

# ***The role of automation and humans in nuclear power plants***

*Report prepared within the framework of the  
International Working Group on  
Nuclear Power Plant Control and Instrumentation*



INTERNATIONAL ATOMIC ENERGY AGENCY

IAEA

**THE ROLE OF AUTOMATION AND HUMANS IN NUCLEAR POWER PLANTS**  
**IAEA, VIENNA, 1992**  
**IAEA-TECDOC-668**  
**ISSN 1011-4289**

Printed by the IAEA in Austria  
October 1992

**PLEASE BE AWARE THAT  
ALL OF THE MISSING PAGES IN THIS DOCUMENT  
WERE ORIGINALLY BLANK**

## FOREWORD

In recent years the need to improve the interface between man and machine has come to the fore, as it has been demonstrated that human error is one of the principal factors contributing to possible accidents. This has been confirmed by risk analyses as well as by the experience gained from accidents and abnormal events at nuclear power plants. At the same time man-machine interaction has been playing an ever increasing role since the new instrumentation and control system can be matched more easily to the needs of the operator. Activities concerning improvements in the control room and man-machine interface in nuclear power plants have increased.

This document provides a basis for assigning functions to men and machines and for achieving a desirable balance. It should be particularly useful to designers of new systems, where a large number of assignment decisions will have to be identified, taken and documented. In addition, the methodology can be used by utilities for plant modification and upgrades. The document may also be employed for examining existing assignments in a system since the principles on which the document is based are generally applicable. The document may be useful to those who develop requirement specifications for automation, to technology designers who design automated machines, and to researchers who intend to further refine the function assignment methodology.

The ultimate worth of the document will depend upon how well it supports users in assigning functions in practical situations. Readers are invited to provide comments and observations to the IAEA, Division of Nuclear Power, based on their experience in using the proposed methodology. If appropriate, the document will subsequently be re-issued, taking such comments into account.

The document is the result of a series of advisory and consultants meetings held within the framework of the International Working Group on Nuclear Power Plant Control and Instrumentation (IWG-NPPCI) in 1989-1990. The final version of the document was prepared with the participation of experts from Canada, France, Germany, Japan, Sweden, the United Kingdom, the USA and the former USSR.

Special thanks are due to Mr. J. Jenkinson of Nuclear Electric plc, United Kingdom, who compiled and edited the document from contributions provided by the expert group members, particularly R. Olmstead of Canada, A. Oudiz of France, W. Bastl of Germany and B. Sun of the USA.

The IAEA officers responsible for preparing this document were V. Neboyan and A. Kossilov of the Nuclear Power Engineering Section, Division of Nuclear Power.

## *EDITORIAL NOTE*

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

*The views expressed in the papers, the statements made and the general style adopted are the responsibility of the named authors. The views 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.*

*Authors are themselves responsible for obtaining the necessary permission to reproduce copyright material from other sources.*

*This text was compiled before the recent changes in the former Union of Soviet Socialist Republics.*

# CONTENTS

1.	INTRODUCTION .....	7
1.1.	Background .....	7
1.2.	Scope of the document .....	9
1.3.	Key terms .....	9
1.4.	General .....	10
1.5.	Influence of plant conditions .....	12
1.6.	Maintenance and testing .....	12
1.7.	Operator support .....	13
1.8.	Approaches to automation .....	13
2.	CAPABILITIES AND LIMITATIONS OF HUMANS AND AUTOMATION .....	13
2.1.	Capabilities and limitations of humans .....	13
2.2.	Capabilities and limitations of automation .....	14
2.3.	Integrating man and automation .....	15
2.3.1.	Achieving system performance .....	15
2.3.2.	Human performance .....	16
2.3.3.	Automation performance .....	17
2.3.4.	A model of man-machine interaction .....	17
2.3.5.	'Hard' manual control, 'soft' manual control and automation .....	20
3.	ACHIEVING A BALANCE BETWEEN AUTOMATION AND HUMAN ACTIONS .....	22
3.1.	General discussion .....	22
3.1.1.	Function analysis .....	23
3.1.2.	Basic principles .....	23
3.1.3.	Systematic design .....	24
3.1.4.	Design team .....	24
3.1.5.	Influencing factors .....	26
3.1.6.	Recognizing component strengths and limitations .....	31
3.1.7.	Task and job content .....	31
3.2.	Assigning functions .....	32
3.2.1.	General discussion .....	32
3.2.2.	Required system performance .....	33
3.2.3.	Human performance data .....	34
3.2.4.	Function classification .....	36
3.2.5.	Hypothesized task assignments .....	39
3.2.6.	Evaluation of assignments .....	40
3.3.	Interfacing with related design activities .....	40
3.3.1.	Operator task specifications .....	40
3.3.2.	Operating procedures .....	41
3.3.3.	Specifying automation .....	41
3.3.4.	Implications of the assignment process .....	42
3.3.5.	Final audit .....	42
3.3.6.	Operational feedback .....	43
4.	RESEARCH MATTERS .....	43
4.1.	Types of human factors research .....	43
4.1.1.	Traditional ergonomics studies .....	43
4.1.2.	Human behaviour studies .....	43
4.1.3.	Field observations .....	44
4.1.4.	Advanced systems studies .....	44

4.1.5. Control room evaluations .....	44
4.1.6. Human error studies .....	44
4.2. Allocation of functions — history and status .....	45
4.2.1. Background .....	45
4.2.2. Types of task .....	45
4.2.3. Attributes of humans and automation .....	45
4.2.4. Relative strengths of humans and automation .....	46
4.2.5. Modelling man–machine interaction .....	46
4.2.6. Machine performance .....	47
4.2.7. A simple model of human performance .....	47
4.2.8. System design goals .....	48
4.3. Assignment methodology status .....	48
5. FUTURE TRENDS AND NEEDS .....	50
5.1. Automation .....	50
5.2. Knowledge based systems .....	50
5.3. Performance data .....	51
6. RECOMMENDATIONS .....	52
APPENDIX A. EVALUATION TECHNIQUES .....	53
APPENDIX B. A TYPICAL ‘FITTS’ LIST .....	55
REFERENCES .....	57
BIBLIOGRAPHY .....	59
ANNEX. PAPERS PRESENTED AT ADVISORY GROUP MEETINGS	
Development and application of computerized operator aids for German nuclear power plants .....	63
<i>W. Bastl</i>	
The balance between automation and human actions: The Sizewell B perspective .....	89
<i>D.B. Boettcher</i>	
Development of an autonomous nuclear power plant under the Nuclear Frontier Research Policy in Japan .....	97
<i>F. Tanabe</i>	
The balance between automation and human actions in Japanese nuclear power plants: Current status and future prospects .....	105
<i>K. Nakamura, S. Hiei</i>	
The balance between automation and operator control .....	133
<i>A. Colas</i>	
Current philosophy in France regarding the required level of automation in nuclear power plants and its relationship with the role of the operator .....	139
<i>J.M. Leckner</i>	
Comments on the balance between automation and human actions .....	147
<i>Y. Shinohara</i>	
Studies on the process operators’ work and control room design in Swedish nuclear power plants .....	155
<i>G. Olsson</i>	
Analysis of the main factors determining the degree of automation in NPPs .....	159
<i>M.N. Mikhailov</i>	
List of Participants .....	173

# 1. INTRODUCTION

## 1.1. BACKGROUND

The need to improve performance and safety of nuclear power plants and other complex industrial processes has led to increased use of automation. In addition, the ongoing revolution in computing and information system technology is leading plant designers, through economic and performance incentives, to continually increase the extent of automation. At the same time, worldwide experience confirms that societies are demanding higher standards of designers and operators of nuclear plants. More automation, as such, is not necessarily the total solution to these problems. A major aim of this document is to promote increased safety by assisting the designer to improve the process of assigning functions to humans and to automation.

Plant designers do not always demonstrate a systematic approach to making the necessary series of critical decisions which assign functions to men or machines, that is to establish the extent and role of automation. This view is supported by data from significant event reports, and from reviews of past and current designs. Similar sources indicate that design teams have not always adequately considered the capabilities and limitations of humans when making these ad hoc decisions. Although post-Three Mile Island studies in Europe, such as that carried out by CEC JRC Ispra in 1980 [1], have examined a comprehensive range of factors material to safe operation including design, training, simulation and management, there has been little formal examination by such groups of the actual role assigned to operators.

Although nuclear power plants are designed to exacting standards, using thorough quality assurance systems, they cannot be made perfect. In practice, the extent to which plant and human behaviour can be analysed and predicted is limited. This situation effectively ensures that there is a continuing role for the operator for the foreseeable future. As automation takes over the more prescriptive tasks, the role of the operator becomes that of a situation manager - an innovator to manage the unexpected.

The first step in achieving the optimum man-machine interface is, where possible, to design the plant so that natural phenomena contribute to its stability and controlability, thereby reducing the active contributions from both man and machines during operation. Much recent attention has been focused on the concept of 'inherently safe reactors', which will simplify safety system requirements and information and control system complexity. If such concepts eventually lead to commercial power reactor designs, there may well be simplifications in plant systems but overall protection, control and monitoring requirements will still require systematic assignment of functions between men and machines.

In the face of this climate, the International Atomic Energy Agency (IAEA), following a recommendation of the International Working Group on Nuclear Power Plant Control and Instrumentation (IWG-NPPCI), formed in 1989 an expert group with extensive experience in nuclear power plant automation. The task of this group was to advise on the appropriate balance between the role of human actions and automation in nuclear power plants. Even the most recent design procedures, e.g. IEC Standard 964 [2], make no attempt to define a systematic method for the assignment of

functions between men and machines. Consequently, the expert group undertook to develop the basis for such a design method. The present report may form the basis for a future design standard. In producing this report, the expert group was fully aware of IEC Standard 964. For clarity, it has been decided to adopt somewhat different terminology from that established in IEC 964. The methodology described is, however, intended to be entirely complementary to the approach defined in the Standard.

Based on earlier research and their own experience, the expert group determined that a single, fully deterministic solution to the task assignment problem is not possible. However, since for reasons discussed in the present report, the tasks performed by the operator are expected to change to those of a situation manager, it is imperative that a systematic process for assigning tasks must be used by the design team. IEC Standard 964 calls for a formal assignment of functions to men and machines to be carried out. This report supports that approach by proposing a methodology to achieve such an assignment. Some of the steps in the proposed assignment process are qualitative in that they require judgmental decisions based on certain principles of cognitive engineering and predefined good human factors practice. The general thrust of the process described is to free the operator from tasks he is not suited for and to assign him the tasks that benefit from uniquely human capabilities such as pattern recognition, extrapolation, aggregation, abstraction and the ability to plan.

The proposed methodology builds upon earlier published work but adopts a pragmatic approach, suited to real-project needs. It is summarised in a simplified diagram (Figure 3.3) illustrating the main features of the task assignment process. Several important and desirable principles and practices from the report can be highlighted:

- (1) Human factors input to any design process should occur at the outset when formative, top-level decisions, including those on system objectives and performance, are being made. If this does not happen, it may not be possible for human factors to have the necessary positive influence on later design decisions.
- (2) The design team performing the assignment process must contain the correct mixture of skilled individuals, with experience of plant design, plant operations and human factors.
- (3) The design team must be trained to be aware of the strengths and limitations of humans in the plant operations environment.
- (4) Automation should be used to provide an extension of man's physical and mental capabilities. Tasks which are rigidly prescriptive, tedious and stressful should be automated, but care must be taken that the resulting job descriptions are such that operator capabilities are fully and properly utilised.
- (5) Wherever possible, systems should be designed on a fail-safe principle and with sufficient reliability to avoid the need for operators to intervene when automation fails. In addition, systems should be designed so that when they fail, they do so gradually, so that operators are not required to suddenly assume control in areas where they may have had little practice or experience. Adopting a 'defence in depth' approach can enable the designer to avoid the need for the operator to take over when automation fails. Ref.[3] discusses this approach in some detail.

- (6) To achieve good results, there must be several cycles of task identification, assignment and evaluation of the total interface. Representatives of the plant operations management must be a party to the evaluation phase and in so doing establish the job descriptions for the key operations staff.

This document is intended for designers, safety analysts, researchers and managers. The assignment of tasks between man and machine may be the most critical activity in the design of new process plants and major retro-fits. It warrants a design approach which is commensurate in quality with the high levels of safety and production performance sought from nuclear plants.

## 1.2. SCOPE OF THE DOCUMENT

The report presents a methodology for achieving a balance between automation and human actions which is intended to form part of and complement a wider set of hierarchical, top-down design activities. The methodology is summarised in Figure 3.3. The methodology is intended to apply to all activities associated with the operation of nuclear power plants, including normal operations, refuelling, maintenance, testing, management of abnormal conditions, etc. To appreciate the basis of the proposed methodology the reader will need to address certain fundamental concepts to do with automation and human performance which are outlined in Section 2 and which discuss the capabilities and limitations of humans and automation. These sections are not an exhaustive list of capabilities although reference is made to sources of such information. The report emphasises the need for technologists to give adequate consideration to human interactions with systems.

Section 3 of the report provides the proposed methodology. The section also provides an introduction to the concepts on which the methodology is based and sets out the iterative, practically-based approach to the assignment process. Sources of data are discussed together with the several factors which influence the overall process. The use of feedback is discussed, together with the role of final audit. Section 3 also expands on the need for and uses of performance data both for the overall system and the human and machine components in it. In Section 4 a resume of relevant research work is given and in Section 5 current trends and the need for additional research work are examined. Section 6 gives recommendations which arise from the work.

## 1.3. KEY TERMS

The way in which certain terms are used in this document may require explanation.

Automation (1): the technique of making an apparatus, process, or a system to operate with self-acting or self-regulating mechanism. The process of automation assigns a hitherto human function to a machine, including the assignment of information processing to support operator decision.

Automation (2): the hardware, software, etc., which comprises the automated systems.

Design Team: the group of individuals who conceive, plan, create, assess, or implement a specific function for plant and related systems and equipments, including hardware, software, procedures, and

interfaces. This includes conceptual design of the control room and other interfaces, assignment of all interface activities and controls to man or machine, and detailed design of the interface.

Machine: a man-made process or device capable of performing one or more tasks assigned to it. The term machine includes a plant, process equipment, instrumentation, information processor, and automation equipment.

Operator: all staff who are involved with the operation, maintenance, testing, and overseeing etc. of nuclear power plant.

#### 1.4. GENERAL

Safe, reliable and economic operation of a nuclear power plant requires sound plant design and effective operation and maintenance activities. In all aspects of operation, human operators are involved with the plant in various ways and to varying extents. Operators generally interact with the process in two ways: firstly, by receiving information from the process through information displays and secondly, by making decisions and imposing these on the plant directly through manual controls and indirectly through automatic control systems. Through these two routes, the behaviour of the operator depends on the information he receives and he may in turn modify the behaviour of the machine through the control process. In many automatic systems the association between man and machine may be less obvious but nonetheless exist in the form of manual intervention in the form of setting, adjustment or control. In other cases, close coupling exists between plant and humans in the form of routine, preventative or corrective maintenance activities.

The way in which the plant is designed and in which the tasks of the operating staff are defined has an important bearing on the way in which the plant runs. For effective design of plant, it is essential to consider the role of automatic systems and the tasks which are given to the human operators. The plant designers carry a responsibility not only of the satisfactory performance of the plant but also the well-being of those who operate and maintain it.

Automation is an established feature of large industrial processes in modern society including aerospace, chemical, paper, food, as well as nuclear power plants. In the development of nuclear power plants throughout the world there has been a trend towards the use of greater amounts of automation. While automation generally improves productivity and efficiency, high levels of automation may lead to a decoupling of the human operator from process and the machine. In reality, automation comprises closed-loop control, sequence control as well as automatic information processing to support operator decision-making (increasingly described as operator aids). The progress which has been made in the technology of electronic devices ranging from instrumentation and data communications equipment, to programmable processors and computing systems, has resulted in increased use of automation.

Factors which reflect this trend include:

- The need to achieve and maintain high levels of safety and reliability both for public protection and for the effectiveness and well-being of operators.
- The need to increase production reliability.

- The need to control plant operations (including maintenance) with increasing optimisation in order to improve plant performance and plant life.
- Increases in plant size and complexity and hence capital investment, which require increased levels of protection and assurance.
- Developments in centralised control and monitoring, which lead to increased amounts of data and the consequent need to process and handle this information.

This document considers these factors in evaluation of the capabilities of man and machine functions and the various factors that influence the balance between automation and human actions in nuclear plant operation.

A review of approaches to automation adopted by a variety of plant designers, consultants and utilities shows that the degree of automation varies from country to country but also from plant to plant. In general, it may be said that in all countries, there has been a trend towards increased automation. This is no doubt partly a result of increased safety expectations, increasing plant complexity and improvements in control and automation technology. Whilst the basic trend is common to a number of countries the rate at which automation has developed has differed. This may be related to economic and socio-technical factors associated with availability of trained personnel and the rate at which organizational structures can evolve.

In general, the use of closed loop control for process parameters such as temperature, pressure, flow, etc. is common. In many plants, automation is extended to include automatic control of plant start up, mode change and shut down. This form of sequence control may be applied to a plant item where complex auxiliary systems are provided, a group of plant items where correct sequence of operations is important or where automatic change-over or standby provisions are necessary or ultimately, to the whole of the plant systems. In this context, the basic operational role of the plant, i.e. base-load or load-following, etc., must be taken into account. Base-load plants may require a lower level of sequence control to reflect the less frequent change of operating mode. Also, the range over which automatic closed-loop controls are required to perform may be less than in a load-following plant. Automation is also employed to reduce scram (trip) frequency and hence improve plant availability by backup controls or limitation systems to prevent plant parameters reaching limits which would invoke protective action. Similar approaches are also used to reduce load cycles on structures and components. Decisions on the extent of automation in these areas may indeed be dictated by a conscious desire to include the operator in plant operations in order for him to retain essential skills.

In almost all cases, protection of plant safety limits and the control of the risk of radioactive release is performed by fully automatic equipment. This is necessary to achieve the very high performance and reliability targets which regulatory authorities rightly demand. Differences do occur between various countries in the way in which protection systems are designed and the extent to which safety is achieved by redundancy of system or equipment. Differences also occur in the way in which continued protection system performance is assured. Traditionally, this has been achieved by regular, methodical testing to defined procedures, with appropriate manual methods for quality assurance.

Differences between plant designs and national practices occur in the extent to which manual intervention in automatic protective sequences is required or is possible. In general, there is a trade off between system complexity and the need for operational flexibility, e.g. manual intervention facilities to allow operators to adjust protection system limits, veto system operation and support protective actions by direct manual intervention in transients. Often, it has been judged that flexible manual intervention facilities are justified to counter the effects of consequential plant or equipment failures.

#### 1.5. INFLUENCE OF PLANT CONDITIONS

The degree to which manual or automatic control and/or information processing is appropriate is influenced by plant conditions. Production of the necessary control and information system specification requires a precise knowledge of plant and process dynamic behaviour. For all normal and for certain abnormal modes where this knowledge is available it can be utilised in the assignment of functions and the resulting control and information system design. However, under severely abnormal or accidental conditions the quality and veracity of such knowledge may be uncertain. In such cases the flexibility and adaptability of the human operator is indispensable.

Where automation is deemed appropriate for some operating conditions there is a need to consider the change of the automatic processes in response to abnormal plant conditions. Safety and reliability considerations indicate that varying degrees of operator supervision are appropriate under different operating conditions in order to achieve required overall system reliability targets.

The area of operator decision support is one where a combination of human actions and automated features is increasingly employed. Here, automation techniques are used to increase the value of the information by processing data of real and current needs and excluding less relevant or untimely information to avoid cognitive overload.

#### 1.6. MAINTENANCE AND TESTING

As plant size and complexity grows, the task of testing and maintaining systems becomes increasingly important in staffing, training and human reliability. Automation is seen as desirable to support this increased dimension in plant operations. Computerised aids have been developed to remove the need for humans to undertake tedious, difficult or dangerous procedures. In the case of testing carried out in a hostile environment (e.g. radiation areas), reduced doses to operators and a potential reduction in the frequency of access to controlled conditions adequately justify an increasingly automated approach. It is clear that automated testing can improve the quality of the test process, bringing increased repeatability and quality assurance. Additional effort must be applied to ensuring that the quality of the automatic test system is adequate and it is suitably certified.

Automated equipment diagnosis has been developed which takes into account long term plant operating experience and the result of testing and analysis. Use is made of signal correlation techniques in order to diagnose plant state and, sometimes, to predict incipient problems. Thus, preventive maintenance can be carried out in order to prevent loss of output or availability. A major additional benefit is derived from the ability of such systems to provide good, auditable test records for subsequent audit or analysis.

## 1.7. OPERATOR SUPPORT

The area of operator decision support is one where a combination of human actions and automated features is seen as increasingly warranted. Here, automation techniques are used to increase the value of the information by relating processed data to real and current needs and excluding less relevant or untimely information to avoid cognitive overload. IAEA-TECDOC-444 [4] reviews a range of operator support aids and discusses factors involved in their selection and implementation.

## 1.8. APPROACHES TO AUTOMATION

In the past 15 years or so, there has been a steady increase in both the production reliability and safety of computer-based equipment that member states have used to automate plants. As a result, there have been less inhibitions to the use of automation. By suitable design, using redundant, diverse or distributed systems, design availability and reliability targets can be readily met. Availabilities in excess of 98-99% are commonly achieved.

The zenith of automation is currently represented by the concept of a fully integrated centralised control-interface, where the vast majority of plant monitoring, decision-making and control functions are subsumed in an integrated, computerized man-machine interface. To some extent, these functions can and have been realised in working designs but technological limits constrain the extent to which high-level information processing and decision-making can be carried out by computer and the regulatory climate determines the extent to which plant safety-related information can be fully automated.

It is possible to predict an expansion of automation, both in scope and degree in the coming period. Reasons for this will include: requirements for higher operating reliability, safety and performance, increasing shortages of skilled, trained staff to operate plants and the availability of cost-effective computer technology. Because of the potential consequences of machine failure in highly automated systems, the design process should seek to introduce additional automation in well planned stages which each build upon the successes of earlier ones.

This document does not attempt to describe all the existing ranges of automation which are to be found nor does it seek to summarise the approaches taken. The reader is referred to IAEA Technical Reports Series No. 239 [5], which provides some examples of approaches to automation. A further useful review of automation practices is contained in Ref. [1].

## 2. CAPABILITIES AND LIMITATIONS OF HUMANS AND AUTOMATION

### 2.1. CAPABILITIES AND LIMITATIONS OF HUMANS

A human operator possesses a number of desirable features which are not present in current levels of automation. Humans are creative, flexible, can use stored knowledge, routines and patterns to cope with novel, unexpected or beyond-design-basis situations. Such conditions could arise because combinations of or sequence of events may occur or develop to produce an unexpected situation. Human ability to recognise patterns within complex sets of information is of particular interest during abnormal and accident situations although this ability is unlikely to be

consistent during adverse conditions, if operators are overloaded with tasks or if the design of the man-machine interface is inadequate. A related skill is the ability to abstract useful information from systems which are 'noisy' as is the human capacity to form overviews or decisions from incomplete sets of information. Whilst human actions cannot be guaranteed to be totally error-free, the human has the ability to detect his errors and correct them, when the information system provides the necessary cues and the control system and plant response allows time for corrective action to be taken.

Data from human error studies confirm that the human tendency to make mistakes is a significant problem. Human errors may be mitigated by the use of procedures for certain types of task but further errors can occur in the use of a procedure if the procedure has shortcomings, an operator relies on memory, departs from the procedure or misinterprets an instruction. This approach therefore requires careful procedure design verification and validation to ensure the documentation is closely matched to the task in hand.

A further problem is that some aspects of operator performance can degrade under certain stressful conditions. However, this degradation is often gradual in nature, and hence, there is the possibility for the operator to seek additional support or modify his strategy in such circumstances. Problems can also occur due to under-stimulation of operators.

## 2.2. CAPABILITIES AND LIMITATIONS OF AUTOMATION

Automation is used in a variety of ways in nuclear power plants. These applications can be classified by the way in which they relate to the human operator and the degree of control or influence he has over them as follows:

- Information and control systems which allow operators to monitor and control processes.
- Computer based operator aids which process and summarise plant information in a succinct form, information analysis systems, information reduction and management systems, equipment monitoring systems, diagnostic systems, procedure support systems, etc.
- Automatic functions which aid or supplement the operator's control over a sequence or process, such as plant sequence control, closed loop control, etc. which can typically be placed under manual control when desired.
- Automatic features which ensure plant safety, such as detecting variables which exceed safe limits and initiating appropriate safety actions, such as reactor scram, initiation of safeguards equipment, etc. Also included in this category are systems which prevent unsafe conditions such as interlocks, etc. Typically there is little scope for operator intervention in such systems.

In certain cases, it is not possible for the feature to be placed under the control of the operator, for example, reactor scram functions. It is often the case that the operator is given part-responsibility to ensure the correct operation of a function. An example of this is the use of operator aids to present information but still retaining the human to diagnose faults and decide on appropriate corrective actions.

This classification is not indicative of the complexity of the automation required to achieve the functions described. For example, an area of high complexity is likely to be that of advanced operator aids, the second category in the above list.

A list of the desirable features of automation is long because systems can be created and tailored to meet the needs of a variety of tasks. Key features of automation which are commonly exploited are: speed, reliability, repeatability, accuracy, rapid response, sustained performance, ability to handle large amounts, high rates and large capacities, etc. The response of automation can increasingly be tailored to given sets of conditions and the behaviour of automation systems can be programmed. The behaviour and response of automation systems can be defined to a large extent and it can be pre-analysed and justified. Automation can be used to carry out tasks which are unsuited to humans because of their arduous, hazardous or repetitive nature.

Undesirable aspects of automation stem from the above desirable features, where the feature is inappropriately matched to the needs of a task. Automatic system performance cannot readily be modified unless such flexibility has been built into the design. As a result, where the needs of a task change or where they differ from the assumptions made by the designer, the system may not perform to expectations.

A further problem comes from the ways in which automation, including both hardware and software, tends to fail. Simple devices, with little or no in-built redundancy, may fail in a discontinuous way, and often become of no use until repaired. If a machine is required to fail infrequently or if it must fail gradually to allow manual intervention, it may be necessary to employ redundancy, diversity or other techniques at the expense of increased maintenance tasks. Aside from the resources required to carry this out there may be increased errors from maintenance and overall system reliability and availability may start to fall.

## 2.3. INTEGRATING MAN AND AUTOMATION

### 2.3.1. Achieving system performance

Successful integration of man and machine in a system requires overall system performance goals to be defined. Designers of technological systems can readily specify availability, reliability, speed, accuracy, etc. This includes the specification of software in the sense of machine instructions. In past and present designs of complex process systems, the same degree of excellence in the specification of detailed human tasks (or the 'software' for human, namely operating instructions and other documentation), has not always been demonstrated.

Traditionally, engineers of many disciplines have been trained to think predominantly in terms of machine capabilities rather than to consider human performance. Operational events in the nuclear industry throughout the world have, in recent years, shown the problems caused by this situation and many reviews of nuclear plant designs have shown the need to give adequate consideration to so-called 'human factors'. Although the human factors specialist (ergonomist, psychologist or engineer) is now much more in evidence in design, operation and review teams, the influence of such skills is still not sufficiently widespread or yet fully effective.

The published literature on human factors contains lists of the various attributes of humans and machines. Section 3.2.3 discusses their

utility and identifies limitations in the use of such data for practical power plant design. Elementary human engineering principles must be adhered to in the assignment of functions and the design of operator tasks but there will need to be a practical infeed from experienced design and operating personnel. A fundamental requirement is that human capabilities and skills are not exceeded by the tasks required of them, under the most adverse conditions. A secondary, but equally important objective must be to optimise the role of humans in the overall man-machine system. These objectives need to be pursued by suitable analysis techniques.

Quantification of human performance must take account of the various human performance shaping factors which apply. Analysis of the human and machine contributions to a system can indicate areas of design which are critical to safety or plant operations or where there is an imbalance between the two contributions. This enables design effort to be effectively targeted to such areas.

A goal of the design team is to achieve an optimum system design which maximises availability/reliability, whilst minimising initial investment and support resources. This implies that for a given set of criteria, there will be an optimum level of automation to be applied. In the broadest sense this characteristic does not apply to human systems, where no such optimum can be easily demonstrated. A single human in a system may exhibit a reliability characteristic. As additional humans are introduced into a human system, some increase in potential reliability may accrue from error checking, etc. but problems may occur due to information flow limitations, control structure effectiveness and job organization complexities.

#### 2.3.2. Human performance

Optimum human performance within a system can only be claimed if the technology designer has matched the tasks assigned to the operator closely with his inherent and acquired capabilities. These depend on the type of personnel chosen, their education, training and development and the experience they have had in plant operations or maintenance. To the extent possible, the designer should establish the characteristics of the intended operator population, either from standard sources, where these are applicable, or if necessary by direct studies of the population. If it is necessary to make assumptions about staff capabilities, these should be fully documented. The design of the man-machine interface should be carried out in accordance with human factors principles to ensure an optimised system.

Human performance in plant operations and maintenance cannot be decoupled from the management and operating climate in which these take place. The way in which individuals see their roles, relate to each other and to the tasks in hand are key factors in achieving optimised performance. Management attitudes and practices can powerfully influence this. Whilst the designer cannot directly control these, he should have an appreciation of the way in which these factors could modify operator performance and operation of systems.

The process of assigning functions must include consideration of the whole job which will result for the operator. The total job content and demands must lie within acceptable limits. Factors such as physical and mental workload, intellectual challenge, motivation, status, career prospects, skill usage, etc. must be considered. If an unacceptable job would result from a particular set of function assignments, it is necessary

to revise the detailed assignments or, alternatively, the personnel selection criteria.

### 2.3.3. Automation performance

For a complex man-machine system, the human and machine components must operate together. The system effectiveness is influenced by the man-machine task specifications and needs which are set by the plant and automatic system design and the points at which optimum machine performance and satisfactory human performance is achieved may not coincide. The designer must ensure that the overall system he designs is robust against the most adverse possible conditions and combinations of events which will apply. The designer must therefore consider the best use of automatic devices to support operators in adverse situations [6].

Optimising automation performance therefore can be regarded as a part of optimising the assignment of functions, since the designers ability to manipulate machine performance is probably greater than his ability to manipulate that of the humans in the overall system. Clearly, the performance of individual machine elements in the system will need to be optimised at a detailed level, but where significant human involvement or interaction is planned, that optimisation must be centred around the needs, capabilities and characteristics of the users.

As plant and automatic systems become more complex, it is increasingly necessary to ensure that the users understand the operation of the automation and what functions it performs. Even more necessary to the user is a knowledge of the functions for which the automation systems have been provided, a knowledge of what they achieve when working normally and (of increasing concern), the way in which they fail and what is required of the operator when they do. In modern automatic systems, there is often a diversity of techniques and equipment. This increases the problems of maintenance support and also makes it more difficult for users to understand the working of a system. Therefore caution must be exercised in designing such systems. These factors require an informed attitude on the part of the designer, trainer and end-user.

Automatic system performance can be improved and the overall man-machine relationship improved by arranging for systems to be self-monitoring and to carry out their own self-test and diagnosis routines. Provided that the way in which the system displays the results of such test is satisfactory and that the user can understand the implications of the result this can produce an improved system. An extension of this concept is provided by integrated process simulations and models which allow systems to monitor a process and to a degree, the monitoring system itself.

### 2.3.4. A model of man-machine interaction

The complex nature of the power plant, and the various differing ways in which individual designers and operators, etc. think about it may be usefully considered in the form of a model. The model described here is based on a distinction between the plant as viewed and understood by designers, analysts, operators and managers. These views are also considered distinct from the 'real' plant, that is the plant which could, in ideal circumstances, be absolutely defined by specifications, tests, experience, etc.

The former views can be considered as 'intellectual' plant data sets and the latter as a 'real' plant data set, which not only embodies the as-designed, factual data, but also represents all the various plant idiosyncrasies of plant construction, layout, etc. The intellectual data sets will also be controlled by errors and omissions which have been built in or acquired.

Within the intellectual data sets we can distinguish various data sub-sets such as the design sub-set, the analysed sub-set, the safety qualified sub-set, etc. In all these cases we define a data set as a depiction of the plant as a number of state descriptors, each having a set of values for a number of variables, e.g. pressure, temperature, flow, etc., along with acceptable values for transitions between defined system states. Furthermore, in operation, there may be constraints put upon operators, e.g. because of material limitations or other reasons, and these may affect the variable constraints and/or the transition limits. An example of this might be the differing requirements of primary circuits during normal operation and warm-up and cool-down to accommodate thermal stresses.

These various data sets are illustrated in Figure 2.1. Operating staff will view the plant as operating in their own personal 'intellectual' data set. At a micro level, these views will be unique to each operator and differences between intellectual sets may exist. In practice, through training, these differences will be minimised but there are implications for conceptual error to be considered here. Clearly, the plant must not be allowed to operate outside known and understood safety limits. Neither can it be allowed to operate outside the certified regulatory limits. The designer must therefore consider the implications of this model, with the possibility of differing information sets and make design decisions which minimise the impact of such differences and allow safety and effective plant operation to be demonstrated.

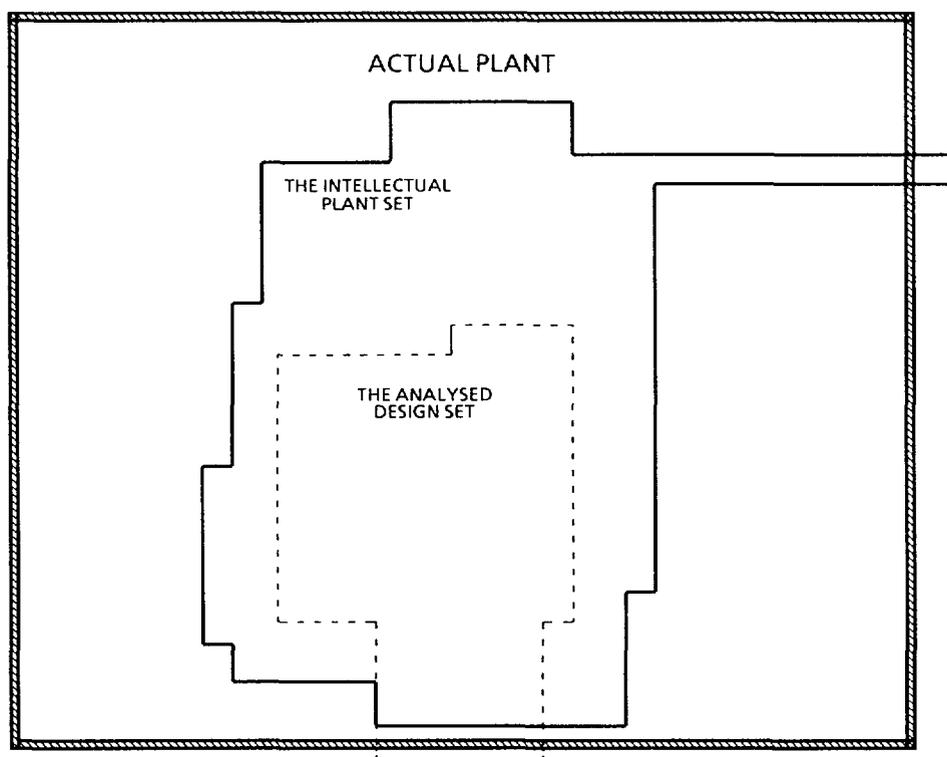


FIG. 2.1. Interacting plant 'data sets'.

The conceptual framework forms part of a wider set of considerations. Figure 2.2 illustrates the relationship between the framework and the actual plant, the operator, design models, operating procedures, and the broader influencing factors in which design takes place. These factors encompass all the features of the open system within which the facility exists or will exist. These include, but not limited to, political circumstances, regulatory considerations, local economic conditions, international factors, labour requirements, etc. Many of these factors are considered in more detail in Section 3.1.5.

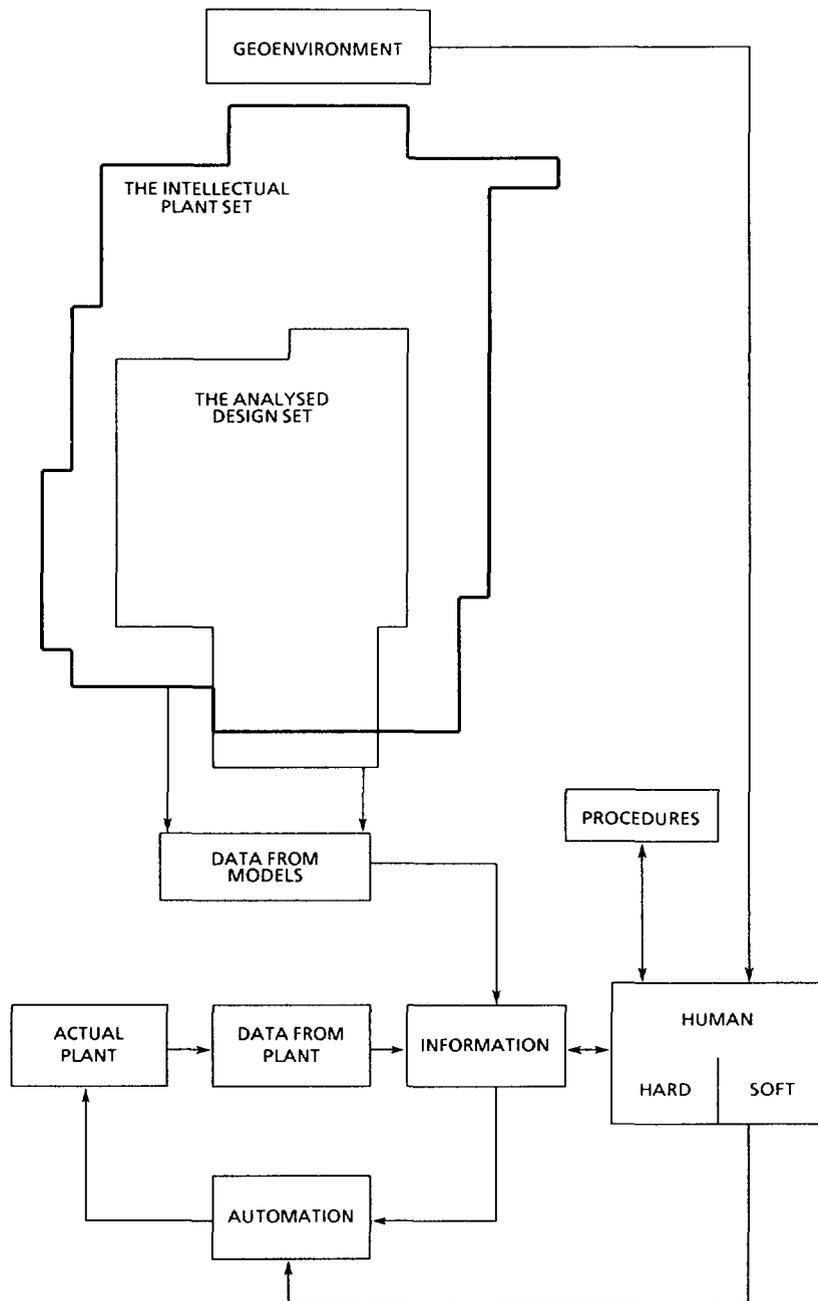


FIG. 2.2. The design environmental model.

### 2.3.5. 'Hard' manual control, 'soft' manual control and automation

In order to properly discuss optimising the balance of functions between man and machine it is important to establish a concept which links the man, the man-machine interface and the tasks which must be performed. Such a framework, illustrated in Figure 2.2, is helpful in establishing the detailed processes which need to be carried out.

Management and control of a nuclear power plant entails the acquisition, assembly and processing by the operating staff of data and information about the current state of the plant and process. The staff also need information about the currently desired state of the plant, any differences between the current and desired states, trends, and a knowledge of how and when to make corrections. The desired state is determined by a set of goals and constraints that originate from several sources, including utility management, plant management, engineering designers, operating staff and, last but not least, regulatory bodies. In recent years, the extent and complexity of such sets of goals have expanded, no doubt to reflect the increased complexity of nuclear plant and associated systems [7].

Consider, first, the total management and control of the domain of new plant design. Initially, all of the functions to be carried out in the new plant will have been determined or 'invented' by the design team, ideally, incorporating an operational input, all working in a creative role. As more is determined and realised about the new process, or by drawing on past experience, it will be decided that out of a possible set of responses or control options for a given plant condition, there is at least one, clear way to proceed. In such a case, a clearly defined operating procedure can be prepared, that predetermines the required operator actions for that set of circumstances.

In practice, a procedure may need to contain various branches, the following of which may depend upon the detailed circumstances prevailing at the time of use. These may include choices which depend upon factors such as resource distribution or the rate at which events are occurring. When discretionary action is required from the operations staff, they can act creatively. If, however, such action is restricted by the set goals and constraints, the potentially creative role of the operator is diminished and his role becomes reduced to ensuring that the set procedure is accurately applied. Operators following set procedures is commonly referred to as 'manual' control, but it can be thought of as a form of automation using the man as a type of pre-scripted component. This can be termed 'hard manual'. For activities that include performance of knowledge-based tasks, such as planning, diagnosing, devising new strategies, etc., we can introduce the term 'soft manual'. This concept is illustrated in Figure 2.3.

A further complexity arises when the plant operates under abnormal conditions. Here set goals and constraints may not exist unless a thorough analysis of plant behaviour under all combinations of fault has been carried out. The designer may seek procedural behaviour from the operator under such circumstances whereas in practice the operator may have to extemporise at just the most inappropriate time, for example, two coincident faults. Where an 'umbrella' approach to safety is adopted for a plant, and safety goals and functions are defined, these problems can be avoided and it will be possible to derive operator tasks and procedures successfully.

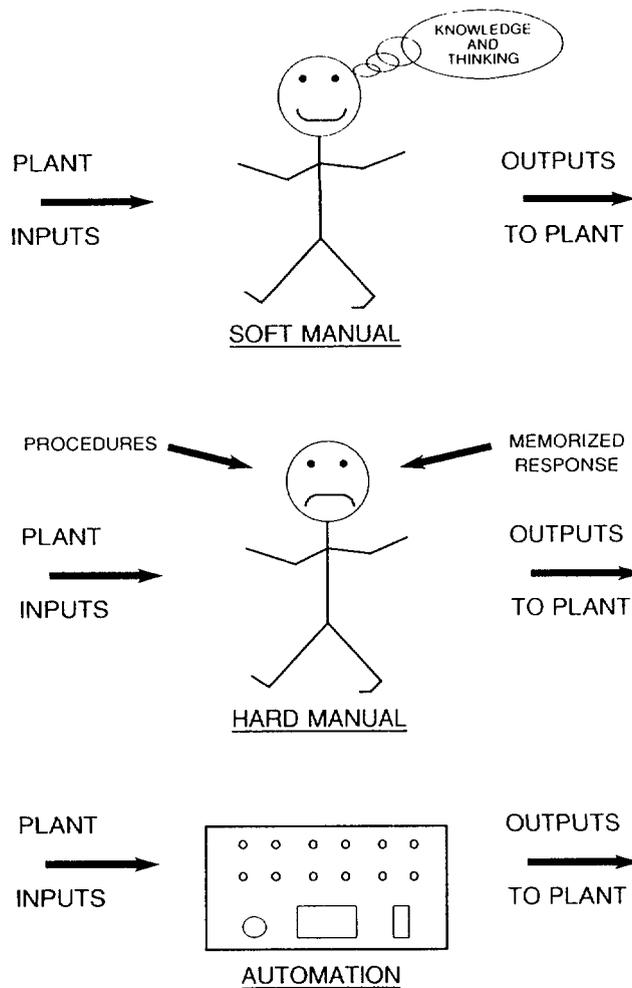


FIG. 2.3. 'Soft' and 'hard' manual control.

It is important to remember that all aspects of control, including in that term the wider aspects of monitoring and surveillance, are derived from the human mind. The designer of a plant or process has the authority to exercise control through automation. Often this is incorrectly stated as the machine having authority. The authority to exercise on-line judgement is clearly the prerogative of plant operations staff. However, amidst these two poles, lies a middle ground occupied by 'soft manual', which involves a sharing of authority amongst designers, experienced operations staff and other experts. Those involved must blend the design and operating knowledge and experience into the bases for automated system design and operating procedures. The methodology proposed in this document provides a mechanism to identify 'hard manual' functions and, where appropriate, assign these to automation.

### 3. ACHIEVING A BALANCE BETWEEN AUTOMATION AND HUMAN ACTIONS

#### 3.1. GENERAL DISCUSSION

Achieving a balance between automation and human actions requires functions which the man-machine system must carry out to be assigned to either machines, human operatives or, more commonly, a combination of man and machine. The process is usually known in the ergonomics literature as 'allocation of functions' but for consistency with IEC Standard 964 [2] this document uses the term 'assignment'. Prior to assignment, the designer considers 'functions'. Once assigned, these can be translated into 'tasks' which are carried out by the requisite part of the system. The assignment process requires four things:

- A detailed knowledge of the individual functions and operations to be carried out for the safe and effective running of the system.
- A knowledge of the capabilities and limitations of the human operator population which is to be employed for operation and maintenance of the system.
- An understanding of the capabilities and limitations of the available technology for design, manufacturing, and implementation of the system.
- Criteria by which to determine how functions should be assigned between man and automation.

In practice, assignment of functions cannot be a simple and mechanistic process. Firstly, the information required to make the decisions may be incomplete or uncertain, particularly in the early stages of the project. Secondly, the criteria against which to make assignment decisions may not be absolute or may apply only conditionally. Thirdly, any individual assignment decision may interact with a previous one, necessitating re-examination and iteration of that decision leading to a revised decision. Thus the assignment of functions process is of necessity an iterative one and must be thought of as a balancing of the several factors which are involved rather than the meeting of a set of fixed design rules.

