IAEA-TECDOC-561

REVIEWING COMPUTER CAPABILITIES IN NUCLEAR POWER PLANTS

SUPPLEMENTARY GUIDANCE AND REFERENCE MATERIAL
FOR IAEA OPERATIONAL SAFETY REVIEW TEAMS
(OSARTs)

A TECHNICAL DOCUMENT ISSUED BY THE
INTERNATIONAL ATOMIC ENERGY AGENCY, VIENNA, 1990

REVIEWING COMPUTER CAPABILITIES
IN NUCLEAR POWER PLANTS
IAEA, VIENNA, 1990
IAEA-TECDOC-561
ISSN 1011–4289

Printed by the IAEA in Austria
June 1990

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

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

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

FOREWORD

The OSART programme has become not only the most visible operational service that the IAEA provides for those of its Member States which operate nuclear power plants, but also an effective vehicle for promoting international co-operation for the enhancement of plant operational safety. In order to maintain consistency in the OSART reviews, OSART Guidelines (set out in IAEA-TECDOC-449) have been developed and used in the past three years. These guidelines specify the objectives (goals) to be considered and the assessments to be carried out in various areas important to operational safety. They are intended to ensure that the reviewing process is comprehensive, but do not set criteria for evaluation of actual performance. This is not necessary in most areas because there is an abundance of relevant published material and an apparent consensus among experts.

There are, however, a limited number of areas where major developments have occurred or are still occurring. Computer technology is an area in which rapid development is taking place. Technology which is state-of-the-art today will be obsolete tomorrow. As the technology is developing so rapidly, new applications may be computerized to further enhance safety and the effectiveness of the plant. Supplementary guidance and reference material is therefore needed to help attain comprehensiveness and consistency in OSART reviews in this area. This document seeks to cater for these needs. It is devoted to the utilization of on-site and off-site computers in such a way that the safe operation of the plant is supported. In addition to the main text, there are several annexes illustrating adequate practices as found at various operating nuclear power plants.

It is hoped that this document will be seen as a valuable contribution to the OSART programme, and that it will support the general drive for excellence in operational safety extending beyond regulatory requirements.

EDITORIAL NOTE

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

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

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

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

CONTENTS

1. INTRODUCTION

This document contains guidance for reviewing a programme for computer capabilities at a nuclear power plant.

The document first discusses what the objectives of a computer capability programme should be. Specific investigations are described, which can be made to determine the degree to which a plant achieves excellence in its programme. The attributes of an excellent computer capability programme are listed concisely. Suggestions are then made on how to phrase review questions, and activities in which the reviewer can participate and areas in which he can verify capability. Finally, there is an appendix containing a short glossary explaining some of the expressions used. The appendix also contains examples of documents relevant to a computer capability programme.

The guidelines and discussions in this document are in no way intended to conflict with existing regulations and rules. The objective is to show how the use of computer capabilities in diverse activities provides significant potential for improvements in the safe operation of the nuclear power plant, as well as in a number of auxiliary activities.

To obtain this benefit, however, when computer capabilities are introduced they must be used to accomplish existing functions with a degree of safety which is equivalent to or greater than that achieved with previous practices, keeping in mind that neither the hardware (computers) nor the software driving them are inherently safe. They must be programmed and used correctly if plant safety is to be enhanced.

Even when they are used in very different applications, the specific features of computerization justify a condensed review of plant computer capabilities. The safety implications of the different possible applications, from use in safety protection systems at one end of the range to administrative tasks at the other, are sufficiently different to justify their classification with respect not to material or equipment used but to safety implication. A prerequisite in assessing the adequacy of the available computer capability is a clear definition of the function to be fulfilled. The organization and sharing of responsibility must take into account both aspects, as well as specifying the function rather than the required technical support in the form of computer and software.

In this document the following classifications of computer applications are adopted:

- Safety-related process applications
- Non-safety-related process applications
- Administrative applications.

