Tree (MORT) of the Department of Energy of the USA.

Nevertheless, significant modifications and improvements were made. Among others, all the three basic elements (Equipment, Personnel and Procedures) in performing any tasks are included in the RCA. The interactions between Equipment and Human (both as individual and as organization) are further explored. Safety culture at three levels (i.e. police establishment, management commitment and personnel response) is as a whole all considered.

This procedure, as any new developments, should be verified for their correctness and effectiveness. A trial period may be necessary to get feedback from the eventual users for improvement. As new operating experience is gained and more events are analyzed, this procedure should be thoroughly reviewed and revised as warranted.

C.K. CHEN

EXECUTIVE SUMMARY

This document describes a method for establishing a standard root cause analysis (RCA) procedure to be used by the staff of the Paks Nuclear Power Plant Ltd. when analysis of equipment and human performance (E&HP) related operational events occurred at Paks Nuclear Power Plant (NPP).

This procedure, called the Paks Root Cause Analysis Procedure or PRCAP, was originally an adaptation of the Human Performance Investigation Process (HPIP) of the US NRC in corporation with some safety management factors in the Management Oversight & Risk Tree (MORT) of the US Department of Energy. Nevertheless, significant modifications and amendments were made to satisfy the specified interests and practices on safe and reliable operations at Paks NPP. PRCAP represents a disciplined approach to systematic investigation and analysis of root causes of events occurred at operating NPPs. PRCAP includes a number of distinct features such as:

- A structured process for systematic performing investigations and analyses based on an event report drafted and reported to plant management shortly after the event;
- A combination of RCA techniques commonly used in many RCA methods for searching underlying facts through apparent symptoms and for organizing findings;
- A screening flow in a Yes/No logic tree for identifying cause categories taking into account the prevention and elimination of an event at different stages/ levels;
- A comprehensive set of cause modules for events at operating NPPs which, consist of possible failures of all three basic elements (equipment, personnel and procedures) in task performance and the environmental and managerial factors in event development.

Although a majority of events at first appear to be of a purely individual or technical nature, careful analysis often reveals a hidden complex structure of interaction between causes. Further analysis may logically lead to some underlying or fundamental organizational factors that deal with how management plans, organizes, controls and provides support to and assurance for the work performance. The RCA experts need to have sufficient expertise and skills to stop the analysis at an appropriate organizational level for making reasonable conclusions.

PRCAP consists of two parts, appendices and annexes. Part I emphasize the analytical process with steps, while Part II describes in detail the tools with examples. Should an expert having sufficient knowledge on RCA techniques have carefully studied Part I, he/she would be able to apply the PRCAP to analyze the root cause of any operational event without recalling Part II. Those who would like to comprehend more details of the RCA tools may study PART II to closely follow each of the steps of the PRCAP process. Examples of analysis of some selected plant operational events are provided in Appendices. Two annexes compare the two searching systems and the two groups of cause modules between HPIP and PRCAP, respectively.

A coding system for allocation of relevant causal factors within the cause modules are used for the convenience of recording and identification, which may also facilitate in the future the development of a computer tool for effective implementation of the PRCAP.

Table of Contents

1. INTRODUCTION

1.1 BACKGROUND

This document describes a method for root cause analysis (RCA), called thereafter the **P**aks **R**oot **C**ause **A**nalysis **P**rocedure or PRCAP in short, is particularly developed to meet the safe and reliable operations of the Paks Nuclear Power Plant (NPP). PRCAP was originally an adaptation of the Human Performance Investigation Process (HPIP) of the US Nuclear Regulatory Commission and the safety management factors in the Management Oversight & Risk Tree (MORT) of the US Department of Energy. Nevertheless, significant modifications and amendments were made which reflects the all-round comprehension of the RCA methods currently used in the world and the specific requirements for RCA at Paks NPP.

HPIP was developed for the US regulatory inspectors and specialized to investigate and analyze human performance related operational events at the NPPs. HPIP is characterized with a collection of RCA techniques, a searching system for cause categories starting with the 'Stimulus' function, and a group of cause modules with 6 cause categories and a total of 84 causal factors.

MORT presents an ideal management system in a tree structure for prevention of the recurrence of incidents and/or accidents. MORT is used as a performance standard to be compared with the real management systems and includes about 100 generic problems. MORT method is based on the energy trace and barrier analysis.

"Equipment" or human as individual "Personnel" is neither formally covered by HPIP nor by MORT. Nevertheless, it is well known that "Equipment" and "Personnel" are two of the three basic elements (another one is "Procedures") in performance of any tasks and they are most likely the direct cause of any event.

PRCAP provides a comprehensive procedure for systematical analysis of the direct cause, contributing causes and the root cause of an operational event. PRCAP has extended the searching system and the cause modules of the HPIP to cover potential contributions of 'Equipment' and 'Personnel' in the RCA. The searching system in the PRCAP starts with the 'Prevention' function. The cause modules in the PRCAP include a total of 7 cause categories and more than 200 causal factors. The PRCAP modules cover all the basic elements (equipment, personnel and procedure) and the essential environmental/ managerial factors, which may contribute to or result in an event.

Additionally, the original RCA techniques were modified to include examples from Western European countries and the IAEA documents. Relative to the HPIP, a different arrangement of the RCA techniques was made in PRCAP. Instead of appearing as attachments to the HPIP, the RCA techniques are placed in the main body of the PRCAP structure. Moreover, a number of criteria and guidance/ guidelines are provided, from the selection of events for the formal RCA, through the analysis of root causes, up to the preparation of the RCA report.

1.2 OBJECTIVES

The main objective of this procedure is to present a process for investigation and analysis of the root causes of operational events. For achievement of the main objective, a series of tools are provided, including various RCA techniques, criteria and guidance or guidelines.

PRCAP applies to all operational events occurred at Paks NPP, which may involve equipment and human performance (E&HP) problems and have nuclear safety and/or quality implications. PRCAP is intended for persons responsible for or designated to analyze root causes of the operating events. However, an expert may only need to select relevant parts of PRCAP to perform the investigation/ analysis, depending on his/ her knowledge and experience.

The subjects to be analyzed in PRCAP are the direct cause, contributing causes and the root cause. Usually, one direct cause, a number of contributing causes and one root cause are identified for an operating event. The objectives of this procedure will be validated through assessment of the effectiveness of the corrective actions implemented on the basis of the recommendations resulting from the application of this procedure.

PRCAP will be subjected to periodic reviews and revisions in accordance with quality assurance requirements and based on the accumulation of the application experiences. Users are encouraged to offer comments and/or suggestions for the improvement of PRCAP

1.3 TERMINOLOGY

1.3.1 Definitions

The most important terms used in PRCAP are defined as below specifically for the purpose of implementation of the PRCAP process. These definitions were essentially adopted from dictionaries and the RCA Guidance Document of the US DOE.

Occurrence:	Anything that takes place or comes about, such as an action, a change, a deviation, a malfunction, a failure, or an anomaly, an incident, an accident.
Event:	A sequence, or sequences, of related occurrences; or a real time or notable occurrence unexpected and usually considered as the result of all the precedent occurrences.
Condition:	Any as-found state, indispensable or necessary in order for an occurrence or a few individual occurrences to happen, whether directly or indirectly.
Factor:	Any of the conditions, actions, changes, influence, or other facts that act singly or with others together to contribute to or result in an event or a chain of occurrences.

Cause or Causal Factor	The cause that logically brings about an effect or results in a consequence that may have adverse safety, quality, health, operational or environmental implications.
Direct Cause:	The cause that directly creates the difference between the expected and the real performance or situation, or that directly resulted in the event
Contributing Cause:	The cause or causes that contribute to or have special bearing on the event but, by itself, would not be inevitable to bring about or result in the event.
Root Cause:	The cause, which is the fundamental aspect of the event and, if eliminated or corrected, the occurring or recurring of this and similar events would be prevented.

These definitions are generally in consistence with those used in the Nuclear Safety Standards of the International Atomic Energy Agency (IAEA).

1.3.2 Other Terms

Another three terms used in the process of determination of the direct cause, contributing causes and the root cause are explained as follows:

Problem:	Problem is usually regarded as a situation where the performance of an element or a system does not meet expectations.

For example, actuation of a protective system constitutes an occurrence, but the problem is not the occurrence. The real problem is the unwanted and unplanned condition or action that resulted in the actuation of the protective system. In case that an operator followed a defective procedure and resulted in an occurrence. The real problem may be the defective procedure, the operator has not committed to an error. However, if the operator had been appropriately trained to perform the task and, could reasonably have been expected to identify the defect in the procedure, then there is a personnel problem.

Apparent Cause:	Apparent Cause reflects symptoms of a deviation, defect or failure, which usually comes into view or becomes notable during the investigation process.
Underlying Cause:	Underlying cause implies latent weakness in the organizational systems, although not direct visible or readily apparent but contained in the nature of the event. Root Cause is usually one of the underlying causes.

For an example, during routine power operation, a feed-water drain line inside confinement ruptured forcing an orderly shutdown to effect repairs. Visual inspection followed by a metallurgical analysis clearly pointed to vibration-fatigue as the cause of the failure. Further, the source of vibration was attributed to improperly supported the drain line. Additional investigation had revealed a design error. All those may be only regarded as apparent causes. The vibration of the drain line was known for many persons in a number of months. Therefore, lack of feedback of operational data to the design engineers was identified by the RCA team and was considered as an underlying cause of the rupture of the feed-water drain line.

Another example, a common mode failure in redundant trains of safety related equipment was attributed to corrosion due to moisture intrusion. However, the investigator/ analyst pursuing the RCA identified that the reason for the moisture intrusion was failure to properly seal the equipment following maintenance. Furthermore, the investigator/ analyst revealed there were no provisions for resealing equipment after maintenance in the procedures and the maintenance staff was simply lack of attention to the assembling work. However, the RCA team did not satisfy these apparent causes and discovered a couple of underlying causes such as maintenance procedures were not provided to the maintenance crew, management did not enforce use of procedures in the work, etc.

1.4 PRCAP PROCESS

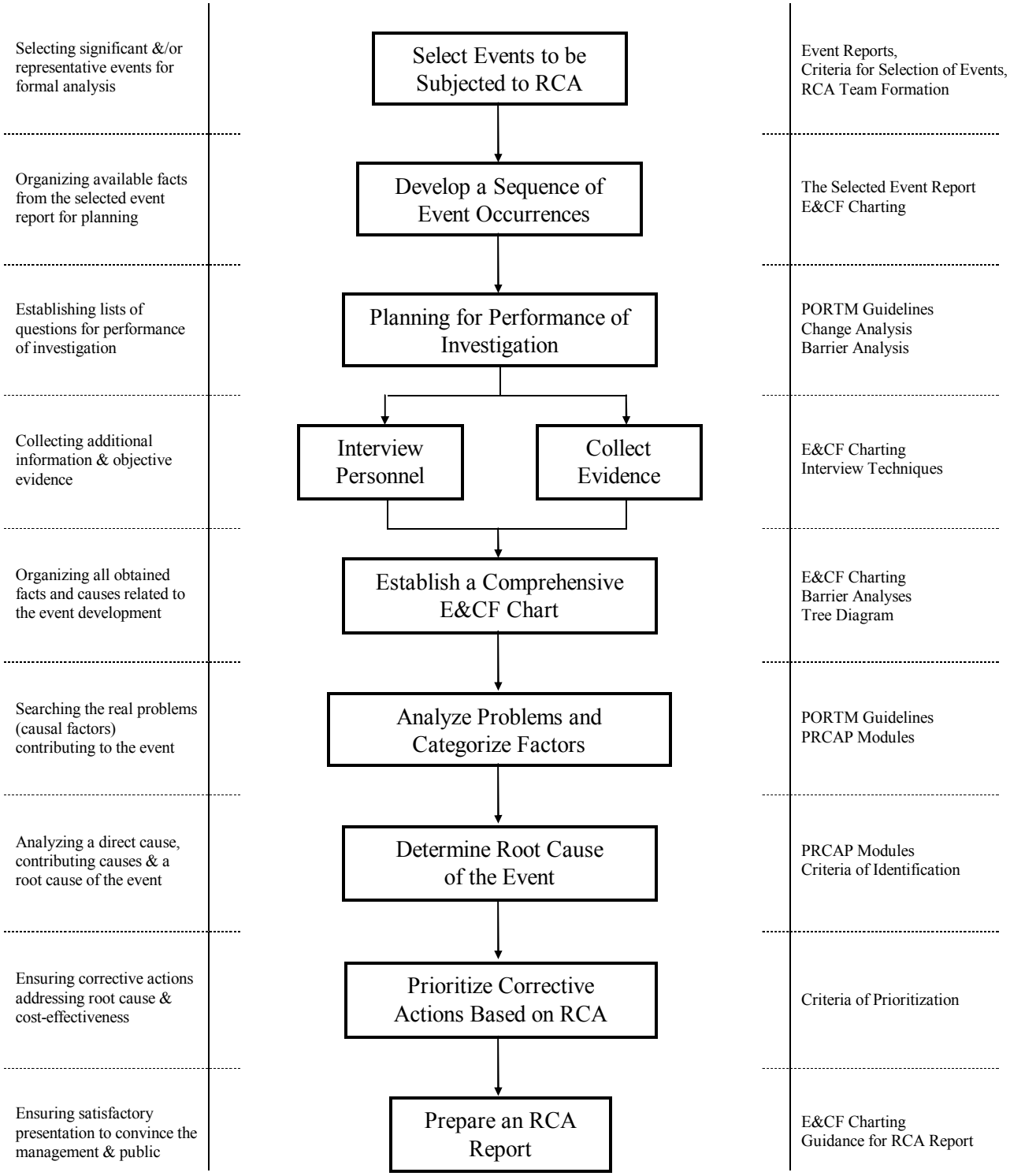
The process included in PRCAP provides for a disciplined approach for systematically selecting and applying different RCA tools while performing in-depth investigation and analysis of E&HP contributors to an event. The complete process is presented in Figure 1.1 and consists of three columns:

- PRCAP Flow, which displays the major steps used to investigate and analyze an event (central column of the diagram);
- Purpose of each of the major steps, which will be described in relevant sections of Chapter 2 of Part I in this document (left column of the diagram);
- Tools, which are the RCA techniques, criteria, guidance/ guidelines used in the major steps and will be detailed in Part II of this document (right column of the diagram).

The PRCAP is presented assuming that the investigator/ analyst will perform an independent RCA of operational events by using all those PRCAP tools. Nevertheless, an expert may choose to modify the whole process and use, as needed, only those portions of the RCA techniques and other tools for performance of investigation and analysis.

FIGURE 1.1: *PRCAP Process*

Purposes	**Process Flow**	**Main Tools**


Selecting significant &/or representative events for formal analysis
Select Events to be Subjected to RCA
Event Reports, Criteria for Selection of Events, RCA Team Formation
Organizing available facts from the selected event report for planning
Develop a Sequence of Event Occurrences
The Selected Event Report E&CF Charting
Establishing lists of questions for performance of investigation
Planning for Performance of Investigation
PORTM Guidelines Change Analysis Barrier Analysis
Collecting additional information & objective evidence
Interview Personnel
Collect Evidence
E&CF Charting Interview Techniques
Organizing all obtained facts and causes related to the event development
Establish a Comprehensive E&CF Chart
E&CF Charting Barrier Analyses Tree Diagram
Searching the real problems (causal factors) contributing to the event
Analyze Problems and Categorize Factors
PORTM Guidelines PRCAP Modules
Analyzing a direct cause, contributing causes & a root cause of the event
Determine Root Cause of the Event
PRCAP Modules Criteria of Identification
Ensuring corrective actions addressing root cause & cost-effectiveness
Prioritize Corrective Actions Based on RCA
Criteria of Prioritization
Ensuring satisfactory presentation to convince the management & public
Prepare an RCA Report
E&CF Charting Guidance for RCA Report

However, among those tools, three are extremely essential to perform RCA when following this process. They are PORTM, the PRCAP modules and the Event & Causal factors (E&CF) Charting. Highlights of PORTM and elements in the PRCAP modules are briefly presented in Section 1.5. Examples of application of the E&CF Charting will be presented in Chapter 2 in incorporation with the illustration of the PRCAP process.

1.5 PORTM AND PRCAP MODULES

1.5.1 Highlights of PORTM

PORTM represents five columns (categories) of process: **P**revention, **O**bservation, **R**esponse, **T**eam Performance, and **M**anagement.

PORTM is a decision tree represented by a series of Yes/No questions for logic identification of E&HP factors in consideration of prevention and elimination of the event development at different stages and/or levels. Application of PORTM will guide the investigator/ analyst during the investigation process to focus on those areas where the causal factors may be present, and during the analysis process to allocate the findings or conclusions into one or more standard categories of the PRCAP modules.

P: Prevention category searches for those deficiencies, which had neither been recognized nor detected but initiated or contributed to the event; it also identifies those conditions, which should have existed or been provided to prevent or mitigate the event.

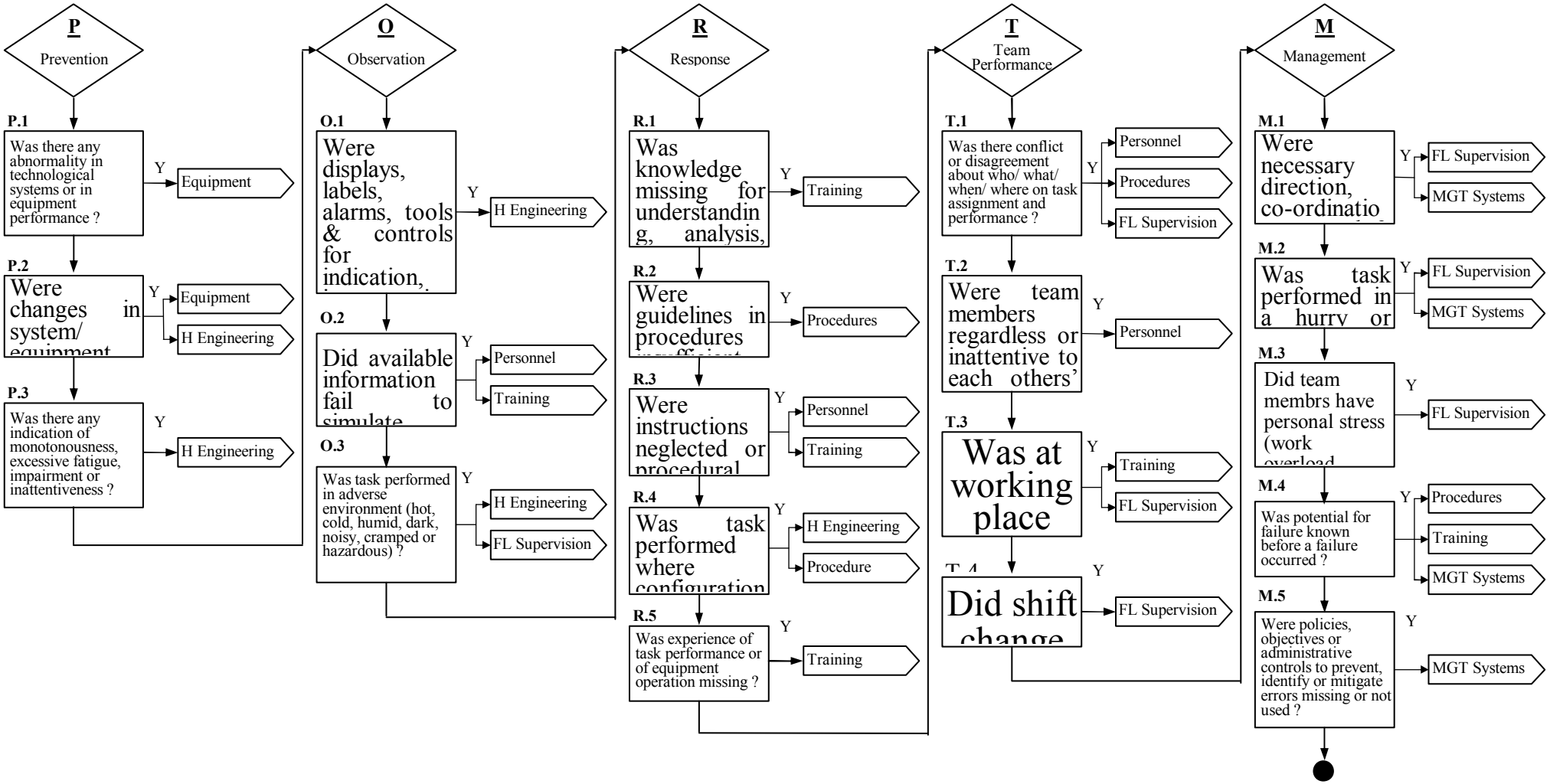
O: Observation category addresses prerequisites for effective responses to abnormalities; it searches for failures in observation of conditions and symptoms and for reasons of such failures that contributed to nonsuccess of detection, identification and diagnostics.

R: Response category searches for those factors that influenced, affected or hindered an individual being stimulated to response to abnormalities, including interpretation of encountered conditions/ symptoms, processing available information, or prompting an expected action.

T: Team performance category applies to problems or difficulties where more than one person was involved and it searches for those factors that affected the process of the team decision-making and the team performance that should have been expected to effectively response to abnormalities.

M: Management category searches for those supervisory and managerial factors (organizational and administrative factors), which had been unable or failed to prevent, detect, correct, and mitigate the erroneous or defective performance of the individual or the team.

FIGURE 1.2: PORTM - GUIDE TO E&HP PROBLEMS AND CAUSE MODULES (See Additional Sheet)



Note: During investigation, ask each of the questions following the flow chart and ask "why" to collect facts, then assess if further investigation is needed in the areas indicate
During analysis, compare each of the factual problems on the E&CF chart to the questions in the flow chart to determine its cause categories, then identify causal factors

FIGURE 1.2: PORTM - Guide to E&HP Problems and Cause Modules

The flow chart of the PORTM system is briefly presented in Figure 1.2.

1.5.2 Elements in PRCAP Modules

The application of the questions in PORTM will lead the investigator/analyst to allocate problems in particular areas for further analysis. These areas are standardized as 7 cause categories:

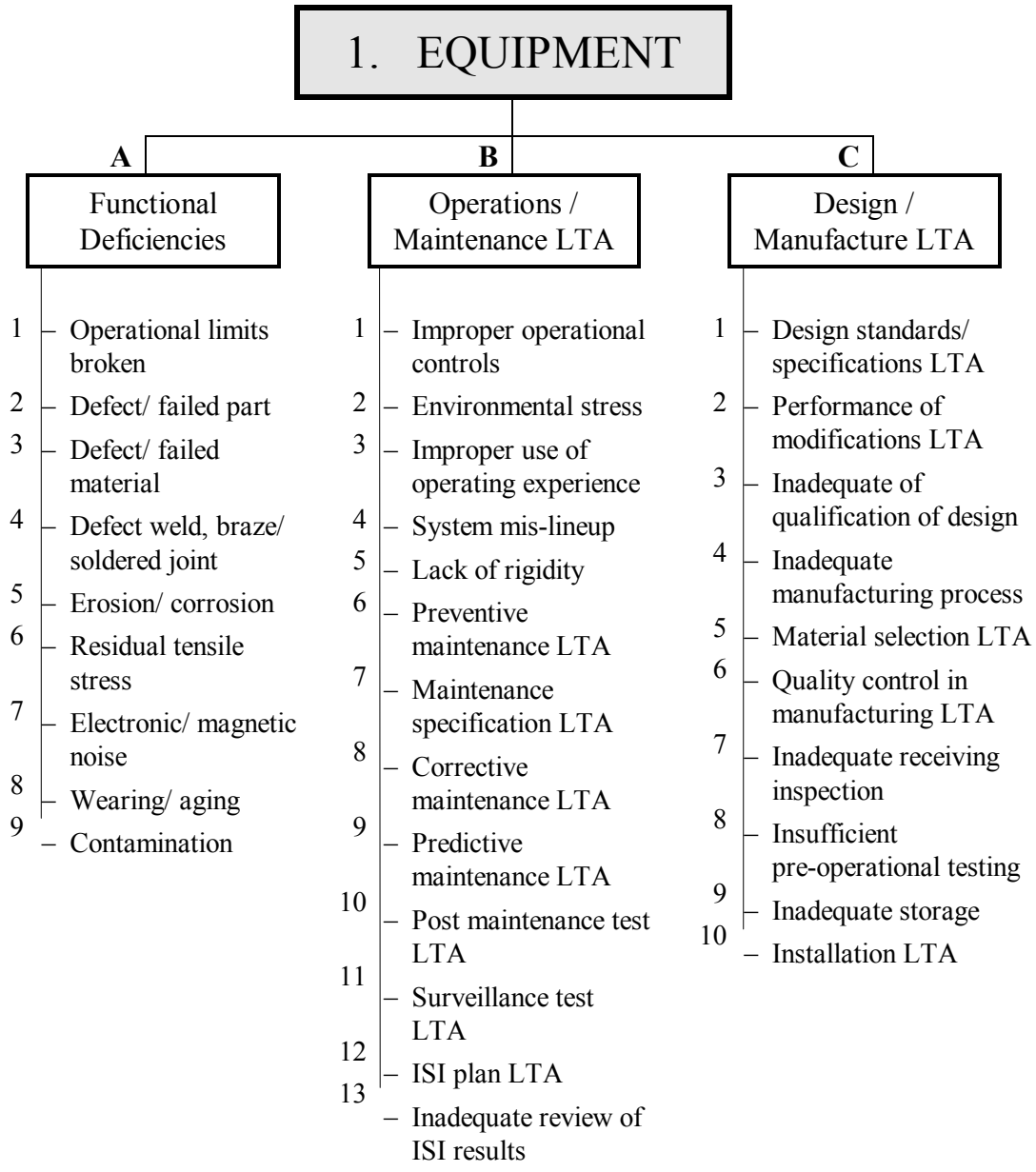
1. **Equipment**,
2. **Personnel**,
3. **Procedures**,
4. **Human-Engineering**,
5. **Training**,
6. **First Line Supervision**, and
7. **Management Systems**.

The seven PRCAP modules or categories of causal factors have been carefully selected to include all three basic elements in the performance of any task and in the evolution of an event (equipment, personnel and procedures) and other environmental, functional and management elements. They are structured with the intention to address all problems that could arise in analyzing the direct causes, contributing causes the root causes of the operational events. Each module is, in fact, formulated in a tree structure with branches and causal factors at three levels. The PRCAP modules is totally composed of 7 cause categories, 24 cause branches and more than 200 causal factors.

The causal factors and the set of questions listed in Chapter 7 may not cover every possible problem to be met. However, they have been designed to cover a broad spectrum of E&HP contributors. The cause branches, causal factors and questions may be modified or improved as practical experience is gained.

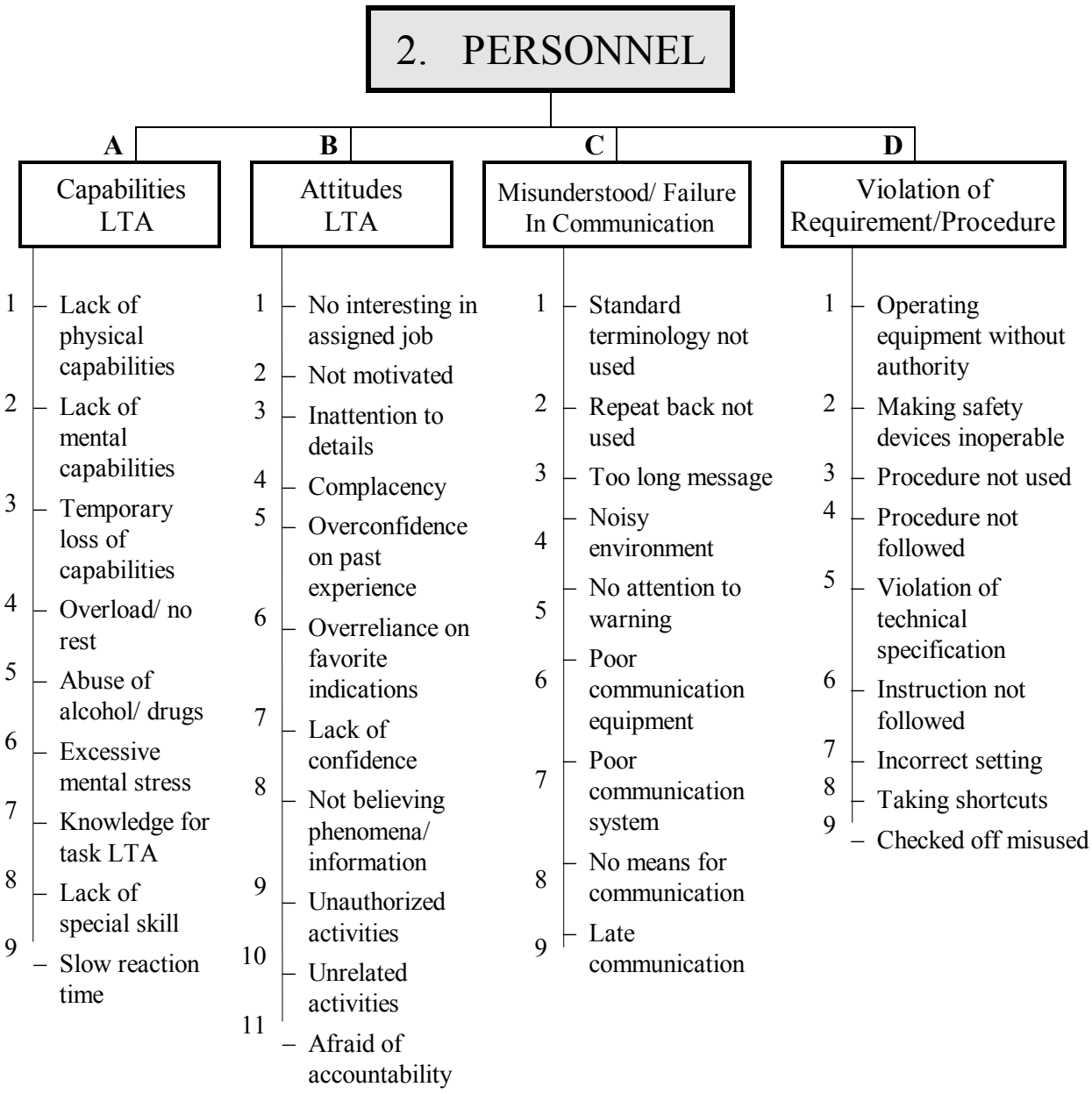
The seven PRCAP modules, together with their coded branches and causal factors are presented in Figures 1.3 - 1.9 respectively.

FIGURE 1.3 ***Module 1 - Equipment***



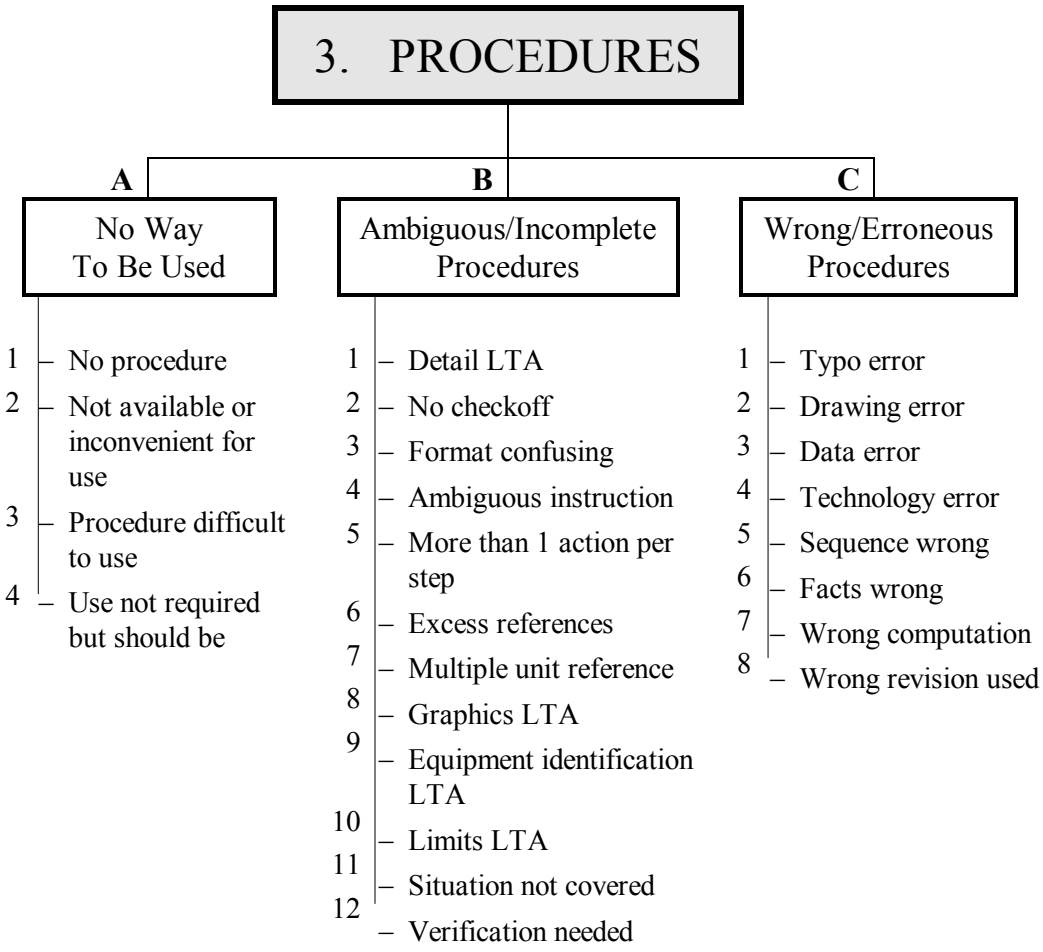
Note: LTA - Less Than Adequate.

FIGURE 1.4 ***Module 2 - Personnel***



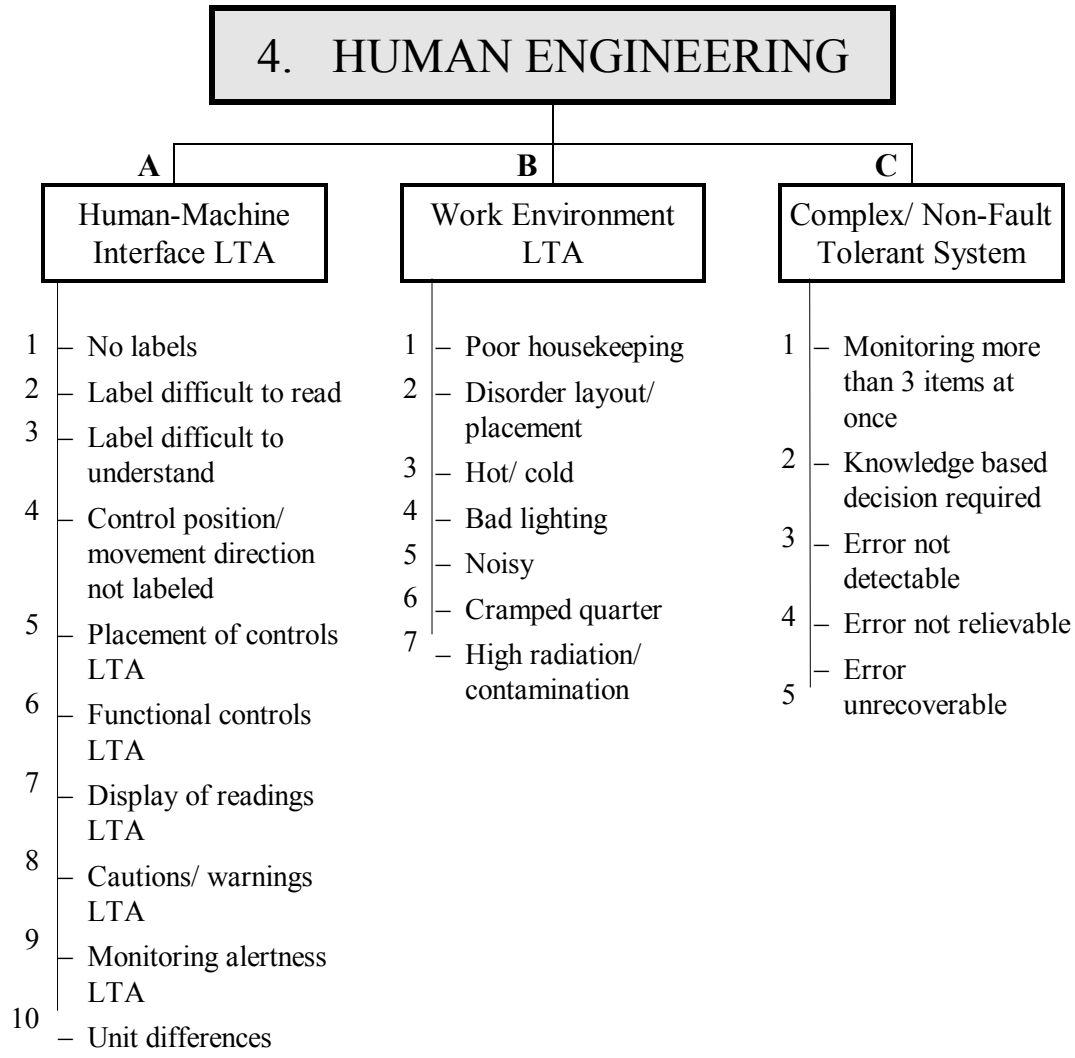
Note: LTA - Less Than Adequate.

FIGURE 1.5: ***Module 3 - Procedure***



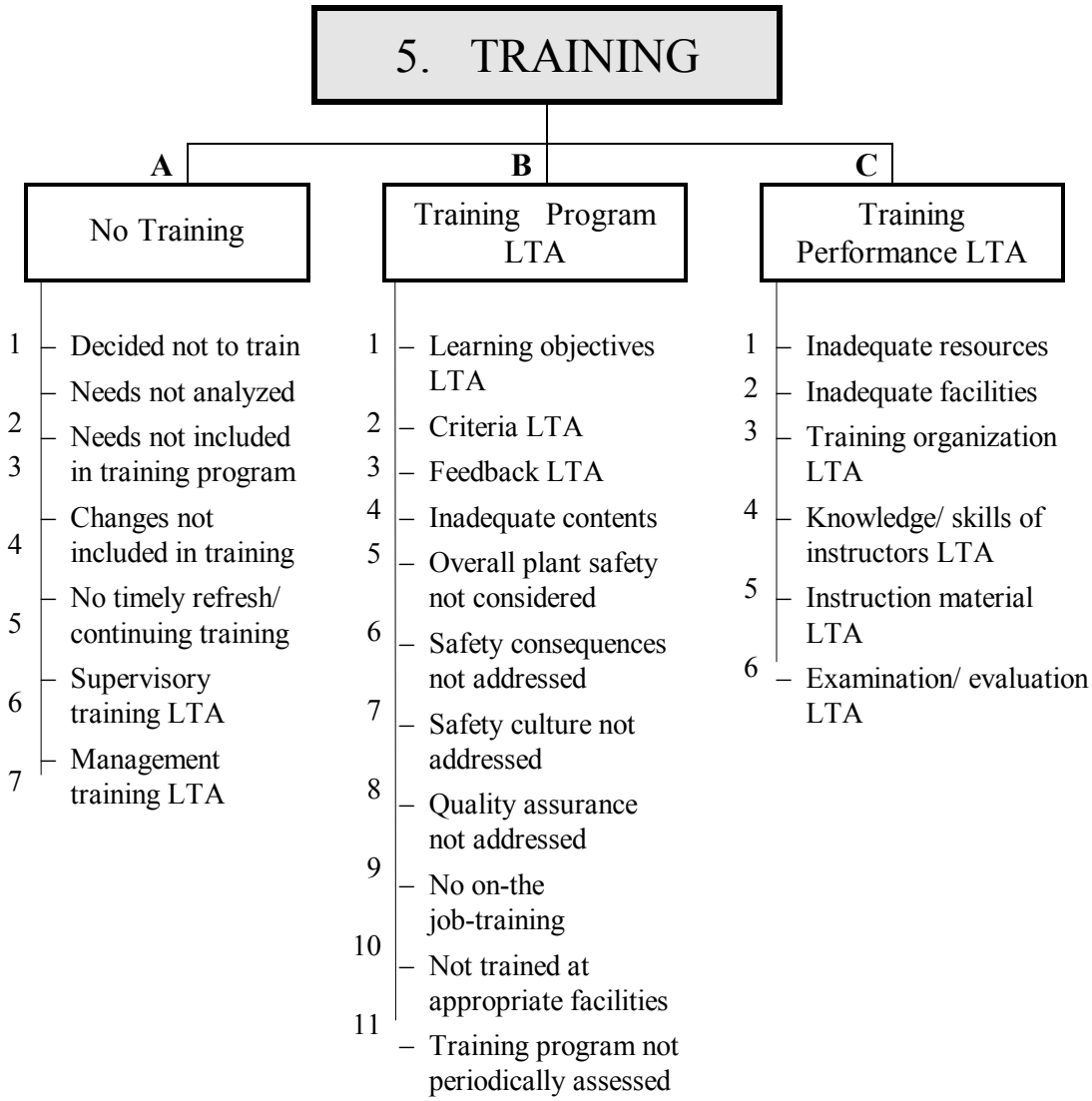
Note: LTA - Less Than Adequate.

FIGURE 1.6: ***Module 4 – Human Engineering***



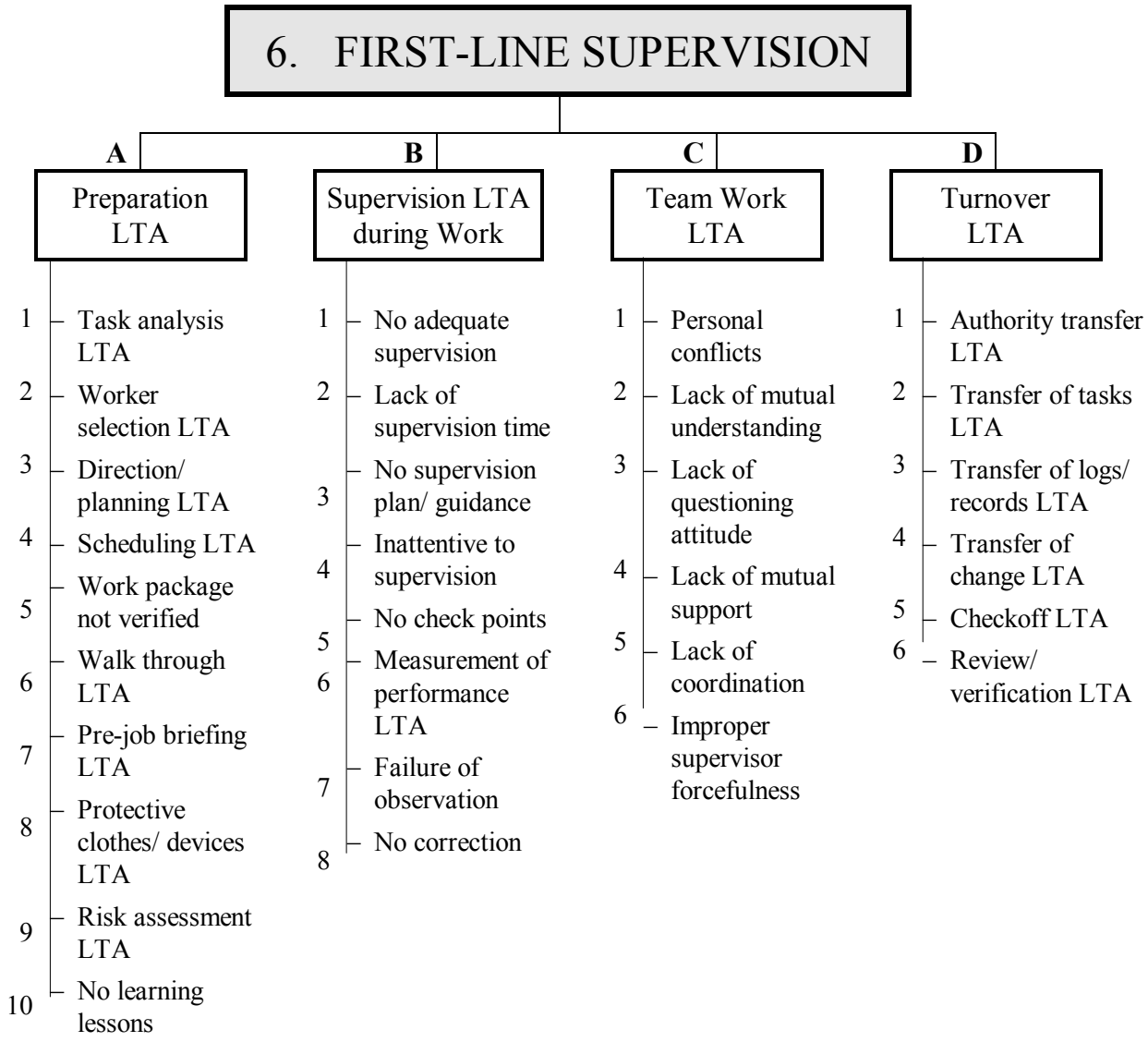
Note: LTA - Less Than Adequate.

FIGURE 1.7: ***Module 5 - Training***



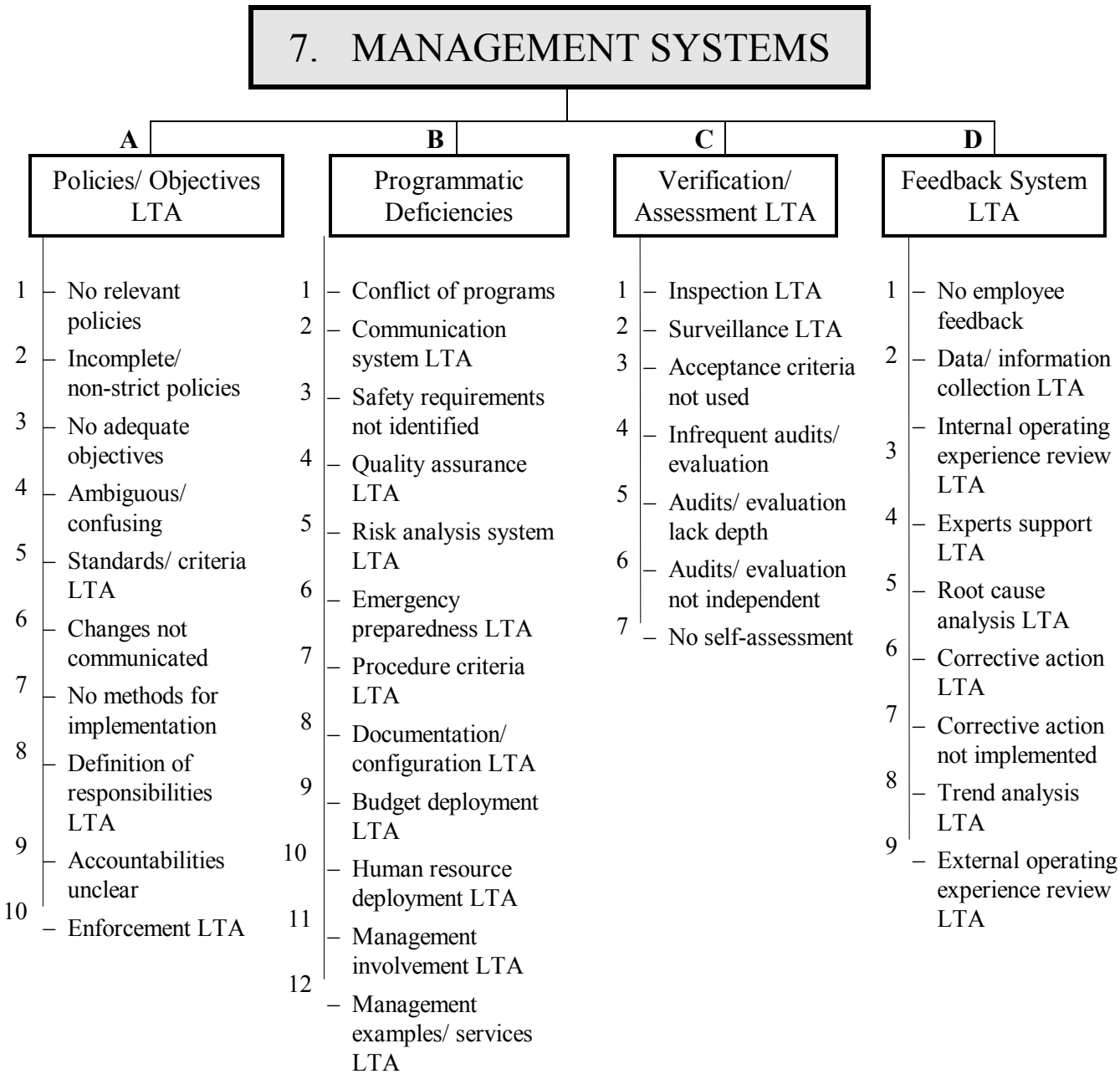
Note: LTA - Less Than Adequate.

FIGURE 1.8: ***Module 6 – First-Line Supervision***



Note: LTA - Less Than Adequate.

FIGURE 1.9: ***Module 7 – Management Systems***



Note: LTA - Less Than Adequate.

1.6 STRUCTURE OF THIS DOCUMENT

PRCAP consists of two parts, appendices and annexes.

1.6.1 Part 1

Part I is deemed the essential part of the PRCAP. Should an expert with sufficient knowledge on the common RCA techniques have carefully studied this part, he/she would be able to apply PRCAP to analyze the root cause of any operational event without recalling Part II. There are two chapters in PART I.

In addition to the background, objectives and structure of this document, Chapter 1 includes definitions of basic terms used in this document, highlights the PRCAP process and presents two of the three most important RCA techniques, developed specifically for application of PRCAP, i.e. PORTM and the PRCAP modules.

Chapter 2 prescribes the PRCAP process, step by step, by analyzing a typical example. The E&CF Charting, which is considered as another one of the three most important RCA techniques in application of the PRCAP, is illustrated in this chapter. This process should be followed during the investigation and analysis process in order to consider all possible causal factors and come to correct conclusions.

1.6.2 Part II

Part II includes eight chapters and is descriptive in nature. Each of the investigation or analysis tools (techniques, criteria, guidelines or guidance) listed in the right column of Figure 1.1, except Event Reports, is described in each of the respective chapters.

Part II is mainly prepared for those who would like to comprehend more details of each of the RCA techniques, criteria, guidance and guidelines that constitute and/or contribute to the investigation/ analysis process. Among others, the three most important techniques (PORTM, PRCAP modules and E&CF charting) are again presented but with more in-depth descriptive guides and supporting examples.

Chapter 3 provides some criteria on selection of events for formal RCA based on the plant event reports promptly prepared and submitted according to the reporting requirements of the utility and the regulatory body. Some suggestions on the formulation of an RCA team, especially on the expertise required for the team experts, are also included.

Chapter 4 introduces, in general, techniques for conducting personal interviews. Emphasis is given to control distortion and elimination of the influence of personalities from both the witness and the investigator.