To ensure true complementary operation between the two components: man and automation, the designer must ensure that man's capabilities are properly employed; being neither exceeded or under-used. For instance, the size and complexity of many existing control rooms can lead to human capability limits being exceeded, in areas such as alarm presentation at high rates under abnormal plant conditions. Conversely, the provision of large amounts of computer control can reduce the role of a skilled operator to one of a disinterested machine minder. The project team who design the system must therefore exercise caution and provide additional automation to counter potential overload, and carefully define the operator's job to ensure that he remains in touch with the automatic process.

In many cases, it may be essential to employ automation to achieve the necessary degree of safety or reliability. In the event of such systems failing, manual intervention would not be practicable because the human performance would not be adequate. However, humans are often expected to take over a machine function when automation fails. Complex, expensive engineering solutions are often necessary to provide the required system reliability and availability. Designers and users of complex systems must

recognise that the use of automation may change the role of the operator in a system and may, for instance, result in him becoming decoupled from the workings of the process he is supervising. The operator may become de-skilled and therefore be unable to take over when the automation fails.

#### **3.1.1. Function analysis**

A key component of the assignment process is the analysis of the various functions which are required to be carried out. The Control Room Design Standard IEC 964 requires such a functional analysis to be carried out. Several techniques are available for this, with the exact choice of technique depending upon the nature of the tasks under analysis, the available skills and resources for analysis and the extent of available plant and operating knowledge (see Appendix A). Where functions have not previously been defined, it may be necessary to carry out some synthesis based on observations of existing functions and other design information.

The function analysis should be broad enough to encompass all areas of plant operation and maintenance and should be carried out with sufficient depth necessary to allow particular automatic features and operator job specifications to be produced. Above all, the analysis must adequately cover operations of the plant under abnormal conditions. The analysis must produce a hierarchy in which the top level functions represent the most general or fundamental objectives of the plant operating staff - i.e. safe, effective generation of electrical power, protection of the public from radiological hazards, etc.

The lowest level set of functions are the sub-functions which must be assigned to man or machine using a methodology such as that described in this document. Application of the methodology described will result in lists of automated functions and functions to be performed by the human operators, which will form the basis for defining operator tasks. It is important that the methodology used and the results obtained be fully documented. This is to enable decisions to be re-examined where necessary and to permit them to be audited when required.

#### **3.1.2. Basic principles**

The actual assignment of functions between man and machine must follow a systematic procedure. This document proposes such a procedure from which a number of underlying ergonomics principles can be derived. These may be stated as follows:

- (a) Human cognitive strengths should be fully exploited by the designer. There are some things that man does better than machines. The three disciplines of engineering, ergonomics and psychology must work in harmony to exploit these strengths.
- (b) Automation should be used to protect society from the fallibility and variability of humans. This requires a detailed analysis of the tasks which are proposed for man, the possible errors and the possible consequences. Areas of risk should be automated if this is practical, feasible and cost-effective.
- (c) Automation should start with the most prescriptive procedural functions first. Those manual functions that are memorised or performed prescriptively by detailed procedures should be automated whenever possible.

- (d) Automation should be used to reduce human cognitive overload. Humans can suffer from information overload and consequent mental overload. This can occur from high information rates, competing tasks or task complexity. Wherever the designer can predict this problem, or whenever operating experience demonstrates it to be so, automation should be used to relieve the human of that part of the function which causes the problem.
- (e) If possible, tasks which have been assigned to automation should not be returned to the man when the automation fails. In general, humans do not act effectively as a back-up to a machine. In most cases, the reason for using a machine is that a human capacity has been exceeded. Consequently, human back-up is unlikely to be appropriate. Machine performance is more consistent if not more available so humans make a poor substitute. Also, human capabilities grow stale with misuse. When a machine fails, to dump a load of tasks onto an unsuspecting operator is a prime example of poor design.
- (f) The correct process for balancing human and machine actions should become an institutionalised part of system design. The right balance will not emerge until there are processes in place and in common use by designers, operators and management, which reflect the correct principles and embody proven practices.
- (g) The evaluation should include consideration of the professional motivation and psychological well-being of the operator.

### 3.1.3. Systematic design

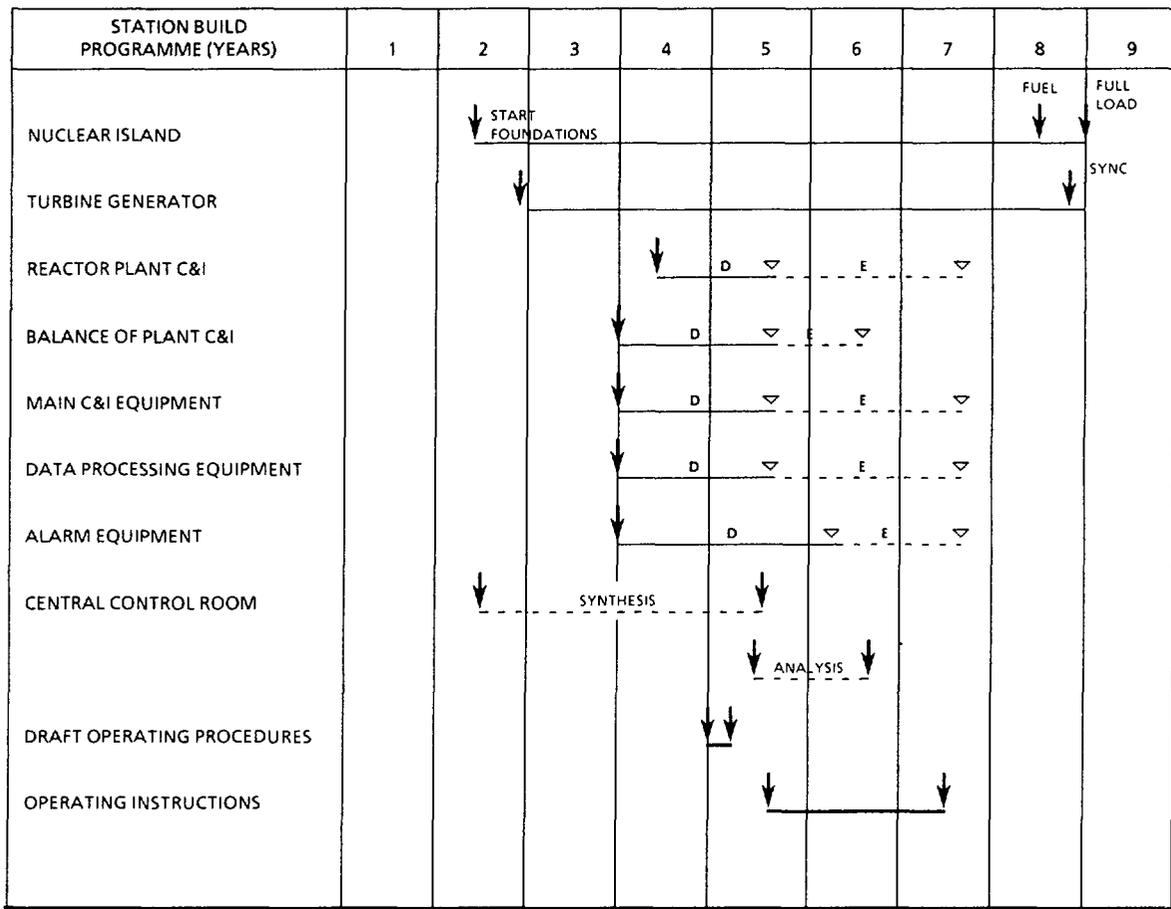
Where assignment criteria are unclear or absent there will always be a tendency to base decisions on past practice, heuristics or intuition. A well-planned and systematic approach with a sound document is essential for the process of justification of a design. The assignment of safety-related functions must be fully justified by an appropriate method [8].

In an ideal situation, the assignment process would consider all possible tasks in an exhaustive manner. In practice this is not possible due to the amount of effort which would be involved, the length of time it would take to carry out and the disproportionate use of resources which would be needed. In a practical situation such as design and construction for a nuclear plant as shown in Figure 3.1, the assignment of functions process must be carried out over the same time period as that for the main and auxiliary plant design.

Taking the above into account, there will be a need to establish a good practice guide to limit the extent and depth of the analysis for the assignment process. These limits must ensure that the analysis is adequate to meet safety and operational needs and that it provides the necessary basis for justification of the design. It is recommended therefore that the analysis be broad in nature, i.e. it should address all areas of the plant for its potential impact and consider all operational conditions, particularly abnormal situations. Where deciding on the required depth of analysis in any one area, the required guideline is that the analysis must be carried to a sufficient depth to allow all automatic features to be fully specified and to allow all operating staff tasks to be defined.

### 3.1.4. Design team

This document makes extensive use of the term 'design team'. In this context the term refers to a multi-disciplinary group which is responsible



D DESIGN PHASE  
E ENGINEERING PHASE

FIG. 3.1. Typical programme of NPP design activities.

for the planning, design, assessment, validation and implementation of the design of the plant, systems and the man-machine interface.

A general problem in the design of control rooms and man-machine interfaces appears to have been that design teams consisted principally of individuals with control and instrumentation experience and with academic training in engineering or a similar technical discipline. Too narrow a perspective does not adequately represent the characteristics of the human operator or the requirements of the operating environment.

An essential requirement for achieving the right balances between manual and automatic is the proper selection of the members of the design team which is responsible for the conceptual and the detailed design of the plant's automation systems and man-machine interface. This holds true for the design of new plants as well as for large retrofits.

A major proportion of the team should include individuals with Engineering backgrounds combined with extensive plant design experience. It is important that this part of the team consists of individuals with sufficient design experience in the mechanical and electrical equipment and process disciplines, etc. to complement the traditional control and instrumentation staff.

The design team should also incorporate human factors professionals together with staff with technical backgrounds who have extensive experience of shift operation in plant control rooms. At least one of the human factors specialists should have an academic background in the cognitive aspects of the discipline and some experience in industrial applications.

### 3.1.5. Influencing factors

Whatever the nature of the system being considered for automation, there will be a number of global factors which influence the general approach and the outcome of certain key decisions. These may typically include: regulatory factors, environment, costs, and many others (see Figure 3.2).

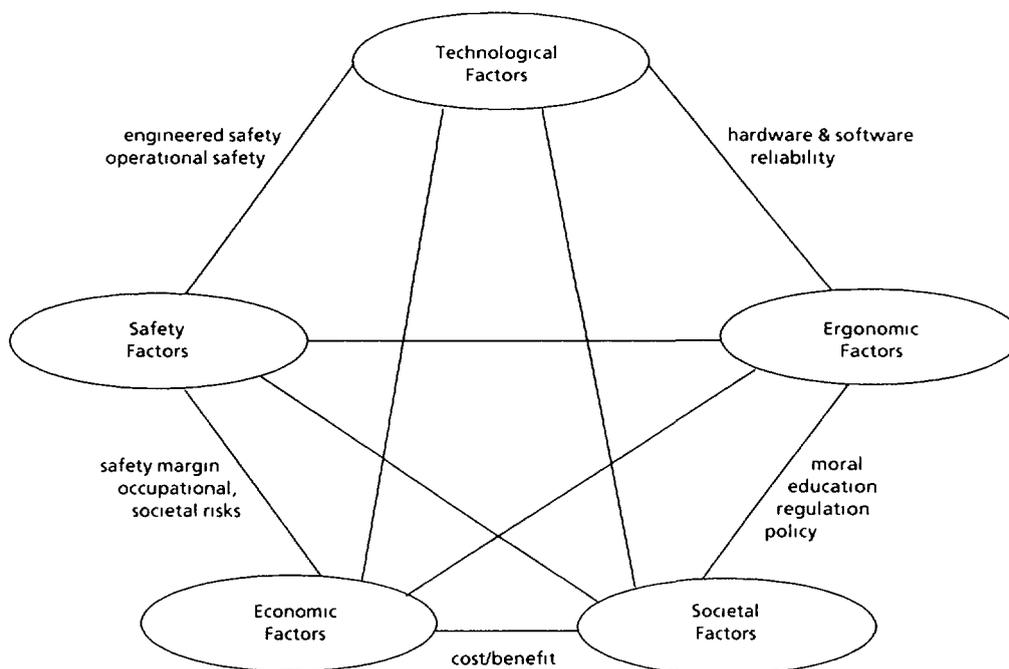


FIG. 3.2. Factors affecting the balance.

The following qualitative factors will modify the relative weighting used in assigning functions. For the purposes of this document these have been termed 'influencing factors', in that they will shape the assignment decision-making process by determining the relative weighting given to choices of where and how much to automate a given part of a system. The factors, of necessity in a document, are presented in an order. This order has been chosen to reflect a generally-accepted set of priorities in decision-making which is deemed to be appropriate to the subject under discussion. The user must, however, decide for himself whether the implied order given here is appropriate to his particular circumstances. Figure 3.3 shows where these influencing factors influence the assignment process described in this document. Note that the term 'safety' does not appear in the list as such. Safety considerations will pervade technical, regulatory and policy factors and it is central to the aims of this document.

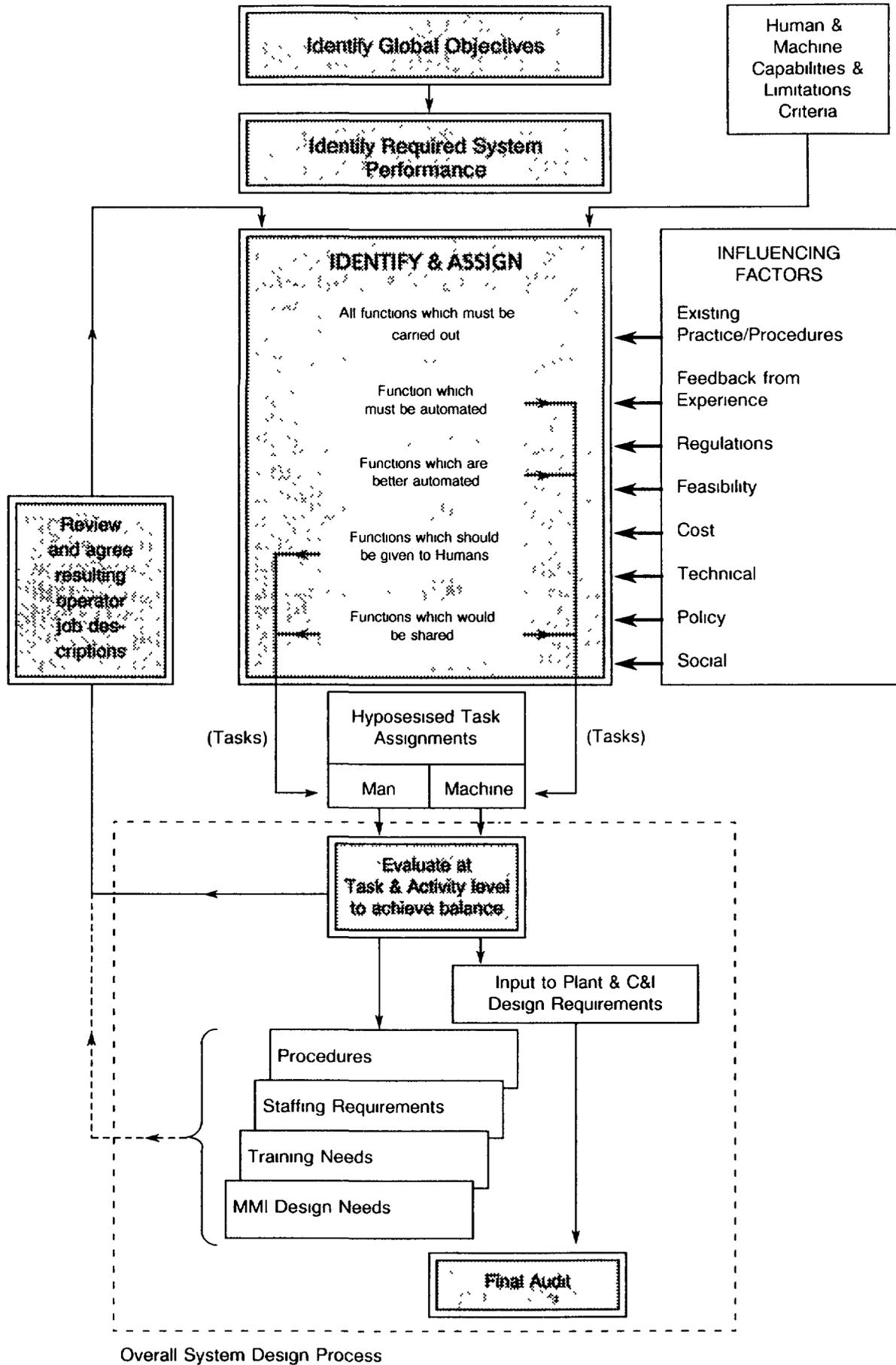


FIG. 3.3. Assignment method.

(a) Existing practices and procedures

Decisions regarding levels of automation and the tasks which operating staff are required to perform must be consistent with the general operating policy of the utility concerned. There may also be existing National practices which influence this. Factors which need to be considered include: numbers of operators in team or crew, age and quality of staff available, present levels of training and qualifications, existing management hierarchies, etc. It will also be necessary to consider existing plant management practices and procedures together with related information support systems. The availability of adequate training simulators may be a key factor in determining the appropriate level of automation to employ in a given case.

(b) Feedback from design and operating experience

A valuable indicator as to the success of a particular approach to automation comes from feedback from existing designs which are in operation. Care must be taken that the feedback is representative. It must come after a period of consistent, post-commissioning operation and there must be sufficient commonality between the source plant and the proposed design. If these cautions are not observed, then general opinions might be swayed by data which is not relevant to the case being considered and hence, inappropriate decisions might be made. A further source of valuable feedback is studies of operator and maintenance errors on operating plants. The existence of such data in the general literature may lead to a number of people holding views on the nature of human error and remedial measures. These general views may be based on loose understandings of involved psychological arguments and a partly informed opinion may not take account of the many specialised details which influence this topic. It is important that specific decisions are based on appropriate plant and personnel data which relate as closely as possible to the actual systems under consideration. To supplement general studies of human error, it is possible to carry out specific examinations of error-likely situations and the potential for human error in defined procedural circumstances. This may involve in-depth, on-site studies by human factors personnel, using techniques such as structured interviews, direct task observations, computer-based task models, etc.

(c) Regulatory factors

A basic starting point for any new design or major modification is to establish the regulatory factors which will control and shape the work. In general, these will be immutable and whilst they may restrict the choices the designer has to choose from, they form a useful fixed basis for design work, from which detailed principles and practices can be derived. In many cases, a utility will possess supporting documentation based on the regulatory framework, which provides supplementary guidance to designers and establishes safety design principles.

(d) Feasibility

The way in which automation is implemented in a nuclear power plant depends upon whether the plant is under development, in construction or in operation. For new plants which are in stages of development or design, the adoption of new technology may be relatively easy and can

be achieved on a larger scale. For a plant under construction, the design may be largely frozen and unless changes to levels of automation are proven to be absolutely necessary the consequent cost and programme factors may out-weigh other motivating reasons for change.

Where a plant is operational, particularly in base-load generating mode, any change to hardware or operational software is only possible during extended outages, except in overriding circumstances. Plant outage schedules have a finite length. This requires that any proposed modification to automation must be fully proven and demonstrated before the implementation window begins. Unless modifications arise from regulatory pressures or legislation, a proposed modification will need to be fully justified in terms of costs and benefits.

There may well be other implications associated with a proposed modification to automation, which go beyond the strict boundaries of automation equipment. For instance, the retrofitting process may involve cutting and modifying pipe-work associated with plant sensors, pulling additional cables, additional data acquisition hardware, additional data management facilities, etc. Thus what may appear to affect only the automation equipment can have significant additional ramifications. Where systems have a safety-related function, there will be additional effort required to justify the details of a proposed change and obtain the necessary authority to proceed. Modifications to equipment in hazardous areas will also need to receive careful attention. The additional degree of effort required in cases where safety is involved may prove prohibitively expensive.

(e) Cost

Decisions on the level of automation to employ cannot be separated from related cost factors. Additional instrumentation and control is often used to redress shortcomings in mechanical and electrical system design and this can be costly. Automation may cost more than an equivalent manual solution, since additional technology will be required. In addition, there will be extra design and commissioning effort and in certain cases, validation and qualification may be required. Having installed additional technology, there will be a need to maintain it throughout its life cycle and it may be necessary to allow for upgrading its functionality or for total or partial replacement of the technology within the life of the plant. Although the capital cost of automation is a relatively small part of total plant costs, the total life cycle costs of ownership must be considered and a proper cost/benefit analysis carried out. The designer must make predictions, based on best available information. It may be necessary to consider a number of bounding scenarios, with various combinations of assignment to operators and to automation, in order to establish the least-risk options. If possible, simplicity of automation should be sought. Conversely, there will be a direct cost associated with the use of operating staff to perform tasks. In addition to direct staff costs for the operating team the designer must also consider the need for spare shift cover, stand-by cover, emergency manning, etc., together with training and support resources. These factors will provide a picture of the direct cost comparisons between automatic and manual provisions but the designer should look further into the operational consequences of automation. If plant availability and productivity can be raised or made more

consistent, there may well be significant commercial benefits to be had through automation. If however, planned automation resulted in a reduction in these aspects of a plant there could be significant commercial penalties.

(f) Technical climate

Today, it is recognised that automation is absolutely necessary for safe, effective operation of modern nuclear plant, it enhances and extends the capabilities of human operators. Whilst automation has a number of desirable attributes, for a number of reasons, both technical and social, in the foreseeable future it is inconceivable that it will totally replace human involvement in plant operation or maintenance. Although research is being conducted into this possibility, it is doubtful if this would ever be possible and even more doubtful if the possibility would be acceptable.

This document outlines the various benefits and drawbacks of automation. As with any other technological system, automated systems are deterministic by design and can not therefore be relied upon to respond predictably to conditions which exceed their design bases. Even if the design process and subsequent validation is exhaustive, the design will in practice be incomplete in some details. Therefore the possibility for systems to produce an undesirable or unacceptable response remains small but finite.

Increasing use of computer-aided design techniques to develop designs, produce software and test correct operation of systems shows promise. By ensuring greater consistency in the design process the number of unproven or unacceptable aspects of a system should be able to be reduced. The problem remains to show that a particular design achieves sufficient quality standards, rather than simply demonstrating the 'As Low As Reasonably Achievable' (ALARA) approach.

(g) Policy matters

Within a national framework or a utility structure there may be policies which determine the way in which plant designs are fixed or allowed to evolve. States may wish to develop particular plant designs for strategic reasons, for internal power programmes or for export potential. Plant types may form part of a family of designs which are related by common features and the need to spread resources across more than one project. Similarly, where older plants are in mid-life or nearing the end of their design life, decisions on automation may be heavily influenced by investment policies.

Where a totally new plant is conceived, it is possible to consider a 'revolutionary' approach, i.e. a totally new assignment of functions, differing from established practice. This may be easier to achieve than a similar revolution in plant design or construction. Indeed, where evidence indicates that existing practices fall short of required or desired targets, it may be preferable to advocate a revolutionary approach to automation. Where this is the chosen course, careful note must be taken of any re-training implications which arise.

(h) Cultural and social aspects

The correct application of automation to a process not only enhances the efficiency, productivity and reliability of the human component in

a system but in doing so, it reduces, or at least substantially modifies, the contribution of the human in the system. For example, the reduced role of the operator in a highly automated plant may represent a social problem for him that can lead to demotivation and significantly decreased performance.

Beyond the detailed technical and human engineering considerations discussed in this document, this change of human role can interact with a number of cultural, social, economic and political factors. Public perception of risk associated with a nuclear plant may not fully accord with the designers view based on actuarial data and accepted analytical principles. Public perceptions may limit the extent to which automation is regarded as desirable in a given application.

The above influencing factors can be taken as 'givens' in the assignment process. The various factors which exist may differ between projects and may be affected by whether a new design is being considered or a modification to an existing process through retrofit. In the latter case, the designer must expect more 'givens' and less flexibility, due to existing plant designs, operating practices, the need for replication, etc.

### **3.1.6. Recognizing component strengths and limitations**

It is essential that the analysis to support the process of assigning functions considers off-normal modes of operation including abnormal situations and accidents. It is particularly important in areas where the human operator in the system is directly responsible for some aspect of safety and where his performance in either abnormal conditions or accident management situations is critical to overall system performance. This will require safety, reliability and availability considerations to be taken into account with safety and protection of capital investment as dominant. In many cases, practical considerations or economics may constrain the number of options which are available to the project team.

The optimum solution to develop a viable way of assigning function or alternatives should:

- enable all safety, functional and performance specifications to be met;
- encompass all credible combinations of plant state, events and beyond-design-basis scenarios. (In practice the analysis will be limited to a manageable sub-set by considering the consequences of abnormal events and accidents);
- make best possible use of the relative capabilities of men and automation, to allow each to complement the role of the other;
- define the correct relationship between men and automation, to ensure that the man keeps in control of the system.

### **3.1.7. Task and job content**

In addition to recognising the limitations of the elements in the man-machine systems, it is also important for human operators to achieve a suitable task loading. The term task loading is used to represent the number of tasks and responsibilities which the human will be required to undertake at any one time.

The totality of the tasks which are assigned to a single operator must, when being carried out under the worst possible circumstances, allow him to maintain an adequate level of operator performance. Conversely, it is important that the human should not be 'under-loaded', i.e. given insufficient or inappropriate tasks. In this case, under-loading the operator can result in waste of resources, inattention, boredom, lack of motivation and consequently poor performance. It is therefore important that the function analysis and subsequent assignment of functions bears in mind the whole of each operator's job, rather than individual tasks and responsibilities. The benefits of, for example, operator training by inclusion of training systems embedded in the man-machine interface should be considered.

A further factor to be considered is the integral nature of the human operator. Whereas machines can be designed on a variable scale of performance and incrementally loaded, human operators are only available as discrete, integral units or groups of units, i.e. the designer cannot reliably design on the basis of half a man or a tenth of a man. In assigning tasks to operators the designer must take account of the resulting, overall job content and how groups of operators will need to work together.

Inappropriate sharing of tasks between operators must be avoided. Tasks may be shared between operators in a group or team but this cannot be done arbitrarily. The role of each person in the system must be considered and appropriately defined. Ideally, the resulting set of roles and tasks would be fully complementary, with a defined degree of overlap and, more importantly, no under-lap. In practice, the designer may have to take account of limitations on the availability of operators and so allow for flexibility in performing tasks. Where team work is called for, communication matters and working structures must also be considered.

### 3.2. ASSIGNING FUNCTIONS

#### 3.2.1. General discussion

This Section outlines a methodology for assigning functions to man and machines and this is illustrated diagrammatically in Figure 3.3. The methodology starts from three sources of information: global project objectives, statements of required system performance, and data on human and machine capabilities and limitations. Although stated this way for brevity, in a practical situation, these three sets will represent a considerable amount of information. Detailed data on required system performance and human and machine performance may not be available at the outset. It will therefore be necessary to employ an iterative approach, taking what is available first and then identifying what is missing. The need for certain source information may become apparent only after initial assignments have been made.

The main part of the assignment process consists of identifying four types of functions which are described in Section 3.2.4. This will produce a list of functions suitable for automation and those which are better suited to humans. At this stage, the lists can only be hypothetical since the design team may not have worked with complete information and may not have considered all interactions and all limiting factors.

An iterative process must now be carried out which re-examines each of the initial assignments in the context of all others and identifies any inconsistencies. Where an assignment produces conflict with accepted human

factors principles, the assignment must be reconsidered and revised. When these two categories of mis-match have been resolved it is then possible to proceed to optimise the assignment in order to achieve the best possible set of working tasks and machine specifications.

### 3.2.2. Required system performance

There is frequently a need to detail system level requirements that can be used as a basis for making decisions on the assignment of tasks and on the design of the user-system interface. Human performance requirements will not be established until tasks have been assigned either to humans or to machines. The performance of the total complex of men and equipment, working together to achieve task goals, can be assessed at a later stage by seeing how well established requirements are being met. It is essential to know, therefore, what overall system performance is required, both as an average and as a minimum acceptable level, and under both normal and adverse conditions.

The performance of software and hardware components can be described and measured by known techniques, using known measures such as speed, size, accuracy, reliability, or repeatability. Some aspects of human performance can also be measured by known techniques, using measures such as speed, accuracy, processing time, production rate, error rate, training time to criterion level, or level of job satisfaction. Simple comparisons between humans and equipment in performing a task have to be seen in the context of the associated tasks that are being performed and the total efficiency in job performance. There can be trade-offs that influence the assignment process.

System performance levels will be influenced by the ways that the humans and the hardware/software components of the system interact dynamically. Information functions should be described systematically, with human-machine interactions mapped in accordance with human factors models. This will cater to information needs, capacities, feedback loops, and cognitive loading levels.

#### 3.2.2.1. The role of probabilistic risk assessment

Probabilistic Risk Assessment (PRA) is increasingly used to assess systems. The use of PRA may be a regulatory requirement in some cases. A complete PRA will take account of human actions in system operation and maintenance and will assign quantified values to these. The results of PRA may indicate where the performance requirements of a function exceed the capabilities of humans and therefore where automation is required.

Great care must be taken to use appropriate human performance data in PRA. However, existing data sources are not fully developed. The results of PRA can provide a valuable aid to judgement regarding assignment of functions but they should not be taken as an absolute basis for design decisions for the following reasons:

- source data accuracy
- source data applicability
- the differing nature of human, hardware and software performance data.

It can be argued that data on hardware reliability, on software reliability and human performance data are each sufficiently different in

nature and meaning to preclude their combination in a single equation or calculation under any circumstances. The degree of confidence with which the behaviour of a hardware system can be predicted is often high. This can be supported by testing and analysis. Worldwide experience with a variety of equipment provides assurance that existing hardware design methods are adequate. Software behaviour is the subject of much study and research. Software-based systems are being used increasingly in nuclear power plant applications, including high-reliability duties such as protection functions, but in most cases, diverse, hardware-based equipment is retained in a back-up role. This hybrid approach indicates the difficulties which exist in achieving and quantifying high software reliability. Human performance data are currently presented in quantitative terms and are often used as such in overall system performance calculations. However, the confidence which can be placed on these data as representing actual human performance under real conditions cannot be as high as that for hardware or software. In practice, many performance shaping factors exist which can modify predicted human behaviour values and these must be considered for each particular application.

### 3.2.3. Human performance data

#### 3.2.3.1. General data

The design team requires access to relevant sources of human factors data, initially to provide a yardstick for general function assignment decisions, and subsequently for refinement of those decisions to meet system performance requirements. The general human factors literature includes data on the effects on human performance of variations in areas such as:

- general user-system interface design
- information system design and layout
- computer generated information presentation
- control system design and layout
- device labelling
- human cognitive functioning (memory and perception)
- inter-person communications
- human error prevention and recovery
- design of documents and procedures
- workplace environment variables
- design and use of protective clothing and equipment
- work design and organization
- work crew organization and functioning
- work shift scheduling.

Much of the data presented in the literature have been specified at a general level of applicability. That is, data on human capabilities and limitations are population findings that may be modified for specific applications where situational variations move the data distribution in predictable ways.

#### 3.2.3.2. Operational experience data

An important indicator of system reliability can be obtained from performance data collected from operating plants. In particular, data on human performance (which is a key part of many operations) can indicate where improvements in plant, automation or methods may be beneficial. These data can also be used as guidelines for the development of additional technology which can be used to improve human performance and productivity.

In recent years, various countries who operate nuclear installations have been concerned to compile banks of data on human performance, from significant event reports, operating experience and specific surveys. Countries which are known to have interests in this area include: the United States of America, France, Germany, Canada, the former USSR, Japan, Finland, Sweden and the United Kingdom. Data sources include internal reports for operating plants, historical records from within the countries, but some arrangements exist for information exchange between countries.

At present, there is no apparent universal standard for data acquisition schemes or data classification. This complicates data exchange and inter comparisons. Since data availability is limited it would seem of merit for such standards to be agreed to enable data to be pooled for common analysis, if maximum use is to be made of available sources of data. IAEA-TECDOC-538, Human Error Classification and Data Collection [9], presents an up to date view of available techniques, problems and potential areas for improvement.

#### 3.2.3.3. Data analysis

Considering data obtained from operational event reports, it can be seen that about half of the events considered were attributable to human performance problems in some way. A similar proportion of the events are commonly traceable to deficiencies in design and manufacturing. There is the underlying fact that design and manufacturing deficiencies, to the extent they stem from human activities, are also attributable to human performance problems. The data indicate that a significant proportion of human errors could have been avoided if designers, trainers and operations managers had paid more attention to recognising human limitations. Information from studies in various countries indicates a similar picture, in that whilst the exact proportions of errors differ, as do the classification schemes, the clear message is that human performance plays a large part in determining overall system performance. At present, the nature of the human error data which is obtained is insufficiently specific to enable firm conclusions about human performance to be drawn and improvements in data collection, analysis and exchange are warranted.

Some results which have emerged from individual human error studies are:

- Activities which provoke a relatively high frequency of performance problems may be manual operations or acts on plant, corrective and preventative maintenance, testing and surveillance in operations and maintenance, equipment operation and safety tagging.

- In terms of locations where human performance problems occur, the highest frequencies occur in the main control room. This is followed by the auxiliary building and the reactor containment area of the Nuclear Steam Supply System. The turbine house and switch-gear rooms in the balance of plant area follow.
- Analysis of major causal factors show reasons why events have occurred. These factors, also include procedures, work-place design (interface and environment), communications, training, managerial methods, work organization, change control and work scheduling.
- Analysis of types of inappropriate action types associated with information acquisition and mental processing, shows that errors of omission can be most frequent. These are followed by errors of transposition, quantitative errors, mis-communication, involuntary acts, untimely acts and out-of-sequence acts.

Whilst data such as these described can provide valuable insights into the understanding of human performance in nuclear plant operations and maintenance, the designer must be cautious about drawing direct conclusions from it. Several factors can affect the validity of the data, including nature of personnel involved, situation-specific considerations, etc. Also, the methods used to collect and analyse the data may affect the results. In such studies, the human is only one element of the overall system and his performance is interactively bounded by the plant and interface machinery. Factors such as the state of the machine, its maintenance history and design and construction factors all serve to complicate the picture and make direct use of data in unrelated application difficult. It is therefore important that the designer employs data which is relevant to the plant and personnel under consideration. As human error reporting schemes become more developed, it becomes increasingly possible to attribute so-called human errors to 'root causes', i.e. the true cause such as poor interface design, poor procedures, inadequate training, etc.

Corrective actions to improve error-likely situations can be many and can involve changes to either man-oriented systems, machine-oriented systems or a combination of both. On the human side, corrective actions may include supervisory re-instruction or cancelling, procedure correction or revision, improvements in administration and documentation, retraining or modifications to training, etc. On the machine side, options may include improvements to equipment design, upgrades in equipment reliability, changes in information displays or sensors, enhanced labelling and demarcation, etc. These may be to enhance the fault-tolerance, or to increase the functionality of machines using automation technology to relieve unacceptable burdens on human operators.

#### 3.2.4. Function classification

Having identified the various functions which must be performed the designer must proceed to classify them. The process described here employs four categories for this classification:

functions which must be automated

functions which are better automated

functions which should be done by humans

functions which should be shared.

The classification is based purely on the nature of the functions being considered and it makes no presumptions about their role. Note that only one of the above categories is absolute in nature, requiring a clear, definitive result. The other three categories are based on qualitative judgements. Thus for instance, the choice of classifying safety-related functions should be based on a detailed consideration of the function and relevant performance shaping factors.

#### 3.2.4.1. Functions which must be automated

This category contains all the functions which, by virtue of their nature and their performance requirements, can only be achieved using automation. As a general statement, these can be defined as those which exceed the capabilities of humans to perform them. In determining whether a function falls into this category the design team must consider the long-term demands of the resulting task, required performance under the worst possible conditions and the variability of human operator. Performance factors which will need to be addressed include; required task rate, accuracy, repeatability, and in particular, the consequences of error.

The first consideration must be to examine any functions for which automation is mandatory. It is desirable that any such assignment of functions are based justifiably on human factors principles but this may not always be so where mandatory requirements are based on established custom and practice. The designer should understand the fundamental reason behind any such mandatory requirements to ensure they are appropriately and responsibly applied.

Functions which should not be assigned to humans include:

- rapid or long-term processing of large quantities of data
- tasks requiring high accuracy information (data processing or manipulation)
- those requiring high repeatability
- those requiring rapid performance
- those where the consequences of error are severe
- those where errors cannot readily be retrieved (corrected)
- those which must be carried out in an unacceptably hostile environment.

Typical applications in a nuclear power plant for which automation will be justified include: reactor and plant protection systems, closed-loop automatic control, information processing, extended sequence control, data recording, analysis and archive. Depending on the particular task performance requirements, in all such cases it will be easy to demonstrate that one or more human capabilities would be exceeded if the task was performed manually. A consequence of the decision to automate a task is that it will have to be described in sufficient detail to enable the necessary machine function to be defined. This will usually require extensive detail to be identified. A common failing of automatic system design is the lack of sufficient design detail, particularly to cover abnormal events accidents conditions. Such detail may be supplied informally by the system implementer without due consideration of the effects on system behaviour. In the absence of such detail in the design

of automatic systems it is sometimes necessary for humans to take over when the automation fails, a task for which they may be ill-prepared and ill-equipped.

When deciding to automate a function, consideration must be given to supplementary tasks, such as maintenance and testing, which are required to allow the automation to perform its role. It is important that the benefits of automating a function are not lost by assigning supporting functions to human actions where the performance of the automatic system would be degraded due to poor maintainability. A typical example of this would be the maintenance and testing of reactor protection equipment. Until recently, this function was often assigned to operating staff with a consequent risk of errors which could degrade the system and cause reactor scrams. Developments in the design of computer-based systems have now made it possible to apply automatic testing to such systems, providing a higher degree of system availability and performance.

#### 3.2.4.2. Functions which are better automated

In an analysis of functions certain tasks may be identified which, although lying within the capability of humans to perform, may be better assigned to machines. These include tasks which are lengthy, require high consistency, high accuracy or which involve a degree of risk to an operator. Tasks which would result in boredom or monotony for an operator also fall into this category. To an extent, the classification of tasks into this category is a function of several factors. Among these it is possible to identify two key influences. Progressive increases in the capability of technology means that more and more functions can be automated. The cost of such technological solutions is often seen to be falling in relative terms and automation becomes an increasing possibility. Secondly, the point at which automation is regarded by users as necessary or a normal expectation changes as societal and work-place values change. This trend is not necessarily a reflection of any inadequacies in human performance but it is often based upon economic considerations.

Practical examples of automation being introduced to replace tedious or arduous human activities include the use of machines to carry out maintenance or surveillance activities, e.g. steam generator examination, tube leak plugging, bolt tightening, etc. Automation is also increasingly being used to carry out lengthy, repetitive testing, such as that for safety and protection systems. Not only does this improve the task role of the operator but it also brings improvements in the consistency of testing and may allow it to be carried out more frequently. As with any function which is intended to be assigned to automation, a firm, detailed task specification will be required.

A further reason for using automation is the potential improvement which it can bring to the design of jobs and working conditions by changing the role humans play in technology based systems. With careful job design significant improvements in operator roles can be achieved and there may be consequential improvements in overall system performance. If care is not exercised, or if basic human factors principles are not adhered to, adverse problems can be created.

#### 3.2.4.3. Functions which should be assigned to humans

Functions which require heuristic or inferential knowledge, flexibility, etc. will need to be assigned to humans. In addition, there

may be practical or technical constraints which make automation of the task impractical and thus require human operation. In many cases, it will be possible to justify assignment of such tasks to the human. However, there is a risk that tasks will be so assigned simply because automation would prove difficult or non-economic in some way. Regrettably, in practice, a function may be assigned to a human simply because there is a lack of a precise specification. It may prove possible to produce a workable system in this way but there is a risk that the result will be unsuitable or inappropriate.

A particular set of functions which must inevitably be left with the human are those which occur in extreme abnormal or accident situations, where human flexibility and high-level skills are essential and the unexpected nature of the task makes specifying automation difficult or impossible. In these areas, automatic processing of information, including the use of knowledge-based systems, offers great potential.

#### 3.2.4.4. Functions which should be shared between men and machines

Many functions in nuclear power plants are carried out by a combination of human action and automation. A common example of this is the use of automation to detect and announce plant conditions, in the form of an operator information system. The human operator uses this information to make judgements, take decisions and execute control actions.

Increasingly, computer-based systems can be used to support operators in the performance of their tasks. There are many benefits which can accrue from the use of technology in this way but it is important to ensure that the design of the support system and of the tasks which are assigned to the operator place him in the correct role in relation to the machine; that is in an intellectually superior position, with the machine serving the operator. Technological advances such as those in artificial intelligence and expert systems suggest that automation of many functions which was hitherto impractical is now a possibility. It is true that automation can be used to an increasing extent in the support of human tasks and to an extent, replace certain aspects of human involvement. However, considerations of system integrity, software validation and verification, consequences of error, etc. place limits on the extent to which safety-critical functions can be placed in the control of computer-based systems. The designer may not be able to use software-intensive solutions for such functions.

#### 3.2.5. Hypothesized task assignments

The results of the function assignment process will be two sets of information which are fed into the overall design process. Firstly, there will be lists of tasks which have been assigned wholly to a single operator or to a group of operators, but because the process described allows functions to be shared between humans and machines, the list will also need to contain shared tasks which relate to these. The list will be used subsequently as an input to statements of MMI and staff requirements, training requirements, operating procedures, rules and supporting job-aids. The second output from the assignment process will be a set of statements of the required automation, information systems and man-machine interface design. These will be used in the design of sensors, signals, etc. and in the detailed design of the man-machine interface including information displays, automatic control system interfaces, manual control interfaces, etc.

These initial lists will form the basis for subsequent iterations. Iteration is necessary because many task assignment decisions will have an impact on other ones. To resolve such questions, it may be necessary to obtain highly specific and detailed information and this may only become available midway through the plant design phase. The approach taken to function assignment must recognise these problems by providing an ongoing, iterative vehicle for examining design decisions in a structured manner.

Since, in order to automate a function, we need precise specifications and criteria, whilst conversely humans are capable of dealing in a flexible way with loosely specified tasks, there will always be a risk that the assignment process will favour manual execution of difficult tasks, in order to produce earlier results. There may exist countering influences in the form of technological and social trends towards increased automation. The assigner of functions should remain true to the necessary principle of task assignment according to best suited attributes of task and performer.

### **3.2.6. Evaluation of assignments**

Evaluation of the adequacy of function and task assignments prior to plant operation is necessary. Since nuclear power plant design tends to be evolutionary rather than revolutionary, there is much benefit in obtaining feedback from appropriate existing designs and practices. The designer should utilise experienced operating personnel in the assignment process, since they can bring direct operating experience to bear on the matter. However, their experience must relate to a plant of a similar generation, and the designer must ensure the operators fully appreciate what he is seeking to achieve in terms of design objectives and the constraints which apply to the work. Unquestioned repetition of even well-proven approaches can lead to unsatisfactory or even unsafe systems.

Whilst 'desk-top' analysis will be useful in evaluating design proposals, there is a need to consider temporal factors. The time available to an operator to perform a task or series of tasks can influence his performance, possibly in a decisive way. To address this, some form of simulation may be necessary. Simple simulators such as mock-ups are of proven worth and if simple time elements can be incorporated, basic evaluation can be carried out. Part-task simulations may also be of benefit. Maximum benefit will be obtained from the use of full-scope simulations incorporating a credible man-machine interface. For large projects, experience indicates that the full-scope simulators have made significant contribution to man-machine interface evaluations. If these can be made available prior to design-freeze of the real man-machine interface, extensive evaluation is possible and subsequent project risk is significantly reduced. In addition to using plant operators in the design process, a valuable contribution will be made by involving training staff who are a valuable source of knowledge, experience and expertise.

## **3.3. INTERFACING WITH RELATED DESIGN ACTIVITIES**

### **3.3.1. Operator task specifications**

One of the outputs from the methodology described will be statements of tasks to be carried out by operating staff. These will include functions which are shared between men and machines. For practical reasons, to allow operating staff requirements and role to be identified and developed, this information must now be expressed in terms of task descriptions, job descriptions and staff requirements specifications. For practical application to control and monitoring of the plant at the

detailed level, operating staff tasks will usually be expressed in the form of operating procedures, operating rules, technical schedules, etc. Notwithstanding this, a definition of the role of each member of the operating staff should be produced, which clearly defines the operator's role and responsibilities in both the maintenance of safety and in achieving production goals. At this stage, a check should be made that there is no conflict between the various safety and production goals which have been defined and that the goal definitions which exist are complete and consistent. Where any potential conflict is identified this must be fully analysed and task specifications revised accordingly. If it is not possible to eradicate such potential conflicts, the operating staff must be provided with adequate guidance to resolve these during operation of the plant.

Operating staff task specifications will also provide a basis on which to confirm information and control interface needs. Examination of the detailed task statements will also enable information display content and form to be confirmed as well as types of input, selection and control devices. From this information and a consideration of the context in which a task or tasks are performed, it may be possible to identify where additional operator support systems or job aids are required. This information will need to be fed into the design process for the man-machine interface and supporting facilities.

### **3.3.2. Operating procedures**

To be effective, operating procedures and related documentation must be designed in accordance with appropriate standards for content, form and presentational style. The design of operating documentation should be based on functional and implementation specifications in the same way as any other engineered feature of the power plant. It may not be possible or practical to pre-define all actions which are required to cover all operating modes of the plant and all operating eventualities. However, the operating staff should be adequately supported by procedures during all conditions of operation, including normal, abnormal and accident conditions.

The design of procedures should recognise this by providing the necessary coverage and employing suitable approaches such as combinations of event-based, symptom-based or function-based documentation, as appropriate. To provide the necessary basis for such procedures, the lists of operating staff tasks must reflect the various operating conditions discussed and any differing operational and safety requirements which exist between them.

At all times, the operating staff must fully understand which functions are delegated to them and which are being handled by automation. Where it is safe, possible and operationally desirable, the operating staff should be provided with means of controlling this assignment, through appropriate selection and control devices. It must be possible for the operating staff to readily assess the state of such assignments at all times through the process information system. Where the assignment can be varied by automatic actions, which may trip functions to a manual state, the information system must unambiguously draw the operator's attention to such changes.