The safety classification of process applications must also be considered with respect to the level of automation of the input and output:

- Computer applications directly involved in the process, receiving direct information and giving direct orders from and to the process.

- Computer applications receiving direct information and providing information to be used by the staff.

- Computer applications for 'manual use' for input and output.

Minimum requirements for redundancy, Quality Assurance, knowledge of users, maintenance, and feedback of experience differ in accordance with these classifications and categories.

2. REVIEW OF COMPUTER CAPABILITIES

References: IAEA, Manual on Quality Assurance for Computer Software Related to the Safety of Nuclear Power Plants. Technical Reports Series No. 282, IAEA, Vienna (1988).
IAEA, OSART Guidelines, Reference Document for IAEA Operational Safety Review Teams, IAEA-TECDOC-449, Vienna (1988).

Objectives

2.1 Programme for computer capabilities utilization

The general objectives in utilization of on-site and off-site computers are in the broadest sense to enhance safety and effectiveness at the plant.

A programme for utilization of computer capabilities should be established and implemented to verify the safe operation of the plant. The utilization of computer applications should be performed in such a way that the safe operation of the plant is supported.

Utilization of computer capabilities may vary greatly between different plants. The programme for utilization should therefore clearly define the categorization of the applications: safety-related or not, and the degree of automation. In the programme there should be a definition of the systems and/or specific equipment that are to be defined as computer systems.

2.2 Computer quality assurance programme

To ensure safe operation of different computer systems and computer applications a Computer Quality Assurance Programme should be established. The programme may be a written paper pointing to different procedures and instructions, or it may be a collection of such documents. Depending on the degree of computer utilization the computer quality assurance programme may vary in scope and content.

A full computer quality programme should contain the following items.

2.2.1 Organization and responsibilities

To accomplish its objectives the programme for computer utilization should contain a clear organizational chart identifying functions, the organizations and individuals responsible for the functions and the

communication links among the functions and the organizations. End-user categories, operating organization, maintenance, testing, inspection and repair functions should be explicitly identified in the organizational chart to cover all aspects of the utilization of computer capabilities, both on-site and off-site.

2.2.2 Computer documentation

Documentation for operating, maintaining and using computer systems, and for computer applications, should be established. All procedures, and other documentation, except those intended for end-users may be a part of the quality assurance programme. There should be a list of documentation available containing: index of applications, functional descriptions, operating procedures, maintenance procedures, emergency recovery procedures, back-up, test, and modification routines, etc.

To ensure that deficiencies are detected and corrected, there should be clearly identified process for preparing, revising and administering these documents. Functions should be identified, not only for writing and preparing procedures and other documents, but also for ensuring their correctness and comprehensibility and for revising them in a timely manner. Responsible individuals should be identified for each function.

For data record and other data printouts as well as data stored on magnetic media for later use or retrieval there should be documented description of responsibilities, storage facilities etc.

2.2.3 Software quality, coding methods and database organization

To ensure high quality in the process of designing and maintaining computer applications a special quality programme for software and database management should be established. Such a programme may deal with organizational issues, software documentation methods, coding methods, media and services control, tools for software design, design control and testing methods.

The IAEA manual on Quality Assurance for Computer Software Related to the Safety of Nuclear Power Plants refered to in the reference list may be utilized for review in this field of computer utilization.

2.2.4 Emergency recovery

In case of computer failure or loss of applications within a specific computer system, procedures should be established for emergency recovery. Procedures should include initiation of activities, trouble shooting, repair, recovery and return to normal operation including items such as closing of work orders.

For the end-user, there should be procedures for manual back-up routines capable of ensuring the safe operation of the plant without support from the computer system or computer application.

2.2.5 Back-up routines

In order to ensure continuous safe operation of computer systems, routines should be established for back-up of secondary memories containing programme code as well as data. Back-up routines should be described in procedrues and contain methods to ensure that copied data are verified in such a way that the copy will operate when needed.