Chapter 5 systematically summarizes four RCA techniques, i. e. Change Analysis, Barrier Analysis, Event and Causal Factors (E&CF) Chart, and Tree Diagram, which are commonly used in almost all RCA methods and are basis for investigation and analysis of the operational events. This chapter was a summary of a series of reference documents taking into account their practical applications.

Chapter 6 explains, in detail, the PORTM searching system. In particular, an example of application is provided by asking and answering all questions in the PORTM flow chart to complete the searching process.

Chapter 7 provides practical worksheets for application of the PRCAP modules. Following application of the PORTM, the cause categories are determined. Answering the more than 200 questions in the worksheets will help further to allocate the findings or conclusions at appropriate places in the second level, cause branches, and the third level, causal factors, in the PRCAP modules.

Chapters 8, 9 and 10 provide general guidance or criteria for determination the root causes, prioritization of corrective actions and preparation for the RCA report, respectively.

1.6.3 Appendices and Annexes

Examples of analysis results of some selected operational events occurred at Paks NPP are provided in Appendices.

Annexes 1 and 2 compare the two searching systems and the two groups of cause modules between HPIP and PRCAP, respectively.

2. STEPS IN PRACP PROCESS

The PRCAP process is generally composed of two successive and overlapping to some extent processes: investigation and analysis.

- Investigation is a detailed systematic search to discover factors and determine the truth of the factors (who, what, where, when, why, and how) related to an event.

- Analysis is a consistent and logic evaluation of all factors related to the event and determination of, based on conceived hypotheses, the direct cause, contributing causes and the root cause with.

During investigation, the RCA team asks questions to those who are interviewed to get evidence from them, relevant records and facts. The investigation results will be summarized on the E&CF chart. The RCA team can not complete the investigation process by its own. During analysis, the RCA team members ask questions and try to get answers among themselves. The end product is the root cause of an event. The RCA team might complete the analysis process by themselves and then seek agreements from all relevant persons.

There are nine steps in the PRCAP process. Step 1 to 5 might be considered as those of the investigation, while Step 5 to 9 might considered as those of the analysis process. The whole PRCAP process is pursued, step-by-step, following a distinct path of PRCAP to the final determination of the root cause.

However, the sequence of the steps is an ideal concept. In practice during the analysis process, retrieval investigations or further investigations for searching and verifying new factors are inevitable or even essential for the determination of the root cause.

2.1 STEP 1 - SELECTION OF EVENTS TO BE SUBJECTED TO THE RCA

Purpose: Selecting significant and/or representative events for formal analysis.

Tools:
- Event reports
- Criteria for selection of events (§ 3.1)
- RCA team formation (§ 3.2)

2.1.1 Step 1.1 - Selection of Events

Generally, analysis of the root cause of an event is comprehensive and time-consuming. There is no need for analyzing all operational events to identify the performance problems within an organization.

Whenever an operational event occurs, the selection criteria should be applied in order to determine whether it is a significant or representative event to be subjected to the comprehensive RCA. The plant historical operational events should also be screened in regular intervals to identify the performance trend and to determine whether any events in the past should be subject to the formal RCA. Maximization of the effectiveness of the formal RCA should be pursued in view of the possible resource constraints (e.g. budget, manpower and production needs).

2.1.2 Step 1.2 - Establishment of an Expert Team

Usually, an expert team should be established for the in-depth analysis of the selected event. Adequate authority, responsibilities and organizational freedom should be given to the established expert team. The team composition should be represented by a range of expertise which includes detailed knowledge of the plant design, organizational structure, related work procedures, required technical disciplines and, additionally, experience in application of the RCA techniques and methods.

The expert team may include individuals from different departments of the plant. Independence of the experts to be selected for performing RCA should be preserved as far as possible. Hence, team members should not have been involved in the event to be analyzed to ensure that independent conclusions and recommendations are developed.

Outside experts may be invited to participate in the analytical process, jointly with the plant team or independently as the external peer, in order to justify and improve the standards of the RCA.

2.2 STEP 2 - DEVELOPMENT OF A SEQUENCE OF EVENT OCCURRENCES

Purpose: Organizing available facts from the selected event report for planning.

Tools:
- The selected event reports
- E&CF charting (§ 5.3)

2.2.1 Step 2.1 - Review of the Available Event Report

Any operational event should be promptly reported according to the established regulatory and/or plant reporting criteria, with regard to both causes and consequences. These event reports are bases for performing the formal PRCAP.

Whenever an event has been selected, the expert team should start with review of the available information contained in the event report. From the title of the report, the INES scale, the event description and the initial analysis of the event, some preliminary comprehension of the event scenario may be acquired. Notwithstanding, a number of questions may appear and further investigation may be deemed as necessary.

2.2.2 Step 2.2 – Categorization of Occurrences

All occurrences related to the event contained in the event report should be identified and listed in a chronological order, so far as possible. These identified occurrences should be categorized according to their pertinence to the problems of the event.

Only should those occurrences that were pertinent to the problems of the event be selected and recorded by the team for further analysis. For each of the selected occurrences, some potential reasons or causal factors should also be pursued from the event report and recorded.

2.2.3 Step 2.3 - Drafting of the Initial E&CF Chart

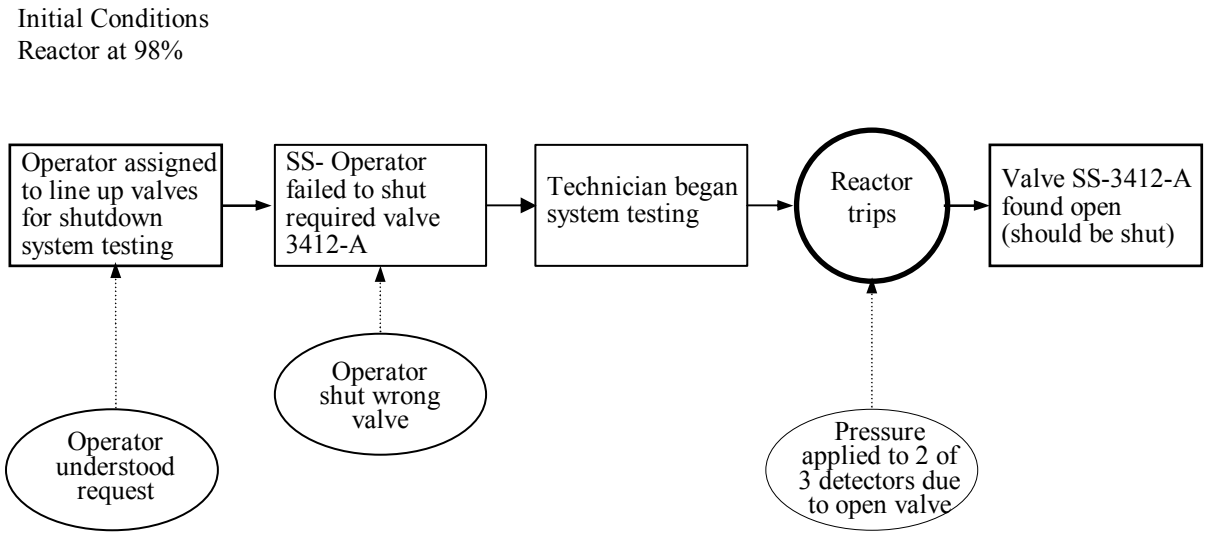


FIGURE 2-1: *An Initial E&CF Chart*

From the available information in the event report, a sequence (or sequences) of pertinent occurrences leading to the event should be defined and drafted on a paper with some available conditions or potential causal factors connected to the sequence. Thus, an initial E&CF chart is formulated with holes and likely inconsistencies that are subjected to further investigation. The initial E&CF chart may be only a skeleton of the final chart, and will be supplemented and upgraded as additional facts are gathered.

Figure 2.1 is an example of an initial E&CF chart, i.e. a sequence of occurrences in a chronological order attached with some conditions or potential causal factors. The event portrayed in this figure will be used as an illustration throughout Part I of this document.

The chart provides a visual tool for studying the occurrences together with their conditions. The causal factors and finally the root cause will be determined by continuously and repeatedly asking questions by using the RCA techniques.

2.3 STEP 3 - PLANNING FOR PERFORMANCE OF INVESTIGATION

Purpose: Establishing lists of questions for performance of investigation.

Tools:
- PORTM guidelines (§ 6)
- Change analysis (§ 5.1)
- Barrier analysis (§ 5.2)

The three above RCA techniques will be used to help the investigator/ analyst to plan and perform the investigation process. Among them, the PORTM guidelines were specifically developed for PRCAP and can be effectively used not only in the investigation process but also in the analysis process.

Application of the RCA techniques is intended to guide the investigator/ analyst during the investigation process by asking standard questions to get specific answers with regard to the particular event.

2.3.1 Step 3.1 - Preliminary Application of PORTM

When the initial E&CF chart is established, the PORTM system (see Figure 1.2) should be applied to search the holes (missing occurrences and conditions) and to identify the potential areas where further investigation is needed. By using the PORTM system, the investigator/ analyst may ask all questions, one by one, following the PORTM flow chart to whoever being interviewed and then ask "why" to collect consistent data and information on the event. If needed, further investigation may be pursued in the indicative areas associated to the flow chart.

The PORTM system would be used several times to several groups of people during the investigation process. The answers received each time in application of the PORTM system should help the RCA team to correct, augment and update the E&CF chart and to plan the next investigation if appropriate, such as:

- Who should be further interviewed?
- What documents should be further reviewed?
- Where should a further survey be performed?

2.3.2 Step 3.2 - Preliminary Application of Change Analysis

Change analysis is used specifically for investigation of problems related to equipment, personnel and procedures. A series of questions on What ? When ? Where ? Who ? and How ? should be asked during the investigation process which will lead toward answering the determination question: Why ? Examples of those questions are:

- What the problem is ?
- Where it existed ?
- When it began ?
- Who was involved ?
- How it developed ?
- Why it occurred ?

Change analysis compares and identifies differences in systems, processes and practices between the last time the task was completed successfully and the time when performing the same task caused an occurrence. These differences are subsequently evaluated to determine how they contributed to the event. The problems resulting from all changes should be recorded on the initial E&CF chart.

2.3.3 Step 3.3 - Preliminary Application of Barrier Analysis

In this procedure, a barrier is something that separates an affected target from an undesirable condition or action. Barrier analysis searches for barriers (either physical or administrative) which were failed or absent in prevention and mitigation of occurrences. The following questions should be asked during the investigation process:

- Where, when and which barriers were broken or failed in the event development?
- What kind of functions these barriers should have provided to prevent or mitigate the event?
- Were there any additional barriers and controls that might have prevented or mitigated the event if they had been in place ?

Barrier analysis identifies all barriers and assesses each of them for its effectiveness. The failed or absent barriers are subsequently evaluated to determine how they contributed to the event. The results of the barrier analysis should be recorded on the initial E&CF chart.

2.4 STEP 4 - INTERVIEW OF PERSONNEL AND COLLECTION OF EVIDENCE

Purpose: Collecting additional information and objective evidence.

Tools:
- E&CF charting (§ 5.3)
- Interview techniques (§ 4)

The basis for RCA is the complete data and information about the event. The information contained in the event report is usually not enough. It would be of great value to employ some investigation techniques in the RCA process for additional facts to demonstrate the objectivity and completeness of the information required for the RCA. The information that should be collected consists of conditions before, during and after the event; personnel involvement; environmental factors; and other information having relevance to the conditions or problems.

There are four common techniques for any investigation or verification activities:

- Interview of personnel,
- Review of records and documents,
- Survey of the work place or the site,
- Experiment or simulation, if necessary.

A repeated use of the combination of at least the first three techniques usually ensures an effective investigative process. Interview of personnel is, in particular, important because of the comprehensiveness of the RCA. The other three techniques are applied to the collection of physical or objective evidence.

2.4.1 Step 4.1 - Interview of Personnel

Interview of personnel involved in the event provides an important source of information, some of which can not be readily obtained by other techniques. Interview of personnel can also verify information provided by other techniques. The initial E&CF chart and the lists of questions from the initial PORTM, Change Analysis and Barrier Analysis, prepared during the planning stage should be used during the interview.

Those people should be interviewed, who are most pertinent to and familiar with the problems of the event, including:

- Those involved with the event,
- Those who were associated with or observed the event,
- Supervision and management personnel of those involved in the event,
- Knowledgeable technical experts and relevant training personnel,
- Other personnel who had performed the same or similar job or tasks in the past.

The analysis team should decide, depending on the nature and significant of the event, to what extent personnel should be interviewed. The analysis team should always consider the interviewee's objectivity and frame of reference. Nevertheless, interviews must be fact finding and not fault finding.

During interviews, the analysis team should discuss the initial E&CF chart with the personnel being interviewed to fill in any holes and to reconcile any inconsistencies in

various accounts of the perceptions and facts. Each person interviewed should be asked:

- Does this chart accurately describe what happened ?
- What additional information can you provide about the causes for theses occurrences in the event progression ?

It is the responsibility of the plant management to ensure that timely availability of those to be interviewed to the analysis team. Individual statements could be obtained if time or the number of personnel involved make the interview impractical.

2.4.2 Step 4.2 - Collection of Evidence

Generally, the results of personnel interview can not be conclusive. Further evidence (objective or physical evidence) should be collected through other investigation techniques.

Original records and relevant documents with respect to the event should be reviewed. Whenever appropriate, the pertinent portions should be used to support the analysis. Examples of records and documents that should be reviewed are:

- Records of task performance, especially records on adverse environment, abnormal phenomena, unusual actions, performance deficiencies;
- Instructions and procedures used for preparation, performing, control and evaluation of tasks;
- Documents recording operational and maintenance information, such as work orders, specifications, log books, analysis/ test results, computer outputs, etc.;
- Reports and documents with regard to recent changes in administrative systems and technological systems;
- Other documents which furnish the objective evidence of the quality of items and activities affecting safety such as procurement documents, surveillance or audit reports, regulatory inspection reports, etc.

Once all data and facts associated with the occurrences have been collected, the information should be verified to ensure the accuracy. The investigation process may be enhanced if some physical evidence is collected through survey of the work place or the site, such as

- Viewing physical layout of the work area,
- Following the sketches of the technological systems,
- Photographing the failed equipment and spilled fluids,
- Studying the ruptured part and its material, etc.

Whenever necessary, walkthrough (survey of the work place or the site) should be performed despite production pressures.

2.5 STEP 5 - COMPLETION OF A COMPREHENSIVE E&CF CHART

Purpose: Organizing all obtained facts related to the event development.

Tools:
- E&CF charting (§ 5.3)
- Barrier analysis (§ 5.2)
- Tree diagram (§ 5.4)

All information obtained during interview of personnel and collection of evidence should be organized and sketched on the E&CF chart. Thus, the E&CF chart is becoming comprehensive and likely completed. The Tree Diagram technique may be used together with the E&CF chart, if two or more independent chains of occurrences were present and it is necessary to arrange them logically.

Figure 2.2 is an example of the comprehensive E&CF chart, which is developed from the initial E&CF chart and incorporated with all the results obtained from interviewees, documentary sources, and other physical evidence during the investigation process.

On the complete E&CF chart, there are one barrier that was broken and one change that occurred during the process of the event development.

Broken barrier: A valve was kept open, which should have been closed to prevent unwanted energy flow between the source and the target (§5.2.1).

Occurred change: A new operator was assigned to line-up valves for the shutdown system testing, who had never been performed this task before (§ 5.1.1).

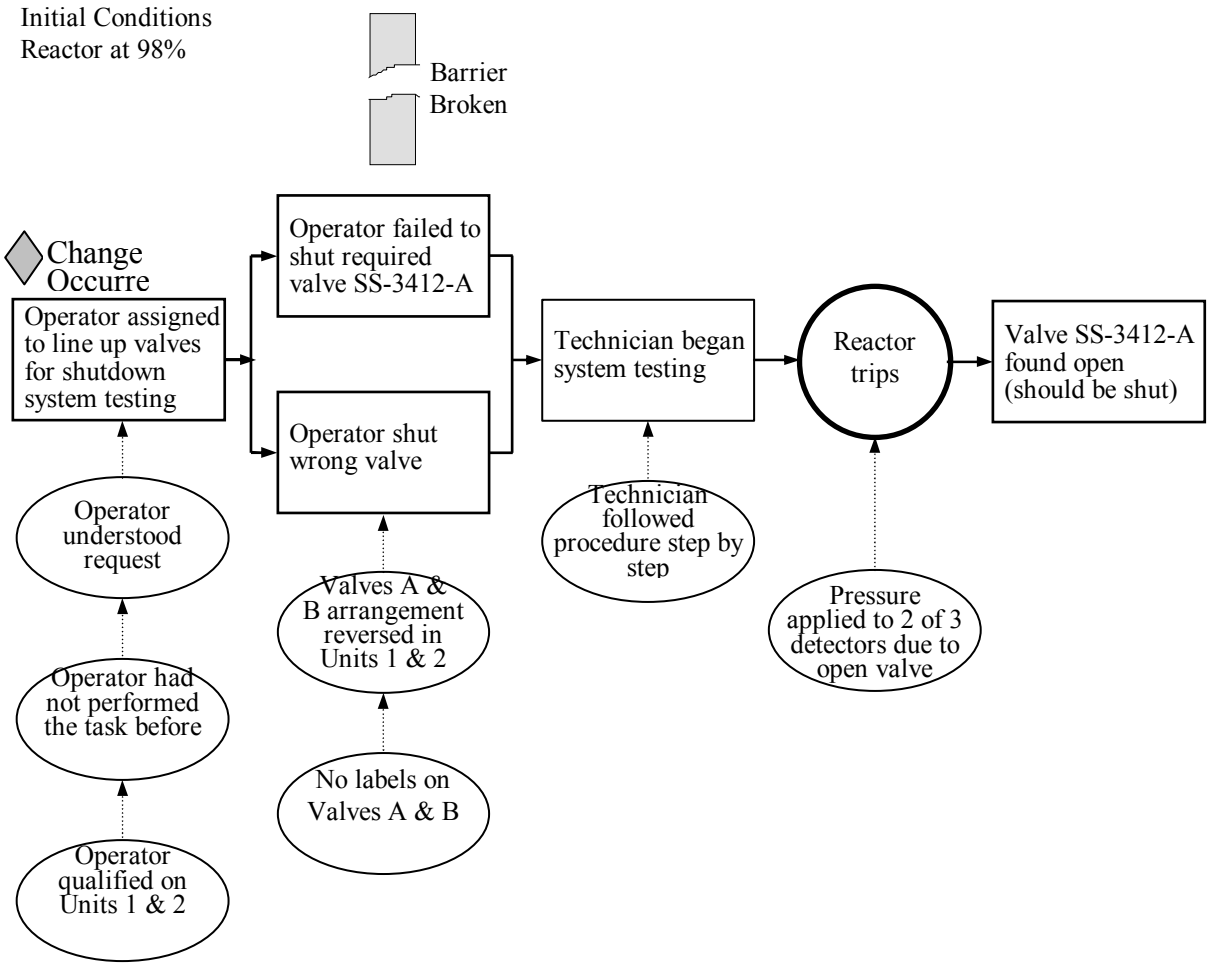


FIGURE 2-2: *An E&CF Chart with Investigation Results*

The comprehensive and completed E&CF chart will be used to analyze the direct cause, contributing causes and the root cause of the event through the next steps described below.

2.6 STEP 6 - ANALYSIS OF PROBLEMS AND CATEGORIZATION OF FACTORS

Purpose: Searching real problems or causal factors contributing to the event.

Tools:
- PORTM guidelines (§ 6)
- PRCAP modules (§ 7)

The analysis process is formally started from review of the completed E&CF chart. All those occurrences and conditions should be verified and, if necessary, re-organized or re-arranged and then analyzed. The results of Step 6 are presented on Figure 2.3.

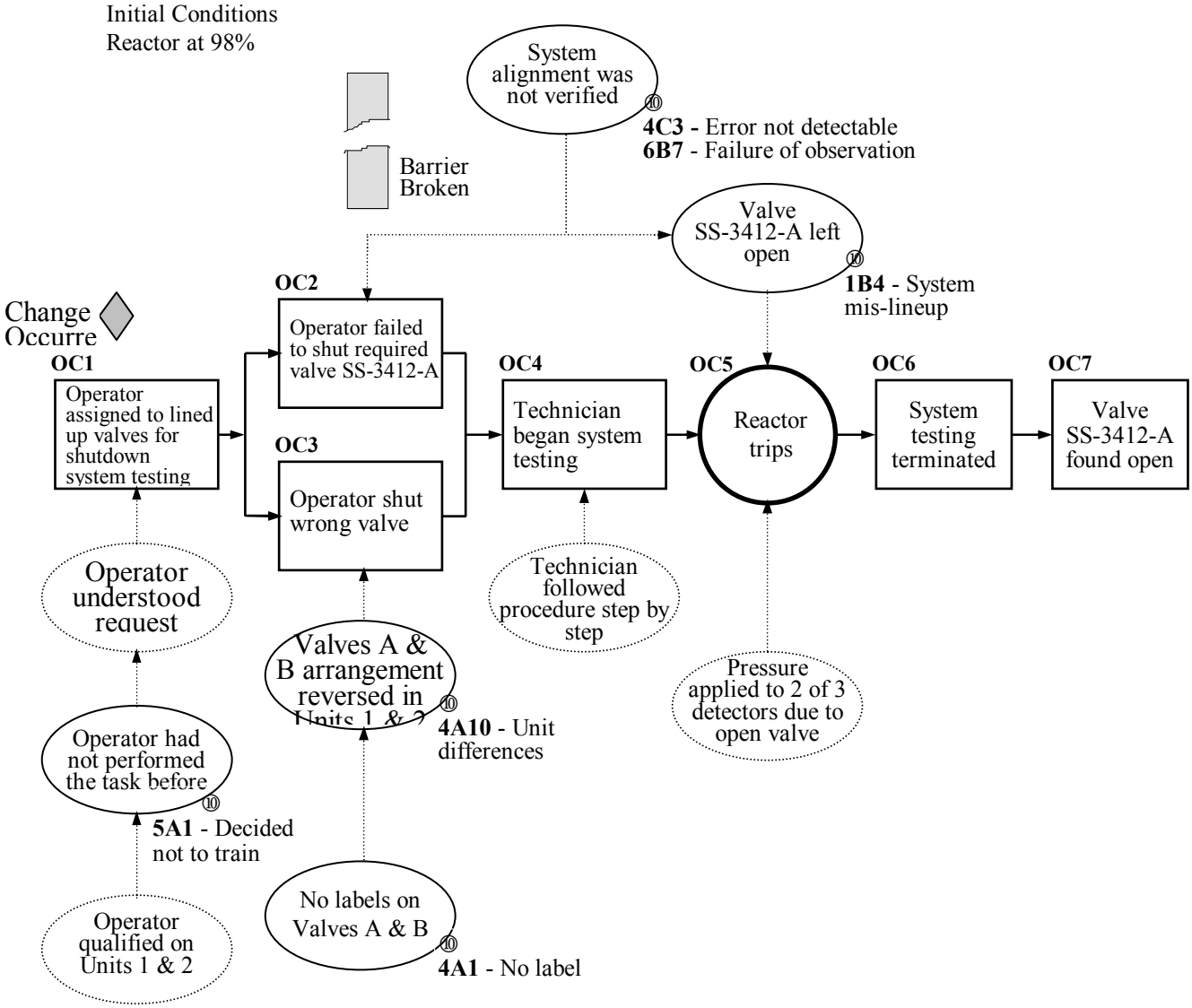


FIGURE 2.3: *An E&CF Chart with Identified Causes*

2.6.1 Step 6.1 – Review of Occurrences and Formulating New Factors

All the occurrences in E&CF chart should be individually reviewed to begin the analysis process. The review may include the sequence or sequences, the completeness, logic, presentation and etc.

Those occurrences, which had really contributed to the event, should be picked up and new factors are established, such as Occurrence 2 on the example E&CF chart. The description of the new factor "Valve SS-3412-A left open" is formulated referring to the criteria for describing the conditions (§5.3.3).

Additionally, a new occurrence "System testing terminated" is inserted into the sequence of the event to make consistent with its first occurrence.

2.6.2 Step 6.2 – Determining the Length of Sequence to be Analyzed

When the E&CF chart is amended and modified as appropriate, the RCA team should determine the scope of the analysis according to the nature of the event and the policy of the management. The E&CF chart of the illustrated example includes occurrences both prior to and post of the event. For the defined limited purpose, the occurrences post of the event are decided not subject to the RCA, which are:

Occurrence 6:

- Occurrence "System testing terminated" is beyond the scope of this event analysis.

Occurrence 7:

- Occurrence "Valve SS-3412-A found open" is beyond the scope of this event analysis.

2.6.3 Step 6.3 - Distinguishing Non-Problem Related Factors

Then, the RCA process should be forwarded to identify which factors were the real problems that contributed to the event. In fact, not all occurrences and conditions (factors) in the E&CF chart do cause problems. The correct identification of the problems is important in guiding the RCA to the right direction. The next analysis should be proceeded only with regard to the factors that are factual problems causing the event. Whenever there are uncertainties in determination of the problems, the PORTM system should be applied to help the identification.

On the E&CF chart of the illustrated example, those factors, which are not real problems, are identified and described as below:

Occurrence 1:

- Factor "Operator understood request" is not a problem and will not be subjected to further analysis.

- Factor "Operator qualified on Units 1 & 2" is agreed after investigation and under the following understanding that the operator is generally

qualified and the task performance was decided not to be included in the training program. Therefore, no further analysis is pursued.

Occurrence 4:

- Factor "Technician followed procedure step by step" is not a problem and will be not subjected to the further analysis.

Occurrence 5:

- Factor "Pressure applied to 2 of 3 detectors due to open valve" did cause the reactor trips, but it is not the real concerns and will be not subjected to the further analysis.

2.6.4 Step 6.4 - Categorization of Causal Factors

The PORTM system should be used again to verify the remaining factors excluded from the above conclusion. However, the technique of application of the PORTM system during analysis is different from that during investigation.

The potential causal factors should be judged and compared with the questions in the PORTM system to determine the cause categories. Based on the characteristics of the factors, some columns of the PORTM system might be highlighted. Depending on the knowledge and experience of the RCA team members, the flow chart in the PORTM system might not be systematically followed. When the cause categories are defined, the PRCAP modules (see Figures 1.3 – 1.9) should be applied to further determine the cause branches and causal factors. The two levels of questions in the PRCAP worksheets (§ 7) would be useful in the determination process.

By application of the PORTM system, sometimes, a few cause categories in the PRCAP modules may be identified for a single problem. The problem identified should be marked beside the factor on the E&CF chart with a triangle together with an assigned cause category.

The results of application of the PORTM system and the PÜRCAP modules to the example event are presented in the illustrated E&CF chart (see Figure 2.4). The casual factors are presented in accordance with the coding system of the PRCAP modules.

Occurrence 1:

- Factor "Operator had not performed the task before" is therefore applicable to R. 5 of the PORTM system, of which the causal factor is identified as:

  Module: 5. TRAINING
  Branch: A. No Training Performed
  Causal Factor: 1. Decided no to train

Occurrences 2 & 3:

- Factor "Valves A & B arrangement reversed in Units 1 & 2" is applicable to R. 4 of the PORTM system, of which the causal factor is identified as:

  Module: 4. HUMAN-ENGINEERING
  Branch: A. Human-Machine Interface LTA
  Causal Factor: 10. Unit differences

- Factor "No labels on Valves A & B" is " is applicable to O. 1 of the PORTM system, of which the causal factor is identified as:

  Module: 4. HUMAN-ENGINEERING
  Branch: A. Human-Machine Interface LTA
  Causal Factor: 1. No label

Occurrence 5:

- Factor "Valve SS-3412-A left open" is applicable to P. 1 of the PORTM system, of which the causal factor is identified as:

  Module: 1. EQUIPMENT
  Branch: B. Operations/ Maintenance LTA
  Causal Factor: 4 System mis-lineup.

2.6.5 Step 6.5 - Searching Underlying Causal Factors

This is one of the most important steps in the analysis process. Unfortunately, it can not be so prescriptive as the previous steps. The analysis results will depend, to some extent, on the knowledge, skill and experience of the members of the RCA team. With regard to the apparent factor "Valve SS-3412-A left open" or the fact "Broken barrier" on Figure 2.3, the RCA team may consider that the operator should not be blamed and ask questions to themselves, such as:

- Why had the defect or failure not been detected and corrected before the technician began the system testing ?

The broken barrier had not been detected and corrected because the system mis-lineup was not known. This answer may immediately generate more questions among the RCA team members such as:

- Why the system mis-lineup was not known by the shift team ?
- Why there was no warning or alarm on the mis-lined system ?
- Had the work performed first time by a new operator been verified ?
- Should the system mis-lineup be corrected automatically ?

Therefore, another fact would be identified, namely,

- "**System mis-alignment was not corrected**"

By applying the column of "Prevention" (P.2) of the PORTM system, a latent weakness in the" Human Engineering" should be recognized that contributed to the event. Applying the PRCAP module, the causal factor of "System mis-alignment was not corrected" is determined as:

Module:	4.	HUMAN ENGINEERING
Branch:	C.	Complex/ Non-Fault Tolerant System
Causal Factor:	3.	Error not detectable.

By applying the column of "Management" (M.1) of the PORTM system, a latent weakness in the" First Line Supervision" should be recognized that contributed to the event. Applying the PRCAP module, the causal factor of "System mis-alignment was not corrected" is determined as:

Module:	6.	FIRST LINE SUPERVISION
Branch:	B.	Supervision LTA during Work
Causal Factor:	7.	Failure of observation.

The fact that system mis-alignment was not corrected reflected two underlying causes associated with the event. An apparent cause usually reflects symptoms of a deviation, defect or failure. While, an underlying cause reflects the defense that should have existed against the deviation, defect or failure. When the underlying causes are identified, the RCA is performed a step deeper in the plant technological systems and a level higher level in the plant organizational structure.

2.7 STEP 7 – DETERMINATION OF THE ROOT CAUSE OF THE EVENT -

Purpose: Analyzing a direct cause, contributing causes and a root cause of the event.

Tools:
- PRCAP modules (§ 7)
- Criteria for identification (§ 8)

When all the causal factors of the real problems of the event have been identified and allocated in proper places of the PRCAP modules, the RCA process should be forwarded to determine the direct cause, contributing cases and root cause in accordance with their definitions presented in Chapter 1.

Even in what at first sight appears to be a very simple linear chain, there could be a hidden complexity. Careful analysis often reveals a very complex structure of interactions between causes. Many occurrences are just symptoms of one or several

underlying latent weaknesses. Moreover, a careful analysis of specific events often reveals general latent weakness in the organizational system, even if these may not be directly related to the observed event.

The root cause is the stopping point in the assessment of causal factors. It is the fundamental aspect of the event, which can be logically identified. If the root cause is corrected, the real problem will be eliminated and will not occur again. The root cause may not only apply to this event or occurrence, but has generic implications to a broad group of possible occurrences, and if it is corrected, all of those occurrences will be prevented.

2.7.1 Step 7.1 - Distinguishing Causal Factors Excluded from Corrective Actions

Causal factor "Valves A & B arrangement reversed in Units 1 & 2" might or might not contribute to the event although it is coded as "**4 A 10**", since the new operator had not performed the task before. Nevertheless, it is neither regarded as the direct cause or contributing cause, nor as the root cause, since this reversed arrangement between Units 1 & 2 may be considered as normal or expected, it is not correctable.

2.7.2 Step 7.2 - Determining the Direct Cause and Contributing Causes

The analysis performed and the conclusions with regard to the direct cause and contributing causes are schematically presented on the E&CF chart in Figure 2.4. The analysis is explained as below:

Direct Cause:

- Causal factor "Valve SS-3412-A left open", coded as "**1 B 4**", is the direct cause of the event, which immediately resulted the trip of the reactor and, of course, the termination of the shutdown system testing.

Contributing Causes:

- Causal factor "No labels on Valves A & B", coded as "**4 A 1**", was determined as a contributing cause, since it by itself would not have caused the event, and it was not regarded as the fundamental aspect or reason of this event.

- Causal factor "Operator had not performed the task before", coded as "**5 A 1**", was not inevitable to result in the event and is assumed as a contributing cause. This was not the root cause either because the operator is "qualified" in view of the management of the organization.

- Factor "System mis-alignment was not corrected" is assumed to be the failures of the human engineering and the supervision and coded as "**4 C 3**" and "**6 B 7**". The inadequate human engineering and supervision are

determined also as contributing causes to the event, since they are not inevitable to resulting in the event, and also not root causes since more fundamental factors may exist as described in the following analyses.

2.7.3 Step 7.3 - Determining the Root Cause

The plant management systems include several levels of management. The four contributing factors suggest that deficiencies existed in the management systems of the line organization. The deficiencies went beyond a single shift crew; within which the shift supervisor did not verify the work of an operator who had not performed the task before. Other deficiencies were not the sole responsibilities of the shift supervisor. Further investigation has identified:

- Most operators and some supervisors in the operating organization knew that no label was on the valves.

- The decision was made by a responsible line manager that the shutdown system testing should not be included in the training program for operators.

- The fact that the current technological system was not capable of detecting such an error should be expected and administrative controls should have been established for compensations and countermeasures.

Then, the RCA team members further ask questions with regard to some unsatisfied answers and discuss problems with knowledgeable and experienced staff and experts for searching the root cause. The questions may be such as:

- Why did the shift supervisor not verify the work the fist time performed by a new operator?
- Why was the deficiency of no label on the valves noticed for a certain time, but not corrected?
- Why the responsible line manager decided that the shutdown system testing was not included in the training program for operators?

New facts were identified that the shift supervisor is generally aware of his duties but the safety significance of the task of the operator was not adequately assessed. Besides, the responsibility of the operator in performing the shutdown system testing was not adequately defined. Finally, the deficiencies of the line management were identified which are regarded as another underlying cause of the reactor trip event, i.e. management failure in safety review of the operator's task in performance of the shutdown system testing. The RCA is thus further pursued to a level higher in the plant organizational structure.

This underlying cause is recognized as the fundamental reason of the reactor trip. By applying the column of "Management" (M.5) of the PORTM system, a latent weakness in the" Management Systems" of the line organization should be determined that

contributed to the event. Applying the PRCAP module, the deficiencies of "Safety requirements not identified" by the operating line organization would be agreed as the root cause, i.e.

Root Cause:

- Causal factor "**Management failure in safety review of tasks**", which is coded as "**7 B 3**" in the PRCAP cause modules:

  Module: 7. MANAGEMENT SYSTEMS
  Branch: B. Programmatic Deficiencies
  Causal Factor: 3. Safety requirements not identified.

Should the deficiency that safety requirements had not been identified have been eliminated, the event would not have happened. In that case,

- The line manger should have recognized the responsibilities of the operators in the performance of the shutdown system testing and, therefore, the shutdown system testing should have been included in the training program for the operators.

- The shift supervisor should have recognized the importance and safety consequences of the shutdown system testing and, therefore, he or his designator should have verified the work the first time performed by the new operator.

The termination of the RCA at this organizational level is deemed appropriate, since no other evidence could be found at the same management level in other organizational units that have contributed to the event. Therefore, no other reasons could be used to pursue the investigation and analysis to the more senior management levels than the operating line organization.

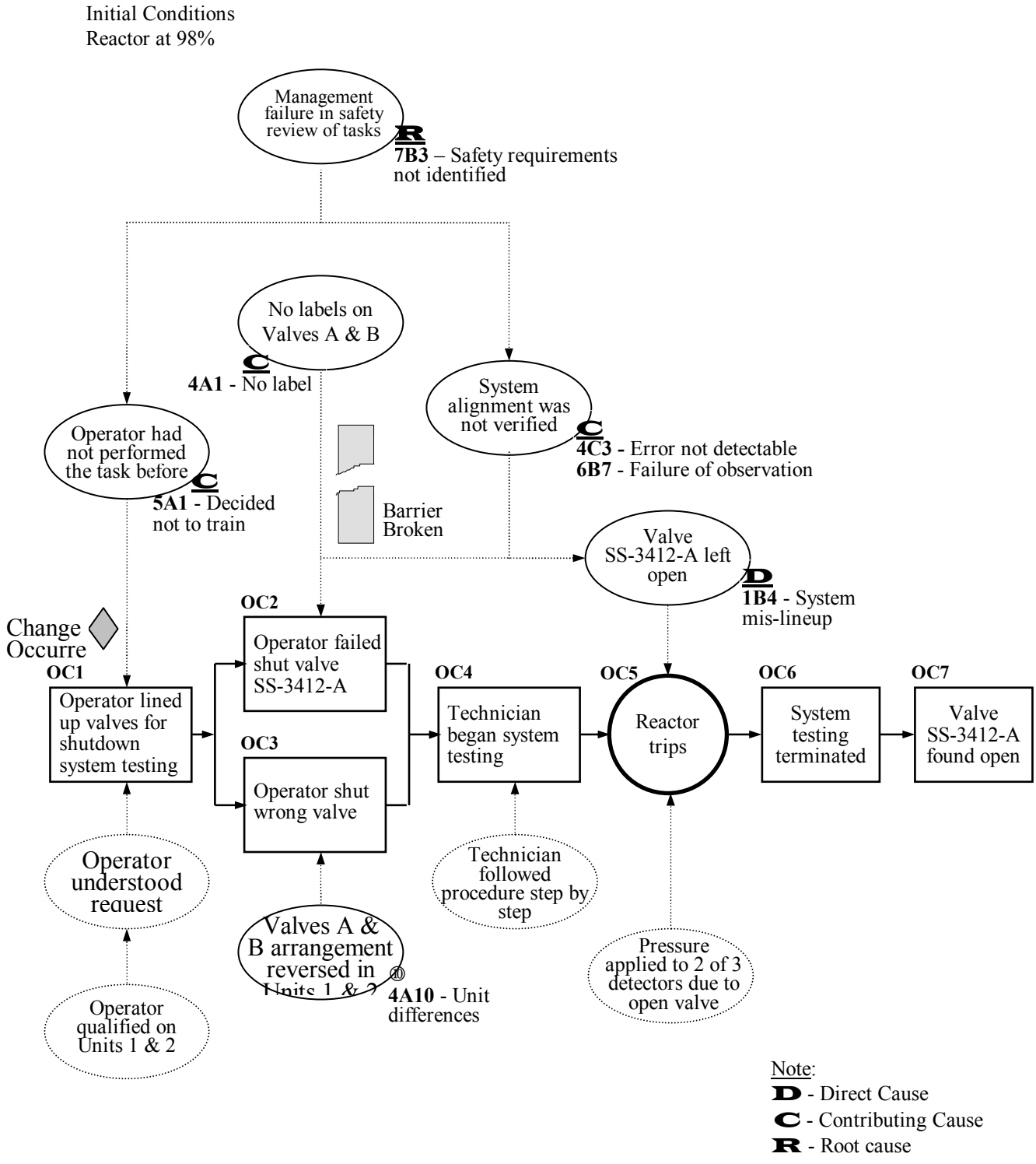


FIGURE 2.4: *An E&CF Chart with an Identified Root Cause*

2.8 STEP 8 - PRIORITIZATION OF CORRECTIVE ACTIONS BASED ON RCA

Purpose: Ensuring corrective actions addressing the root cause & cost-effectiveness.

Tools: - Criteria of prioritization (§ 9)

The goal of the RCA is aimed at prevention of events, not fault finding. Effective planning and implementation of the corrective actions is the successive step of the RCA. The concept of the total quality management (TQM) is: "Events should be viewed as opportunities to improve Management Systems rather than as opportunities to assign blame."

When a problem occurs, it is important to identify and correct the direct cause. In many cases, correction of the direct cause may immediately provide inexpensive solutions and short-term benefits. However, the same or similar problem may later occur again because the failures or inadequacies in the management processes and in the organizations were omitted and excluded.

The root cause is the one most responsible for the event, or the one because of which the event was inevitable. Correction of the root causes has proven to be the most cost-effective investment in the solution of the E&HP related problems to ensure the long-term safety and reliability in an operating NPP. However, implementation of corrective actions may involve additional considerations such as change of the plant production programs and schedules, re-allocation of the limited budget and human resources. Because of the near-term importance or the earliest convenience, correction of some causal factors may be planned ahead of the correction of the root cause.

As an example, the direct cause of the 'System mis-alignment' will, without question, be corrected before the reactor is restarted. However, correcting the mis-alignment cannot provide a guarantee that the system testing will be successful the next time. The contributing cause 'No label' will be easily corrected, as it has been identified and easily corrected.

The correction of the root cause should start with a serious study of the safety significance of the task. Based on the study the root cause will be corrected, i.e. the safety requirements in performance of the shutdown system testing will be identified. Therefore, the another two contributing causes will be subsequently corrected, i.e. appropriate provisions for supervision of the task performance are to be established and the training program for the operators upgraded. Accordingly, all operators are to be trained in conformance to the new training requirements and the activities of the line-up of the valves verified.

2.9 STEP 9 - PREPARATION OF AN EVENT RCA REPORT

Purpose: Ensuring satisfactory presentation to convince the management and public.

Tools:
- E&CF charting (§ 5.3)
- Guidance for RCA report (§ 9)

The purpose of the RCA report is to convey in clear and concise language the analytical process and results with regard to the determination of the root cause. The RCA should be pursued up to a proper organizational level. The format and contents of the RCA report should be in conformance with the quality assurance requirements. The following may be appropriate to be included in the RCA report:

- Review of the initial plant status,
- Description of the event and consequences,
- Illustration of the chronological sequence of occurrences,
- Description of relevant technical systems and management systems
- Indication of type of failures or unexpected performance,
- Analysis of the direct cause and contributing causes,
- Analysis of the root cause,
- Determination of the corrective actions,
- Conclusions on prevention of recurrence and lessons learnt.

The analysis results should be displayed with the help of the four RCA techniques. Among them, the E&CF chart is the most effective tool in that it graphically displays the sequence of occurrences and the relationship of the occurrences with all factors, barriers and presumptions. The E&CF charting technique helps to ensure objectivity and is easy to communicate with those not very familiar with the RCA techniques and methods. In addition, concise and complete narration is also necessary for addressing the objectivity of the analysis and the logic conclusions on the identified direct cause, contributing causes and the root cause.

The report should convey the extent and depth of the analysis and demonstrate its consistency with existing regulatory and management policies and objectives. The report should convince the plant management and the public that the root cause identified is reasonable and correctable. Suggestions for prioritization of corrective actions should be included in the report with consideration of other factors such as budget, resources, production schedules, organizational units involved and impacted etc.

3. CRITERIA FOR SELECTION OF EVENTS AND RCA TEAM FORMATION

Comprehensive root cause analysis could be time-consuming. The effective implementation of PRCAP precludes the need for analyzing all events. Whenever an operational event occurs, however, the selection criteria should be applied in order to determine whether it is a significant event to be subjected to the comprehensive RCA. In reviewing the newly reported event, the historical operational events may also need to be screened in order to identify whether there are repetitive occurrences or failures so as it also worthwhile to be subjected to the comprehensive RCA process.

Maximization of the effectiveness of the formal RCA should be pursued in view of the possible resource constraints (e.g., budget, manpower and production needs). Therefore, criteria should be established for selection of events and for establishment of an expert team qualified and experienced to ensure the effectiveness of RCA in accordance with PRCAP.

3.1 CRITERIA FOR SELECTION OF EVENTS

For the cost-effective utilization of the resources, the plant management should establish criteria for selection of events to perform the RCA. The criteria should include nuclear safety and other considerations.

3.1.1 Safety Related Criteria

Events falling in the following categories should be selected for root cause analyses, such as:

- Severe or unusual plant transits,
- Major damage to equipment important to safety,
- Common mode failures of safety related equipment,
- Malfunctions or improper operation of safety systems,
- Excessive radiation exposure or severe personnel injury,
- Unexpected or uncontrolled release of radioactive material,
- Fuel handling or storage events with implications for nuclear safety,
- Deficiencies discovered which could have lead to any of the above events.

3.1.2 Other Considerations

Events, which are significant to the plant reliability or which have been repeatedly occurred, should also be analyzed for their root causes, such as:

- Event causing significant unavailability of the plant,
- Events having not been considered in the design basis,
- Industrial safety events, which resulted in fatality, hospitalization or permanent disability,
- Minor events with similar deviations and frequently occurs (these types of events can often be precursors of more serious ones),
- Near misses (events that could have resulted in actual consequences if had not been occasionally corrected).

3.2 RCA TEAM FORMATION

3.2.1 Organizational Arrangements

With regard to the investigation/ analysis of the plant operational events, the following organizational arrangements usually can be observed:

- Routine activities, performed by an organizational unit for recording and reporting, and
- Specific activities, performed by an ad hoc or an expert team for in-depth analysis of the root cause of the selected events.

Adequate authority, responsibilities and organizational freedom should be given both to the unit in the plant feedback system for the routine activities and to the established ad hoc experts team for analyzing the significant and/or complicated events.

3.2.2 Organization of an Expert Team

Usually, an expert team should be established for the in-depth analysis of the selected event. The expert team may include individuals from different departments of the plant. Independence of the experts to be selected for performing RCA should be preserved as far as is possible. Hence, team members should not have been involved in the event to be analyzed to ensure that independent conclusions and recommendations are developed.

Periodically, outside experts may be invited to participate in the analytical process, jointly with the plant team or independently as the external peer, in order to justify and improve the standards of the RCA. In that case, the team leader should be given the sufficient authority to request the plant staff of support and co-operation during the investigation process and the direct channel to have access to the plant management.

3.2.3 Expertise Required

The team composition should ensure to cover a range of expertise, including detailed knowledge of

- Design of the plant systems,
- Relevant management policies, programs and instructions,
- Organizational structures including responsibilities,
- Plant operation and maintenance procedures,
- Event reporting criteria,
- Respective technical disciplines.

Besides, another most important aspect is that they fully understand the PRCAP methodology and have been trained accordingly. Preferably, they should also have some knowledge of other RCA methods.

The respective technical disciplines may include, for example:

- Plant operations,
- Mechanical engineering,
- Electrical engineering,
- Control and instrumentation,
- Chemical engineering,
- Radiation protection,
- Human/ organizational factors,
- Interview techniques.

The team leader should have the role of a coordinator/facilitator with wide experience in interview and analysis techniques.

4. INTERVIEW TECHNIQUES

The event report drafted shortly after the event aiming at informing management and authorities may not always contain all information necessary for a comprehensive RCA. Missing information should be obtained through interviews of plant staff, review of plant records, on-site visits of plant systems and equipment, etc.

In the context of RCA, 'interview' implies a cooperative informal meeting where the interviewer approaches the interviewee as an equal. The term witness is applied equally to all individuals possessing information relating to an event. Interviews can (and sometimes should) be an integral part of the fact-finding aspects of RCA. The interviews are concerned with witnesses present at or in the vicinity of the location of an event.

In most events, the people who are involved do not really observe all that happened. The occurrences during the pre-event phase tend to be of routine and seldom draw the undivided attention of the 'event participants.' Also, few people are trained to be observers; they do not really see what they are looking at and do not make a practice of recording detail of the little they actually do see.

In most events, the people involved do not know all that happened. Differing observations are made, depending on technical background, experience, personal values and physical point of observation. The effectiveness of the interviews is greatly influenced by the atmosphere and environment of the interviews. The following guidelines are helpful:

- Interviews must be fact finding and not fault finding;
- Interviews should be conducted in a blame free environment;
- The interviewer should always consider the interviewee's objectivity;
- Walk-through should be considered as part of the interview;

4.1 CONTROLLING DISTORTION OF STATEMENTS OF THE WITNESS

Factors affecting witness statements include:

- Emotion and excitement tend to produce distortion and exaggeration, especially in the verbal description of an occurrence or event. Accuracy depends partly on the observer's mental state at the time;

- Exaggeration tends to creep into the interview because some witnesses tend to temper their statements in the hope that their observations will be accepted by the interviewer;

- A common witness failing is 'transposition.' The witness reports all the facts, but places them out of sequence of the actual occurrences;

- Omissions are common in witness statements simply because the witness does not consider certain information important.

The experienced investigator should pick all those up and attempt to have these areas clarified when the witness prepares a written statement.

4.2 INFLUENCE OF PERSONALITY OF THE WITNESS

There is no foolproof method of ensuring valuable information from interviews. Interviewees (and interviewers) have personal traits that impact the quality of statements:

- Extrovert witness: Usually a convincing person with positive response, adamant about the observations, conclusions and suggestions. The evidence may not be as accurate as it appears, however;

- Introvert witness: Normally appears as a seemingly poor witness because of being unsure of facts and indecisive in responses. The interview may seem as a waste of time, but might produce the most valuable information;

- Suspicious witness: Person who is reluctant to get involved, guards the privacy and resents being questioned. May discourage the investigator before revealing any information;

- Prejudiced witness: Psychologically ill-suited for interview because of the belief that the supervisor, manager or co-worker, against which he is prejudiced, is always wrong.

4.3 INFLUENCE OF PERSONALITY OF THE INVESTIGATOR

Witnesses are greatly influenced by the personality and mannerisms of the investigator. Few people like to give statement/testimony even when sure of the facts. Mainly because of not knowing how the facts will be used. Many have had bad experiences with higher level managers and staff officials and distrust their motives behind investigations.

- The 'commanding' type investigator may frighten the witness into silence, induce the witness to forget detail or feel pressed to give some information when he real has no certain facts or knowledge;

- The over-confident investigator overestimates his personal ability to obtain information. Consequently, he accepts the first statements on any aspect as complete and factual;

- The over-eager investigator induces errors and contradictions in the investigation through asking excessive questions, and by offering multiple-choice answers;

- The timid investigator raises witness' doubts with superficial comments as whether provided information will serve any useful purpose;

- The prejudiced investigator may only note expected/anticipated comments, thus impacting the event investigation.

4.4 THE INTERVIEW PROCESS

Before beginning the interview process, the investigator should possess the 'big picture' of the event to place him on the same level as the witnesses. The interview process consists of:

- Selecting a place for the interview;

- Establishing communication to ensure that all relevant information is collected;

- Taking an initial statement by asking the witness to relate, in his own words what he knows about the event; what he said, what he heard, what he felt, what he did immediately after the event;

- Expanding the interview for details. After the witness appears to have exhausted his self-recall, the investigator should use predetermined questions to prompts further recall or expand initial information in depth;

- Closing the interview. Questioning the witness for suggestions on prevention of the event is a good method of closing the interview after other questioning is exhausted.

5. BASIC ROOT CAUSE ANALYSIS TECHNIQUES

RCA techniques are specifically developed for investigation and analysis of causal factors. There is no single, universal technique that fits all situations. There is no 'black-box' approach to RCA. To accomplish the investigation and analysis of the causal factors of a complicated event, it is necessary to use a combination of RCA techniques. The four basic RCA techniques are:

- Change Analysis,
- Barrier Analysis,
- Event and Causal Factors (E&CF) Chart,
- Tree Diagram.

No fixed rules exist for the selection of technique(s). Almost any of the techniques could work for any simple problem. The experience and knowledge of the investigator/analyst determines which technique should be used most profitably. Some guidance is to be given for reference at the end of this Chapter on how to establish the optimum approach to select the applicable techniques.