### **3.3.3. Specifying automation**

Specifications of the tasks to be carried out by machine, the automation component of the system, will form a major input to the design

of plant systems and associated protection, control and instrumentation. They may also influence the design of plant components themselves. It will not be possible to consider automation requirements in isolation from operator tasks, since inevitably there will be some human involvement in automatic systems, albeit in the form of supervision, surveillance or maintenance activities. The two sets of task specifications, those of the operating staff and those assigned to automation, must be considered together, and appropriate account taken of the many interactions that there will be between them.

#### 3.3.4. Implications of the assignment process

Use of a well-balanced assignment process will optimise the contribution of both men and machines to overall system performance. In practice, a truly optimum balance may be difficult to achieve, due to lack of precise information or uncertainties and assumptions which have had to be made. If it is necessary to make compromises during the assignment process, as it undoubtedly is in many practical situations, the designer must, above all, ensure that safety objectives are met at all times and under all conditions of operation.

Often, it will be found that a number of possible assignment patterns will prove equally adequate to meet the specified system needs. In such cases the designer should select a set of assignments which best accord with proven experience and practice. Whatever solution is adopted, the designer should ensure that the basis for that choice is documented and understood by all who will use that information in the course of their subsequent work.

The overall objective of the assignment process is to obtain a satisfactory balance between automation and human actions, not a perfect one. Experience in member states shows that a balance can be obtained with a range of solutions. Very rarely will a single, unique result be indicated, particularly when maintenance activities are also taken into account. Neither will a common approach be justified across the whole of the plant activities being considered. This is particularly so when considering safety-related questions, where overall system reliability and performance will constrain many of the available possibilities.

If task assignments are inadequate this may be revealed during testing or operation of the plant through reduced output, increased downtime, increased human error and may lead to a higher than desired risk to safety. Whatever the parameter, in such cases there will be incentives to achieve an improved balance and as a result, more effective plant operation.

#### 3.3.5. Final audit

The assignment process is completed by a final audit phase, to be carried out at a suitable time. The purpose of this phase is twofold. Firstly, it serves to validate the many decisions which have been made during the assignment and project development phases and secondly, it provides an opportunity to ensure that documentation of those decisions is adequate to allow subsequent re-examination and possible revision.

The assignment process will provide a documented basis for decisions-making in system design. Notwithstanding the iterations described and the inherent checks and balances which will result, there will be merit in carrying out a final audit of the resulting system. In the case of a modification to an existing plant or process, the audit

should consider both the changed portion and the modified process to ensure completeness of analysis.

The audit process should check the extent to which the original objectives have been met and document any significant departure, anomalies or conflicts which can be identified. Judgement on the adequacy of the final system must rest with the end users , provided that compliance with safety and performance standards can be adequately demonstrated. Final audit can form part of a wider review of facilities and provisions. Again, if the assignment process has been well-documented, audit will be greatly assisted.

#### **3.3.6. Operational feedback**

It is important to regularly examine feedback from operating experience with the system and other related systems to ensure that the original balance remains valid and to identify any need for revisions to the original assignments if operating experience so indicates.

### **4. RESEARCH MATTERS**

This section discusses the general situation with respect to research into assignment of functions, the historical antecedents of the current situation and certain developments in design methodologies. It is not intended to be a comprehensive review of the literature but rather a summary of what is deemed to be germane to the present subject.

#### **4.1. TYPES OF HUMAN FACTORS RESEARCH**

Ergonomics, or as it has also become known, human factors, traces its development as a scientific discipline back some 40 years to 1949. Since then a variety of studies have been carried out into man and his relationship with his working environment. These studies can be classified under a number of broad headings.

##### **4.1.1. Traditional ergonomics studies**

These were historically the first and have been the most numerous studies to deal with 'classical ergonomics', i.e. studies of the physical and mental capabilities of humans in a variety of tasks. They consider environmental factors such as heat, light, noise, together with work capacity, error rates in repetitive situations, use of colour and other codes, etc. Such studies provide much useful data for the design of machines, control rooms, etc. and whilst they are of lesser relevance to the topic of this document, their role must not be understated.

##### **4.1.2. Human behaviour studies**

Studies of human behaviour seek to understand the underlying psychological bases and cognitive mechanism which characterise human activities. Studies include attempts to model human decision-making activities. Whilst there are several well-grounded theories, there is not universal agreement on the subject and it is often difficult to apply the existing knowledge in practical situations for industrial design and audit work.

#### 4.1.3. Field observations

Observation of operators, etc. at work have been carried out using a variety of developed techniques. These have included studies at chemical, petro-chemical and nuclear plants which feature continuous processes. Some of these studies have addressed the impact of automation on human operators.

Utilities such as Electricité de France have developed these studies in nuclear plants during in-plant visits and computerised techniques for data collection and analysis have been used [10]. In Germany, investigations of this type have been performed by TÜV-Rheinland [11]. Further analyses using nuclear plant simulators have been carried out by the United Kingdom, Germany [12], USA and France. Such studies have led to a large quantity of data on human behaviour in nuclear power plant operations, including maintenance. Care is needed in using data obtained from simulators or indeed from real plants. The designer must ensure that the data relates sufficiently well to the problem he is addressing, since it is often not possible to generalise too far with data specific to a given operational situation.

#### 4.1.4. Advanced system studies

A number of research institutes (Electric Power Research Institute, Essex Corp., OECD Halden Reactor Project) have carried out studies of operators interacting with advanced computer-based systems. There are on-going programmes in several areas. Many of these studies are aimed at optimising the relationship between the operator and systems which support him in adverse or difficult and challenging situations. Development and study teams have typically incorporated combinations of skills, such as engineering, computer science, psychology, ergonomics, etc.

#### 4.1.5. Control room evaluations

Several studies have been carried out to evaluate complete control rooms or major modifications to interfaces, e.g. CE mock-up of System 80 Main Control Room, KWU mock-up of KONVOI/PRINS/PRISCA Main Control Room and studies by Electricité de France engineers and ergonomists using a full-scope simulator.

#### 4.1.6. Human error studies

Several workers have studied this topic and have proposed classification schemes to enable human errors to be systematically studied. Developing from this work, several utilities have carried out analyses of operational events in order to consider the root causes of human error and to develop remedial approaches. International organizations such as OECD, IAEA, World Association of Nuclear Operators and national ones such as the Institute for Nuclear Power Operations and KWU have also sponsored studies and classification schemes. Utilities have been able to use the results of such studies to revise decisions on automation, e.g. in France, periodic testing of reactor protection was automated in order to obtain improved error rates during testing. In Germany, large scale introduction of automation (limitation systems) changed the role of the Main Control Room staff from 'operators' to 'observer' and 'long-term accident managers' to a large extent [13].

## 4.2. ALLOCATION OF FUNCTIONS - HISTORY AND STATUS

### 4.2.1. Background

For reasons stated earlier this document uses the term 'assignment' to describe the process by which functions are translated into tasks which can be carried out by automation and humans. The majority of ergonomics research uses the terms 'allocation of functions' to describe the same process. This section therefore retains the latter term where appropriate.

The general principles of allocation of functions have been well established by research which dates back some 40 years. The concepts of systems engineering, components within those systems and the relative performance of the parts and the whole are accepted tenets, which are supported by practical experience in their application to a variety of industrial and other situations. Design methodologies have been proposed, developed and proven which allow non-specialists to apply known principles and hence achieve sound system designs. However, as plant designs have become more complex the required level of sophistication has also risen and system performance targets have had to be raised. A consequence has been that the process of allocating functions must be carried out more systematically to ensure that overall system performance can be achieved reliably.

This search for improved design quality requires a greater understanding of the way in which the components of a man-machine system behave. Knowledge of machine performance has continued to grow, as indeed has machine capability, with a consequent ability for designers to specify and obtain higher levels of performance from that part of a system. Knowledge of human behaviour has not grown at anything like the same rate and of course the rate at which the human component is evolving is infinitesimally small.

### 4.2.2. Types of task

Research into what has commonly become known as allocation of functions, i.e. the assignment of individual tasks and groups of tasks to either man, machine or a combination of both, in complex industrial systems can be traced to the work of Paul Fitts in 1951. His fundamental axiom was to render unto humans those tasks at which they excel and to give to machines those functions which are best done by them. For example, rapid and reliable processing of mathematical data is best achieved using a computing machine of some sort. Similarly, moving large loads with high precision is a task for a machine. Conversely, pattern recognition within a noisy information environment or handling of occasional information overloads are areas where humans can excel over machines. Similarly, tasks which require intuition or inventive solutions cannot be readily assigned to a machine and these must be assigned to man. It must be noted that these examples reflect the prevailing state of technology at the time the theory was propounded. Advances in computer-based devices and in software have modified the previously clear cut boundary which Fitts perceived.

### 4.2.3. Attributes of humans and automation

Fitts' concept was to identify various attributes of both humans and technological systems which reflected their differing abilities and capabilities and to express these in the form of standard lists. These lists were then used to classify tasks as to be performed either by man or machine. Numerous examples of such tables can be found throughout the

ergonomics literature and by way of example one such list is given in Appendix B.

One problem with this approach is that of currency of the data represented. Whilst data about human capabilities remains substantially valid over time, advances in technology result in rapid changes to what can be reasonably expected from the machine. A more telling problem is that of usability of the data. Experience shows that such tabulations are relatively crude in the advice they give and that they may be regarded only as introductory material for the novice worker. Experienced designers will find the general nature of the data and the lack of guidance on how it is affected by practical situations a severe limitation. Edwards and Lees [13] summarise the problem thus: "Clearly, such lists can only provide a very rough guide to the principles of allocation, since they attempt to summarise in a small space both the relevant knowledge about human performance and the current state-of-the-art in hardware and software development. Nonetheless, they do provide, particularly for the newcomer to the field of systems engineering, a frame of reference and some preliminary orientation towards the problem".

#### 4.2.4. Relative strengths of humans and automation

Jordan [14] clarified the basic problem with Fitts' approach by asserting that such comparison tables will commonly favour the machine, particularly if they use quantitative data. Attempts to quantify human behaviour have not been totally satisfactory and although it is possible to measure human performance to an extent, databases of such information are not easily and satisfactorily combined with the more factual and actuarial data obtained from studying machines. This is particularly true in nuclear power plants when human reliability is studied in the context of overall system reliability [15].

Jordan expressed this problem in the following terms: "Man is not a machine, at least not a machine like the machines made by men". The conclusion must be that men and machines both have properties which can contribute to overall system operation. Machines are consistent but inflexible; men are inconsistent but flexible. Many such opposing attribute-pairs can be identified. The challenge to the system designer is to utilise both sets of attributes in an optimum manner in creating his design. Man and machine work best in a complementary manner where the design of their individual roles is in harmony. In many cases this will involve a sharing of tasks between man and machine and the allocation process becomes one of controlled sharing.

Chapanis [16] continues this theme when he argues that the systems engineer, when taking the fundamental decisions about the functions to be performed by the various parts of a system, must throughout keep in mind that the separate parts of the system must cooperate effectively. Decisions about the machine component are based partly on what the machine can and cannot do. The capabilities of machines are well known but vary with time as automation capabilities increase. The present rate at which machine performance improves is increasingly large and is much greater than that which prevailed in the 1960s.

#### 4.2.5. Modelling man-machine interaction

In discussing the assignment of functions, many workers invoke a relatively simple model of the human being in a system. The essential components of such a model are man, the machine and the environment, which

operate to form a closed-loop system. Man and machine relate to each other through the man-machine interface, across which information flows in one or more directions, and the whole takes place in the context of some environment and its related factors. This approach to modelling is of key importance in the understanding of the allocation of functions process, since it exemplifies the concept of man and machine working together, rather than in isolation.

Considering first the working environment, in many cases it is possible to describe with good accuracy the factors which pertain to a given task situation. For an existing work situation, quantification of these factors will usually be possible using well-established physical principles and measuring techniques.

Furthermore, the way in which most of these factors affect human performance is also well understood. A single factor may affect performance but the designer must also consider factors in combination and some data is available to support this. In general, there is good understanding of how the various factors affect sensory and motor performance and to an extent this is also true for what might be called the 'lower level' mental processes, e.g. memory, recall, data handling, etc. What is less well understood however, is the way in which for instance, stress affects nuclear power plant operators, although recent work (e.g. OECD Halden Reactor Project, Norway) has looked at this more closely.

#### 4.2.6. Machine performance

Turning now to machine behaviour, this can be readily decomposed into well understood functions. Since a machine is commonly designed to a performance specification, and with specific objectives in mind, the behaviour of that machine, either under normal or defined abnormal circumstances, will usually be well understood. Whereas early research into process plant and associated machine behaviour concentrated on mechanical and electro-mechanical performance, this has largely given way to studies of the way in which complex information processing machines (computers and computer-based systems) can utilise information, and improved ways of constructing such machines. Key developments in recent years have been to do with so-called machine intelligence in the form of Artificial Intelligence (AI) and Expert Systems. There are also increasing developments in advanced automatic systems such as adaptive controls. Emphasis is now being placed on neural networks and the role they might play in future systems. Such developments are beginning to be considered for use in nuclear power plants in the form of real-time, computer-based operator aids [17].

#### 4.2.7. A simple model of human performance

In the decomposed model, man is regarded as having three basic functions: sensory inputs, mental data processing functions and output (control) actions. Data from the machine is taken in, processed by the operator and used to make decisions. Depending upon the circumstances, these decisions may result in output actions which are communicated to the machine. This is a grossly simplified model but serves to assist the design process by identifying human functions which can be related to performance targets and to performance shaping factors. Much work has been done to understand the way in which humans carry out these elemental functions.

Research into human sensory behaviour (the input functions in the model) is well established and numerous sources of data are available. A similar situation exists with human output capabilities, i.e. the motor and motor-perceptual skills. When we consider the connecting function i.e., that of mental information processing, the picture is somewhat different. It is clear from research studies and from observation of work situations, that human behaviour involves more than simple low level mental processes.

An operator will use memory, comparisons with past experiences, recall of learned rules and training, etc. He will co-ordinate what he perceives with strategies he may have formed for handling similar events but may not always be aware of what he is doing. There is also the question of skilled behaviour developed by practice. There is a considerable body of literature on these topics, with workers such as Reason, Rouse, etc being prominent today. However, whilst there are several current theories to support the way in which humans appear to process information and arrive at decisions, together with associated models of human behaviour, there is little which can be regarded as definitive. Several of the models serve to assist discussion of the problem and to allow further theories to be developed but when attempts are made to correlate theoretical predictions of human behaviour with real-world data, the results are variable. It appears that humans are variable in their behaviour and the way in which they relate to other humans and to the work situation and these factors militate against sound, verifiable human performance modelling.

#### 4.2.8. System design goals

Earlier research took as its goal the optimisation of the human and machine components in a system in order to archive some overall system objectives. These objectives might be to make a product, process some information, control a phenomenon, etc. In most cases, the objectives are specified in terms of the overall performance required. As performance requirements have increased, increased attention has had to be paid to factors which can lead to degradations in the performance of the human component in a system. Situations which challenge the performance of humans can increasingly be seen to relate to the social and socio-environmental aspects of working situations, particularly where increased automation has led to a change in role of the human from one of system component to one of system manager.

Kantowitz and Sorokin [18] support this need for any system design to be based on sound definition of goals. They also point out that assignment of functions determines not only how well the overall man-machine system will operate, but also the quality of the working life for the persons involved with the system. It can be argued that such goals should, inter alia, include the well-being and job-satisfaction of the operator. This view is often seen to be in conflict with the traditional 19th century based concept of humans as an expendable part of a system and its later 20th century derivatives of humans as 'flexible' components of a system, which can be relied on to meet extremes of demands using extremes of behaviour.

#### 4.3. ASSIGNMENT METHODOLOGY STATUS

As shown above, initial attempts to provide an assignment methodology to support the assignment of functions were based upon a simple view of the relative attributes of men and automation. Although later workers showed the limitations of this approach, it has the merit of simplicity and continues therefore to have some utility. An even simpler approach is to

automate everything which can be automated. Although lacking in elegance, this approach is increasingly popular given that the capabilities of machines can be increased for relatively little cost nowadays. A consequence of this approach is that the human being is given the leftovers from the process, rather than having a set of tasks deliberately assigned to him.

Two major problems can arise from either overloading or under loading the human being. In many cases, such problems may remain un revealed during normal operation, but it is common for the results of such a coarse approach to be revealed in an unacceptable manner during abnormal operation or transient management, where operators fail to cope successfully due to performance overload or insufficient skills due to lack of involvement or practice. Again, inappropriate allocation of functions can result in increased stress for the operators, with consequent degradations in performance during operational situations where maximum performance is sought from the human components in the system.

Improved approaches which overcome some of these problems rely on a more sophisticated classification of functions. In many practical situations, there will be constraints on the designer which effectively dictate a particular allocation. Custom and practice, or indeed statutory requirements may dictate that a particular function be carried out in a certain way. Furthermore, a priori decisions by management may reduce the designer's freedom. Where the designer is concerned with a modification to or a partial extension of an existing system he may not have the freedom to examine previous allocation decisions and hence may not be able to achieve optimized allocations.

The most comprehensive approach to the problem of allocating functions in nuclear power plants was produced by Pullian, Price, et al. in 1983 as NUREG CR-3331 [19]. This report was preceded by a comprehensive review of the subject (NUREG CR-2623), including a useful set of references to which the interested reader is directed [20]. The expert group acknowledges the value of these two documents, on which the present report is based. However, whilst the approach adopted in NUREG CR-3331 is comprehensive, it is questionable whether the methodology proposed is realistic in a true design situation. The methodology consists of many stages of analysis which, if performed for each and every function of a new plant design, would represent a significant engineering resource. Also, the methodology does not fully account for the practical 'sharing' of tasks which occurs when the operator is provided with means of intervening in automatic processes and when automation is used to support operator decision making. The present report seeks to address these points by presenting a pragmatic, and more cost-effective method for assigning functions in the context of a large project.

In many instances, it will be necessary to provide a quality assured design in which all decisions regarding allocation of functions are documented and supported by adequate data. Approaches have been developed which seek to provide quantification of the factors involved by establishing decision criteria based on safety, availability, reliability, maintainability, cost, etc., and then assigning quantitative values to each factor. Paired comparison techniques are then used to establish relative importances and weighting the results. It is difficult to see this approach yielding unequivocal results or becoming widely used but it may have merit in causing the designer to consider all relevant factors in more systematic manner.

## 5. FUTURE TRENDS AND NEEDS

### 5.1. AUTOMATION

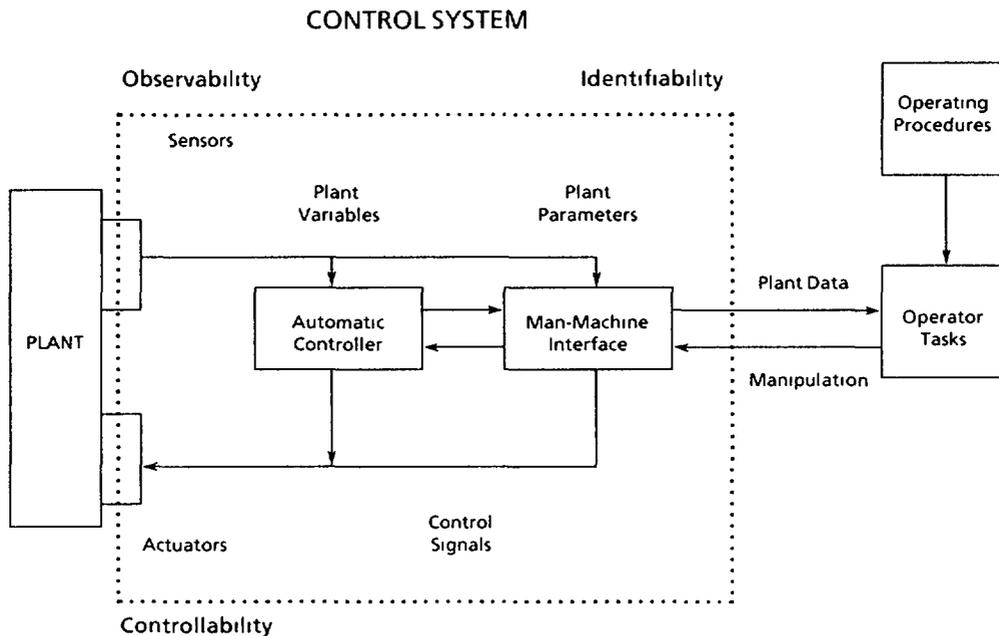
In nuclear power plants, automation of information acquisition, processing and display is an established feature. Similarly, automatic control of plant functions is a key feature of operation. Automation of safety and protective actions has long been necessary in order to achieve system reliability targets. Recent disastrous industrial accidents (Bophal and Chernobyl) have focused world attention on operator errors and have stimulated proposals for increased automation to reduce operator errors. Furthermore, as digital technology becomes increasingly available and economical, there is a trend by designers to produce more integrated systems which encompass many of the plant monitoring and control aspect. Additional operator support functions are being incorporated, particularly to support fault identification and analysis and to extend critical function monitoring and present procedures on graphical CRT displays. These developments are taking place in many design agencies and utilities throughout the world and reflect a desire on the part of all operating staff and managements to provide improved monitoring of plant operations and added assurances regarding safety. Increased use is also made in the field of robotics for maintenance activities, particularly in arduous condition areas. These topics are discussed by Bastl [21,22].

In order to address the increasing use of technological solutions in the design of nuclear power plant systems and equipment, designers are adopting a more system-based approach. For the designers, the additional technological features provide further challenges in terms of justifying their style, form and integration into the overall plant control and monitoring systems. Integrated systems provide greater potential for presenting high level information to operators and improving their comprehension of complex events. The additional levels of automation will tend to insulate the user from the raw system and exacerbate any problems caused by machine failure and mal function. This concern is partially solved by systematic and rigorous verification and validation of the automated systems performed by the users. The designer should ensure there is a nett gain in overall functionality when new technologies are incorporated into an existing system.

### 5.2. KNOWLEDGE BASED SYSTEMS

In recent years, the use of expert systems with artificial intelligence and techniques has become more of a working reality. Many applications are employing such devices in non-critical operational roles, such as personal advice consultation systems, diagnostic features, etc. In some cases, such devices are being evaluated in safety-critical roles, e.g. rule compliance monitors. Developments are expected to appear in areas such as knowledge-based monitoring, abnormality diagnosis, together with the creation of advanced information systems which embody information filtering, reduction and processing features. In general, increased attention needs to be paid to software and system quality assurance aspects, particularly for safety-critical applications. By their nature, true expert systems are non-deterministic. This presents a particular challenge for safety applications. Some attempts have been made to address this problem [23, 24].

The increasing use of computer capability to enhance operator performance has led to changes in the role of operating staff from a role of traditional equipment operator to one of high-level process plant system



*FIG. 5.1. Control system and operator.*

manager. This provides increased operator support via improved information displays which aid perception of operating state. Incorporating fast, real-time simulators into the normal control interface is another possibility under consideration. This could make possible the prediction of the results of operator actions and thus aid the quality of decision-making, particularly in complex situations. A further possibility is the dynamic assignment of functions by the automatic systems under abnormal or accident conditions when operators require additional support and hence a larger proportion of routine or procedural functions carried out by automation. Such an approach would need consider the intellectual superiority of the human operator and ensure that he retained the ability to exercise overall control when he desired, but under automatically applied constraints where critical safety functions are concerned.

### 5.3. PERFORMANCE DATA

There is a need for designers to obtain a better understanding of human behaviour in complex systems. Although significant initiatives have been seen in many member countries, this topic remains one of International concern and in order for human performance data to be shared and compared there is a need for improved data collection, analysis and exchange systems. To be useful in practical system design, human performance studies must be concerned with producing credible, realistic data from situations which reflect realistic operational situations. For nuclear plant applications, research using real-time simulations, such as full scope plant simulators and, to the extent possible, by examining real operating situations, either by live studies or analysis of operating data, will prevail over more academic studies using non-operational subjects in laboratory conditions.

The human decision making model of Rasmussen which proposes skill, rule and knowledge based facets of behaviour is well recognised as a philosophical function for applications of man-machine interface technology. Experience in applying this model to practical design situations suggests the need to further refine the concept to provide a

better understanding of the way in which the various levels in the model relate to each other and how practical operator behaviour maps onto each of the levels.

For nuclear power plant applications, there is an increasing need for improved design methodologies which result in automatic system designs which are more human centred. Research is needed to provide such methods and validate to the satisfaction of designers, plant operators and regulators. The studies must include task assignment, number of operators required, operator roles, team organization and interaction, job content, etc. There is therefore a clear need for research into human performance and human behaviour in all aspects of system operation. In high-risk industries, where system performance is critical to safe operation, human behaviour under extreme circumstances becomes of dominant interest. In all these areas, the extent of available knowledge is insufficient and some workers are researching these topics. There is scope for more work specifically directed to the needs of the nuclear power industry.

## 6. RECOMMENDATIONS

From the efforts of the expert group and the results contained in this document, the following recommendations are made:

- (1) The researchers and designers are recommended to promote the use of more systematic approaches to identify and assign functions in nuclear power plants.
- (2) A route for achieving this would be to initiate an International Research Programme which would apply the methodology proposed in this document to a number of suitably sized test situations encompassing review of existing designs and trial new designs. Results to be sought from the Programme would include realistic experience in the application of the methodology, data on its cost-effectiveness and a judgement of how well it accords with regulatory needs. Such a programme would examine functional decomposition methods, incremental application of the proposed assignment methodology and the extent to which the method is auditable.
- (3) In order to further support the work of this document the following actions will be useful:
  - To promote improved systems for human performance data collection, and as importantly, international data exchange between parties. Factors to be examined should include common data structures and data classification systems.
  - To identify the cost implications of human errors in nuclear power plants and promote improved use of root-cause analysis.
- (4) Available information on the nature and compatibility of performance data for hardware, software and human performance should be analysed in order to evaluate the integrity with which each can be combined in overall calculations of system reliability in existing PRA methods.
- (5) Managers of design teams should ensure that the compositions of such teams include human factors specialists and staff with operational experience, particularly in the early phases of design.

**Appendix A**  
**EVALUATION TECHNIQUES**

Technique	Typical use
Hierarchical Task Analysis (HTA)	Task Identification
Task Decomposition	Task Needs Identification - performance requirements - knowledge required - displays and controls
Functional Decomposition (IEC Standard 964)	Control Room MMI Design
Function Analysis System Technique (FAST)	Function Relationships where no procedure exists
Time Line Analysis	Work Load
Operational Sequence Diagrams	Work Space Layout
Activity Analysis	Work condition, team organization, task organization
Network Analysis	Sequence of Operations
Flow Process Charts	Plots of operator activity or information flow time sequences
Task Criticality Rating	Consequence/Risk Analysis
Selection Analysis	Determine skills, knowledge, special aptitude and physiological characteristics needed to perform tasks
Training Analysis	Determine if special training/training equipment needed
Decision-making Analysis	Determine types of decisions required of personnel and information needed to make decisions
Link Analysis	Determine interactions and communications between people in systems

---

Technique	Typical use
Behavioural Task Analysis	Analysis of troubleshooting and non-troubleshooting tasks
Equipment Analysis	Identifying equipment maintenance needs
Functional Analysis	Isolating discrete and measurable functions of equipment
Correlation Matrices	Summing up all links between operators, work-stations and/or equipment

---

**Appendix B**  
**A TYPICAL 'FITTS' LIST**

Functional attributes of men and machines

---

<b>Man</b>	<b>Machine</b>
+ 'Single Channel' device	+ 'Multi Channel' device
- Limited capacity for information processing	+ High capacity possible
- Poor computational skills	+ Excellent computing power
- Limited reliability	+ High potential reliability
Limited repeatability- high short-term precision	+ High repeatability- continuous performance possible
+ 'Graceful' performance degradation	- Sudden performance degradation - redundancy required in system
+ Good Long-term memory possible	+ 'Infinite' memory capacity
- Relatively poor short-term memory	- Volatile memory
+ Self error-correcting	- Needs error-correcting system
+ Complex Pattern Recognition- can simplify complex situations	- Requires exact programming to handle patterns-modern techniques not yet proven
+ Loose job specification- flexible in Approach	+ High repeatability- needs exact 'job' specification
+ Can generalise & make inductive decisions	- 'Narrow' behaviour for efficient working
Can handle short-term overloads	+ Robust against overloads if so designed

---

## REFERENCES

- [1] COMMISSION OF THE EUROPEAN COMMUNITIES JOINT RESEARCH CENTRE, Status Report on Assistance to Operators of Nuclear Power Plants in Emergency Situations in Europe, (4 Vols.), Ispra (1980).
- [2] INTERNATIONAL ELECTROTECHNICAL COMMISSION, International Standard IEC 964, Design for Control Rooms of Nuclear Power Plants (1989).
- [3] INTERNATIONAL ATOMIC ENERGY AGENCY, Basic Safety Principles for Nuclear Power Plants, Safety Series No. 75-INSAG-3, Vienna (1988).
- [4] INTERNATIONAL ATOMIC ENERGY AGENCY, Improving Nuclear Power Plant Safety Through Operator Aids, IAEA-TECDOC-444, Vienna (1987).
- [5] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Power Plant Instrumentation and Control, A Guidebook, IAEA Technical Reports Series No. 239, Vienna (1984).
- [6] MOUTREY, G.B., JENKINSON, J., The Role of Operating Staff in Automated Systems for Nuclear Power Station Control and Monitoring, INPO/EdF Human Performance Workshop, Lyon (1980).
- [7] LIPSETT, J.J., OLMSTEAD, R.A., STEVENS, J.E.S., Balancing the Roles of Humans and Machines in Power Plant Control Rooms, AECL-9955, Chalk River Nuclear Labs., Canada (1989).
- [8] BRAZENDALE, J., Allocation of Functions Between Man and Programmable Electronic Systems in Safety-Related Applications, Health & Safety Executive, Bootle, UK (1988).
- [9] INTERNATIONAL ATOMIC ENERGY AGENCY, Human Error Classification and Data Collection, IAEA-TECDOC-538, Vienna (1990).
- [10] BOHR, E., HENNICH, J., PREUSS, W., THAU, G., Human Factors in Nuclear Power Plants, IfU/TW-Rheinland, Cologne (1977).
- [11] BECKER, G., PAGE, S.J., HEYDEN, W., LIERE, B., Behaviour of NPP main control room staff, IfU/TW-Rheinland, Cologne (1983).
- [12] ALEITE, W., GREMM, O., "Status of NPP Automation in the Federal Republic of Germany" Balancing Automation and Human Action in Nuclear Power Plants (Proc. IAEA/NEA(OECD) International Symposium Munich, 1990) Vienna (1991).
- [13] EDWARDS, E., LEES, F.P., Man and Computer in Process Control, Institution of Chemical Engineers, London (1972).
- [14] JORDAN, N., Allocation of Functions Between Man and Machines in Automated Systems, Journal of Applied Psychology 47, 161-165 (1963).
- [15] SWAIN, A.D., GUTTMAN, H.E., Handbook on Human Reliability with Emphasis on Nuclear Power Plant Applications, NUREG-1278, NUCLEAR REGULATORY COMMISSION (1980).
- [16] CHAPANIS, A., Man-machine Engineering, Wadsworth Publishing, CA, (1965).

- [17] UNIPEDE NUCLECONT Expert Group 10, Computerised Operator Support Systems and Lifetime Extension/Replacement Strategy for Instrumentation and Control Systems in Nuclear Power Plants, Special Report to UNIPEDE Congress, Copenhagen (1991).
- [18] KANTOWITZ, B.H., SORKIN, R.D., Allocation of Functions (in Handbook of Human Factors, Ed. Salvendy, G., Wiley, New York) (1987).
- [19] PULLIAN, R., PRICE, H.E., et al; A Methodology for Allocating Nuclear Power Plant Control Functions to Human or Automatic Control, NUREG/CR-3331, NUCLEAR REGULATORY COMMISSION (1983).
- [20] PRICE, H.E., MAISANO, R.E., The Allocation of Functions in Man-Machine Systems: A Perspective and Literature Review, NUREG/CR-2623, NUCLEAR REGULATORY COMMISSION (1982).
- [21] BASTL, W., "The Key Role of Advanced Man-Machine Systems for Future Nuclear Power Plants", Man-Machine Interface in the Nuclear Industry (Proc. IAEA/CEC/NEA(OECD) Conference (Tokyo 1988) Vienna (1988).
- [22] BASTL, W., Computerised Aids and Human Factors in Nuclear Power Plant Operation Where To Go from Here?, International Seminar on Human Interface, Kyoto, Japan (1988).
- [23] ELECTRIC POWER RESEARCH INSTITUTE, Approaches to the Verification and Validation of Expert Systems for Nuclear Power Plants, EPRI Report NP-5236 (1987).
- [24] ELECTRIC POWER RESEARCH INSTITUTE, Verification and Validation of Expert Systems for Nuclear Power Plant Applications, EPRI Report NP-5978 (1988).

## BIBLIOGRAPHY

BENTO, J.-P., Analysis of Human Performance Problems at the Swedish Nuclear Power Plants, Proc. IEEE 4th Conference on Human Factors and Power Plants, Monterey, CA (1988).

BISHOP, J., Managing Human Performance, INPO/EdF Human Performance Workshop, Lyon (1986).

DELIANT, J., GHERTMAN, F., Identifying Root Causes of Operations Errors, IN/O/EdF Human Performance Workshop, Lyon (1980).

FITTS, P. M. et al, Human Engineering for an Effective Air Navigation and Control System, Nuclear Regulatory Commission, Washington D.C. (1951).

GHERTMAN, F., GIFFON-FOUCO, M., Investigation of Human Performance Problems at French Power Stations, (Proc. Conf., 3rd IEEE Conference on Human Factors and Nuclear Safety, Monterey, CA) (1984).

INTERNATIONAL ATOMIC ENERGY AGENCY, Man-machine Interface in the Nuclear Industry (Proc. Conf., Tokyo, 1988), IAEA, Vienna (1988).

INTERNATIONAL ATOMIC ENERGY AGENCY, Balancing Automation and Human Actions in Nuclear Power Plants (Proc. Conf. Munich, 1990), IAEA, Vienna (1990).

JANKALA, K. E., VAURIO, J. K., WORIO, U.M., Plant Specific Reliability and Human Data Analysis for Safety Assessment, Nuclear Power Performance and Safety, (Proc. Conf. Vienna) (1988).

KEENER, B.A., Industry Perspectives and Lessons Learned on Procedure Writing, Keener, INPO/EdF Human Performance Workshop, Lyon (1986).

MESLIN, T., IDEC, E., MONSERIN-DUPIN, F., Statistical Analysis of Operator Performance During Accident Simulation, INPO/EdF Human Performance Workshop, Lyon (1986).

MEYER, F., Safety Experience in the Biblis Nuclear Power Plant, INPO/EdF Human Performance Workshop, Lyon (1986).

SWATON, E., Human Contributions to Safe Operation: Blessing or Menace?, IBC Conference on Human Reliability in Nuclear Power, London, UK (1989).

TECHNICAL RESEARCH CENTRE OF FINLAND, Artificial Intelligence in Nuclear Power Plants, (Proc. Conf., Espoo, Finland, 1989), IAEA/IWG NPPC&I Specialists Meeting (1990).

WALKER, I., Candu Human Performance Analysis, INPO/EdF Human Performance Workshop, Lyon (1986).

WILLIAMS, J.C., Human Factors Analysis of Automation Requirements—A Methodology for Allocating Functions, 10th Advances in Reliability technology Symposium, Bradford UK (1988).

VANDERGRIFT, J.D., PATRICK, P.W., Training Not Necessarily The Cure, INPO/EdF Human Performance Workshop, Lyon (1986).

ZIMMERMAN, R., ETSCHBERGER, K., MUCKL, W., Problems for Man In Modern Process and Supervision, Regelungstech, Prax, Vol. 17, No 8, Germany (1975).

**Annex**

**PAPERS PRESENTED AT ADVISORY GROUP MEETINGS**

# DEVELOPMENT AND APPLICATION OF COMPUTERIZED OPERATOR AIDS FOR GERMAN NUCLEAR POWER PLANTS

W. BASTL

Gesellschaft für Reaktorsicherheit (GRS) mbH,  
Garching, Germany

## Abstract

The possibility of introducing a new quality of information for operating nuclear power plants has been considerably increased since the necessary hardware and basic software is available (at increasingly lower costs) to perform even complicated data and information processing in an industrial environment. This led to considerable work in an area often addressed as computerized operator aids. Although these aids are to provide information (only) and leave the final decisions and actions with the operator, it must not be failed to notice that an automation process at the information level took place, with many of the consequences we are concerned with when being faced with full automation, i.e. including the action on the process. Questions are: transparency of information, quality of information, reliability of information system, operators dependency on information, etc.

GRS has contributed to the development of operator aids in the following four areas:

- signal validation
- plant information and diagnosis
- mechanical component information and diagnosis
- hard- and software qualification

This paper presents the main developments, applications and future plans.

## 1. SIGNAL VALIDATION

Signal validation is more and more recognized as a necessary component in computerized information systems which have to interpret and condense a huge amount of sensor data. The output of these information systems depends strongly on the accuracy of the incoming primary data: Faulty primary data will lead to faulty output conclusions which may never be detected.

A system for the validation of signals coming from the plant with a fixed scanning rate (of about 1 sec for analog signals in German nuclear power plants) has to decide very rapidly on the correctness of these data to prevent a delay in the diagnosis of the following plant information system. Thus the main demand on on-line signal validation is to work in real time. Special algorithms for the detection and identification of faults are required as well as a hardware suited for fast processing.

The aim of signal validation is the detection of a change in a signal's magnitude or behavior not originating from the normal dynamics of the plant. Such a change can be caused by two reasons: First, the sensor or the electronics belonging to it have failed, accordingly called a sensor fault, or second, the component where the sensor is located is in an abnormal state, accordingly named process fault. The distinction between the two types of faults cannot be performed by means of the fault identifying algorithms without having additional knowledge, e.g. that a measurement signal representing the water level of a vessel can change because of a (temperature) drift in the measuring device or as a consequence of a small leak in the vessel. Thus, from the signal validation point of view, the classification of the fault's time constant is more appropriate than the distinction between sensor and process faults. Depending on the time constant of the fault, different principles must be used for the detection and identification of abnormal changes in measurement signals.

### 1.1 A Three Level Conception for Fault Detection processing Measuring Signals in the Time Domain

For the reliable detection of faults during steady and dynamic plant operation conditions as much information as possible is needed. This information can be obtained from three levels of knowledge, the signal level, the process level and the system level. Accordingly, GRS has developed a three-level concept called LYDIA (earLY sensor and component fault detection and DIAGnosis).

At the signal level hardware redundancy (if available) can be used for validation. Two or more signals representing the same physical quantity are compared to each other and small deviations between the signals can easily be determined. The algorithms belonging to this signal level are appropriate for the identification of faults of any time constant and do

not require additional proceduring knowledge; they are well established and need not be discussed in detail.

Signals representing different physical quantities and belonging to the same component, e.g. a vessel or a steam generator, are being processed at the process level. The relationship between these signals is described analytically by a physical model, thus causing analytical redundancy. Several methods of modern control theory are available in order to interpret the physical model. They are well suited for detecting sudden changes in measurement signals. For signal validation at the process level a computer program called IFDI-module has been developed at GRS. This program is based on different methods of analytical redundancy which have been modified and adapted to the requirements of an on-line fault detection in real time [1].

Very slowly varying faults can be identified by monitoring larger parts of the plant which consist of several components. A new method of fault detection at this system level has been developed by GRS which models the system under consideration as a Petri Net [2]. It compares the actual state of conservation quantities with the initial state. On the one hand the complexity of the fault-detecting algorithm is very low, but on the other hand a lot of proceduring knowledge is needed. The system's future behaviour can be predicted.

## 1.2      Applicational Aspects

The IFDI-module mentioned above has been tested on-line in the LOBI-MOD2 facility of the Joint Research Centre Ispra, Italy [3]. The results have shown the capability of our conception. It has been demonstrated that the IFDI-module is able to identify sudden changes in measurement signals of different height in real time which are not caused by the dynamics of the plant.

The Petri Net based technique of fault detection at the system level has up to now been tested off-line only. The plant data, stored on a magnetic tape, originate from the Biblis-B nuclear power plant.

The algorithms of each fault detection level are implemented in a separate computer program. At the system level only one program is needed while at the process level one IFDI-module is required for each component (at

the signal level one module for each group of redundancies). To enable an easy application, a CAE-tool (CAE: Computer Aided Engineering) automatically adapting the IFDI-modules to the single components, has been developed.

### 1.3 Next Steps of Development

A first test of the entire three-level conception LYDIA concerning the secondary side of a power plant is in preparation. The GRS simulator ATLAS will be used to generate the measurement data and to simulate normal and abnormal operation conditions considering about 300-400 measurement signals of the secondary side. The performance of LYDIA will be tested processing these data while sensor and process faults are simulated in addition.

To enable real time processing a transputer system will be used. Due to the parallel structure of the problem such a hardware is well suited for on-line fault detection in plants or in other complex technical facilities; at the same time pairs of hardware redundancies (signal level), different components (process level) as well as the whole system (system level) are to monitor independently of each other. After each software module has processed its part of the measurement data and has decided about their correctness, a diagnosis unit has to interpret all the modules' messages. To perform this, techniques of Artificial Intelligence will be used.

## 2. PLANT INFORMATION AND DIAGNOSIS

The desire for improved information in the control room may be driven by different ideas, e.g. reduction of information load, enhancement of plant status information, operator guidance during plant disturbances, etc. When realizing these ideas one has to be able to perform all types of signal handling, to use algorithms or even simulators in order to fulfill the desired information task. For this reason GRS developed GENERIS, a program package for a generic information system which can be used for any information task [4]. It is a comprehensive and flexible system which allows later extension of the information tasks without consistency problems. Up to now, five different applications have been realized in coope-

ration with a plant manufacturer (Siemens/KWU and NPPs Biblis B, KKP 2, Gundremmingen B and C):

- symptom oriented display of disturbed plant situations,
- status surveillance of components and plant systems,
- alarm reduction,
- post trip analysis,
- integrated disturbance analysis.

Original software development costs for each of these functions would be in the order of 2 mill. US \$. Using the GENERIS-software package the development costs can be reduced to about 20 %.

## 2.1 Symptom Oriented Display of Disturbed Plant Situation

There is no doubt that qualified operating personell can safely operate the plant using conventional instrumentation and following the rules of the operation manual. Recently a diverse method, the so-called symptom-oriented approach, has been introduced. For this, special safety goals had to be defined such as subcriticality of the reactor, containment integrity, core cooling and heat removal, etc. Information on violation of safety goals, failing of relevant systems and appropriate actions is presented on colour screens demanding extensive information processing, in many cases at high integration level.

In an on-line test application at Biblis B three graphical representations (dynamic pictures) had been developed and implemented: P,T-diagram, heat-balancing of the residual heat removal circuit, overview of safety relevant filling status. The implementation has been tested by gathered signal flows of the past. The test showed that a comprehensive and clear information representation is possible when using fullgraphic colour screens. Their operational qualification was successfully shown during the test phase [5].

## 2.2 Status Surveillance and Alarm Reduction

In order to enable the presentation of a complete overview of the plant status on a colour graphic screen and to keep an actual update all signals which describe the status of a component are logically combined to a so-

called status vector. Each of these status vectors may be combined with its technologically corresponding partners to a new status vector which then describes a higher level system [6].

During the Philippsburg application a total of about 600 of those status vectors have been defined by the plant vendor (SIEMENS/KWU). All of these vectors are combined in a corresponding status signal for each functional unit. As the vector is represented in a so-called status word (16 bit), the display system can easily utilize the information provided on components and functional units to determine colours and other status information in plant schematic diagrams. For example, not only the status of a pump (on/off), an external/internal fault, or a power-operation/start-up/shut-down is delivered from the status vector, but also whether or not a signal is plausible.

Taking into consideration the large number of unnecessary alarms often appearing during plant disturbances, the reduction of the latter is a very desirable goal. To successfully decrease the number of alarms the dynamic behaviour needs to be analysed and then modeled so that the respective situations can be identified. Once such a situation has been detected a list of associated alarms bound for suppression can be activated.

Using the same modeling method as for status surveillance, a suppression rate of about 88 % could be obtained in KKP 2 application. There were two main suppression strategies:

- suppression of alarms in dependent systems where the original fault was to be found in a support system and
- special situations with individual suppression of selected alarms.

### 2.3 Post Trip Analysis

One of the most important tasks after a trip or similar event in the plant is to determine whether or not the sequence of protective events has occurred as designed with regard to chronology as well as to completeness. Although this task, too, can be modeled by using the methodologies described above, there are some additional problems to be considered. While alarm reduction and status surveillance determine which message is to be delivered or which alarm is to be suppressed the very moment the

event pops up, in post trip analysis this can be done only after a surveillance time frame has been completed. This means that from the occurrence of the event until the moment the final information is given, up to 20 minutes may elapse. To make the models behave properly, intensive use of so-called time-delays is required.

As for today, there have been four applications: KKP 2, Biblis B, and Gundremmingen B and C. The basis of the application is an average of 130 time-frames to be monitored and encompassing around 30 signals each.

#### 2.4 Integrated Disturbance Analysis

For this application disturbances as well as any kind of deviation from the operational desired status of the plant or of its components are picked up. Considering the history of signal values, especially of the gradients of analog values, it is possible to detect such disturbances from the very beginning. By preanalysed models for disturbance sequences operator support is provided for diagnoses as well as for prognosis. Normally only those sequences are modeled which yield enough time for the operator to initiate actions to rectify the disturbance or at least to mitigate the effects.

In order to achieve these goals it has been necessary to build up a function oriented information structure and a hierarchical presentation scheme which has been realized with colour graphic overview pictures and trend curves. A prototype application focusing on the feedwater system has been performed in Biblis B [7].