2.2.6 Modification, update and correcting routines

Within the quality assurance programme procedures and routines for modification, update and fault correction should be established for the software as well as for the hardware. Preferably, these routines will be in accordance with routines established for all other equipment used within the plant. Nevertheless, descriptive documents should exist for these activities. Procedures and routines should be in use for the whole modification process: idea, review, construction, implementation, test and verification.

2.2.7 System security

To ensure the safe operation of the plant it is of importance that only authorized personnel have access to the computer system, in order to prevent sabotage or alterations by mistake. There may be several levels of access reaching from the end-user's access to certain applications, to the programmers' access to the kernel of the operating system or maintenance personnel access to the computer itself. Restriction of access may be accomplished in different ways, e.g. by the usage of pass-words or by restricted access to the premises. System security, authorization, access to hardware and usage of pass-words should be described in procedures.

2.3 Computer effectiveness and application effectiveness

As mentioned earlier, the general objective in the use of on-site and off-site computers is in the broadest sense to enhance safety and effectiveness at the plant. Computer applications are tools used by operators and other personnel at the plant. In order to meet the objectives it is important that these tools are effective and easy for the end-user to use. To help in assessing the degree to which objectives have been attained, the computer capability and computer utilization programme at the plant should contain tools to measure the effectiveness and ease of use of all applications. There should also be a strategy for making further improvements and developments within the field of computerization.

2.3.1 Measurement of availability and performance

The effectiveness of computer systems may be measured in many different ways. One basic measurement is of availability. Availability must be a well defined characteristic. Normally a system is available when the computer system, including input and output equipment, and basic applications are available for the end-user. A programme should be established for follow-up of availability. The programme should contain tools for evaluation of degradation of hardware equipment to ensure that items with a high failure frequency will be exchanged or modified in order to reduce the failure rate.

Performance tests should be performed on process computer systems or applications to verify that they are capable of handling plant disturbances or incidents in such a way that data is not lost, and that the end-user has access to data in the format needed to cope with the specific situation.

2.3.2 Measurement of ease of use

Measurements of ease of use may be accomplished through interviews with operators and people in other end-user categories. Such interviews should include questions regarding ease of use, clarity, readability, correctness of data etc. A programme should be established at the plant for this activity.

The programme should include routines for evaluating questionnaires as well as routines for use in deciding how to implement improvements.

2.3.3 Strategy for improvements and development

There are few fields of technology in which development is more rapid than computers. Computer technology which was state-of-the-art today is obsolete tomorrow. As a result, new applications may be computerized with the objective of improving speed and/or accuracy of calculations. The relatively short 'life-time' of computer hardware is also an incentive to implement a strategy to improve and develop the utilization of computer systems and/or computer applications at nuclear power plants.

There should be a long-term plan at the plant which includes a strategy for hardware exchange and a development plan for applications.

2.4 Experience feedback

The feedback of experience in computer utilization may be divided into three categories:

- Feedback from the end-users (see 2.3 above).
- Feedback from regulatory bodies or institutions such as IAEA, INPO, UNIPEDE etc.
- Feedback from other users of the same types of computer system or application.

In order to retrieve as much information as possible, a programme should be established to derive experience feedback from all three categories. Experience feedback from end-users is dealt with under point 2.3 above. Experience feedback from regulatory bodies and institutions is dealt with under the scope of operating experience in the OSART Guidelines.

For experience feedback from other utilities or other users of the same equipment or the same applciations, the formation of formal or informal users' groups is one of the best ways of obtaining access. If possible such a programme for co-operation should be established at the plant or within the company.

2.5 Supply of spare parts and service agreements

In order to maintain a high availability for the computer system and to ensure access to applications important for the safety of the plant, provision should be made to ensure long-term access to spare parts for the hardware, hardware service assistance, and supplier assistance for training of hardware technicians and programmers. Such a programme could be in the form of a service agreement with the vendor of the computer system or an agreement with some other institution or company which meet stipulated requirements. Long-term spare part supply could also be accomplished by storing parts on site.