The techniques of Change Analysis and Barrier Analysis are mostly used in the establishment of questions during the investigation process. The technique of the E&CF Chart is most suitable for organization of the obtained information and for presentation of the analytical results. These techniques normally would be used iteratively until a relatively complete and satisfied E&CF chart and all necessary explanations are made. The Tree Diagram could be used to establish the logic sequence at the later stage in the analysis process.

5.1 CHANGE ANALYSIS

Change Analysis is based on the concept that for a problem to exist, or event to occur some changes to the normal situations must have occurred. Therefore, investigation of any changes that have taken place will give guide to determination of causes of problems and identification of remedies.

Change Analysis looks at a problem by analyzing the deviations between what is expected and what actually happened. The investigator/ analyst asks what differences occurred to make the outcome of this task or activity different from all the other times this task or activity was successfully completed.

The technique consists of asking questions: What? When? Where? Who? How? Answering these questions should provide direction toward answering the root cause determination question: Why?

There is not a rigid structure or detailed prescriptive process for Change Analysis. The questioner compares the present status (the unexpected real situation) with the prior status (when it was appropriate) to identify what has changed in the system between the time it worked and the time it failed. Later, analysis of these changes will determine whether and how they contributed to the event.

5.1.1 A Set of Investigation Questions

Change Analysis is a very useful and effective technique to be included in the set of tools for event investigation. It helps to focus collection of data during the early stage of the investigation process and helps to identify potential causes for further investigation. The following sample of questions help identify changes between what is expected and what actually happened:

WHAT ?

* Condition

  - What was the condition ?
  - What occurred to create the condition ?
  - What occurred prior to the condition ?
  - What occurred following the condition ?
  - What occurred changing the condition ?
  - What occurred terminating the condition ?

* Activity

  - What activity had been performed prior to the condition ?
  - What activity was in progress when the condition occurred ?
  - What activity was in progress when the condition was identified ?

- What associated activities had been performed outside the work place prior to the condition ?
- What associated activities were in progress outside the work place when the condition occurred ?
- What associated activities were in progress outside the work place when the condition was identified ?

* Equipment

- What equipment initiated the condition ?
- What equipment was affected by the condition ?
- What equipment mitigated the condition ?
- What are the equipment's functions ?
- How does the equipment work ?
- How is the equipment operated ?
- What failed first ?
- Did any thing else fail due to the first problem ?
- What preventive maintenance has been performed on the equipment ?
- What modifications have been made to the equipment ?

WHEN ?

- When did the condition occur ?
- What was the facility's status at the time of occurrence ?
- When was the condition identified ?
- What was the facility's status at the time of identification ?
- When was the condition worsened/ improved ?
- When was the condition recovered/ corrected ?
- When was the event reported/ analyzed ?

WHERE ?

- Where did the condition occur ?
- Where was the involved/affected equipment ?
- What about the work environment there ?
- Where were the physical locations of barriers, failed or missed ?
- Where the associated activities outside the work place were performed prior to the condition ?
- Where the associated activities outside the work place were performed when the condition occurred ?

WHO ?

* Operating Personnel

- Who were involved in the condition ?

- Who observed/ identified the condition ?
- Who worsened the condition ?
- Who missed the condition ?
- Who corrected the condition ?
- Who reported the condition ?
- What were the training/ qualifications of these personnel ?
- What were the attitudes of these personnel ?
- What were their activities at the time of involvement with the condition ?

* Supervisor

- Did the personnel involved have adequate instruction ?
- Did the personnel involved have adequate supervision ?
- Were the personnel involved coordinated well ?
- Did the personnel involved cooperate well ?
- Did the work team have adequate level of experience ?

HOW ?

* Procedure

- Was there an applicable procedure ?
- Was the procedure available at work place ?
- Was the correct procedure used ?
- Was the procedure followed ?
- Was the procedure adequate to do the task ?
- Was the procedure an approved and current version ?
- Was the procedure compliance with applicable regulations and standards ?
- Was the procedure legible and understandable ?
- Was the procedure confusing or misleading ?
- Did the procedure cover all involved systems ?
- Did the procedure have sufficient detail ?
- Did the procedure have steps in the proper sequence ?
- Did the procedure require adequate work review ?

* Practice

- Was the schedule realistic, approved and communicated to every body associated with the work ?
- Was the work load on the personnel adequate and not causing undue overtime ?
- Whether the task was performed in a hurry or in an adverse environment ?
- Whether the personnel followed procedures in sequence or “blindly” without thought ?

- Were adequate measures available for administrative controls, verifications and supervisions ?

Some of these questions may not be applicable to any given situations. Some amount of redundancy exists in these questions to ensure that all items are addressed. It is necessary that redundant/ additional questions were provided to continue the questioning process toward answering the root cause determination question: Why ?

5.1.2 A Structured Analytical Approach

Change Analysis is typically composed of six steps, which are schematically presented in Figure 5.1. The six steps are:

(1) Considering the situation during an occurrence,
(2) Considering the desirable/ expected situation prior to the occurrence,
(3) Comparing these two situations,
(4) Identifying all differences/ changes,
(5) Analyzing those differences which affected on the occurrence,
(6) Integrating obtained information into the RCA process.

Initially, the findings obtained during the investigation process do not come out in logical or subject order. Notes of interviews and documents reviews should be summarized and reorganized at first to identify Items (1) and (2).

FIGURE 5.1: ***A Structure for Change Analysis***.

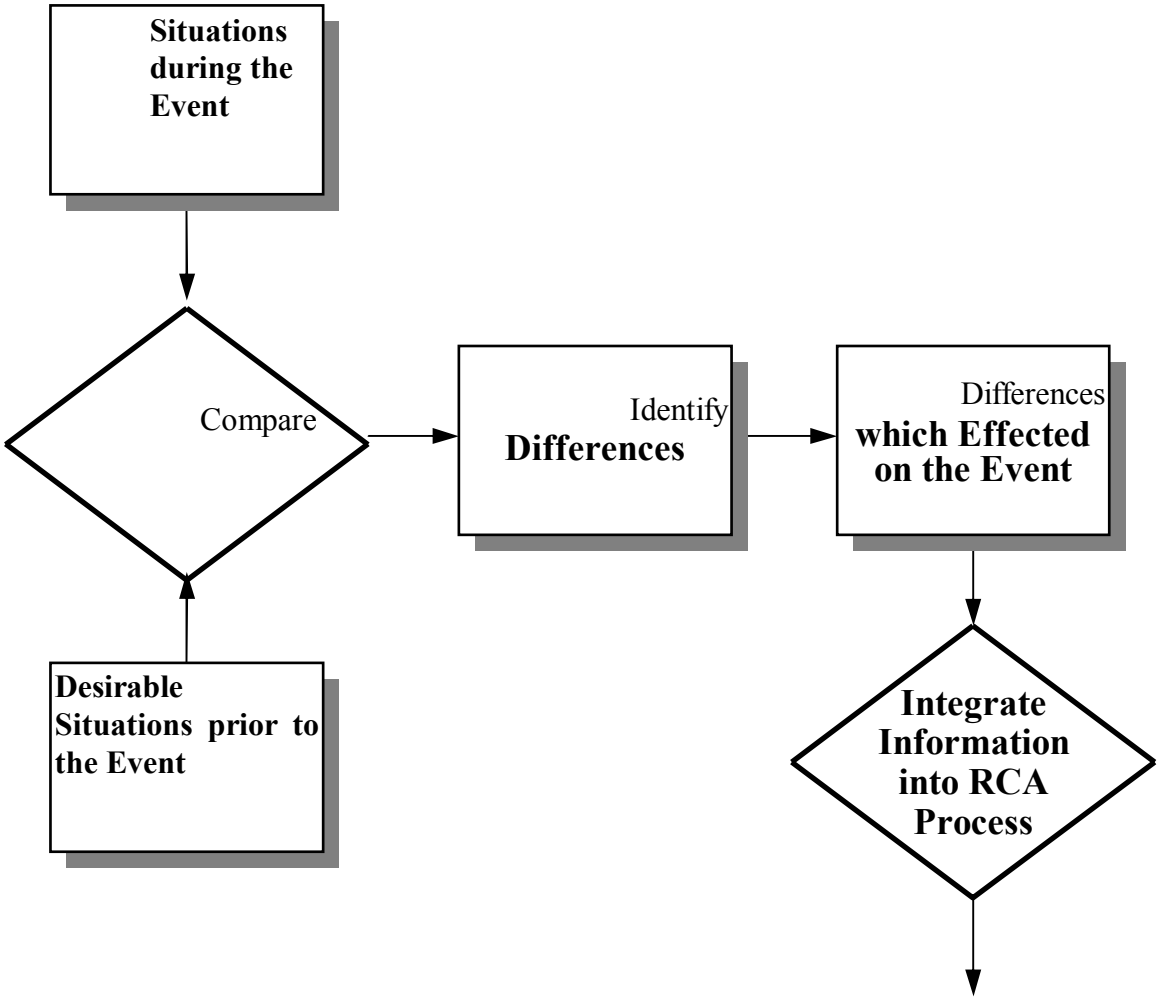


Figure 5.2 provides a basic format for change analysis. There are four blank columns in this format representing contents of Items (1), (2), (4) and (5) on the schematic, respectively. This format is intended to provide general guidance and suggestions in exploring potential affective changes that might be contributing to an event. This format is used as a draft worksheet and should be appropriately modified to fit the subject event.

FIGURE 5.2: *Change-Based Event Analysis Worksheet*

Factors	Situations during the Event	Situations prior to the Event	Differences	Differences Affecting on the Event
What Object(s) Energy Defects Protective devices				
Where On the object In the process Place				
When In time In process				
Who Operator Fellow worker Supervisor Others				
Task Goal Procedure Quality				
Working Conditions Environmental Overtime Schedule Delays				
Trigger Event				
Management Controls Control chain Hazard analysis Monitoring Risk review				

When causes are not easily identified, the visibility given by the matrix with regard to known information would allow the investigators/analysts to exercise their knowledge

and expertise in identifying causal factors. If possible, experimental verification of causes is recommended.

Change Analysis is a good technique to use whenever the causes of the event are obscure, the start of the investigation seems difficult, or a quick answer is needed. The more remote or ambiguous the causes, the more likely that the matrix in the change analysis worksheet will provide some clues. This technique focuses on elements that have changed and is more appropriate for evaluation of failures of the three basic elements (equipment, personnel and procedures). Change Analysis is more suited for dealing with simpler situations. In complicated situations, it is important not to overlook gradual changes or the results of a composition of changes.

Change Analysis has particular value as a preventive technique; that is, by being aware of changes contributing to the event, management may implement preventive measures in a planned and systematic manner. In the prevention context, potential changes provide an opportunity for corrective actions before the exponential growth of the changes.

5.2 BARRIER ANALYSIS

Barrier Analysis is seeking to identify physical or administrative barrier functions that should have prevented or eliminated the occurrences of an event. Barrier Analysis provides structured guidance for the investigator/ analyst to examine basic ingredients of the event development. Barrier Analysis can be used independently or used together with E&CF Chart to identify possible causal factors. Barrier Analysis requires familiarity with the concept of defense-in-depth concept. However, the term of barriers used here in not the same as defined in the IAEA publication of INSAG-3.

5.2.1 Characteristics of Barrier Functions

Barriers protect facilities and people from unexpected and undesirable energy flows, actions, conditions or situations. Barriers can be physical (e.g., pressure vessel, containment, protective clothes, etc.) or administrative (e.g. procedure, instructions, verifications, supervisions, etc.) in form. Barriers are implemented to ensure desired or expected performance of equipment and personnel. A single barrier is rarely relied upon.

In this document, neither physical nor administrative barriers will be sub-categorized in detail. Most causal factors in the PRCAP modules might be also considered as LTA of barriers. Basic characteristics of Barriers are as follows:

- Types
  - Physical barriers
  - Administrative barriers
- Functions
  - Prevention of unwanted energy flows
  - Confinement of radioactive material
  - Protection against hazards
- Locations
  - Between source and target
  - Surrounding target
  - Separation through time and space

In the investigation of factors or identification of causal factors, three types of problems of barriers are normally considered:

- Barriers not provided or not used
- Barriers failed
- Barriers non-existent because being impractical.

5.2.2 A Set of Investigation Questions

During the investigation process, the investigator/ analyst should be guided by a series of questions formulated to help determine what barriers failed and resulted in the event. Knowing which physical barrier failed or was missing still may not explain the causes of the event. It is important to keep asking questions, such as why a critical physical barrier was left out or failed, why the technological system or the management systems did not prevent the failure or was not aware of the failure before it occurred. It is essential to determine what is needed to prevent recurrence of an event. A sample of questions are listed as below:

- What barriers existed between the successive occurrences or problems?
- If there were barriers, did they perform their functions? Why?
- Were any barriers not functioning as designed? Why?
- Was the barrier design adequate? Why?
- Were the barrier adequately maintained?
- Were the barriers inspected prior to the expected use?

- Could the affected item withstand the condition without the barriers? Why?
- What kind of other controls could be the barriers subject to?
- Was the necessity of the presence of the barrier foreseen by anyone?
- Is it practical to have further steps to reduce the consequences of the barrier broken?

- Were adequate human factors considered in the design of the facilities?
- What additional administrative controls should be added?
- Did the environment mitigate or increase the severity of the occurrence? Why?
- Was there sufficient information regarding the status of operation or maintenance of the barriers?

5.2.3 A Simple Form for Performing Barrier Analysis

Barrier Analysis usually involves using a form such as the one in Figure 5.3. This form may be modified to suit a particular application, but the sample form has shown work well in most cases. The final step in Barrier Analysis is to identify and examine the precursors associated with the event. That is "What occurrences, energy flows, and barrier failures preceded the specific ones under assessment, which were necessary for the event to occur? Barriers should be indicated on the E&CF Chart.

FIGURE 5.3: ***An Example of Barrier Analysis Worksheet.***

Loss/ Consequence	Target	Hazard	Barrier	Analysis	Probable Cause

5.2.4 Analysis of Barriers With the 'AEB Technique'

The Accident Evolution and Barrier (AEB) technique was developed at Stockholm University through of the Swedish Nuclear Power Inspectorate (SKI). In the AEB technique, an event is thought of as a sequence of interactions between the human system and the technical system. In each sequence there are barriers which can arrest the sequence and prevent the unwanted development of an event. The AEB technique does not give an account of all occurrences in the event, only errors or failures that are necessary for an event evolution are represented in the sequence of occurrences to be analyzed. The AEB technique consists of two main steps in application:

1) Modeling the systems interactions in a flow chart.
2) Analysis of the functions of the barriers.

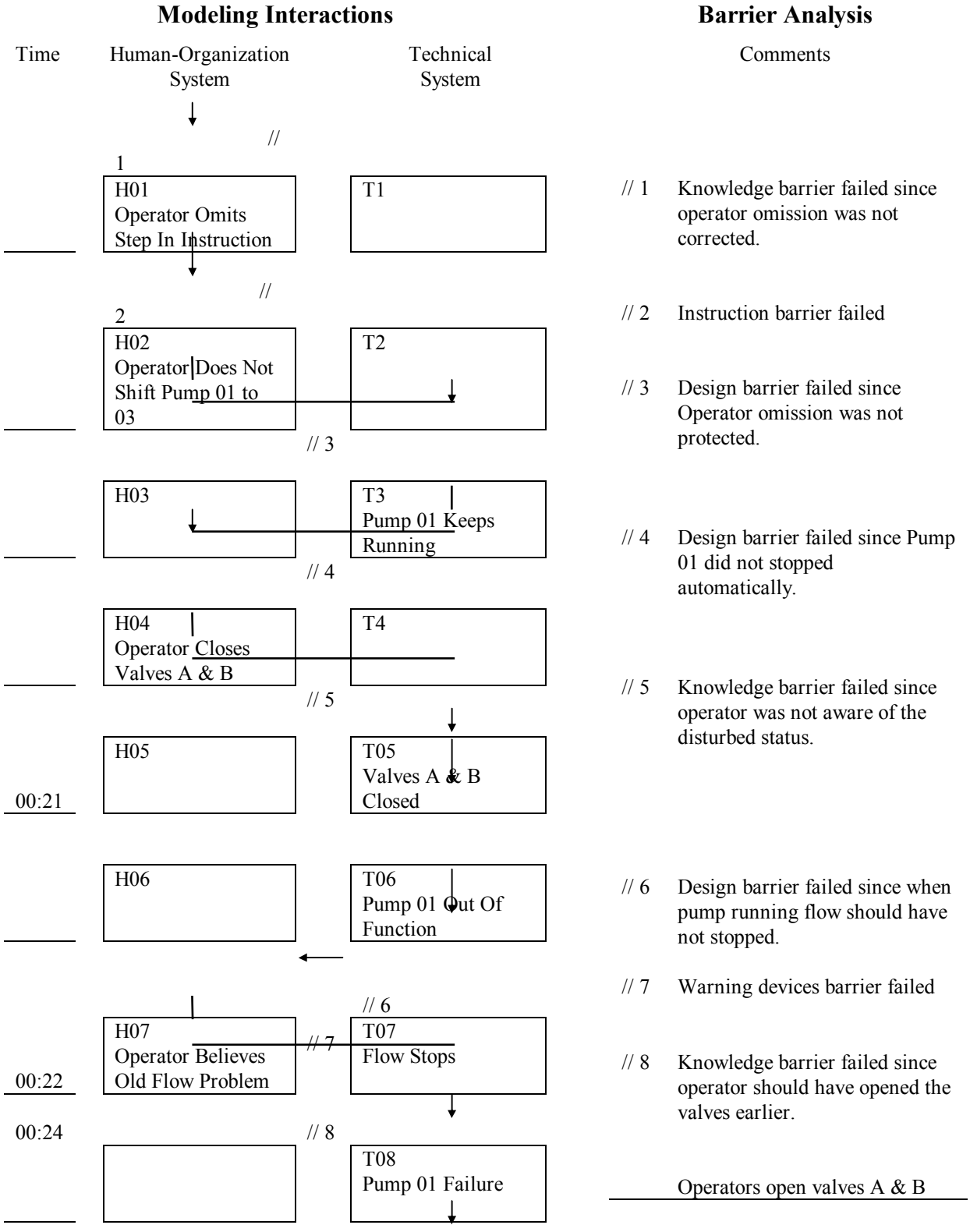
A flow chart is developed using pre-printed forms with two columns of empty rectangular boxes; the human-organization systems appear in the left column and the technical system in the right column. The investigator/analyst fills in the empty rectangles with applicable text describing the errors or failures. Next, the text-boxes are connected through links and arrows denoting the progression or the evolution towards an event in a sequence related to the time dimension. Each link between two successive failures is analyzed with regard to the failing or missing of the barrier functions. The AEB flow chart uses three symbols:

- Rectangles denoting human performance problems, system reactions or failures necessary for the event evolution.
- Arrows describing the development of the event in an approximate chronological order.
- Double slashes (//) indicating barrier functions which can stop the event evolution or which have been inefficient in doing so.

The purpose of the AEB analysis is to identify broken and non-existing barrier functions and to find, construct and improve barrier systems that could be used in arresting future event evolution. The AEB model has the following implications:

- The event consists of a sequence of human-organizational and technical errors or malfunctions, which can be arrested by barrier functions.
- The barrier functions that can arrest the event evolution may be performed by either the human-organizational or by technical systems.

FIGURE 5.4: *An Example of AEB Application.*



5.3 EVENT AND CAUSAL FACTORS (E&CF) CHART

The E&CF chart is designed to depict the occurrences and their conditions in a simple diagrammatic form. The E&CF chart documents the sequence of occurrences that happened in a process from the beginning to the end of the event, and indicates all contributing factors (conditions, changes, broken barriers and etc.). Use of the E&CF chart facilitates understanding the event evolution and identifying all concerns (problems or failures). The E&CF charting technique is based on incident theories that support:

- Event is rarely occasional,
- Event is the result of evolution of a number of occurrences,
- These occurrences can be arranged in a sequence or a few sequences,
- Each occurrence has its conditions or is subject to certain changes or failures,
- Event can be usually attributed to multiple causes,
- Root cause is the fundament cause of them.

The E&CF chart visualizes the cause-and-effect relationships among occurrences and conditions. Therefore, it is also very effective in communicating the findings and conclusions to the managers and other audiences.

5.3.1 Steps in Drafting the Initial E&CF Chart

Step 1: The first step in the E&CF charting is to list all occurrences having identified of the event in a chronological order. These occurrences can be classified as:

- Occurrences prior to the event,
- The event itself,
- Occurrences after the event.

Each occurrence should be listed with one subject and one verb. The descriptions of occurrences would be active rather then passive statements and have to be kept relatively short.

Step 2: The second step is to select the sequential length of the chart, i.e. to determine the starting and the end points for the next RCA. For example, whether the E&CF chart should be ended at the event, or the remedy and emergency actions thereafter should be included.

Step 3: The third step is to select those occurrences pertinent to the concerns of the event. The selected occurrences are then connected into a sequence or a few sequences on a paper to form the skeleton of the initial E&CF chart. Occurrences should be enclosed in rectangles with the same descriptions as in the list. It is worthwhile to reduce the list to include only the most relevant

information. Figure 5.5 provides a table used to categorize the occurrences in terms of the pertinence to the event.

FIGURE 5.5: *Categorization of Occurrences*

OCCURRENCES		Pertinent to Problems of Event		
		Yes	Not Sure	No
Time	Prior to Event			
	Event			
	Post Event			

Step 4: The fourth step is to define the scope and detail of the analysis in consideration of the available resources, including ability to interview of personnel, review of documents, recruit of experts from on-site as well as from off-site. The appropriateness of the scope and detail should be finally determined by the possibility of the achievement of the corrective actions established according to the RCA. For any event, the investigator/ analyst should determine the scope and detail according to plant policies and practices on a case-by-case basis.

Step 5: The fifth step is to identify the conditions related to each occurrence according to the available results. Conditions should be enclosed in ovals. The descriptions of conditions would be passive rather than active, whenever possible.

Sometimes, a single condition may influence more than one occurrence, as well as another condition. In this case a line should be drawn to connect the single condition to all infected occurrences and other conditions by it. The occurrences also must not lie in a single chain (sequence), but may involve confluent and branching chains. In fact, the investigator/ analyst has the choice of expressing the event development as a group of confluent chains which merge at a key occurrence, or as a primary chain of sequential occurrences into which all conditions feed to, or as a combination of the two.

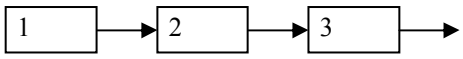
Step 6: The sixth step is to complement and augment the initial E&CF chart through further investigations. During the investigation process supplemented occurrences may be identified. Then the investigator/ analyst should ask questions for each of the occurrences "Why did the occurrence happen ?", followed each answer keep asking "Why did it (newly identified condition) happen ?" until you arrive at the most basic explanation.

5.3.2 Format Criteria of the E&CF Chart

Standardized symbols should be used when constructing E&CF charts. The following symbols are recommended:

(1) Occurrences should be enclosed in rectangles , and conditions in ovals ;

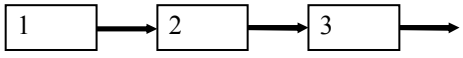
(2) Occurrences should be arranged chronologically from left to right and connected by solid arrows;



(3) Conditions should be connected to each other and to occurrences by dashed arrows;

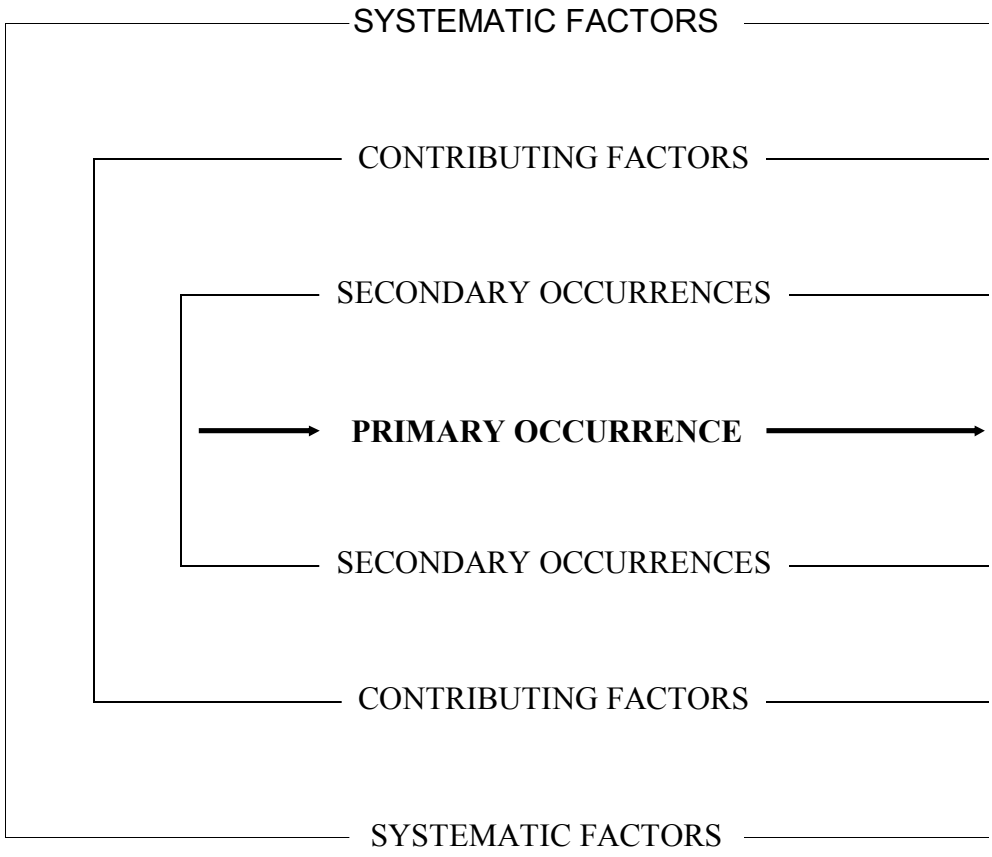
(4) Each occurrence and condition should either be based on valid factual evidence or clearly indicated as presumptive by dashed line rectangles and ovals;

(5) The primary sequence of occurrences should be depicted in the middle of the chart and occurrences should be jointed by bold arrows;



(6) Secondary event sequences, contributing factors and other factors should be depicted on horizontal lines at different levels above or below the primary sequence as indicated in Figure 5.6.

FIGURE 5.6: ***Occurrences and Causal Factors Relations.***



5.3.3 Criteria for Description of Occurrences

The following five criteria should be considered when describing the individual occurrences:

(1) An occurrence is a single and discrete happening, not a relative stable condition or circumstance. It should not be by a statement of an issue or a conclusion. An occurrence should be described e.g. “Pipe wall ruptured”, not “The pipe wall had a crack in it”.

(2) Each occurrence should be described by a short sentence with only one subject and one verb e.g. “Mechanic checked front-end alignment”, not “Mechanic checked front-end alignment and adjusted camber on both front wheels”.

(3) Each occurrence should be precisely described e.g. “Operator pulled headlight switch to on-position”, not “Operator turned light on”.

(4) Each occurrence should be quantified where possible e.g. “Plane descended 350 meters”, not “Plane lost altitude”.

(5) Each occurrence should be derived directly from the occurrence or conditions preceding it. When this is not the case, it usually indicates that one or more steps in the sequence have been left out.

5.3.4 Practical Experience

The E&CF Charting technique provides a systematic approach to collection and organization of available data and information. The construction of the E&CF chart should be started as soon as factual information is more or less sufficient to image the event development. Initially, there will be many holes, inconsistencies and deficiencies. The initial E&CF chart will help the investigator/ analyst to plan further investigations. In proceeding of next steps, efforts should be made to fill these holes and get accurate tracking of the logical interactions among the occurrences and conditions that resulting in or contributing to the event.

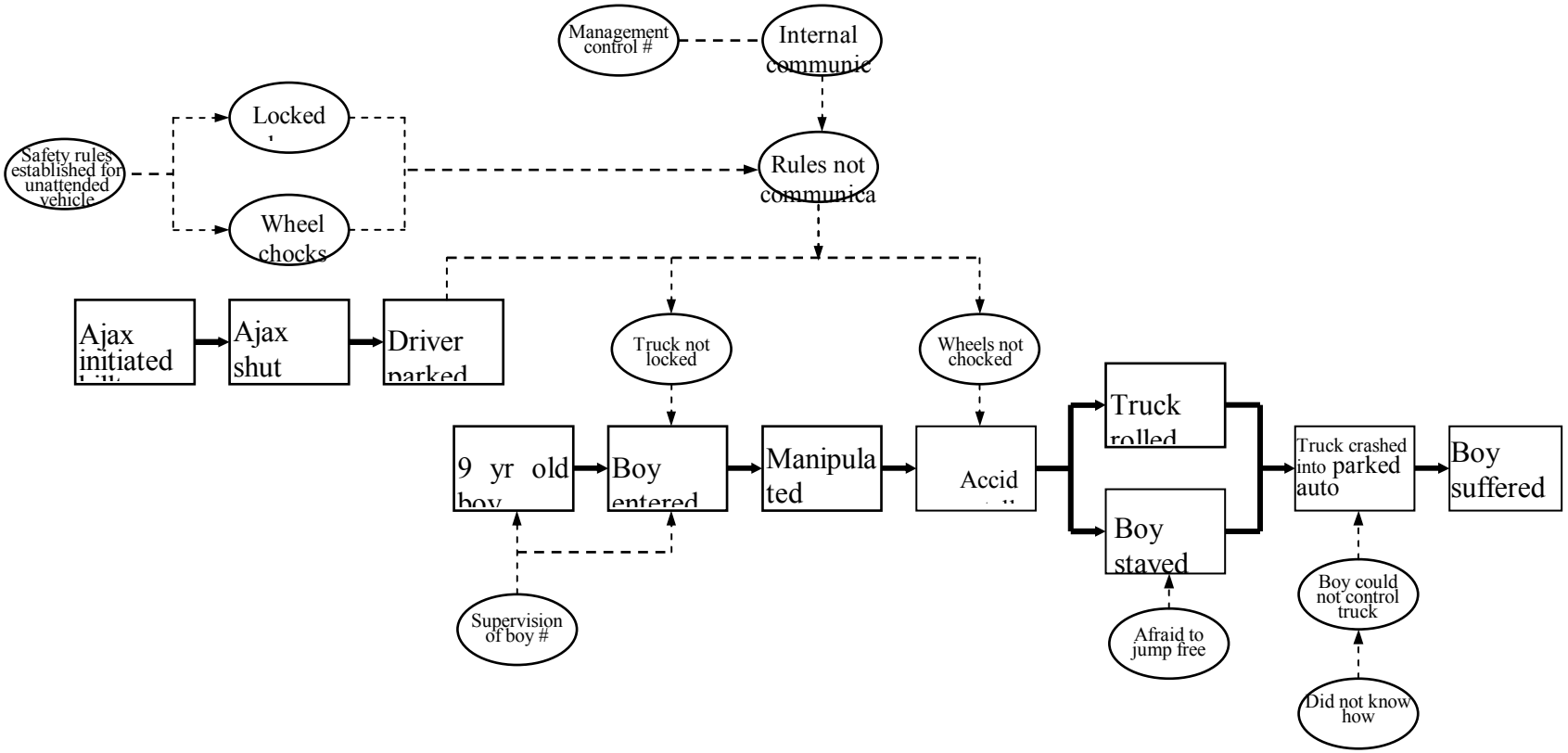
The initial E&CF chart as a working chart will be augmented and upgraded several times during the investigation/ analysis process by recording more detailed information through correlating with the use of Change Analysis, Barrier Analysis and Tree Diagram, and by performing logical deduction and induction. Two examples of the typical E&CF Chart is given in Figures 5.7 and 5.8.

In summary, the following reminder with seven points may help the practical application of the E&CF charting technique:

(1) Beginning early based on available information,
(2) Including appropriate sequence length and level of detail,
(3) Using the recommended format and description criteria,
(4) Correlating properly with other RCA techniques,
(5) Performing consistently logical deduction and induction,
(6) Updating the work chart continuously based on new findings,
(7) Making a simple final chart with the summarized important information.

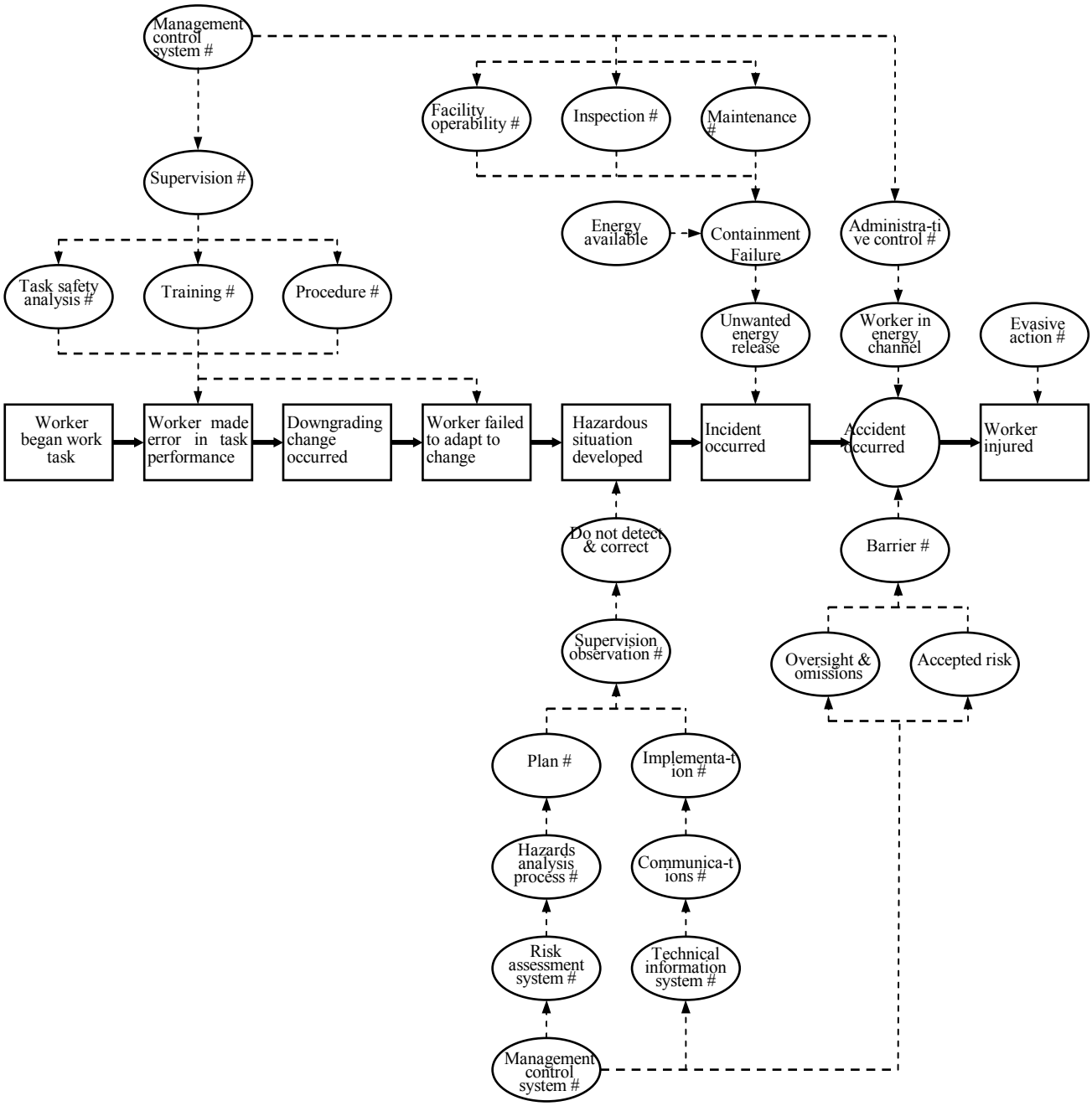
FIGURE 5.7: ***Example 1 of an E&CF Chart***.
(Attached Sheet)

FIGURE 5.7: *Example 1 of an E&CF Chart*



.

FIGURE 5.8: ***Example 2 of an E&CF Chart***



5.4 Tree Diagram

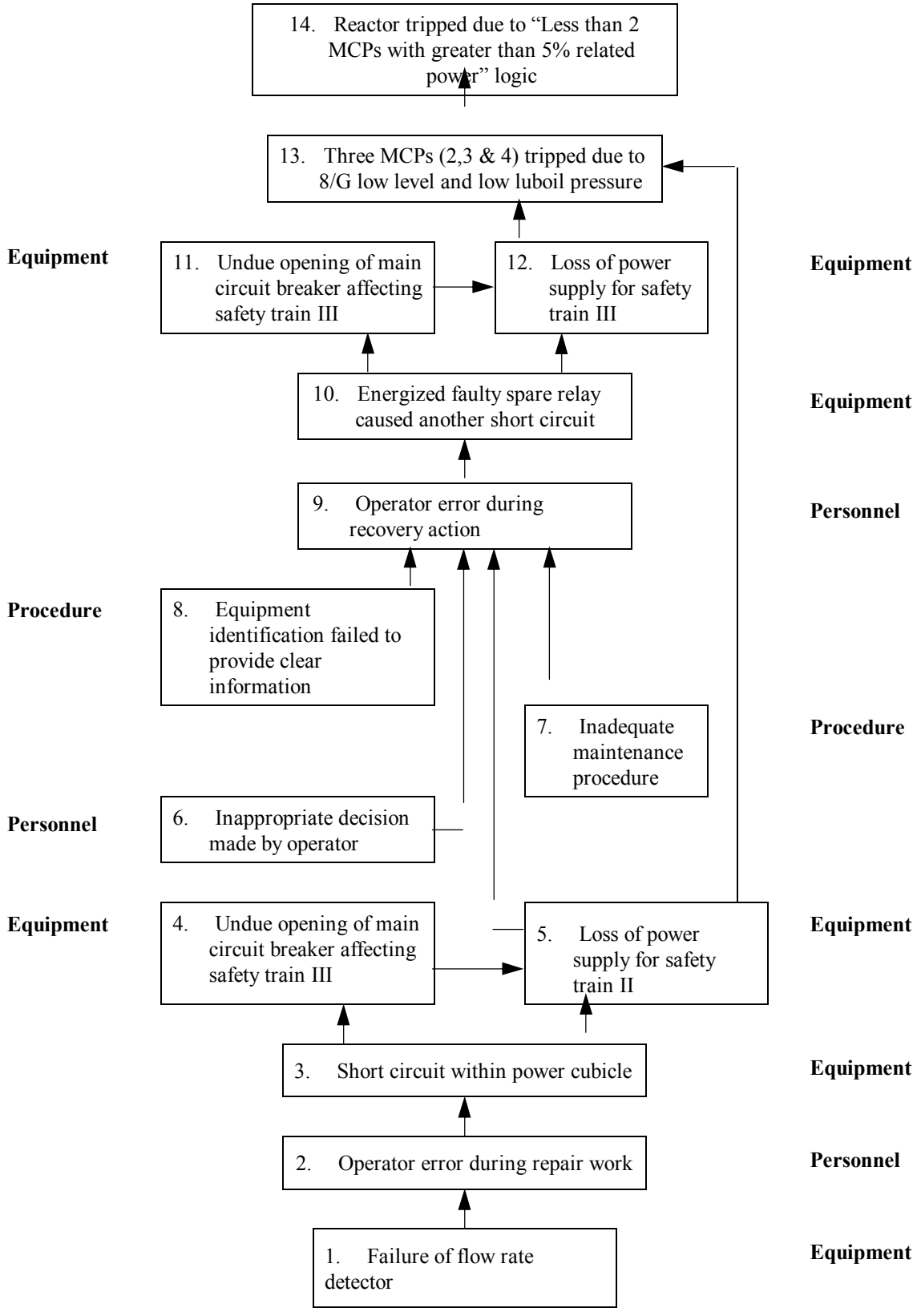
During an investigation/analysis process, an occurrence may not follow another resulting in an event. Many occurrences and conditions appear randomly or over a great time span and do not lend themselves to exact sequencing on a chart. Therefore, it is necessary to identify the independent occurrences and to arrange them in a logical progression, showing the logic relationships between them.

By 'independent' is meant that the occurrence is not a direct result of a preceding occurrence. For example, the occurrences 'operator fails to perform as expected because by following a procedure' and 'the procedure did not give the right guidance' are dependent. In a case of an operator failing to perform as expected after a leakage takes place, say, from a defect coupling, there are two independent occurrences.

The Tree Diagram is a graphical structure logically describing an event and the occurrences and their causal factors. The undesired event appears as the top occurrence and a tree structure of the occurrences is developed. The top occurrence is linked to the contributing factors (branches) by logic gates and statements.

A gate symbol can have one or more inputs, but only one output. There are only two basic logic gates: the AND-gate and the OR-gate. The AND-gate is the condition that is true or can occur only when all inputs are present. In RCA, the AND-gate is rarely applied. Therefore, in practice, the top occurrence is connected to the lower tiers by lines and statements. Figure 5.8 is a typical example of the application of the Tree Diagram technique, in which the failed elements are identified either as the equipment, personnel or the procedures.

FIGURE 5.9: *An Example of Tree Diagram*.



5.5 Selection of RCA Techniques

E&CF Charting is the most effective when used together with other RCA techniques that corroborate observations and findings. Critical changes marked on the E&CF chart might illustrate important causal factors. Broken barriers on the E&CF chart would facilitate the examination of assumptions about the event evolution and the identification of energy channels that cause the occurrence. Tree diagram could suggest two or more chains of occurrences should construct the E&CF chart.

In some cases, however, individual techniques might also be applied to analysis of the root cause of an event. The probable process for selection of the adequate RCA techniques is schematically showed in Figure 5.9.

FIGURE 5.10: *RCA TECHNIQUES SELECTION PROCESS (1 of 2)*

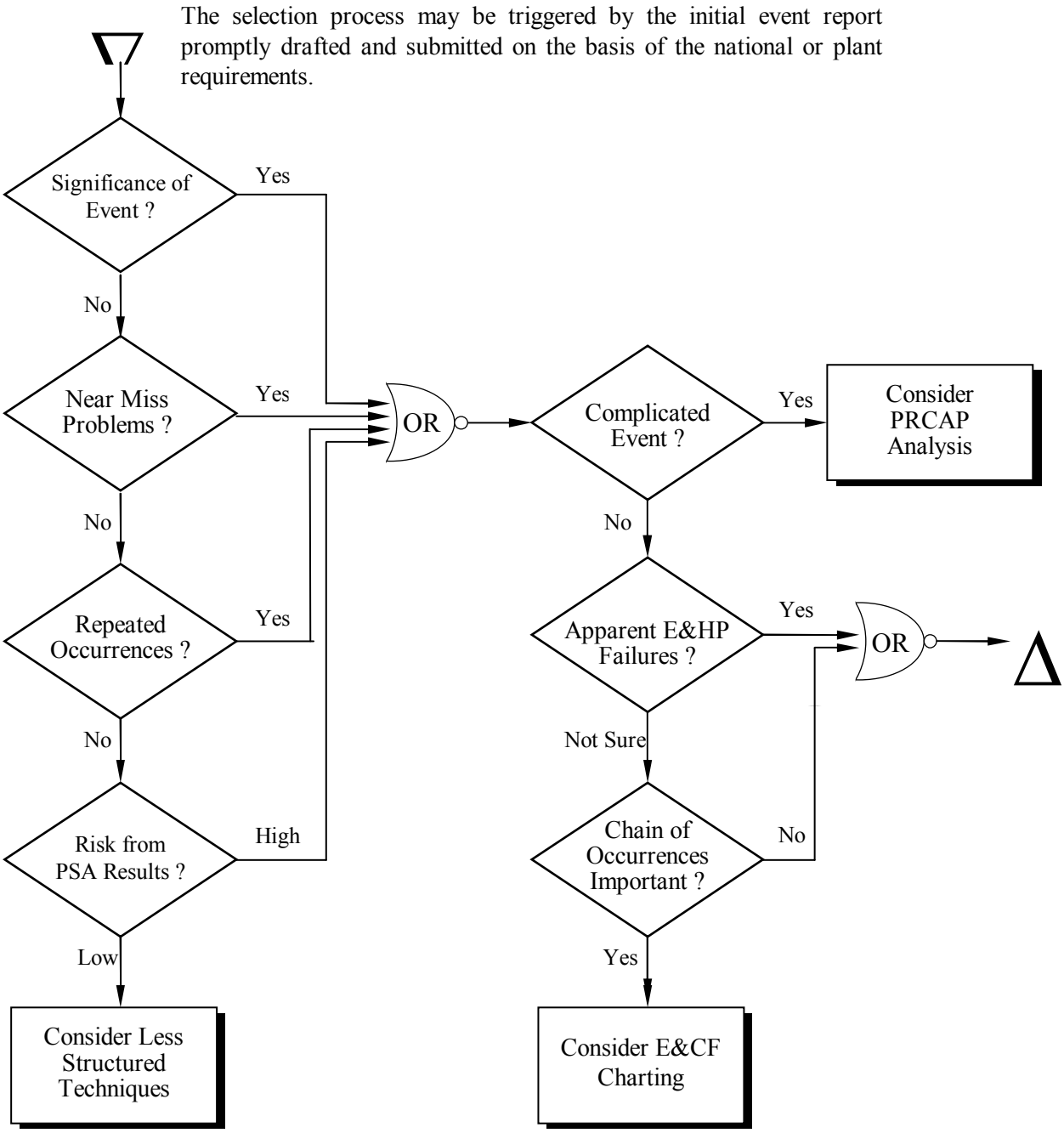
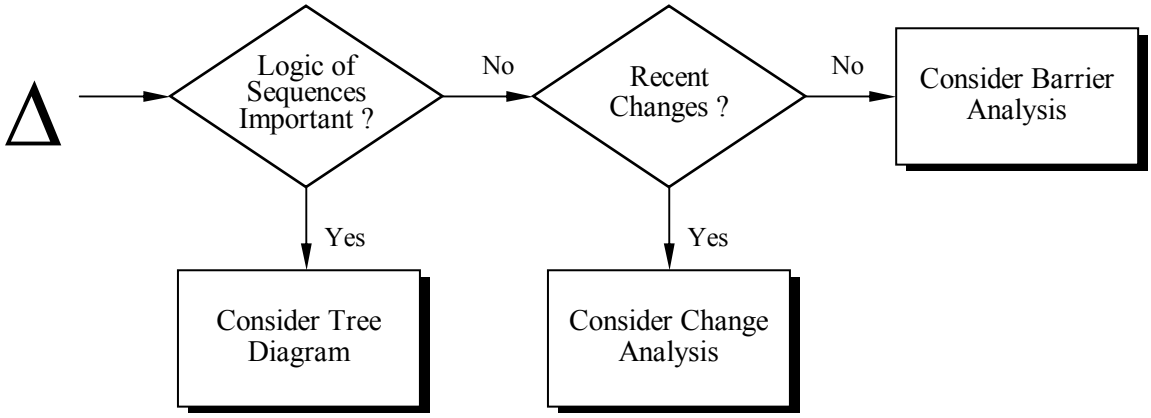


FIGURE 5.10: *RCA TECHNIQUES SELECTION PROCESS (2 of 2)*



.

6. PORTM - A SEARCHING SYSTEM FOR CAUSE CATEGORIES

PORTM represents five columns (categories) of process: **P**revention, **O**bservation, **R**esponse, **T**eam Performance, and **M**anagement. PORTM is not a rigid element, instead it should be revised and enhanced to reflect the changes to plant policies, programs and practices.

6.1 OBJECTIVES OF PORTM

PORTM is a searching tool to help the investigator/ analyst decide where to concentrate the investigative effort without overlooking important aspects that influence equipment and human performance.

The PORTM system provides a set of basic questions to help the investigator/ analyst to allocate efforts where the root cause of an event involving E&HP problems are most likely to be identified. The PORTM system provides guidance to less experienced investigators, and should be used as a check list by experienced investigators.

Together with a preliminary E&CF chart, PORTM should be used in developing the investigation plan to identify:

- What information is lacking for a completed E&CF Chart,
- What areas of equipment performance and human performance need further analysis;
- Who should be interviewed, what questions should be asked, and what additional information should be collected from documents (e.g., control room logbooks, maintenance logs, inspection records, plant computer files).

Primarily PORTM is intended as an iterative investigative process. After a first preliminary evaluation of the evidence the PORTM is revisited to ensure that any facts are not overlooked.

6.2 CONTENTS OF PORTM

There are 5 elements in PORTM, which should always be applied:

Prevention (P.1 to P.3):

P: Prevention category reflects and searches those adverse conditions or deficiencies, which should have existed in advance to an occurrence. Those causal factors (adverse conditions or deficiencies) are cues or likely initiators of the occurrence but

have neither been detected, discovered, nor been recognized and predicted by preventive actions under current practices. This category also implies to the possibility of prevention of occurrence at a very early stage.

Examples:

There was an abnormal situation in technical systems or a malfunction of equipment but had neither been exposed nor discovered by an operator.

Observation (O.1 to O.3):

O: Observation category addresses prerequisites for effective responses to abnormalities; it searches for failures in observation of conditions and symptoms and for reasons of such failures that contributed to nonsuccess of detection, identification and diagnostics, such as personnel fail to be stimulated, fail to become aware of important information, fail to follow requirements or unable to process available information. Observation occurs in the control rooms by reactor operators observing indications, alarms and/or annunciators, or locally in the plant by auxiliary operators or maintenance staff performing routine inspections.

Examples:

The operator failed to diagnose the abnormality or malfunction because the display was cluttered and the volume of the alarm signal was overwhelmed by the ambient noise of the workspace, or because the operator was inattentive to important information.

Response (R.1 to R.5):

R: Response category searches for those factors that influenced, affected or hindered an individual being stimulated to response to abnormalities, including interpretation of encountered conditions/ symptoms, processing available information, or prompting an expected action. Response as a result of "Observation" may include questioning and decision making, communicating or taking physical actions. This category mainly addresses failures or weaknesses in the personal diagnostics, decision-making process and capabilities for expected actions.

Examples:

The operator decided that the alarm received was important, needed immediate response, he read an alarm response procedure, and took action to shut a valve as an immediate response to the alarm.

T: Team performance category applies to problems or difficulties where more than one person was involved and it searches for those factors that affected the process of the team decision-making and the team performance that should have been expected to effectively response to abnormalities. This category addresses cooperation, coordination of the team members, and decision-making process, feedback mechanism within the team. It is also devoted to

identification of problems in turnovers or other interface problems between different teams.

Examples:

A second shift operator mis-understood turnover information and failed to realign a system because he believed the previous shift had already completed the system realignment, or he misunderstood his supervisor's verbal instructions and shut the wrong valve.

Management (M.1 to M.6):

M: Management category searches for those supervisory and managerial factors (organizational and administrative factors), which had been unable or failed to prevent, detect, correct, and mitigate the erroneous or defective performance of the individual or the team. Included are policies, objectives, staff and resources, authority and responsibilities, management programs and systems, including safety culture, quality assurance program, feedback systems, and etc.

Examples:

The operator failed to fill-out a required, safety-related procedure because he was in a hurry to get the job done to meet a production schedule target.