Fig. 1 shows the developed overview-picture. It provides information about the status of the systems of the secondary side of a PWR: steam generation, heat sink and coolant transportation. The measured values of the main variables are shown (e.g. as bargraphs or as digital values) as well as subsystems status information and whether necessary signal correlation still persists. Various possibilities to transfer information to the operator have been exploited; e.g. colours to indicate the degree of severity of a disturbance, symbols to visualize deviations from normal and tendencies, text inserts to highlight system statuses, bargraphs and actualized digital values.

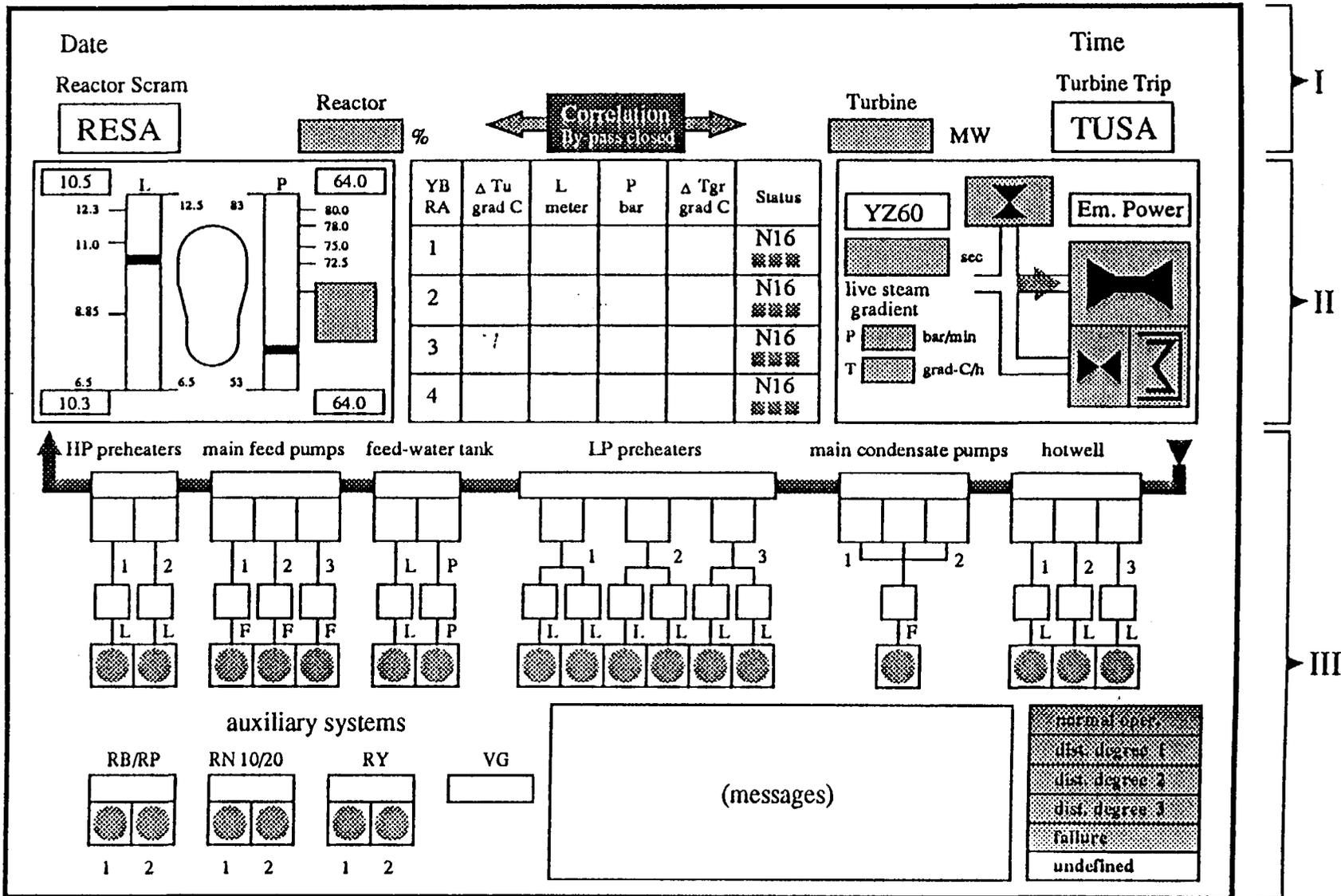


Fig. 1: Integrated disturbance analysis (overview picture)

The application was tested with actual process data of a NPP during a disturbance (loss of main heat sink). The main result was that valuable additional information can be given to the operator. Next steps of development will be the implementation of a picture hierarchy and an explanation module to give the operator the opportunity to go into detailed subsystem information presentation in case of subsystem faults.

Each of the five applications mentioned in chapter 2 has been realized in such a way that it can be extended on the basis of additional system analysis.

### 3. MECHANICAL COMPONENT INFORMATION AND DIAGNOSIS

Similar to the systems discussed before, which provide better information about the overall status of the plant by process parameter and system status analysis, an important progress has also been achieved in the fields of surveillance and early failure detection at the component and equipment level. Typical for these methods is the use of stochastic primary information, as a consequence of which much more effort has to be placed on signal analysis and interpretation than on "normal" reactor instrumentation. Depending on the problem, either analysis methods in time or frequency domain are applied. Very often essential information is taken from the interrelations between different channels (correlation analysis, burst pattern analysis). Methods which have been or are being developed at GRS comprise sensor surveillance, leakage detection, anomaly detection in processes and monitoring of passive and active components.

Concerning the mechanical state of the plant, there was little or no direct information to the operator in the past; he rather had to draw his conclusions from the process behaviour supplemented just by a few sensors indicating the status of active components. Since the 70ies research work in Germany has been performed by GRS and industry with the aim to develop methods and systems for on-line assessment and diagnosis of mechanical structures in the primary system. Emphasis was laid particularly on the early detection of mechanical deficiencies of reactor internals and primary circuit components. Indirect measuring methods based on acoustic, vibration, and process signal analysis have been developed successfully. Presently available in all German nuclear power plants are loose parts monitoring systems and available in all PWRs are vibration monitoring systems.

GRS has concentrated its efforts especially on signal interpretation in order to enhance the precision and reliability of the analysis with respect to potentially arising mechanical faults. Current activities are directed

- to gather operator experiences from different plants in suitable data banks,
- to built up a detailed knowledge base for interpretation of signal patterns and feature trends,
- to enhance the effectiveness by applying more automated and "intelligent" systems on-site, and
- to improve the man-machine interface.

### 3.1 Signal Interpretation for Validation and Loose Parts Monitoring

Extensive work performed during preoperational tests and at-power measurements with correlation and long-term investigations in several plants as well as theoretical 3-loop and 4-loop model investigations have led to a broad and detailed knowledge base: the vibrational behaviour is represented now by means of fully interpreted power density spectra, with the mechanical vibration of components allotted to the measured peak frequencies. Acceptable or not-acceptable (failure-caused) trends and margins of peaks and coherences have been determined or estimated.

Meanwhile a number of successful diagnoses led to a high acceptance of the vibration analysis by the utilities and the licensing authorities. Examples of such diagnoses are the predictions of failed hold-down springs at the flange of the reactor vessel and of loosened screws at the secondary core support (flow baffle). Both failure warnings could take place five months before the next refueling so that the repair could be well prepared. Other examples are described in [8].

Also the Loose Parts Monitoring Systems (KÜS) are multi-sensor-systems consisting of a set of accelerometer gauges distributed at the reactor pressure vessel (6 sensors) and the steam generators (at least 2 each). In loose parts monitoring delay times of bursts in different channels and the shapes of these bursts are used for location and energy/mass estimation by the analyzing specialist. For this purpose the burst patterns of actual impacts are displayed in parallel with a high resolution for related signals. The patterns have to be assessed and interpreted based on the

theory of stress wave generation (Hertz theory) and pulse propagation in solid structures and by means of experimental results of reference impact tests with known impact energies and impact locations. A number of events and successful diagnoses performed in the last 15 years have led to a broad acceptance of this diagnostic technique [9].

### 3.2 Improving the Man-Machine Interface

In plants of different size and power, GRS has collected an enormous number of noise signatures of normal and abnormal process conditions, of operationally influenced or failure-caused deviations, of burst patterns, of feature trends, etc. during the past years. Data banks for vibration and loose parts monitoring have been established at GRS enabling a fast access to reference signatures for comparison purposes. This continuously growing knowledge-base can be used to consult the utilities or authorities and to assist them in signal interpretation as well as for the current research activities directed to the development of automated knowledge-based diagnosis systems.

The following questions have been investigated in order to improve early failure detection based on noise diagnostics:

- How to ensure fast access to the GRS signature data bank in order to assist the on-site personnel in interpretation?
- How to transfer the centralized know-how to the plants and to install more intelligent systems on-site? How to automate the monitoring and signature storage procedures?
- What are the needs for signature and feature presentation and which communication capabilities are needed for the man-machine-dialogue?

Considerable progress could be achieved for these tasks; especially solutions for the man-computer interface were improved. For vibration and noise signals, GRS is able to provide three ways of assistance in data analysis (Fig. 2):

- 1) For older plants without advanced systems the signals are synchronously recorded in PCM-technique on magnetique tapes and analyzed at

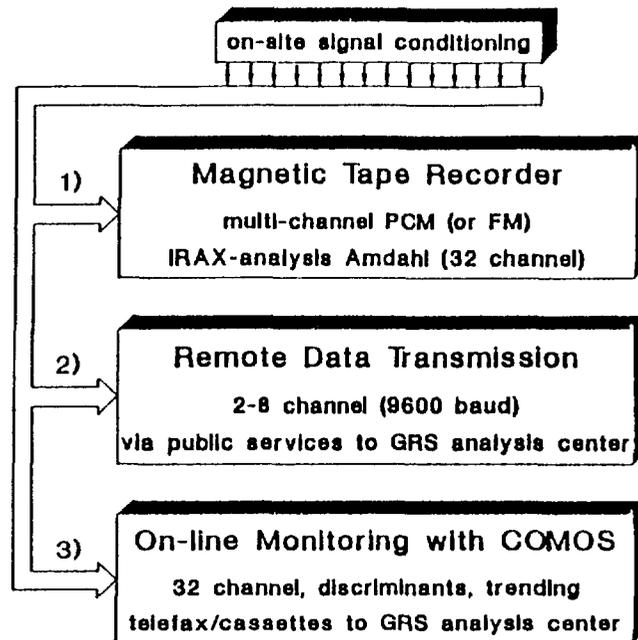


Fig. 2: Three modes of noise and vibration data link to GRS

the GRS analysis center (standard analysis since several years). Using the code package IRAX all auto and cross correlations of up to 32 channels are calculated with just one short computer run. The results are stored at a matrix tape and can be displayed at a CRT. The dialogue capabilities have been improved essentially. All desired functions coded in different colours can be superimposed by the analyst at a colour graphic screen and interpreted with respect to deviations from stored reference functions. The functions needed for the documentation are plotted.

- 2) Between the GKN-1 plant and GRS data analysis center a test and demo-system for remotely controlled fast data transmission has been established using the public telephone network. Whenever anomalies are detected on-site or when interesting operational conditions are given, a data-transfer for up to 8 channels with 9600 bauds can be started. The interpretation using the GRS signature data bank can be done immediately in the laboratory [10].
- 3) The third possibility is a new development of GRS, the Condition Monitoring System COMOS [11]. The system provides monitoring, storage, and diagnosis capabilities on-site and transfer of reduced data to the GRS analysis center (using tape cassettes, telefax, etc.). Statistical

quantities (discriminants) are used for feature monitoring and trending within allowed bands of deviation. These properties are important especially for fast escalating failures (e.g. shaft-ruptures of main coolant pumps). But also on-line-monitoring of all the other vibration signals of the primary circuit can be performed automatically in a second mode (with a smaller calculation rate). Up to now, COMOS-systems are already working in seven PWRs: GKN 1, GKN 2, KKG, KKI 2, KKP 2, Biblis A, Biblis B.

For the analysis of signals from loose parts monitoring, the computer-based system MEDEA mainly consisting of a ten channel transient recorder, a 32-bit workstation with CRT and mass memories is used in the GRS analysis centre [9]. Burst pattern data are transferred by FM-magnetique tapes, streamer tapes, floppies or, in the near future, via modems and telephone lines, to GRS. The burst patterns are classified with respect to different features and stored in the data bank. For that purpose, the patterns are at first displayed at a colour screen allowing the specialists to identify and determine the features. By extensively using the cursor, the values are fed into the computer calculating the necessary measures. Software-packages for location and mass estimation are available.

#### 4. HARD- AND SOFTWARE QUALIFICATION

The introduction of computers into information and diagnosis systems of nuclear power plants allows for a smoother and thus safer control of the plant. However, the qualification of computer systems consisting of highly integrated hard- and software of a virtually unlimited potential of possible logical reactions imposes a new dimension of qualification problems.

##### 4.1 HARDWARE QUALIFICATION

In addition to development systems, logic analysers and emulators, GRS employs instruments for computer-aided analog, digital or mixed-mode circuit-simulation especially for the purpose of carrying out up-to-date evaluation of hardware. The simulators (e.g. PSpice, LASAR6) are installed on high-speed computers (VAX 8700) so that computing times are kept within manageable limits, even when simulating very extensive and

complex circuits. With the help of the above-mentioned circuit simulators, the software-based modelling, simulation and testing of the hardware can be commenced already during the planning phase. The elaborate task of setting up laboratory samples during the early stages of development becomes superfluous. Usually it takes just a few minutes to create a computer model of alterations in circuits and analyse its effects. Computer-aided circuit simulation also allows a systematic analysis of the time response of hardware as well as the influence of tolerances. A prerequisite for the implementation of the above-mentioned simulators is the availability of the software models for the circuit elements. However, a hardware modeller also permits the inclusion of real circuit elements when modelling an entire circuit (e.g. an entire board) with LASAR6. This proves to be particularly advantageous if no software has yet been developed for an element (e.g. a novel element).

Another important tool is the fault simulator integrated in LASAR6. Analyses of the effects of failures in digital circuits, e.g. computer modules, can be carried out with its help. At present the fault simulator is being used in research projects to investigate the effectiveness of self-monitoring programs for computer modules. In the case of structure models (gate models) of microprocessors (8080, 8085, 8086/88) particular emphasis is laid on investigating the extent to which faults can be detected by means of self-tests, the possibilities of optimization and the reason why certain faults cannot be detected. Such data are indispensable in evaluating the effectiveness of fault identification measures when analysing the reliability of fault tolerating computer systems.

## 4.2 SOFTWARE QUALIFICATION

The three principles necessary for developing software which is to fail only with a specified minimum probability are fault-avoidance, fault-removal and fault-tolerance. Fault-avoidance is achieved during the constructive task of establishing software along a predefined life cycle according to good software engineering practice. Fault-removal is the analytic task of finding and correcting faults which are remaining in spite of careful software construction. Fault-tolerance aims at detecting failures during the execution of a program system including a following recovery procedure and a subsequent failure-masking. Thus failures, occurring in spite of constructive and analytic measures taken against, are tolerated.

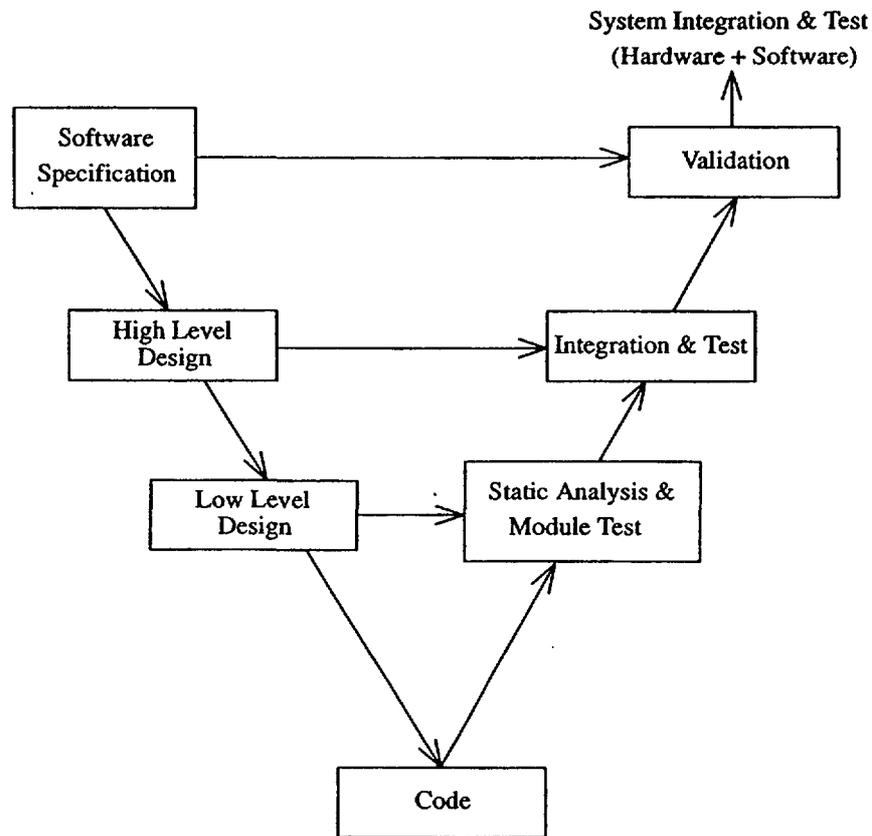


Fig. 3: The V-life cycle of software development

The term "software" denotes a set of products which are generated during the software life cycle (see e.g. the V-life cycle in Fig. 3). Software qualification means to demonstrate the conformity of the design and code levels with the functionalities laid down in the software specification. This is achieved by means of analytical techniques such as inspections, walk-throughs, static analysis, tests, etc.

GRS has developed a set of analytical methods and techniques which are well suited for the assessment and qualification of diagnosis systems [12]. Computerized tools supporting these methods, some of which will be described subsequently, have also been developed. Most of the information and diagnosis systems in German nuclear power plants are implemented either in Assembler or in Fortran language. The efforts of GRS have therefore been focussed on the development of analysis methods and tools formulated for these languages.

#### 4.2.1 STATIC ANALYSIS

Static analysis as part of software reliability assessment in general, aims at the detection of faults and anomalies, at the preparation of tests and at the collection of metrics for a qualitative and quantitative description of software attributes. In addition to these objectives, however, the demonstration of conformity between functions which are implemented in a program and those which are specified in the software specification can be achieved by means of static analysis.

Fig. 4 shows a general scheme of software development and static analysis.

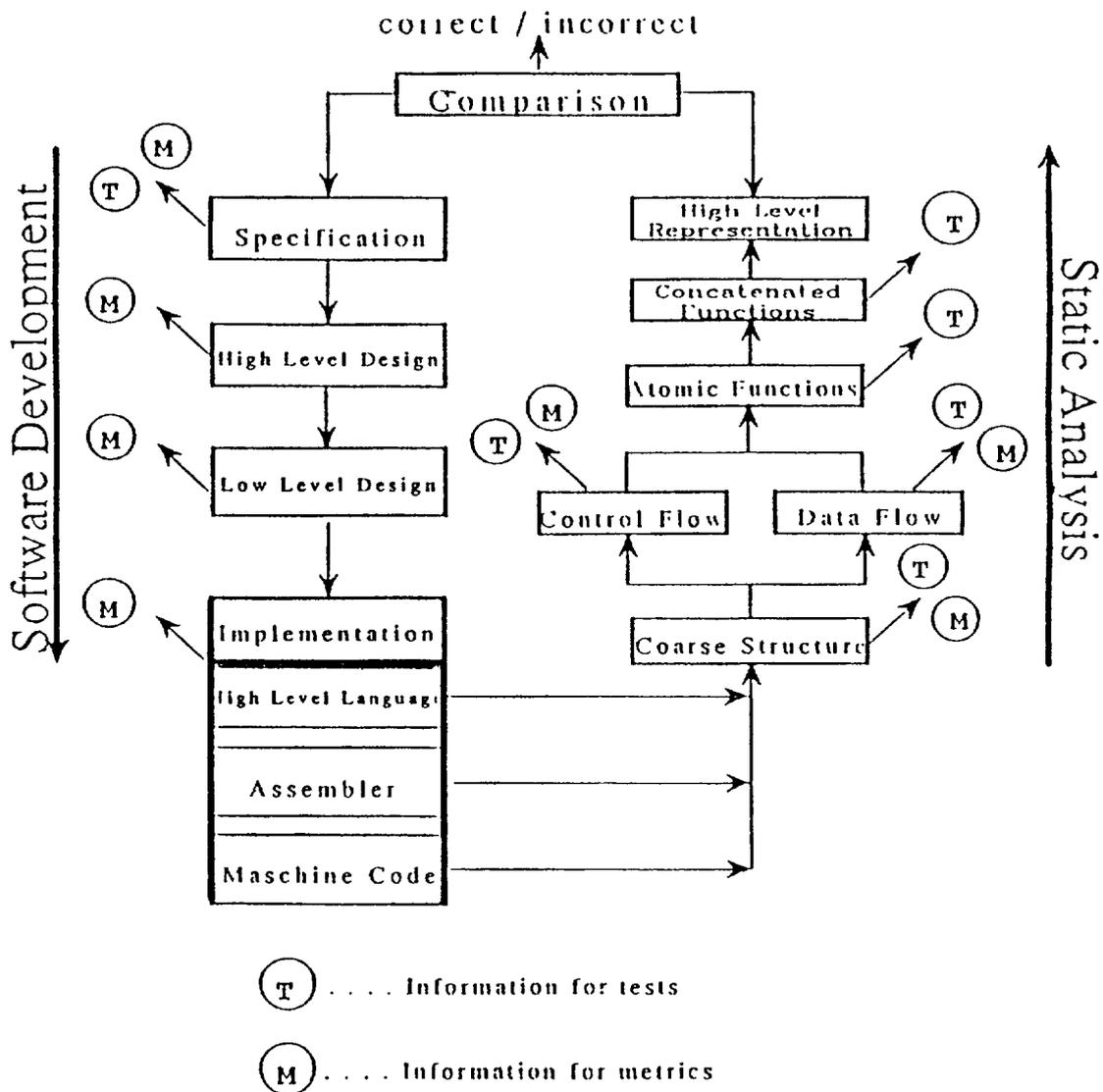


Fig. 4: Software development and static analysis

The left-hand column is a simplified software development route (ignoring the verification steps at each level) which ends in the implementation of a program being represented as either a high level language, assembly language or machine code. Some highly safety critical applications require to start the analysis from the machine code as the ultimate form of a program in order to avoid a rigid verification and validation of complex software such as a compiler. A tool supporting this approach will be described later.

The column on the right-hand side shows a possible approach of static analysis. At first the coarse structure (e.g. calling hierarchy) is identified, then the more detailed structure with regard to control and data flow. Up to this level, static analysis is being well supported by computerized tools. The next step is based on a common view of control and data flow, i.e. what happens with the data when a distinct path or set of paths is being traversed. This is the identification of "atomic functions" which are (not well defined) small actions, e.g. read an array, perform some linear operations on it and write the result in another array. These functions are then concatenated to more comprehensive ones until all program functions are represented in a way which allows a comparison with the specified functions. Should e.g. the specification contain logic diagrams, the high level representation derived by static analysis should also be a logic diagram. During this procedure information for the preparation of tests and for the extraction of metrics can be obtained, thus the main four objectives of static analysis are:

1. Collection of product metrics
2. Preparation of tests
3. Identification of faults and anomalies
4. Demonstration of conformity of implemented functions with specified ones

### COLLECTION OF PRODUCT METRICS

The first step of static analysis is a meaningful partition of the source code to be analyzed. Partitioning includes the identification of the coarse structure of a program, e.g. in terms of subroutines, modules, functions etc., as well as a breakdown into smaller units which form the basis for the representation of the control flow (e.g. basic blocks, sequential

parts, linear code sequence and jump). This in turn requires the scanning through the source code instruction by instruction. Scanning as well as the identification of the coarse structure can provide for a lot of primitive metrics such as no. of modules, no. of lines of code, no. of specific instructions, no. of operands/operators, etc. from which more sophisticated metrics can be computed. These metrics may be used to draw conclusions (compute correlations) to software quality attributes. The relationship between quality attributes and metrics, however, is still a matter of research.

### PREPARATION OF TESTS

During the process of static analysis as shown in Fig. 4, the analyst gains a deep insight into the program's coarse structure (hierarchy, module interconnection) and fine structure (control flow). Also known by now are functions which are performed by small code units up to concatenated ones (realistically between up to 50 and 100 third generation language instructions). Due to this knowledge, functional as well as structural tests can be prepared.

### IDENTIFICATION OF FAULTS AND ANOMALIES

Several classes of faults can be found by means of static analysis. During preparation and performance of control flow analysis, typing errors and codes which are not reachable are recognized. Concerning assembler programs, the use of wrong registers and flags is indicated, a fact that may result in both control and data flow errors.

Data flow analysis is concerned with the use of variables, i.e. variables referred to but not defined (error message) or defined but never referred to (warning). Mode checking reveals anomalies in the mode of variables and constants, in assignments and expressions as well as in the number and mode of formal and actual parameters of CALL statements (e.g. subroutines and functions).

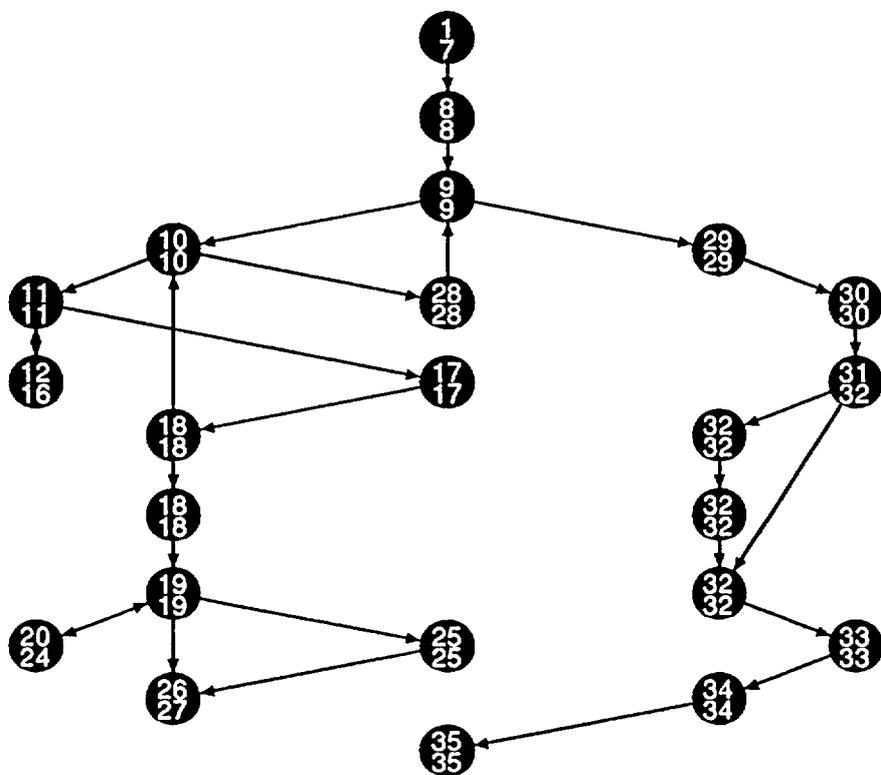
## DEMONSTRATION OF CONFORMITY OF IMPLEMENTED FUNCTIONS WITH SPECIFIED ONES

The most ambitious objective of static analysis is the demonstration of conformity of the actually implemented functions with those fixed in the program specification (see Fig. 4) In this approach a reverse development procedure from a low level program representation (machine code, assembly language, high level language) to a high level one is involved. For a large part of this procedure no computerized tool support is available, i.e. it is performed purely mentally. This implies that the approach is a) error-prone and b) time consuming, thus in general it will only be applied to small programs. Both disadvantages can be drastically reduced if the program to be analyzed is well structured and readable. Readable in this context means that the code itself should be readable. It needs not necessarily be well commented; in many cases it will even be delivered without any comment to the analyst in order to maintain independence between the developer and the analyst to avoid common errors. Another powerful possibility of reducing the error-proneness of the mental approach of reverse development is to specify test cases on the basis of the knowledge of control flow, data flow and functional behaviour of the analyzed program. A method for this kind of static analysis which is particularly suited for assembler programs, has been developed by GRS.

The source code is represented by a graphic which reveals control and data flow in a program. Starting with this graphic and the source code, the analyst develops reversly towards a high level representation which can be compared to the program specification [13].

## TOOLS FOR STATIC ANALYSIS

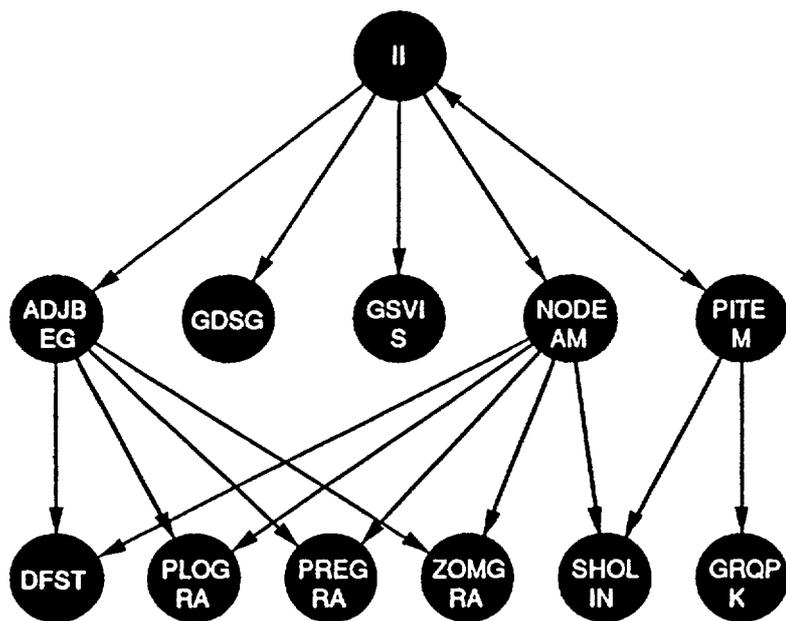
As already mentioned the process of static analysis can be based on tools up to the step exhibiting control and data flow. Some tools provide for more than control and data flow, but in most cases these additional features are applicable only under severe restrictions of the code. The control flow is represented by many tools similar to those shown in Fig. 5, as they use a graph-theoretic approach to break down the source code to be analyzed. Thus the sequential parts of the control flow are represented by nodes of a graph; the lines between the sequential parts become directed arcs of a graph.



**M E N U :**  
 REACHABILITY +  
 REACHABILITY -  
 REACHABILITY \*  
 PREDECESSORS  
 SUCCESSORS  
 NODE CONTENT  
 HARDCOPY  
 ZOOM  
 EXIT +

**A C T I O N :**  
 MC CABE -> 6

Fig. 5: Control flow graph



**M E N U :**  
 PREDECESSORS  
 SUCCESSORS  
 SYMBOL LINES  
 VIEW SOURCE  
 ZOOM  
 HARDCOPY  
 EXIT

**A C T I O N :**  
 SYMBOL II

Fig. 6: Data flow graph of the variable II

## THE FORTRAN ANALYZER FANAL

The FORTRAN-Analyzer FANAL is used to analyse the control and data flow. Its main interfaces are a text string (source code) as input, a cross reference list (normally produced by a compiler) as input, the representation of a directed graph in form of a data structure as output, a dialogue input, and some graphical representation of directed graphs as a user interface. FANAL provides possibilities of an interactive traversal of the control flow graph to show the reachability of nodes (forwards, backwards, both directions) to chosen parts of the graph. Fig. 5 is an example of a control flow representation.

Concerning data flow the tool enables the representation of data dependencies. A typical question is: Which variables are used to generate the value of a distinct variable? The answer of FANAL to a question like this is shown in Fig. 6.

## THE COMMON ASSEMBLY LANGUAGE ANALYZER STAN

The common assembly language CAL [14] is defined on the basis of the assembly language of the 8-bit processor Z80, 16-bit processors MC68000 and INTEL 8086 and 32-bit processors VAX and IBM Series-1. These different processors, which are commonly used in many applications, give hope that CAL can also cover the instruction sets of further microprocessors. STAN converts the CAL-Code of each routine into a directed graph. Structural analysis of this graph identifies all loops including their nestings. A subgraph is attached to each loop. The resulting subgraph hierarchy reveals the structure of the CAL-Code (Fig. 7).

For each subgraph of each routine a print-out of the following details is given: type of the subgraph, level in hierarchy, number of nodes (blocks and sub-subgraphs), the start block, the exit blocks, the return or stop blocks, the latch blocks (blocks with an arc back to the start block), and the loops contained in the subgraph. It is also possible to generate plots of these subgraphs. During structural analysis STAN also generates some subordinate results such as labels which are not used or the irreducibility of a routine graph, one of the most serious violations of the rules of structured programming.

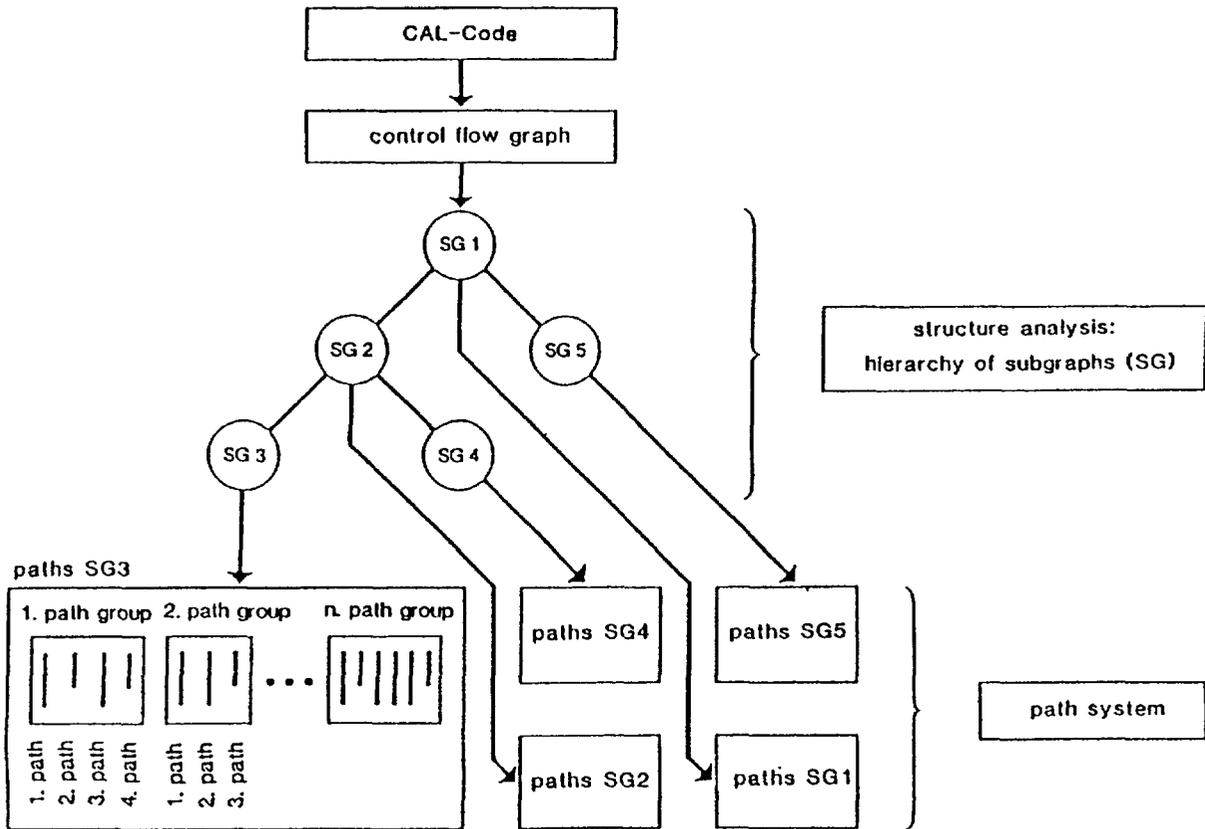


Fig. 7: Scheme of the generation of program structure

Just as control flow analysis deals with uncovering the flow of control in a given program, the data analysis deals with the definition-usage of variables in programs and tries to locate the improper use of variables. The two types of anomalous situations dealt with by data flow analysis are the use of uninitialized variables and unused definitions of variables.

Certain "gross" data flow anomalies can be discovered simply by the variable cross-reference for the program under consideration. If the cross-reference shows only references but no definitions to a variable, then this is unmistakably a case of the use of an uninitialised variable. Similarly unused definitions can be detected, this approach, however, is not always adequate. If for example cross-reference shows some definitions and some references for a variable, it is not clear whether each reference is preceded by a definitions. It is then necessary to take into account various paths in the program and arrange that irrespective of the path taken through the program a definition always precedes any reference to a given variable. Such an analysis is done by Reaching Definitions Analysis.

The Reaching Definitions Analysis is carried out for each procedure or routine in the given program. The method combines information about variable references and definitions obtained from cross-reference with control flow graphs of routines obtained during structural analysis. The approach used by STAN is an iterative one, which works on the unreduced control flow graph of a routine as against some methods requiring graph reductions and special node orderings. For a more detailed descriptions of the data flow analysis of STAN see [15].

#### 4.2.2 QUALIFICATION OF REAL-TIME SYSTEMS

A specific problem within the qualification of software is the demonstration of the behaviour of parallel processes using common resources and the behavior of interrupt driven software. For the modelling, simulation and analysis of such systems, Petri-Nets have been chosen by GRS, which combine mathematical strength with a simple and evident graphical representation. The analysis of real-time behaviour can be performed by interactive stepwise simulation of the system states or by automatically controlled simulation [16]. At the time being these techniques are combined with algebraic specification techniques, i.e. the declarative definitions of algebraic specification are transformed into a dynamically representable net form [17].

#### REFERENCES

- [1] Prock, J.: Sensor Fault Detection in Dynamical Systems. Proc. IAEA-specialists' meeting on early failure detection and diagnosis in nuclear power plants, June 20.-22. 1989, Dresden, Germany
- [2] Prock, J.: A New Technique for Fault Detection Using Petri Nets. Automatica 27 (3) 1991
- [3] Prock, J., Ohlmer, E., Labeit, M.: On-line Test of Signal Validation Software on the LOBI-MOD2 Facility in Ispra, Italy. Nucl. Technology, subm. for publ.

- [4] Felkel, L., Schüller, H., Eisgruber, H., Hoffmann, H.: Application of an Advanced Software Concept for Operator Aids in Nuclear Power Plants, Computer Applications for Nuclear Power Plant Operation and Control, ANS International Topical Meeting, Pasco, Washington, USA, Sept. 8-12 (1985)
- [5] Bastl, W., Hoffmann, H.: Fortschritte in der Entwicklung eines rechnergestützten Informationssystem (RIS) für den Betrieb von Kernkraftwerken, Kerntechnik 50 (1987), No. 2, Carl Hanser Verlag München 1987
- [6] Kraft, M., Wöhrle, G., Pigler, F.: An Advanced Alarm and Status Management System for the 1300 MW Philippsburg Nuclear Power Plant, Unit 2, Computer Applications for Nuclear Power Plant Operation and Control, ANS International Topical Meeting; Pasco, Washington, USA, Sept. 8-12 (1985)
- [7] Bastl, W.: Integrated Disturbance Analysis (IDA), a Basis for Expert Systems in Nuclear Power Plants, Artificial Intelligence and other Innovative Computer Applications in the Nuclear Industry, ANS Topical Meeting, Snowbird, USA, Aug. 8 - Sept. 2 (1987)
- [8] Schütte, A., Sommer, D., Weingarten, J., Wach, D.: Utility Experience in Reactor Noise Analysis in German LWR's, SMORN V, Munich 1987, Progress of Nuclear Energy Vol. 21, Pergamon Press (1988)
- [9] Olma, B.J., Schütz, B.: Advanced Burst Processing Methods in Loose Parts Monitoring, SMORN V, Munich 1987, Progress of Nuclear Energy, Vol. 21, Pergamon Press (1988)
- [10] Rösler, H.: Ein System zur Online-Fernübertragung von Signalen eines Schwingungsüberwachungssystems (Remotely Controlled Online-System for Data Transmission of Vibration and Noise Signals), GRS-Report No. GRS-A-1391 (1987)
- [11] Sunder, R., Van Niekerk, F.: COMOS - an Online System for Problem-Orientated Vibration Monitoring, SMORN V, Munich, Progress of Nuclear Energy Vol. 21, Pergamon Press (1988)

- [12] Brummer J., Goßner S., Hoffmann, W., Kersken, M.: Bewertungsmethoden für die Qualifizierung neuer Sicherheitsleittechnik, GRS-A-1516, Januar 1989
  
- [13] Kersken, M., Rietzsch, L., Mertens, U.: Qualification of a computer system for the limitation of power density in a reactor core, Proc. COMPSAC 84, Chicago, Nov. 7-9, 1984, IEEE Computer Society
  
- [14] Dahll, G. et al: Tools for standardised software safety assessment, Report of the OECD Halden Reactor Project HWR-211 (May 1987)
  
- [15] Maertz, J., Dhodapkar, S.D.: Data flow analysis of common assembly language programs by means of static analysis tool STAN, Hardware and software for real time process control, North Holland, 1989
  
- [16] Brummer, J.: A graphical simulator for P/T-Nets, EHPG-Meeting, Bolkesjö, Norway, Febr. 1990
  
- [17] Brummer, J.: Representation and verification of discrete-event systems by means of Petri-Nets, Proc. 3rd Int. Workshop Software Engineering & its applications, Toulouse, France, Dec. 1990

## THE BALANCE BETWEEN AUTOMATION AND HUMAN ACTIONS: THE SIZEWELL B PERSPECTIVE

D.B. BOETTCHER  
Nuclear Electric plc,  
Knutsford, Cheshire,  
United Kingdom

### Abstract

Sizewell B is the first of a family of four similar 1100 MWe Pressurised Water Reactor Power Stations planned by the CEGB for sites around England. The civil and mechanical design of these power stations follows closely that of the Westinghouse/Bechtel designed Standardised Nuclear Unit Power Plant Stations (SNUPPS) units at Wolf Creek and Callaway in the United States, with changes where necessary to meet CEGB requirements or to comply with British licensing requirements. The electrical and C&I systems are, however, very different in detail from those of a typical US PWR power station. The functional specifications of the electrical and C&I systems are based upon those of the SNUPPS units but the designs of the systems have evolved under a number of influences including previous CEGB practice, unique British licensing requirements and the opportunities offered by modern systems using microprocessor technology.

This paper presents a personal view of the possibilities and limitations of automation and human actions based on experience of the specification and design process. It also discusses the approach to automation which has been adopted for Sizewell B and the small family of PWR stations that is to follow it, briefly touches on the PWR teams current philosophy for accident management and the possible future development of advanced C&I systems for accident management and operator information.

### POSSIBILITIES AND LIMITATIONS OF AUTOMATION

#### Definitions

*Automation:* What do we mean by automation? The interpretation which comes immediately to mind is the automatic control of some process variable such as level in a vessel or temperature of a process. For the purposes of this paper I would like to use a wider definition of automation as follows;

"Automation is the allocation of a control function to a machine rather than to a human operator."

Such a definition includes not only the sense and command features of a reactor protection system or automatic control system, but also features such as interlocks which place limits on the scope of possible actions by a human operator, relieving the operator of the burden of observing these limits himself. I propose to use this definition for the purposes of this paper because I think it helps to keep in mind that there are many constraints on the scope of possible human actions in a modern nuclear power station.

Fault/Accident: Throughout this paper I will use the term "fault" to mean an event which challenges nuclear safety, might require the operation of the safety system and is included in the design basis of the plant. I will use the term "accident" to mean a fault which has escalated to the point of major fuel damage or some other severe consequence and hence whose frequency is kept so low as to be considered incredible.

#### Reasons for automating

Before starting to ask the question of "How much automation?", one must ask the question "Why automate at all?". There are two fundamental reasons for providing a minimum level of automation;

- 1) The speed, accuracy or reliability of a required action or response is outside the capability of a human operator. It would therefore be physically impossible for a human operator to perform the task. This not only includes consideration of whether the operator can respond to an event sufficiently quickly, or can control a process variable to the required degree of accuracy, but also includes consideration of whether the task is tedious or repetitive and a human operator would suffer from boredom, loss of concentration or de-motivation if required to perform the task for a significant period.
- 2) A reduction in the number of operators required to operate a station can be achieved, or the total workload may exceed the capability of the available operators, even if the individual tasks are within their capabilities. The first of these two may be the most important from the point of view of the utility, because it reduces operating costs, but the second is the more important when safety is considered.

#### Factors to be taken into consideration

In deciding how to strike a balance between automation and human actions in Nuclear Power Plant Operations, the following factors must be taken into consideration;

- 1) The capabilities of human operators and machines.

The differing abilities of humans and machines are often characterised by designers in terms of differences in reliability. Designers tend to perceive machines as being highly reliable in carrying out the actions they have planned for them, and their performance as not being prone to degradation under conditions which would affect a human operator by placing him under mental or physical stress, whereas they are less inclined to place a high reliance on a human operator because they have little control over his thoughts and actions.

The human operator has, however, a higher degree of functionality than even the most complex of today's machines. The difficulty of designing a complex machine with a high degree of functionality as well as a high reliability is recognised by designers, and the designs of systems important to safety are deliberately kept simple in order that their reliability and performance can be assured. Human operators are sometimes thought of as having a low reliability compared to machines and to be prone to making errors in following procedures or when carrying out control actions. However, given time, conducive conditions in which to think and correct information, a human operator can understand complex circumstances and produce the correct control action or response.

- 2) The ability of the designers to foresee all the possible circumstances.

It should always be borne in mind that the designers of a power plant cannot foresee all of the events or circumstances which might befall the plant. This is recognised to some extent by the concept of the "design basis", or range of events considered when designing automatic safety systems or specifying post fault monitoring instrumentation.