For servicing of hardware and for training purposes a test system may be used. The use of a test system ensures that hardware replacement parts are fit for use. A test system may also be utilized for the testing of new applications.

2.6 Training and qualifications

Finally, the key ingredient of a computer capability programme is the people involved. Documents and documenting procedures are important to the programme, but it is the people who make the programme work. The people should be well qualified and should not only understand their respective duties but should also show awareness of the importance of their contributions. They should, as well, want to be personally active in ensuring the safety of the plant. It is only with this attitude to safety on their part that computer capabilities will be used effectively.

3. PREPARATORY WORK

3.1 Documents to be made available for review at the plant

All or part of the following list of documents should be available for review at a specific plant, depending on the extent to which computer capabilities are used.

- Programme describing the utilization of computer capabilities.
- List or schematic describing computer applications.
- Definition of safety-related and non-safety related computer applications or systems, including administrative applications or systems.
- Definition of which applications or hardware installations are treated as computer systems -- e.g., are microprocessor equipment controllers to be treated as computer systems or as controller systems?
- Administrative procedures which define the organization, objectives and responsibilities of computer personnel.
- Computer QA manual and/or software QA manual.
- Qualifications of personnel involved.
- Selected procedures.
- Log-books.
- List of documents for hardware and software maintenance.
- Procedures for modifications, updates and correction routines.

4. INVESTIGATIONS

4.1 Introduction

The investigations section of this document is written to give the team member a frame work of key investigation points. It is not the intention to limit the investigations to a questionnaire; instead, this part of the document should help the team member to identify all three types of activities of a good investigation -- questionnaires, participation and verification.

It should be noted that an important element of the investigation is the free exchange of information, ideas and thoughts.

In view of the fact that computer capabilities could be a large subject at an advanced plant the investigations to be performed have been divided into three categories:

- Investigations which should always be carried out, as they are generic.

- Investigations which may be carried out if sufficient time is available.

- Investigations which may require the reviewer to have deep background knowledge of computer technology.

4.2 Investigation on category 1 objectives

The objectives to investigate are:

- Programme for computer capabilities utilization
- Organization and responsibility
- Computer documentation
- Emergency recovery
- Back-up routines
- Modification, update and correcting routines
- System security
- Computer effectiveness and application effectiveness (in part)
- Experience feedback (in part)
- Training and qualifications.

With reference to section 4.5 (phrasing of questions) and 4.6 (activities for participation or verification), the investigator should start by verifying that a programme exists for the utilization of computer capabilities. He should check that the plant has defined whether or not individual computer applications are safety-related, and whether or not they define equipment utilizing, for example, microprocessors as computer systems.

The reviewer should verify also that there are organizational charts for the computer utilization programme, that they meet the objectives, that they show how responsibilities are shared between the plant and its corporate head office (if applicable) and that this sharing of responsibilities is in line with the organizational chart.

For computer documents the reviewer is advised to ask for a list of documentation and by picking examples verify that documents have been updated to reflect the actual situation, and that procedures for preparing, revising, administrating and storing of documents are followed. In the list of documents there should be an index or list of applications which should be in line with the overall programme for computer utilization at the plant.

For the objectives of emergency recovery, back-up routines, modification, update and correcting routines, system security and training and qualifications, the reviewer is advised to ask for procedures and written documentation, and to verify that these objectives are met. Refer also to paragraph 4.6 for participation and verification.