6.3 THE PORTM PROCESS

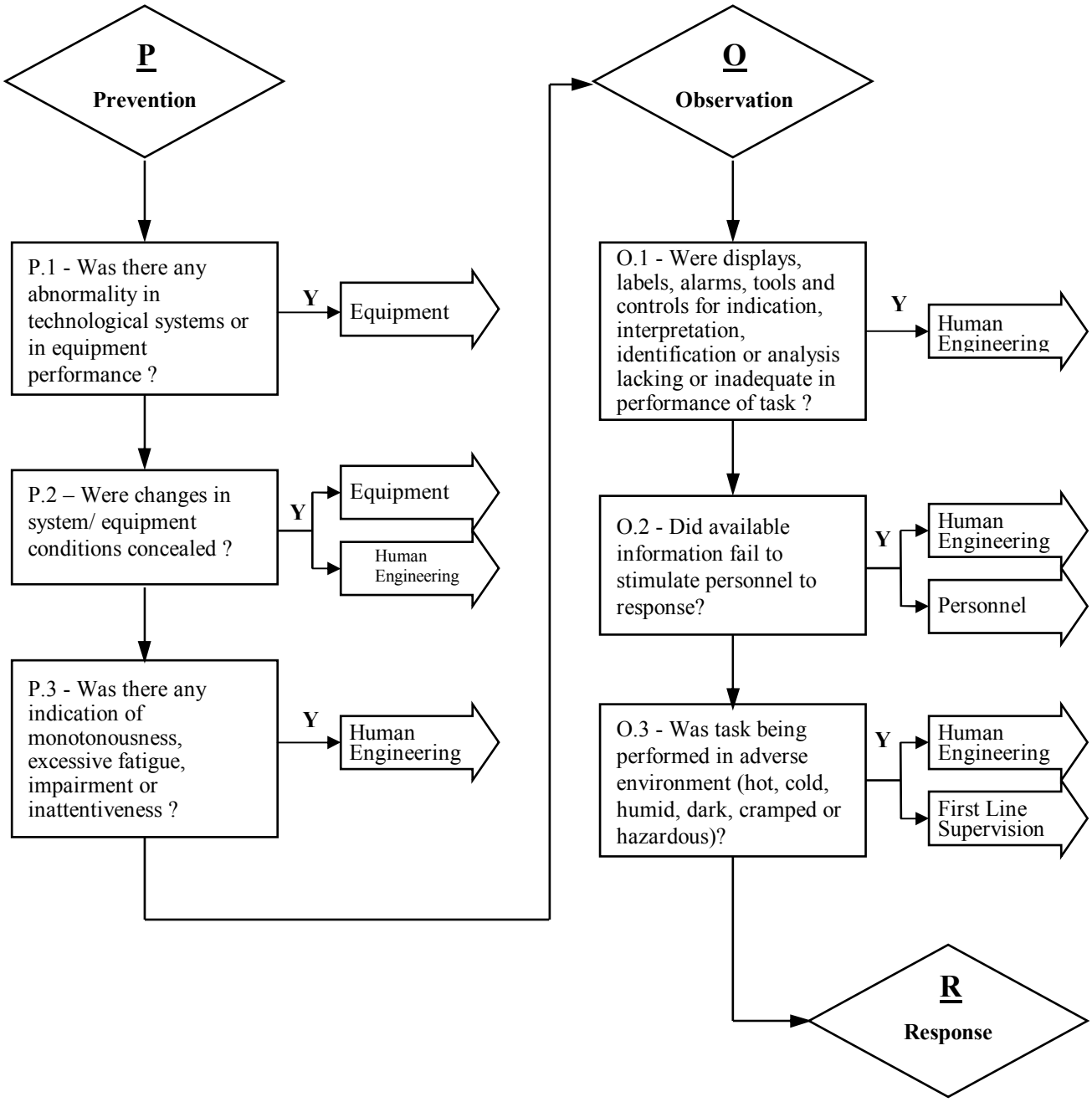
Aided by a series of basic questions, PORTM (**P**revention, **O**bservation, **R**esponse, **T**eam Performance and **M**anagement) supports the investigator/ analyst in searching for causal factors within the PRCAP modules. These questions are presented in a Yes/No logic tree. The answers to these questions will lead the investigator/ analyst to those areas where there exist some causal factors that are most likely to have contributed to the event.

PORTM represents a series of conditions or actions, which should have existed or should have been performed to eliminate or mitigate an event.

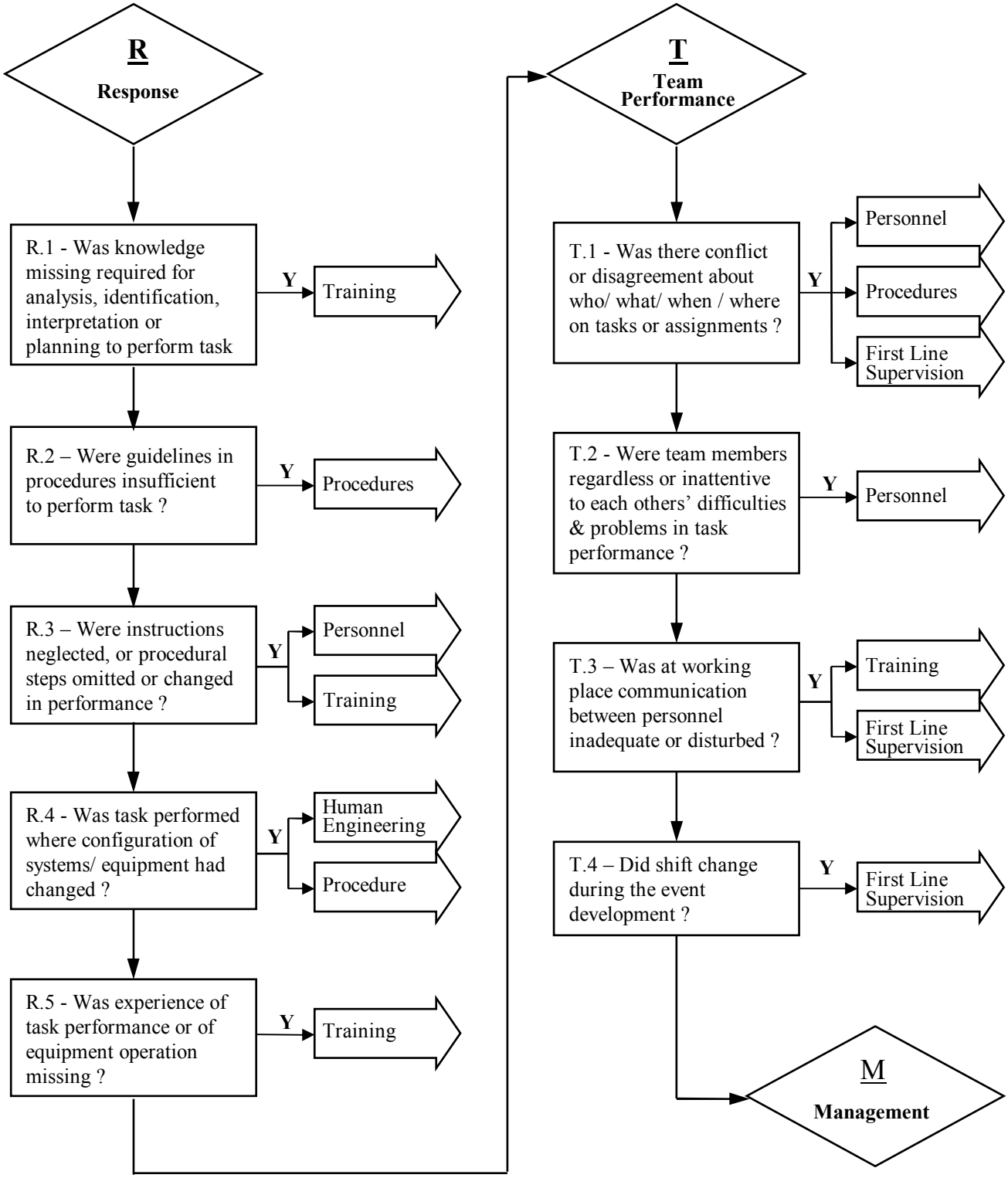
The following flow chart includes five categories (columns) of processes, reflecting step-by-step searching efforts for root causes of the operational events in reference to the standard PRCAP modules. The five PORTM categories (columns) of processes are:

- **P**REVENTION
- **O**BSERVATION
- **R**ESPONSE
- **T**EAM PERFORMANCE
- **M**ANAGEMENT

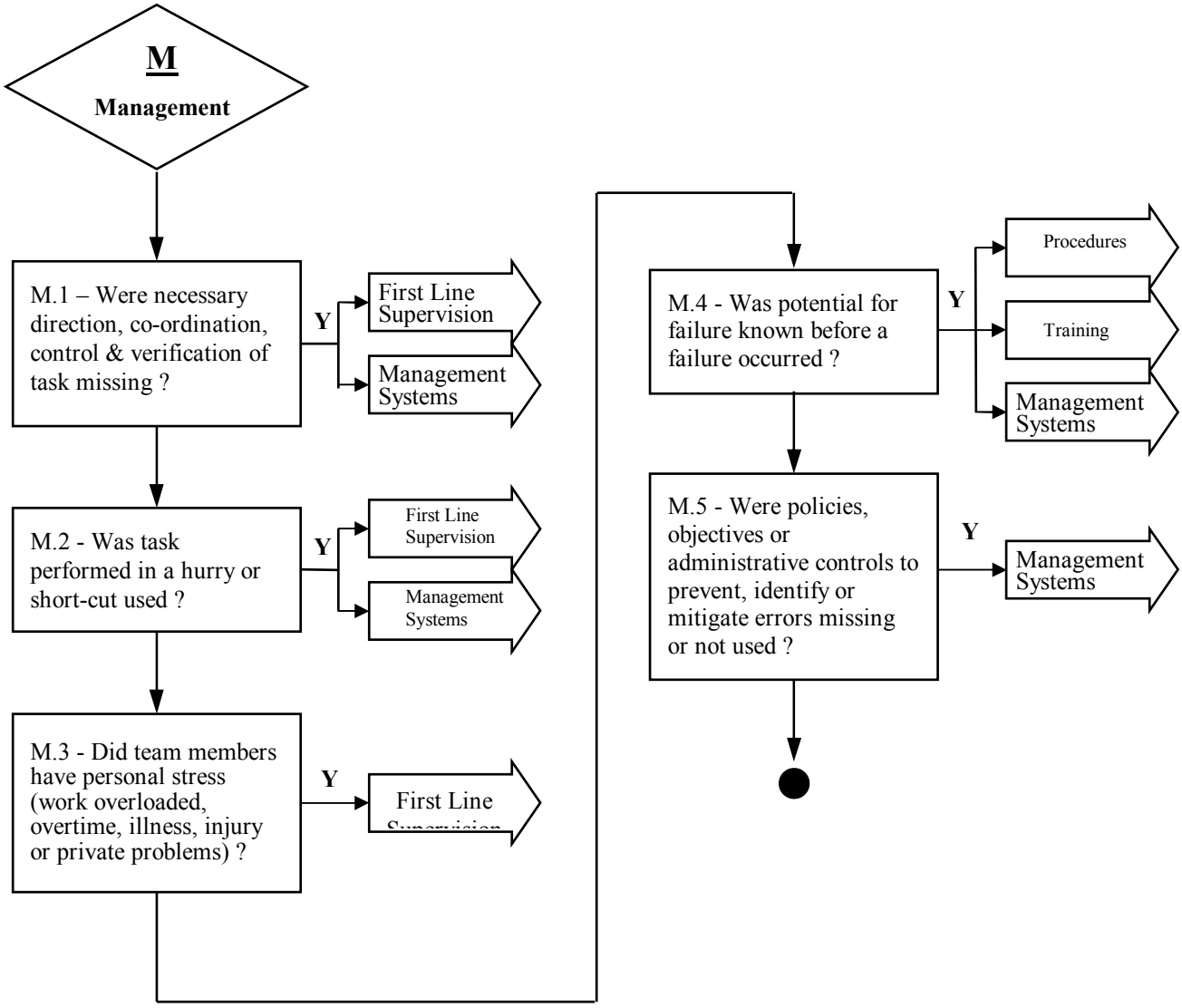
PORTM: The '**Prevention**' & '**Observation**' Categories



PORTM: The '**Response**' & '**Team Performance**' Categories



PORTM: The '**Management**' Category



6.4 AN EXAMPLE OF PORTM APPLICATION

6.4.1 Event Description

Two ion chambers were left mis-positioned during reactor operation and were severely damaged by exposure to high radiation fluxes.

These ion chambers provide reactor flux monitoring during reactor shutdown and reactor start-up until criticality is achieved. The two ion chambers are located in instrument ports through the neutron shied that surrounds the reactor vessel. The position of the ion chambers is controlled from the control room. The chambers can be moved closer to the reactor vessel to increase their sensitivity to neutron fluxes. After the reactor is critical and before operation of the reactor at high powers, the ion chambers are fully retracted and a lead shield shutter is closed in front of the chamber. This prevents damage to the ion chambers for high radiation fluxes by decreasing the incident radiation on the chamber.

After the reactor was shutdown, the damage to the ion chamber was discovered when the flux monitoring system did not respond properly when energized to monitor shutdown flux levels. Investigation revealed the chambers had been left adjacent to the vessel with their shield shutters open following a reactor scram recovery. Because of extensive exposure to high radiation flux, the chambers were damaged beyond further use or repair. Replacement of the chambers took 120 hours of critical path outage time. Adequate monitoring of shutdown neutron flux was maintained by alternate system that relied on different sensors.

6.4.2 Using PORTM to Guide Analyzing the Event

The use of PORTM is demonstrated by applying each of the questions under the five columns or categories in sequence. The answers or the investigation results are presented below the questions respectively.

(1) **P**REVENTION

P 1: Was there any abnormality in technological systems or in equipment performance ?

Yes. The ion chamber was damaged. Investigate "**Equipment**".

P 2: Were changes in system/ equipment conditions concealed ?

Yes/ **No**. A light on a control panel in the main control room indicated the ion chamber position relative to vessel (full withdraw – light out, not withdraw – light on). An operator saw the position indicator light on, but he did not pay

attention to the reason. Investigate "**Equipment**" and "**Human Engineering**".

P 3: Was there any indication of monotonousness, excessive fatigue, impairment or inattentiveness ?

No.

(2) **O**BSERVATION

O 1: Were displays, labels, alarms, tools and controls for indication, interpretation, identification or analysis lacking or inadequate in performance of task ?

Yes. The position indicator light was although noticed by an operator. However, the position indicator light was not labeled adequately to allow the operator to know that the light off meant the chamber was fully withdrawn from the vessel and the light on meant the chamber was not fully withdrawn form the vessel. Labeling was Yes/ No only. Moreover, there was no alarm to indicate mis-positioning of the chamber during power operations.
Investigate "**Human Engineering**".

O 2: Did available information fail to stimulate personnel to response ?

Yes. An operator saw the position indicator light on, but the indication was not an alarm indication that lead to the procedure for response rather a position indicator for the operator information. However, there is a procedure requiring that the operator check the position indicator light before de-energizing the flux monitoring system. Investigate "**Personnel**" and "**Training**".

O 3: Was task performed in adverse environment (hot, cold, humid, dark, cramped or hazardous) ?

No.

(3) **R**ESPONSE

R 1: Was knowledge missing for understanding, analysis, planning, interpretation or performance of task ?

Yes. Knowledge of equipment response was missing. The operator was new and had not operated the flux monitoring equipment prior to the event. He did not realize the significance of chamber position when the system was turned off. Investigate "**Training**".

R 2: Were guidelines in procedures insufficient to perform task ?

Yes. Procedure only provided guidance to response alarms but did not include light on indication. Investigate "**Procedure**".

R 3: Were instructions neglected or procedural steps omitted or changed in performance ?

Yes. Procedure requiring that the operator check the position indicator light before de-energizing the flux monitoring system was not followed. Investigate "**Personnel**" and "**Training**".

R 4: Was task performed where configuration of systems/ equipment had changed ?

No.

R 5: Was experience of task performance or of equipment operation missing ?

Yes. The operator had no experience and had not operated the flux monitoring equipment prior to the event. Investigate "**Training**".

(4) **T**EAM PERFORMANCE

T 1: Was there conflict or disagreement about who(m)/ what/ when/ where on task assignment and performance ?

No.

T 2: Were team members regardless or inattentive to each others' difficulties or problems in task performance ?

No.

T 3: Was at working place communication between personnel inadequate or disturbed ?

Yes. The communication between team members as well as during shift change was not adequate (see below). Investigate "**Training**" and "**First Line Supervision**".

T 4: Did shift change during the event development ?

Yes. Shift change occurred during the procedure and the steps preceding shutdown of the flux monitoring equipment was divided between the two shifts. Every one was busy and a lot was going on during procedure, especially just before the shift change. The first shift supervisor thought his operator had withdrawn the chambers and when the second shift supervisor ask his operator

if this was true, the operator misunderstood and thought he was being told it had been done already. The operator said OK, meaning he understood, but the supervisor took OK to mean yes the chambers had been withdrawn and checked the step off. Investigate "**First Line Supervision**".

(5) **M**ANAGEMENT SYSTEMS

M 1: Were necessary direction, co-ordination, control and verification of task missing ?

Yes/ No. Direction and co-ordination between team members were required and performed. The supervisor told the operators what the next step was and then marked off the step when completed. However, control and verification were not properly performed. The first shift supervisor thought his operator had withdrawn the chambers, but in fact not. The second shift supervisor told his operator to shut off the equipment, but both did not followed the procedure to check whether the equipment had been withdrawn and put in the correct position. Because the event involves errors of both shifts, investigate "**First Line Supervision**", and "**Management Systems**" of the line operating organization.

M 2: Was task performed in a hurry or short-cut used ?

Yes. Task was performed in a hurry as everyone was involved in completing the shift and shift turnover. Investigate "**First Line Supervision**" and "**Management Systems**".

M 3: Did team members have personal stress (work overload, overtime, illness, injury or private problems) ?

No.

M 4: Was potential for failure known before a failure occurred ?

Yes. Potential for failure was known prior to the event, but is was said procedures were in place to prevent events ?. Investigate again "**Procedures**" , "**Training**" and "**Management Systems**".

M 5: Were policies, objectives or administrative controls to prevent, identify or mitigate errors missing or not used ?

Yes/ No. Administrative controls to prevent the event were not followed properly although safety policies and objectives were established. Investigate "**Management Systems**".

7. WORKSHEETS OF PRCAP MODULES

PRCAP provides a set of modules for categorization of factors influencing equipment and human performance (E&HP). The PRCAP modules are used to allocate root causes of problem areas identified by PORTM. The structure of the PRCAP modules is the same as a complete cause tree. Purpose of the tree structures is to identify the specific areas to be subjected to further analysis. In principle, the tree structures are equivalent to MORT, but they reflect the current comprehensive concerns on the E&HP factors within the commercial nuclear power industry. There are a total of seven modules:

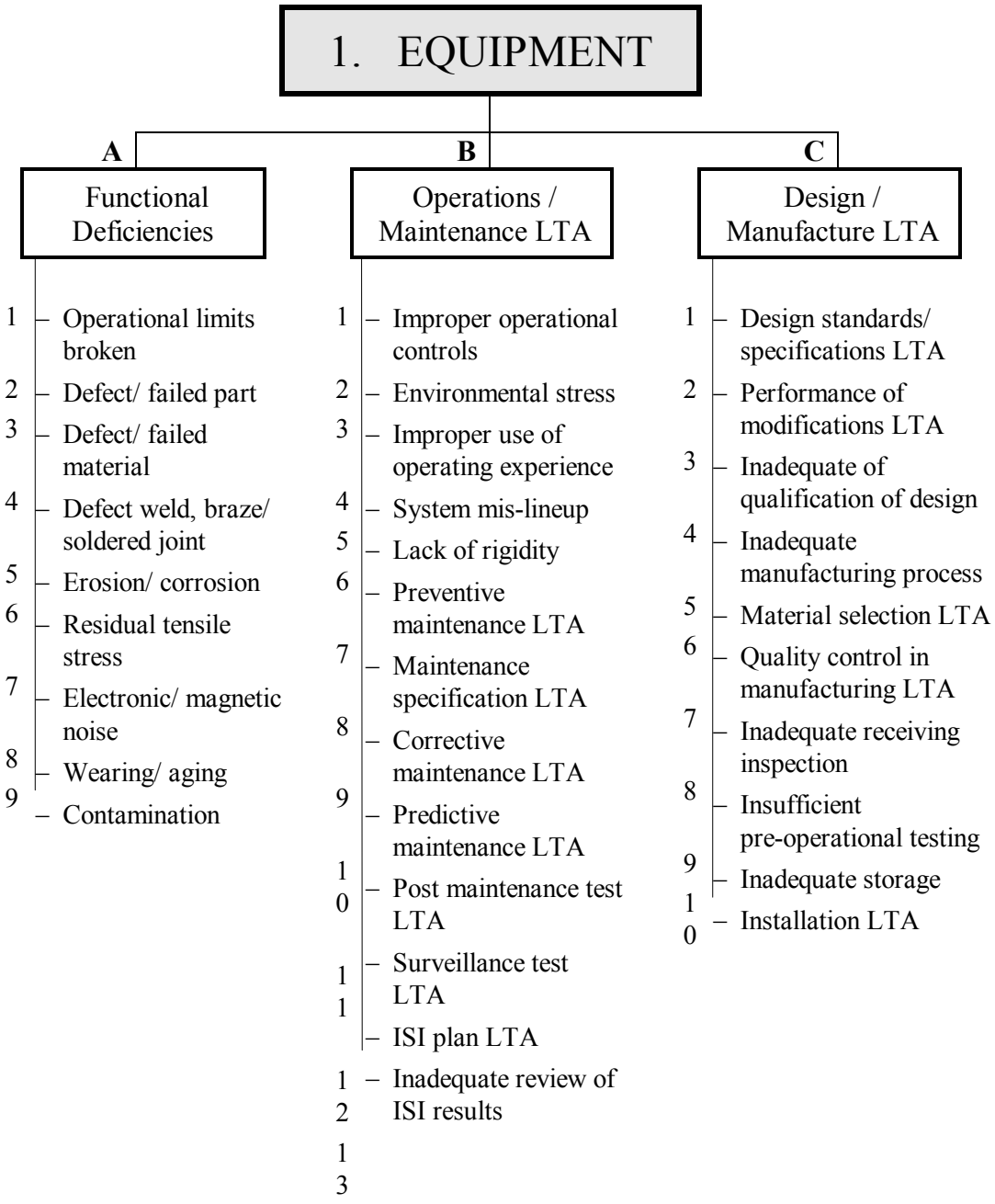
(1) Equipment,
(2) Personnel,
(3) Procedures,
(4) Human-Engineering,
(5) Training,
(6) First Line Supervision, and
(7) Management Systems.

The PRCAP modules consist of, 7 cause categories, 24 cause branches and more than 200 causal factors. Modules, branches and causal factors are coded. Each of the PRCAP modules is provided with a set of work sheets of questions corresponding to the ready-made tree structure to assist the investigator/ analyst in determining if any E&HP contributors of the event came from that particular area.

In fact, the PORTM system and the work sheets together provide a set of questions at three levels. Namely, the PORTM system helps the investigator/ analyst to determine the cause categories (the top level of the modules) of a problem, the set of questions in the work sheets assist the investigator/ analyst in determination of the cause branches and causal factors (two lower levels in the modules).

In using these forms in the work sheets, first consideration should be given to the screening questions for the cause branch level. If a cause branch is identified, then the investigator should ask the questions associated with this cause branch to try to pinpoint the causal factors.

7.1 MODULE 1 - EQUIPMENT



LTA - Less Than Adequate.

Note: For systematic analysis of equipment failures, the starting point is always to observe the failed parts of the equipment. In identification of the causal factors of the equipment failures, the functional requirements and reliability of the equipment should be reviewed and the external influences considered. The analysis of equipment failures should be based on detailed knowledge of failure modes and failure mechanisms. The plant specific operating experience

should be taken into account to determine if there have been recurrences, similar failure patterns, or adverse performance trends.

CAUSE MODULE 1 - EQUIPMENT

Cause Branch 1A - Functional Deficiencies

CAUSE BRANCH SCREENING QUESTION		Ask questions below to find causal factors if answer is :
(A_1) Was equipment failure attributable to performance deficiencies or functional degradations?		Yes
(A_2) Was equipment failure readily identified through inspections or surveillance in the established practices?		Yes
QUESTION	**Problem If**	**CAUSAL FACTOR**
(1) Did the equipment failure occur due to violation of equipment technical specifications?	Yes	• ***Operational limits broken***
(2) Did equipment fail due to a part of it defected or failed?	Yes	• ***Defect/ failed part***
(3) Did equipment fail due to material deficiencies?	Yes	• ***Defect/ failed material***
(4) Was there any problem of the joint parts of the equipment?	yes	• ***Defect weld, braze or soldered joint***
(5) Does equipment have visible traces of chemical residue/ crystals on inside or outside surface?	yes	• ***Erosion/ corrosion***
(6) Does equipment have visible fracture, flaw or crack on surface?	yes	• ***Erosion/ corrosion*** • ***Residual tensile stress***
(7) Was the equipment failure attributable to the unknown noise in its instrument?	Yes	• ***Electronic/ magnetic noise***
(8) Was the equipment failure attributable to the undue wearing or aging?	yes	• ***Wearing/ aging***
(9) Was the equipment failure attributable to the contamination of dust, debris, radioactivity or others?	yes	• ***Contamination***

CAUSE MODULE 1 - EQUIPMENT

Cause Branch 1B - Operations/ Maintenance LTA

CAUSE BRANCH SCREENING QUESTION		Ask questions below to find causal factors if answer is :
(B_1) Was the equipment failure attributable to abnormal operational conditions or environmental stress?		Yes
(B_2) Was the equipment failure attributable to errors of omissions during maintenance, in-service inspection or surveillance tests?		Yes
QUESTION	**Problem If**	**CAUSAL FACTOR**
(1) Did the equipment failure occur or was the failure preceded by unusual or unexpected plant state evolution (e.g. abnormal load cycling, mechanical/ acoustic vibration, chemistry, or steam quality)?	Yes	• ***Improper operational controls***
(2) Did the equipment failure occur or was the failure preceded under excess environmental stress (e.g. excess temperature, pressure, humidity, vibration, etc.)?	yes	• ***Environmental stress***
(3) Was the equipment failure a recurrence and corrective action readily apparent?	no	• ***Improper use of operating experience***
(4) Was the system failure due to that mis-positioned valves broke barriers and lead to unwanted energy flow?	yes	• ***System mis-lineup***
(5) Was failure due to routine load cycling or temperature cycling?	yes	• ***Lack of rigidity***
(6) Did multiple failures arise from the application of the manufacturer's maintenance specifications?	yes	• ***Maintenance specifications LTA***
(7) Was preventive maintenance not planned, not performed on time or as intended?	no	• ***Preventive maintenance LTA***

CAUSE MODULE 1 - EQUIPMENT

Cause Branch 1B – Operations /Maintenance LTA(Continued)

QUESTION	Problem If	CAUSAL FACTOR
(8) Were before the failure there indications of precursors or warnings about problems?	yes	• ***Corrective maintenance LTA***
(9) Was the failure due to improper identification of abnormality or adverse trend of equipment performance?	yes	• ***Predictive maintenance LTA***
(10) Was the failure due to no or improper test after maintenance of equipment?	yes	• ***Post maintenance test LTA***
(11) Had the equipment been tested under the plant surveillance test program?	no	• ***Surveillance test LTA***
(12) Had the in-service inspection (ISI) plan adequate extent/ coverage, and was it sufficiently detailed?	no	• ***ISI plan LTA***
(13) Were in-service inspection (ISI) results recorded and adequately evaluated?	no	• ***Inadequate review of ISI results***

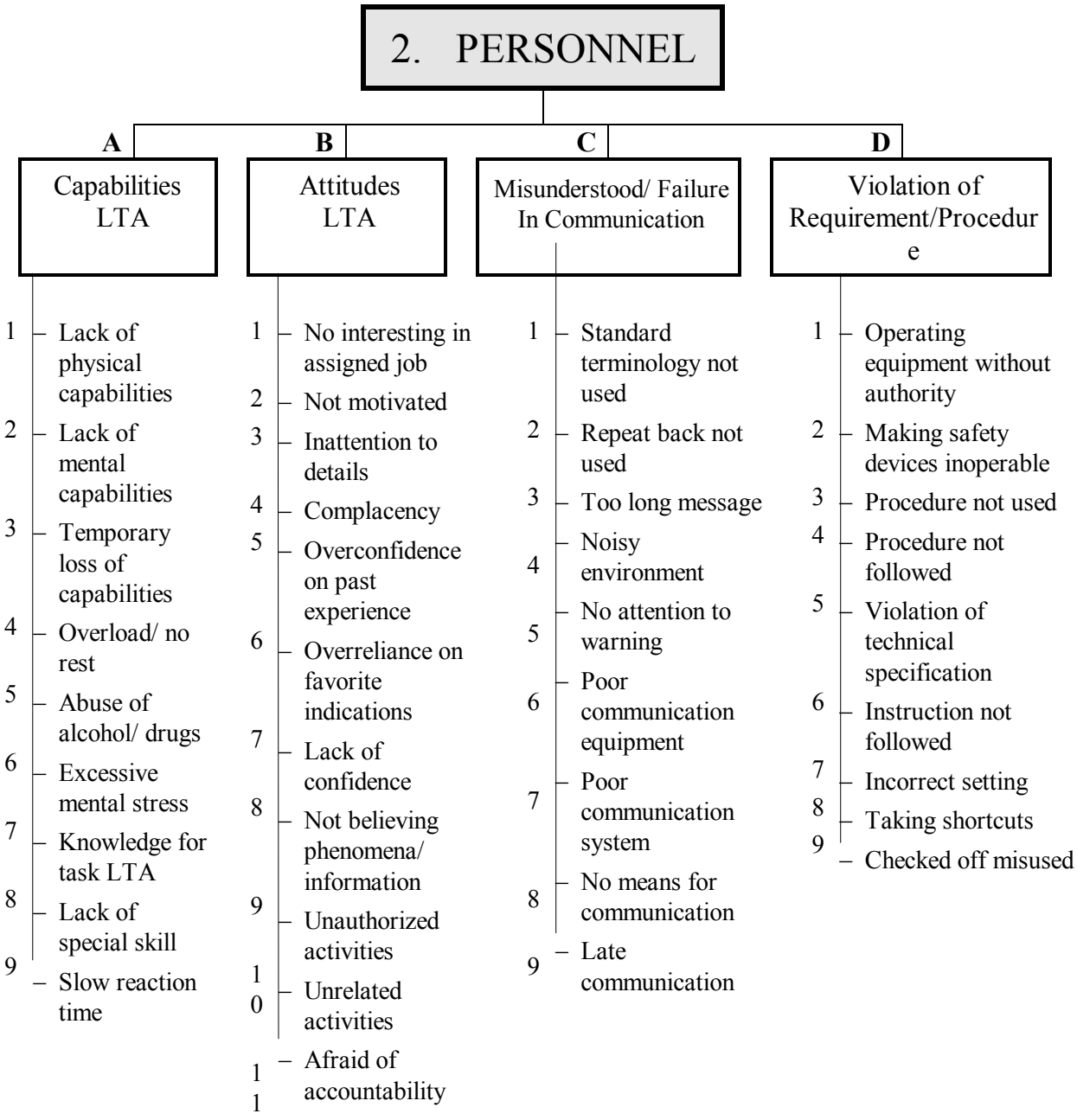
CAUSE MODULE 1 – EQUIPMENT

Cause Branch 1C – Design/ Manufacture LTA

CAUSE BRANCH SCREENING QUESTION		Ask questions below to find causal factors if answer is :
(C_1) Was equipment failure attributable to other than operational influences, such as design, manufacture, fabrication, and outside the control or influence of normal, routine maintenance and testing?		YES
QUESTION	**Problem If**	**CAUSAL FACTOR**
(1) Was the design relevant to the actual operating environment or operational requirements?	no	• ***Design standards/ specifications LTA***
(2) Was failure due to performance of modifications in an existing plant/ system configuration?	yes	• ***Performance of modifications LTA***
(3) Did failure involve more than one piece of equipment of same or similar design?	yes	• ***Inadequate qualification of design*** • ***Inadequate manufacturing process***
(4) Was failure one or more recurrences during routine operation?	yes	• ***Inadequate qualification of design*** • ***Inadequate manufacturing process***
(5) Was failure due to improper or inadequate/ incompatible materials?	yes	• ***Material selection LTA***
(6) Was failure attributable to lack of control and verification during manufacture or fabrication?	yes	• ***Quality control in manufacturing LTA***
(7) Had failed equipment been subjected to sufficient receiving inspection or adequate acceptance criteria?	no	• ***Inadequate receiving inspection***

CAUSE MODULE 1 – EQUIPMENT		
Cause Branch 1C – Design /Manufacture LTA(Continued)		
QUESTION	**Problem If**	**CAUSAL FACTOR**
(8) Had failed equipment been subjected to sufficient pre-operational testing?	no	• ***Insufficient pre-operational testing***
(9) Was the failure attributable to the storage (out of permitted time, corrosion, temperature, duties, etc.)?		• ***Inadequate storage***
(10) Did equipment failure result from mechanical impact?	yes	• ***Installation LTA***

7.2 MODULE 2 - PERSONNEL



LTA - Less Than Adequate.

Note: For analysis of the personnel failures, the starting point is to analyze the improper actions or no action of the person(s) directly involved in the occurrences. Both internal and external factors of the personnel failures should be considered. The investigator/ analyst should review relevant personal files, interview all associated persons and their supervisors, as appropriate. However, the purpose of the investigation is not to determine who should be blamed, but rather to identify the root cause of the event to eliminate the recurrence of similar failures.

CAUSE MODULE 2 – PERSONNEL

Cause Branch 2A - Capabilities LTA

CAUSE BRANCH SCREENING QUESTION		Ask questions below to find causal factors if answer is :
(A_1) Was the occurrence caused by inadequate personal physical or mental capabilities?		Yes
(A_2) Were the personal capabilities lost or decreased in the course of the occurrence development?		Yes
QUESTION	**Problem If**	**CAUSAL FACTOR**
(1) Did the person have inadequate physical capabilities (e.g. deficiencies in strength, vision, hearing, or communication problems)?	yes	• ***Lack of physical Capabilities LTA***
(2) Did the person have inadequate mental capabilities (e.g. low intelligence level, slow reaction time)?	yes	• ***Lack of mental Capabilities LTA***
(3) Did the person temporarily loss or decrease capabilities due the sickness or injury?	yes	• ***Temporary loss of capabilities***
(4) Was the person excessive fatigue due to overload or no rest during a period of current time?	yes	• ***Overload/ no rest***
(5) Was the personal excessive fatigue or emotional upset impaired under influence of alcohol and/or abuse of other drugs?	yes	• ***Abuse of alcohol/ drugs***
(6) Did the person have excessive mental stress due to schedule pressure, plant reward/ reprimand policy, or personal life problems?	yes	• ***Excessive mental stress***
(7) Was the personal special knowledge inadequate for the job/task (Lack of experience, orientation, or training)?	yes	• ***Knowledge for task LTA***

CAUSE MODULE 2 – PERSONNEL

Cause Branch 2A – Capabilities LTA(Continued)

QUESTION	Problem If	CAUSAL FACTOR
(8) Was the personal special skill inadequate for the job/task (lack of coaching, inadequate practice, etc.)?	yes	• ***Lack of special skill***
(9) Was the reaction time of the person traditional slow?	yes	• ***Slow reaction time***

CAUSE MODULE 2 – PERSONNEL

Cause Branch 2B - Attitudes LTA

CAUSE BRANCH SCREENING QUESTION		Ask questions below to find causal factors if answer is :
(B) Was the occurrence caused by personal failure or bad performance due to inadequate attitudes towards the work or task?		Yes
QUESTION	**Problem If**	**CAUSAL FACTOR**
(1) Was an occurrence or bad performance caused because the person was not interested in the job assigned?	yes	• ***No interesting in job***
(2) Was the person less willing to perform the task in compliance with all requirements due to poor motivation?	yes	• ***Not motivated***
(3) Was there insufficient degree of attention to details resulting in using wrong equipment or procedure, or omitting steps in a procedure?	yes	• ***Inattention to details***
(4) Was there complacency resulting in lack of perceived need for concern?	yes	• ***Complacency***
(5) Was there overconfidence on the past operating experience (either successful or failed experience)?	yes	• ***Overconfidence on past experience***
(6) Was the misdiagnosis caused by overreliance on favorite indications and ignoring other information?	yes	• ***Overreliance on favorite indications***
(7) Was the occurrence caused by lack of confidence in performing tasks, using unfamiliar equipment, etc?	yes	• ***Lack of confidence***
(8) Was the occurrence caused by not believing the phenomena faced or information provided?	yes	• ***Not believing phenomena/ information***

CAUSE MODULE 2 – PERSONNEL

Cause Branch 2B – Attitudes LTA (Continued)

QUESTION	Problem If	CAUSAL FACTOR
(9) Was the occurrence caused by personal performing unauthorized or disapproved activities?	yes	• ***Unauthorized activities***
(10) Was the occurrence dealing with that the person was doing unrelated activities during the shift?	yes	• ***Unrelated activities***
(11) Was the occurrence developed by no timely reporting due to being afraid of perceived accountability	yes	• ***Afraid of accountability***

CAUSE MODULE 2 – PERSONNEL

Cause Branch 2C – Misunderstood /Failure in Communication

CAUSE BRANCH SCREENING QUESTION		Ask questions below to find causal factors if answer is :
(C) Did an occurrence happen because the person misunderstood information or there was a failure in timely communication ?		Yes
QUESTION	**Problem If**	**CAUSAL FACTOR**
(1) If the wrong action was taken or the wrong equipment was operated, was standard terminology used to communicate about the action and the equipment?	yes	• ***Standard terminology not used*** Note: If standard terminology is not part of the plant policy, if the policy was violated, or if standard terminology is not stresses in training, investigate **Management System** and **Training** modules.
(2) Did the personnel involved repeat back the message to verify that the message was heard and understood correctly?	no	• ***Repeat back not used*** Note: If repeat backs are not part of the plant administrative controls, if the controls were violated, or if repeat backs are not stressed in training, investigate **Management System** and **Training** modules.
(3) Was a message or instruction mis-understood because it was too long and couldn't be accurately understood and remembered?	yes	• ***Too long message***
(4) Did noise interfere with the listener's understanding of the message or instruction?	yes	• ***Noisy environment***
(5) Was the person being communicated no attention to warning?	yes	• ***No attention to warning***

CAUSE MODULE 2 – PERSONNEL

Cause Branch 2C – Misunderstood /Failure In Communication (Continued)

QUESTION	Problem If	CAUSAL FACTOR
(6) Was the communication equipment good so that the voice or message could be heard under normal ambient noise conditions?	no	• ***Poor communication equipment***
(7) Was the voice communication system inadequate to support the needed communications during the occurrence (e.g. overloaded channels)?	yes	• ***Poor communication system***
(8) Was there no method or system at the place for communicating messages or instructions to the personnel involved during the occurrence?	no	• ***No means available***
(9) Was needed information unable to be provided because the occurrence developed too fast to permit communications?	yes	• ***Late communications***

CAUSE MODULE 2 – PERSONNEL

Cause Branch 2D – Violation of Requirements/ Procedures

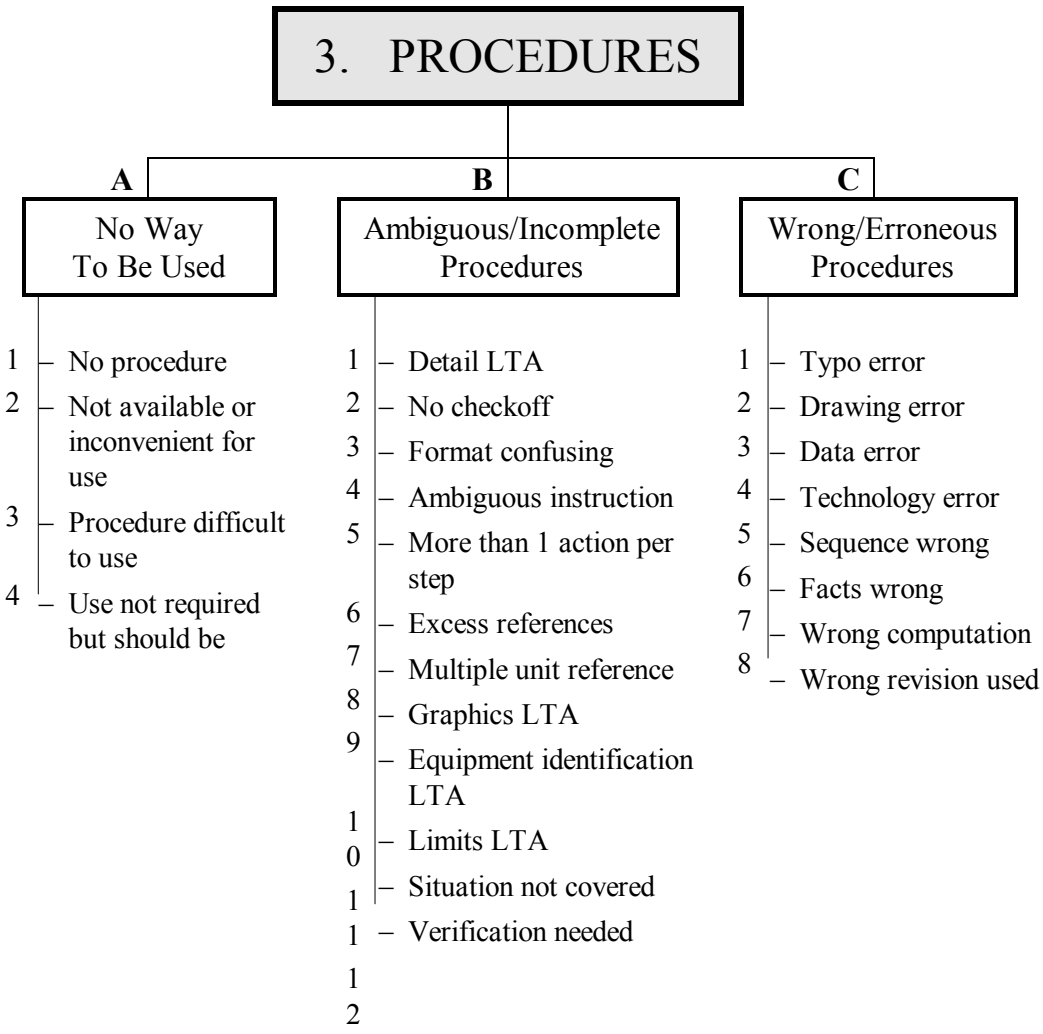
CAUSE BRANCH SCREENING QUESTION		Ask questions below to find causal factors if answer is :
(D) Did an occurrence happen because the person violated the established requirements or procedures?		Yes
QUESTION	**Problem If**	**CAUSAL FACTOR**
(1) Was the occurrence caused by personal operating equipment without authorization or certification?	yes	• ***Operating equipment without authority***
(2) Was the occurrence caused because personnel have made safety devices inoperable?	yes	• ***Making safety devices inoperable***
(3) Was the occurrence caused because personnel did not use procedure while there is one available?	yes	• ***Procedure not used***
(4) Was the occurrence caused because personnel did not follow conditions, steps or any other requirements in the procedure?	yes	• ***Procedure not followed***
(5) Was the occurrence caused by personal violating technical specifications?	yes	• ***Violation of technical specifications***
(6) Was the occurrence caused because personnel did not follow instruction while there is one required?	yes	• ***Instruction not followed***
(7) Was the occurrence caused because the setting of parameter or equipment was made wrong?	yes	• ***Incorrect setting***

CAUSE MODULE 2 – PERSONNEL

Cause Branch 2D – Violation of Requirements/ Procedures (Continued)

QUESTION	Problem If	CAUSAL FACTOR
(8) Did the person follow procedure steps and avoid taking shortcuts provoked by his assumptions or his colleagues to complete job quickly?	no	• ***Taking shortcuts***
(9) Was a checkoff misused (possibly by doing several steps at once rather than doing one step, checking it off, then doing the next)?	yes	• ***Checkoff misused***

7.3 MODULE 3 - PROCEDURE



LTA - Less Than Adequate.

Note: Procedures should provide reliable and adequate guidance for personnel to perform a task under certain conditions. When insufficient and improper guidance were considered as the causes of the occurrences, the applicable procedures for the tasks involved in the event should be reviewed for their technical and human factor problems, such as adequacies in technical contents, presentation formalities and administration of the procedures. The investigator/ analyst should also address what achievements are expected versus the consequential occurrences and how the procedure was intended to be used versus how it was actually used.

CAUSE MODULE 3 – PROCEDURES

Cause Branch 3A - No Way To Be Used

CAUSE BRANCH SCREENING QUESTION		Ask questions below to find causal factors if answer is :
(A) Was the task done without a procedure when a procedure should have been used? Note: Failure to follow/use procedures is normally a violation of management policy. Therefore, the investigator should also consider causes in the **Management System** module.		Yes
QUESTION	**Problem If**	**CAUSAL FACTOR**
(1) Is there should be a procedure, was one available?	no	• ***No procedure***
(2) Was the procedure not readily available (e.g. one mast copy that had to be reproduced) or inconvenient to use (e.g. some working conditions or locations such as tight quarters, contamination zones, or protective clothing made handling procedures inconvenient)?	yes	• ***Not available or inconvenient for use***
(3) Did personnel performing the job consider the procedure exceptionally difficult to use and, therefore, decide not to use it?	yes	• ***Procedure difficult to use*** Note: If better training would have made the job easier to perform and thus the procedure adequate, investigate **Training** module. If better pre-job briefs/ walk-throughs by supervision would have made the job easier to perform and thus the procedure adequate, investigate **Supervision** module.
(4) If a procedure exists and is recommended for use but not required, should it be required because of the significance of the job?	yes	• ***Use not required but should be***

CAUSE MODULE 3 – PROCEDURES

Cause Branch 3B – Ambiguous/ Incomplete Procedure

CAUSE BRANCH SCREENING QUESTION	Ask questions below to find causal factors if answer is :
(B) Was an occurrence caused because of following a defective or incomplete procedure?	Yes

Discussion for Questions 1 & 2: If an error occurred while performing a procedure, the investigator should verify if the procedure used is technically accurate and complete in comparison with technical documentation and expert knowledge.

QUESTION	Problem If	CAUSAL FACTOR
(1) Is the procedure written at an inappropriate level of technical detail given the training and experience required for personnel performing the work?	yes	• ***Detail LTA***
(2) Are user checkoffs missing form the proper points that would guard against omitting significant steps?	yes	• ***No checkoffs***

Discussion for Questions 3 to 13: The presentation of procedures contributes significantly to usability. Poor procedure writing practices my cause personnel confusion and errors. An evaluation of procedure presentation is done by comparing procedure characteristics to human factors criteria concerning the organization, format, style and content of procedures.

(3) Does the organization/ format of the procedure permit it to be easily, rapidly, and precisely read and understood? Does the organization of the procedure conform to the facility's guidance concerning organization into sections (e.g. objective, initial conditions, immediate actions, subsequent actions, diagnostic aids)?	no	• ***Format confusing***
(4) Does the format of the procedure allow the user to find and comprehend essential information efficiently and effectively, that is:		

CAUSE MODULE 3 – PROCEDURES

Cause Branch 3B – Incorrect/ Incomplete Procedure (Continued)

QUESTION	Problem If	CAUSAL FACTOR
(a) Does the arrangement (e.g. use if indentation) of the action steps and their supporting information enhance comprehension?	no	• ***Format confusing***
(b) Is the vocabulary used simple, familiar, and specific to accurately convey the intended meaning?	no	• ***Ambiguous instructions***
(c) Are abbreviations, acronyms, and symbols used familiar to the user?	no	• ***Ambiguous instructions***
(d) Are the instructions in the procedure unclear because of poor sentence structure or punctuation?	yes	• ***Ambiguous instructions***
(e) Are formulas and calculations as simple as possible and is adequate space provided to perform the calculations?	no	• ***Format confusing***
(f) Are warning and caution notices accurate, concise, and without action steps?	no	• ***Format confusing***
(g) Are conditional statements or logic sequences constructed using the principles and techniques of formal logic so that they are logically correct?	no	• ***Ambiguous instructions***
(5) If part of a step was skipped, did the step contain more than 1 action statement (was the step written in a paragraph format rather than in crisp action statement)?	no	• ***More than 1 action per step***

CAUSE MODULE 3 – PROCEDURES

Cause Branch 3B – Ambiguous/ Incomplete Procedure (Continued)

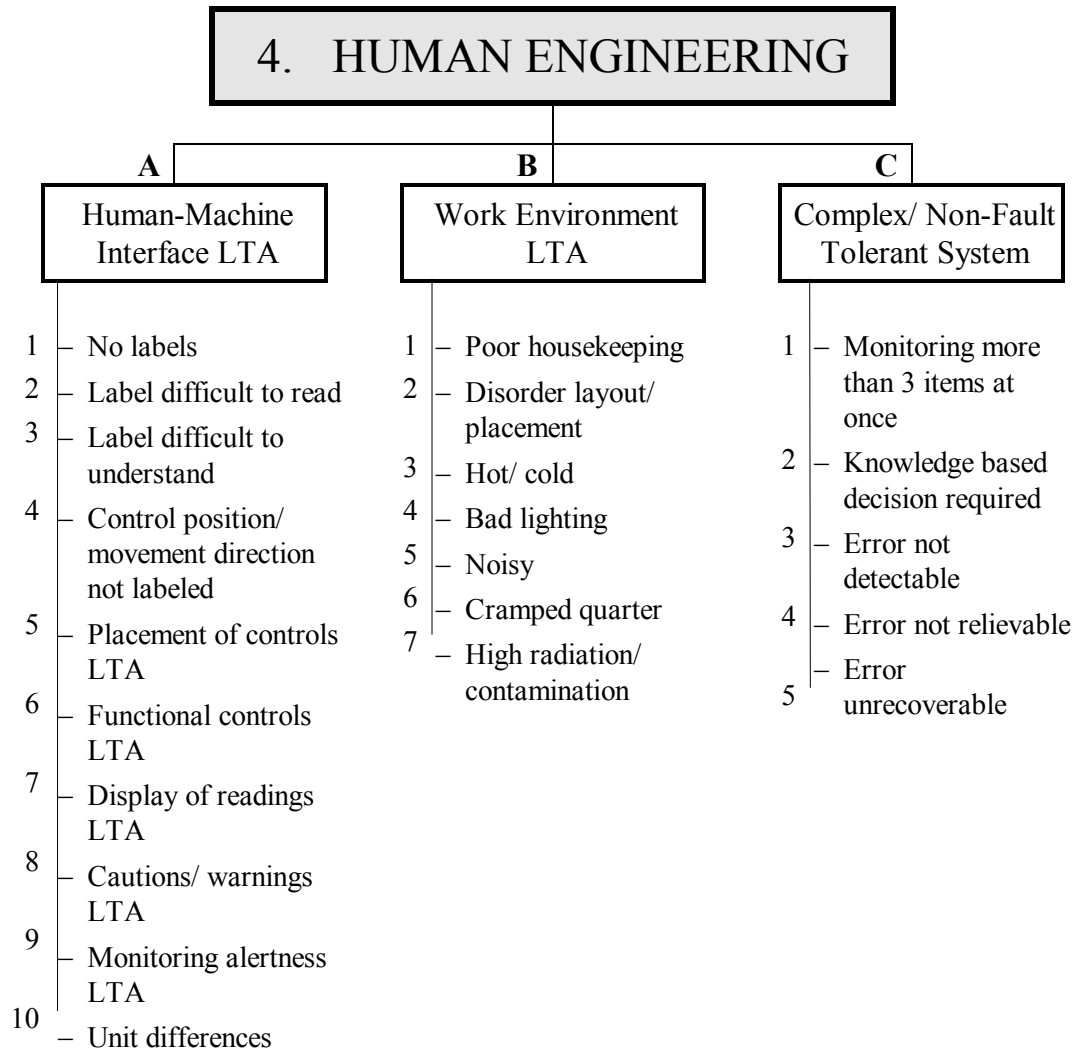
QUESTION	Problem If	CAUSAL FACTOR
(6) Did the procedure refer to more than two other procedures causing the operator to become confused or omit steps in one of the multiple procedures?	yes	• ***Excess references***
(7) Did the procedure contain references to multiple plants or units that may have caused confusion or errors?	yes	• ***Multiple unit references***
(8) Was an error made while using unclear, confusing, or misleading graphs, illustrations, one-line diagrams, or system drawings in the procedure?	yes	• ***Graphics LTA***
(9) Does component/equipment identification in the procedure agree with actual field equipment identification or label?	no	• ***Equipment identification LTA***
(10) Were limits/operating ranges expressed in a "+ or -" format instead of in absolute numbers (e.g. 1.32 ± 0.69 is more likely to cause an error than 0.63 to 2.01)?	yes	• ***Limits LTA***
(11) Were instructions left out that should have been included, or did the procedure fail to address all situations that reasonably should have been expected to occur during completion of the procedure?	yes	• ***Situation not covered***
(12) Does the procedure, if significant to safety, require verification (by a second checker) to confirm that the objective of a task or series of actions has been achieved?	no	• ***Verification needed*** Note: If there is no policy requiring verification on procedures having significant safety or production loss risk, investigate **Management System** module.