The accidents of greatest consequence which have occurred in the nuclear industry to date have been "beyond design basis", that is faults which the designers did not consider credible. Characteristic of such accidents has been that, although the safety systems performed pretty well as intended, actions by the operators prevented the safety systems from achieving their objectives. Largely due to these accidents, the design bases of modern power plants now include recognition of human factors, and there is a tendency to more automation and the removal of the ability of the operators to defeat the actions of the safety system.

The designers of a nuclear power plant must be careful that in their desire to prevent the operator from causing or worsening an fault, they do not preclude him from taking actions which might recover a situation they have not foreseen. An operator who is well trained and knowledgeable can react to the behavior of a plant in a way that the designer, no matter how much he has drawn on previous experience when designing the plant, cannot. Interlocks and automatic overrides of operator actions should prevent the operators from placing the plant into a less safe state following a fault, but should not stop the operator from initiating safety actions or from performing manual control actions to place the plant in a safer state.

#### APPROACH ADOPTED FOR BRITISH PWR FAMILY

The approach adopted by the CEGB for the Sizewell B Power station and the PWR stations which are to follow is as follows;

- 1) Automate the protection of limits important to safety.

Because of the importance to safety of not allowing certain limits to be exceeded, the protection of these limits is always allocated to automatic safety systems. These automatic safety systems are deliberately kept simple in functionality, being as far as possible simple trip detectors and logic processors, and are subject to the highest degree of quality assurance and scrutiny by designers and the regulatory authorities. The automatic safety systems employ techniques such as redundancy and diversity to achieve a very high degree of reliability.

Safety limits are placed on plant conditions such as reactor power, temperature, pressure etc under all operating conditions. On reaching these limits the reactor is shutdown and safeguards plant is initiated as necessitated by the plant conditions. Simple operator actions to initiate or control safeguards equipment are expected some time after the trip, or for slowly developing faults, but such actions are on a timescale of many minutes or hours and are supported by clear information presentation. A design rule is that for design basis faults, operator actions from within the control room are not required within thirty minutes of a reactor trip or alarm, and that actions outside the control room are not required for at least one hour. After these periods the operator may be expected to take some actions but these must be within his capability and he must be provided with the necessary information.

Operator involvement is required to apply vetoes to safety system actuations when a mode change is desired eg from shutdown power levels to operational power levels, or from pressurised operation when the emergency core cooling system is armed to shutdown operation when the cold overpressure prevention system is armed. The number of such operator interventions are minimised and the successful application of the veto depends on the presence of a permissive signal in addition to the operator's request. The permissive signal indicates that plant conditions are in the correct range before the veto is allowed, for example; when the reactor is at a low temperature the residual heat removal system must be in operation and it is then permissible to veto the initiation of auxiliary feed, which would otherwise occur on low steam generator level, to allow a steam generator to be drained down for inspection. Moving out of the permissible range causes the veto to be automatically removed.

The operator can initiate reactor trip or actuate a safeguards system, but in general he cannot override the operation of the safety system from the control room while the plant conditions requiring the action persist. For example, if the reactor is hot and pressurised and the level in the steam generators is low, the safety system will continue to send a signal to the auxiliary feed system requesting it to start. This signal from the safety system will override a manual stop signal issued from the control room. Only when the level in the steam generators exceeds the low level setpoint will the signal from the protection system terminate and manual signals from the control room have effect.

2) Automate those functions which are automated on existing PWR plants.

One of the principal reasons for choosing a PWR reactor for the next generation of British nuclear power stations was to take advantage of the vast experience of worldwide experience in constructing and operating this type of plant. In order to incorporate this experience the CEGB have incorporated as much as possible of the functional design of the control systems of the reference SNUPPS plants into the design of Sizewell B, only making modifications in an evolutionary and carefully considered manner. The majority of the automatic control for normal operation of the plant; scheduled pressuriser level against average coolant temperature, scheduled reactor temperature against power, feed flow responding to changes in steam flow and steam generator level, etc, are therefore similar to those found on the typical US PWR plant.

Because the importance of these control actions to safety is less than the actions of the safety system, and because the control algorithms do not cover all of the desired operating modes of the plant, the operator is allowed to take manual control of the components normally controlled by these systems.

3) Automate operations outside the capability of human operators.

Actions requiring a degree of control which human operators cannot achieve, or have in practice had difficulty in achieving, are automated. A number of modifications and extensions to the Sizewell B control systems have been made for this reason. Principal among these changes are;

- 1) Developments in the automatic control of feed flow in response to steam generator level when at low power during startup.
- 2) Automatic control of the turbine bypass system to achieve a steady rate of cooldown from hot to conditions where the residual heat removal system can be used.

- 3) Automatic control of pressuriser pressure in response to reactor temperature during heatup and cooldown operations.

These extensions to the scope of the control systems compared to those of the SNUPPS reference plants have come about due to a variety of reasons such as; recommendations from CEEGB staff who have operated PWR stations in other countries, analysis of experience feedback and task analysis. However, all of the changes affect control functions which human operators on current stations have sometimes had difficulty in performing, as evidenced by experience feedback reports, indicating that they may be working at the limits of their capabilities.

#### Limits on extent of automation

It is often noted that once the operator is taken out of the control loop, his understanding or mental picture of the plant is not maintained so well as when he is required to participate. This type of consideration has not resulted in a reduction in the amount of automation to be provided for Sizewell B. However, the extent of automation on Sizewell B over and above that of SNUPPS has been restricted to a minimum amount which can be shown to be within the capability of existing technology to deliver, and to be worthwhile on the basis of experience in the industry. The temptation to automate to the maximum extent possible, and hence to minimise the involvement of the operator in the control of the plant, has been resisted. In addition, to help the operator in maintaining his understanding of the plant, comprehensive information is provided in the main control room in a clear and readily assimilable form via mimics of the plant on both hard panels and computer based displays.

Automation does not extend to mode changes associated with routine operations such as startup from cold shutdown or shutdown from power operation to refuelling shutdown, because these operations are carried out infrequently and additional staff can be brought in to provide assistance. Providing that the operations are within the capability of a human operator, the need for automation of such relatively infrequent events becomes a purely commercial question. The cost/benefit ratio is against providing automation for such operations because they are relatively infrequent and the potential manpower savings are small.

#### ACCIDENT MANAGEMENT

The design basis of the Sizewell B power station is that the automatic safety systems will detect the occurrence of faults and either terminate the fault via an interlock or will automatically shut the reactor down and initiate safeguards plant as necessary to place the plant into a safe shutdown state. The operators will then take the actions necessary to secure the plant in a long term safe shutdown condition. There is no requirement for short term operator intervention and interlocks will prevent operator errors from placing the plant into an unrecoverable state when intervention is required. The design of the automatic safety systems is such that the operators are able to initiate actions to place the plant into a safer state, but that they are positively prevented from reducing safety margins to an unacceptable degree.

Although the possibility of a severe accident at Sizewell B is regarded as so low as to be incredible, the operations of the automatic systems would not prevent the operators from carrying out actions to mitigate such an event. In addition, because of the length of time before an accident might challenge the integrity of the containment, there is the possibility of operator actions at

the plant or switchgear if for some unforeseen reason he must defeat an automatic action.

The response of the operators to plant conditions following a fault is dictated by written procedures. There is a single procedure to be used immediately after a reactor trip occurs which then directs the operators to confirm that the reactor is shutdown and that safeguards plant has started, assists diagnosis of the fault type and then refers the operators into a separate procedure for the particular fault. To cater for the possibility that the operators may mis-diagnose the fault or through some other circumstance find themselves unable to follow the fault specific procedure, a procedure based upon the concept of the maintenance of critical safety functions is available. This procedure guides the operator to take actions aimed at restoring or maintaining functions such as decay heat removal, reactor pressure vessel and containment integrity etc.

Although not written specifically for the purpose of addressing severe accidents, the concept of the maintenance of critical safety functions would be applicable under such circumstances. The PWR team have determined that in order to be effective, these critical safety function procedures should be as simple as possible and will be written rather than computer based. It is also a principle that the operators should base their actions on information which has not been subject to processing or interpretation by machines and that computer aid, although useful, will not be relied upon in situations calling for the use of these procedures.

On line simulators and expert systems.

The CEBB has investigated the possibility of on line simulation, and work is still continuing in this area. The PWR team have considered the possible uses of on line simulation for Sizewell B and have concluded that it is most promising in the area of performance optimization during normal operation, although further development in computer modeling codes and hardware need to take place before such a use becomes cost effective. The most promising future use of expert systems which is currently envisaged is in alarm handling and analysis, although the PWR team are not currently performing work on this topic.

It is not anticipated that expert systems or on line simulations will be able to make significant contributions to accident management in the near future. Part of the reason for this is that the codes and hardware need much development but a more significant reason is the difficulty in qualifying the hardware and software to the high levels of assurance needed before reliance could be placed on them during an accident. It is possible that on line simulators could have a role to play in aiding the experts in the technical support centre in understanding the course of an accident, and hence improve their ability to advise the control room operators, but for the foreseeable future it seems that the actions of the control room operators following a fault or accident should be based on simple and direct measurements of plant conditions and on the use of written procedures.

## SUMMARY

The design of the Sizewell B plant and the small family of stations to follow it are based firmly on existing stations which have an established history of successful operation. Although the hardware to be used in the Electrical and C&I systems has been updated to take benefit from the latest developments in solid state and microprocessor electronics, the extent of automation is based

on that of the operating plants with logical extensions where experience has indicated that improvements are possible. The design basis of the safety systems includes considerations of human factors and includes interlocks and overrides to positively prevent the operators from placing the plant into an unsafe state. The use of expert systems and on line simulators to improve the performance of power plants is regarded as a real possibility for the near future. Operator actions following a fault are based upon simple direct indications of plant conditions and the management of beyond design basis accidents would be facilitated by written critical safety function procedures.

# DEVELOPMENT OF AN AUTONOMOUS NUCLEAR POWER PLANT UNDER THE NUCLEAR FRONTIER RESEARCH POLICY IN JAPAN

F. TANABE

Tokai Research Establishment,  
Japan Atomic Energy Research Institute,  
Tokai-mura, Naka-gun, Ibaraki-ken,  
Japan

## Abstract

The artificial intelligence (AI) is a rapidly growing technology in line with innovative progress of computers and has reached to the stage of investigating methodologies for knowledge acquisition and/or learning in order to realize more sophisticated expert systems than presently achieved.

In mega-technology systems like nuclear power plants, it is important to increase the level of safety not only by focusing on equipments and/or facilities but also by highlighting human behaviour and man-machine interface, i.e. human factors. It is, therefore, expected that more reliable operation, diagnosis, maintenance, repair, etc. can be achieved through the development of AI technologies which are rigorously applicable to nuclear power plants. The ultimate goal in this direction is the development of an autonomous nuclear power plant.

Two steps have been set forth towards the goal. The objective for a medium term is set for realizing a plant that will be provided with a system to support persons in operation and maintenance. The objective for a long term should be aimed at an autonomous type plant that will self judge, self correct and self control.

The paper describes briefly the "Programme of Artificial Intelligence Technology Development for Nuclear Energy Use" and an autonomous nuclear power plan, which was developed by five governmental research organizations.

## 1) Overview

### a. Policy on Nuclear Underlying Technology

The Atomic Energy Commission of Japan renewed in 1986 "The Long Term Program for The Development and Utilization of Nuclear Energy" in which highlighted were the establishment of nuclear power as core energy, nurturing basic and creative science developments and contribution to international co-operation.

With regard to the nurturing of creative science, the Program pointed to the need to move from the past pattern of "catching-up" with technologies of advanced countries to "creative". The Program further pointed to the need for effective promotion of innovative projects and building up of basic research with promotion of underlying technology which may bridge them and bring a breakthrough in the current nuclear

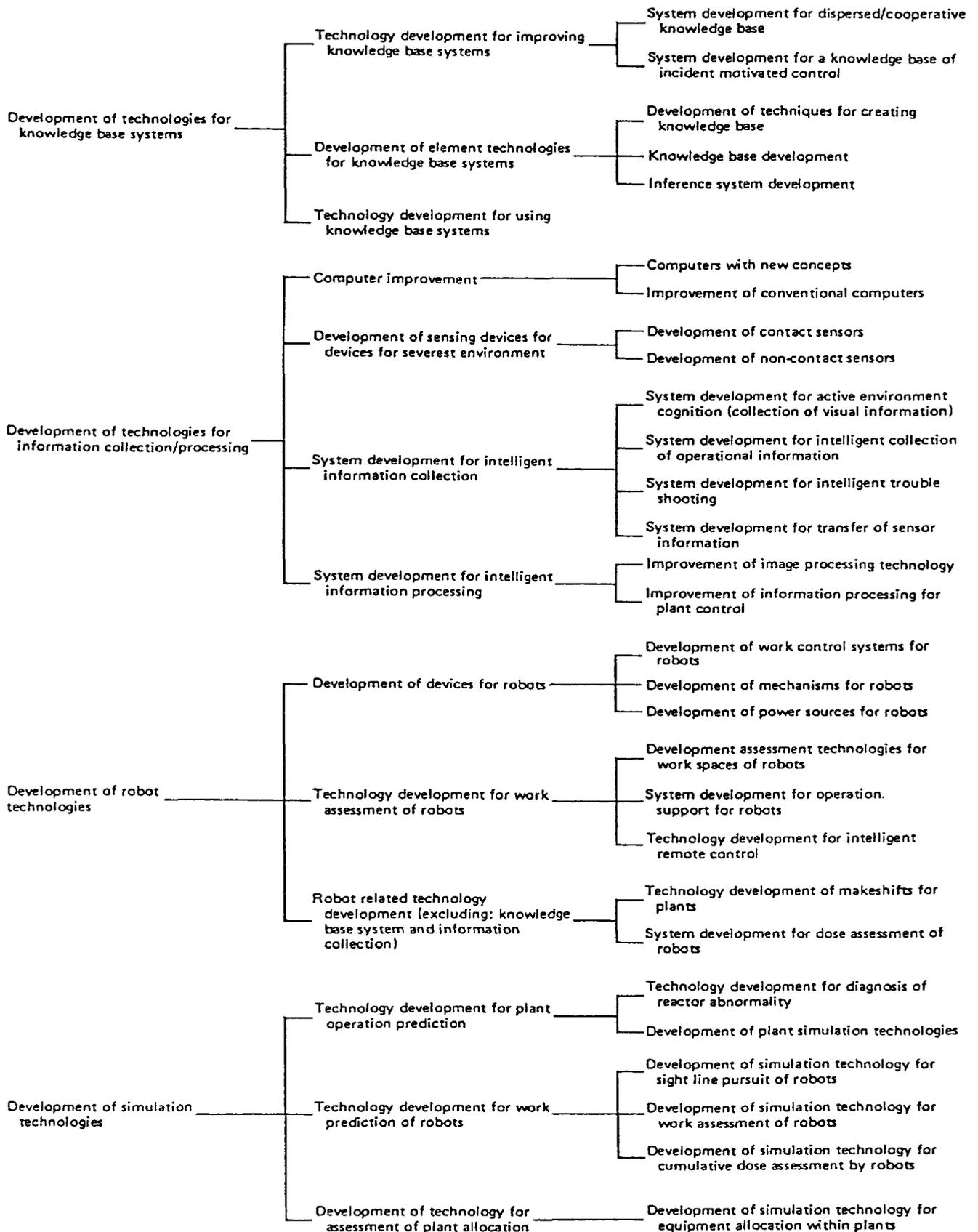


FIG. 1. Artificial intelligence technologies for nuclear energy development.

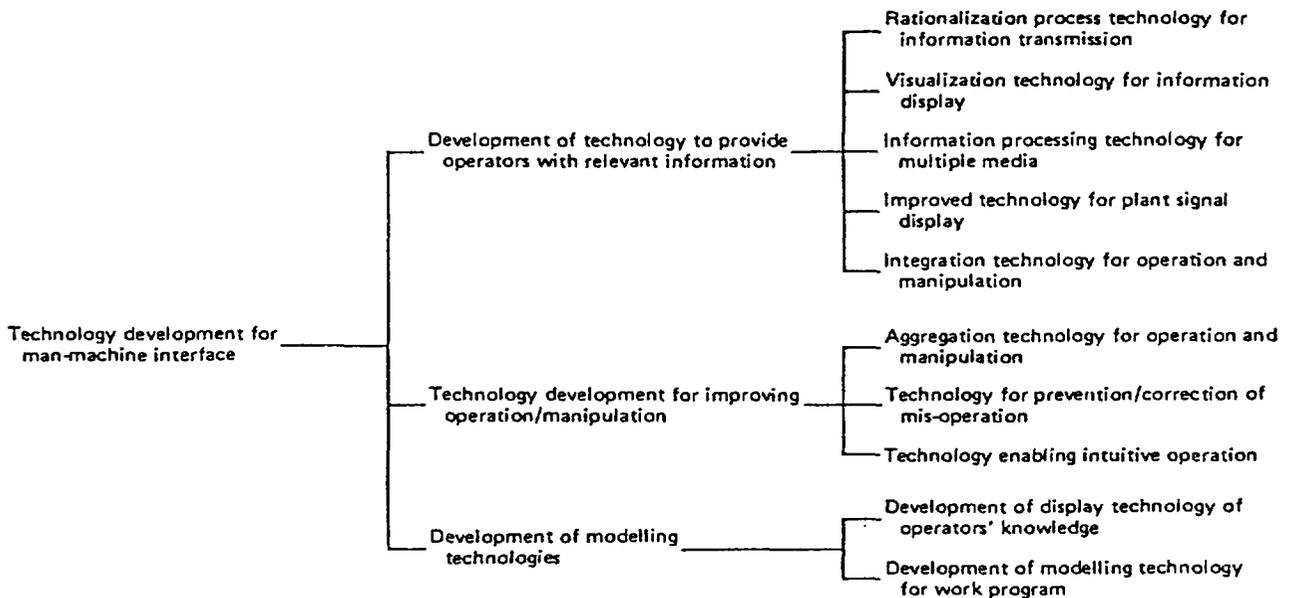


FIG. 1. (cont.)

technology. In this respect the Commission further adopted in 1987 "The Policy on Nuclear Underlying Technology Development" which includes "The Program of Artificial Intelligence Technology Development for Nuclear Energy Use".

#### b. AI and Autonomous Nuclear Power Plant

The artificial intelligence (AI) is a rapidly growing technology in line with innovative progress of computers and has reached to the stage of investigating methodologies for knowledge acquisition and/or learning in order to realise more sophisticated expert systems than presently achieved. Further the development of robotics is being strongly pushed forward, aiming at increasing reliability of systems as well as releasing humans from boring routine works. These technologies are expected to be applied in many scientific fields in a future, accepted as technologies which may improve man-machine interface problems in complex systems.

In mega-technology systems like nuclear power plants, it is important to increase the level of safety not only by focusing on equipments and/or facilities but also by highlighting human behavior and man-machine interface, i.e. human factors. It is, therefore, expected that more reliable operation, diagnosis, maintenance, repair, etc. can be achieved through the development of AI technologies which are rigorously applicable to nuclear power plants. The ultimate goal in this direction is the development of an autonomous nuclear power plant.

Two steps have been set forth towards the goal. The objective for a medium term is set for realising a plant that will be provided with a system to support persons in operation and maintenance. The objective for a long term should be aimed at an autonomous type plant that will self judge, self correct and self control. The basic element technologies needed to establish the nuclear AI has been identified. They are technologies for knowledge base system, information collection/processing, robot, simulation and man-machine interface. Research items relevant to each element technology are shown in Figure 1.

PNC (Power Reactor and Nuclear Fuel Development Corporation) :

- o R & D of AI for assistance in the operational management, control and diagnosis of nuclear plants

JAERI (Japan Atomic Energy Research Institute) :

- o Human acts simulation technology development

IPCR (Institute of Physical and Chemical Research) :

- o Application of robots to maintenance work

ETL (Electrotechnical Laboratory) :

- o Development of environment recognition technology

SRI (Ship Research Institute) :

- o Development of intelligence forms of man-machine interface for plant operation

FIG 2 Research institutes involved in projects

### c. Research Structure

Research projects to realise such advanced AI have been started accordingly in 1987 at five governmental research organizations under the initiative and coordination by Science and Technology Agency (STA). They are Power Development and Nuclear Fuels Corporation (PNC), Japan Atomic Energy Research Institute (JAERI), Institute of Physical and Chemical Research (IPCR), Electrotechnical Laboratory (ETL) and Ship Research Institute (SRI). Research projects have been established organization-wise, based on its own speciality and expertise, under which research items to enhance the basic element technologies are interrelated. The research projects undergoing at the organizations are shown in Figure 2.

## 2) Concepts of Autonomous Plant

The concepts of an autonomous plant have been given primarily by PNC who is taking the role of coordination of the participating organizations in this research.

### a. Levels of Autonomous Plant

An autonomous plant is classified into three levels;

- (1) Fully automated operation plant
- (2) Autonomous plant which is operated without man
- (3) Autonomous plant whose operation and maintenance is unmanned.

At the first level, the plant has the ability to monitor the fundamental functions of the plant. The movement of the plant depends on objective, aim and intention of its system and always recognizes whether it is under good or abnormal conditions. For this level of autonomy, the plant becomes fully automatic and decides which operation is adequate to bring the plant status to optimal condition according to a certain pre-defined standard, and it is necessary to recognize accurately the plant status even if it is an abnormal condition.

The second level is a more advanced autonomus system. The system has an ability of self-improvement and it can always shift to the most optimal status or it has an ability of a safe shutdown without fail in the case of any abnormal or emergency condition. Because the decision making by the system in this level is perfect, plant operation without man becomes possible.

The third level includes self-organization as a character, so the plant system repairs its faults by itself. The plant being unmanned includes maintenance and repair works.

#### b. Plant Outline

At the first level, the area of the central control room according to human requirements is decreased because the plant is fully automatic and the number of operator is reduced. In the case of an unknown event which can not be solved by the AI system of the plant, it is necessary that the plant has quite advanced man-machine interface devices with which operators can recognize properly the plant behavior and movements of the automatic machines within a short time because at that time the operation is the operator's responsibility.

For example large scale screen or voice input-output devices are installed at the central control room. But under normal conditions, the operation is not conducted by the human operators. The patrol by operators at the plant site several times per day becomes unnecessary in principle and intelligence sensors or devices for data acquisition and monitoring at certain points would be adequately installed instead. Only in the case of an anomaly at plant site which can not be handled by the AI, the operator will go to the plant site to check the anomalous status. The maintenance engineers repair damage of equipment. Although the automation of periodic inspections is advanced, men do the work in principle.

Because the operation is unmanned at the second level, the central control room will be unnecessary. A communication device is installed at an office by which the plant manager knows the plant summary. At an abnormal plant state the plant is automatically recovered by the judgement of AI or it changes smoothly to stable shutdown status by safety system. The intelligence sensors conduct equivalent works conducted by human patrols at site and therefore human monitoring becomes unnecessary. The repair and periodic inspection works are the same as of the first level.

The operation of the third level is the same as that of second level which is unmanned. Repair works are conducted by

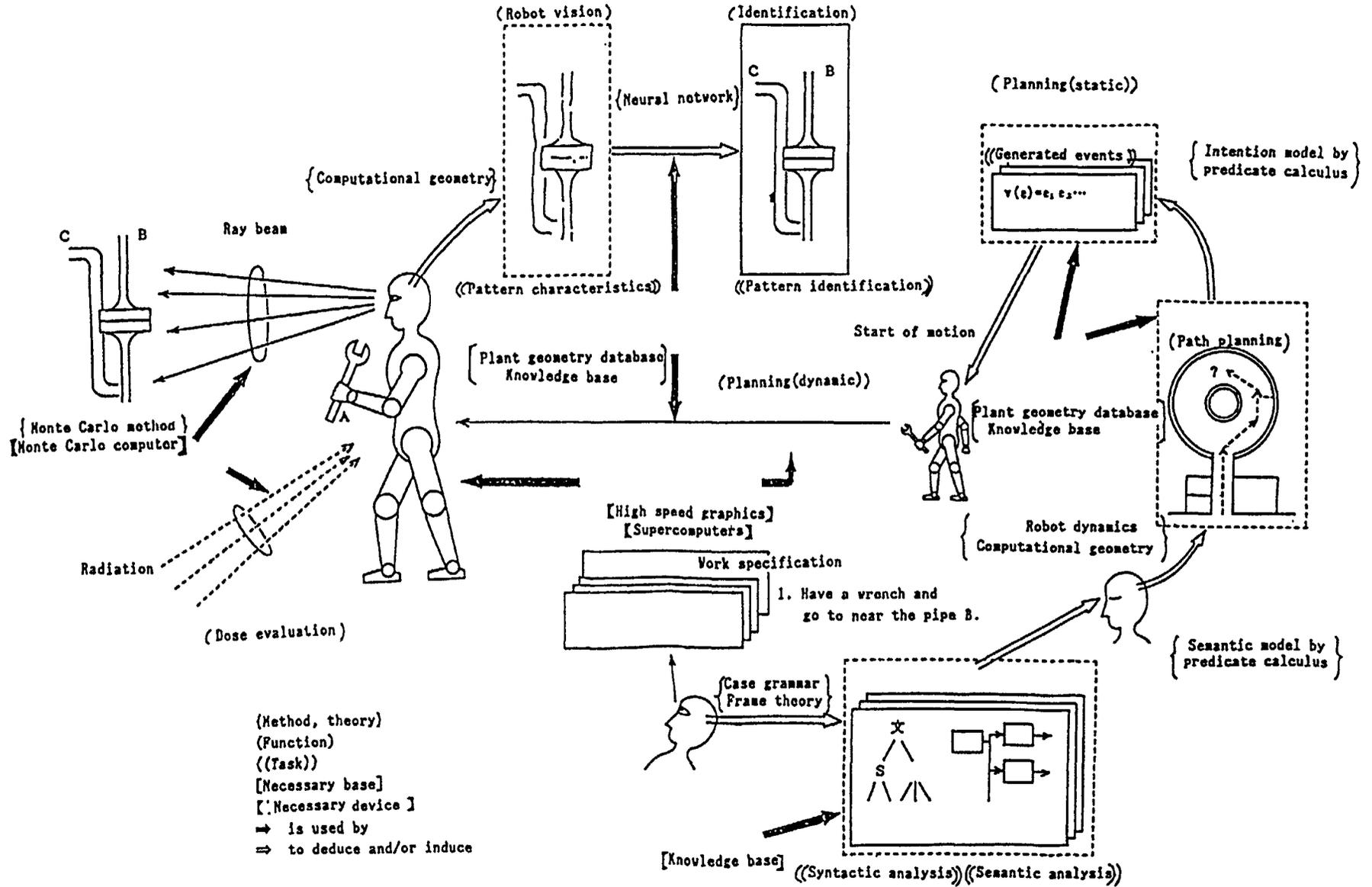


FIG. 3. Concept of the human acts simulation program (HASP).

robots not by men. Also in-service inspection and periodic inspection include the overhaul of plant equipment which are not conducted by men.

### c. Role Allocation of Human and Machinery System

#### Level one:

Because the AI system of the plant monitors the plant status and judges the movement according to a standard, the patrol or monitoring work generally conducted by operators or maintenance engineers at the present time becomes unnecessary. Because at this level the AI is not developed so as to manage all the plant status, it is necessary for manual decision making and operation for events which are not included in the operational manuals. For this aim, advanced man-machine interface is necessary. And the plant operators are unnecessary at the time of normal conditions, because operations such as plant start-up, shut-down and power adjustment and fundamental patrol at site are conducted by machinery systems. But at the time of abnormal conditions the operators are required to adequately manage the situation, and hence education and man-power development of the operators involve many difficulties.

So sufficient education and training systems such as simulators, facility or computer assisted instruction systems should be installed.

#### Level two:

For this level it is not necessary that operators always stay at the plant, because the machinery system brings the plant to the safety stop and cold stand-by even if an abnormal event occurs. At the stable stop state the repair work is conducted by the off-site maintenance engineers who are dispatched.

#### Level three:

In principle it is not necessary that man always be stationed at the plant because all works including repairs are conducted by machinery systems.

### 3) Example of On-going Research Project

#### a. Human Acts Simulation Program (HASP)

The human acts simulation program (HASP) aims at simulations of human acts by computer under a routine and/or an emergent situation in nuclear facilities. The HASP has started as a ten year program at JAERI since 1987. It has three purposes;

- (1) Developments of the basic technology for intelligent robots
- (2) Developments of the technology for an intelligent and automatic nuclear power plant
- (3) Spreads of the attained AI techniques to nuclear researchers.

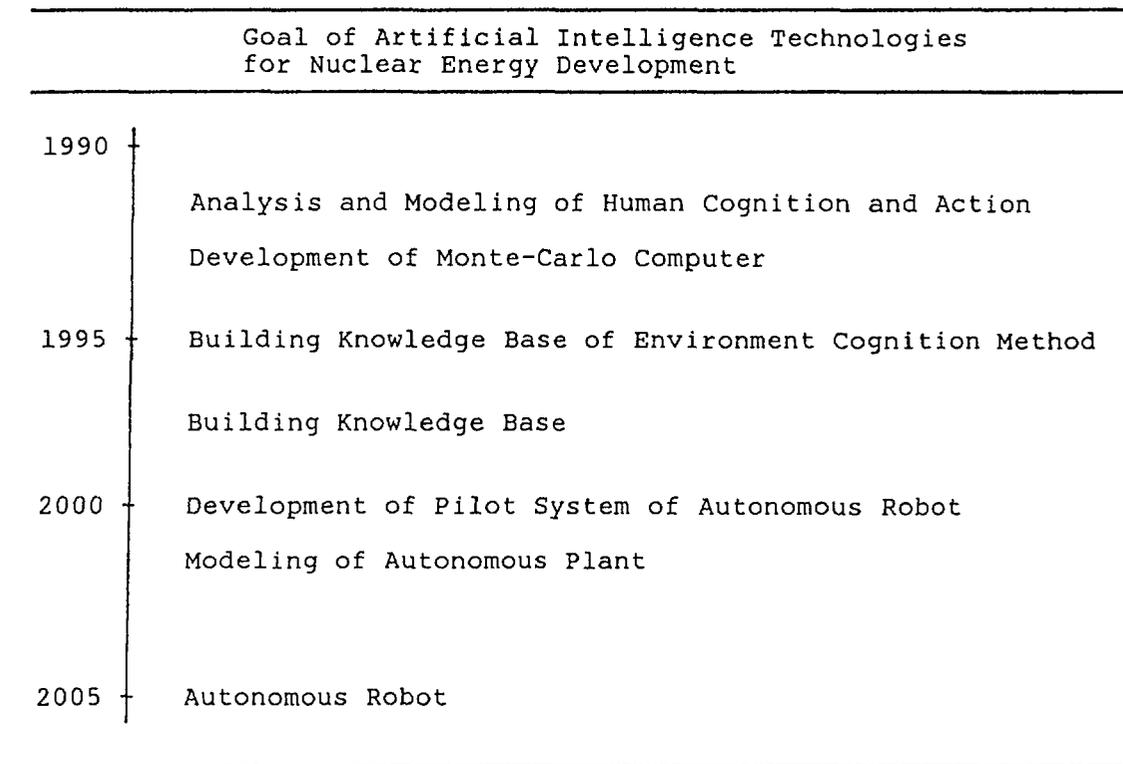


FIG. 4. Long and medium term development schedule.

In the HASP, the knowledge base system, plant geometry database, scene identification, robot vision, robot dynamics, Monte-Carlo methods, action planning and dynamic dose evaluation are being studied. The concept of HASP is shown in Figure 3.

#### 4) Development Schedule

The development schedule has been figured only for a medium term at present. The end of term is 2005, and key techniques which form a major part of the autonomous plant will be developed by that time. The schedule is roughly shown in Figure 4.

# THE BALANCE BETWEEN AUTOMATION AND HUMAN ACTIONS IN JAPANESE NUCLEAR POWER PLANTS: CURRENT STATUS AND FUTURE PROSPECTS

K. NAKAMURA

Agency of Natural Resources and Energy,  
Ministry of International Trade and Industry

S. HIEI

Institute of Human Factors,  
Nuclear Power Engineering Test Center

Tokyo, Japan

## Abstract

Basic concept of automation is generally understood to define, in the sense of the roles of man and machine, a substitution of automatic operation for manual handling of sequential process of facilities. This proposition is the common relating to the so-called huge system with such technological innovations as automatic control, information processing and computerized data processing.

Recently, there is a growing importance for the automation to further enhance safety and reliability of nuclear power plants.

The paper describes the current status and future prospects on balance between automation and human actions in Japanese nuclear power plants.

## 1. CURRENT STATUS OF INCIDENTS/FAILURES INCLUDING HUMAN ERRORS, CAPACITY FACTOR, AND EXPOSURE REDUCTION

### (1) INCIDENTS/FAILURES INCLUDING HUMAN ERRORS

Figure 1 shows the trend of incidents and failures in Japanese nuclear power plants after 1969, when light water reactor started its commercial operation, up to 1987.

During this 18 years period, the number of nuclear power plants have been increased by 34 units while the rate of occurrence of incidents and failures, as shown in black dots, tends to decrease after the peak of 4 cases per reactor year in 1971 and is stabilized at the level of 0.6 cases per reactor year after 1984.

This was contributed to the efforts of the government, electrical utilities and manufacturers, who stressed on the fulfillment of countermeasures to prevent recurrence of the incidents and failures, improvement of reliability of systems and components, and grading up of the operational administration of the nuclear power plants. Rate of occurrence of incidents and failures due to human errors is shown in circle. This has the general tendency of the same level while rate of occurrence of total incidents and failures is steadily decreasing.

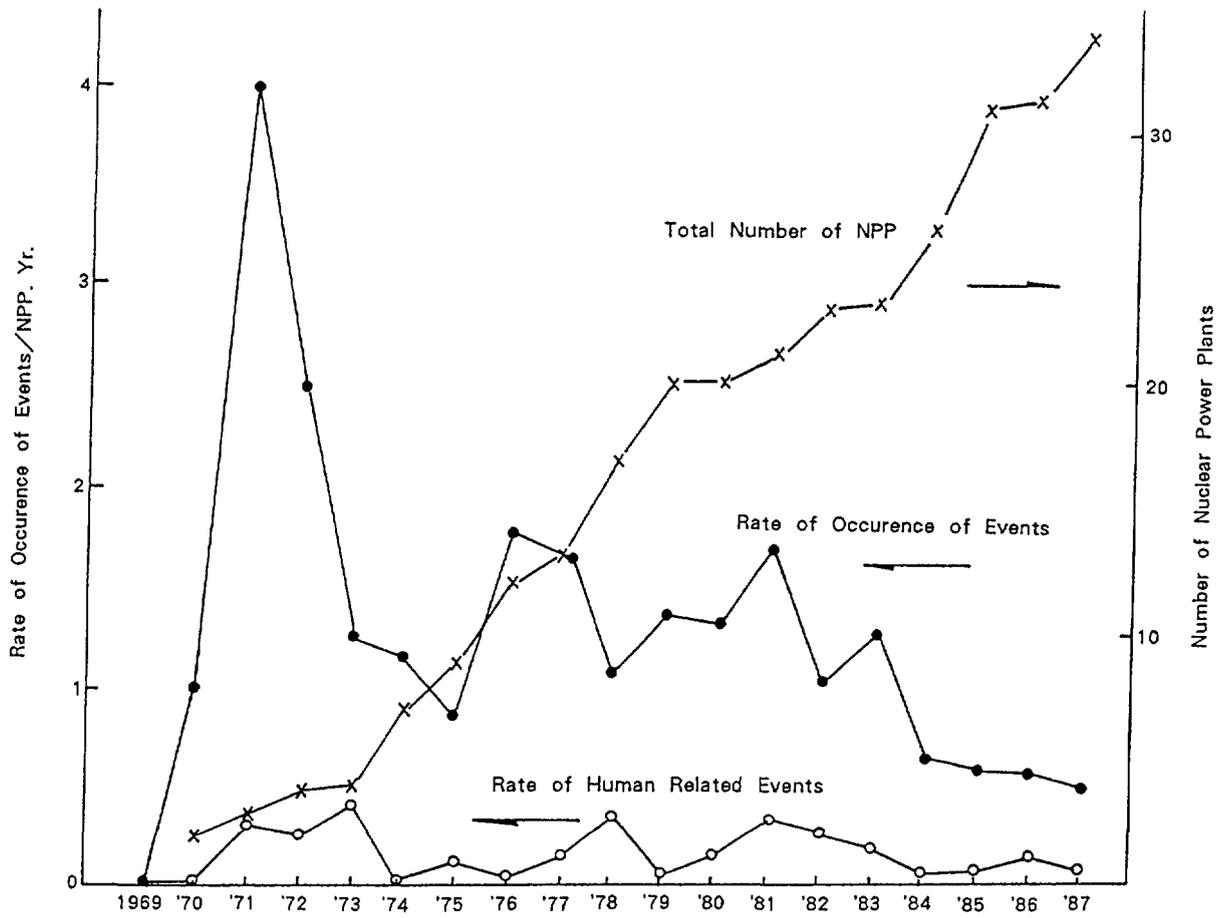


FIG. 1. Trend in NPP construction and rate of occurrence of events.

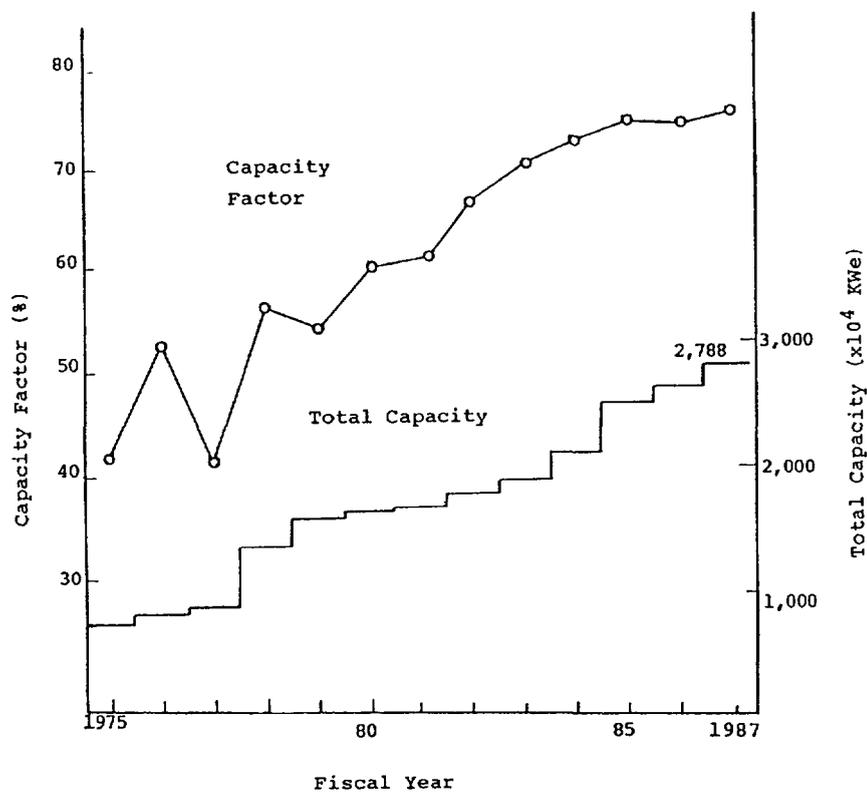


FIG. 2. Total capacity and capacity factor.

In reviewing effect of incidents and failures based on human error, of total of 41 cases of incidents and failures due to human error, 54% caused reactor shutdown and 15% caused power decreasing - resulting approximately 70% of human related incidents and failures effected plant output.

Considering this fact, it could be understood that the human error is an extremely important factor from the reliability respect of the nuclear power plant.

(2) CAPACITY FACTOR

The nuclear power generation ratio of 1987 marked 31.7%, the first time over 30% line. The nuclear power generation ratio has been steadily increasing since the first operation of a commercial reactor. The ratio was registered as 6.5% for 1975 and 17.2% for 1980 (Figure 2).

This improvement in nuclear power generation ratio is due to its increasing capacity factor of over all nuclear power plants.

As depicted in this figure, 1987 average capacity factor for 34 nuclear power plants marked the highest ever record of 79.4%. The capacity factor is the total power generated x 100, divided by the output, multiplied by the total calendar time (number of hours). This factor has steadily increased since 1982 when it was registered as over the 70% for the first time.

These increasing capacity factors are considered due to the close cooperation of both private and governmental efforts to enhance safety and reliability by reflecting resultant improvements from the operational experience in Japanese nuclear power plants.

(3) EXPOSURE OF EMPLOYEES

As shown on the figure 3, the total occupational exposure dose per reactor unit is tending to decline year by year since around the 1978 when the SCC problems came out.

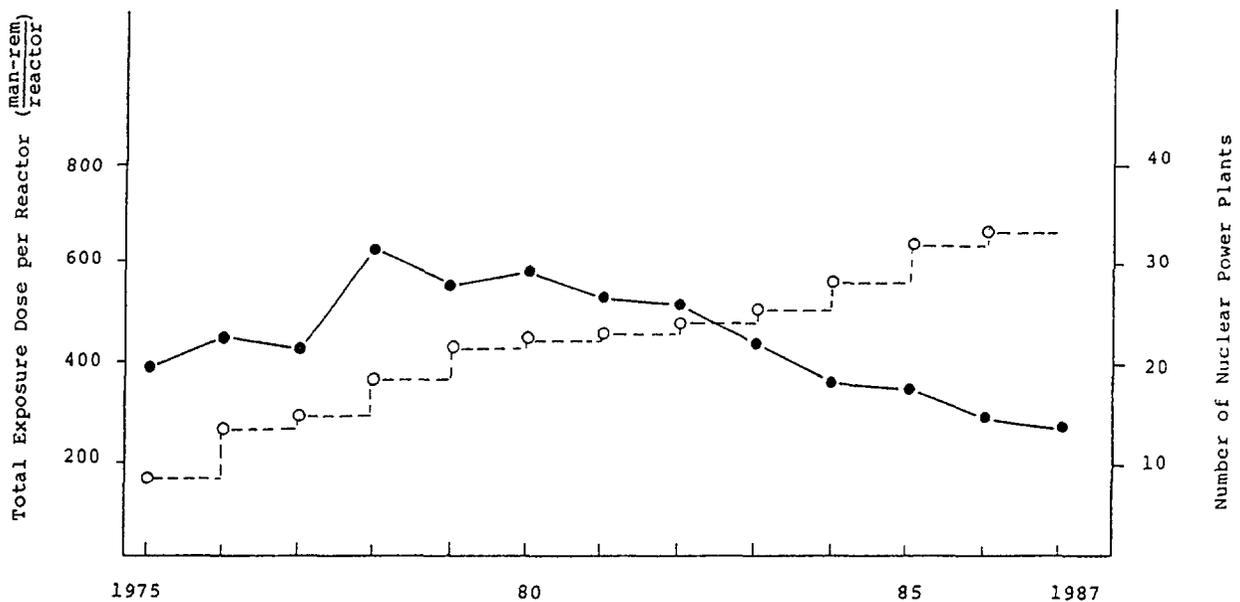


FIG. 3. Total exposure dose per reactor (man.rem/reactor).

The total occupational exposure dose per reactor stood at 270 man-rem for 1987.

For reducing exposure dose, the government and the electric utilities actively promote the development and application of automated equipments for periodical inspections. It is important for maintenance and inspection works to consider, on man-machine interfaces, the possibility of occurrence of human error due to the limitation of working conditions under radiation exposure in addition to the working circumstances of high temperature, humidity and limited space for the plant maintenance and inspection.

## 2. ENHANCEMENT OF SAFETY AND RELIABILITY - GOVERNMENTAL PROMOTION

### (1) LWR IMPROVEMENT AND STANDARDIZATION

LWR improvement and standardization program was initiated in fiscal 1975, with the aim of improving reliability and raising the availability level of LWRs, plus reduction of occupational radiation exposure. The first phase covered the years through fiscal 1977, and the second, fiscal 1978 to 1980. The results of the program are reflected in plants now operating, under construction, and in preparation. The third phase, which began in fiscal 1981, dealt with improvement and standardization over two generations: the improvement of existing LWRs and the development of advance LWRs (Table 1).

MITI now ended the program with completion of the third phase in fiscal 1985.

Those nuclear power plants in which the improvements and standardization program had been introduced have been producing the anticipated results in term of reduction of equipment/system incidents and

TABLE 1. LWR IMPROVEMENT AND STANDARDIZATION PROGRAM

		1st Phase (1975 to '77)	2nd Phase ( '78 to '80)	3rd Phase ( '81 to '85)
Main Expected Results	Improvement in Reliability and Capacity Factor	$\approx$ 70% (o Anti SCC Mtl) (o Improved S/G)	$\approx$ 75% (o Improved CRD) (o " Fuel)	① Development of Advanced LWRs * A-BWR o Internal PLR. Pumps o FM-CRD, etc * A-PWR o Large Reactor Core o New type S/G, etc.
	Shortening of Periodical Inspection Duration	$\approx$ 85 Days [o Conventional LWRs 90 to 100 Days o Enlarged PCV o Improved FHM]	$\approx$ 70 Days (o Aut. Replace Mech. for CRD) (o Improved Fuel Inspect. Syst.)	
	Reduction of Exposure Dose. [in comparison with conventional LWRs]	$\approx$ 75% [o Prevent/Removal Syst. of Clad o Auto. S/G Tube Inspect]	$\approx$ 50% [o Ext. of Auto ISI o Auto. of Water Analyzer]	② Improvement in Coventional LWRs ③ Standardization Program
Remarks (Typical Plants to be applied)		BWR : 2F-2 H-3 PWR : Sendai-1 Tsuruga-2	BWR:K-2/5 PWR:Genkai- 3/4	① K-6/7 A-BWR T/O 1996/97 ② To be applied to NPP designs later than '86

accidents, enhancement of instrument/control systems, shortening of periodical inspection duration, and exposure reduction. In turn, these improvements are supposed as main contributor to the afore-mentioned reduction of incidents/failures, increasing capacity factor consequently, and reduction of exposure.

(2) LWR SOPHISTICATION PROGRAM

(1) ENVIRONMENTAL CHANGES AROUND LWR

Today LWRs play a central role in the oil alternative energy options of this country as a result of the program. The growing importance of nuclear generation in the overall composition of the electric power sources, however, coupled with the delay in the commercialization of fast breeder reactors with the consequent extended LWR life, the need to utilize plutonium in LWRs induced by such reactor strategy in the fuel cycle, and the need for increased nuclear safety, reliability and economy have pointed to a new need in LWR technology development (Table 2).

a. INCREASING DEMAND FOR NUCLEAR POWER GENERATION

Resulting from the continuous and steady improvement and development in nuclear power plants of which the first commercial reactor started its operation in 1966 in Japan, the nuclear power generation marked 31.7% of the total power generation in 1988, and is considered as more increasing from view point of additional completion of nuclear power plants under construction.

TABLE 2. LWR SOPHISTICATION PROGRAM

	Existing LWRs (Results in FY 1984)	Sophistication of Existing LWRs	Development of A-LWRs	Development of AA-LWRs
Economic improvement	—	—	10% Reduction in kWh Cost from Existing LWRs	10% Reduction in kWh Cost from A-LWRs
Improvement of Availability Factor	75.3% [Continuous Operation Time: 11 Months, Periodical Inspection Time: 80 - 120 Days]	80 - 85% [15M 60D]	85 - 90% [Over 15M 50 - 60D]	90 - 95% [Over 18M 40 - 50D]
Saving of Uranium	—	—	10 - 20% from Existing LWRs	Over 10% from A-LWRs
Reduction of Exposure Dose	370 man-rem/reactor-year	2/3 of Current Average	50 - 100 man-rem/reactor-year	Less 50 man-rem/reactor-year
Reduction of LLW Products	1,600 drums/reactor-year	—	100 - 200 drums/reactor-year	Less 100 drums/reactor-year
Expansion of Candidate Site	Bedrock Limit to Feasible Siting Places	—	—	To Expand Feasible Siting Land by Siting on Quaternary Period Layer and Adoption of Earthquake Isolation Design of Plants
Max. Capacity	1,100 MW Class	1,100 MW Class	1,300 MW Class	1,500 - 1,800 MW

b. PROLONGED ROLE OF LWRs

The commercialization of FBR is not expected to be realized before 2010, considering the alleviation of uranium supply and the limitations of its economic feasibility, despite of the former Nuclear Power Development and Utilization Long Term Plan by the Atomic Energy Commission of Japan. The role of LWRs will be, therefore, prolonged to meet the main source of electric power supply.

c. DEVELOPMENT OF NUCLEAR FUEL CYCLE

The nuclear fuel cycle should be promoted cohering with the strategy of reactor type in the comprehensive consideration of the nuclear systems. In the anticipation of the prolonged role of LWRs, use of plutonium will be a future subject in LWRs.

d. FURTHER ENHANCEMENT OF SAFETY

Since the accident of Chernobyl No. 4 reactor on April, 1986, there is growing need for further enhancing safety and reliability of nuclear power plants.

e. IMPROVEMENT IN ECONOMY

Nuclear power generation is considered more economical because of the stability against the change of fuel cost which is comparatively smaller part of running cost than other alternatives. Although longer the operation, more advantage the generation cost of nuclear power, more improvement in its economy is expected taking consideration of its effect on the overall generation cost.

(2) MEASURES FOR ENVIRONMENTAL CHANGES

In order to steadily introduce/develop LWRs playing a central role in the oil alternative energy options, sophistication of LWRs should be promoted based on the following viewpoints corresponding to the environmental changes around LWRs.

a. ENHANCEMENT OF SAFETY AND RELIABILITY

- i) Sophistication of Design Concepts:
  - o Increased safety system
  - o Advanced siting techniques
  - o Earthquake isolation structures
  - o Demonstration of sophisticated aseismic technologies
- ii) Sophistication of Operational Control System:
  - o Development of man-machine system
- iii) Reduction of Exposure Doses
  - o Development of inspection-free materials

b. REQUEST TO PLAY A CENTRAL ROLE OF ELECTRICAL POWER SUPPLY

- o Shift of Electrical Supply Pattern from Base Load to Load Following
- o Development and Verification of Fuel for Load Following

c. MEASURES FOR NUCLEAR FUEL CYCLE

- i) Correspondence with Nuclear Fuel Cycle
  - o Quantitative and technological assessment and review on fuel fabrication, reprocessing and waste management
- ii) Promoting Use of Plutonium
  - o Promoting the plu-thermal, and assessment/and review of high conversion type LWRs

d. IMPROVEMENT IN ECONOMY

- i) Sophistication of Operating Reactors and Advanced Type Reactors
  - o Various demonstration tests
- ii) Extension of Operating Cycle
  - o Development and verification on high burn-up fuel

e. OTHERS INTERNATIONAL COOPERATION

- Study of suitable reactor type for developing countries
  - o Assessment and review of small and medium type LWRs

(2) PROMOTING ORGANIZATION AND SUBJECTS OF LWR SOPHISTICATION PROGRAM

MITI established, on April 1987, a "Committee on promotion of LWR sophistication" putting together the two existing committees: "Committee on Standardization of nuclear power equipment" and "Committee on improvement and standardization of nuclear power plants" which had reported to the director general of the Machinery and Information Industries Bureau, MITI, and the Director-General of the Agency of Natural Resources and Energy, MITI. The committee will undertake the overall assessment of public research, including that carried out by the Nuclear Power Engineering Test Center, and that done by such as the power companies' joint research, related to the sophistication and advancement of LWR technology, as well as recommend areas of research that require government support.

The new committee will report to the policy subcommittee on such matters relevant to policy decision making on sophistication.

3) FULFILLMENT OF SECURING COUNTERMEASURES FOR NUCLEAR POWER GENERATION SAFETY - NUCLEAR POWER SAFETY PROGRAM "SAFETY 21"

Promotion of securing safety operation for nuclear power plants in Japan has resulted in the high level of safety in nuclear power plants. All those engaged in the nuclear power generation should, however, continue to do their sincere efforts for increased safety to obtain a better understanding from people. We should not be self-conceited with our safety nuclear power operation for more than 20 years, but do learn lessons reviewing the causes of the Chernobyle accident, and reflect them appropriately into our own safety securing measures. This program is currently underway with both government and private industry firmly safety further, and setting up systems necessary for attaining these goals (Table 3).

TABLE 3. NUCLEAR POWER SAFETY PROGRAM 'SAFETY 21'

	BREAKDOWNS
1. FULFILMENT OF SAFETY REGULATIONS BY MITI	(1). Sophistication of Safety Regulations - o Exchange information etc. (2). Correspondence to New Fields ----- o FBR etc. (3). Measures for Increased Tasks
2. IMPROVEMENT IN UTILITY INDUSTRY'S SAFETY MAINTENANCE	(1). Elevation of Managerial Functions (2). Qualitative Improvement of Ope. & Mainte. Staff (3). Utilization of Ope. & Mainte. Information
3. PROMOTION OF R & D FOR INCREASING SAFETY	(1). R & D for Prevention of Human Errors --- o Human Factors Research o Operator Aid Syst, etc (2). Tech. Development for Prior Prevention - o Diagnosis & Evaluation of Accidents & Failures Syst. etc (3). Research on the Behavior of Nuclear Reactors
4. PREPARATION OF EMERGENCY PLANS	(1). Sophistication of Emergency Communication Network (2). Preparation of Emergency Operation Manuals (3). Development of Equipment for an Emergency
5. INTERNATIONAL COOPERATION	(1). Cooperation in an Accident (2). Information Exchange (3). Cooperation with Developing Countries

(1) FULFILLMENT OF SAFETY REGULATIONS BY MITI

a. Sophistication of Safety Regulations

MITI will improve technical standards by making maximum use of information and experience accumulated so far through licensing and inspecting activities, and endeavor to complete a cross-check system using safety analysis codes, as well as actively introducing the latest information. In addition, the Ministry will complete the licensing system for responsible operators of nuclear reactors. MITI is now preparing the system, and plans to implement it to cover qualifications, acquisition and intensified, renewal conditions of qualifications.

b. Corresponding to New Fields

"Corresponding to new fields" means intentionally improving technical standards to make them conform to such aspects as bringing advance power reactors into practical use and the decommissioning of reactors, and carrying the nuclear cycle into a business.

c. Measures for Increasing Tasks

MITI will utilize expert third party organizations to make use of private organizations in such formulated services as inspection among governmental regulatory activities for safety, because of the improved technical ability of the private sector.

## (2) IMPROVEMENT IN UTILITY INDUSTRY'S SAFETY MAINTENANCE

### a. Elevation of Managerial Functions

For elevation of managerial functions, the industry will reinforce the foundation of the managerial system for safety.

### b. Qualitative Improvement of Operators and Maintenance Staff

The industry will secure and train highly qualified operators and maintenance staff in accordance with the employment schedule as nuclear power plants are increasing.

The industry will also endeavor to transfer appropriate, to the next generation, its experiences and information accumulated in the beginning and trouble time of nuclear power plant utilization, since incidents and failures are decreasing in their number/frequency resulting from higher safety operation.

With regard to qualitative improvement of the staffs of subcontractors, the industry will also conduct their education and training.

### c. Utilization of Operation and Maintenance Information

The industry will systematically collect and arrange information on operation, maintenance and human errors, and make use of the information for prior prevention of accidents by analyzing and evaluating it.

## (3) PROMOTION OF R & D FOR INCREASING SAFETY

In order to further improve in safety, both governmental and private sectors will challenge the following subject introducing update information and new technologies.

### a. Research and Technical Development for Prevention of Human Errors

Research and technical development has taken place mainly in equipments or facilities ("hard") to secure safety, however, it is recognized important to research human interactions ("soft") in order to further improve in safety.

For research and technical development on prevention of human errors, the governmental and private sectors under shared charge, will carry out research on such "Human Factors" as human action and behavior in a normal and abnormal conditions, and the development of the "Operational Aid System" applying the optimization of the man-machine interface and the knowledge engineering.

### b. Technological Development for Prior Prevention of Accidents and Failures

In order to provide for prior prevention of accidents and failures, both the governmental and private sectors will develop the techniques for diagnosing and evaluating deterioration, and the machinery and equipment in which new materials have been used.

The technique of diagnosing and evaluating deterioration is to be developed, with the aim of grasping accurately soundness of the various machinery and equipments in conformity with the changes in plants resulting from many years of operation

c. Research on the Behavior of Nuclear Reactors

In research on the behavior of nuclear reactors, which offers basic information when the overall safety of nuclear power plants is grasped, a considerable amount of results has been accumulated. In order to further improve safety, the governmental and private sectors will continue to advance analytic research on the behavior of nuclear reactors on the assumption of a severe accident, and research into the behavior of nuclear reactors through the probabilistic risk analysis method.

(4) PREPARATION OF EMERGENCY PLANS

Measures to cope with an emergency will be prompted with preparation against the worst possible emergency as follows, although all possible measures have been taken for safety of nuclear power plants.

- a. Sophistication of Emergency Communication Network for Faster and More Accurate Communication among Central, Local Governments and the Industry.
- b. Preparation of Emergency Operation Manuals and Implementation of Education and Training for an Emergency.
- c. Technological Development of Equipment for an Emergency, such as Preventive Robots.

(5) PROMOTION OF INTERNATIONAL COOPERATION ON SAFETY

a. Cooperation in an Accident

In order to fulfill its international responsibility, the Japanese government will cooperate through IAEA and OECD-NEA, in establishing an international framework, such as the system for information exchanges and mutual assistance in any emergency arising from an accident.

b. Information Exchange

Both the governmental and private sectors will exchange information on operational experiences in nuclear power plants, and technical research and development for improvements to safety on a bilateral basis and/or multilateral basis.

c. Cooperation with Developing Countries

Developing countries are becoming increasingly keen for nuclear power generation and have great hopes for Japanese cooperation as a nuclear developed country. In order that Japan may cooperate with developing countries in safety assurance of nuclear power plant, the governmental and private sectors will increase the number of trainees received, and send talented persons according to each role to be shared.

(4) Accident Management against Severe Accident

Accident management here is narrowly defined as measures and/or actions taken by the nuclear power plant operators that could prevent accident development or significantly mitigate the consequences caused by accidents beyond the area of the design basis, i.e. severe accidents.

A severe accident can hardly be expected to occur in Japanese nuclear power plants, as sufficient countermeasures for securing safety are systematically implemented and maintained under the efforts by the utilities and the guidance of the government. Hence no reflection to the current regulation practices are foreseen at present against severe accidents.

It is, however, considered to be of further enhancement of safety to investigate in advance various countermeasures effective to cope with severe accidents including functions of the equipments which are not regarded in the evaluation of design basis, and to provide operators with such measures in the form of procedures.

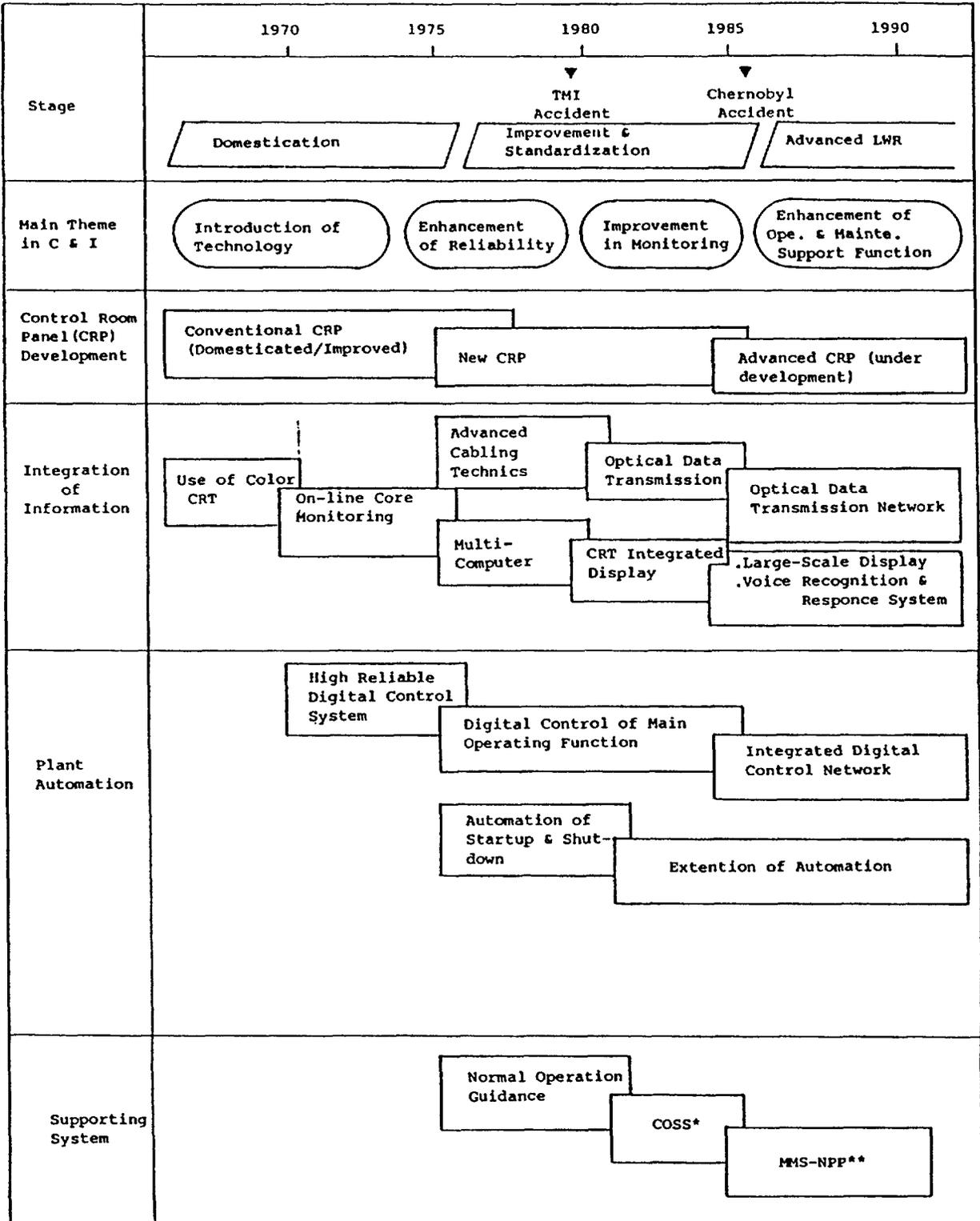
The Nuclear Safety Commission began to give attention to accident management after the TMI accident. However the substantial increase of the Commission's efforts are being made after the Chernobyl accident. Many R & D works in the area of accident management have been encouraged accordingly both in the government sector and utility sector.

It should be necessary to develop symptom oriented or function oriented procedures for severe accidents because the range of their scenarios would be unpredictably wide and of variety. The MITI has been encouraging the utilities to develop such advanced type procedures. The Science and Technology Agency (STA) has, on the other hand, been supporting governmental research laboratories, primarily Japan Atomic Energy Research Institute (JAERI), to conduct relevant research activities whose outputs will form a technical basis for the development of such procedures. They are firstly the development of PSA methodologies and their applications to model Japanese LWRs, secondly research on severe accident phenomena including experiments and code development and thirdly the investigation of recovery methods for severe accidents using a large scale thermal-hydraulics test facility.

In the JAERI's PSA research program, the methodologies for reliability analysis and core melt accident analysis have been carried out and established. These methodologies are being applied to various safety issues. The largest application of these methodologies is the PSA of a model Japanese BWR through which effective operator actions to mitigate the core melt accident have been identified.

The severe accident research at JAERI has been conducted with the objectives to identify phenomena associated with a severe accident in a LWR, to develop analytical tools for estimation of source terms and to quantify uncertainties in risk analysis and safety margin of a LWR. Among other experiments, the containment integrity experiments will be the largest and be initiated in 1990.

The large scale thermal-hydraulic test facility ROSA-IV of JAERI will be extensively utilized to verify the current standard recovery procedures and to investigate procedures for prevention of core damage.

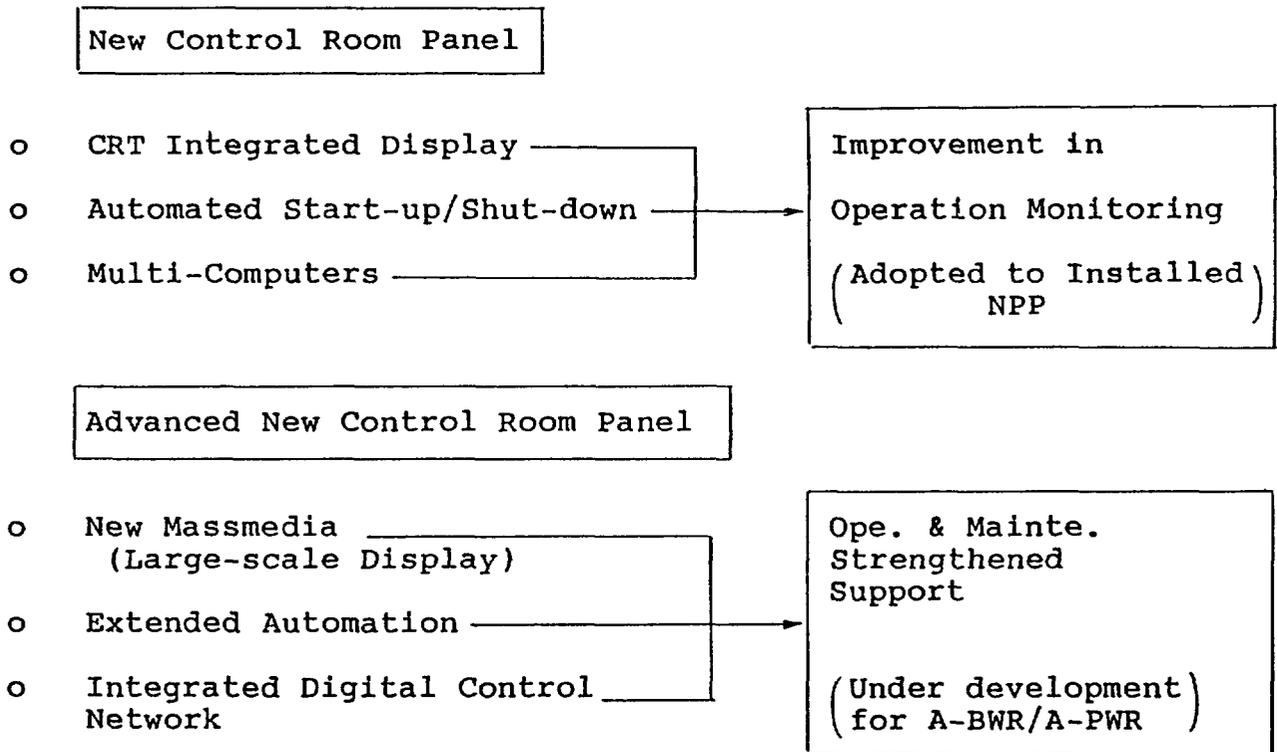


\*COSS: Computerized Operator Support System  
 \*\*MMS-NPP: Advanced Man-Machine System for Nuclear Power Plant

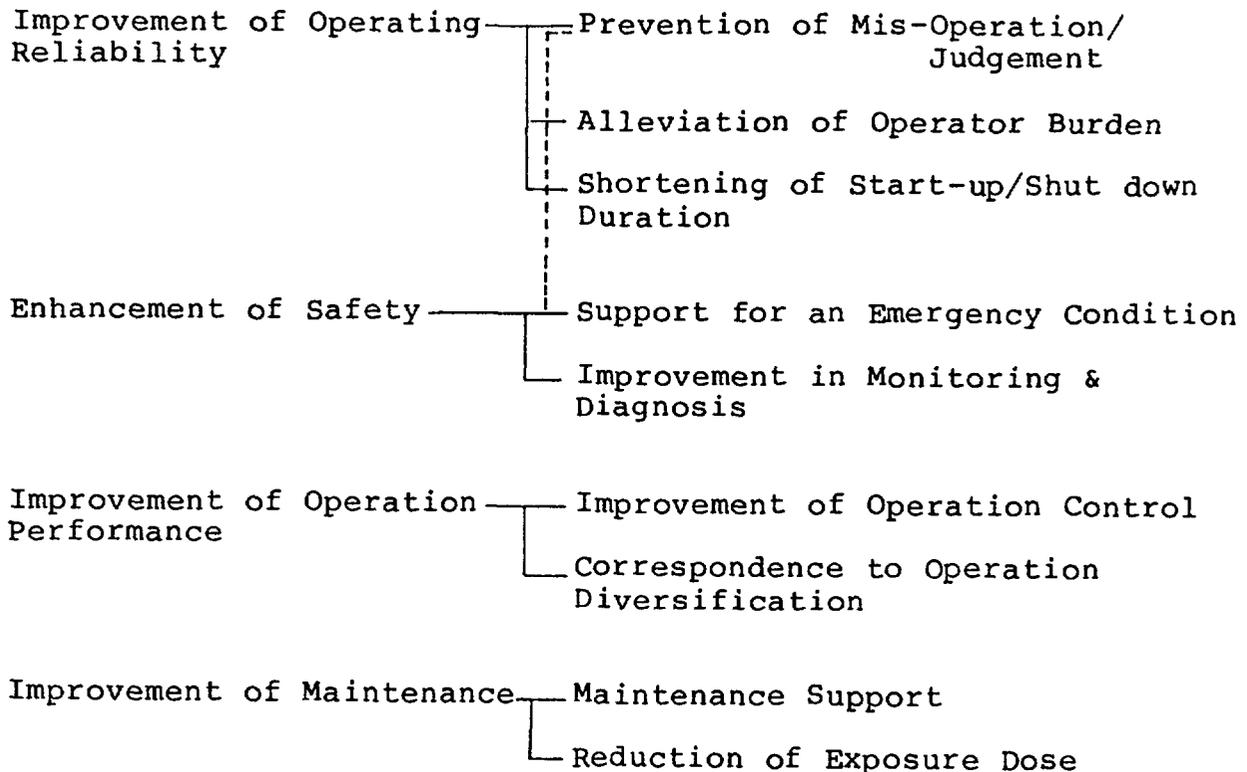
FIG. 4. Technical development of improved and sophisticated operations.

### 3. TECHNICAL DEVELOPMENT OF IMPROVED AND SOPHISTICATED OPERATION

#### (1) CURRENT STATUS OF SOPHISTICATED OPERATION TECHNOLOGIES



#### TARGETS OF OPERATION SOPHISTICATION



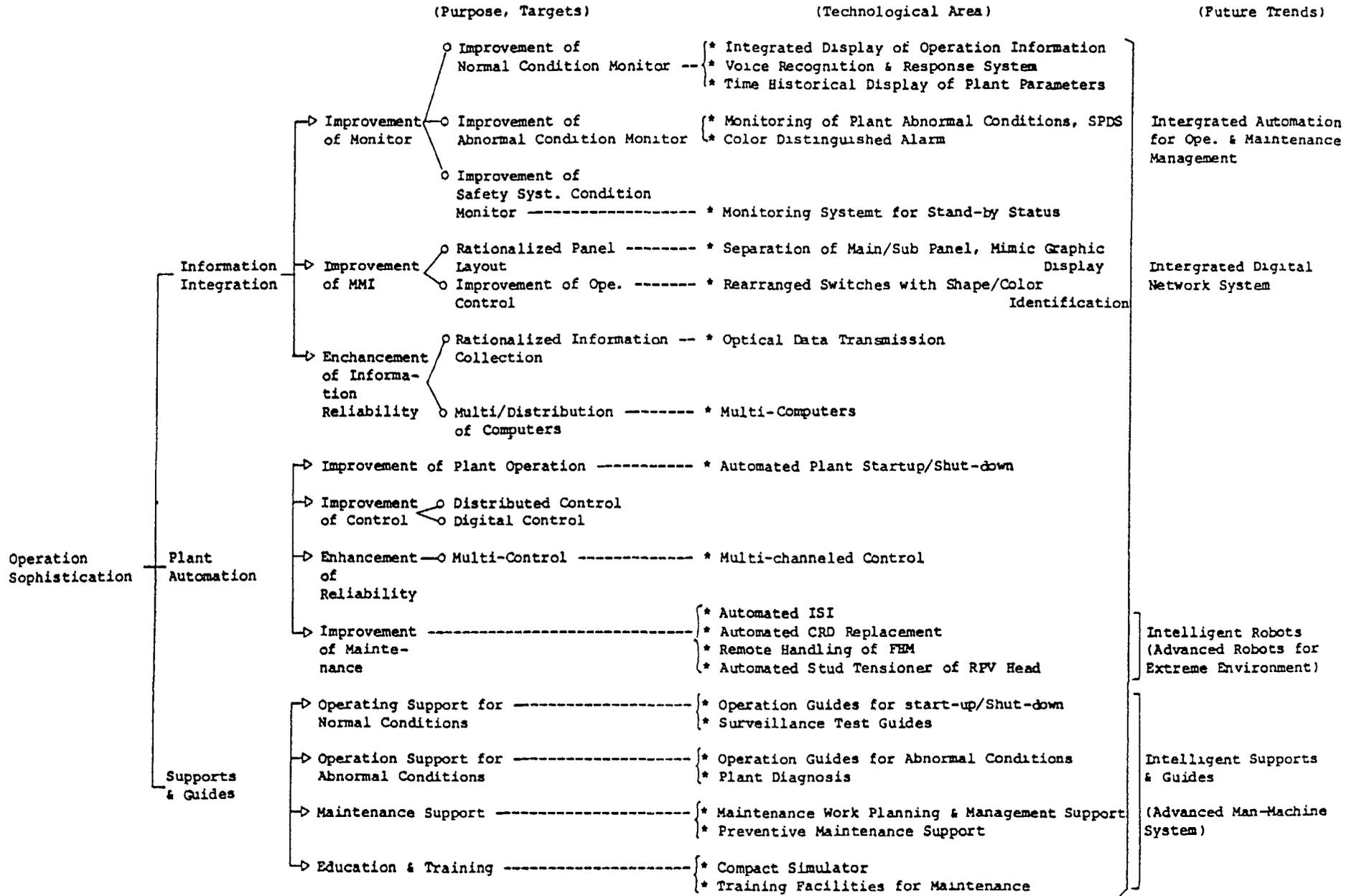


FIG. 5. Technologies of operation sophistication and relevant areas.

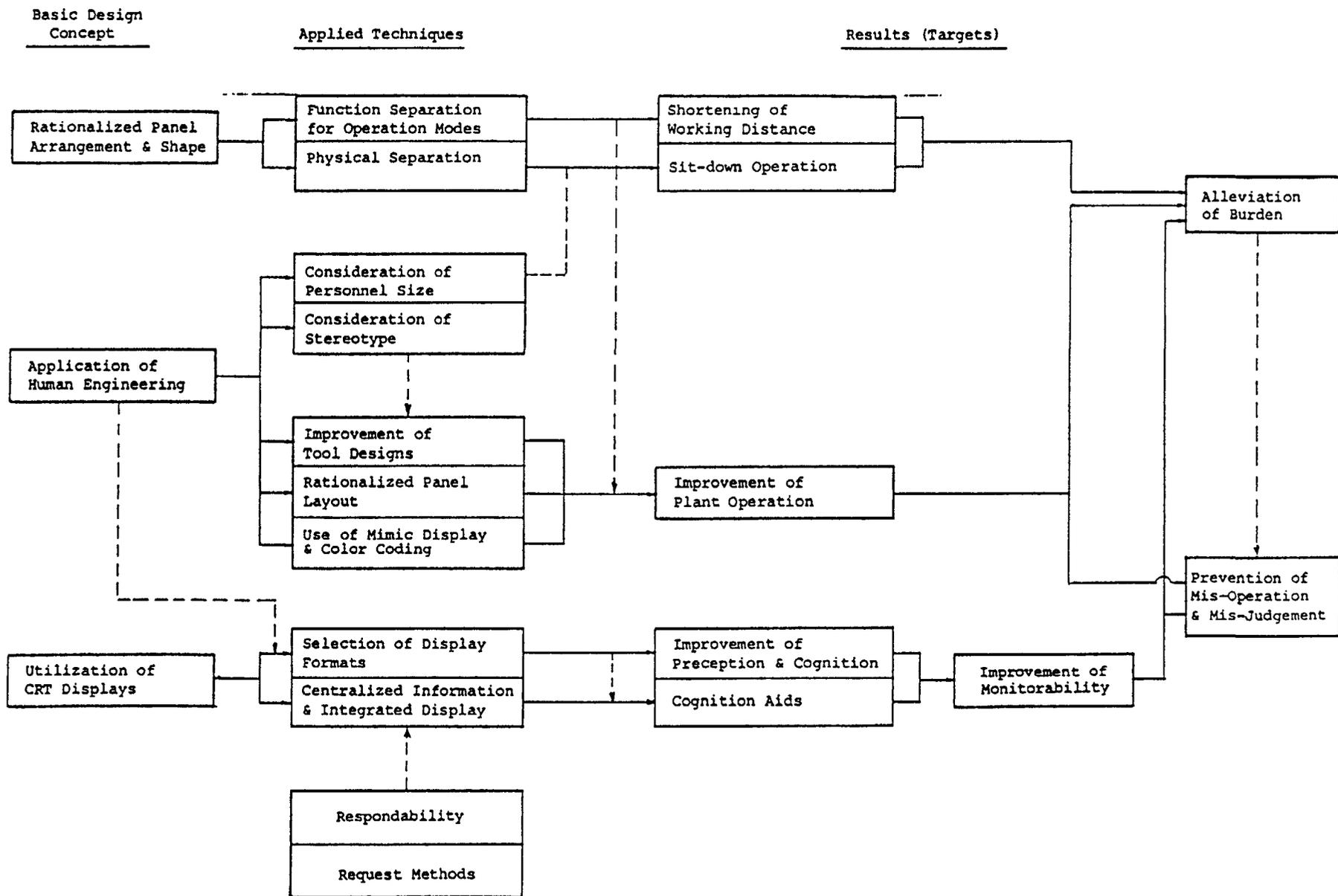


FIG. 6. Basic design concept for new control room panel.

## (2) INTEGRATION OF OPERATION INFORMATION

### Target

- ① Improvement in Normal Condition Monitoring  
--- Stable and Efficient Operation
  - o Alleviate Operator Burden
  - o Prevent Mis-operation/Mis-judgment
  - o Secure Easily the Soundness of Systems
- ② Improvement in Abnormal Condition Monitoring  
--- to Prevent an Accident Expansion and Secure Safety
  - o Detect Early the Defect and Find the Cause
  - o Grasp Accurately Conditions
  - o Correspond Appropriately to Conditions

### Current Status

- ① Rationalize Panel Arrangement/Shape
- ② Apply the Human Engineering
- ③ Utilize Positively CRTs

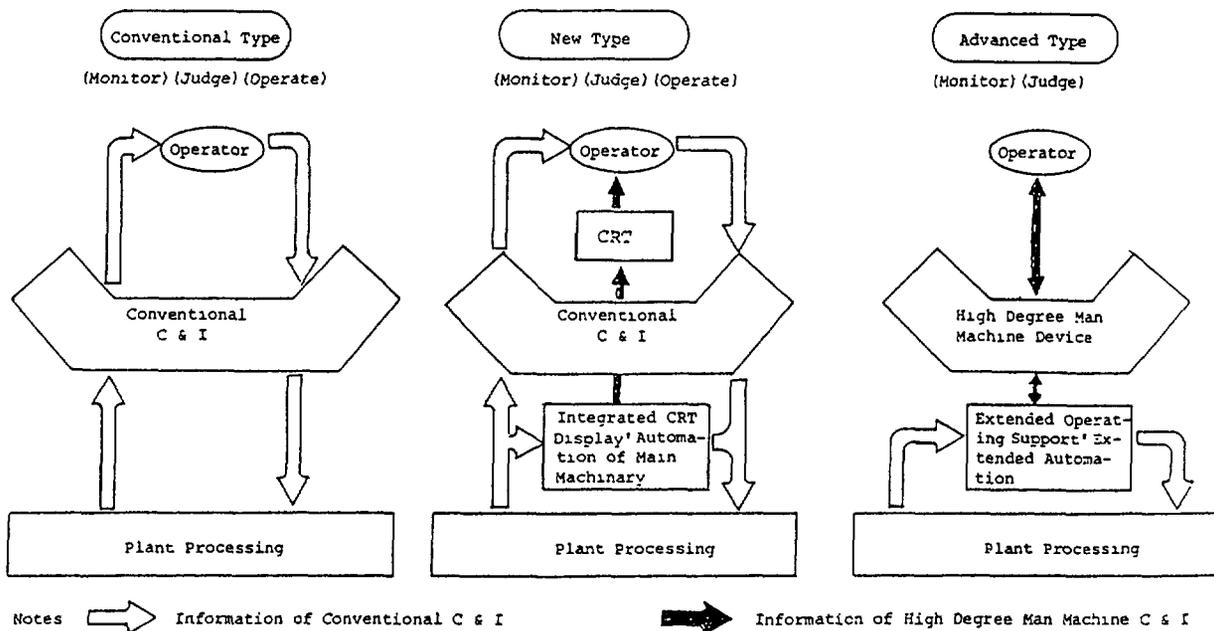
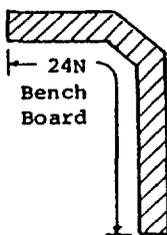
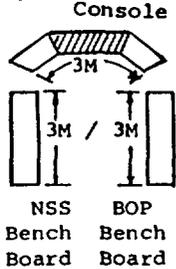
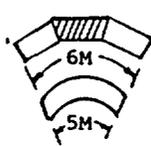


FIG. 7. Development of man-machine interface and automation.

No.	I t e m		Conventional CRP	New CRP	Advanced CRP
1	Man-Machine Device	Color CRT	Partial	0 (YES)	0 (YES)
		Large-scale Display	-	-	0
		CRT Operation	-	-	0
2	Plant Automation	Sub. Loop	0	0	0
		Start-up & Shut down	-	0	0
		Control Rod	0	Operation Guide	0
		Plant Transient	-	-	0
		Surveillance Test	-	Operation Guide	0
3	Intelligent	Core Performance Prediction	-	0	0
		System Readiness Monitor	-	0	0
		Summary Status Monitor	-	0	0
		Plant Trip Event Sequence Monitor	-	0	0
		Plant Trip Status Monitor	-	0	0
		Voice Recognition and Response System	-	-	0
		Plant Summary Monitor	-	-	0
		Maintenance Support	-	-	0
4	Configuration	Digital	Partial	Main System	Digital Network
		Optical Data Transmission	-	Partial	Optical Data Transmission Network
		ECCS RPS	Hard wired	Hard Wired	Soft Logic
		No. of Operator	11 man/2 unit	11 man/2 unit	7 man/2 unit
		Panel Layout	 <p>24N Bench Board</p>	 <p>Operator Console 3M / 3M NSS Bench Board    BOP Bench Board</p>	 <p>Large-scale Display 6M 5M Operator Console</p>

CRP = Control Room Panel

FIG. 8. Comparison of main specifications for different control room panels (example).

**Purpose** Improvement in Operation Monitoring by Utilizing Appropriately CRT Display Function

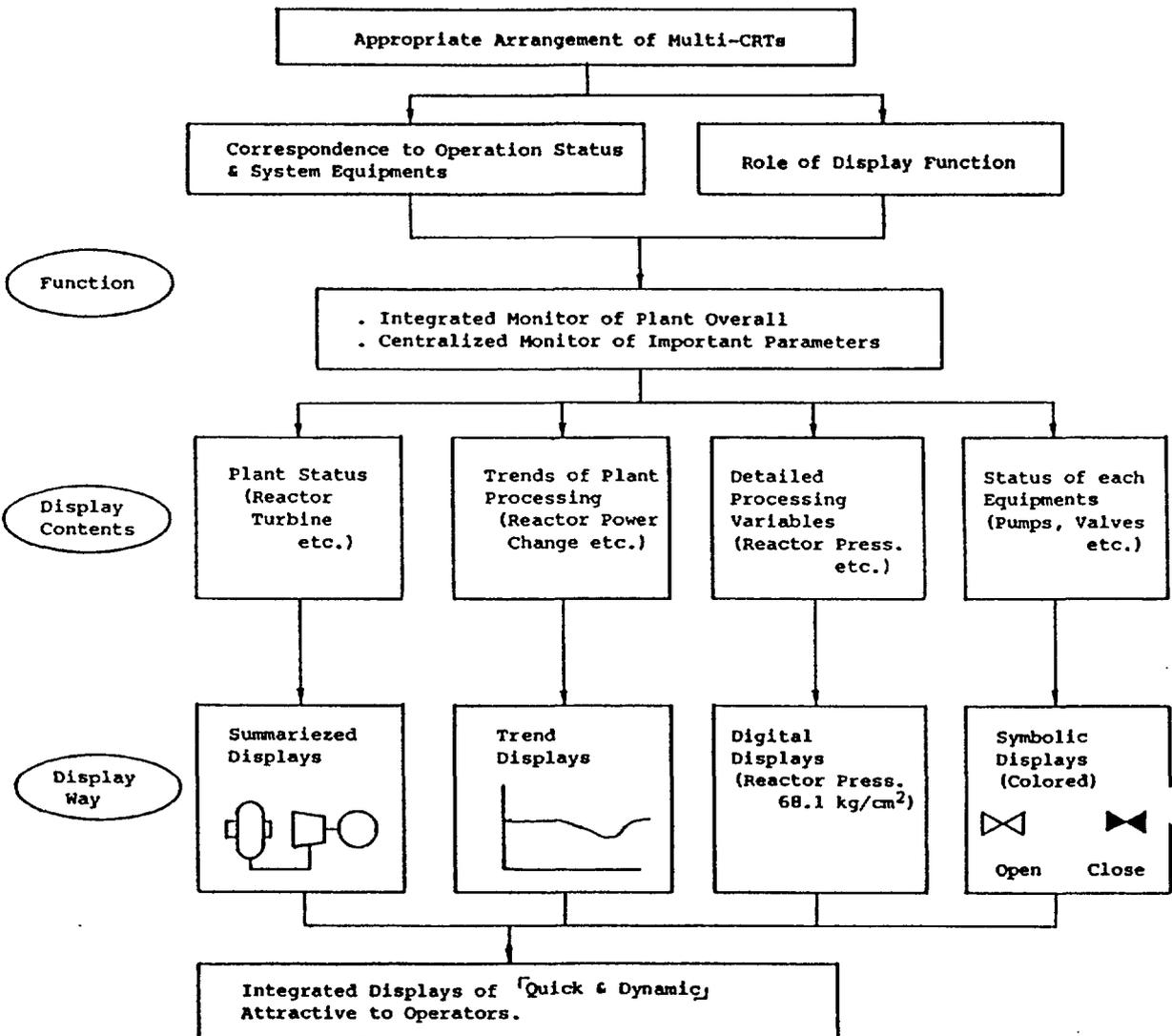


FIG. 9. Functions and characteristics of CRT display.

TABLE 4. AUTOMATED OPERATION/FUNCTIONS (MAIN ITEMS)

Category	No.	Automated Operation/Functions	New Control Room Panel	Advanced Control Room Panel
Plant Start-up & Shut-down	1	Reactor Water Level Control in Startup	O	O
	2	Control Rod Operations	OG	O
	3	Turbine Start-up, Speed-up, Stop	O	O
	4	Start-up/Stop/Changeover of Reactor Feed Pumps & Condensate Pumps	O	O
	5	Operation of Turbine Gland Steam Seal Syst.	△	O
	6	Vacuum-up/break, & Operation of Off-gas Syst.	△	O
Plant Transients	7	Generator Synchronizing & Initial Loading	O	O
	8	Feedwater Syst. Control Interlocking	---	O
Surveillance Test	9	Regular Operations of Aux. Equip. After a Trip	---	O
	10	Surveillance Test of Main Equipments	---	O
	11	Surveillance Test of Safety Related Syst.	OG	O

Notes O: Automated    △: Semi-automated    OG: Operation Guides (Manual)

- Separation of Input and Output Information (Signals)
- Self & Mutual Diagnosis Function
- Switch over based on Redundant Voting System

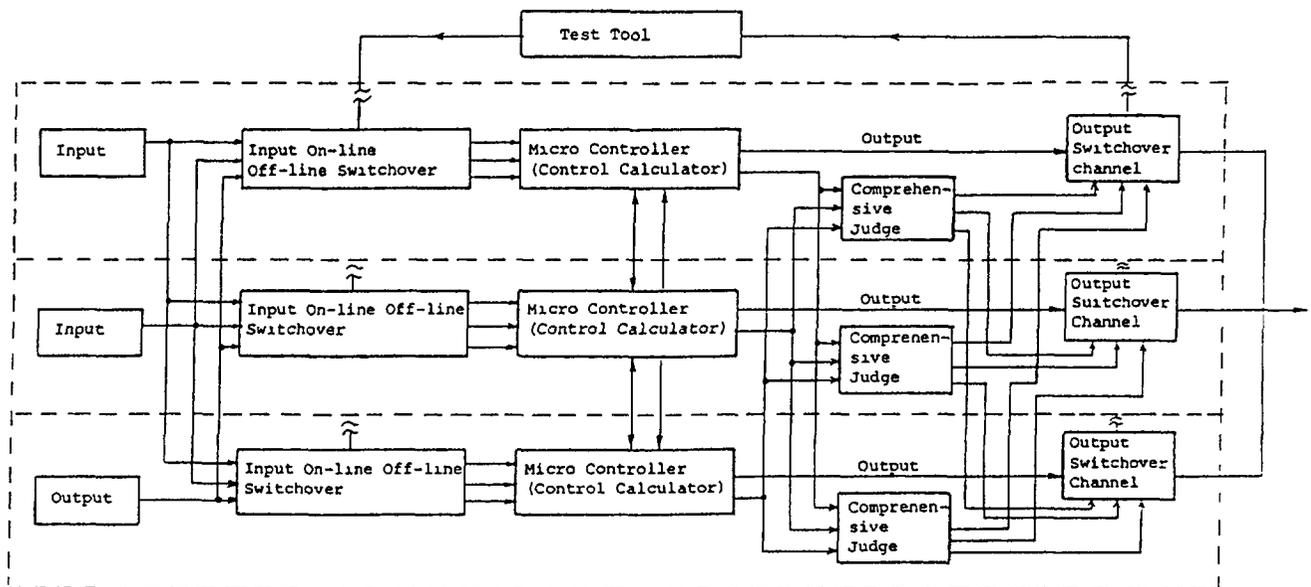


FIG. 10. Example of highly reliable digital control system structure (multichannel of major systems such as reactor coolant flow control and feedwater flow control).