CAUSE MODULE 3 – PROCEDURES

Cause Branch 3C - Wrong/ Erroneous Procedure

CAUSE BRANCH SCREENING QUESTION		Ask questions below to find causal factors if answer is :
(C) Was an occurrence caused by using a procedure which includes wrong/erroneous formats or contents?		Yes
QUESTION	**Problem If**	**CAUSAL FACTOR**
(1) Was a typographical error in the procedure responsible for the event?	yes	• ***Typo error***
(2) Was a drawing error in the procedure responsible for the event?	yes	• ***Drawing error***
(3) Was an error made in the procedure during recording or transferring data?	yes	• ***Data error***
(4) Was the technology or process applied in the procedure wrong and responsible for the event?	yes	• ***Technology wrong***
(5) Are tasks and action steps sequenced according to technical necessity and physical layout of equipment involved?	no	• ***Sequence wrong***
(6) Are the steps in the procedure factually correct (e.g. proper set points, valve numbers, valve positions/settings, etc.)?	no	• ***Facts wrong***
(7) Was an error in the formulas or calculations in the procedure?	yes	• ***Wrong computation*** Note: If independent verification was not used, investigate **Management System** module.
(8) Was the wrong revision of the procedure used?	yes	• ***Wrong revision used***

7.4 MODULE 4 - HUMAN ENGINEERING



LTA - Less Than Adequate.

Note: Human engineering deals with criteria in design and in working environment that support reliable human performance and facilitate people doing tasks in a consistently correct manner. The investigation of whether human engineering played a role in an event must be conducted on-site. The investigator/ analyst must assess available lighting, environmental factors, space requirements, and inconsistencies with human engineering principles to be able to estimate the contribution of human engineering to the human errors.

CAUSE MODULE 4 - HUMAN ENGINEERING

Cause Branch 4A - Human-Machine Interface LTA

CAUSE BRANCH SCREENING QUESTION	Ask questions below to find causal factors if answer is :
(A) Was an event caused by poor interaction/ coordination of personnel with the equipment, systems, facilities, instrumentation, or controls with which they work?	Yes

Discussion for Questions 1 to 3: If the employee located, identified, or operated the incorrect component or equipment, the investigator should walk down the error-related task(s) and assess the adequacy of the applicable labels.

QUESTION	Problem If	CAUSAL FACTOR
(1) Do labels exist on components and equipment that must be located, identified, or operated to complete the task(s) ?	no	• ***No labels***
(2) Are the labels easily read, i.e.: • Easily read under operations, and maintenance conditions? • Not obscured by other equipment? • Visible during control actuation? • Of a color that contrasts with equipment background? • Adequate contrast between lettering and label background?	no	• ***Labels difficult to read***
(3) Are the labels clear and unambiguous, i.e.: • Located close to the items they identify? • Use standard, unique names, acronyms, abbreviations, and part/system numbers? • Consistent with nomenclature used in procedures? • Distinguishable between units in multi-unit plants?	no	• ***Labels difficult to understand*** Note: If not consistent with procedures, investigate **Procedures** module.

CAUSE MODULE 4 - HUMAN ENGINEERING

Cause Branch 4A – Man-Machine Interface LTA(Continued)

QUESTION	Problem If	CAUSAL FACTOR
Discussion for Questions 4 to 12: If an error occurred while reading a display or during attempted actuation of a control, then the adequacy of the display or control itself should be evaluated.		
(4) Is the control adequately labeled, i.e.: • Discrete functional control positions identified? • Direction of motion (increase, decrease) identified?	no	• ***Control position/ movement direction not labeled***
(5) Is a relationship between the display and its associated controls obvious?	no	• ***Placement of controls LTA***
(6) Is the control adequate for the function it performs, i.e.: • Sufficient range of control? • Easily adjusted with the required level of precision? • Recognizable in terms of its function? • Of the type normally anticipated for the operation concerned?	no	• ***Functional controls LTA***
(7) Is the display's face graduated and numbered so that readings are related in a direct/ practical way to the user's task, i.e.: • Consistent with degree of precision and accuracy needed? • Indicated values do not require mental conversions? • %-indication is meaningful to task ? • Scale spans expected range of parameter?	no	• ***Display of readings LTA***

CAUSE MODULE 4 - HUMAN ENGINEERING

Cause Branch 4A – Man-Machine Interface LTA(Continued)

QUESTION	Problem If	CAUSAL FACTOR
(8) Are the visual or acoustic c***autions/ warnings*** involved in the task in question specific and unambiguous, i.e.: • Concise, short messages? • Consistent abbreviations and acronyms?	no	• ***Cautions/ warnings LTA***
(9) Alertness during monitoring diminishes over time, thus if a signal was missed, did the task require monitoring a stable indicator for greater than 30 minutes?	yes	• ***Monitoring alertness LTA***
(10) If a person involved in the occurrence could be assigned to different units/ plants, did differences in equipment or controls/ displays between the different units/ plants contribute to the occurrence?	yes	• ***Unit differences***

CAUSE MODULE 4 - NUMAN ENGINEERING

Cause Branch 4B - Work Environment

CAUSE BRANCH SCREENING QUESTION	Ask questions below to find causal factors if answer is :
(B) Did the work environment contribute to poor human performance (e.g. poor housekeeping, inadequate lighting, extreme temperatures, high radiation or contamination, or excessive noise)?	Yes

Discussion for Questions 1 to 7: Human performance can be degraded by environmental stress factors. The investigator should determine whether any of these stressors were present at the time the error was made. The investigator should walk-through the work areas and interview personnel involved to evaluate whether excessive physical stresses contribute to the occurrence:

QUESTION	Problem If	CAUSAL FACTOR
(1) Poor housekeeping (e.g. were labels obstructed by trash or equipment that should be stored)?	yes	• ***Poor housekeeping***
(2) Layout or placement of equipment and tools disorder?	yes	• ***Disorder layout/ placement***
(3) Temperature/ humidity?	yes	• ***Hot/ cold***
(4) Poor lighting (too much, too little, glare producing)?	yes	• ***Bad lighting***
(5) High ambient noise levels?	yes	• ***Noisy***
(6) Cramped quarters?	yes	• ***Cramped quarters***
(7) Were errors caused due to hurry under high radiation or contamination was present?	yes	• ***High radiation/ contamination***

CAUSE MODULE 4 - NUMAN ENGINEERING

Cause Branch 4C – Complex/ Non-Fault Tolerant System

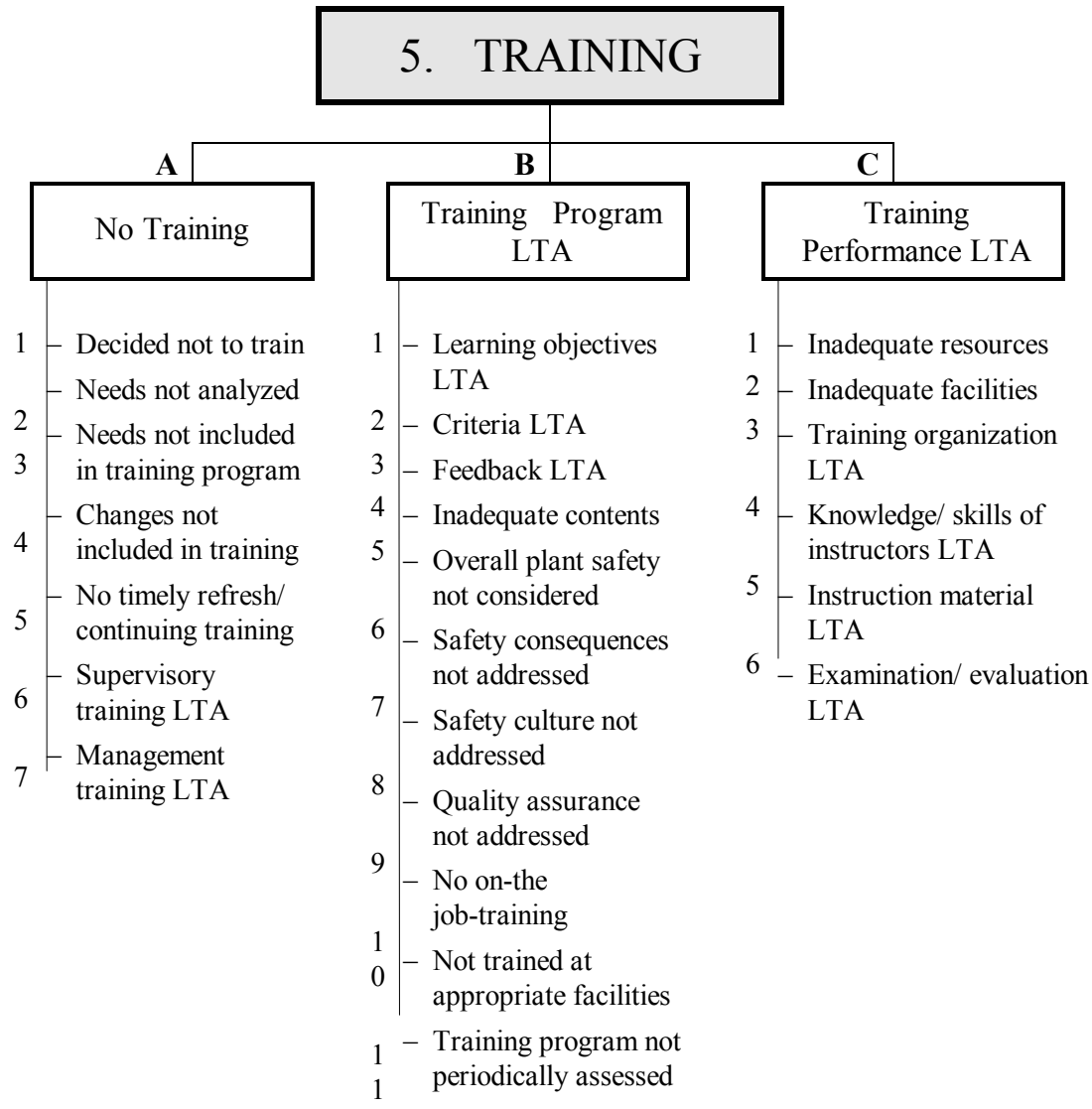
CAUSE BRANCH SCREENING QUESTION			Ask questions below to find causal factors if answer is :
(C_1)	Was a difficulty caused by the system being overly complex or complicated?		Yes
(C_2)	Was a knowledge-based decision routinely required when a simpler decision could have been required by a better designed system?		Yes
(C_3)	Was monitoring of more than 3 simultaneous variables required which caused confusion or indecisiveness that caused the occurrence?		Yes
(C_4)	Were errors undetectable or did the system not allow the correction of errors once detected?		Yes
	QUESTION	**Problem If**	**CAUSAL FACTOR**
(1)	Were personnel required to monitor an excessive number of items or variables simultaneously, causing personnel to overlook of fail to notice necessary information?	yes	• ***Monitoring more than 3 items at once***
(2)	Was difficulty caused by a situation or system routinely a knowledge-based decision for a successful out come when a simpler decision could have been required by a better designed system?	yes	• ***Knowledge based decision required***
(3)	Were safety-related systems or equipment errors undetectable before a failure or occurrence happened?	yes	• ***Error not detectable***

CAUSE MODULE 4 - HUMAN ENGINEERING

Cause Branch 4C – Complex/ Non-Fault Tolerant System (Continued)

QUESTION	Problem If	CAUSAL FACTOR
(4) If a control was accidentally actuated (bumped), is accidental actuation of the control minimized, i.e.: • Location and orientation of controls such to minimize accidental actuation? • Controls physically guarded to prevent accidental actuation?	no	• ***Error not relievable***
(5) Were errors not recoverable before a failure occurred?	yes	• ***Error not recoverable***

7.5 MODULE 5 - TRAINING



LTA - Less Than Adequate.

Note: Training as a contributor to an event may indicated if an individual failed to perform or failed to correctly perform a required task that was involved in the event. The investigation of training includes an assessment of the training program and its documentation, discussions with other operating and supervisory persons, and discussion with personnel in the training department. The investigator/ analyst should determine if the training problem is specific to a single individual, or reflects a programmatic deficiency. The assessment should cover both the initial training and the continuing training to determine whether the trainees were provided with the qualification to perform the job of interest and to maintain the job proficiency.

CAUSE MODULE 5 – TRAINING

Cause Branch 5A - No Training

CAUSE BRANCH SCREENING QUESTION		Ask questions below to find causal factors if answer is :
(A) Was the occurrence caused by a lack of training on a particular person or subject?		Yes
QUESTION	**Problem If**	**CAUSAL FACTOR**
(1) Was there a decision that no training should be provided to the worker involved in the occurrence or in the area of the task related?	yes	• ***Decided not to train***
(2) If the workers who performed tasks involved in an occurrence received no tasks related training, were special needs of training for those tasks analyzed?	no	• ***Needs not analyzed***
(3) Were needs of training for those identified tasks included in the training program and implemented?	no	• ***Needs not included in training program***
(4) If the occurrence involved changes in equipment, procedures, or job duties, were those changes incorporated in the training program and implemented?	no	• ***Changes not included in training***
(5) If the workers who performed the tasks infrequently (e.g. once in more than 6 - 12 months), did the workers received refresh/ continuing training in an appropriate interval?	no	• ***No timely refresh/ continuing training***
(6) Was supervisor provided with adequate supervisory training in leadership and co-ordination?	no	• ***No relevant supervisory training***
(7) Was management personnel provided with adequate training in managerial techniques and skills?	no	• ***No relevant management training***

CAUSE MODULE 5 – TRAINING

Cause Branch 5B - Training Program LTA

CAUSE BRANCH SCREENING QUESTION		Ask questions below to find causal factors if answer is :
(B) Was the occurrence caused by deficiencies in the training program in learning objectives, contents or methods to perform the tasks?		Yes
QUESTION	**Problem If**	**CAUSAL FACTOR**
(1) Were the learning objectives established to provide adequate training on all aspects of the tasks of interest?	no	• ***Learning objectives LTA***
(2) Were criteria established in scope, depth, and level of detail to develop the training program?	no	• ***Criteria LTA***
(3) If a similar occurrence happened before, are lessons learned form operational experience incorporated in a timely manner into the training program?	no	• ***Feedback LTA***
(4) Were the following contents included in the personnel training: • Systems/ components being operated or worked on? • Tools/ equipment used to perform tasks? • Procedures/ references to perform tasks?	no	• ***Inadequate contents***
(5) Did the training contents include topics on relations of the tasks performed to the overall plant operations?	No	• ***Overall plant operations not considered***
(6) Did the training contents include potential consequences of inappropriate actions to the plant safety?	no	• ***Safety consequences not addressed***

CAUSE MODULE 5 – TRAINING

Cause Branch 5B - Training Program LTA (Continued)

QUESTION	Problem If	CAUSAL FACTOR
(7) Did the training contents include safety culture requirements and practices?	No	• ***Safety culture not addressed***
(8) Did the training contents include job quality (performance) and quality assurance (QA) standards?	No	• ***Quality assurance not addressed***
(9) Did the training program include adequate structured on-the job training to practice learned knowledge and skills?	no	• ***No on-the job-training***
(10) Were the personnel trained at appropriate facilities (e.g. part-task simulator, full simulator, or mock-up), if required?	no	• ***Not trained at appropriate facilities***
(11) Was the training programme regularly assessed for its improvement?	no	• ***Training programme not periodically assessed***

CAUSE MODULE 5 – TRAINING

Cause Branch 5C - Training Performance LTA

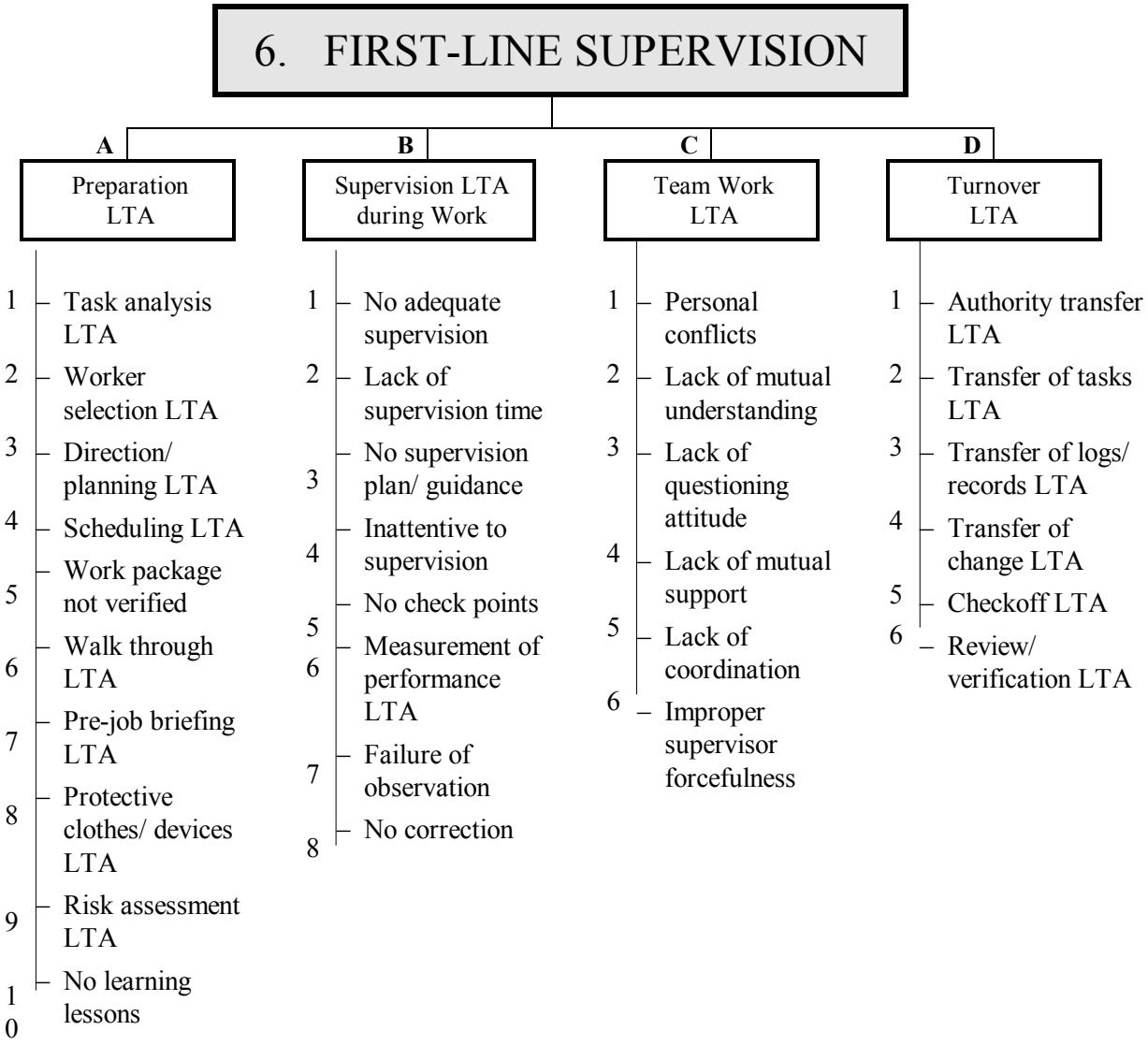
CAUSE BRANCH SCREENING QUESTION		Ask questions below to find causal factors if answer is :
(C) Was the occurrence caused by deficiencies because the training was not performed adequately due to inadequate training organization, instructors, materials or any detailed arrangements?		Yes
QUESTION	**Problem If**	**CAUSAL FACTOR**
(1) Were adequate resources available to support the implementation of the training program?	no	• ***Inadequate resources***
(2) Were adequate facilities (classrooms, teaching aids, etc.) available to support the implementation of the training program?	no	• ***Inadequate facilities***
(3) Did the training organization have sufficient qualified staff, level of authority, specified responsibilities and sufficiently supported by the plant management?	no	• ***Training organization LTA***
(4) Were the professional knowledge and skills of the instructors adequate to implement the training program?	no	• ***Knowledge/ skills of instructors LTA***
(3) Was the instruction material provided to the trainees accurately reflect or simulate the actual job circumstances?	no	• ***Instruction material LTA***
(4) Was the instruction material provided to the trainees complete, legible, and with all necessary drawings, figures, tables etc?	no	• ***Training Performance LTA – instruction material LTA***
(5) Were the presentations clear, aids material (handouts, slides, etc.) available, pace of teaching appropriate?	no	• ***Training Performance LTA – presentations LTA***

CAUSE MODULE 5 – TRAINING

Cause Branch 5C - Training Performance LTA (Continued)

QUESTION	Problem If	CAUSAL FACTOR
(6) Were the trainees appropriately evaluated (e.g. through examination and performance of tasks) during and upon completion of training to ensure mastery of required knowledge and skills?	no	• ***Examination/ evaluation LTA***

7.6 MODULE 6 - FIRST-LINE SUPERVISION



LTA - Less Than Adequate.

Note: Supervisory problems are in many cases underlying causes of an event and are obvious during interviews of the personnel involved and walkthroughs of the sites affected. Usually, the level of supervision required or the optimal amount of the supervisory involvement in a task is a function of:

- Workers' training and experience,
- Level of detail of procedures,
- Communication and timing requirements between work groups
- Frequency of task performance,
- Impact of the task on the plant safety.

CAUSE MODULE 6 - FIRST-LINE SUPERVISION

Cause Branch 6A - Preparation LTA

CAUSE BRANCH SCREENING QUESTION			Ask questions below to find causal factors if answer is :
(A_1)	Did an occurrence happen because of the inadequacies in the level of workers training and experience, level of details of procedures, verbal communication requirements, and plant safety indications, etc.		Yes
(A_2)	Was an occurrence caused by failure of first-line supervision to provide adequate preparation (including capable workers, job plans, or walk-throughs) for a job/ task?		Yes
	QUESTION	**Problem If**	**CAUSAL FACTOR**
(1)	Was the task not adequately analyzed in advance by the supervisor before it was assigned to the worker for performance?	no	• ***Task analysis LTA***
(2)	Did immediate supervision assign capable workers to perform the job? (e.g. workers who have worked excessive overtime, workers who have impaired capabilities due to substance abuse problems, or workers who have not completed required training for a particular job)?	no	• ***Worker selection LTA***
(3)	Did immediate supervisor provide any direction or planning for the task implementation (especially if the worker performing the task was new or not well-trained or less practiced)?	no	• ***Direction/ planing LTA***
(4)	If the schedule of the task was not compatible with the actual workload or other approved plant activities:		

CAUSE MODULE 6 - FIRST-LINE SUPERVISION

Cause Branch 6A - Preparation LTA (Continued)

QUESTION	Problem If	CAUSAL FACTOR
(a) Did rushing due to excessive workload cause an error?	yes	• ***Scheduling LTA***
(b) Was the contrary to other plant activities attributable to the error?	yes	• ***Scheduling LTA***
(5) Did immediate supervision verify the correctness, completeness, or otherwise appropriateness of the work package?	yes	• ***Work package not verified***
(6) If the task was performed on the wrong equipment or with a wrong procedure, did immediate supervision perform an adequate walk-through (inspect work areas, check equipment and procedure, etc.) with workers before starting the work?	no	• ***Walk through LTA***
(7) Was the pre-job briefing to workers by immediate supervision incorrect, incomplete, of inadequate such that the workers did not understand the objectives, did not have all the information necessary to perform the job correctly?	yes	• ***Pre-job briefing LTA***
(8) Did the occurrence happen because the worker was not provided with adequate personal protective clothes/ devices?	yes	• ***Protective clothes/ devices LTA***
(9) Was performing of the task involved risks so that technical specifications would be violated, or safety system functions would be inappropriately defeated?	yes	• ***Risk assessment LTA***
(10) Did the supervisor inform the workers of previous events caused by doing the similar job inadequately?	no	• ***No learning lessons***

CAUSE MODULE 6 - FIRST-LINE SUPERVISION

Cause Branch 6B - Supervision LTA During Work

CAUSE BRANCH SCREENING QUESTION		Ask questions below to find causal factors if answer is :
(B) Was occurrence caused by inadequate or lack of barriers and controls that should have been provided by the supervisor?		Yes
QUESTION	**Problem If**	**CAUSAL FACTOR**
(1) Did immediate supervision fail to provide adequate support, coverage, or oversight during task performance?	yes	• ***No adequate supervision***
(2) In addition to doing his own work, did the supervisor have enough time to supervising his subordinates?	no	• ***Lack of supervision time***
(3) Did the supervisor have a supervision plan or guidance to monitor the work performance?	no	• ***No supervision plan or guidance***
(4) Did the supervisor attentively and seriously carry out the supervisory functions during work process?	no	• ***Inattentive to supervision***
(5) Did the performance of supervision include checks at established hold or surveillance points?	no	• ***No check points***
(6) Did the supervisor have adequate means to measure the performance of individual workers?	no	• ***Measurement of performance LTA***
(7) Did the supervisor make an effort to timely observe activities performed by the team?	no	• ***Failure of observation***
(8) Did the supervisor make an effort to timely correct performance errors, deficiencies, or weaknesses?	no	• ***No correction***

CAUSE MODULE 6 - FIRST-LINE SUPERVISION

Cause Branch 6C - Team Work LTA

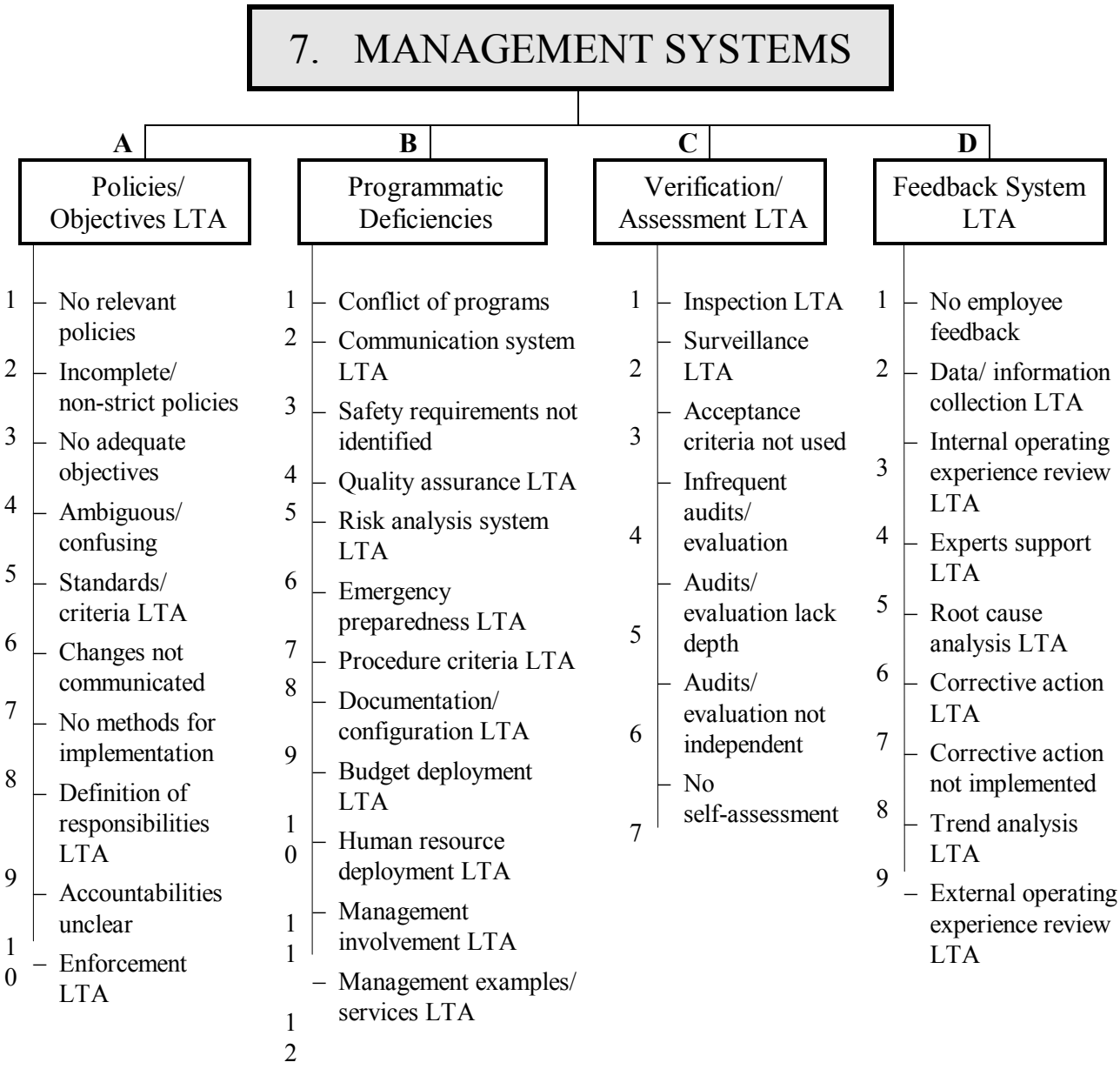
CAUSE BRANCH SCREENING QUESTION		Ask questions below to find causal factors if answer is :
(C) Supervisor is responsible for the team building. Was the occurrence caused by a poor response of the operating team because of poor team work?		Yes
QUESTION	**Problem If**	**CAUSAL FACTOR**
(1) Were there are any conflicts between individuals of the team which have affected work performance?	yes	• ***Personal conflicts***
(2) Was the occurrence caused by lack of mutual understanding among team members?	yes	• ***Lack of mutual understanding***
(3) Were directions by the supervisor understood by the team members to be improper but were carried out without questioning?	yes	• ***Lack of questioning attitude***
(4) Was there a healthy working environment among the team members to support each other's work?	no	• ***Lack of mutual support***
(5) Was each of the team members' work coordinated well by the supervisor?	no	• ***Lack of coordination***
(6) Did the team members fail to question improper readings or indications because of the supervisor's forcefulness?	yes	• ***Improper supervisor forcefulness***

CAUSE MODULE 6 - FIRST-LINE SUPERVISION

Cause Branch 6D - Turnover LTA

CAUSE BRANCH SCREENING QUESTION		Ask questions below to find causal factors if answer is :
(D) Supervisors are responsible for the correct shift turnover. If an occurrence happened in the second shift, did the turnover with the first shift affect the development of the occurrence?		Yes
QUESTION	**Problem If**	**CAUSAL FACTOR**
(1) Was the supervisory authority properly transferred and accomplished during shift turnover?	no	• ***Authority transfer LTA***
(2) Were the tasks being performed appropriately transferred and understood during shift turnover?	no	• ***Transfer of tasks LTA***
(3) Did incorrect, incomplete, or otherwise inadequate turnover of logs, protocols and other important records during shift relief contribute to or fail to prevent the occurrence?	no	• ***Turnover of logs and records LTA***
(4) Were any changes or abnormal situations described to and made understood the second shift personnel?	no	• ***Turnover of changes LTA***
(5) Were any configuration changes, records and other conditions checked off during the shit turnover?	no	• ***Checkoff LTA***
(6) Were any configuration changes and records reviewed and verified by the second shift personnel?	no	• ***Review and verification LTA***

7.7 MODULE 7 - MANAGEMENT SYSTEMS



LTA - Less Than Adequate.

Note: The Management Systems module refers to the organizational factors and administrative controls, by which the work is accomplished, employees are motivated, and problems are discovered and corrected. Assessment of the management systems should be performed through interviews with personnel (including managers at adequate levels) associated with the event, and reviews of relevant documents related to the plant policies, programs and administrative procedures. The conclusions will address deficiencies of the management systems rather than the errors committed by individual managers.

CAUSE MODULE 7 - MANAGEMENT SYSTEMS

Cause Branch 7A - Policy/ Objectives LTA

CAUSE BRANCH SCREENING QUESTION			Ask questions below to find causal factors if answer is :
(A_1)	Was the event caused by policies and objectives, which were no-existing, confusing, incomplete or not strict enough or otherwise inadequate?		Yes
(A_2)	Were the policies and objectives not used, adhered to, followed or intentionally followed incorrectly?		Yes
QUESTION		**Problem If**	**CAUSAL FACTOR**
(1)	Was there a written up-to-date policy or policies relevant to the problems likely to be encountered during the conduct of tasks and necessary to ensure the task quality and work safety?	no	• ***No relevant policies***
(2)	Was the policy or policies incomplete, non-strict or inadequate to provide principles and requirements for work performance and control?	yes	• ***Incomplete/ non-strict policies***
(3)	Were adequate objectives established with respect to the policies and specified to the individual tasks performed?	no	• ***No adequate objectives***
(4)	Was the policies or management objectives ambiguous, confusing, difficult to understand or interpret?	yes	• ***Ambiguous/ confusing***
(5)	Were appropriate standards and criteria used for implementing the policies/ objectives and for determining the effectiveness of the implementation?	yes	• ***Standards/ criteria LTA***
(6)	Have policies, objectives or their priorities been recently changed and not informed the personnel involved in the event?	yes	• ***Changes not communicated***

CAUSE MODULE 7 – MANAGEMENT SYSTEMS

Cause Branch 7A – Policies/ Objectives LTA (Continued)

QUESTION	Problem If	CAUSAL FACTOR
(7) If a policy or objective was not followed or intentionally followed incorrectly, was a practical method provided for correct implementation, and for observing and correcting mistakes?	no	• ***No method for implementation***
(8) Was there a clear written statement of responsibilities within the relevant organizational structure, which was understood by throughout the organization?	no	• ***Definition of responsibilities LTA***
(9) If failure to perform a required activity caused an event, was accountability for the consequence of the failure appropriately defined and understood in advance?	no	• ***Accountability not clear***
(10) Has failure to follow policies and objectives gone uncontrolled and uncorrected because of no enforcement measures and examples?	yes	• ***Enforcement LTA***

CAUSE MODULE 7 - MANAGEMENT SYSTEMS

Cause Branch 7B - Programmatic Deficiencies

CAUSE BRANCH SCREENING QUESTION			Ask questions below to find causal factors if answer is :
(B_1)	Did the event reflect wide spread problems/ weaknesses in the organization?		Yes
(B_2)	Could have the event been prevented by management involvement in review and correction of deficiencies in any management programs?		Yes
QUESTION		**Problem If**	**CAUSAL FACTOR**
(1)	Was failure in performing a particular task attributable to the conflict in different programs or in their implementation?	yes	• ***Conflict of programs***
(2)	Did the event occur due to lack of an adequate system for communication of policies, objectives and management concerns to the personnel?	yes	• ***Communication system LTA***
(3)	Were all safety requirements, including regulations, internal standards and customer's requirements, identified, communicated and applied in the task performance?	no	• ***Safety requirements not identified***
(4)	Was failure in performance due to lack of a system to identify and implement relevant quality assurance requirements?	yes	• ***Quality assurance LTA***
(5)	Was there a mechanism to systematic analysis of risks associated with the tasks by using adequate methods and techniques?	no	• ***Risk analysis system LTA***
(6)	Was emergency plan and procedures provided to response and mitigate the impacts of the event?	no	• ***Emergency preparedness LTA***

CAUSE MODULE 7 – MANAGEMENT SYSTEMS

Cause Branch 7B – Programmatic Deficiencies (Continued)

QUESTION	Problem If	CAUSAL FACTOR
(7) Were there specific criteria established, made aware of and used for the writing of procedures?	no	• ***Procedure criteria LTA***
(8) Do drawings or prints that were used during the event reflect current 'as built' conditions?	no	• ***Documentation/ configuration LTA***
(9) Were adequate budgets provided to the organization unit and activities devoted to the assurance of quality and nuclear safety?	no	• ***Budget deployment LTA***
(10) Were adequate human resources provided to the organization unit and activities devoted to the assurance of quality and nuclear safety?	no	• ***Human resources deployment LTA***
(11) Was the event related to that management did not understand and was not involved in the work process?	yes	• *Management involvement LTA*
(12) If the event involved a safety culture issue, did the management fail to provide examples and/or services during the work process?	yes	• *Management examples/ services LTA*

CAUSE MODULE 7 - MANAGEMENT SYSTEMS

Cause Branch 7C - Verification/ Assessment LTA

CAUSE BRANCH SCREENING QUESTION			Ask questions below to find causal factors if answer is :
(C_1)	Could have the event been prevented by having adequate verification/ assessment programs to discover and correct the underlying causes?		Yes
(C_2)	Could have the event been prevented by management involvement in self-assessment of performance deficiencies and organizational weaknesses?		Yes
QUESTION		**Problem If**	**CAUSAL FACTOR**
(1)	Were inspections performed at the line organizations independent enough to verify the task performance and results?	no	• ***Inspection LTA***
(2)	Was surveillance performed regularly by independent or supervisory personnel during the task performance?	no	• ***Surveillance LTA***
(3)	Was performance assessed against the established specifications and/or acceptance criteria?		• ***Acceptance criteria not used***
(4)	Were audits or evaluation performed too infrequently to detect the deficiencies?	yes	• ***Infrequent audits/ evaluation***
(5)	Were audits or evaluation not performed thoroughly enough to detect the deficiencies in the equipment or systems?	yes	• ***Audits/ evaluation lack depth***
(6)	Did failure to provide independent audits or evaluation contribute to the event?	yes	• ***Audits/ evaluation not independent***
(7)	Was periodic self-assessment (including management self-assessment) conducted to identify the weakness in organizations or potential performance problems?	no	• ***No self-assessment***

CAUSE MODULE 7 - MANAGEMENT SYSTEMS

Cause Branch 7D - Feedback System LTA

CAUSE BRANCH SCREENING QUESTION			Ask questions below to find causal factors if answer is :
(D_1)	Were employee suggestions, which would have prevented the event, not received and reviewed?		Yes
(D_2)	Was an event caused by failure to provide corrective actions for known deficiencies, by corrective actions inadequate or not implemented timely?		Yes
(D_3)	Was an event caused by failure to analyze performance trends based on review of operational experience?		Yes
QUESTION		**Problem If**	**CAUSAL FACTOR**
(1)	Was employee feedback, which would have prevented the event was not by management and/or by the plant feedback system? There may be one of following reasons: • Did the employee concerns fail to reach the adequate level of management that could initiate effective corrective actions? • Did the feedback system fail to provide prompt response to the employee suggestions? • Did employee believe they should not report problems unless they had a solution of the problem? • Is there no formal system or mechanism to pass employee feedback to senior management?	yes	• *No employee feedback*
(2)	Was there an investigation system for timely collection of internal data/ information related to operational events?	no	• ***Data/ information collection system LTA***

CAUSE MODULE 7 – MANAGEMENT SYSTEMS

Cause Branch 7D – Feedback System LTA (Continued)

QUESTION	Problem If	CAUSAL FACTOR
(3) Was personnel interview adequately performed in a blame-free environment to ensure the objectivity and correctness of the information obtained?	no	• ***Interview of personnel LTA***
(4) Was the failure a single occurrence (i.e., never happened before)?	no	• *Internal operating experience review LTA*
(5) Were events significant to safety adequately analyzed to identify the root causes for the purpose of prevention of recurrence?	no	• ***Root cause analysis LTA***
(6) Were sufficient and qualified experts from the plant and out-side provided as support if necessary for analysis of root causes of events?	no	• ***Experts support LTA***
(7) Was corrective action for known deficiencies not recommended, or was implemented corrective action unsuccessful in preventing recurrence?	yes	• *Corrective action LTA*
(8) Was recommended corrective action for a known deficiency not timely implemented or installed before recurrence of the deficiency?	yes	• *Corrective action not implemented*
(9) Could trend analysis of operational experiences suggest effective corrective actions which should have prevented an event?	yes	• *Trend analysis LTA*
(10) Was event caused by a problem that had occurred at other facilities but was not corrected at this facility because of inadequate dissemination and analysis of industry trends and operating experience?	yes	• *External operating experience review LTA*

8. GUIDANCE FOR DETERMINATION OF ROOT CAUSES

Modern safety practices in the nuclear industry build on: 1) application of the lessons learned from past events in the plant operations and maintenance; and 2) sharing of operational experience either by direct information exchange or via international organizations. PRCAP brings a logical structure as well as consistency to the systematic analysis of operational events. Without the structure and consistency full benefit would not be derived from operational experience evaluations.

Effective plant safety management relies on proper evaluation of the causes of operational events. Each operational event presents opportunities to improve safety as well as operability. The effectiveness of the event analysis efforts is at first measured by their ability of identifying the ***direct cause of an event***. Usually the identification of a direct cause of an event is simple, and correction of the direct cause may immediately bring about a problem solution. In some cases, the direct cause might also be hidden, thus requiring extensive analysis efforts. Here the investigator/ analyst must continue the questioning process to collect enough facts to determine the direct cause.

The causes which are hidden are usually called the underlying causes. Often, the underlying cause implies latent weakness in the organizational systems, although not direct visible or readily apparent but contained in the nature of the event. Root Cause is usually included in the category of underlying causes.

During the analysis process, identified causes are pursued, step-by-step, from the direct cause through the contributing causes, until the root cause is determined. Contributing causes may be various. In addition to the three basic elements (equipment, personnel and procedures) and environmental factors, the investigator/ analyst should analyze organizational deficiencies both at the working level and at the management levels, which may be the underlying causes contributing to and resulting in the event and termed as the contributing causes.

For determining the root cause, additional questions may be used in terms of each problem, such as:

- Why was it not prevented?
- Could it occur next time?
- Did it represent a widespread programmatic deficiency?

The root cause is the fundamental reason for the event. In other words, the event was inevitable because of the existence of the root cause. By definition, a root cause can be logically identified and is correctable and, if eliminated or corrected, the event would have been prevented and/or would never recur. The root cause may also have generic implications to a broad spectrum of possible occurrences or events, and if it is corrected, all of those occurrences/events will be prevented.

Organizational deficiencies can exist anywhere in an organization and are as common at the executive management levels as at the first line organization or worker level. In fact, deficiencies at the lower organizational levels invariably mirror similar defective performances at higher levels. To understand the root cause, one must also understand the existing policies, programmes and management considerations:

- Were the causes reflect some latent weaknesses in the plant management systems ?
- Had the latent weaknesses identified in the event analysis been discussed previously ?
- What could have been done to foresee or to prevent the event ?

It is essential that the investigator/ analyst probing deeply into both the occurrences and the conditions that create the unwanted situations. The investigator/ analyst should look beyond the errors and failures that immediately precipitated them. The analysis should not be limited to the readily observable, but also include the management systems and administrative controls so that the actual root cause can be identified and the corrective actions determined that should be taken to prevent recurrence.

The root cause is the stopping point in the analysis process. The RCA team needs to have sufficient expertise and experience to stop the investigation and analysis at an appropriate organizational level for making conclusions. It is suggested that only two or more than two causal factors identified at an equal organizational level in the management system, the investigator/ analyst may explore the root cause further at a higher organizational level. It is suggested, too, wherever causal factors of an event are found in two or more than two cause modules, the questions in PORTM system should be applied again.

9. GUIDANCE FOR PRIORITIZATION OF CORRECTIVE ACTIONS

The objectives of the RCA include identifying corrective actions adequate to prevent recurrence of the event. The identification of corrective actions begins by listing causal factors for each of the problems. In order to ensure the corrective actions are viable, the following questions should be applied:

- Would the corrective actions prevent the recurrence?
- Are the corrective actions feasible?
- If the initial action of the corrective actions taken, would it be appropriate and effective?
- Does the corrective actions meet the organizational policies, objectives and priorities?
- Does the corrective action introduce new risks or affect safety of other plant systems?

Proposed corrective actions should be reviewed to ensure the above criteria have been met. Next, implementation of prioritized corrective actions should be scheduled. Those responsible for or affected by any part of the corrective actions, including their management, should be involved in the review process.

For the effective implementation of the corrected actions, a corrective action program/ plan should be established, which is based not only on the specified causes, but also on factors such as lessons learned from other facilities, appraisals and employee suggestions. A successful corrective action program requires management involvement so that necessary resources are made available. Additional questions and considerations in developing a corrective action program include:

- Does the program address all the causes?
- Does the program prioritize the corrective actions for implementation?
- Is the implementation of the corrective actions measurable?
- What are the consequences of implementing the corrective actions?
- What are the consequences of not implementing the corrective actions?
- What are the costs of implementing the corrective actions?
- Will training be required and readily prepared as part of the corrective action implementation?
- In what time frame can the corrective action program reasonably be accomplished?
- What resources are required for development and implementation of the corrective action program?
- What impacts will be present or potential for other work groups after implementation of the corrective actions?

10. GUIDANCE FOR PREPARATION OF AN ROOT CAUSE ANALYSIS REPORT

The purpose of an RCA report is to convey the results in a clear and concise language. The report constitutes a record of the analytical efforts through which the event has been examined with thoroughness, accuracy and objectivity. The report should explain the technical issues of the causal factors and describe the management systems that should have prevented the occurrences. The following points provide guidance for writing the RCA report:

1) Summarize Change Analysis

Events often occur in the context of something that deviates form the normal situations or the routines, e.g. a new person, a new procedure, re-organization, etc. Most reports were grossly deficient in identifying changes that contributed to the series of occurrences that led to the event. Therefore, the RCA report should carefully address the impacts from changes. However, the number of changes identified should not so great and only important changes, pertinent to ask question: who, where, what, when, how and why should be included.

2) Make A Summary E&CF Chart

The working E&CF chart contains much detail so it is of great value in investigation and analysis. A summary chart should be prepared and included in the report for the purpose of the concise and easy-to-follow orientation to the event sequence for the report readers, while the working chart as an attachment.

Using the E&CF chart, all causes of the event can be easily communicated to the readers with a wide variety of experience and technical background. Also the clear and logical evolution of the event presented in the chart will facilitate agreement between the report drafter and report reviewers and will minimize negative reactions from those whose performance deficiencies contributed to the occurrences.

3) Include Broken Barriers on the E&CF Chart

Broken barriers on the chart visualize the E&HP problems. By using the MORT concept, the trace of the unwanted energy channels, its transfers and interruptions will facilitate the verification of the hypothesis of the event evolution. When necessary, use the AEB technique to present interactions between the human system and the technical system for some highlighted occurrences; use the tree diagram technique to address the logic sequence of the event development.

A properly designed technical system is error tolerant. This means, it is designed and operated in such a way that errors are prevented or mitigated before they lead to events. Examples include barrier functions associated with redundancy, diversity and good

man-machine interfaces. Organizational barriers are always weak barriers. Their effectiveness depends upon human behaviors, and humans are error prone.

4) Identify the Root Cause at an Appropriate Level

Clear distinction should be made between root cause and apparent or direct cause of the event. The root cause is the fundamental reason for the event. The root cause is usually hidden and planted in the organizational structure but can be logically identified and is correctable which, if eliminated or corrected, the event would have been prevented and/or would never recur.

Deficiencies both at the working level and at the management level should be analyzed to identify the root cause. However, the RCA team needs to have sufficient expertise and experience to stop the analysis at an appropriate organizational level for making conclusions o convince everybody.

5) Prioritize Corrective Actions

The purpose of performance of the RCA is to implement corrective actions for each of the identified causes to prevent event recurrences. The RCA report should make suggestions for prioritization of corrective actions in consideration of other factors such as budget, resources, production schedules, organizational units involved and impacted etc.