(3) PLANT AUTOMATION

Target

- ① Enhance Operating Reliability  
--- Alleviate Operator Burden and Save Labor
- ② Improve Operating Performance  
--- Improve in Operation Control
- ③ Reduce Exposure Dose  
--- Curtail Field Operation

Current Status (New Control Room Panel)

- ① Automate Plant Start-up/Shut-down
- ② Multiplex Main Digital Control Channels
- ③ Develop Normal Operation Guides & Surveillance Test Guides

(4) COMPLETION OF INFERENCE SUPPORT

a. OPERATION & MAINTENANCE SUPPORT

Purpose

- ① Enhance Further Operating Reliability  
--- Early Detection of Defects, Early Identification of Causes and Securance of Safety
- ② Support Planning of Operation and Maintenance
- ③ Provide with User Friendly MMI

Current Status

- ① Computerized Operator Support System (COSS)  
Developed Already by Cooperation of Governmental and Private Sectors in 1980-'84.
- ② Advanced Man-Machine System (MMS-NPP)  
Developing A.I. Applied Systems  
Phase I: Conceptual Design (1984 - '86)  
" II: Detailed Design & Verification Test (1987 - '91)

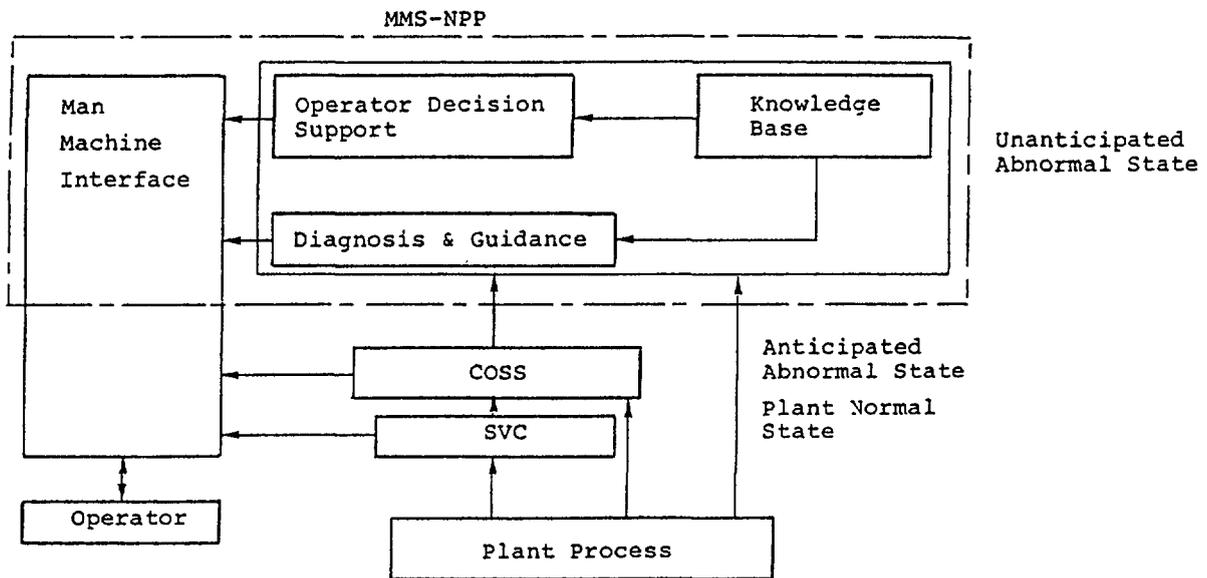
b. EDUCATION AND TRAINING

Purpose

- ① Improve Ope. & Mainte. Skills by Systematic Training
- ② Prevent Human Errors

Current Status

- ① Popularize Self-training Using Training Facilities Inside Utilities --- Compact Simulators & Mock-up for Maintenance Work
- ② Introduce Operator Qualification --- for Shift Supervisors
- ③ Human Factors Research



MMS-NPP: Advanced Man-Machine System for Nuclear Power Plant

COSS: Computerized Operator Support System

SVC: Supervisory Control System

FIG. 11. Operation support systems and relevances.

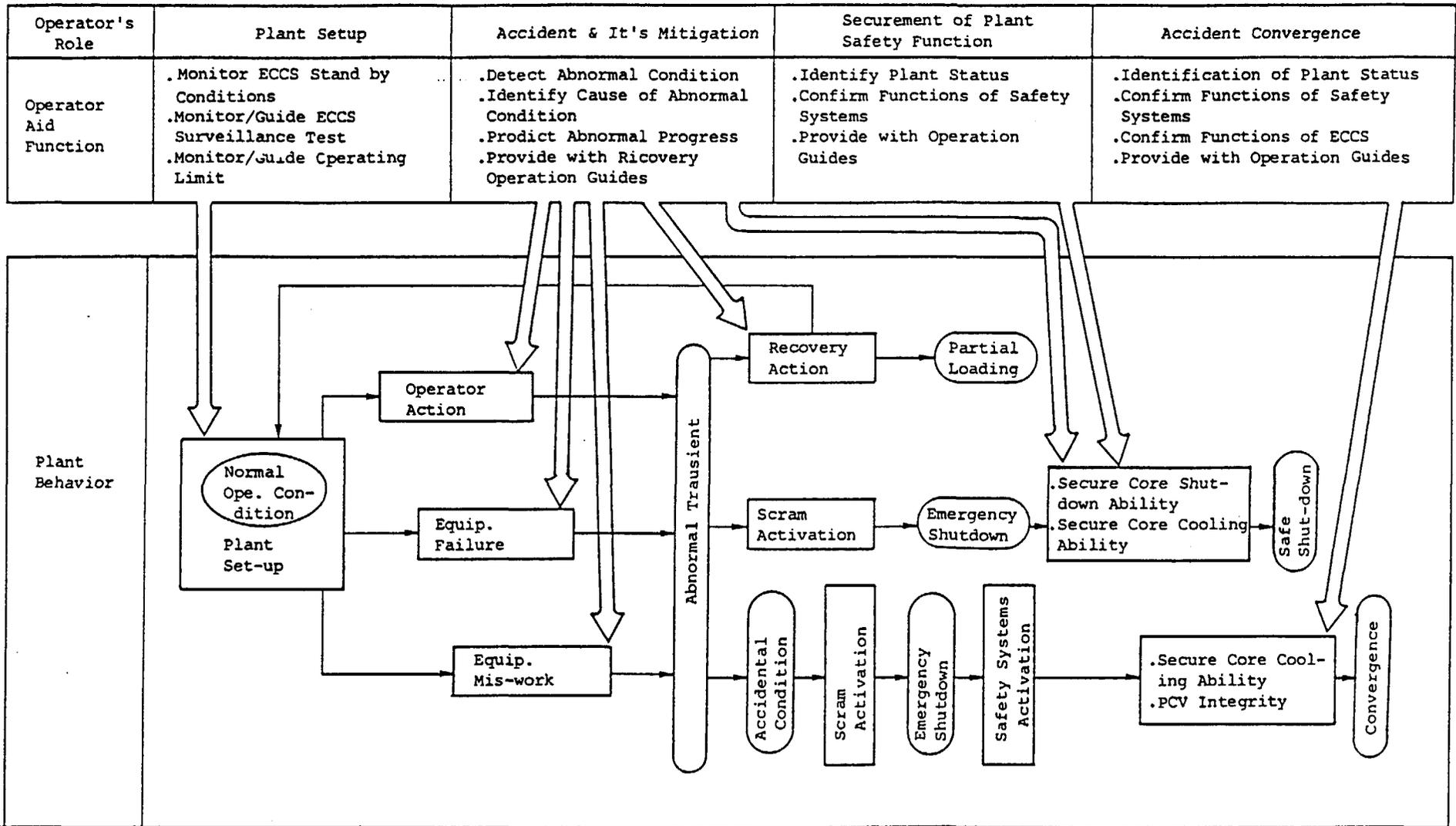


FIG. 12. Functions of COSS corresponding to plant conditions.

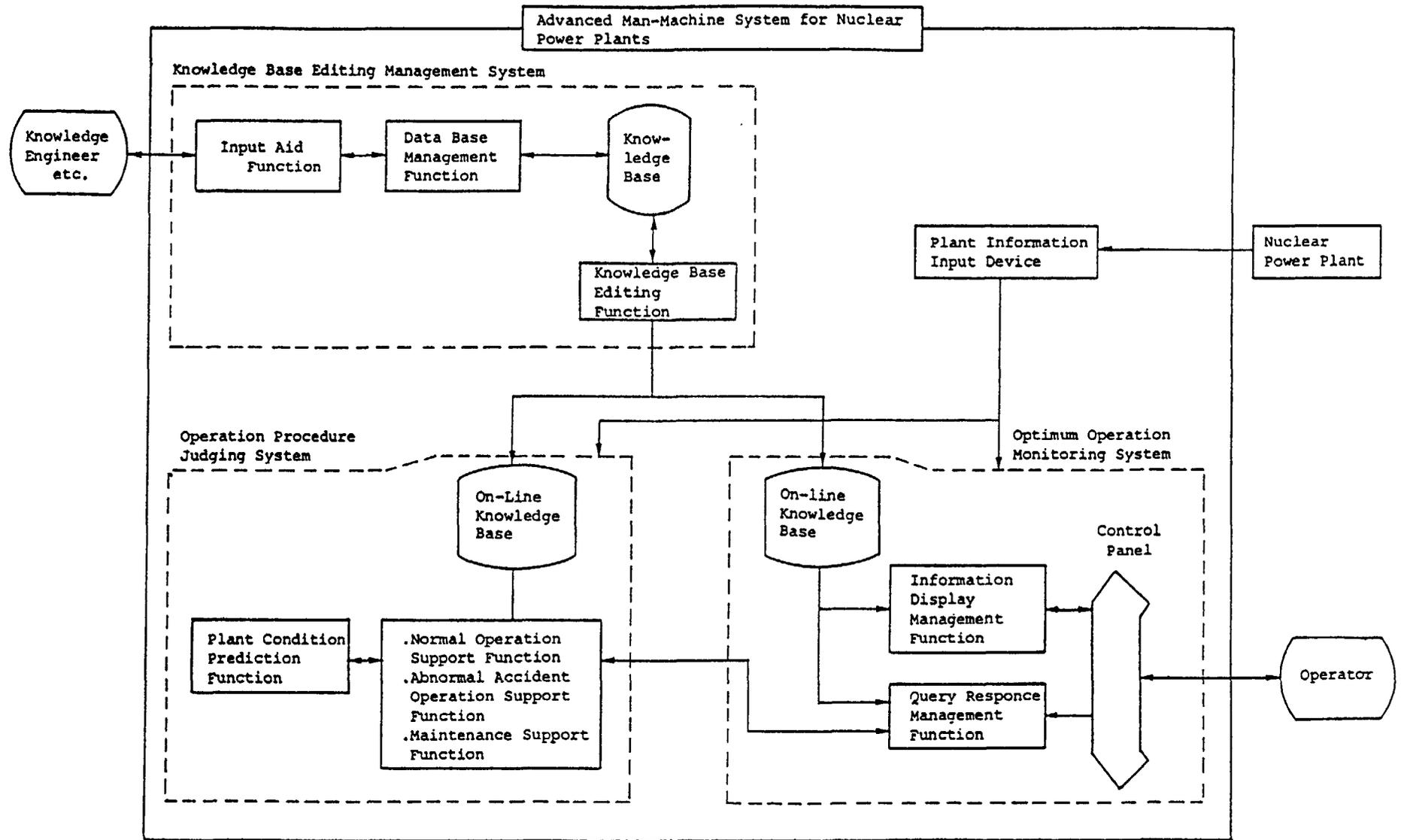


FIG. 13. Function and constitution of advanced man-machine systems for nuclear power plants (MMS-NPP).

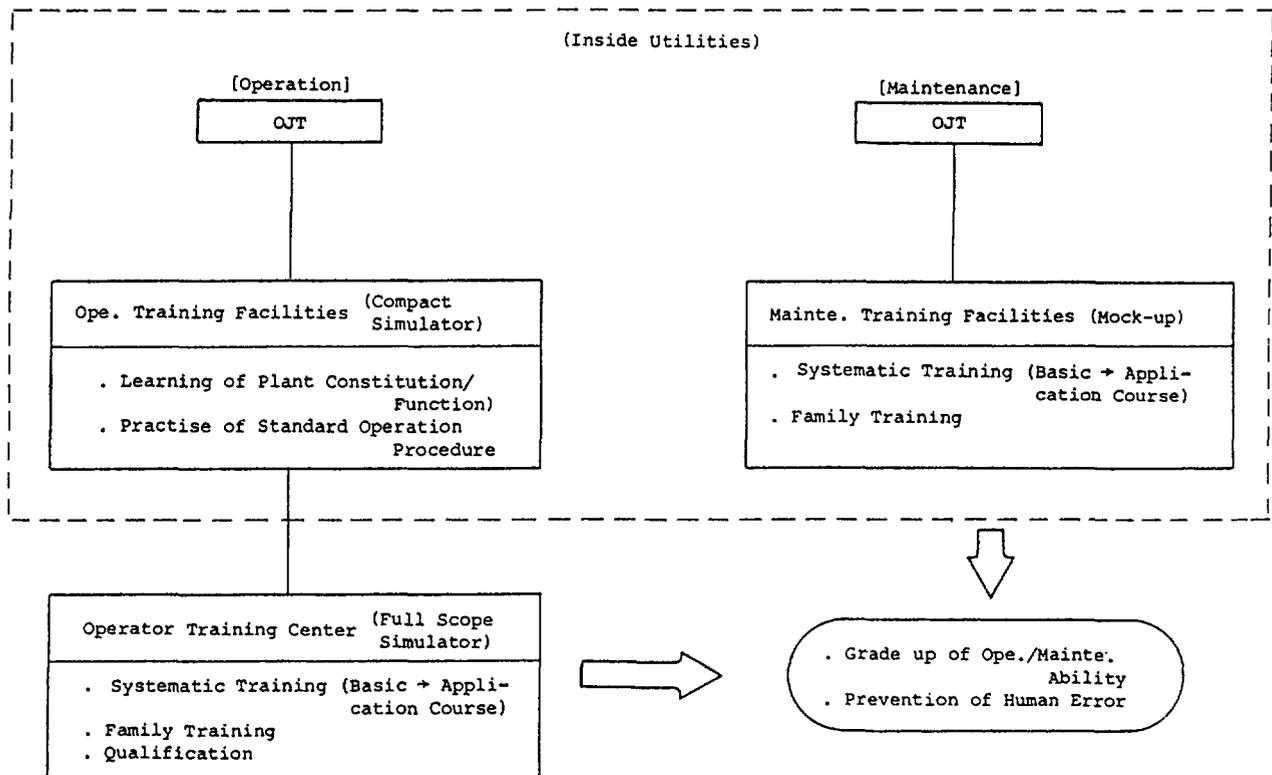


FIG. 14. Education and training system for operator/maintenance staff.

#### 4. FUTURE TRENDS AND PERSPECTIVES

##### (1) Comprehensive Automation of Operation Control

- o Enhancement of Operation Reliability and Extension of Automation
- o Integrated Data Communication System for NPP
- o A.I. Inference Support and Robot

##### (2) Optimization of Man Machine Interface

- o Multi-massmedia
- o Harmonization between Man and Machine

##### (3) Human Factors Research

- o Research on Human Behavior and Team Dynamics & Performance
- o Optimized Role Allotment for Man and Machine

#### 5. INTERNATIONAL COOPERATION

- o Knowledge or Know-how to Operate NPP Safely and Reliably Should be a Common Property of the World.
- o Current Status of Development and Utilization of Nuclear Power Depends Not Only on a Nation's Effort, but Also on the Internationally Exchanged Technologies.

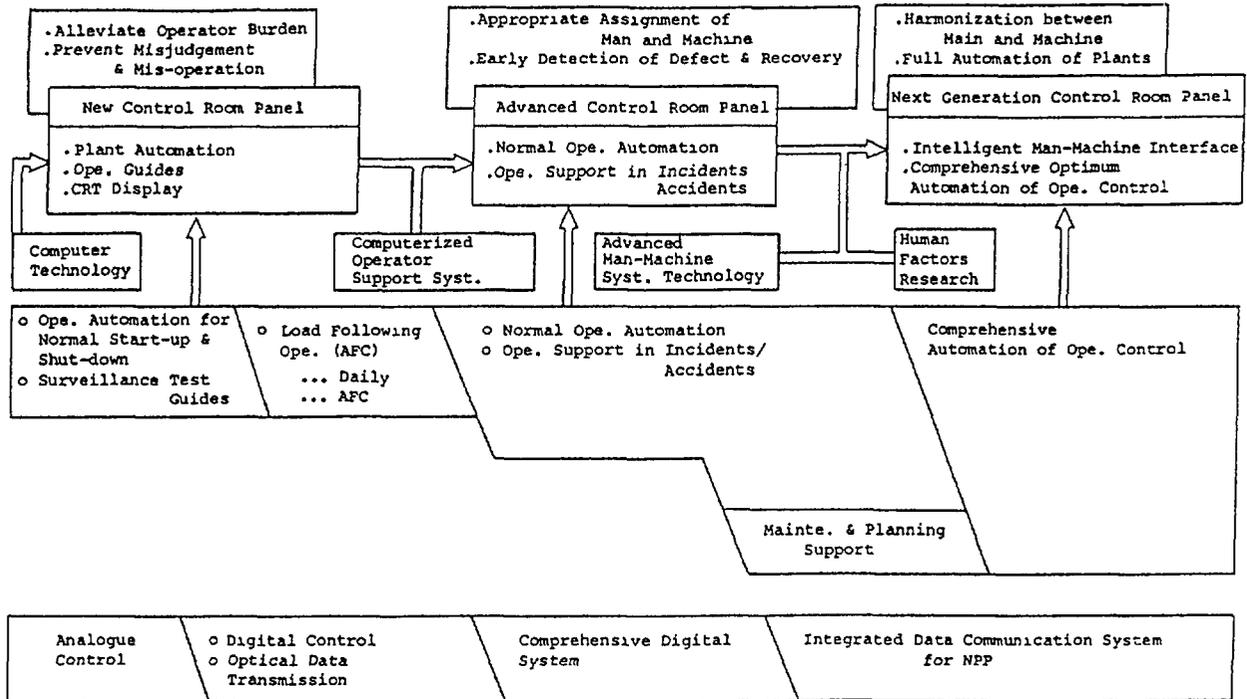


FIG. 15. Trends and perspectives for operation sophistication technology.

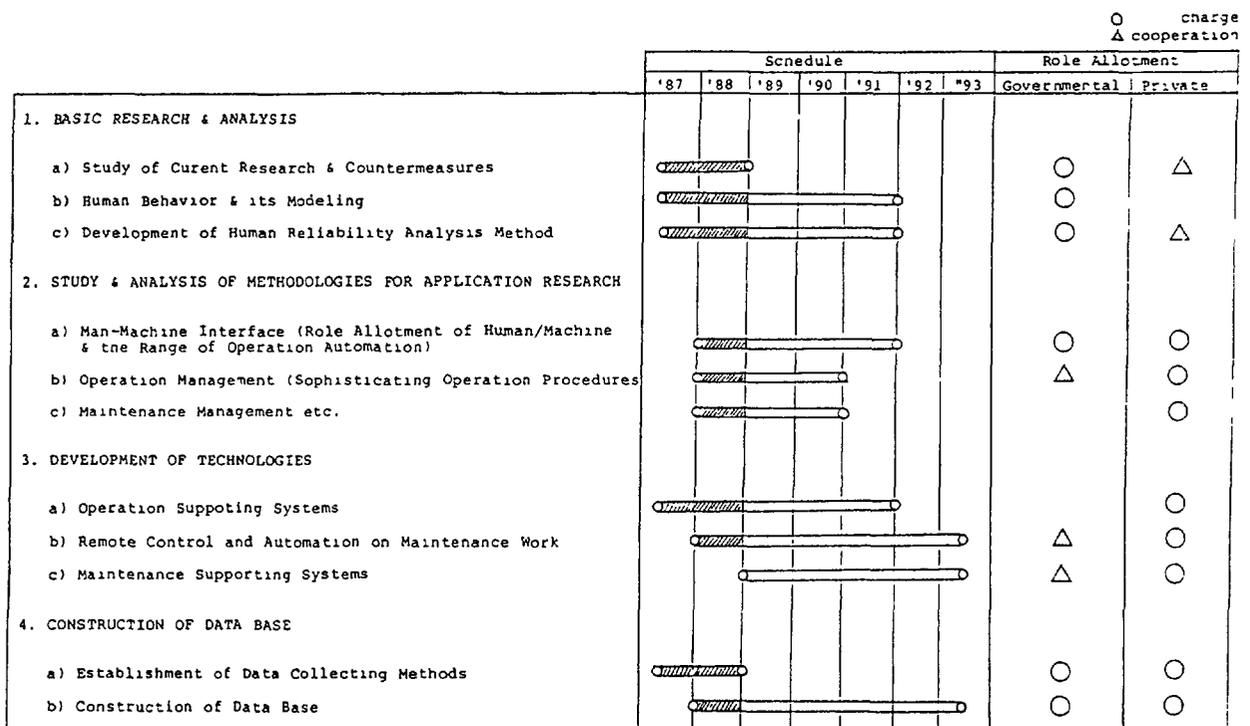


FIG. 16. Long term plan for human factors research.

## Annex 1

### Topical Items on Balance between Automation and Human Actions in Nuclear Power Plants

- (1) Automation and Accident Management  
... In accident management situations presumably various (not firmly planned) manual actions have to be performed. How much do they effect automation? Does automation prevent those actions? To which extent human intervention with respect to the automatic systems themselves is necessary?

What sort of accident or how extent of accident situations should be considered, will depend on the current technological and qualitative level of nuclear power generation in a country. Measures applied in our design are summarized as follows;

- 1 Safety related systems are designed in actual practice to start/stop automatically when an incident/accident happens. No human action is needed accordingly.
- 2 Plant automation and guides cover also some of major operation procedures required in the plant startup/shutdown and surveillance tests. (Table 4)

- (2) Advanced (computer based) Information Systems  
... Management of primary data with regard to higher level information as a first step towards automation, information, qualification.

Control and instrument systems of important plant systems are multi-channeled in order to enhance reliability of the systems. In addition, several information processing and CRT displays have been developed applying computerized technologies and utilized to support usefully operator's monitoring and inference. (Figures 10-14)

- (3) Expert Systems and Procedures

Many expert systems have been developed as mentioned in the above items in which expert systems providing control room CRTs with operation guides are included.

- (4) Expert Systems and Automation  
... merits of using expert systems, qualification problems, advantages and disadvantages of conceptual solutions, potential or expert systems in NPPs

Expert systems developed are designed to alleviate operator burden of monitoring and inferring and to further improve in operation reliability.

A Computerized Operator Support System (COSS) for plant abnormal conditions was developed as a five-year project (1980-1984), under the sponsorship of MITI. The main purpose of COSS development was to implement the lessons learned from the Three Mile Island accident. The design concept of the operator support functions and the method to implement it were established and the prototype systems of COSS for BWR and PWR plants were developed.

With completion of the COSS development, a subsequent project to develop an advanced Man-Machine System for Nuclear Power Plants (MMS-NPP) has been initiated. This eight-year project aims at realization of the advanced operator support system by applying innovative technology such as artificial intelligence (AI) techniques, especially knowledge engineering, and sophisticated man-machine interface devices.

A major goal of this system is realization of human friendly and intelligent operation support by man-machine interactive interface, matching with the operator's cognitive processes, by adopting the update computerized technologies, knowledge engineering and new massmedia techniques.

The verification tests will be conducted by using plant simulator in the final year.

(5) Advanced Automation Systems

... future applications of on-line simulators

On-line simulators are being applied to the control rod operation and core performance monitoring, being contributable to help operators monitor and infer.

(6) Diagnostic and Prognostic Systems

... role for operational disturbances and accidental situations

These systems are included in the above said MMS-NPP system in which an operation support system in an abnormal condition serves as these functions.

(7) Safety Aspects/Guidelines

... automation performance dependent upon system failures (abnormal deviation of process parameters), automation failure and back-up controls, manual intervention as a means of back-up control, qualification measures, reliability requirements for automatic systems (reliability hierarchy dependent upon importance for safety), how to assess human reliability versus reliability of automatic systems, advanced signals management and level of set points (analytical redundancy, on-line computer algorithms).

- 1 So-called ten (10) minute design criteria is applied to safety related systems so that they can be automatically and sequentially operated with no manual actions for ten (10) minutes after their start-up in an incident/ accident. In addition, some of major operation procedures are automated in the plant startup/shutdown and surveillance tests, as mentioned.

- 2 Control and instruments of major systems are designed multi-channeled to prevent the impact of a single failure so that operation reliability as well as automated functions can be secured plant overall.
- 3 No particular reliability are requested, at present, for automatic systems, however, their installations are subject to high quality control and field tests.
- 4 Effective assessment methods have not been developed yet in terms of human reliability versus reliability of automatic systems.
- 5 Advanced signal management and level of set point such as analytical redundancy are now under a study.

# THE BALANCE BETWEEN AUTOMATION AND OPERATOR CONTROL

A. COLAS

Service de la production thermique,  
Electricité de France,  
Paris-La Défense,  
France

## Abstract

The technological progress in the field of automation and industrial data processing can pose the following problem: "operator or logic controller" instead of "operator and logic controller". In most situations this question can be considered from two viewpoints: from the basis of experience and from using a conceptual approach.

The paper reviews this two possibilities: part 1 - the lessons EDF has drawn from experience, and part 2 - the present doctrine.

## Part 1 — The lessons EDF has drawn from experience

At the present time, EDF operates some fifty 250 MW units and the experience that it has gained can be summarized as follows.

There have been three successive stages. First, conventional power plants. Second, the development of the French graphite moderated, gas cooled reactor programme. Third, the advent of pressurized water reactors, representing a major advance in automation.

The conventional plants, which are now beginning to age, were equipped with the control and instrumentation systems available at the time. The equipment was controlled with turn-push lights. The equipment status indications and operating parameters were given on indicators and recorders. A protection system based on the exceeding of thresholds and a control system of conventional technology completed the system. Control consisted of configuring and adjusting the installation part by part. In passing, it must be mentioned that more recent conventional plants are extensively automated.

The French natural uranium fuelled, graphite moderated, gas cooled reactor programme served, among other things, as a test bench for the development of complex installation automation systems. Although the first two plants were equipped with conventional control and automation systems, the next two represented a significant advance. They were equipped with sequential logic controllers implementing complete functions. The logic controller operates step-by-step, checking that the preceding step has been completed before beginning with the next. A single command initiates a complete sequence. Certain systems provide control at function level. Other more complicated systems coordinate the functions between each other. The plant is provided with a complex overall protection system.

One of the particularities of this control and instrumentation system is in the signalling. In view of the degree of automation of the command and protection functions, information concerning the state of the equipment and the operating parameters is output on printers as it becomes available. This gave the operators the feeling of being "blind". With their "reduced vision" of the state of the installation, they frequently called upon the watchmen to make on-the-spot checks. Lacking a detailed view of the situation, they committed a number of errors, making the wrong settings, which resulted in excessive tripping of the protection systems.

The lessons of this experience were used in Bugey A Power Plant. Certain simple automatic sequences were deleted and left to the operators. Mimic boards showing the installations were added, as well as a more conventional manner of signalling the state of the equipment and the operating parameters.

New conditions appeared between 1960 and 1970 with the adoption of the PWR system in France. The American design corresponding to the Westinghouse license and the new regulations decided upon by the safety authorities resulted in a step backwards compared to the technology of the natural uranium fuelled, graphite moderated, gas cooled reactor systems.

The safety authorities refused safety qualification of the electronic components used for automation, considering their reliability uncertain and demanding broader industrial experience. They also imposed periodic tests of the function safeguard systems. Control and instrumentation technology thus reverted to the level to be found in conventional power plants and the early natural uranium fuelled, graphite moderated, gas cooled installations, with certain differences. Doubling the channels and the control and instrumentation systems was imposed. The progress in control and automation with electromagnetic relay systems due to the requirements of the safety authorities resulted in a more effective reactor protection system. A surveillance computer without safety qualification was added but merely supplied important information on screen as it became available. The lack of ergonomic preparation of the man-machine interface and the general hardware resulted in grouping the control and instrumentation devices on boards and desks in an inconvenient manner. It was not until between 1980 and 1982 that the configurations of these desks were fundamentally changed.

The opportunity of the change from the three steam generator 900 MW generation to the four steam generator P4 1,300 MW generation was taken to rethink the control and instrumentation system. Three major modifications were made. The most important was the introduction of a safety-qualified multi-level logic controller system. This necessitated careful selection of the components, the design and above all of redundancy and default signal processing modes. The logic controllers essentially replaced the greater part of the electromagnetic relay systems, combining control functions, simplifying stream tests and improving reactor protection. The lesson concerning grouping of the control and instrumentation equipment by function was applied. Progress was also made in the use of the surveillance computer, giving better on screen display of alarms. A selection system causing display of

only the alarms corresponding to the actual state of the installations made it possible to simplify the alarm management work of the operators.

The 1,400 MW N4 generation constituted a milestone. An in-depth study of the data processing interface was carried out in 1982 ready for the future units: Chooz B from 1990. This project, which was managed by EDF, brought together the designers of the data processing system, the users of the plants, specialists in ergonomics and specialists in human factors. The system was first tested on a simulator. During three test sessions between 1987 and 1990, more than 100 operators will have tested this new control room in all its configurations. More than 1,000 hours of man-machine interface specialist time have been consecrated to these tests. It should be noted that this more technologically advanced and ergonomically sophisticated system is not safety qualified. An auxiliary panel enabling return of the installations to a safe state from all the operating configurations in the case of failure of the data processing system is thus an integral part of the control and instrumentation. This data processing interface integrates the display of procedures which can be executed directly, alarm sheets which can also be executed directly, unavailability of equipment tagged or under testing, operating diagrams, display of the operating point relative to the authorized limits and provides numerous other operating facilities for the operators.

Here, it should be borne in mind that the changes made to the entire generation of pressurized water reactors have benefited from the thinking after TMI and Chernobyl, but also from the systematic analysis of more than 3,000 operating events which have occurred since 1984 in the French nuclear installations.

## **Part 2 — Present doctrine**

Let us now consider the conceptual approach that EDF has developed, essentially on the basis of experience. First of all, I am forced to admit that there is nothing very original in this approach. It is simply the point of view that currently prevails in our organization.

### **Operator or logic controller**

instead of **Operator and logic controller?**

The question should no doubt be posed, but it is not necessary to dwell upon it, the answer goes without saying. There is no other choice possible than the association of operators and logic controllers. The two systems constituted by "operators" and "logic controllers" can at times do the same thing. Generally speaking, one is better than other in certain areas. For each particular activity, that offering the best performance is chosen, creating a harmonious and complementary whole combining the operator and the logic controller. The similarities and the differences in capacity offer functional redundancy which is useful for safety reasons as well as in terms of industrial performance. Let us now consider the characteristics of each.

The computer or industrial logic controller frequently operates best in the present. It can scan a wide range of information in a reliable manner. It can have enormous memory capacity. On the other hand, it is difficult to get it to make comparisons with past events. A situation has many aspects and it is difficult to programme a logic controller for this type of activity. It derives and integrates, accurately and reliably monitoring trends. It can easily compare an instantaneous value with a reference value. On the other hand, the operator performs far better when it comes to interpreting a changing situation which resembles one which he has experienced two years earlier in another plant. The operator is thus better at making projections into the future. While the logic controller is still monitoring a pressure which is rising but has not yet reached the critical threshold established for it, the operator has seen the danger and already decided to change the sequence of events.

On the other hand, the logic controller reads the instructions given to it at extremely high speed. It is an ultra-rapid and reliable servant. Who could still imagine beating a calculator in speed and accuracy! But the ultra-rapid and ultra-reliable logic controller executes the programmes that the designer has loaded — that the designer has created by imagining the possible situations. These possible situations, together with the parameter limits and technology limits, represent a finite domain beyond which the machine cannot go.

Faced with this, man has his five senses. He is capable of discovering, judging and recombining the different components of a situation, and integrating them in analysis. His reasoning which recreates the situation at each stage is slow compared to that of the machine and subject to error but is constantly readapted, and thus in phase with the situation whatever it may be. If the sequence of events changes, the logic controller will detect this earlier but when the logic controller has become completely lost in an unknown situation, the operator is still capable of finding his way. For every advantage there is a price to be paid. Man needs to be able to understand if he is to act, which may result in him being critical of what he is asked to do. There are occasions when a disciplined logic controller is better than a critical operator. But this is not always the case.

The logic controller follows its instructions. Its vigilance is total. It is therefore more reliable, at least as long as it remains serviceable! But it can also break down. At the present time, it is increasingly capable of detecting faults in its own operation and even of identifying their causes. But once it is in this situation and has given its error message, what more use is it? And how can it repair itself?

The operator has at least the advantage, even though he may make errors more frequently, of having a critical approach which leads him to correct certain of his mistakes and total failure, as in the case of the logic controller, is extremely rare!

It is universally acknowledged that making diagnostics is a characteristically difficult activity. To make a good diagnostic it is necessary to select the pertinent information and develop a sound line of reasoning to reach a correct picture of the situation. If a logic controller is supplied with the information and the processing capability, it will be

faster and more reliable than an operator. But it is not possible to foresee everything, particularly the combinations of symptoms characteristic of all possible situations. The development of expert systems capable of conditional analysis of an extremely complex nature associating hundreds or thousands of parameters represents a new dimension in processing and identifying situations. The operator who discovers three or four features of a situation already found important in the past can be equally effective. He can of course make mistakes. He can even get caught up in a line of misguided reasoning which can cause him to deny facts which he cannot reconcile with the image he has formed of the situation.

Here is a field in which complementarity and redundancy between logic controller and operator is of primary importance. EDF has begun a number of programmes for the application of expert systems, particularly in the processing of alarms. Even though it must be admitted that creating the basic expertise is a lengthy task, what is at stake is so important that it appears to be worth a major investment.

We have reached the conclusion. It is clear that to oppose logic controller and man would be to seriously misunderstand the problem. The complementarity is obvious. Two delicate questions remain to be solved:

- First is to determine who is to be the head of the "man and logic controller family". Equality is unthinkable in view of the difference in aptitude, not to mention sensitivity. Man's sensitivity is broader. He draws more experience from events he has experienced. He is capable of anticipating. It is thus normal that he should be the "conductor" and plays the role "guide" vis-à-vis the logic controller.
- Second is how a balance can be struck between man and logic controller. As man is destined to be the "conductor" he must conserve an overall view of the "musicians" and the "music" played by each — even if at times he is a musician like the rest of them.

The logic controller, active and reliable servant or servile operator's assistant, must be restricted to a role which the operator can easily circumscribe. One logic controller can regulate a given function while the operator supervises the system. Another can be used to automatically carry out a given sequence etc. If the logic controller is to find a place in this world which is based on human laws, it must act as a human would and not as a master controller with a complex and mysterious role. We believe that considerable progress remains to be made to obtain a happy marriage between man and logic controller. In this marriage, the operator must rise to the situation. As head of the family, he must understand and control the actions of his partner. He must be trained and experienced in this task.

Competent operators with logic controllers assigned to global identifiable tasks, this in short is what appears to be the key to success.

**CURRENT PHILOSOPHY IN FRANCE REGARDING THE  
REQUIRED LEVEL OF AUTOMATION IN  
NUCLEAR POWER PLANTS AND ITS RELATIONSHIP  
WITH THE ROLE OF THE OPERATOR**

J.M. LECKNER  
Electricité de France,  
Paris-La Défense,  
France

**Abstract**

Automation is an essential feature of NPPs. The degree of automation can be seen to be increasing, owing to technical and social factors, but also as a result of advances in information technology. Deciding upon the appropriate level of automation, the allocation of functions to man, or to a machine or a combination of both may be one of the most critical aspects of NPP design.

The paper describes the desired balance of automation in nuclear power plants and the required relations between man and a machine on a basis of EDF's experience.

The main actors in the operating management process have to be humans; automation can only assist and provide an additional help in situations where human actions are less efficient. In this way, automated systems could become valuable tools and this is the basis of EDF's current developments.

At the last meeting of the consultative group, Mr. Colas developed preliminary concepts on the subject we are addressing today. It is not my intention to repeat these concepts in detail, but to describe some of them through two specific points.

- The first consists of a table comparing the main human and machine functions.
- The second involves three examples of automation applications studied by EDF.

Lastly, I would also like to describe EDF's current thoughts and ensuing activities on a national level concerning the desired balance of automation in nuclear power plants, and the required relations between the two players: man and machine.

To start, we should ask a question: what is our current state of knowledge on this subject?

Results based on experience are limited. To assist us in choosing the desired balance, we have only limited data available, which furthermore has been known to us for quite some time. I doubt that this holds anything new for you.

- **The first set of data shown in Tables 1 is the result of work carried out mainly by Chapanis and Woodson in the USA and Montmollin in France. The table below shows the strong and weak points in both human and machine functioning.**

Part one shows the main human functions concerning data perception. By analogy, this important feature of human functioning has also been attributed to machines.

Table 1 - Part 1

FUNCTION	HUMAN CHARACTERISTICS	MACHINE CHARACTERISTICS
DETECTION (i.e., perception of stimuli, signs and signals)	<ul style="list-style-type: none"> <li>- Stimulus scale limited by senses</li> <li>- Detects very low intensity stimuli</li> <li>- Relatively good sensitivity</li> <li>- Easy to reprogram filtering</li> </ul>	<ul style="list-style-type: none"> <li>- Very extended stimulus scale</li> <li>- Detects low intensity stimuli with difficulty</li> <li>- Excellent sensitivity</li> <li>- Hard to reprogram filtering</li> </ul>
DISCRIMINATION (i.e., ability to differentiate perceptions, recognize them and file by category)	<ul style="list-style-type: none"> <li>- May span a rather wide range of physical dimensions</li> <li>- May use a rather low S/N ratio</li> <li>- Poor channel capacity</li> <li>- Stored high complexity models</li> <li>- Consistency of shape perception (e.g. perspective)</li> <li>- Perception of depth and relief</li> </ul>	<ul style="list-style-type: none"> <li>- Spans only a very narrow range of physical dimensions</li> <li>- Cannot generally use a low S/N ratio</li> <li>- Large channel capacity</li> <li>- Stored models with potentially very high complexity</li> <li>- Very low perception consistency</li> <li>- Problematic perception of depth and relief</li> </ul>
INTERPRETATION (i.e., ability to give a meaning to signals or data and to vary such meanings)	<ul style="list-style-type: none"> <li>- Very high programming and reprogramming flexibility. Self-learning is possible (experience). Modification of codes during thinking process ("invention")</li> <li>- Can handle incidents, even when completely unexpected</li> <li>- Code and language memory: unknown but virtually unlimited</li> <li>- Can use redundant information, organize fragments of information into significant "wholes", which are interconnected</li> <li>- Induction and generalization capability</li> <li>- Reasoning: imprecise, but can use short cuts</li> </ul>	<ul style="list-style-type: none"> <li>- Low reprogramming flexibility. Rigid codification. Limited self-learning (experience). Very limited "invention" capabilities.</li> <li>- Handles incidents with difficulty</li> <li>- Very good memory of codes and languages</li> <li>- Very limited organization of perception</li> <li>- Incapable of generalization and induction</li> <li>- Very accurate. Cannot use short cuts</li> </ul>

The second part of this table shows functions that may be classed as data processing.

Table 1 - Part 2

FUNCTION	HUMAN CHARACTERISTICS	MACHINE CHARACTERISTICS
CALCULATION	- Slow and imprecise	- Very fast and accurate (for integration and differentiation in particular)
STIMULUS-RESPONSE - COUPLING	- Can adapt several types of response to a given stimulus - Relatively slow and unstable reaction time	- Can adapt only a limited number of responses to a given stimulus - Fast and stable reaction time
RESPONSE	- Limited in terms of accuracy and power - Repeated, fast response hard to maintain	- Very extended in terms of both power and accuracy - Repeated, fast response easy to maintain

Lastly, the third part of this table lists what we consider as capabilities.

Table 1 - Part 3

FUNCTION	HUMAN CHARACTERISTICS	MACHINE CHARACTERISTICS
AUTONOMY	- High movement and maintenance autonomy (homeostasis)	- Very low movement and maintenance autonomy
RELIABILITY	- Rather low - In particular, subject to variations over time	- Can be excellent - Generally constant
PERFORMANCE DURATION	- Short, if breaks are not arranged (tiredness). But capable of "super-performance" (stress)	- Unlimited: requires only limited number of breaks. Not capable of "super-performance"

This comparative data set is the only knowledge base available at present. Summarizing this data base allows us to create a second table in which each function is ranked according to whether humans or machines are more efficient. Table 2 below shows the results of this comparison.

Table 2

## OVERALL COMPARISON BETWEEN HUMAN AND MACHINE PERFORMANCE

Function	Human	Machine
Detection	+	-
Discrimination	+	-
Interpretation	+	-
Calculation	-	+
Stimulus-response coupling	=	=
Response	-	+
Autonomy	+	-
Reliability	-	+
Performance duration	-	+

However, this doesn't help us make real decisions as to allocation of tasks, except to show that, overall, humans are more gifted than machines.

Therefore, the first question we must ask ourselves is: what role should we assign to humans? In other words, who will be the main player in a given situation? What level of autonomy will he/she have? And who will be the master and who the servant?

We cannot design the working environment of the future without having a reliable answer to these questions. This is a serious problem not only for designers, but also for us, as operators.

I have drawn some examples concerning this key subject from our maintenance and operating situations. All these situations have been designed to assist the operator in his work, by improving the operating environment, or by simplifying his unit operating strategies.

I would like to describe three types of situations.

The first is the periodic testing of reactor protection systems.

Following many incidents of human error during these tests, a decision was made to build an automatic device to improve the working environment. This automatic tester performs all test sequences except two that are still carried out by the operator.

The operator's role is primarily passive, except for the two manual sequences. The automatic tester verifies, processes and checks operating data (detection, discrimination, interpretation, calculation

and proposed stimuli and responses are handled completely by the automated system, as well as operating features such as reliability and operating time - see tables).

The test sequence now lasts two hours for each redundant A and B channel; before, it lasted 24 hours and two operators were totally responsible for the entire test procedure. Today, apart from the two sequences already mentioned, the operator's role consists in monitoring each sequence and authorizing the automated tester to pursue the test. (Tables 1 and 2 show that the only function remaining the sole province of humans, i.e., autonomy, cannot be fully achieved due to the absence of all other functions.

This is, however, a major improvement. After a period of satisfactory operation, different malfunctions once again occurred, largely during manually-operated test sequences. Analysis showed that the tester was being used by a new group of operators. The original operators were completely familiar with the test sequence and operated by extracting the necessary data as the test was performed. Due to various developments within the division and personnel transfers, these operators were replaced by new, less experienced personnel.

Because these new operators were totally inexperienced, and thus unfamiliar with the data used by the automated tester, they validated data after reading sequence results on the control screen. This lack of information and experience often led the new operators to working "blindly" and therefore making mistakes.

The second example is also taken from maintenance operations: repair of the automatic alternator voltage regulation system.

Following the installation of this system, electricians were often called upon to repair defective electromechanical equipment. First, however, they had to discover the cause of the failure. Initially, a large number of maintenance actions were required, but this gradually declined. Maintenance actions by specialists has now fallen to about 2-3 per year per plant.

As already mentioned, the maintenance workers' malfunction diagnosis capability has gradually been eroded. Since the operator has to be assisted in his work, a solution could lie in the design of an expert system. However, there is the question of data acquisition, and whether it could be used by the hardware designer at the beginning of the automation project. However, in this case I do not believe it is possible.

My last example concerns the use of computerized procedures.

A program of design principle evaluation has been compiled within the framework of work on the future control room for the 1,400 MWe PWR series. In both operational and ergonomic terms,

evaluation focused on the suitability of the concept of a computerized control room for all operating situations encountered in nuclear power plants. The evaluation program was spread over a four-year period. Results have been integrated by the manufacturers of the future Chooz B plant, which is due to enter service in early 1993.

One of the main results of the evaluation involves the use of computerized procedures. In most operating situations, except accident conditions, little use has made of these aids. Operators usually resorted to conventional illustrations, which enabled much greater autonomy in terms of operating strategies. The use of these procedures, especially during night shifts, gave operators an "economic" means, in psycho-physiological terms, of managing situations as they arose.

During accident situations, design requirements stipulate that physical states operating procedures have to be used. This entails strict sequence flow and chaining. When this happens, operators have to concentrate totally on information displayed on the screen, which limits communications between the two operators. Activities then focus essentially on data exchange management and the control facilities on the control panel, thereby limiting capacity to detect anomalies should an unforeseen event occur.

**Sometimes in incident situations, when operators focus less on the screens, certain actions are forgotten because they are not mentioned in the operating procedures.**

The problem remains the same: how will operators react in the event of unforeseen circumstances, and how efficient will they be?

## **Conclusion**

Should operators simply be considered as managers?

In this case, computerized procedures assume major importance and no departure from these procedures can be permitted. The computer interface must take priority over human activities -- resulting eventually in a gradual loss of knowledge and experience. In the event of a complicated, new or unexpected situation, human skill will not always be immediately available.

Skill represents the accumulation of knowledge, human procedures and reasoning modes needed to define operating strategies.

It is also an assembly of structures which are available and appropriate for accomplishing complex, ever-changing tasks. Skill enables operators to anticipate events and adjust the task sequence accordingly.

Or would it be more appropriate to consider operators as a controller responsible for the installation? If this is the case, computerized tools become operational aids and offer additional support for the reasoning behind, and definition of diagnostics.

EDF is currently tending to place humans back in the driver's seat, although this depends on skills, experience and professional qualifications. This implies that special attention must be paid to training. Indeed, perhaps present qualifications ought to be developed in order to adapt to new levels of automation. I believe that this is essential for quality work and high safety levels. The main actors in the operating management process have to be humans; automation can only assist and provide additional help in situations where human functions are less efficient. In this way, automated systems could become valuable tools and this is the basis of our current developments.

## COMMENTS ON THE BALANCE BETWEEN AUTOMATION AND HUMAN ACTIONS

Y. SHINOHARA

Department of Reactor Engineering,  
Japan Atomic Energy Research Institute,  
Tokai-mura, Naka-gun, Ibaraki-ken,  
Japan

### Abstract

During past two or three decades many of industrial plants have become more and more large-scale and complex, which was possible by the enhancement of automation of their operation. However, very rapid increase in the scale and complexity of the plants sometimes caused accidents; sometimes by failure of automatic system hardware or software and sometimes by operator's error.

Since the status and general trends in Japan related to this problem has already been reported in the previous meeting on the subject, the paper gives very briefly some general comments on this problem based on the practical experience with the development of computerized control system for a large-scale test facility constructed at the Japan Atomic Energy Research Institute (JAERI) in which the Reactor Control Laboratory has participated with special attention to its man-machine interface design.

The balance between the automation and human action in the operation of complex plants depends on various factors such as technological, economical, ergonomical and societal factors which are more or less mutually interrelated and may vary with time. Since hardwares of the automated system may fail and men may make errors, the level of automation should be determined by taking all these factors into consideration so that it may be welcome by the operators as well as by the society. In this connection, more research must be made to investigate an appropriate guideline for determining proper level of automation of complex plants having large potential risks.

### 1. Introduction

During past two or three decades many of industrial plants have become more and more large-scale and complex, which was possible by the enhancement of automation of their operation. However, very rapid increase in the scale and complexity of the plants sometimes caused accidents; sometimes by failure of automatic system hardware or software and sometimes by operator's error.

The operator's errors in such complex plants were often found to be due to the mismatch between the man and machine in the complex man-machine system, which gave rise to the important problem of the balance between automation and human actions in their operation. This problem is more important for such plants having large potential risks as nuclear power plants because a severe

accident in such a plant may cause not only large economic loss to the plant owner but also serious damage to the society and natural environment.

Since the status and general trends in Japan related to this problem has already been reported in the previous meeting [1,2], in the following will be given very briefly some general comments on this problem based on the practical experience with the development of computerized control system for a large-scale test facility [3] constructed at the Japan Atomic Energy Research Institute (JAERI) in which the Reactor Control Laboratory has participated with special attention to its man-machine interface design.

## 2. Automation and Operator's Role

Whether a plant is to be operated manually or automatically, for the plant to be controlled safely, it may be stated using the concepts in the control theory in a broader sense that the plant together with its control system should always satisfy such necessary conditions as the observability, controllability and identifiability for all the plant variables and parameters which are related to the safety, as is conceptually illustrated in Fig. 1.

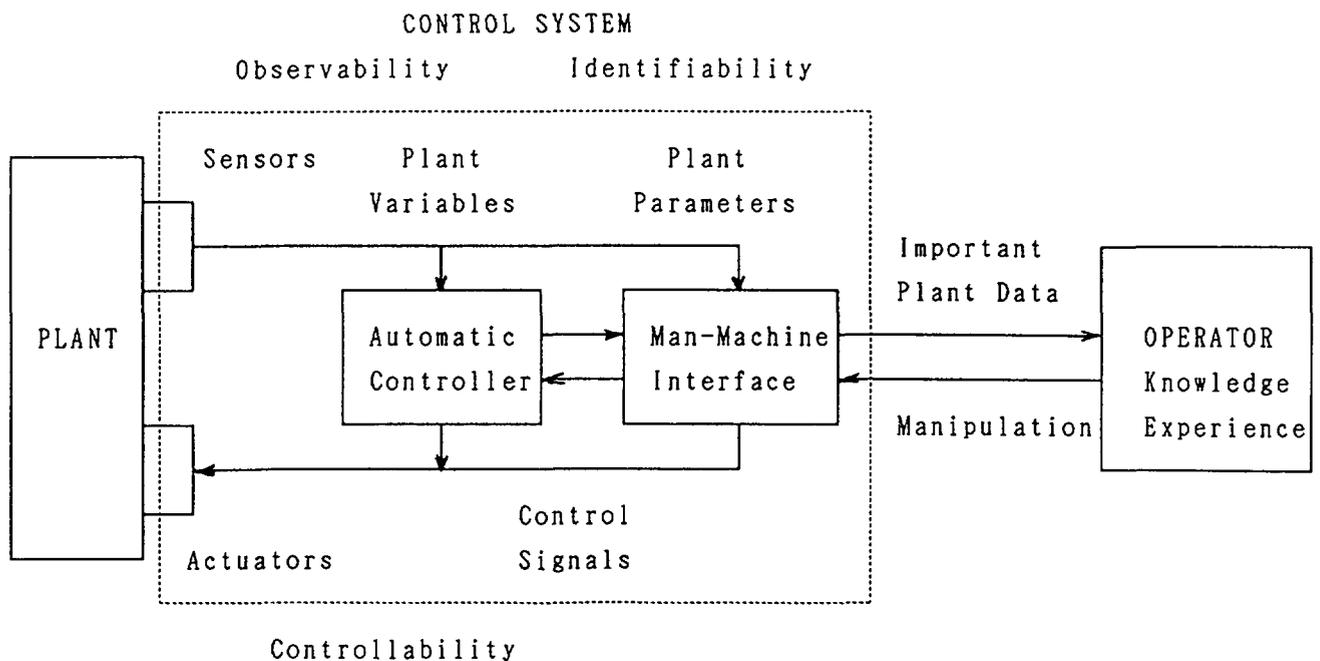


FIG. 1. Control system and operator.

Although these concepts are natural and have been formulated mathematically within the framework of linear system theory, it is not always easy to ascertain them when the real plant becomes a complex non-linear system because these conditions will generally depend upon the state of the plant in non-linear systems. For example, the Chernobyl accident can be considered as a typical case of loss of the controllability condition where the reactor was brought to a state outside of its controllable region.

In a complex plant, the number of variables which must be monitored and controlled generally becomes so large that it is indispensable to automate as many of monitoring and control functions as possible in order to assure safe and efficient operation of the plant by organizing the overall control system in a functional hierarchy. The more the plant operation is automated, the more the role of the operator shifts from performing lower-level control function to managing upper-level supervisory function, as is seen in many of highly automated complex industrial plants. This shift of the operator's role gave rise to various new problems in complex man-machine systems.

Because the automated control functions including protective functions can be designed only for the plant state which can be foreseen in the design stage, the operator must intervene in the control function when the plant state is brought outside of the region which is covered by the automated system. Since such a case is rather rare in a well designed automated system, such problems arise as whether or not the operator can make proper decision in a rare situation which he has seldom experienced and whether or not it is better to keep the level of automation not so high that the operator may experience more frequently how to manage manually the abnormal situation of the plant.

### 3. Factors Affecting the Balance

The extent to which a plant operation can be or should be automated depends upon many factors such as technological, economic, safety, ergonomical and societal factors as is illustrated in Fig. 2.

The technological factors include such items as the knowledge about the physical mechanism and operational characteristics of the plant, the reliability of hardwares and softwares necessary for automation of its operation and

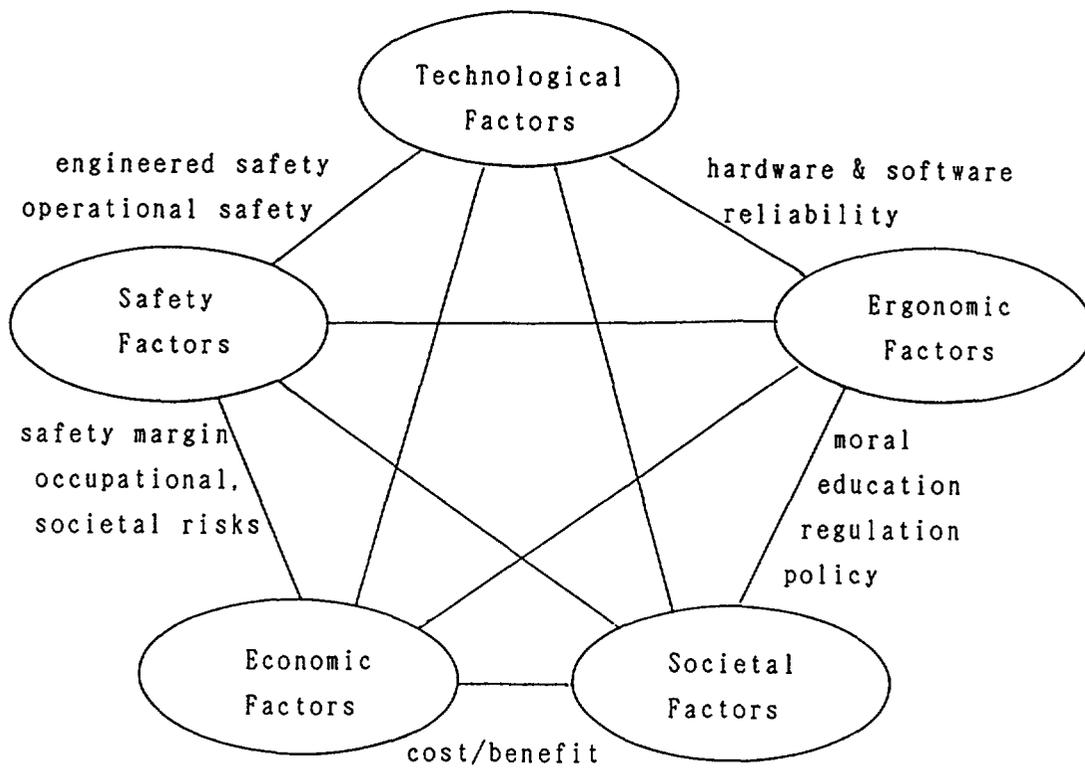


FIG. 2. Factors affecting the balance.

are closely related to the safety factors. For example, if the reliability of the available hardwares and/or softwares to be used are not sufficiently high, the level of the automation of the plant operation should be limited to such a level that the failure of the automatic system does not affect directly the safety of the plant.

The safety factors includes such items as the safety margin, engineered and operational safety, occupational and societal risks. The safety of the plant is directly related to the economic factors since an accident in the plant may cause a serious economic loss.

The economic factors include the cost of the hardwares and softwares for automating system operation and the benefits gained by automation such as improvement of plant productivity and man-power saving.

The ergonomic factors include physiological factors such as the average information processing speed, reaction time and fatigue characteristics of human being and the psychological factors such as the mental stress and moral of an operator or a group of operators. These factors are the most influential ones to the problem of balance between automation and operator action.

The societal and institutional factors include such items as tradition, policy, regulation, education and moral which may have influences also on the psychological factor of operators.

The above mentioned factors are more or less mutually interrelated and variable. Therefore, the answer to the problem of balance between automation and human actions may also vary with time. Since the technological and economic factors may change much rapidly than the societal and ergonomic factors, a plant whose operation was considered difficult or inappropriate to be fully automated a few years ago due to lack of adequate knowledge about the plant performance and of the related technology might be automated almost fully with today's advanced technology and accumulated knowledge.

#### 4. Case of HENDEL Plant

The large-scale test plant HENDEL (Helium Engineering Demonstration Loop) constructed at the JAERI is a non-nuclear facility for testing various high temperature components at the maximum helium gas temperature of 1000 C for the development of high temperature gas-cooled reactors and has a complex structure consisting of many subsystems. In designing this plant which must be able to be operated flexibly as the test facility according to various test programs, it was decided to develop a fully computerized control system to facilitate its operation.

The basic design philosophy of this computer control system was that its man-machine interface should be organized in such a way that it is rather simple in appearance and the whole plant can be operated easily even by a single operator. Here the role of the operator is mainly to supervise the plant status, to input the temperature program for the test and to change the control settings and parameters when required. It was then taken into consideration the operators who have been accustomed to the conventional analog control system but had no prior experience with any digital computer control system. Therefore, the man-machine interface was designed through discussions with technical staffs and operators concerned.

The control system was designed as a two-level hierarchical computer control system consisting of a minicomputer for the upper-level centralized supervisory control and several microcomputers for the lower-level distributed local closed loop controls. The control system performs all necessary control

functions including diagnostic and protective functions. In addition to these computers, microprocessor-based backup controllers having analog type man-machine interfaces were also provided for critical control functions in order to enhance overall control system reliability.

To make the man-machine interface as simple and compact as possible, it is composed of the CRT display units and a mosaic panel with a mimic diagram for plant status monitoring, the push-buttons for plant operation and information selection and the alarm annunciators. The operational status of the plant can be displayed numerically and graphically on each CRT display unit by selecting a desired one from a set of screen menus.

In the graphical display of process values are used basically familiar types of graphs such as bar-chart and trend recorder as well as mimic diagrams with indication of the associated numerical values. Alarm informations are automatically displayed on CRT display units in the predetermined locations irrespective of the selected menu. Suppression of redundant and less significant alarm informations is taken into consideration in order to avoid the operators' confusion which may be caused if too many alarms are generated at one time.

A large mosaic panel with a mimic diagram of the whole plant is also used to facilitate the operator's recognition of overall plant status since the CRT screen is not large enough for displaying such a mimic diagram and also the operators who have been accustomed to the conventional type of control panel expressed some anxiety in using only CRT display units. On this panel are displayed primarily ON or OFF states of the principal components.

For the purpose of plant operation and information selection, specially arranged boards of push-buttons for easier access to various control functions are mainly used although standard key boards of computer terminals can also be used for parameter modification and so forth.

Successful operation of the HENDEL during past eight years since 1982 without any trouble due to its automation shows that the fully computerized control system of the HENDEL plant with properly designed man-machine interface was favorably accepted by the plant operators who had no prior experience of using such a computerized man-machine interface.

Even the operators who expressed some anxiety of using a new type of man-machine interface could become accustomed to it more quickly than we

expected. Younger operators had no difficulties and are rather pleased to use such a computerized system. Although the control system is so designed that the plant can be operated by a single operator, it is actually operated by four operators from administrative rather than technological reasons.

#### 4. Conclusion

Based on the historical trend of automation technology in many of industrial plants and our successful experience with a fully computerized computer control system for a test plant which has been being operated for eight years, it is concluded that modern high technology provides us the possibility of enhancing the safety and economy of operating complex plants by introduction of properly designed automatic systems.

However, the balance between the automation and human action in the operation of complex plants will depend on various factors such as technological, economical, ergonomical and societal factors which are more or less mutually interrelated and may vary with time. Since hardwares of the automated system may fail and men may make errors, the level of automation should be determined by taking all these factors into consideration so that it may be welcome by the operators as well as by the society. In this connection, more research must be made to investigate an appropriate guideline for determining proper level of automation of complex plants having large potential risks.

#### References

- [1] Nakamura, K.: Current Status and Future Prospects on Balance between Automation and Human Actions in Japanese Nuclear Power Plants. Paper presented at the Advisory Group Meeting, 1989
- [2] Tanabe, F.: The Development of an Autonomous Nuclear Power Plant under the Nuclear Frontier Research Policy in Japan. Paper presented at the Advisory Group Meeting, 1989
- [3] Fujii, Y. et al.: Design and Operational Experience of the Man-Machine Interface of a Fully Computerized Control System. IAEA Conf. Man-Machine Interface in the Nuclear Industry, IAEA-CN-49/27, Tokyo, 1988

# STUDIES ON THE PROCESS OPERATORS' WORK AND CONTROL ROOM DESIGN IN SWEDISH NUCLEAR POWER PLANTS

G. OLSSON  
Uppsala University,  
Uppsala, Sweden

## Abstract

The Swedish nuclear power programme comprises 12 plants, 9 BWRs and 3 PWRs, taken into operation during the period 1972 - 1985. During this period there has been a remarkable development of the control systems. The level of automation has been risen and computer systems have been installed for process information support to the operators. Though all systems and subsystems have been carefully evaluated before implementation, also from a human factor's point of view, no evaluation has been done of the effects of computerization and automatization on the operators' tasks and jobs in a more holistic sense. From a human reliability point of view it is still an open question whether or not the changes in technology have improved operation safety.

The paper presents some results of the study, the main purpose of which is to analyze this question by comparative studies of the operators' work and working conditions in the 12 plants. In a first phase a comparative study is made of the oldest and the newest BWR plants, Oskarshamn 1 (O1) and Oskarshamn 3 (O3).

## Background and purpose of the study

The Swedish nuclear power programme comprises 12 plants, 9 BWRs and 3 PWRs, taken into operation during the period 1972 - 1985. During this period there has been a remarkable development of the control systems. The level of automation has been risen and computer systems have been installed for process information support to the operators. Though all systems and subsystems have been carefully evaluated before implementation, also from a human factors' point of view, no evaluation has been done of the effects of computerization and automatization on the operators' tasks and jobs in a more holistic sense. From a human reliability point of view it is still an open question whether or not the changes in technology have improved operation safety. The main purpose of the study is to analyze this question by comparative studies of the operators' work and working conditions in the 12 plants. In a first phase a comparative study is made of the oldest and the newest BWR plants, Oskarshamn 1 (O1) and Oskarshamn 3 (O3).

## Research approach

In the conceptual framework of the study human reliability is seen as a dependent factor of educational, organizational, and technical characteristics of the total work system in a power plant and must be studied by analyses of the operators' behaviour in, experiences from, and attitudes to their tasks and jobs. Operators are seen to be not single individuals but members of the shift team working in the control room, i.e. one shift supervisor, one reactor operator, one turbine operator and two station technicians. The research design can be illustrated by figur 1.

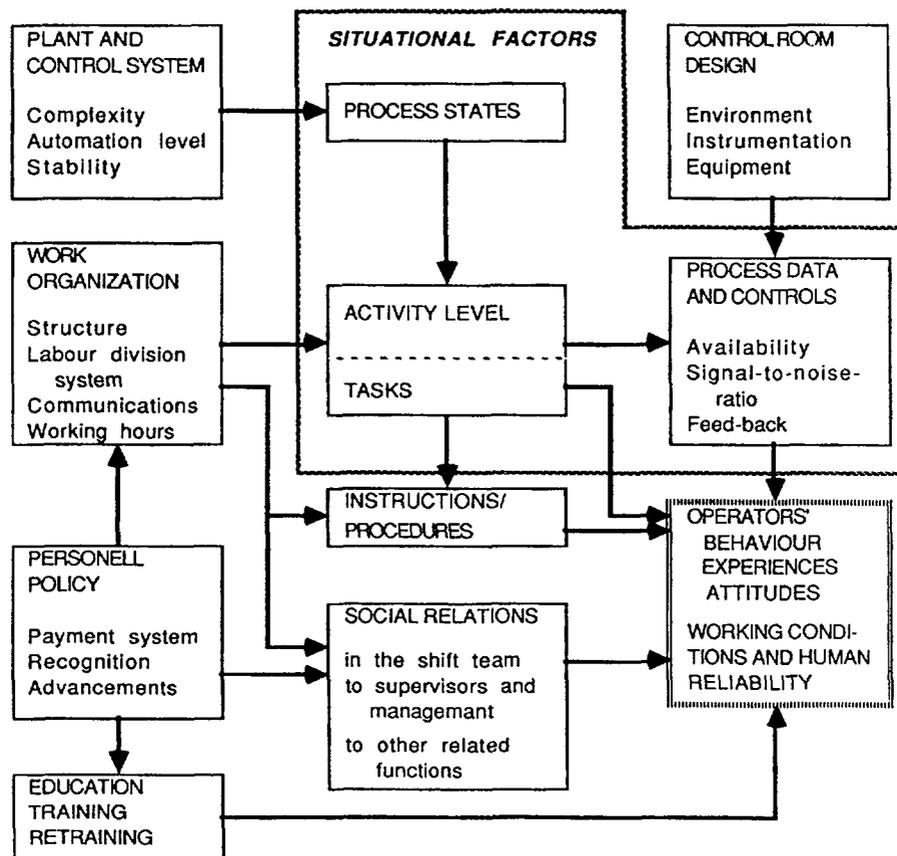


Fig. 1. Research model for comparative studies of NPP operators' work.

The tasks of the operator team are to a large extent determined by the plant and control system design and can be classified in relation to variations in the process states. How different tasks are shared by the individual operators in the team is determined by the work organization and the formal labour division system. Operational characteristics of the plant and the control system combined with structural organizational factors are taken as determining factors for *what* the operators are supposed to do, i.e. their tasks, but also as determining factors for variations in activity level for the operators. Activity level and its variations are seen as an important determining factor for the operators' mental load and opportunities for skill utilization and retention. Thus, activity level is one factor determining *how* the operators can solve their tasks.

Other how-determining factors are qualification status of the operators, partly determined by education, training and retraining programmes, design and application of job instructions and procedures, and the control room design.

Considering the huge amount of displays and controls in a NPP control room, classical ergonomic thumb rules for control room design have a limited application. An evaluation of control room design must therefore be related to different tasks, especially critical tasks from a safety point of view, from which the process information needed can be derived. How computers are utilized in this context for filtering and organizing process information is of a special interest in the study.

## Methods and data collection

The studies are performed as case studies of the plants. Each case study is started up by direct observations in the control rooms followed by individual interviews of selected operators. Based on the results of these interviews questionnaires are designed for a survey of all operators. Interviews and questionnaires cover items like education and training/retraining, experiences of the control systems and the control room design, experiences from tasks at different process states, job instructions, work organization and social relations.

Frequency and duration of different tasks are studied by work sampling and activity charts supplemented by data from documents on regulated and periodic tasks like testing, logging etc. Together with data from operation reports these data are used for analyses of activity level variances.

Some critical tasks (transient handling) will be selected for task analyses and for studies in full scale simulators, where operators' behaviour in problem solving will be observed and recorded.

Other review methods will be used for analyses of work organization, instructions and procedures, and control room design.

## Results

The data collection started up in spring 1988 by direct observations in the two control rooms followed by operator interviews during autumn 1988. During the winter 1989-90 a questionnaire survey of all operators in O1 and O3 has been performed. Data from the interviews and the questionnaire survey are still being analyzed and at present no detailed results can be presented. Preliminary results are, however, that the control system of the older plant is in most aspects favourable compared to the new plant as judged by the operators.

# ANALYSIS OF THE MAIN FACTORS DETERMINING THE DEGREE OF AUTOMATION IN NPPs

M.N. MIKHAILOV

Research and Development Institute of  
Power Engineering,  
Moscow, Union of Soviet Socialist Republics

## Abstract

The "man-machine" interaction plays an important part in developing such complex installations as Nuclear Power Plants (NPP). Special attention was focussed on this problem after accidents in "Three-Mile-Island" and Chernobyl NPP.

Inspite of the great efforts and resources that are consumed in this area, the formalized methods and approaches to achieve the optimal balance between the automation and human actions are absent up till now. The decisions being made depend, to a great extent, on the designers skill. Such a situation is explained by the integrated approach to the problems, the need to allow for a great number of factors both quite apparent and indirectly influencing.

The paper describes the main factors determining the degree of an automation on NPP:

- specific features of concrete NPP;
- safety;
- personnel dose rates;
- general situation in the NPP automation area;
- economic performance and social consequences.

## 1. INTRODUCTION

The "man-machine" interaction problems play an important part in developing such complex installations as Nuclear Power Plants (NPP). Special attention was focussed on this problem after accidents in "Three-Mile-Island" and Chernobyl NPP.

Inspite of the great efforts and resources that are consumed in this area, the formalized methods and approaches to achieve the optimal balance between the automation and human actions are absent up till now. The decisions being made depend, to a great extent, on the designers skill. Such a situation is explained by

the integrated approach to the problems, the need to allow for a great number of factors both quite apparent and indirectly influencing. Note, that all these factors exert strong influence on each other, so variation in one of the factors results in variation of most of them. From this it follows the iteration design method that permits to run the whole design process or its separate stages over and over again. As a result of such design process, it is apparent that it is impossible to obtain an optimal function distribution version and the more or less satisfactory agreement is achieved. The most important condition of the rational version is the test of decisions at different simulators: from the functional and engineering simulators to full-scale ones - testing the appropriate stages and parts of the project at each of simulators.

## 2. MAIN FACTORS DETERMINING THE DEGREE OF AUTOMATION ON NPP

### 2.1. Main factors Contents

Fig.1-6 illustrates the contents of the main factors determining the degree of automation on NPP. Below is given the appropriate comment.

### 2.2. Specific Features of concrete NPP

The "inherent safety" level is one of the important characteristic of a nuclear reactor, i.e. the features intended to ensure safety on the basis of natural feedbacks and process (self-control, thermal inertia, etc.). Physical and dynamic characteristics (power density, transient time, instabilities nature in the reactor, etc.) are closely related to these

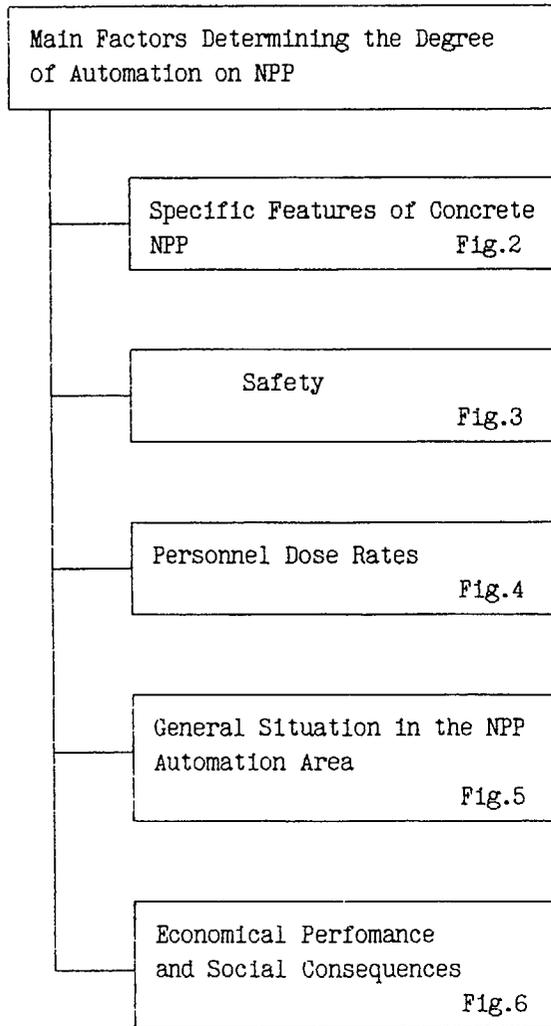


Fig.1

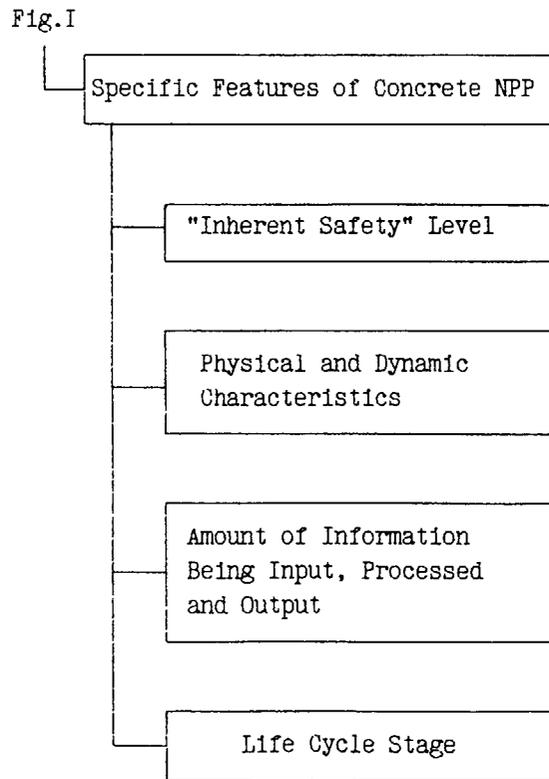


Fig.2

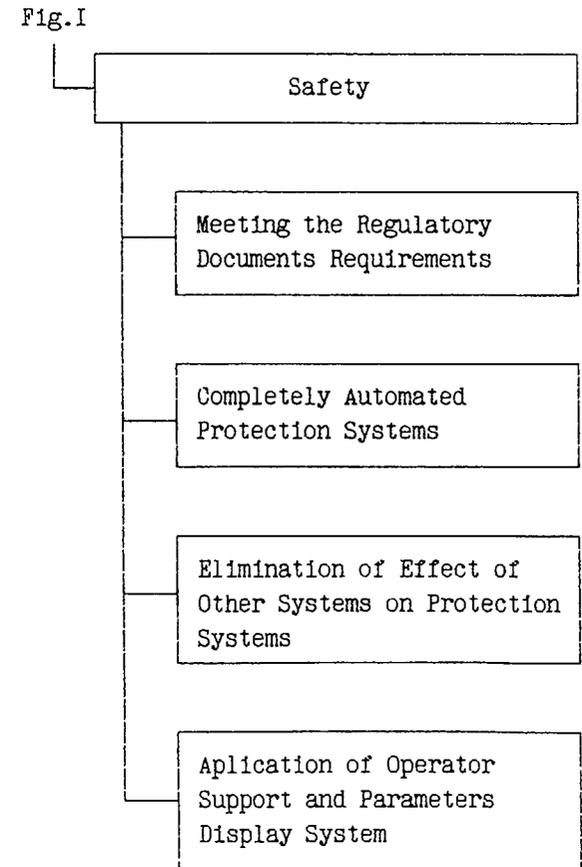


Fig.3

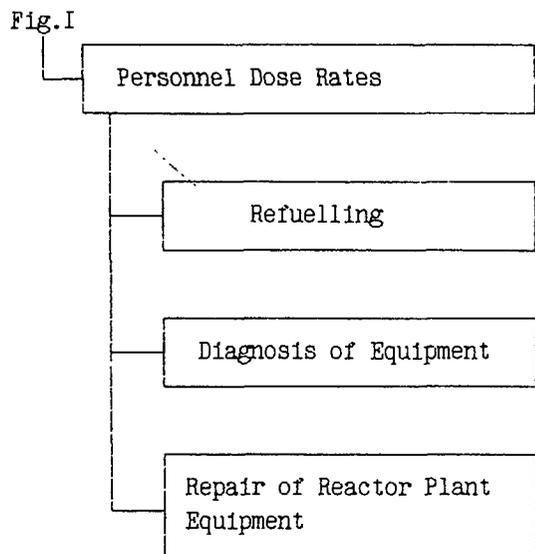


Fig.4

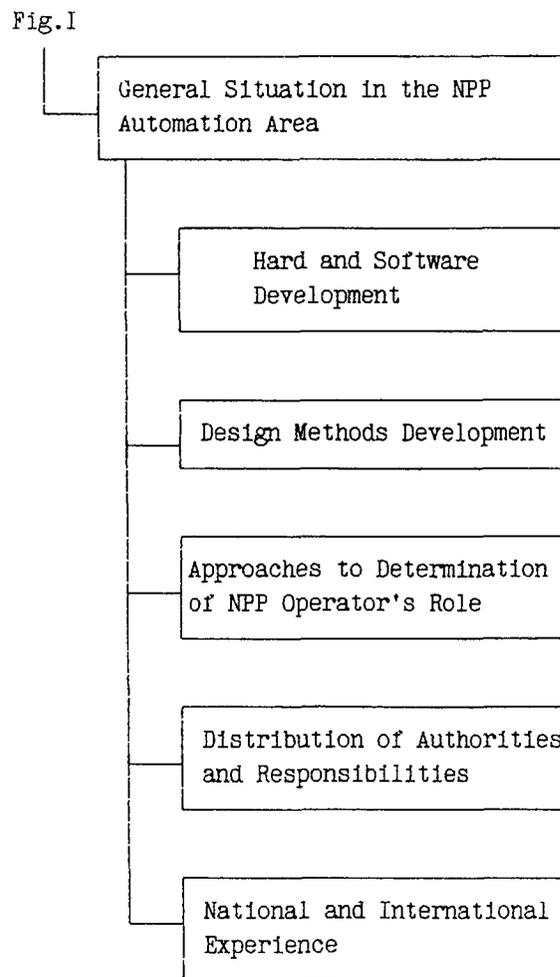


Fig.5

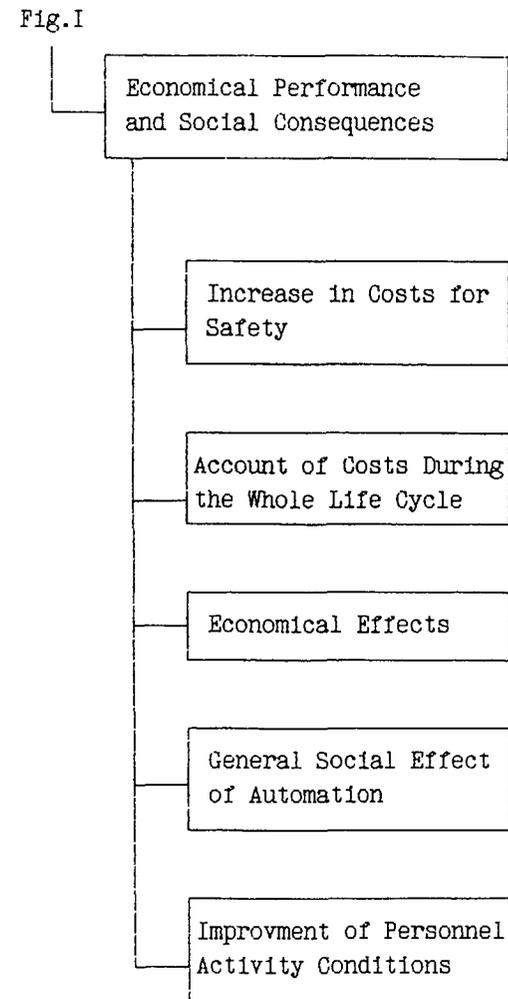


Fig.6

features. It is apparent that the more "stringent" characteristic's result in need for higher automation degree, for example, to calculate the power density and temperature distributions in the reactor, linear power load on fuel elements, to introduce the multizone local automatic regulators, etc.

The increase in power and complexity of the NPP results in significant increase in amounts of data processed as well as the amounts of channels for measuring and controlling the actuators. The amount of detectors of different types in the up-to-date units may exceed 10000, the amount of the actuators - over 1000 and that of calculated values - tens of thousands, some of which should be output to the NPP operative staff. The need for significant automation of the data input and processing functions, for control action generation, etc., is resulted from it, with the compulsory self-testing and diagnostics of these processes to minimize the probability of error occurrence.

The solution of problems on level of automation depends significantly on a life-cycle stage of the NPP that should be automatized - the NPP being designed anew, in operation or under significant reconstruction. As the experience has shown, the most significant variations in distribution of functions between the automation and human actions come about in designing the NPP of new generation which is usually related to the variation in power and in the reactor type. There are few possibilities for the NPP being under operation. In these cases they are usually limited by insignificant modernizations directed towards the elimination of detected errors or towards the innovations that don't require the significant alterations.

As far as the reconstructed installations, the designers and operational staff are usually choosing for the best solutions which is the agonizing process for them, as, from the one hand,

there is the potential possibility to introduce a lot of innovations, especially with due account of the experience gained and from the other one - there are a huge number of limiting factors such as: a need to reconstruct the installation facilities, high cost, limitation of reconstruction period, etc. So, more often it is to be develt on the compromise version being not such a progress as it could be in case if the same NPP was constructed anew. Moreover, the experience shows that those modern decisions that are made at the NPP being under construction within several years following the construction of the previous one of the same type, can be very seldom used at the power units constructed previously. One of the important conclusions that can be made on the basis of the aforesaid, resides in that the designers should allow for the possibility of the control systems evolution.

### 2.3. Safety

The main NPP safety regulations are described in the appropriate national Regulatory Documents (e.g. "General Safety Regulations for the NPPs" in the USSR /1/). It is obvious that the NPP control should be provided in such a way to meet the requirement of the above-mentioned documents. From the point of view of balance between the automation and human actions it is advisable to highlight the most important regulations for the NPP safety.

The protection systems should be completely automatic with the introduction of the technical means for preventing the human intervention into the actions of these systems within 10-30 min, as well as with the developed self-diagnostics that permits to detect the hazardous failures.

The designers should guarantee that control and monitoring systems do not affect the safety systems. It can be achieved both by the technical means and organizational measures.

The use of the operator support systems including those of on-line display of current safety parameters to the personnel is a compulsory condition.

Thus, the above-mentioned requirements together with some ensuing particular consequences dictate the designers to make a lot of decisions on distribution of functions between the automation and human.

#### 2.4. Personnel Dose Rates

The operating staff performing several types of operations and maintenances related to the normal NPP operating modes can be irradiated. Such type of works are as follows:

- refuelling, including in the operating reactor (e.g. such an operation can be performed up to several times per day in the RBMK-type reactors);
- state diagnostics of pipelines and other equipment;
- reactor and primary equipment repairs.

In all above-mentioned cases the designers and customers are facing a difficult optimization problem on distribution of functions between the machine and the human. The economical and social factors are evidently played an important part. The experience shows that more often the compromise decision is the use of manipulators or other remotely manipulated equipment rather than completely automatic robotics. The refuelling equipment for the RBMK reactors as well as remotely controlled equipment for the pipeline integrity surveillance may serve as an example. Note, that this equipment has its own control systems that help the

operating staff to monitor the process, to control it and to perform the data processing.

## 2.5. General Situation in the NPP Automation Area

Undoubtedly, that such factors as: progress in equipment and design methodology developments, approaches to the definition of personnel role, distribution of authorities and responsibilities and the gained national and international experience have a strong impact on the solution of problems on distribution of functions between the automation and the human.

Rapid progress of electronics and information technologies permits the designers to broaden and extend the automation functions continuously. The modern hardware may exhibit a certain "intelligence" due to the application of programmable facilities, has high reliability and the developed self-diagnosis means with the acceptable costs, dimensions and other characteristics. The example of the actual application of the software and hardware development result are

- protection systems realizing more complex algorithms and taking into account the power distribution by the core volume;
- operator support systems including the use of expert systems;
- systems to decrease the redundant information that implement the different algorithms for the data flow abridgement including during the accident conditions.

The design methods are eventually developed step by step. Simulation is a powerful mean permitting to distribute the functions between the automation and human more rationally.

In this case the simulators of different types can be used, they are as follows: functional, engineering, full-scale, etc.,

each of which is intended to perform the appropriate tasks but all of them provide the solution of complex problem.

The personnel activity concept is one of the principal moments in distributing the functions between the automation and the human. There are two approaches in determining the operator role which can be referred to as "passive operator" and "active operator" concepts. According to the first concept all possible situations both under normal and abnormal NPP operating conditions are provided in thoroughly developed instructions and the operator should act in accordance with these instructions only. The second concept provides the presence of experienced operator who knows everything well and understands the processes that he controls. It can be explained by the fact that most experts point to the practical impossibility of providing for all probable situations with multiple nuances, so it is impossible to develop the instructions for all cases. However, it is clear, that the operator can effectively act if he has enough time i.e. if he has little time to react upon one or another situation, the automation may be the single acceptable way to perform the appropriate functions. Under such understanding of the operator role the problem of operator activity organization can not be considered as a problem of creating conditions to simplify his activity or to reduce the level of his skill and should become a problem of providing the possibilities for successful decision-making both under normal and abnormal operating conditions. It is important to provide such activity organization and such a level of the operator training when their presence increases the reliability to a greater extent than creates the accident risk. It is evident that the choice of one or other operator's role concept dictates the requirements for creating the appropriate operator training

system - professional choice, education, training, practical study, experience accumulation, readiness support, etc.

The problem on distribution the authorities and responsibilities between the designers and operating staff is closely connected with the operator's role concept.

This is a very complex juridical aspect of NPP automation that needs to be thoroughly analyzed. So, here we can outline the main thesis only.

As noted in the appropriate USSR Regulatory Documents the operator of the NPP provides its safety and bears full responsibility for it; moreover, this responsibility is not decreased due to the self-dependent activity and responsibility of other firms performing operations or offering services for the given NPP. In other words, full responsibility is always placed on the operating staff (operative, maintenance and managing staff), so there are authorities to make all operative decisions. At the same time it is evident that partial responsibility between the operators and designers is redistributed in the direction of increasing a partial responsibility of hardware and software designers, if automatic functions are increased.

The " safety culture" is connected with what has already been mentioned. As stated in the USSR Regulator Documents the "safety culture" is a skilled and psychological training of personnel when the NPP safety provision is a priority objective and an internal demand resulting in self-consciousness of responsibility and in self-monitoring while performing the operations that effect on the safety.

In a specific design the distribution of functions between the automation and human is based on the designers experience that is largely determined by the national achievements. Moreover, the NPP automation National standards are played an important role. At

the same time, the other countries achievements significantly effect both on the projects being developed and on the standards available. These standards are being constantly improved. Just so the international cooperation in the NPP automation area, as well as the exchange of experience, recommendations and standards development, etc. play an important role.

## 2.6. Economical Performance and Social Consequences

The economical and social factors for distributing functions between the automation and human are closely interrelated to any other factors, so below are given the general remarks. As the experience has shown both in the USSR and abroad, the cost to develop, manufacture and test the systems as well as the hardware and software as applied to NPP some times higher than those of other industrial projects. This is connected with the need for high quality, reliability and safety assurance as well as for implementation of complex and long-term licencing procedures in the Supervision Authorities.

It should be noted that the direct economical effect of increasing the level of automation is not always positive, since an increase in a number of automatic devices can result in an increase in total costs without an increase in process control quality and besides doesn't always result in reduction of a number of personnel. At the same time there are real examples, when the operation at nominal power is impossible without computer systems, as a human can not control the reactor without any parameters being calculated /2/. It is apparent that in such cases the increase in a level of automation is economically very effective. Note, that it is necessary to take into consideration the costs over the whole life cycle of the systems including the service,

development, modernization, replacement, etc. while calculating the economic indices.

The total social effect of automation is worthy of notice while considering the social consequences. As the experience shows, the public opinion is favourably disposed towards the increase in a level of automation, the use of computers, displays, etc. Moreover, the social factor has an effect on final decision-making whether such NPP should be constructed, in general, or not.

The conditions of the activity of NPP personnel are improved as the level of automation increases due to a decrease in number of routine and non-creative types of works, dose rate reduction while performing the operations related to the irradiation possibility, the promotion of some procedures requiring high physical efforts, etc. However, it should be particularly emphasized, that the human activity conditions can be sometimes complicated as a result of inadequately thorough development of the automation project. For instance, if to place a great number of displays at the control panel and to output all possible NPP data to them, the operator will not be able to make effective decisions, especially under abnormal conditions. It outlines the need for taking into account all interrelated factors on distributing the functions between the automation and the human.

### 3. CONCLUSION

The performed analysis of the main and allied particular factors that effect on the level of automation on NPP, shows that the problem of distribution function between automation and human action is very complex. All factors are closely related to each other and have an appreciable influence on each other, so the

designers should place more emphasis not only on what will be created as a result of the project realization but on how the design process is being performed.

The national experience of the designers play an important part. At the same time, the problem status in other contries effects significantly both on the position of the designers themselves and on that of the supervisory authorities. That is why the close international cooperation including the exchange of knowledge, development of standards, rules, recommendations and other types of documents play an important role.

#### REFERENCES

1. Общие положения обеспечения безопасности атомных станций (ОПБ-88). ПНАЭ Г-И-ОИИ-89. Москва, 1989.

2. An automated data system for the monitoring of RBMK-1500 reactors: current status and potential (IAEA-CN-49/98).

E.O.Adamov, P.A.Gavrilov, A.I. Gorelov, A.I.Efanov, M.N.Michajlov, N.A. Sazonov. Man-machin Interfase in the Nuclear Industry. IAEA, Vienna, 1988.

## LIST OF PARTICIPANTS

CANADA

Innes, L.G. (3)  
Atomic Energy Control Board  
P.O. box 1046  
Ottawa, Ontario, K1P 5S9

Olmstead, R.A. (1,2,3,4)  
CANDU Operations  
Atomic Energy of Canada Ltd  
Sheridan Park Research Community  
Mississauga, Ontario, L5K 1B2

FRANCE

Colas, A. (1)  
Département Exploitation du SPT  
Electricité de France  
13, Esplanade Charles de Gaulle  
F-92060 Paris-La-Défense

Leckner, J.M. (3)  
EDF/Nuclear and Fossil Generation Division  
Operations Analysis Section  
Humans Factors Group  
Quartier Michelet  
13-27, Esplanade Charles de Gaulle  
F-92060 Paris-La-Défense

Oudiz, A. (1,2)  
Département d'Analyse de Sûreté-IPSN  
Centre d'Etudes Nucléaires  
Commissariat à l'Energie Atomique, B.P. No. 6

GERMANY

Aleite, W. (1)  
Siemens AG-UB KWU  
P.O. Box 3220  
D-W 8250 Erlangen

Bastl, W. (1,2,3,4)  
Gesellschaft Für Reaktorsicherheit (GRS)mbH  
Forschungsgelände  
D-W 8046 Garching

JAPAN

Hiei, S. (1)  
Institute of Human Factors  
NUPEC  
Fujita Kanko Toranomom Bldg.  
3-17-1 Toranomom Minato-ku  
Tokyo 105

Kato, Y. (1)  
Hitachi Works  
Hitachi Limited  
3-1-1, Saiwa-cho  
Hitachi-shi, Ibaraki-ken 317

Nakamura, K. (1)  
Nuclear Power Safety Administration Division  
Agency of Natural Resources and Energy, MITI  
1-3-1, Kasumigaseki, chiyoda-ku  
Tokyo 100

	Shinohara, Y. Department of Reactor Engineering JAERI Tokai-mura, Ibaraki-ken, 319-11	(3)
	Tanabe, F. Human Factors Research Laboratory Department of Reactor Safety Research Tokai Research Establishment JAERI Tokai-mura, Naka-gun, Ibaraki-ken 319-11	(1)
<u>RUSSIA</u>	Kuzhil, A.S. I.V. Kurchatov Institute of Atomic Energy Kurchatov Square, 2 Moscow	(3)
	Mikhailov, M.N. Research and Development Institute of Power Engineering 2/8, Krasnosel'skaja 107113 Moscow	(3)
	Mitrofanov, B.N. All-Union Research Institute for NPP Operation Ferganskay 25 109507 Moscow	(1)
<u>SWEDEN</u>	Olsson, G. University of Uppsala, CMD S-752 23 Uppsala	(3)
<u>UNITED KINGDOM</u>	Boettcher, D.B. Nuclear Electric plc Project Management Board Booths Hall Chelford Road, Knutsford Cheshire WA16 8QG	(1)
	Jenkinson, J. Human Factors Group Nuclear Electric plc Barnett Way, Barnwood Gloucester GL4 7RS	(1,2,3,4)
<u>UNITED STATES OF AMERICA</u>	Eckenrode, R. Human Factors Branch International Programs Human Factors Assessment Branch Office of Nuclear Reactor Regulation NRC Washington, D.C. 20555	(3)
	Sun, B. Control and Diagnostics Program Nuclear Power Division Electric Power Research Institute 3412 Hillview Avenue Palo Alto, CA 94303	(1,2)

INTERNATIONAL  
ATOMIC ENERGY  
AGENCY

Dastidar, P. (3)  
Division of Nuclear Power

Dusic, M. (1)  
Division of Nuclear Safety

Neboyan, V. (1)  
Division of Nuclear Power

Swaton, E. (1)  
Division of Nuclear Safety

Kossilov, A. (Scientific Secretary) (2,3,4)  
Division of Nuclear Power

International Atomic Energy Agency  
P.O. Box 100, A-1400 Vienna, Austria

- (1) Advisory Group Meeting, Vienna, 17-21 April 1989
- (2) Consultants Meeting, Vienna, 27 November - 1 December 1989
- (3) Advisory Group Meeting, Vienna, 14-18 May 1990
- (4) Consultants Meeting, Vienna, 26-28 November 1990