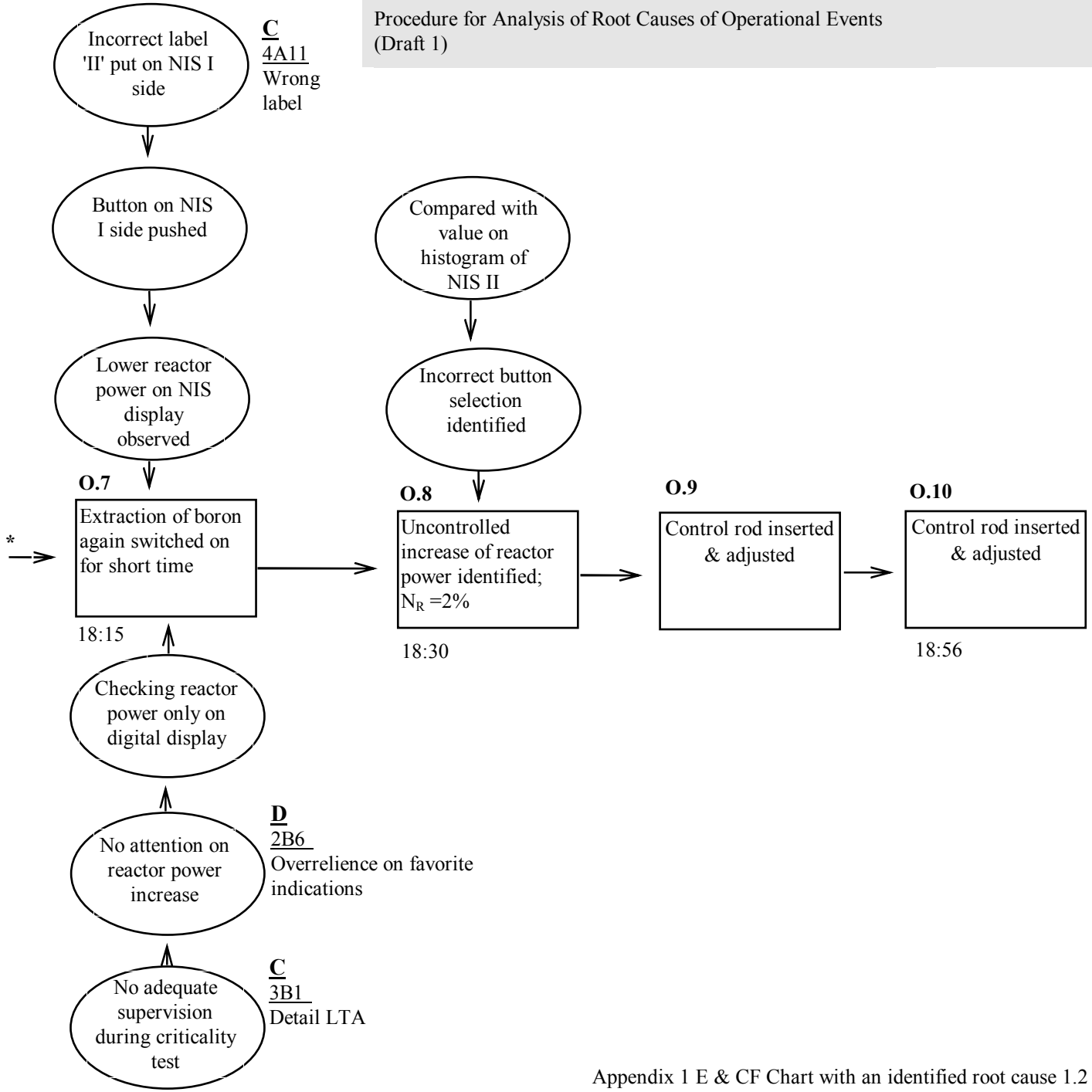
The direct cause is usually to be corrected immediately after its identification. The root cause is although the fundamental cause of the event but may only be corrected at the later stage of the implementation of the corrective action program depending on the strategy of the plant management. The effectiveness of the corrective actions should be measurable.

6) Solicit Support from PSA

Achievement of the plant operational safety is dependent on two kinds of analyses: event analysis and risk analysis. These activities are related in the sense that what has been happened in the past makes it easier to look for what can possibly happen in the future. The RCA report should solicit support from the available documents of the plant probabilistic safety assessment (PSA), if applicable, to verify the analysis results.

11. ABBREVIATIONS & ACRONYMS

AEB	Accident Evolution and Barrier
ASSET	Assessment of Safety Significant Events Teams
DOE	(US) Department of Energy
E&CF	Event and Causal Factor
E&HP	Equipment & Human Performance
HPIP	Human Performance Investigation Process
IAEA	International Atomic Energy Agency
INES	International Nuclear Event Scale
ISI	In-service Inspection
LTA	Less Than Adequate
MORT	Management Oversight & Risk Tree
PORTM	Prevention-Observation-Response-Team Performance-Management
PRCAP	Paks Root Cause Analysis Procedure
PSA	Probabilistic Safety Assessment
RCA	Root Cause Analysis
SKI	Statens Kärnkraftinspektion (Swedish Nuclear Power Inspectorate)
TQM	Total Quality Management



Appendix 1 E & CF Chart with an identified root cause 1.2

Remarks on Development of
Paks PORTM System

The Paks Root Cause Analysis Procedure (PRCAP) includes a special PORTM (Prevention - Observation - Response - Team Performance - Management) system. It was developed on the basis of the HPIP's SORTM (stimulus - Operation - response - Team Performance - Management). The following page provides a table to compare the basic elements in the PRCAP PORTM system and those in the HPIP SORTM system. The details of the PORTM system are attached as another document - Chapter 7 "Paks PORTM System"

PORTM includes five categories, namely:

- **P**REVENTION
- **O**BSERVATION
- **R**ESPONSE
- **T**EAM PEROFRMANCE
- **M**ANAGEMENT

PORTM represents a series of conditions or actions, which should have existed or should have been performed to eliminate or mitigate an occurrence. The Guidance is used for searching root causes of the operational events in the standard Paks Cause Modules. In comparison with the HPIP's SORTM, some modifications are made:

1) The first category is changed from 'Stimulus' to 'Prevention', since a module 'Equipment' is added and the starting point for RCA must be before 'Stimulus'.

2) The second category is changed from 'Operation' to 'Observation'. The intention is to address the human performance needed before an 'Operation'.

3) The term 'Response' is retained for the third category, however, the content logically includes some actions under the previous category 'Operation'.

4) The Fourth category is retained with emphasis on the performance of the cooperation and coordination activities within a team and between teams.

5) The fifth category is retained. Note that 'Management' in PORTM means the act, manner or practice of managing an business or an organization; while 'Management Systems' in the Cause Modules indicates the areas where the causal factors of an occurrence or an event may be identified.

It is understood, of course, either the structure or the contents of the present ENCONET drafts are only suggestions and subject to the comments, modifications, and agreement of the Paks management and staff.

Comparison of SORTM and PORTM Systems

HPIP - SORTM (Page E-3, Vol. 2)			PORTM (Proposed 14-06-97)		
SORTM	Description	Example(s)	**PORTM**	Description	Example(s)
Stimulus	The Stimulus category involves human performance initiators. Theses may cause an occurrence when personnel fail to become aware of important information.	An example is the operator failing to hear or see an alarm because the display is cluttered and the volume of the alarm signal is overwhelmed by the ambient noise of the workspace.	**P**revention	Prevention category reflects and searches those adverse conditions or deficiencies, which should have existed in advance to an occurrence. Those causal factors (adverse conditions or deficiencies) are cues or likely initiators of the occurrence but have neither been detected, discovered, nor been predicted by preventive actions under current practices. This category also implies to the possibility of prevention of occurrence at a very early stage.	There was an abnormal situation in technical systems or a malfunction of equipment but had neither been exposed nor discovered by an operator.
Operation	The Operation category applies to the portion of the occurrence that required mental processing of information from the stimulus.	Examples include an operator deciding that the alarm received is important and needs immediate response or an operator reading an alarm response procedure and deciding to shut a valve as part of her immediate action.	**O**bservation	Observation category addresses requisites for response to any symptoms and searches for those causal factors that contributed to failures of detection and diagnostics, such as personnel fail to be stimulated, fail to become aware of important information, fail to follow requirements or unable to process available information. Observation occurs in the control rooms by reactor operators observing indications, alarms and/or annunciators, or locally in the plant by auxiliary operators or maintenance staff performing routine inspections.	The operator failed to diagnose the abnormality or malfunction because the display was cluttered and the volume of the alarm signal was overwhelmed by the ambient noise of the workspace, or because the operator was inattentive to important information.
Response	The Response taken as a result of 'Operation' may include physical action, communications, or changes in mental states.	An example is an operator shutting a valve as an immediate response to an alarm.	**R**esponse	Response category searches for those human factors that influence, affect or hinder an operator in the control rooms or a staff anywhere to interpret the encountered symptoms, to process the available	The operator decided that the alarm received was important, needed immediate response, he read an alarm response procedure, and took

HPIP - SORTM (Page E-3, Vol. 2)			PORTM (Proposed 14-06-97)		
SORTM	Description	Example(s)	**PORTM**	Description	Example(s)
				information, or to prompt an expected pertinent action. Response taken as a result of "Observation" may include changes in mental status, communications or take physical actions. This category mainly addresses failures or weaknesses in the personal diagnostic and decision-making process.	action to shut a valve as an immediate response to the alarm.
Team Performanc e	Team Performance applies to difficulties where more than one person was involved in the applicable portion of the occurrence. This category involves shift turnover and coordination/communication efforts.	Examples include a second shift operator misunderstanding turnover information and failing to realign a system because he believed the previous shift had already completed the system realignment or an operator misunderstanding his supervisor's verbal instructions and shutting the wrong valve.	**T**eam Performance	Team Performance category applies to problems or difficulties where more than one person is involved and searches for those causal factors affecting team performance or decision-making process, or unable to prompt expected actions by the team. This category addresses cooperation, coordination and feedback mechanism within the team and is devoted to identification of problems in turnovers or other interface problems between different teams.	A second shift operator mis-understood turnover information and failed to realign a system because he believed the previous shift had already completed the system realignment, or he misunderstood his supervisor's verbal instructions and shut the wrong valve.
Managemen t	The Management category applies for the applicable portion of the occurrence that involves management factors. These include organizational and staffing issues, failure to implement corrective action for repetitive failures, and problems with the safety culture that lead to violation of safety policies.	An example would be an operator's failure to fill-out a required, safety-related procedure because he was in a hurry to get the job done to meet a production schedule target.	**M**anagemen t	Management category applies to and searches for those supervisory and managerial factors (organizational and administrative factors), which affect the effective E&H performance and contribute to occurrences or other causes. Included are policies, objectives, staff and resources, authority and responsibilities, management programs and systems, including safety culture, quality assurance program, feedback systems, and etc.	The operator failed to fill-out a required, safety-related procedure because he was in a hurry to get the job done to meet a production schedule target.

Remarks on Development of Paks Cause Modules

The Paks Root Cause Analysis Procedure (PRCAP) includes seven Cause Modules (Equipment, Personnel, Procedures, Training, Human Engineering, Supervision, and Management) for categorization of causes (causal factors) of operational events with the addressing of the human performance. The following page provides a table to compare the basic branches in each of the PRCAP Modules with that in the HPIP Modules. The related work sheets are attached as another document - Chapter 6 "Paks Cause Modules"

It is understood, of course, either the structure or the contents of the present ENCONET drafts are only suggestions and subject to the comments, modifications, and agreement of the Paks management and staff.

(1) Equipment

This is a new module with three branches. The basic branches and related cause factors have been established as draft.

Nevertheless, the work sheets will be developed during the course of the implementation of the next contract.

(2) Personnel

The Module "Verbal Communication" in HPIP is replaced by the Module "Personnel" in the Paks Cause Modules. The contents related to communication have been all included in a branch of the Personnel Module. The Branch "Turnover LTA" is moved to the module "Supervision" because turnover is considered as a collective activities of both the whole shifts. Eliminating analysis of personnel failures in RCA is the NRC's policy. However, for an utility like Paks, personnel failure must be considered and connected to the work consequences, even if in a no-blame environment.

However, neither HPIP nor MORT includes enough analysis on failures of the human performance (as individual). The two new branches and work sheets have to be developed on the basis of the applicable part of the Human Performance Enhancement System (HPES) of the US INPO.

(3) Procedure

The main efforts made were to modify the terms in the Paks Module in order to distinguish the failure of the procedure itself and the failure of not using or not following the procedure caused by the human being. To a certain extent, branches were rearranged and some new causes were added.

(4) Human Engineering

No essential modification.

(5) Training

Significant additions were made in the Paks Module on the basis of the applicable part of HPES of the US INPO. The LTA of the training program and the performance was separated in two branches.

(6) First Line Supervision

The module title was changed from "Immediate Supervision" while the term of immediate supervision still retains in the text because it is understood that the cause factors are dealing with the immediate supervision within the first line organizations rather than at the senior or middle management levels. The branch of "Turnover LTA" was included here and separated into two branches for two different aspects of control of turnover and team work. All four branches were enlarged by incorporating the applicable part of MORT of the US DOE Guidance.

(7) Management Systems

Modification is proposed to be made to a large extent. This HPIP module includes good causal factors and work sheets. However, the branches will be reconsidered according to the Paks management practices. The contents will be enlarged by incorporating the applicable part of MORT of the US DOE Guidance.

This Paks Module on "Management Systems" will be developed during the course of the implementation of the next contract. As prerequisites, review of some Paks policy and management documents (such as safety policy statement, quality assurance program, etc.) will be necessary.

Comparison of Paks and HPIP Cause Module Branches

NRC HPIP CAUSE MODULES		PAKS PRCAP CAUSE MODULES
	(1)	**Equipment** – Functional Deficiency – Operations/ Maintenance LTA – Design / Manufacture LTA
Verbal Communication – Misunderstood Verbal Communication – No Communication or Not Timely – Turnover LTA	(2)	**Personnel** – Capabilities LTA – Attitudes LTA – Misunderstood/ Failure in Communication – Violation of Requirements/ Procedures
Procedure – Not Used – Followed Incorrectly – Wrong/ Incomplete	(3)	**Procedure** – No Way To Be Used – Ambiguous/ Incomplete Procedures – Wrong/ Erroneous Procedures
Human Engineering – Man-Machine Interface – Work Environment – Complex System – Non-Fault Tolerant System	(4)	**Human Engineering** – Man-Machine Interface LTA – Work Environment LTA – Complex/ Non-Fault Tolerant System
Training – No Training – Understanding LTA	(5)	**Training** – No Training – Training Program LTA – Training Performance LTA
Immediate Supervision – Preparation – Supervision During Work	(6)	**First Line Supervision** – Preparation LTA – Supervision LTA During Work – Team Work LTA – Turnover LTA
Management Systems – Standards, Policies, or Administrative Control (SPAC) LTA – SPAC Not Used – Management Attention and Oversight – Corrective Actions – Employee Communication/ Organizational Culture LTA	(7)	**Management Systems** – Policies/ Objectives LTA – Programmatic Deficiencies – Verification/ Assessment LTA – Feedback System LTA

Title: Method of Psychological Root Cause Analysis of Human Factors

Authors: Eduard Volkov, Vladilena Abramova

Science Research Centre “Prognoz”, Kurchatov Street 21, Kaluga Region, Obninsk, Russian Federation

www.hf-knowledge.ru

Date: 1999, 2005

1.1 PSYCHOLOGICAL ROOT CAUSE ANALYSIS OF HUMAN FACTOR

Introduction

The method was developed by use IAEA adopted concept of disposed defence in depth to prevent events, ASSET Guidelines, IAEA-TECDOC-632, 1991.

The method is used by human factor specialists in order to analyze human errors (erroneous actions).

The worker performed erroneous action is considered like an individual who has abnormalities in activity structure. Activity structure contains motivation-attitude area, cognitive area and operation mechanisms. Abnormalities in each area could define characteristics of erroneous action.

Initial stage (Investigation team first meeting)

Main goal for human factor specialist on the stage is to help the event investigation team to fix/or fix not a fact of human factor participation in the event.

Additional goal if fact of human factor is fixed – to develop information gathering plan about the event and participants.

On the stage human factor specialist takes part in first meeting of the event investigation team together with technical specialists. The team uses method "Event and causal factor charting". The method consists in stepped analysis when team members reproduce all event details and determine casual relationships between individual cases and circumstances, develop logical and chronologic sequence.

Investigation team together with human factor specialist defines what was incorrect in personnel actions, defines what knowledge, skills are necessary to implement work reliably, estimates characteristics of physical-chemical, sanitary-hygienic and ergonomic work conditions, organizational factors, also defines consequences of erroneous actions for technics, personnel and population.

Human factor specialist fulfills the following sequence of steps:

- detection abnormalities in personnel actions,
- detection abnormalities in equipment operation and procedure failures which have promoted personnel erroneous actions.

Investigation team determines kind of event: a) equipment failure, b) personnel erroneous action, c) procedure failure. Scheme of event kind determination one can see on Figure 28.

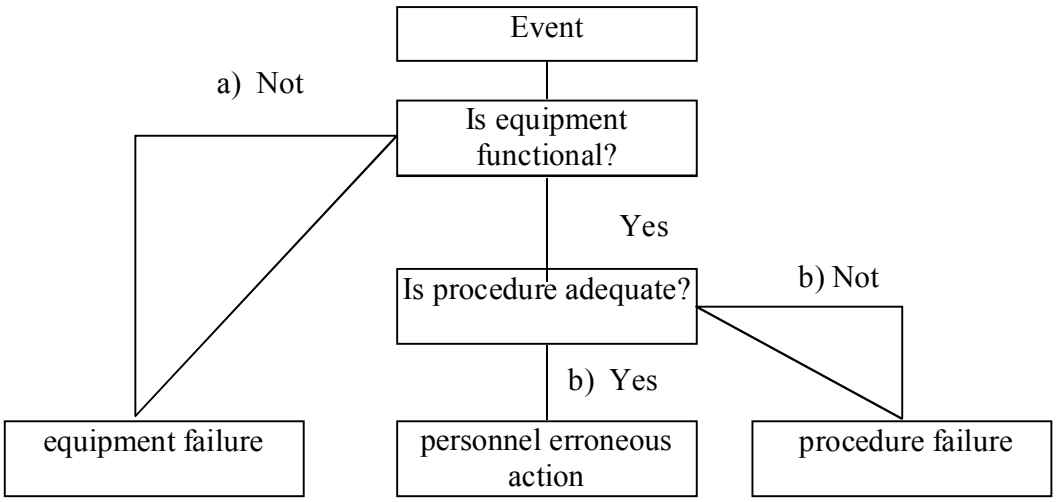


Figure 28. Scheme of event kind determination.

If investigation team fixes a fact of human factor participation in the event, human factor specialist starts to implement next stage of the psychological analysis.

To develop information gathering plan human factor specialist should use Table 1. The analysis basic elements and information sources.

Table 1. The analysis basic elements and information sources.

Analysis basic elements	**Areas of erroneous actions precursors**	**Information sources**
A. Work activity subject, who had error	1. Motivation and attitudes. 2. Job relevant individual traits. 3. Psycho-physiological traits (cognitive processes: perception, attention, memory, thinking, central nerve system characteristics) 4. Professional skills and knowledge. 5. Fitness for duty (mental overstrain, emotional overdrive, mental overwork, mental passivity, illness)	Fitness for duty control (before work) date. Data of psychological and psycho-physiological control, medicine providing. Qualification, training and knowledge examination data. Job assessment process data. Data of interviews with: - persons who had errors; - colleagues of their; - managers; - instructors.
B. Task	1. Goal and implementation plan. 2. Allocated resources:	Arrangements, orders for the task implementation. Data of interviews with :

	- time; - equipment; - documentation; - personnel.	- persons who had errors; - colleagues of their; - managers.
C. Means to implement work	1. Equipment. 2. Documentation. 3. Personnel.	Equipment analysis (ergonomic): - information display system; - controls; - instruments, - materials. Document analysis: - procedures; - instructions; - journals; - control maps.
D. Work conditions	1. Physical conditions on work place. 2. Work place organization. 3. Ergonomic shortcomings of technology. 4. Latent ergonomic errors of the project and installation when earlier stages of nuclear facility life circle. 5. Work schedule.	Work place express-analysis data. Data of interviews with: - persons who had errors; - colleagues of their; - managers.
E. Interaction, management	1. Communication (information exchange) 2. Feed back (mutual control and action correction). 3. Group dynamics (leadership, relations, conflicts)	Data of professional selection. Date of simulator training results (team work) Data of social-psychological evaluation of group dynamics (leadership, relations, conflicts and so on) Data of interviews with: - persons who had errors; - colleagues of their; - managers; - instructors.

1.6. Work results of human factor specialist on this stage are:

- list of main facts connecting with the event;
- event chronology;
- fixed/not fixed fact of human factor role in the event and list of participants (activity subjects).
- information gathering plan about event and event participants.

Information gathering

Main goal of information gathering stage – to obtain fact material on the event circumstances focusing on human factor aspect.

During information gathering human factor specialist considers these main elements (see Table 1):

- task;
- work conditions;
- means to implement work;
- personnel interactions, management;
- work activity subjects took part in the event.

In accordance with the information gathering plan human factor specialist:

- gets necessary documentation connected with work\task implementation;
- gets data about human resource management processes realization in respect of the event participants: personnel selection, job assessment, training, psychological and social support;
- gets data on work with operative personnel realization: briefings, operational meeting, on-the-job training and so on;
- conducts work place express analysis;
- conducts interview with the event participants;
- makes more exact staff members who were the event participant.

2.4. The interview goal is to remove psycho-emotional stress connecting with the events and establish acceptable conditions to collaborate the event participant.

Interview questions could be:

1) Do you see (realize) your errors in the occurred event?
   If not – how do you explain this event?
   If yes – did you know/understand what did you do when event or it was suddenly, by accident?
2) What has prevented you to behave correctly:
   - psychological state (what concrete?);
   - external disturbances (which ones?: technical, communicative, lack of good interactions with colleagues, other?)
3) What could you suggest that another workers will escape the same situation?

Human factor specialist should pay attention to last projective question of the interview. An answer on the question could be a base to make recommendations for work condition improvement.

In order to sort information gathering process it should fill special unified "casual factor modules" with obtained information, interview and observations. (Annex 6.17.1).

Then human factor specialist should generalize all marked problem issues and make more exact workers who were participants of the event.

Human factor specialist must find out have analogous events occurred, should be used documentation belonged to that event.

In final of the information gathering stage human factor specialist must formulate hypothesis on erroneous actions type and also about root causes led workers to error.

Human factor specialist work result on the stage:

- gathered, structured in accordance with Table 1 and formalized (see modules of Annex 1) information about the event and participants;
- finalized list of the event participants;
- hypothesis on erroneous action type and causes.

Direct cause and erroneous actions identification.

A goal of human factor specialist work on the stage is to detect direct reason of erroneous action and kind of erroneous action.

To detect direct cause of erroneous action human factor specialist must get answers on these following questions:

to activity object – **What was happened?**
to activity subject – **What has been done?**

Psychological analysis should be focused on workers (or group of workers) who were involved in the event. Action analysis is conducted for all activity aspects:

- information perception;
- situation assessment;
- decision making;
- action execution;
- interaction with others workers, procedures, documents.

During the process of psychological analysis it is necessary to answer on three main questions: Why? For what? How?

Questions “Why did he (they) behave that way?”, “How did he (they) assess situation to make that decision?” allow to get information about task implementation in aspects of perception and situation assessment, in particular about:

- incorrect information perception;
- incorrect information understanding;
- incorrect assessment of collected information, current situation.

Questions “For what did he (they) behave that way?”, “What goal?” allows to get information about:

- incorrect goal determination;
- incorrect determination of goal achievement conditions;
- incorrect making of activity strategy.

Question «How did he (they) act to reach a goal?” allows to get information about:

- incorrect implementation of planned actions;
- incorrect interaction during decision making process (Man-Man, Man-Procedure, Man-Documentation).

These following kind of erroneous actions could be detected:

- incorrect implementation of technological operations, influence on defense components, automatic devices;
- inactivity, lapse of necessary actions;
- installation of defective equipment;
- violation of technical service and maintenance technology;
- errors of equipment control, inspection, test and debugging;
- uncoordinated actions in group interaction when reactor operation;
- uncoordinated actions in group interaction when technical service and maintenance;
- other erroneous actions of personnel.

Human factor specialist work result on the stage:

- detected direct cause of erroneous actions (for each event participant);
- detected kind of erroneous action (for each event participant).

Erroneous action type identification.

The stage goal is to find out type of erroneous action for each event participant. Human factor specialist should use the following human error typology (Figure 29):

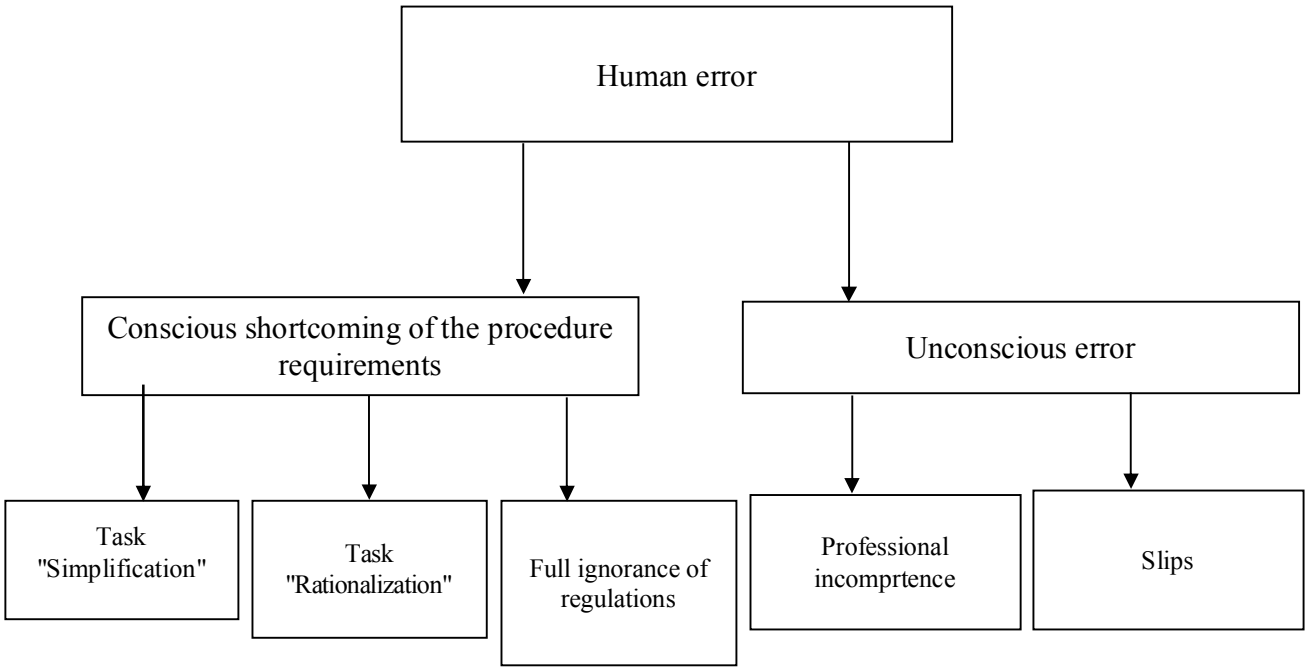


Figure 29. Human error typology

Human factor specialist forms conclusion about erroneous action type by use results of previous stages and block-schemes of erroneous action types (see Annex 2). Main indicators to detect class of erroneous action are premeditation (deliberateness) and unexpectedness (unconsciousness). As a result human factor specialist detects type of erroneous action: slips, violation or motivation error).

Human factor specialist work result on the stage:

- determination of erroneous action type for each event participant.

Erroneous action root causes identification.

A main goal of human factor specialist work on the stage is to identify root causes of erroneous actions of the personnel taken part in the event.

To do that human factor specialist must compare the information obtained in previous four stages.

Depending on found out facts during the comparison human factor specialist should get and analyze additional information about one or few aspects of an activity internal/external conditions and means (See Figure 30).

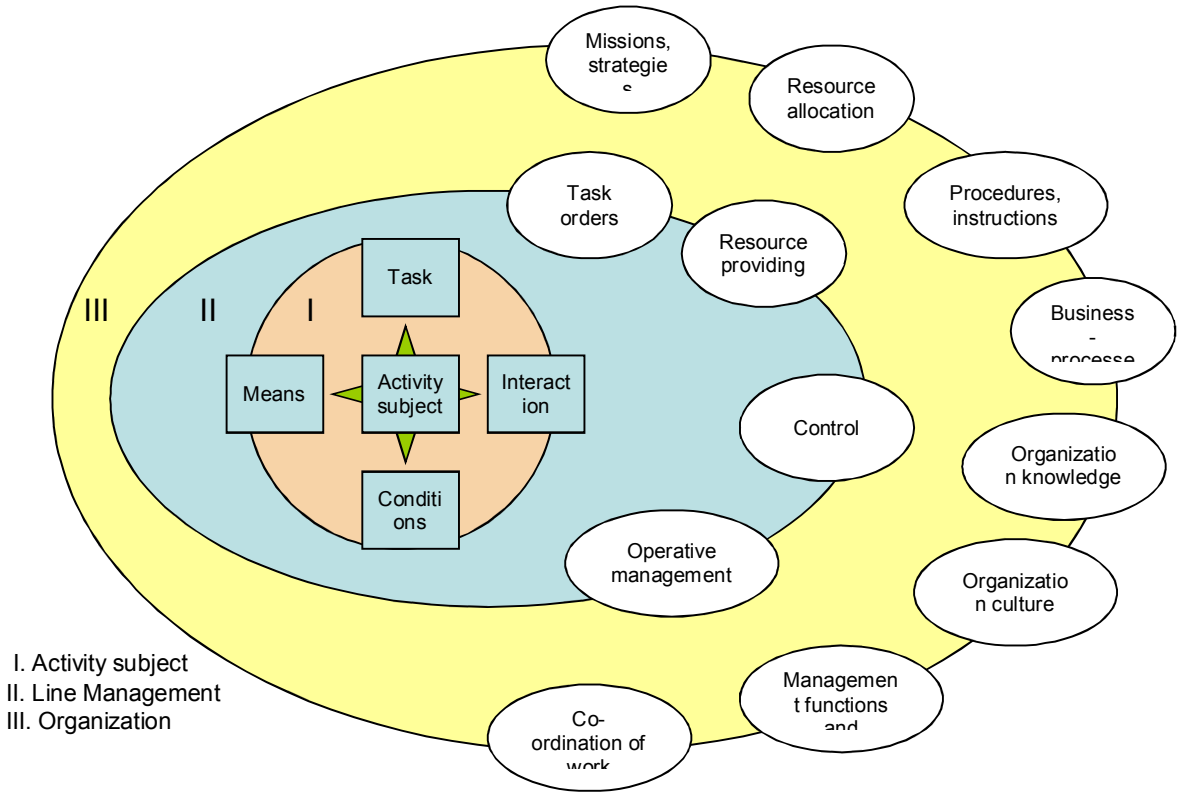


Figure 30. Internal and External activity means and conditions

Also it is necessary to take into account social psychological, social economic and political factors like an external conditions which could influence on psycho-emotional steadiness important for reliable work implementation. It could be considered for these levels:

- group/shift;
- management and organization;
- external to NPP environment (groups, project or contractor organizations and so on).

Level of activity internal means and conditions (activity subject).

These following root causes on psycho-physiological level could be present:

- when perception, the worker did not observe, did not hear signal or had seemed that the signal presents;
- delayed reaction;
- low level of stress resistance,
- lower functions of memory and thinking;
- slowness of information processing and decision making processes;
- inability to act in high risk conditions.
- sudden acute attack of disease;
- alcohol, drug intoxication.

These following root causes on motivation and attitude psychology level could be present:

- distortion of a system of social values;
- lack of interest to a work;
- low rating of a work significance;
- formal respect to a work;
- indiscipline;
- lack of duty feeling.
- lack of questioning attitude;
- lack of a loyalty to an organization

These following root causes on individual psychology level could be present:

- lack of will;
- lack of responsibility;
- unwillingness to act reasonable in changed conditions;
- uncommunicativeness;
- estrangement;
- emotional unsteadiness;
- lack of self-control.
- Habit to act stereotypically.

These following root causes on social psychology level could be present:

- inability and/or unwillingness to work in team;
- conflict behavior;
- inability to manage people;
- transfer of own negative emotions on a work environment.

These following root causes on professional knowledge, skills could be present:

- weak professional qualification;
- lack of erudition;
- lack of expertise;
- inability to use practically professional knowledge;

Level of activity external means and conditions.

These following root causes on work places and documentation ergonomics could be present:

- unpractical and uncomfortable pose;
- shortcomings of console, armchair, controls, communicative devices design and layout;
- incorrect distribution of physical and psycho-emotional load during work day;
- mismatch between temporal characteristics of work operations and ergonomics standards;
- adverse microclimate conditions;
- extreme conditions connecting with sound, light, radiation impact and so on;
- mismatch between technical equipment/documentation and human being capacities of

cognitive processes and also features in speed, power and accuracy of movements;
- mismatch between characteristics of work documentation and ergonomics standards.

These following aspects of an organizational factors level could be source of root causes:
Organization goal and strategies.
- management policy and strategic planning in support of the mission of the organization.
- business planning process;
- development and implementation of higher-level plans;
- organizational structure, accountabilities and authorities distribution;
- long term follow-up and control mechanisms, problem identification and resolution.

Management functions and oversight
- identification, development and support of managers in order to allow them to carry out their functions as required. This may include identification of good managers with leadership skills and allocation of appropriate resources to support leaders.
- empowerment, to enable managers to act on their authority;
- promotion and reinforcement of safety practices;
- definition and establishment of goals and standards;
- establishment of a framework for a reliable, traceable and efficient decision-making process;
- establishment of an information management process to identify, acquire, distribute, store and operate necessary information in a precise and timely manner;
- collection, tracking, trending and analyzing of safety and other performance information;
- promotion of an organizational learning process to identify problems and to learn from past experiences and improve performance;
- identification and resolution of problems (gather information to assess the situation, find solutions, evaluate different alternatives, implement decisions taking into account appropriate information and personnel, supervise execution, and monitor the results);
- detection and management of possible internal conflicts between safety and economical benefit;
- management of technical and organizational change;
- planning and scheduling of the work processes including workload management;
- establishment of an effective communication process with other interest groups, including the regulatory body, contractors, local public, media, trade unions, etc;
- monitoring the resource allocation process which ensures that the right people are in the right position with the appropriate support;
- establishment and monitoring of good work practices and processes (enforced by, walk around, housekeeping standards, material conditions, etc.).

Resource Allocation.
- Identification, acquisition and development of necessary know-how and technical resources;
- Balance between economic pressure, safety requirements and timetables;
- Organizational structure for resource allocation decision making process (degree of centralization);

- Control and monitoring process for human and technical resources;
- Logistics;
- Assignment of organizational (social) support;
- Involvement of Human Factors and other appropriate personnel in work design;
- Support of business planning;
- System support to operational functions.

Human resources management.

- recruitment and selection of personnel based on predetermined qualifications including experience, education, and training;
- assignment of personnel to roles, responsibilities and accountabilities as described in position descriptions and standards;
- attention to the psychological and psycho-physiological condition of available manpower;
- assignment of personnel to roles, responsibilities and accountabilities as described in position descriptions and standards;
- shift organization rules;
- working hours and overtime policies;
- staffing policies and procedures;
- adaptation of the organization to changes in technology;
- use and evaluation of contractors;
- management of job rotation and promotion;
- evaluation of motivation, performance and professional competence through formal appraisal process;
- professional evolution, career development;
- tracking reasons for staff turnover;
- job security issues;
- succession planning to anticipate and fill vacancies;
- reward and recognition system;
- appropriate support of personnel to do their jobs;
- monitoring morale and attitude relative to a safety culture.

Personnel training

- organization of the training process to ensure a continuous improvement in knowledge, skills and abilities to meet job requirements and organizational goals and strategies;
- establishment and evaluation of different types of training, e.g. initial training, refresher training, remedial training and determine different strategies for training, e.g. class room, on-the-job, distance, self-paced, simulator, etc.;
- implementing training methods and developing training materials with consideration of the development of training media and psychological aspects of learning;
- individualization of training;
- implementation of a QA process for training;
- continuous evaluation of training programs;
- training according to actual needs;
- allocation of resources needed for training including the appropriate selection of

instructors;
- periodic training for career development;
- monitoring the adequacy of instructors and materials;
- training on new technologies as needed;
- professional educational support.

Co-ordination of Work
- organization of inter-related work activities;
- identification of roles, responsibilities and delegation of responsibilities;
- shift work, shift turnover and team composition;
- inter- and intra-organizational communication and co-ordination;
- prioritization, planning and scheduling of work activities;
- planning of work to allow an appropriate workload distribution;
- logistics, assistance and support;
- management of personal workload and work-flow;
- traceability of work activities;
- coordination of contractors with licensee employees.

Organizational knowledge
- understanding of the structure of the organization and the different interfaces between organizational units;
- knowledge about formal and informal communication channels and the interrelationships between an organization's sub-systems;
- individual awareness of roles and responsibilities and one's own place in the hierarchy of the organization;
- implicit knowledge about work practices;
- corporate memory of past experiences and organizational knowledge represented by the employees;
- management of the communication of the organizational knowledge;

Procedure determination and inculcation (proceduralization).
- appropriate standardization and formalization of recurring and critical work activities taking into consideration personnel experience and knowledge;
- clear information of potential risks during activities;
- presentation of procedures based on human factors and ergonomic principles and taking into account past errors;
- participation of operators in the development, design and modification of procedures.
- administrative aids;
- administrative control, ensuring the quality of procedures in accordance with work practices and of the procedure modification process;
- good balance between the strict proceduralization and standardization of work activities and the skills and experience of the personnel;
- influence of quality management systems on proceduralization.

Organizational culture.

- safety culture as an aspect of the organizational culture where safety is a critical factor in the norms, values and attitudes of every employee throughout the organization;
- basic (shared) assumptions about how work has to be done in normal operations and in emergency situations;
- safety awareness of individuals;
- organizational support for employee socialization, i.e., important informal activities.
- reward and recognition system reinforcing safety work performance;
- attitude towards and interaction with the regulatory body;
- awareness of implicitly sanctioning certain behaviors and disapproving other behaviors;
- supervisors and peer employees acting as role models (i.e. showing acceptable behavior);
- open communication lines.

Organizational learning.

- feedback of operational experience and its utilization;
- pro-activeness instead of a re-activeness;
- transformation of individual tacit knowledge into explicit organizational knowledge;
- questioning attitude;
- promotion of common understanding of processes and responsibilities;
- learning from generic issues;
- identification, ownership and resolution of problems;
- recurrent self assessment;
- capacity and readiness to learn;
- continuous improvement.

Communications.

- information flow between the organization and other entities (e.g. the regulator and contractors);
- information flow between different layers of the organization, both vertical (between different level of management and employees) and horizontal (between different departments or projects);
- intra-organizational communication i.e. within groups, between group members;
- appropriate use of different means to convey information;
- timeliness of information transfer;
- awareness and effective application of the contents of message;
- openness from top to bottom and vice versa;
- formalization of the communication processes;
- quality of the document management process;
- tools and concepts to code and submit information;
- informal and unofficial communication practices;
- redundancy of messages;
- managerial oversight and supervision communication process;
- visual behaviour, written words, face-to-face communication.

5.5.3. These following root causes on external to nuclear facility environment could be present:

- political situation;
- legal system;
- economic conditions;
- cultural aspects;
- other institutions and organizations (for example unions);
- regulatory authorities;
- public opinion and perception;
- media reports;
- employees perception of their job status.

Human factor specialist work result on the stage:

- generalized list of erroneous action root causes (for each event participant).

Identification of erroneous action sources (areas) and safety decrease points.

A goal of human factor specialist work on the stage is to define internal and external means of personnel activity which had led to erroneous actions.

Human factor specialist identifies erroneous action sources basing on generalized list of root causes. To define safety decrease points specialist conducts investigation of the corresponding areas**.**

Human factor specialist work result on the stage:

- list of erroneous actions areas and corresponding safety decrease points.

Corrective measures development.

Human factor specialist develops corrective measures in accordance with result of the psychological analysis of human errors. Corrective measures are developed for each root cause of erroneous action.

Each worker taken part in the event should be considered like a dynamic, interrelated and interdependent element of a set of more complex systems. These systems changes influence on this worker directly, mediately, singularly or multiple. From other hand, human being is also complex and variational system.

In order to guarantee corrective measures effectiveness these following criteria must be used for each one:

- Does the corrective measure cover fully corresponding direct and root causes?
- Could the corrective measure prevent realization of direct and root causes in the future?
- Will the corrective measure have economic effect? What is a cost to realize the corrective measure? Capital cost? Operation and maintenance cost?

- Does the corrective measure allow to provide safe and reliable electric power production?
- Are all negative consequences of the corrective action fulfillment known well?
- What will be consequences of the corrective measures non-fulfillment?
- It will be needed to train personnel?

All corrective measures for each personnel shortcoming including external factors influencing on a worker's capacity for work and reliability, must be interconnected between each other, have not contradictions, must heighten positive effect on each other.

It should be taken into account when choosing corrective measures belonging to personnel:
- individual traits,
- features of value and motivation system,
- qualification,
- possibilities and restrictions in human being behavior management.

Approximate list of correction measures connecting with human factor is represented in the Table 2.

Table 2. Correction measures list, human factor aspect.

Event causes areas	**Corrective measures**
Production culture, including safety culture	1. Adoption of a system of discipline regulation. 2. Improvement work organization (ergonomic expertise of work places and technological processes, work conditions, production esthetics). 3. Training course "Safety culture". 4. Training on development of psychological attitude for safe work. 5. Business games and social psychological training to develop responsible respect to job implementation and safety. 6. Development of encourage/punishment system. 7. Conducting focused interview with workers who had erroneous actions.
Social self-control	1. Communicative training. 2. Group interactions improvement.
Psycho-physiological self-control	1. Psychological training on self-control development and supporting capacity to work. 2. Adherence of work and rest regimes.
Attention and memory	1. Training for memory and attention.
Steadiness to stress, monotony	2. Psychological training on steadiness to stress. 3. Autogenic training.
Fitness for duty	1. Enhancement of functional resources. Prevention of nervous-mental tension.

	2. Rehabilitation procedure in accordance with medicine recommendations. 3. Enhancement of fitness for duty control procedure before work.
Professional knowledge and skills	1. Lack of knowledge elimination. 2. Improvement of training quality. 3. Use of human factor specialist in simulator training. 4. Development of encourage system for professional competence. 5. Improvement of operating experience process. **6.** Improvement of manager's role to inform personnel about psychological root cause analysis of human factor results.
Normative documentation, regulations	1. Technical and psychological expertise of the documentation. 2. Making document edition. 3. Training.
Organizational factors	1. Monitoring of organizational factors dynamics. 2. Monitoring of cultural climate dynamics in groups. Diagnosis of personnel moral values dynamics. 3. Communicative training. 4. Use of psychological knowledge for human resource management processes.

Preparation of final conclusion.

A goal of human factor specialist on this stage is to prepare report (conclusion) containing results of fulfilled psychological analysis and to give it for investigation Team Leader. The report has unique form which must be filled. It is used like a part of the event report.

Annexes

ANNEX 6.17.1 Casual factor modules

Structure of these casual factor modules is based on a structure of Table 1 "The analysis basic elements and information sources" and are used to fix information about all analysis basic elements when information gathering stage.

Set of modules A «Activity subject»

Module A-1 «Motivation and attitudes»

1	**Why motivation was inadequate?**	Rate

1.1	The work was unplanned for the worker, поручена как наказание	
1.2	The work has been charged like a punishment	
1.3	The worker had not been informed about task	
1.4	Briefing before work was not so clear for the	
1.5	The worker tries often to escape an implementation of such tasks	
1.6	The worker tries to implement work better than usually	
1.7	The worker tried to implement the work quickly, so it was necessary to finish before shift turn.	
1.8	The job was ordered by no “good” manager and the worker wanted to “show him his place”	
1.9	The worker had intention «to leave the job for next shift»	
1.10	The worker followed strictly to manager’s order, though known that it is incorrect to do that.	
1.11	The worker has taken the blame upon oneself in order to not spoil relations with manager.	
1.12	Other (please, write):	

Module A-2 «Job relevant traits»

2	**Why JRPT were inadequate?**	Rate
2.1	The worker rare implements job carefully and honestly, tries to shift own duties to others	
2.2	The worker is dependent, implements job well only when leaded by manager	
2.3	The worker risks often and groundlessly	
2.4	The worker is not disciplined, not exigent to oneself, negligent	
2.5	The worker has difficulties when team work	
2.6	The worker needs to be under control	
2.7	The worker has protest feeling when there is necessity to obey regulations, orders	
2.8	The worker makes thoughtless decisions too fast and easily	
2.9	The worker, when erroneous activity, was at odds with somebody	
2.10	The worker has bad habits (alcohol and so on)	
2.11	The worker has a weak psychological readiness to work	

2.12	Other (please, write):	

Module A-3 «Psycho-physiological traits»

The module is destined to indicate presence of inadequate psycho-physiological traits indicators (cognitive processes: perception, attention, memory, thinking, central nerve system characteristics) and conditions promoting a display of them.

3	**Psycho-physiological traits were inadequate?**	Rate
3.1	The worker is irritated, unsteady, quarrelsome often.	
3.2	The worker endures routine tasks and monotony very bad.	3
3.3	The worker is absent-minded, inattentive, concentrates hardly on a task.	
3.4	The worker has difficulties in work implementation when time pressure.	
3.5	It is hardly for the worker to estimate work conditions.	
3.6	The worker has delayed reaction on incoming signals.	
3.7	The worker has rapid, but often incorrect reaction on incoming signals.	
3.8	Other (please, write):	3

Module A-4 «Professional knowledge, skills»

The module is destined to indicate characteristic of professional activity conceptual model completeness, features of training process.

A-4	**Were professional knowledge and skill insufficient?**	Rate
4.1	The worker understood a task.	
4.2	There was not training on the task fulfillment.	
4.3	Did the worker study corresponding theoretical courses?	
4.4	Did the worker have a self-training?	
4.5	Did the worker have a period of probationer?	
4.6	Is the task highlighted in a training course?	
4.7	Have the worker been under tutorship?	
4.8	Did the worker have training on work place?	
4.9	Have the worker been trained with use of simulators?	
4.10	Неадекватная оценка умения выполнять задачу	
4.11	The worker fulfilled the task for the first time.	
4.12	The worker has not enough experienced.	

4.13	Other (please, write):	

МОДУЛЬ А-5 «Fitness for duty»

The module is destined to indicate characteristic of worker negative functional state and conditions provoking appearance of these characteristics.

5	**Why functional state (fitness for duty) was inadequate?**	Rate
5.1	Did the worker demonstrate tiredness?	
5.2	Did the worker have activity disorganization?	
5.3	Does the worker have decreasing of attention and operative memory, perception and thinking features?	
5.4	The situation was new, complex and requiring reliable decision for the worker?	
5.5	Is the worker under influence of negative external social factors (criticism, family problems and so on)?	
5.6	Did the worker have increased level of anxiety.	
5.7	Lowering of functional reserve.	
5.8	Lower activity tone.	
5.9	The worker has difficulties in job implementation, especially when long-term loading.	
5.10	Process of mobilization to implement a task has difficulties.	
5.11	The worker during job implementation had boredom, sleepiness condition.	
5.12	The worker had lost attention for situation when event.	
5.13	готовности действовать при возникновении проблемной ситуации	
5.14	The worker was ill when event time.	
5.15	Other (please, write):	

ANNEX 6.17.2.

HUMAN ERRORS IN JOB

Doing in-depth evaluation of events, engineers did find some trends regarding behavioral factors such as confusion, unawareness and lack of attention attributable to the acting person. This is very often a quick judgement, and analytical efforts to study internal attributes of persons involved in NPP events are needed. It may be helpful to use behavioral psychologists explanations and go further and build pragmatic approach of human errors such J. Reason or J. Leplat. These authors studied the problem of the responsibility of acting persons under certain circumstances, and found that reactions were highly dependent on external aspects. However, they studied also thought processes involved in human behavior. Undoubtedly it is important to take into consideration these internal processes to develop effective corrective measures to decrease the frequency and severity of human errors.

Event reports generally eliminate this problem of responsibility by indicating that it is not their purpose to attribute blame, but rather to analyze how the error comes about. This is also a means of showing that the error results from a combination of several factors, the most important of which having nothing to do with the individual who is fully responsible. However, it is not a good idea to eliminate completely the individual responsibility for an error. It is known that the individual demands a certain degree of autonomy in his work, and he, ipso facto, accepts responsibility for the actions in which he is involved, either as an individual or as a member of a team.

The concept of responsibility is a particularly complex one. Responsibility can be defined in terms of many different parameters: Moral, civil, penal, individual or collective etc. They are objective and subjective responsibilities. Objective responsibility refers to an act's compliance with an external rule. Subjective responsibility takes intent into account. Both components can be found in the concept of human error. An objective component of responsibility can be found, insofar as the concept of error refers more or less clearly to that of the norm: An error occurs because not everything that should have been done was done. The subjective component leads to questions: To what extent is an individual involved in the production of what is considered to be an error, to what extent could he prevent this error, and did he recognize the error as such?

We don't want to give quick and simple answers to the question: "How can we define being responsible for an error?". It is necessary to clarify the analysis of the error and to provide useful elements to improve the human error question. The analysis of the intention in the acting process can be useful to elucidate the roots of the error, and discuss the level of responsibility of the person involved. This also can be also helpful to identify accurately and adequately links with other factors (technical, organizational, etc.) and give a hierarchy in the different roots of errors.

Models to help the error analysis

Some elements from cognitive psychology can be transformed into a simple model showing the different steps involved in the process for tasks performed by a person on the job. The general model (see Figure 2.1) shows the successful completion of a task. By contrast, other models show a rupture in this process, and explain different types of errors, violations, mistakes, slips.

The general model explains the links among the planned required state of the system, prescribed task, and the other individual aspects, such as understanding, intention and action. An error is a discrepancy between the result of the actions and the planned result of the task to reach a required state, a rupture in the flow of the process. According to the place of the rupture, the roots of errors are not the same, because the components of the model are not sensitive to the same factors. Thus, the extent of the responsibility of the person involved is different. Consequently the corrective measures against errors should also be different. The different types of errors are given below.

The successful job process

The general model (see Figure 31) shows the mechanism for success in actions:

- The "prescribed task" corresponds in detail to the "actions to reach the required state";
- The operator/person understands the "prescribed task" or the "actions to reach the required state" themselves;
- His intention reflects the "actions to reach the required state", his instrumental intention is coherent with the goal and in accordance with the available schedule, resources and tools. If the operator follows completely his original goal intention and acts according to his instrumental intention, without disruptions, he will succeed and reach the goal: The system reaches the state 2.

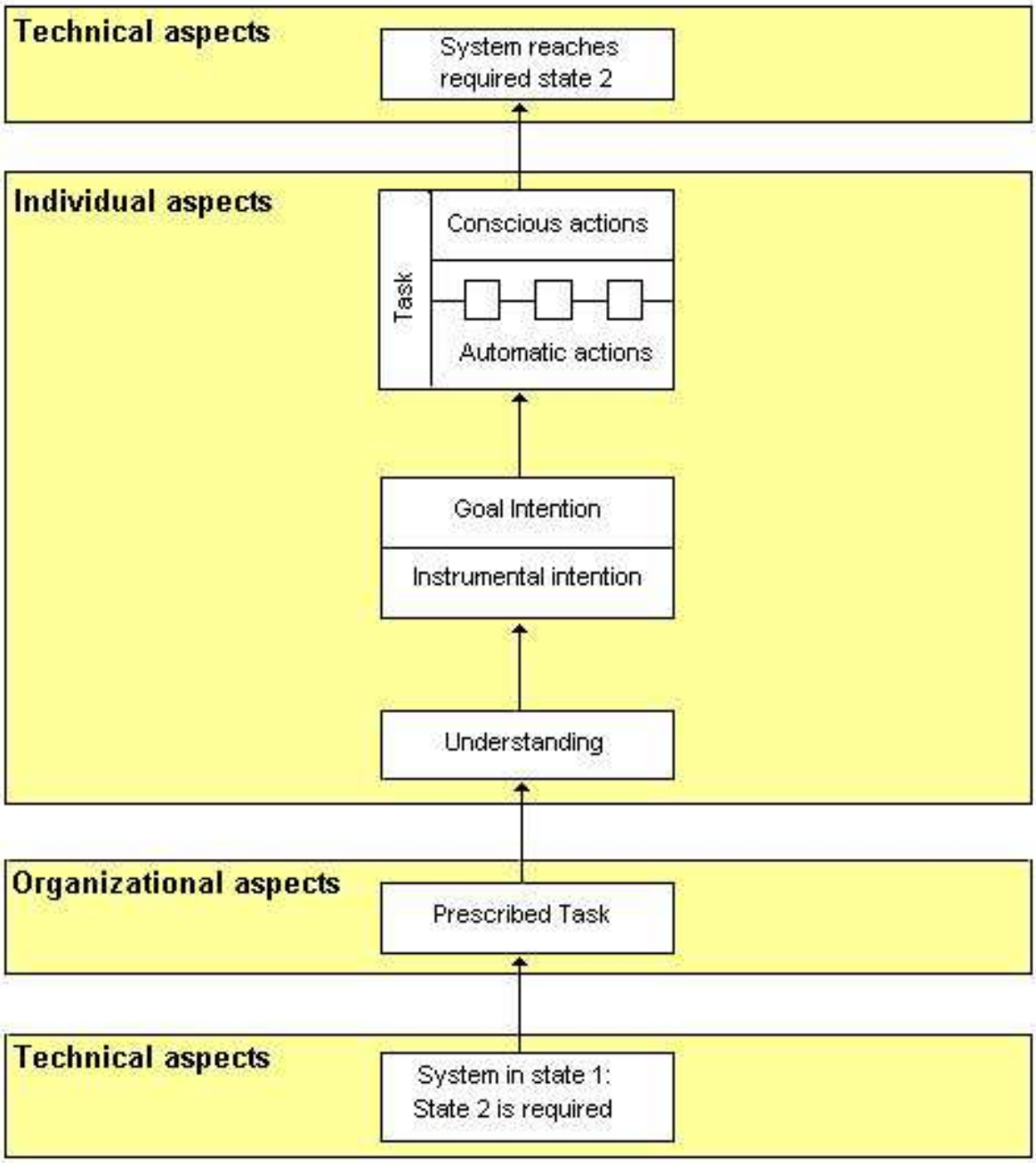


FIG. 31 Graphical representation of the general model

The general model is developed with the use of the following definitions:

Prescribed Task: "Prescribed task" means prescriptions which can cover the procedures and assignments. They can vary in the degree of detail, however, the term - prescribed task - will be used for all considered cases. The prescribed task reflects the different steps and the order of the

actions. Such prescribed actions should ensure a state of the system without risks evaluated from experience or analysis.

Understanding: Two levels of understanding are distinguished in this study:

- The beginner may understand the sequence of the procedure and know how to apply it to the system;
- The experienced person understands the process, the consequences of the actions on the process, including implicit risks not described by procedures.

Intention: The concept of intention encapsulates the idea of picturing, triggering and directing actions. This concept is related to that of scheduling. The intention is present when an individual operates toward achieving the goal, chooses means to to achieve the goal and corrects them if necessary. The transition from intention to action is then a result of a decision-making process which brings into play the context, the importance of the task as regards motivation, and the expectation of success.

In the context of this general model, the intention of a person corresponds to a specific task. This intention could be valid for a few minutes or for a few days (during the actions).

In this study, two important distinctions regarding "intention" were used: Goal intention and instrumental intention. The intention consists of two components:

- "What result has to be achieved" - goal intention;
- "How to act" - instrumental intention.

The goal intention is formed before the corresponding actions.

The instrumental intention relates to the methods of performing the task in compliance with the mental representation of the result and reflects the readiness of a person to use specific means, tools and technology. It provides a comprehensive view of all the steps and means which the person plans to reach the goal, including different points of view like his or her personal attitude, the use of tools, the help of other people, the level of quality achievable in the available time, etc.

Task and actions

Task. All the actions performed at the right time in the right sequence to bring the system from the initial to the required state. In this sense the task is on a higher hierarchical level than the action.

Actions. Conscious or unconscious work steps to perform a task, i.e. to change the systems state from the initial state to the required one.

Actions to reach required state. Actions, required by design fundamentals and physical laws, to bring the system from the initial state to the final required state.

Automatic actions. With experience and skill development, the structure of the task execution changes. The steps in developing automatic execution are the following:

At the beginning of the skill development, basic actions are linked together, achieving conscious intentions, then gradually, the status of the actions changes. These operations become automatic such that "soon they require no conscious control". Subsequently, these actions become part of another operation, with a complex make-up.

Controlling the basic units, originally what was a closed-loop operation, gradually becomes an open-loop operation: "The action is directed by a feed-forward rather than a feed-back principle". In other words, the mental pictures of the goal are adequate for implementing the imagined action without the need for conscious control. Thus, at the same time, conscious goals cover increasingly larger groups of execution.

The types of disturbances for a sequence of automated actions are confusion, omission results and lapses. If an intended action is skipped, an omission, if an action is replaced by an action in the intention of another (parallel) task, a lapse results. Confusion can be the result of an unconscious choice (wrong switch, wrong way to find a system, etc.).

The detailed model

The detailed model in Figure 2.2 shows the links among the individual aspects, technical, organizational and extra-organizational aspects. The organization prescribes the task but also provides the training to improve the understanding of the system. The organization can also promote other criteria which can influence the intention of the people (e.g. reduce the cost, the delay, etc.). Some external factors encountered during working conditions, can be contingent on the organization. Of course, understanding depends on the experience and competence of persons. Extra-organizational aspects (e.g. restricted time schedule, etc.) can have such an influence on persons that they develop an intention not in compliance with their proper understanding. The contingency of the situation can change some internal conditions of the persons (fatigue, awareness, etc.).

Small models for each type of error

Model of violation

The sources of errors are commonly very often described by omission, confusion, carelessness, etc.

Figure 32 shows the graphical model of violation. Although the person has a good understanding of the "prescribed task", he develops an intention not in compliance with his understanding. The reason for this may be derived from different sources (internal or external). This kind of behaviour is called a violation. As an example, the operator wants to follow his "personal intention" due to personal motivation (e.g., the operator does not follow the procedure in order to go home earlier etc.). In this case the operator is fully responsible for his action.

There are other cases, in which the part of responsibility must be investigated in more detail and more general situations must be taken into account. For instance, (a) the person wants to satisfy other criteria like personal safety aspects, power production or even the efficiency of the larger project that includes this particular task. Recommendations have to be addressed to this kind of compromise, something must be done to clarify the decision making; (b) the person thinks that he knows a better solution than provided by the procedure; (c) the person can't perform the task because the conditions have changed and the task cannot be done as prescribed because of time constraints, or work load, or because tools are not available; (d) the person is tired and has changed his work procedure. The identification of such conditions may change judgements and recommendations for the individual and the organization.

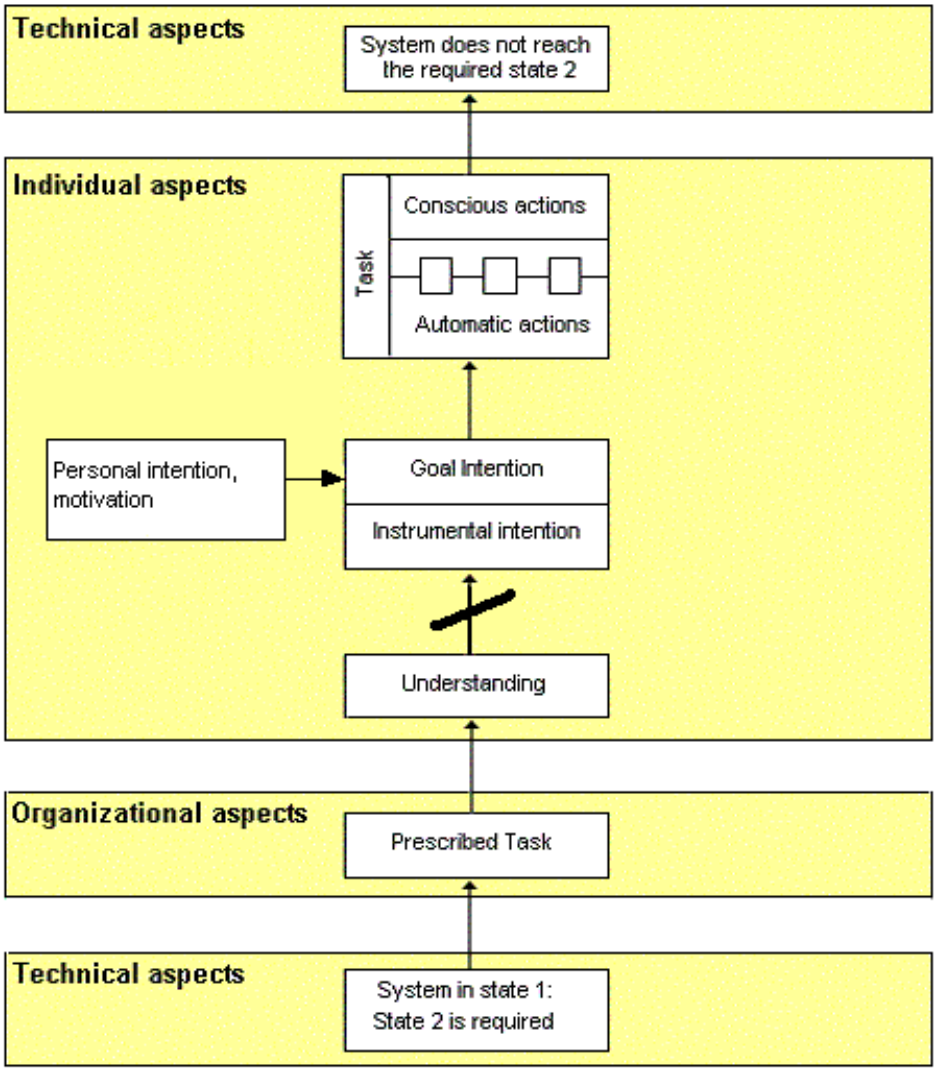


FIG. 32 Graphical representation of the detailed model

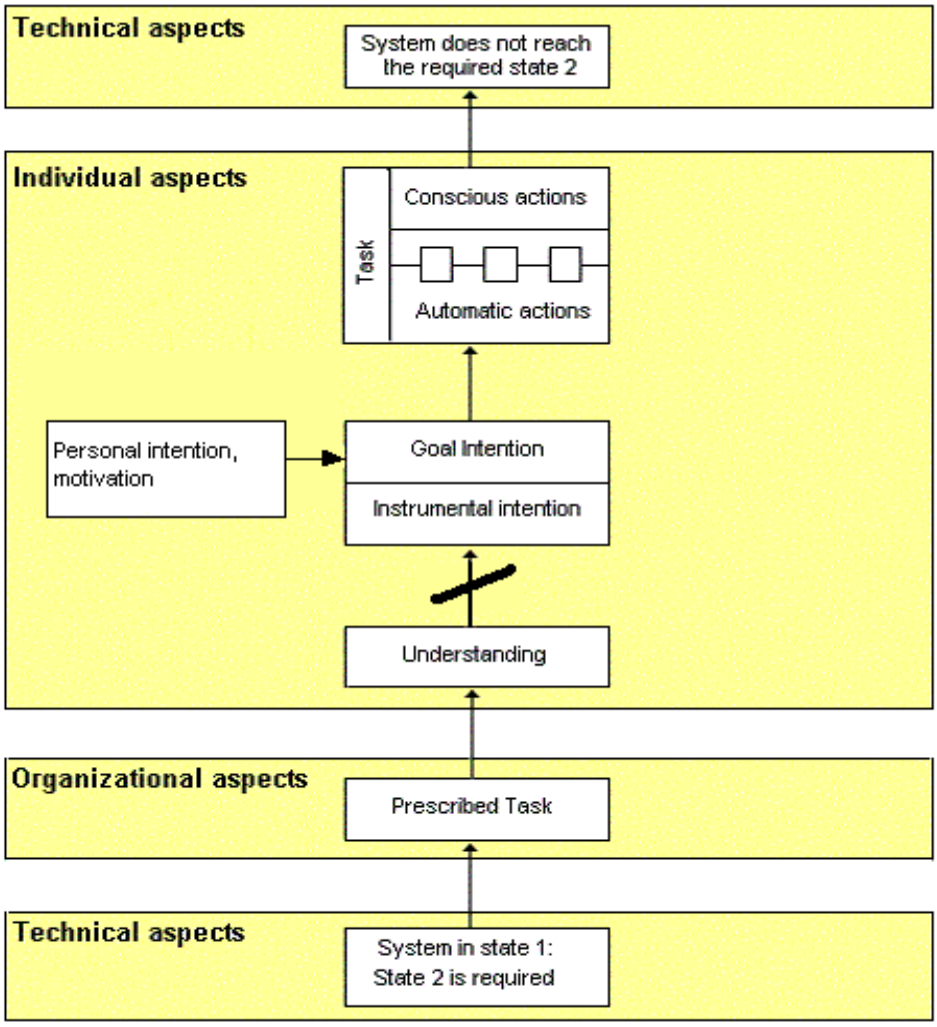


FIG. 33. Graphical model of violation

Model of mistake

Figure 34 shows the graphical model of mistakes. The intention is wrong or the instrumental intention is not appropriate, because the understanding is not in compliance with the "prescribed task". This can be explained by the total or partial ignorance of the operator due to internal or external factors.

Internal factors could be described by the following facts:

- Incompetence of the operator, who failed to understand or to recognize the task, or failed to determine how to use or to use the tools needed for achieving the objective.
- Forgetfulness (especially when situations occur infrequently or are unplanned).

- External factors could be described by the following facts:
- Task is poorly defined because it is poorly understood, even by the experts, or no enough defined with respect to the knowledge of the worker who will perform it.
- Task is performed in conflicting situations. It is possible that the organization has solutions for these conflicts, but these have not been clarified.
- The conflicts between speed and accuracy, and quality and quantity need more knowledge to be performed correctly.

Insufficient training has been provided to the individuals who have to perform the task.

When the analysis shows clearly (or by deduction) that the persons concerned did not understand the procedures, the aforementioned factors should be examined in-depth in order to provide more accurate recommendations for improvement, i.e., training of any persons involved in the NPP incident.

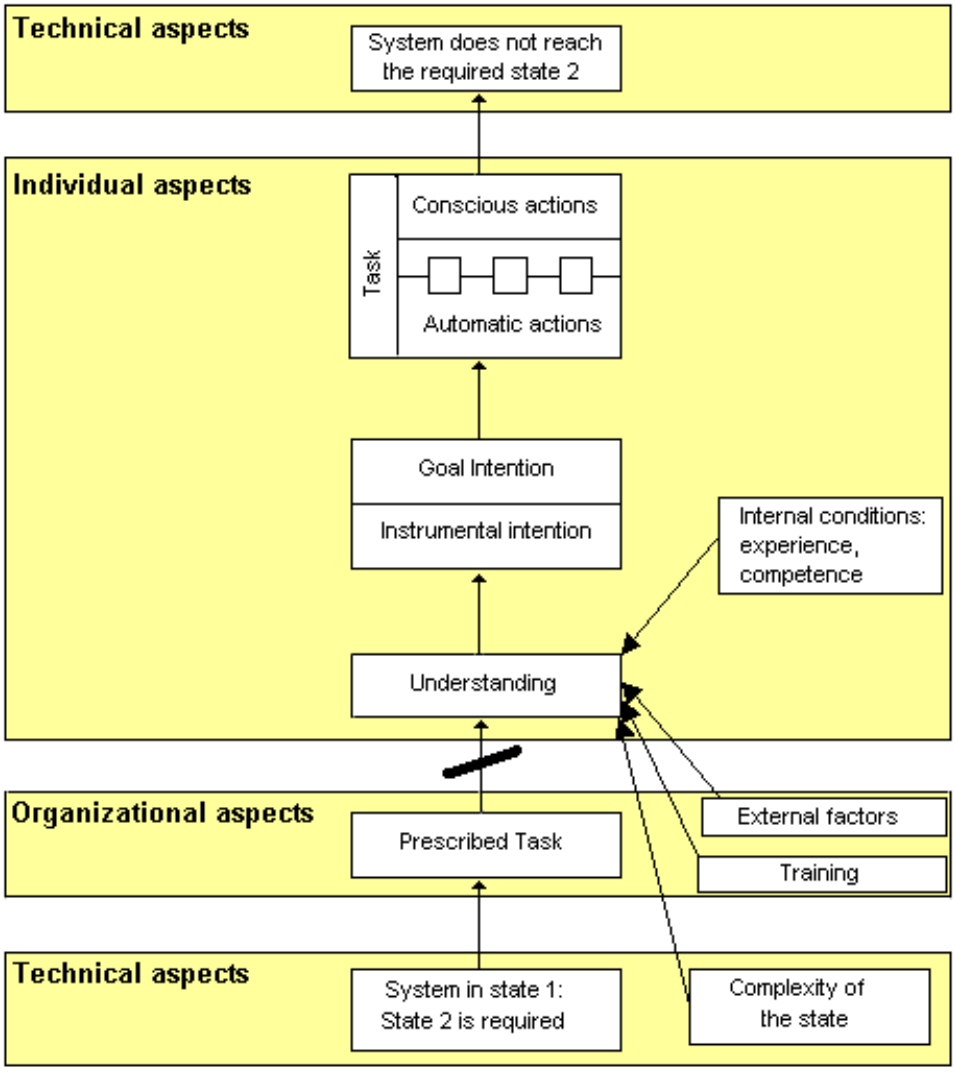


FIG. 34 Graphical model of mistakes

Model of slips

Figure 35 shows the graphical model of slips. The intention was good, the action is wrong. This family of errors concerns all events where the analysts can say that the person did not pay attention (carelessness). Slips occur when an action is not in compliance with the intention because something occurred during the execution of automatic actions. (distractions, interruptions, multitasking, etc.). A good understanding of the definition of automatic actions is

very important here. Also, a detailed analysis of the task has to be done during the root cause analysis in order to determine which part of the task may contain unconscious, automatic actions.

What are the factors which lead to automatic actions, possibly with disastrous consequences? Organizational conditions of work give more chance for these effects to be produced: particularly, hyper-specialization, excessive training for short-cycle and repetitive tasks, speed and output limitations which instil a need for increasingly developed automation.

Technical conditions and Man Machine Interaction can introduce error conditions:

- The absence of equipment standardisation (a new item of equipment with a mechanism which invalidates the operator's responses, although these were correct for the old system);
- Design of equipment that does not make allow for sensory-motor stereotypes, or the properties of perception systems, or representation systems acquired by experience;
- Management of experience: When a person acquires experience in doing a certain task, the original "knowledge based" activities for performing the individual steps of the tasks move down to "rule based" and finally "skill based" activities. An experienced person no longer thinks in steps but rather in sequences (rules) of steps which are executed automatically with little attention. In this operational state the person is more prone to slips and lapses. This carries the danger that a whole sequence of actions may be omitted or replaced by another sequence (lapse) not in the intention of this task.

In addition, another effect may occur that also gives some potential for errors: during the gain of experience, the task becomes less and less demanding for this person. This may lead to a loss of motivation which is an essential prerequisite for a good performance.

As a conclusion, automated actions are a result of experience and are needed for efficient work. To decrease this type of error, it is necessary to analyse the technical and organizational causes of such underlying automatic response in order to modify these attitudes. To interrupt an automatic action including a specific safety risk, it is necessary to propose other recommendations than " pay attention", for example, to create a stopping point in a phase, or to include a more conscious action or control and surveillance by other persons.

Organizations can find solutions by management of experience. Usually organizations solve the problem of motivation and the use of too much reflex and cognitive bias in work by career development of the skilled person, i.e., by promoting him to a higher position where he can use his knowledge supervise people in this specific task . These skills are very precious for organizations for mastering the process. These kind of skills may be developed in large complex tasks where they can get an integral view of their job. Personnel should have the opportunity to get experience in other related tasks in order to change their point of view.

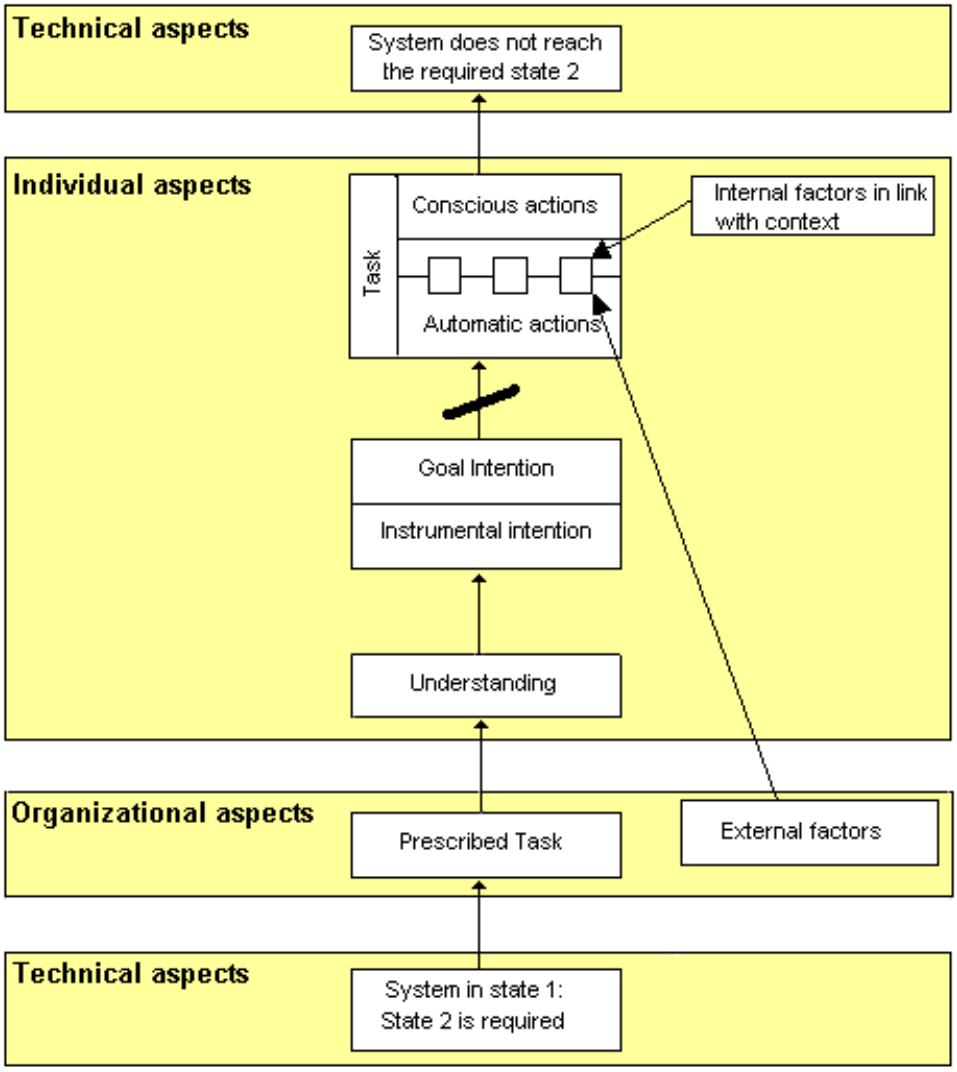


FIG.35. Graphical model of slips

Model of errors due to the decomposition of tasks

Figure 36 shows errors caused by interface problems. While organizing the work, the actions prescribed in the same procedure can be performed by different persons. The interruption in the task can be fixed before beginning the work or the interruption occurs at the end of the shift. When the shift changes, communications are more or less sufficient to help the other persons to continue the task. The responsibility for some important phases of the task cannot be explained well enought (for example, putting back or removing certain pieces used during tasks can be forgotten and this can change the design of the plant). The error by the person in charge of the second part of the work depends on different factors:

- Different understanding by two persons of the same procedure;
- Different intentions after reading the procedure by each person can redefine two tasks that will not be in compliance;
- Lack of communication about the condition of the interfaces between subtasks often leads to errors;
- Lack of communication during parallel tasks in the same procedure;
- Important details seen by the first person are not transmitted to the second person. (e.g., Dismounting and mounting a valve).

This would not be the case if the task is performed by the same person, since he includes this information automatically in his task. The challenge is here to be conscientious and to explain explicitly such automatic actions to the other person.

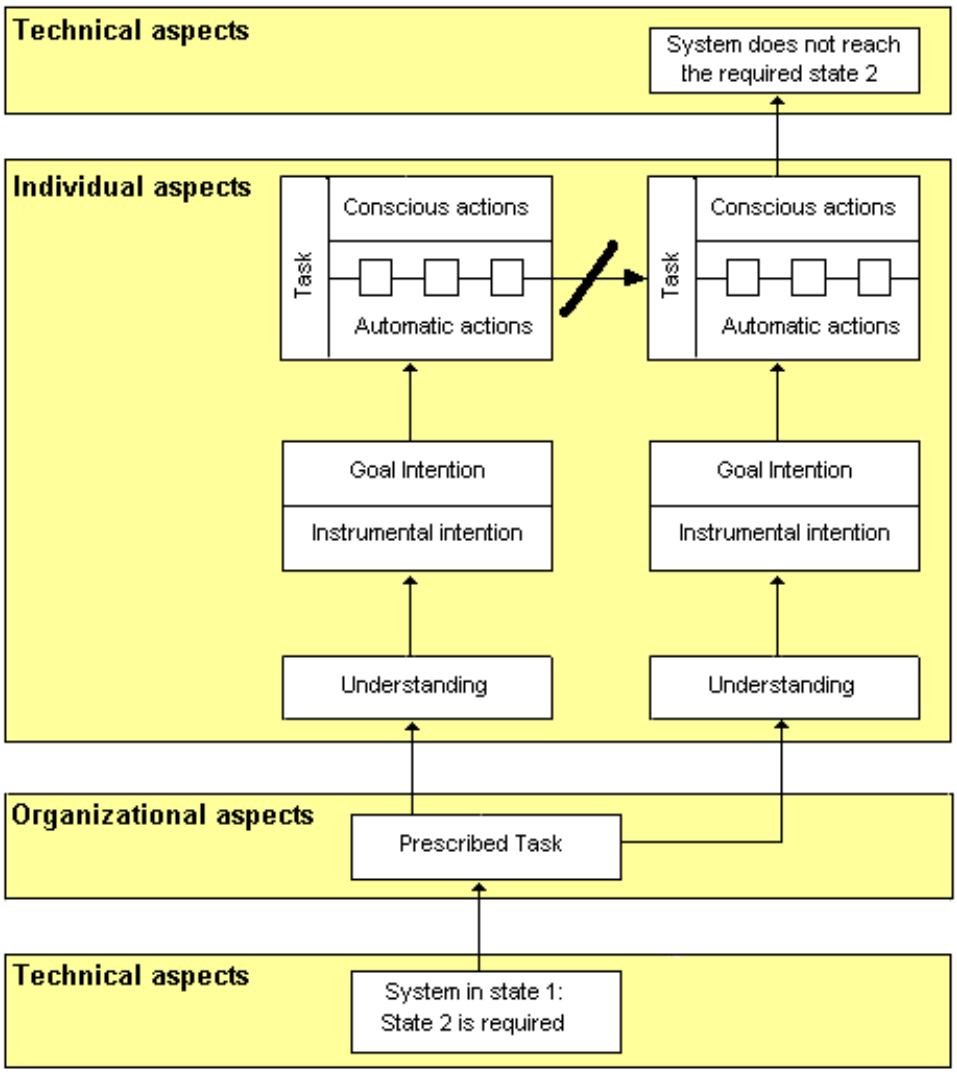


FIG. 36. Graphical model of errors in the interface between actions

SOL - Safety through Organizational Learning

A methodology for systematic event analysis

MTO Mensch-Technik-Organisation GmbH & Co. Consulting KG (*Man-Technology-Organization)*
Hardenbergstr. 9, 10623 Berlin, www.mensch-technik-organisation.de; info@ mensch-technik-organisation.de

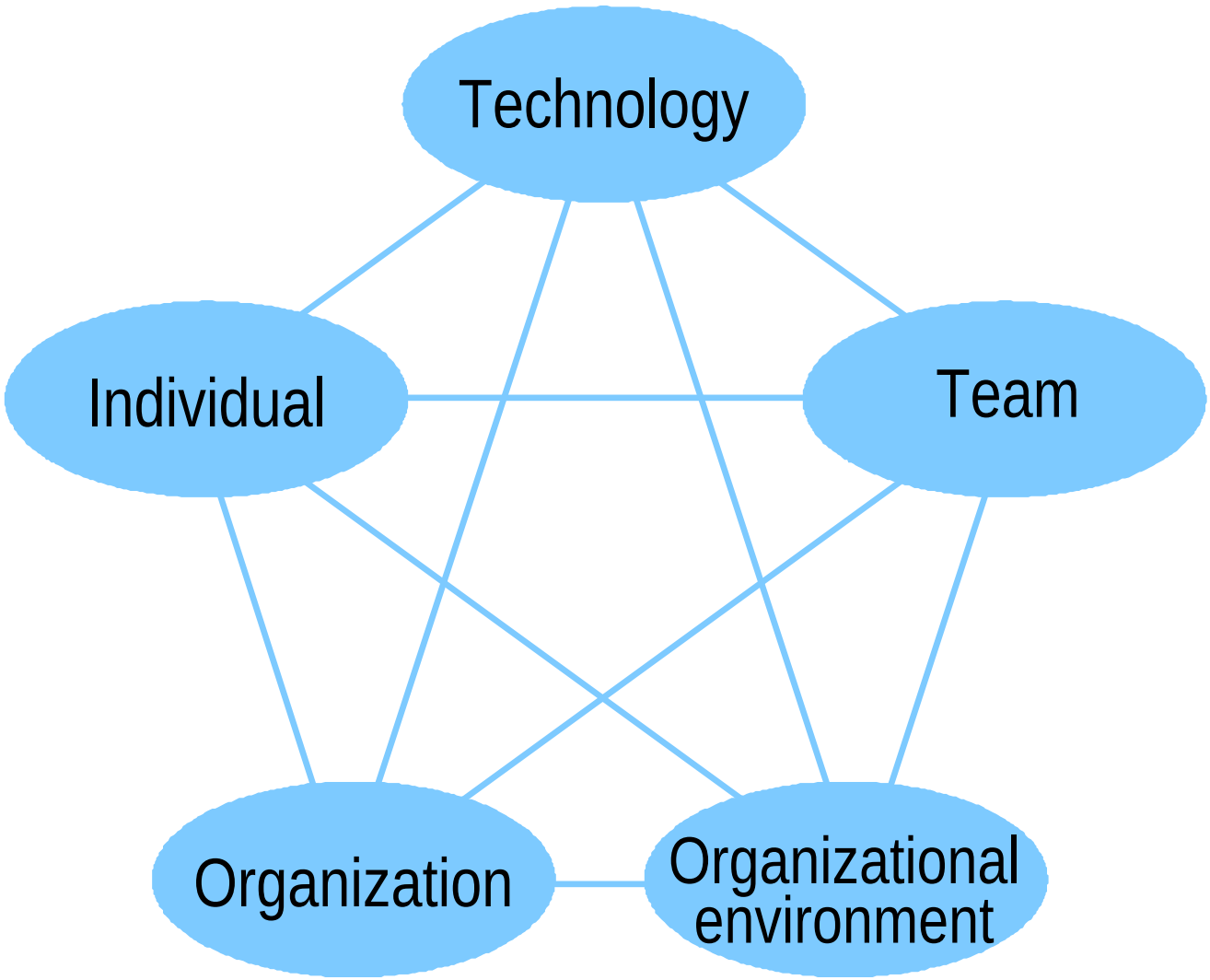
1. Emergence of events
2. Event analysis
3. SOL Safety through organizational learning
4. The software SOL-VE

1 Emergence of events

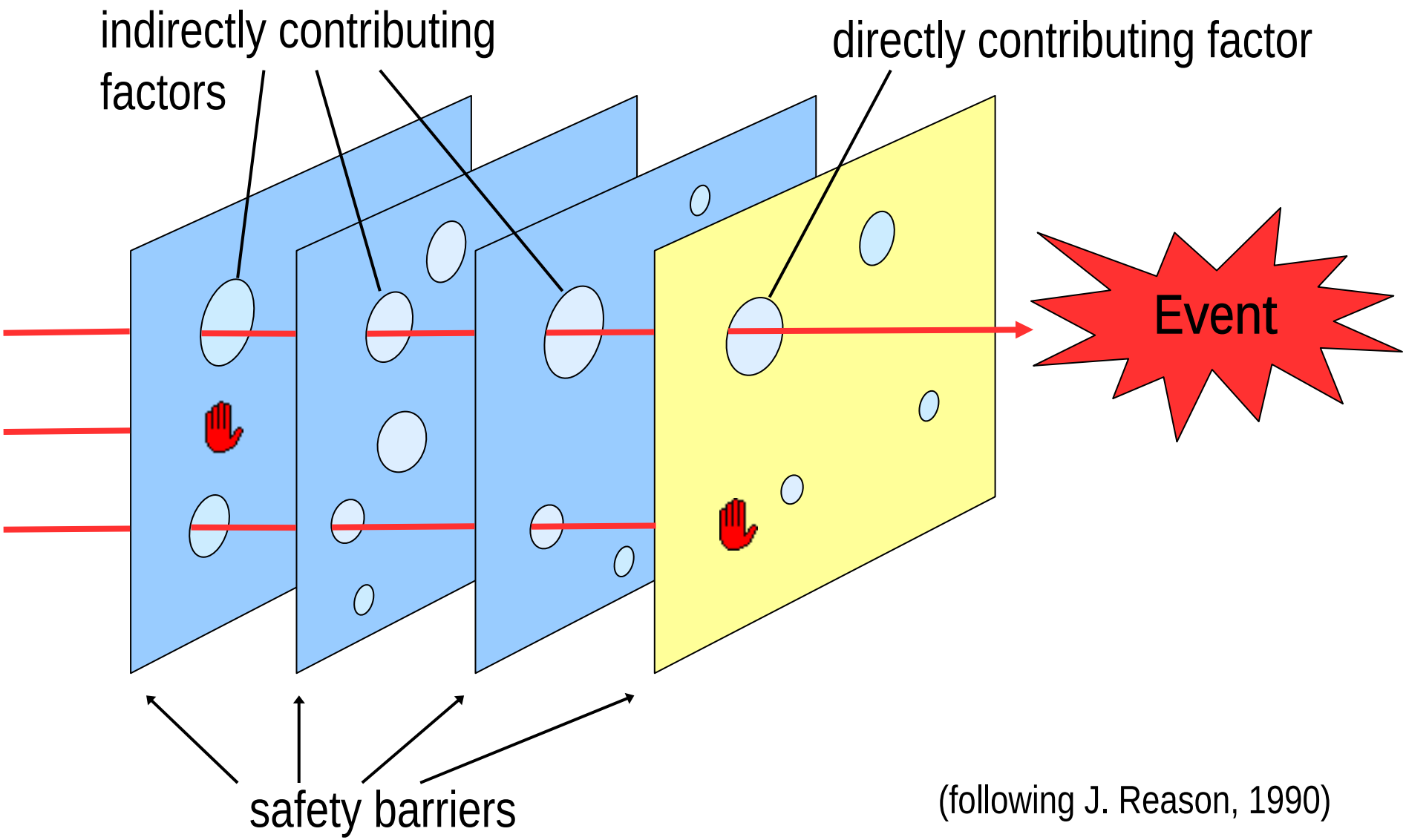
Systemic view on safety

- → In each organization two subsystems contribute to its goals (efficiency, productivity, safety): the **technical** and the **social subsystem**.
- → Problems arises at the interfaces of the two systems
  - →To solve any problem at the interface, both subsystems has to be considered simultaneously
- → For the analysis of safety problems, the socio-technical systems approach has been enlarged:
  - → one technical subsystem
  - → four social subsystems

Systemic view of safety (5 subsystems)

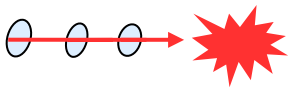


How does an event occur ?

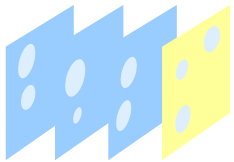


(following J. Reason, 1990)

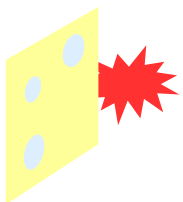
SOL - Concept for the emergence of events



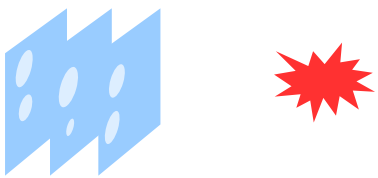
→ Events can be described as a chain of single events



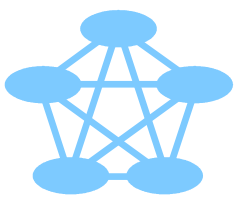
→ Events occur through interaction of **directly** and **indirectly** contributing factors



→ Directly contributing factors are directly tied up with the event



→ Indirectly contributing factors are temporally and spatially remote from the occurrence of the event



→ **directly** and **indirectly** contributing factors are located in the five subsystems technology, individual, team, organization and organizational environment

2 Event analysis

Goals of event analysis

- → **Identification of weaknesses** of the system:
- → **Systematic modeling** of the system: Modeling of dependencies and interactions as an also potential input into probabilistic risk analysis
- → Increase of **systemic thinking**: Conduction and discussion of event analyses show systemic dependencies and tight coupling of technical, individual and organizational factors
- → **Prevention**: Identification of appropriate recommendations after a systematic analysis
- → Starting and supporting a process of organizational learning
- → Not: Finding and blaming the one who is responsible!

Event analysis for Organizational Learning

- → Qualitative, not quantitative approach
- → The focus must be to find and discuss possibilities to improve the system in order to avoid reoccurrence of similar events
- → Focus on all factors which may contribute to an event – including human and organizational factors
- → Analysis method should be applicable by trained company staff.

Event analysis

An **event analysis** is the socially accepted reconstruction of an event to be analyzed, i.e. the identification of *what* happened and *why* it happened.

- For the *what* it is necessary to describe as detailed as possible the course of the event.
- For the *why* it is necessary to identify as much contributing factors as possible.

The main problem according to these points is, that it is necessary to go beyond the given information, i.e. to make causal inferences.

3 SOL - Safety through Organizational Learning

SOL and SOL-VE

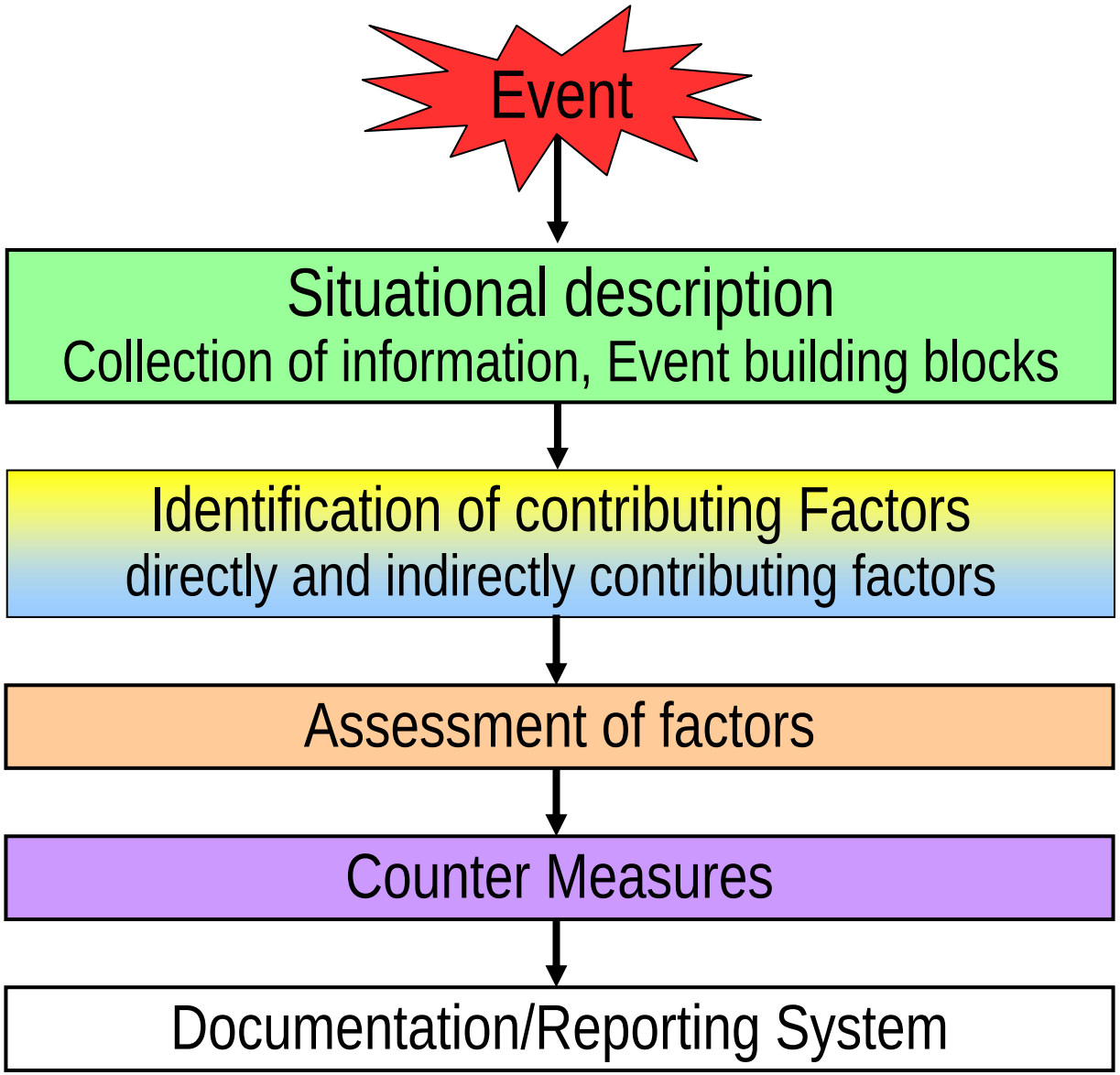
→ *SOL - Safety through Organizational Learning* is a method for in depth analysis of safety related events

→ *SOL-VE (Safety through Organizational Learning – versio electronica)* is a MS Windows-based software tool for SOL analysis.

SOL and SOL-VE

- → 1992: Start of SOL development; Conceptual work
- → 1996 - 1998: Development and test of SOL for application in chemical plants (sponsored by German Federal Environment Agency)
- → Since 2000: Numerous SOL-analysis by MTO in Germany for different operators of NPP (RWE, E.ON, EnBW, Vattenfall)
- → 2003: SOL and SOL-VE are licensed for all German NPP as the standard methodology for in-depth-analysis
- → Since 2004: SOL and SOL-VE are licensed by all Swiss NPP as the standard methodology for in-depth-analysis

SOL event analysis procedure



Course of event analysis with SOL

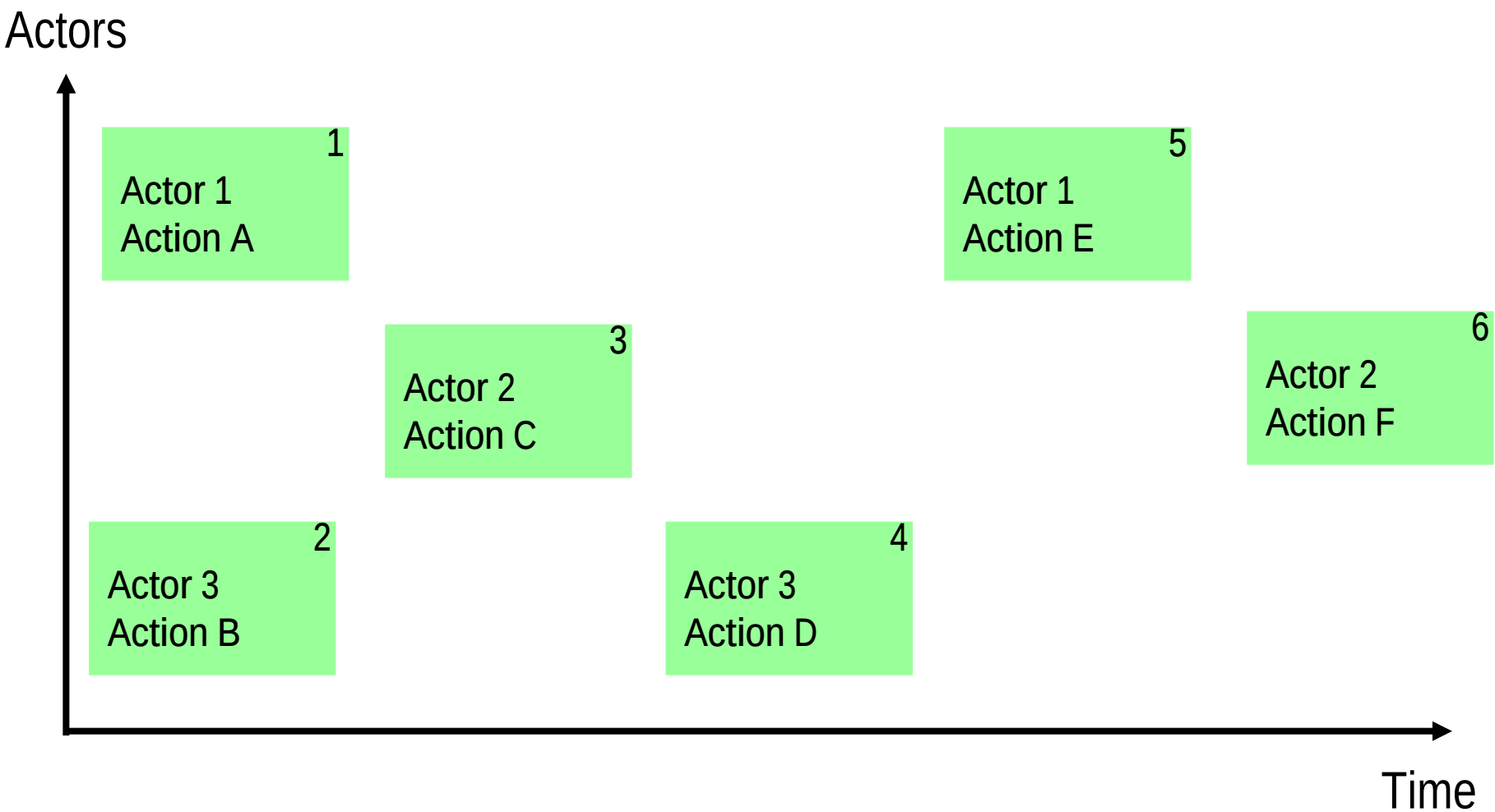
1. Collecting information
2. Disassembling the event (event building blocks)
3. Arranging the event building blocks

→ 4. Questioning the facts

→ 5. Identification of contributing factors

3. Arranging the event building blocks

SOL time-actor diagram



4. Questioning the facts

SOL directly contributing factors

A Representation of Information

B Communication

C Working conditions

D Personal performance

E Violation

F Technical components

SOL indirectly contributing factors

1. Representation of Information
2. Communication
3. Working conditions
4. Personal performance
5. Violation
6. Operation scheduling
7. Responsibility
8. Control and supervision
9. Group influence
10. Rules, procedures, and documents
11. Qualification
12. Training
13. Organization and management
14. Feedback of experience
15. Safety principles
16. Quality management
17. Maintenance
18. Regulatory and consulting bodies
19. Environmental influence

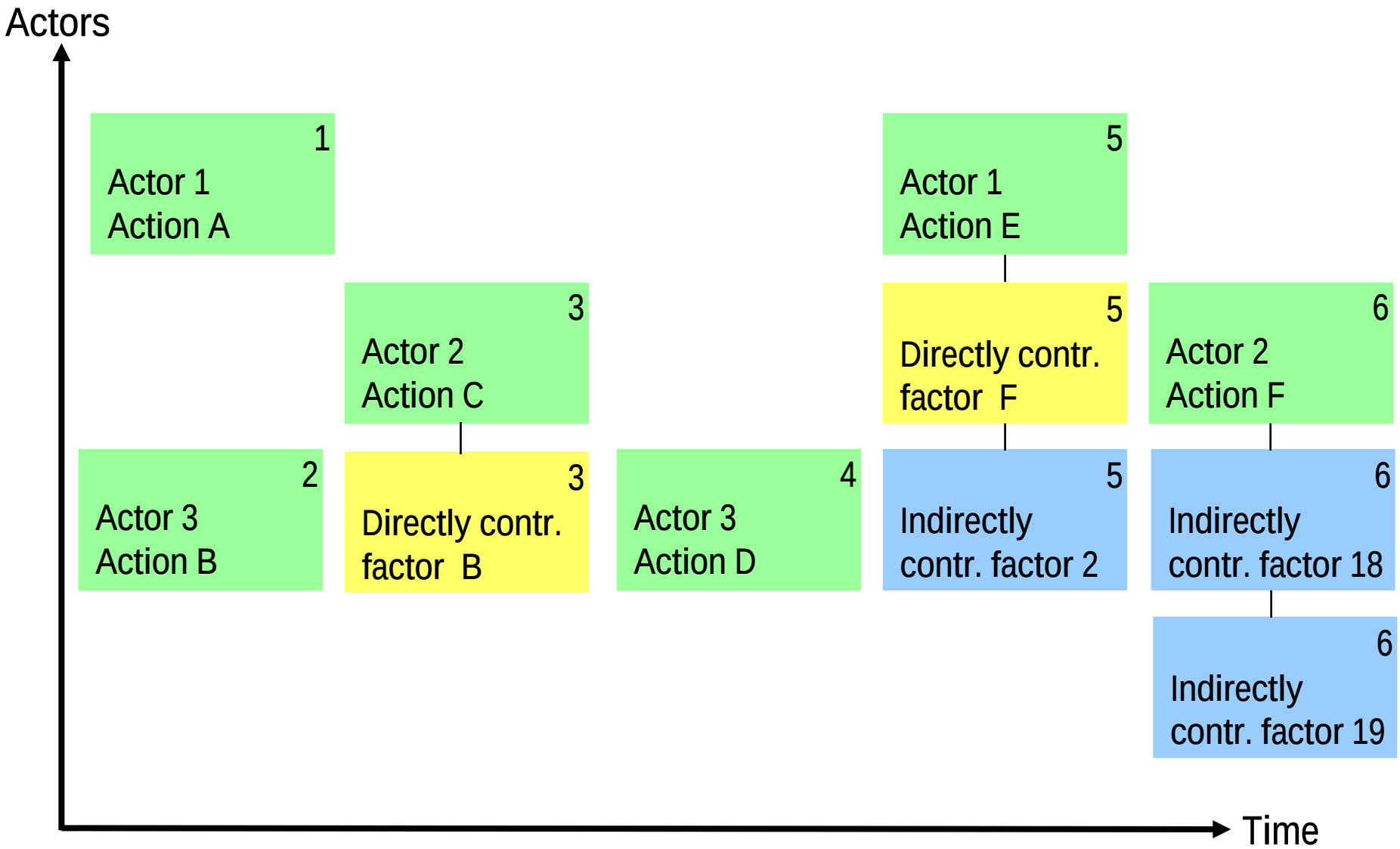
SOL: Identification Aid

- → The SOL methodology has an **identification aid** which consists of a descripton of possible contributing factors. Each factor is described by a *main question*, by *examples* and has *references* to other factors.
- → The examples do not cover all possibilities, but allow to understand the meaning and range of a given factor, i. e. the function of the example is to encourage analysts to use their own experience and competence **creatively**.
- → From each directly contributing factor is a *reference* to several indirectly contributing factors. This guides the user through the analysis.

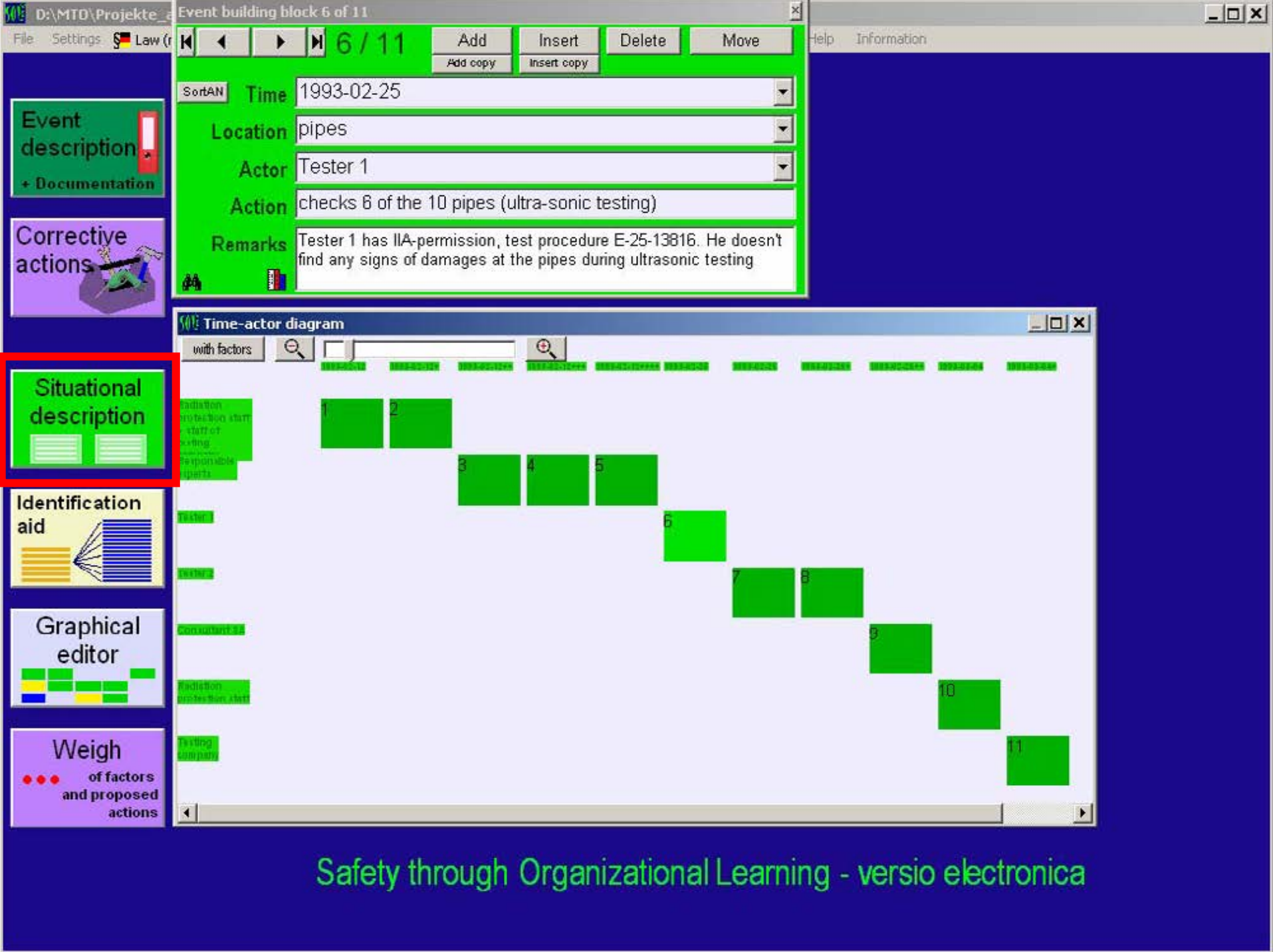
SOL identification aid

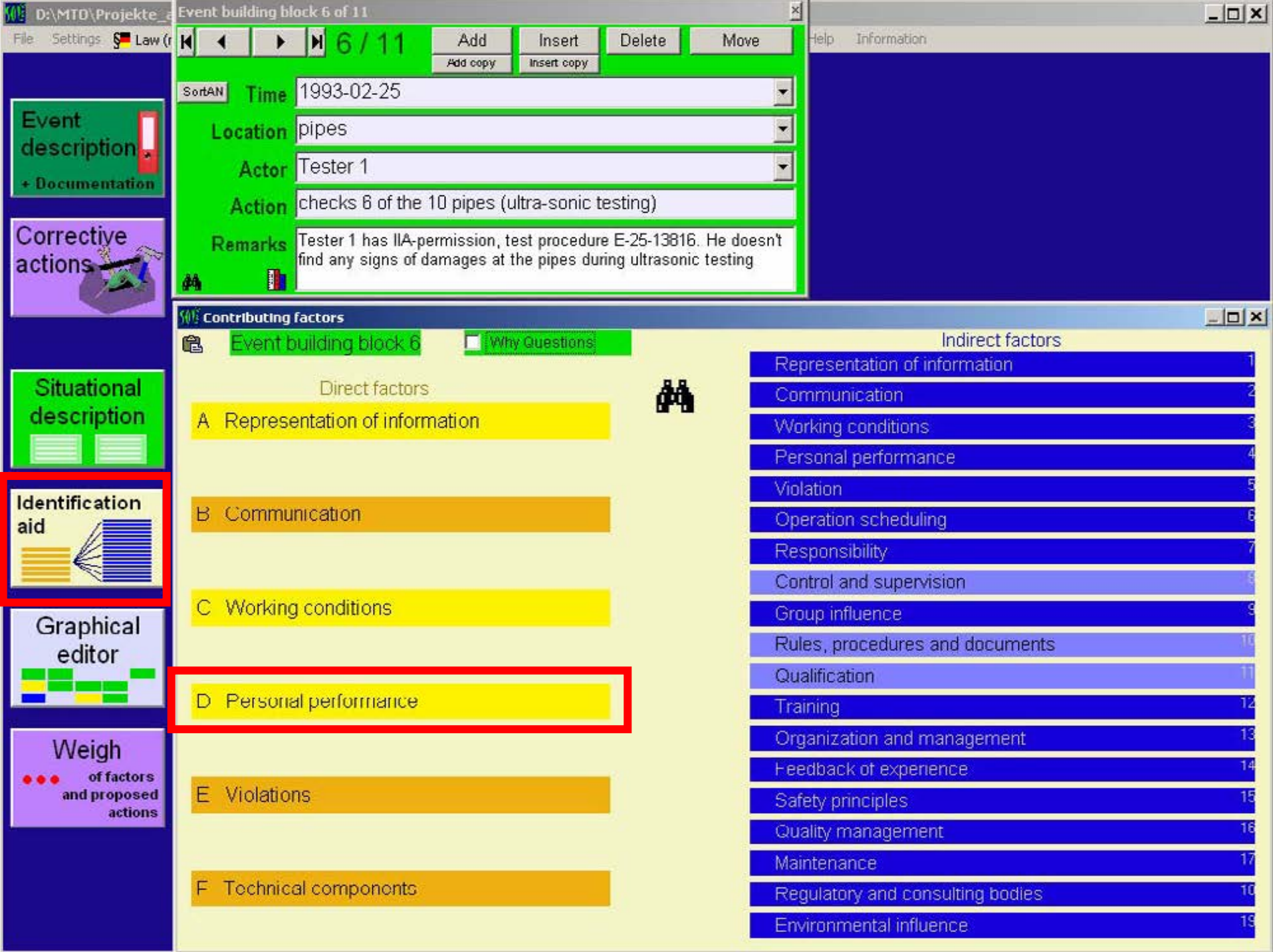
Directly contributing factor	points to	Indirectly contributing factor
E. Violation *"Has there been a violation?"*	1 3 5 6	**8. Control and supervision** *"Was the operators' performance not sufficiently controlled or supervised?"*
Examples are: • inappropriate transfer of processes from other situations • work performance that violates at least partly prescribed rules • inadmissible reductions during work performance • non-compliance with the safety regulations • evading of control principles ("4-eyes-principle") • ...	8 9 10 11 12 13 18	*Examples are:* • missing "4-eyes-principle" • missing protection against violations of the "4-eyes-principle" • missing control of the work by supervisors or co-workers • inadequate supervision • missing self-control of work results • attaching too much importance to work results in comparison to safe performance • ...

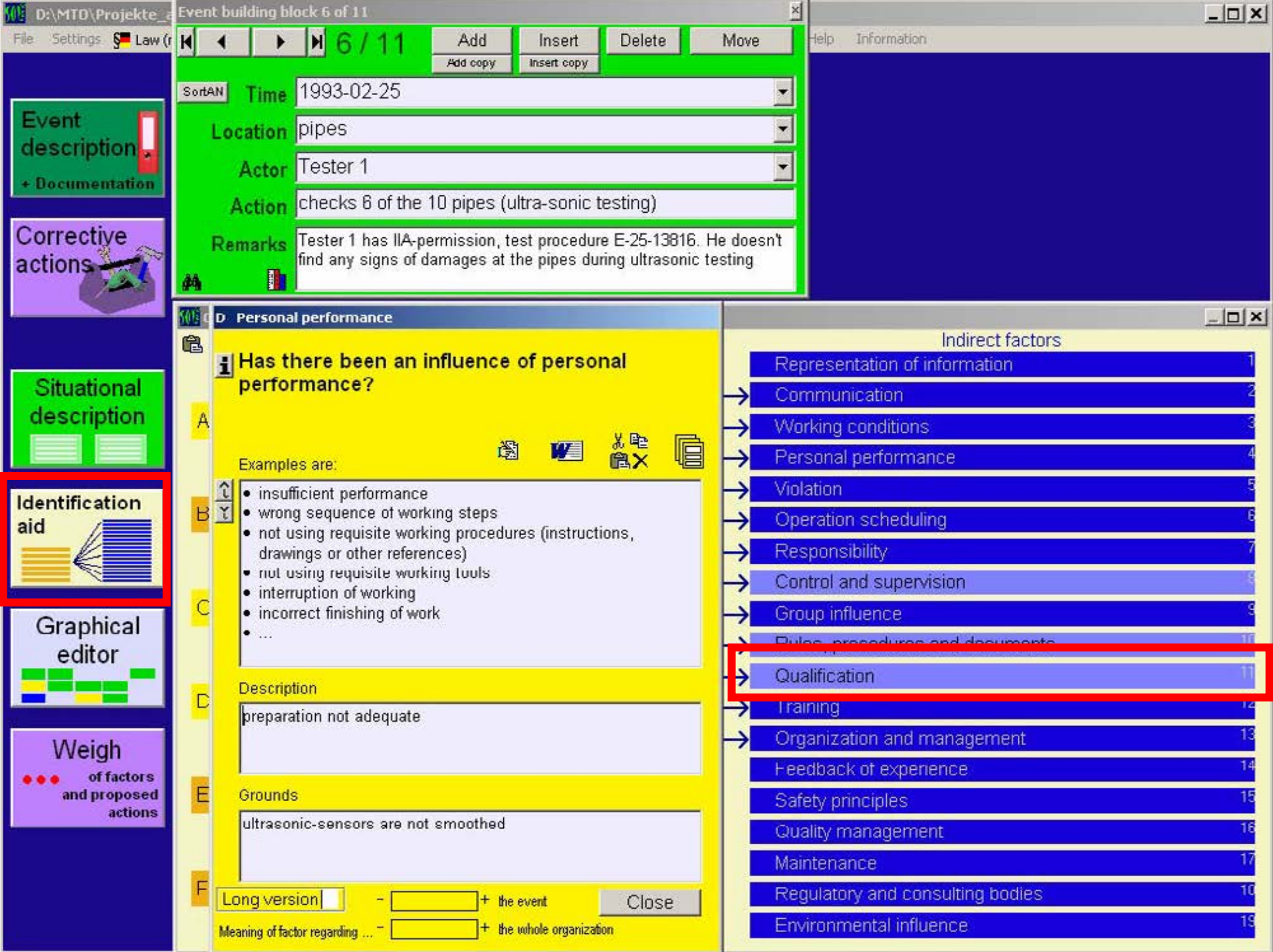
SOL time-actor diagram with contributing factors

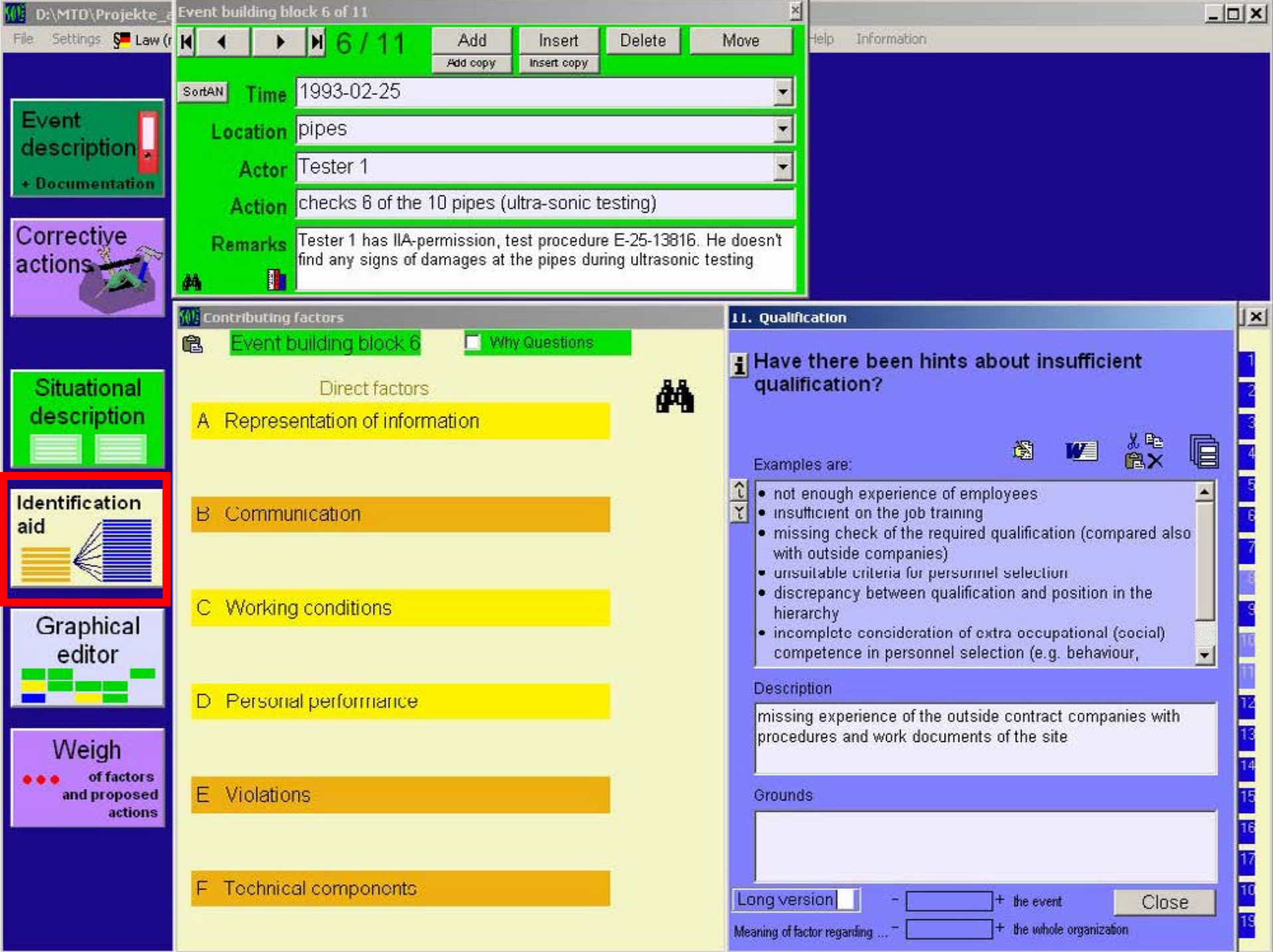


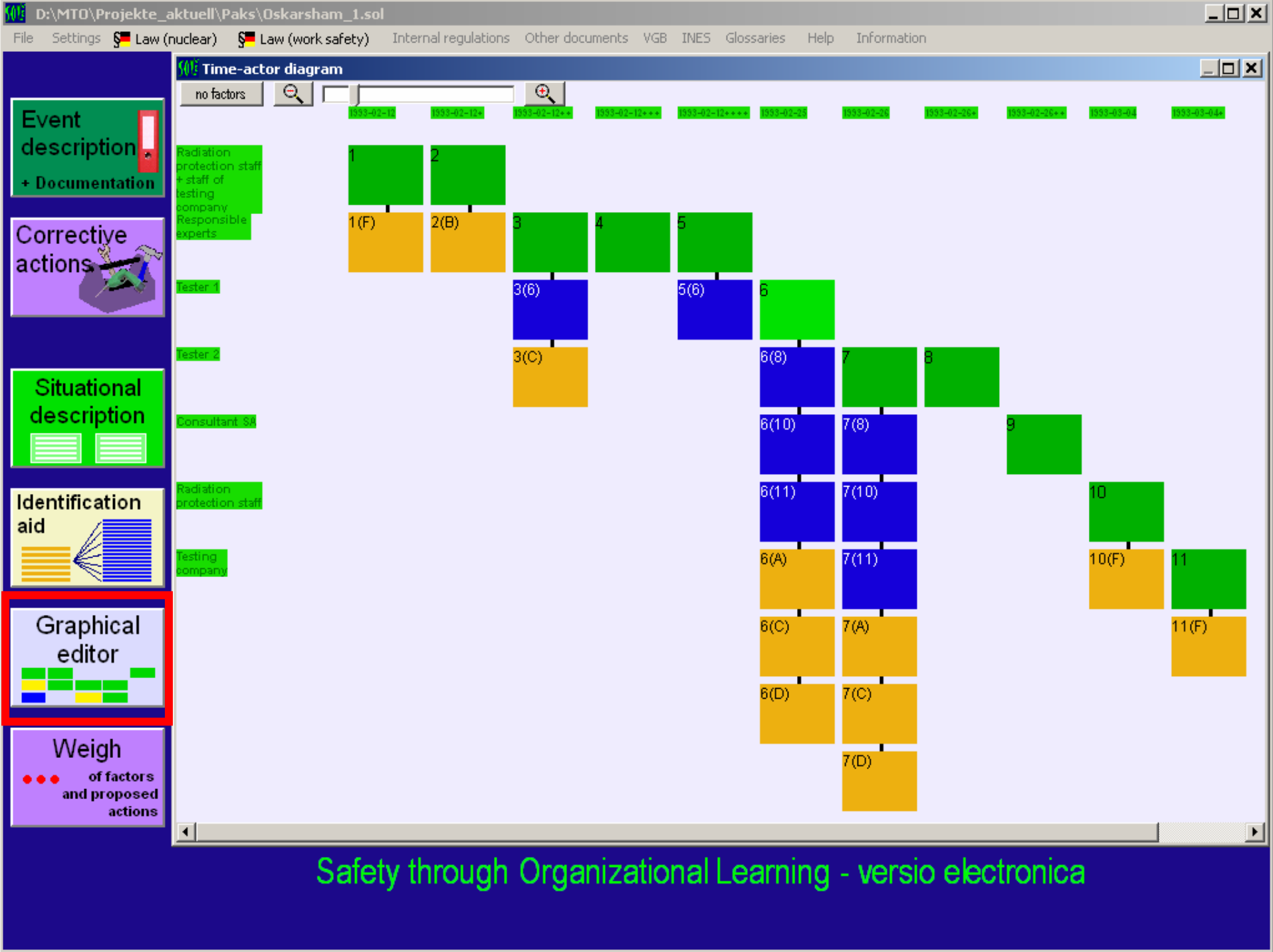
4 The software SOL-VE


D:\MTO\Projekte_a
File
Settings
Law (r
Help
Information
Event building block 6 of 11
6 / 11
Add
Add copy
Insert
Insert copy
Delete
Move
SortAN
Time
1993-02-25
Location
pipes
Actor
Tester 1
Action
checks 6 of the 10 pipes (ultra-sonic testing)
Remarks
Tester 1 has IIA-permission, test procedure E-25-13816. He doesn't find any signs of damages at the pipes during ultrasonic testing
Event description
+ Documentation
Corrective actions
Situational description
Identification aid
Graphical editor
Weigh
of factors and proposed actions
Time-actor diagram
with factors
Safety through Organizational Learning - versio electronica


D:\MTO\Projekte_a
File
Settings
Law (r
Help
Information
Event building block 6 of 11
6 / 11
Add
Add copy
Insert
Insert copy
Delete
Move
SortAN
Time
1993-02-25
Location
pipes
Actor
Tester 1
Action
checks 6 of the 10 pipes (ultra-sonic testing)
Remarks
Tester 1 has IIA-permission, test procedure E-25-13816. He doesn't find any signs of damages at the pipes during ultrasonic testing
Event description
+ Documentation
Corrective actions
Situational description
Identification aid
Graphical editor
Weigh
of factors and proposed actions
Contributing factors
Event building block 6
Why Questions
Direct factors
A Representation of information
B Communication
C Working conditions
D Personal performance
E Violations
F Technical components
Indirect factors
Representation of information 1
Communication 2
Working conditions 3
Personal performance 4
Violation 5
Operation scheduling 6
Responsibility 7
Control and supervision 8
Group influence 9
Rules, procedures and documents 10
Qualification 11
Training 12
Organization and management 13
Feedback of experience 14
Safety principles 15
Quality management 16
Maintenance 17
Regulatory and consulting bodies 18
Environmental influence 19


D:\MTO\Projekte_a
File
Settings
Law (r
Help
Information
Event building block 6 of 11
6 / 11
Add
Add copy
Insert
Insert copy
Delete
Move
SortAN
Time
1993-02-25
Location
pipes
Actor
Tester 1
Action
checks 6 of the 10 pipes (ultra-sonic testing)
Remarks
Tester 1 has IIA-permission, test procedure E-25-13816. He doesn't find any signs of damages at the pipes during ultrasonic testing
Event description
+ Documentation
Corrective actions
Situational description
Identification aid
Graphical editor
Weigh
of factors and proposed actions
D Personal performance
Has there been an influence of personal performance?
A
Examples are:
B
insufficient performance
wrong sequence of working steps
not using requisite working procedures (instructions, drawings or other references)
not using requisite working tools
interruption of working
incorrect finishing of work
...
C
Description
preparation not adequate
D
Grounds
ultrasonic-sensors are not smoothed
E
F
Long version
the event
Close
Meaning of factor regarding ...
the whole organization
Indirect factors
Representation of information 1
Communication 2
Working conditions 3
Personal performance 4
Violation 5
Operation scheduling 6
Responsibility 7
Control and supervision 8
Group influence 9
Qualification 11
Training 12
Organization and management 13
Feedback of experience 14
Safety principles 15
Quality management 16
Maintenance 17
Regulatory and consulting bodies 18
Environmental influence 19


D:\MTO\Projekte_a
File
Settings
Law (r
Help
Information
Event building block 6 of 11
6 / 11
Add
Add copy
Insert
Insert copy
Delete
Move
SortAN
Time
1993-02-25
Location
pipes
Actor
Tester 1
Action
checks 6 of the 10 pipes (ultra-sonic testing)
Remarks
Tester 1 has IIA-permission, test procedure E-25-13816. He doesn't find any signs of damages at the pipes during ultrasonic testing
Event description
+ Documentation
Corrective actions
Situational description
Identification aid
Graphical editor
Weigh
of factors and proposed actions
Contributing factors
Event building block 6
Why Questions
Direct factors
A Representation of information
B Communication
C Working conditions
D Personal performance
E Violations
F Technical components
11. Qualification
Have there been hints about insufficient qualification?
Examples are:
not enough experience of employees
insufficient on the job training
missing check of the required qualification (compared also with outside companies)
unsuitable criteria for personnel selection
discrepancy between qualification and position in the hierarchy
incomplete consideration of extra occupational (social) competence in personnel selection (e.g. behaviour,
Description
missing experience of the outside contract companies with procedures and work documents of the site
Grounds
Long version
the event
Meaning of factor regarding ...
the whole organization
Close


D:\MTO\Projekte_aktuell\Paks\Oskarsham_1.sol
File
Settings
Law (nuclear)
Law (work safety)
Internal regulations
Other documents
VGB
INES
Glossaries
Help
Information
Event description
+ Documentation
Corrective actions
Situational description
Identification aid
Graphical editor
Weigh
of factors and proposed actions
Time-actor diagram
no factors
1993-02-12
1993-02-12+
1993-02-12++
1993-02-12+++
1993-02-12++++
1993-02-25
1993-02-25
1993-02-26+
1993-02-26++
1993-03-04
1993-03-04+
Radiation protection staff + staff of testing company
Responsible experts
Tester 1
Tester 2
Consultant SA
Radiation protection staff
Testing company
1
2
1(F)
2(B)
3
4
5
3(6)
5(6)
6
3(C)
6(8)
7
8
6(10)
7(8)
9
6(11)
7(10)
10
6(A)
7(11)
10(F)
11
6(C)
7(A)
11(F)
6(D)
7(C)
7(D)
Safety through Organizational Learning - versio electronica

TRIPOD BETA

Guidance on using Tripod Beta in the investigation and analysis of incidents, accidents and business losses

energy institute

TRIPOD BETA

Guidance on using Tripod Beta in the investigation and analysis of incidents, accidents and business losses

January 2014

Version 5

Published by
ENERGY INSTITUTE, LONDON
The Energy Institute is a professional membership body incorporated by Royal Charter 2003
Registered charity number 1097899

The Stichting Tripod Foundation is a non-profit organisation. Income from the sale of this publication is reinvested into the continuous development of the Tripod methodology, and helping to improve the standard of risk management and incident investigation in industry.

ISBN 978 0 85293 673 3

Published by the Energy Institute.
Registered Charity Number 1097899
www.energyinst.org

CONTENTS

CAVEAT

Tripod Beta is a robust and powerful technique for incident investigation and analysis. However, effectively analysing incidents using this technique requires a high level of understanding and competence in both investigation techniques and Tripod Beta. Whilst this publication details the Tripod Beta methodology, before the methodology is used during a real incident investigation, it is strongly recommended that the user has undergone Tripod Beta training and accreditation.

The Stichting Tripod Foundation has an accreditation process in place to help develop and ensure the competency of Tripod practitioners. To become an accredited Tripod Beta Practitioner, the practitioner should first attend an accredited training course, and then practice, refine and demonstrate their understanding of the Tripod Beta methodology by submitting two incident investigation reports for assessment by an accredited Tripod Beta Assessor.

This publication is intended for use by those who have begun, or have completed, this accreditation process.

For more information, visit www.tripodfoundation.com

FOREWORD

Learning from accidents and incidents is imperative for improving all business processes and performance including those for quality, productivity, economic, and health, safety and environment (HS&E). However, all too often, incident investigations do not go far enough to:

- determine the human factors contribution to an incident (beyond simply attributing it to 'human error'), and
- uncover the underlying organisational weaknesses that allowed that incident to happen.

Addressing these underlying organisational issues makes it more likely that similar incidents, with similar causes, can be avoided in the future.

Tripod Beta is an incident investigation and analysis methodology based on the Swiss cheese model. It was created to help incident investigators to analyse incidents in a way that allows them to understand the influences on humans from the operational environment in which the incident occurred. From this, the hidden organisational deficiencies that created this environment can be identified, and improvements to business processes made.

Tripod Beta analysis is extremely versatile and can be used in any industry or organisation and for all types of business upsets and incidents. The purpose of this publication is to explain the Tripod Beta methodology and also provide guidance on its application. It is aimed at those who are either:

- not familiar with this method, or
- familiar with it but require practical guidance on its application.

This publication first provides background on why incidents should be investigated and why they occur, introducing the Swiss cheese model and Tripod theory of accident causation. It then introduces the Tripod Beta methodology of investigation and analysis, before setting out guidelines on its use. Finally, guidance is provided on generating remedial actions from Tripod Beta incident analyses.

The EI and Stichting Tripod Foundation welcome feedback on this publication. Feedback or suggested revisions should be submitted to:

Technical Department
Energy Institute
61 New Cavendish Street
London, W1G 7AR
e: **tripod@energyinst.org**

ACKNOWLEDGEMENTS

Tripod Beta: Guidance on using Tripod Beta in the investigation and analysis of incidents, accidents and business losses was commissioned by the Stichting Tripod Foundation (STF), and authored by David Edwards.

During this project, STF members included:

Robin Bryden	Shell
Tony Gower-Jones (Secretary)	Centrica
Jop Groeneweg (R&D)	Leiden University/TNO
Sally Martin (Chair)	Shell
Willem Peuscher (Treasurer)	Shell
Razif Yusoff	Shell

The STF would like to acknowledge the contribution of the accredited Tripod Assessors to this project:

Peter Berlie	Kritericon BV
Bob Fox	BOHIKA cc
Ed Janssen	Ed Janssen Risk Management Consultancy
Ken Maddox	EPEX
Jan Pranger	Dutch Society for Safety Science/Krypton Consulting BV
Victor Roggeveen	Foundation for Clinical Safety Science/Pelican Consulting BV
John Sharp	Professional Coaching Australia
John Sherban	Systemic Risk Management Inc.

The following additional individuals are also acknowledged for their contributions to this project:

David Aghaiyo	Shell
Oscar Diederich	AdviSafe
Dieter Schloesser	LyondellBasell
Peter Wielaard	Better Work Together

Technical editing was carried out by Stuart King (EI).

Affiliations correct at time of publication.

1 INTRODUCTION

1.1 WHY INVESTIGATE INCIDENTS?

The investigation of, and learning from, incidents and accidents is fundamental to the risk management of organisations. In particular incidents should be investigated:

– To learn, grow, evolve and prosper:
  - To prevent further adverse incidents.
  - To demonstrate to regulatory authorities an organisation's commitment to establish what went wrong and to take actions to prevent recurrence.
  - To prevent future business losses due to disruption, stoppages, lost orders and costs of criminal and legal actions.
  - To improve leadership, morale, and attitudes to risk reduction measures.
  - To obtain everybody's cooperation for new or improved measures by their involvement in decisions taken to correct identified weaknesses.
  - To develop management skills involved with investigations that can be applied to other areas of an organisation, thereby improving efficiency and effectiveness.
  - To enhance an organisation's reputation.

– To meet ethical and moral obligations:
  - To prevent harm to people, environment, and also to the business from recurring incidents.

– To meet management system requirements:
  - To comply with the requirements of the organisation's management systems (e.g. health safety and environment (HS&E) system and quality management system) to investigate incidents.
  - To identify weaknesses in the management system.
  - To understand how and why things went wrong.
  - To provide a true insight and understanding of what really happens, how work is actually done and identifying any shortcuts or malpractices.
  - To identify risk management deficiencies, enabling improvements to lessen risk and apply lessons learned to other parts of an organisation.

– To meet legal compliance:
  - To comply with the laws of the country in which an organisation or company is operating.
  - To be able to better defend against any civil legal action/litigation.
  - To provide an organisation's insurers with information in the event of claims.

1.2 WHY DO INCIDENTS HAPPEN?

1.2.1 The Swiss cheese model

The Swiss cheese model of incident causation, originally popularised by Professor James Reason of the University of Manchester, is used extensively in the risk management of human systems in aviation, engineering and healthcare organisations and is often referred to in incident reports. The model likens an organisation's defences between a source of harm (e.g. a fuel source), and an undesirable outcome (e.g. a fire), as a series of barriers, represented by layers of Swiss cheese (see Figure 1).

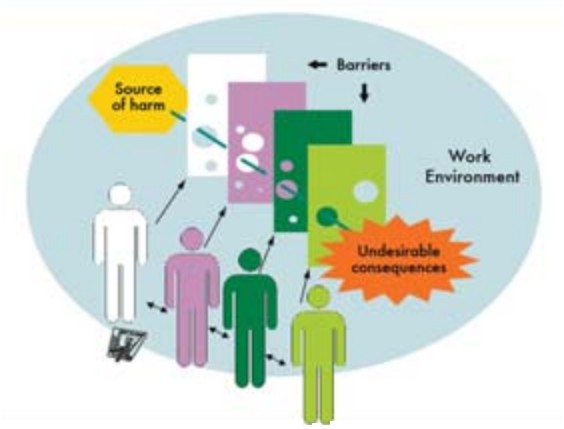


Figure 1 Swiss cheese model

These barriers are not perfect and will occasionally fail due to human and system weaknesses. These failures are shown as holes in the cheese slices and are continually varying in size and position. Normally the holes do not align and so the source of harm is prevented from creating harm. However, when the holes in all the barriers align, an incident occurs. Increasing the number of barriers in place would reduce the likelihood of all the holes aligning but this could be impractical or not cost effective. Eliminating the causes of the holes in the cheese, i.e. the causes of barrier failures, is the more effective solution.

To reduce risk within an organisation, barriers are established and maintained as part of a management system, and these span strategic, tactical and operational areas. Barriers are practical functions, as required by policies, standards and safety studies, and implemented using procedures, equipment and maintenance activities. The barriers are put in place and maintained by people with the competence to do so, in line with standards and specifications. 'Holes' appear in the barriers when individuals fail to keep them functional or in place, e.g. doing a critical task incorrectly or not doing a critical task at all. These human failures can, in turn, be traced back to influential causes, i.e. the preconditions, and the associated organisational weaknesses that created those preconditions. The model sequences human failures in terms of 'active failures' (immediate causes) and 'latent failures' (underlying causes).

Immediate causes are the substandard acts of people that led directly to a barrier failing and an incident. **Underlying causes** are those weaknesses hidden and dormant within an organisation which created the adverse influences (preconditions) that made the substandard act more likely to happen.

In summary, whilst incidents happen when people fail to keep the barriers functional or in place, e.g. people doing the wrong thing or people not doing what they should do, this is not generally due to flaws in the individual's character (e.g. greed, ignorance, malice or laziness), but because of flaws in the organisation's systems for managing risk.

See the STF and EI website for more information on the Swiss cheese model www.energypublishing.org/tripod/theory

1.2.2 Tripod theory of incident causation

The Tripod theory of incident causation is based on the Swiss cheese model and originated from research undertaken in the late 1980s and early 1990s into the contribution of human behavioural factors in incidents. It was undertaken by the Universiteit Leiden and the Victoria University, Manchester, and was commissioned by Shell International.

'Human error' is often quoted as the 'source' of many accidents. Whilst acknowledging that human error often triggers incidents, Tripod emphasises that these human errors do not occur in isolation but are influenced by external (e.g. organisational or environmental) factors.

Rather than focusing on blaming the individual that made the error, the Tripod approach concentrates on the logical analysis of these 'error inducing' systemic influences. It believes that minimising human error is far more effectively achieved by controlling the working environment – 'You can't change the human condition, but you can change the conditions humans work under' (Reason and Hobbs, *Managing maintenance error: a practical guide*, 2003).

Tripod integrates the adverse organisational and environmental influences on human behaviour so that the underlying causes of an incident can be identified, enabling effective remedial measures to be taken. These adverse influences are created by 'organisational weaknesses' which arise due to imperfect decisions made in the past. These decisions were probably arrived at with the best information then available, and their effects would have been dormant and hidden until later identified as contributing to an incident. The decisions may have been 'correct' at that time but subsequently become fallible due to an organisation's evolution, changing values and beliefs, culture, and technological advances, etc.

In Tripod, these adverse influences are called **preconditions** and are the environmental, situational or psychological system states or states of mind. They influence a person, or group of people, resulting in them performing critical tasks incorrectly or not doing these tasks at all. This action, or failure to act (called substandard acts), is the **immediate cause** (sometimes called an active failure) of a barrier failing.

The preconditions themselves arise from systemic/organisational factors and, in Tripod, these factors are called **underlying causes** (or latent failures). They can lie hidden and dormant, like pathogens in the environment, for a long time and do no harm until they interact with local factors, ultimately resulting in barriers failing and an incident occurring. Underlying causes indicate defects in the organisation's management system and are remote in time and distance from the incident location. Examples of these causes are weaknesses in policy, culture, design, training requirements, supervision and operating procedures. Remedies to improve these management systems, business processes and organisational culture issues (e.g. optimising maintenance schedules, minimising time pressures, ensuring effective competence management) often take time and resources to implement but do have wider implications and benefits, especially in terms of incident prevention and improving business performance.

The three entities (underlying cause, precondition and immediate cause), are collectively called the **Tripod causation path**, and their relationship to one another is shown diagrammatically in Figure 2.

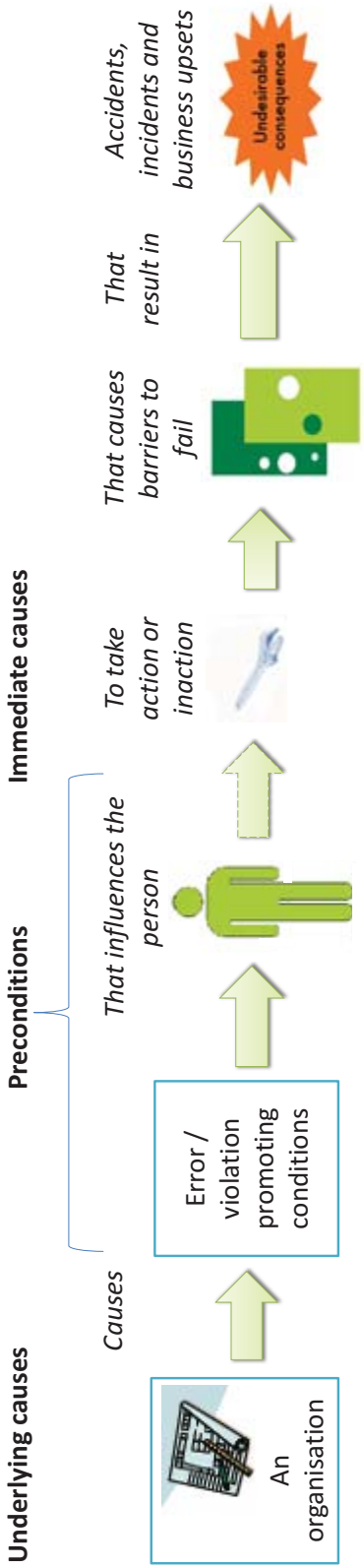


Figure 2 The Tripod causation path

2 TRIPOD BETA

2.1 OVERVIEW

In essence, Tripod Beta is a method of conducting an incident analysis in parallel with the evidence-gathering (investigation) process. It is based on the Tripod theory of incident causation; however, it goes further by also creating a model of the chain of events before and after the incident and, from that, identifying the barriers involved that should have prevented it. It covers the entire incident investigation, analysis and reporting process, which ultimately identifies the weaknesses or gaps in an organisation's management system and organisational culture that allowed the incident to occur.

The key steps in an incident investigation/analysis should be to identify the:

– chain of events from the normally controlled cause of harm to the ultimate outcome(s) (the undesirable consequences);
– barriers that should have stopped the chain of events, and
– underlying causes of why barriers didn't stop the chain of events.

However, most incident investigation techniques only deal with the chain of events and the barriers that failed. Often this results in only the symptoms and immediate causes of failure being addressed. Unlike Tripod Beta, few techniques deal systematically with the analysis of the reasons for the failures of barriers and help develop actions for correcting their underlying causes.

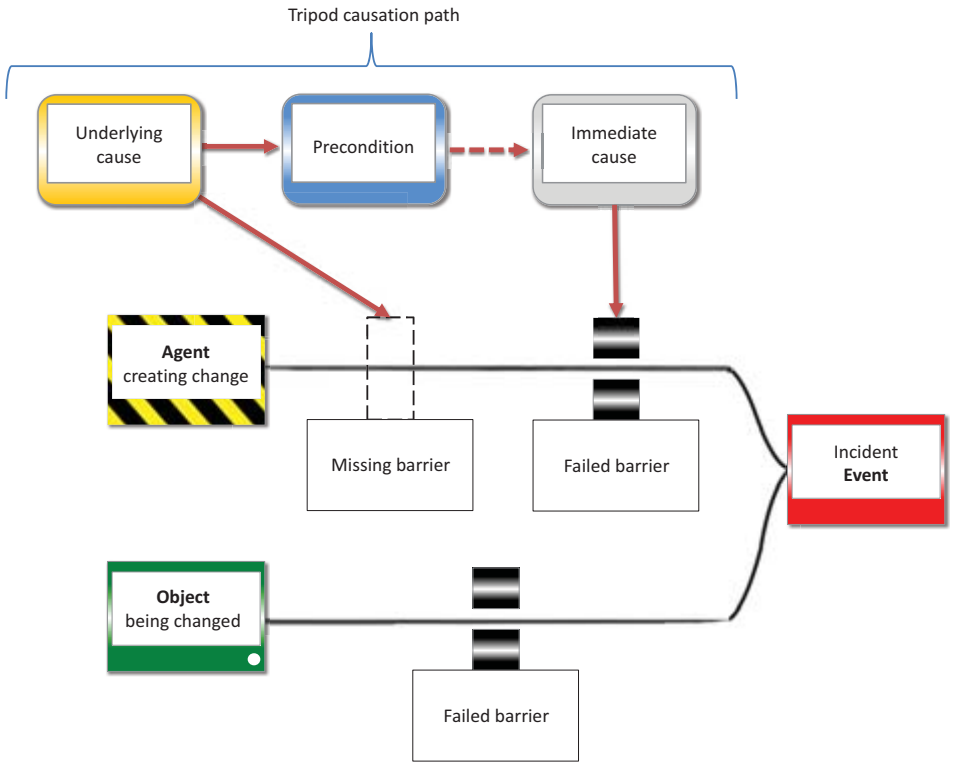


Figure 3 The Tripod causation path in the context of Tripod Beta

The Tripod Beta process starts by identifying the logical sequence of events in the physical progress of an incident and, from this, a graphical representation of the incident is created. This graphical model is known as the **core diagram**. It is designed to give an investigation team a mental picture of exactly what happened in the incident and help them recognise the likely sequences of events and relevant facts.

The next step is to identify the reasons underlying each failed, inadequate and missing barrier, many of which originate from weaknesses elsewhere in the business. These are often in decisions or actions taken by planners, designers or managers remote in time and location from the frontline operators. This is illustrated on the **Tripod Beta tree** which graphically shows the underlying causes for each failed, inadequate and missing barrier.

An example Tripod Beta tree illustrating the incident causation pathway is illustrated in Figure 3.

2.2 THE INVESTIGATION AND ANALYSIS PROCESS

To prevent an incident from recurring, the objective of an incident investigation and analysis is to identify and correct the barrier failures and the underlying causes that created, or contributed to, an incident. The systematic approach in achieving this is to first create possible conceptual models that describe the incident. This is based on information provided in an initial incident report and on how it is believed the incident occurred. Evidence is then collected and assessed to test, modify and eventually arrive at a truer model of the incident. This is the scientific approach to incident analysis used in a Tripod Beta analysis.

In the initial stages of an investigation the terms of reference of the investigation (i.e. its scope and remit) are established with an investigation team leader appointed to an investigation team. The team should include an accredited Tripod Beta Practitioner who, with involvement of team members who have the right knowledge and experience, will develop the Tripod Beta analysis of the incident. Subject matter experts (SMEs) should also be assigned to the team or consulted as appropriate.

Evidence gathering is used to construct a Tripod Beta model of the incident. In Tripod Beta, gathering incident evidence is iterative with the analysis process. This interaction between these two processes provides confirmation of the relevance of the gathered information and highlights further avenues of investigation. This enables investigators and analysts to systematically, efficiently and comprehensively:

– direct their evidence gathering;
– confirm the relevance of this evidence;
– highlight avenues of investigation ultimately leading to the identification of underlying causes;
– identify and resolve any logical anomalies whilst the investigation is still active, and
– produce a definitive and informative report.

The classification and linkage of the model's elements represent the cause-effect logic of the incident. Construction of the model also highlights investigation leads and information gaps that help the investigation team to cover the incident in sufficient depth and breadth to understand its full circumstance.

From the initial investigation report, Tripod Beta models are produced, refined and validated in light of further evidence. This continues until all relevant information has been identified and the Tripod Beta tree accurately reflects the incident. Finally, the incident report, with recommendations, is produced.

The overall phases of the investigation process are shown here and in Figure 4.

1. **Initial findings**: Concentrates on the incident site and its immediate surroundings, gathering the evidence concerning the events and their consequences.
2. **Organising evidence**: Information is organised to develop the chain of events. A timeline, e.g. a sequentially timed event plot (STEP), is a useful method for this to be achieved.
3. **Initial Tripod Beta model**: The core diagram of a Tripod Beta model defines what happened in the incident, in terms of **Agents**, **Objects** and **Events** and sets of Tripod Beta **trios**.
4. **Evidence gathering**: Further information is gathered through interviews, documentation reviews and research. Physical evidence relating to 'papers, people, parts and positions' is gathered and the Tripod Beta incident model adjusted accordingly.
5. **Detailed analysis and completion of the Tripod Beta model**: Failed management measures (barriers) are identified, validated and added to the Tripod Beta core diagram. Further investigations, studies and research identify the immediate causes and preconditions of failed barriers and also their underlying causes. This is an iterative process where, due to emergent evidence gathering, it may be necessary to revisit and change previous ideas about the barriers or causes. The interaction between the Tripod Beta analysis and evidence gathering continues until the investigation team conclude that they have satisfactorily completed the analysis of the incident.
6. **Report**: A draft report is presented to enable a critical discussion, followed by a decision on the adequacy of the analysis. Remedial actions are subsequently defined and added to the report.

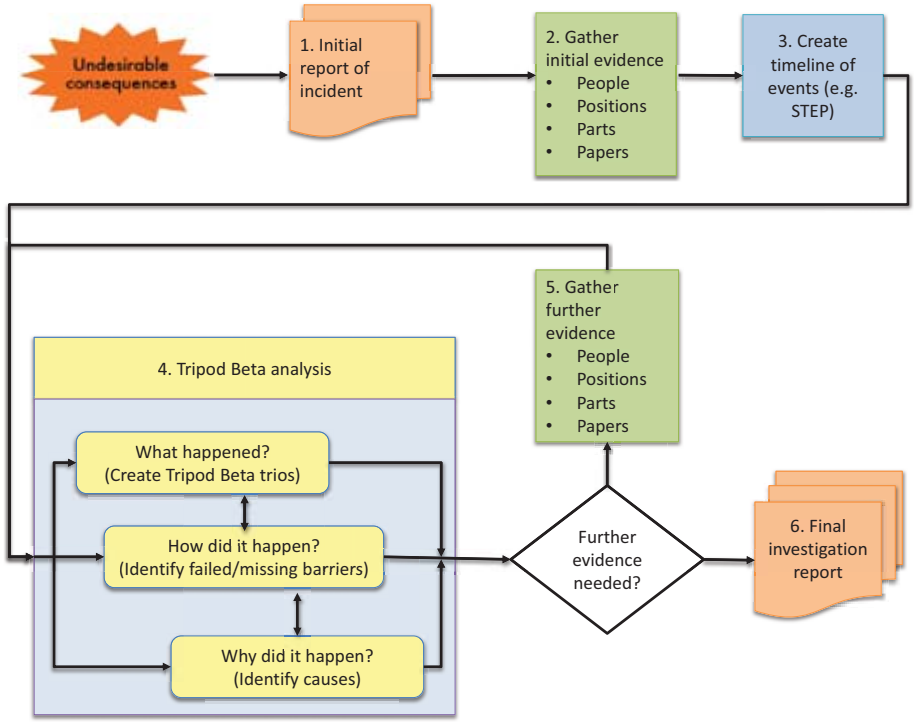


Figure 4 Investigation and analysis process

Following the Tripod Beta investigation and analysis, it will be possible to:
- give a precise description of the events leading to the incident, the incident itself and the response to the incident;
- describe the consequences of the incident in terms of injury, damage or loss;
- identify what barriers were in place, or should have been, to prevent the escalation of the incident;
- identify the substandard acts which led to barriers being breached;
- identify the preconditions which led to the substandard acts, and
- establish the systemic underlying causes of the incident.

At any time during the analysis, supporting notes describing evidence, facts, suppositions, opinions, etc. can be written for each element in the model which ultimately facilitates the generation of a report.

Tripod Beta analysis is extremely versatile and can be used in any industry or organisation and for all types of business upsets and incidents, including, but not limited to:
- people's safety, health and wellbeing;
- process safety (asset integrity);
- environmental impacts;
- financial losses – cash flow, competitiveness and profitability, budget overruns, tax;
- production losses;
- security lapses – damage or theft of property, unauthorised entry;
- social – impact on community;
- legal – non-compliance with laws, failure to obtain licences and visas;
- IT system failures – e.g. hardware, software, virus, unauthorised intrusions, data theft;
- damage to reputation;
- quality shortcomings, and
- project delays and losses.

Tripod Beta is well suited to deal with asset integrity and major hazard incidents as well as the more frequent personal safety incidents.

2.3 LEVELS OF INVESTIGATION – WHEN TO USE TRIPOD BETA?

Whilst it is important that all accidents and incidents are investigated, it is not realistic for them all to be treated the same. Moreover, investigating all incidents with the same level of rigour would waste human resources and not be effective. Accordingly, not all incidents require the formality, depth and thoroughness of a full Tripod Beta investigation and analysis.

To determine the different levels of investigation it is generally accepted practice to classify them by their severity, i.e. degree of harm caused. For near-miss incidents, where damage was fortunately limited but could have caused severe harm in other similar circumstances, a risk assessment matrix can be used to determine the level of the investigation – e.g. as set out in the Hearts and Minds *Risk Assessment Matrix* tool (www.energyinst.org/heartsandminds). However, the organisation should be aware that severity does not always equate to learning potential.

Levels of investigation will be influenced by many factors, e.g:
- legislation in the country of the incident;
- the actual or potential severity of the incident;
- guidance on these levels already in place for an organisation;

Tripod Beta: Guidance on using Tripod Beta in the investigation and analysis of incidents, accidents and business losses

ISBN: 978 0 85293 673 3

Full version available at:

http://www.energypublishing.org/tripod/beta

Published by the Energy Institute, in support of the Stichting Tripod Foundation

Energy Institute
61 New Cavendish Street
London W1G 7AR, UK

t: +44 (0) 20 7467 7100
f: +44 (0) 20 7255 1472

The Stichting Tripod Foundation is a non-profit organisation. Income from the sale of this publication is reinvested into the continuous development of the Tripod methodology, and helping to improve the standard of risk management and incident investigation in industry.

www.tripodfoundation.com

ISBN 978 0 85293 673 3
Registered Charity Number: 1097899