To assess computer and application effectiveness, and experience feedback, the reviewer is advised to ask for procedures and written documentation that verifies that these objectives are met. He should refer to paragraph 4.6 of this document (participation and verification). It is also advised that he should interview end-users, i.e. control room operators, about their attitude to the utilization of computer capabilities. The questions presented may be:

- Describe and explain which computer applications you use the most.
- How are these applications utilized in your job?
- How do you know that the information you obtain from the computer system is correct? If you do not, please explain how you deal with the information concerning plant safety?
- Who helps you if you do not understand an application or if you are not able to understand the information you receive? Who is the responsible person?
- In your opinion is the information presented in a useful format and could you explain it? If not, how do you draw this information to the attention of the responsible person?
- Is the system easy to use? Please explain.
- How is operators' experience feedback reported to the responsible person?
- Is your feedback handled in an effective way in your opinion? If not, please explain.
- Is the system available when you need it? Please inform me of your view of how availability impacts on your job.
- Do you have enough CRTs and are they placed in an area of easy access and use? If not, explain why.

Questions similar to the above should also be put to higher levels of plant management in order to obtain a wider view of the utilization of computer capabilities.

4.3 Investigation on category 2 objectives

The objectives to investigate are:

- Computer effectiveness and application effectiveness (in part)
- Experience feedback (in part)
- Supply of spare parts and service agreements.

Although computer effectiveness and application effectiveness are covered in the investigation of category 1 objectives, there are additional aspects which may be investigated if relevant, and if there is time available.

Verify that availability measurements take place and that the measurements are evaluated. Verify that objectives in this area are met by conducting performance tests. Verify that procedures are followed and, if possible, be present when tests are performed. Verify that the objective of having a strategy to make improvements and to develop systems is met by checking long-term planning at the plant.

Experience feedback is also covered in part in the category 1 investigation. To meet criteria of excellence in this area, experience feedback should draw not only from end-users on site.

Verify that feedback from regulatory bodies and/or institutions is taken into account in accordance with procedures or other written documents. Verify if possible that the plant or the company participate in formal or informal users' groups.

Verify that measures are taken by the plant to assure the supply of spare parts, and hardware and software specialist assistance from vendor or other institutions. Verify also that training assistance from vendor or another institution is available. If test systems are used at the plant or available at another location, inspect and verify that they are used according to procedures.

4.4 Investigations on category 3 objectives

The objective to investigate is:

- Software quality, coding methods and database organization.

This objective is important but, in order to verify that it has been achieved, in-depth knowledge of software techniques might be needed. To verify this, procedures and written documents should be presented and the source code, database management and general handling routines for software should be checked. The Manual on Quality Assurance for Computer Software Related to the Safety of Nuclear Power Plants (IAEA Technical Report Series No. 282) may be used.

4.5 Phrasing of questions

To obtain information on the items that have been identified and that are essential to an excellent use of computers, questions to plant personnel should be phrased in such a manner as to obtain useful information. Questions which can be answered by 'yes' or 'no' do not generally produce useful information. For example, the question 'Do you understnad this program?' will probably produce the uninformative answer 'yes'. To help obtain useful

information the questions can be phrased in such a way as 'Please show me documentation' and 'Please describe your understanding'. For example, to obtain information on the program, the question can be phrased in such as way as 'Please show me documentation describing the program's functions, and please describe the functions and how you use them'. Asking the person to describe his or her understanding will also show whether this is consistent with the documented information that is produced.

4.6 Activities for participation or verification

Participation in activities when actual tasks are performed may complement the use of questionnaires. Another complementary activity is actual verification of how activities have been or are being carried out.

These are examples of activities suitable for participation and/or verification:

- Verification of, and/or participation in, the performance of manual back-up routines for use in case of computer failure.
- Verification that source code for programs are written according to specified rules.
- Participation in, and/or verification that, back-up routines for back-up secondary memories are carried out according to procedures.
- Inspection of storage facilities for back-up copies.
- Participation in performance tests.
- Verification that modifications have been implemented in accordance with procedures. This could be, for example, checking that documentation has been correctly updated.
- Participation in planning or review meetings concerned with modifications.
- Participation in, and/or verification that, repaired circuit boards are run on a test system before installation.
- Participation in routine or special scheduled meetings, e.g. feedback meeting, user group meeting, department meeting.
- Participation in training activities.

5. ATTRIBUTES OF AN EXCELLENT PROGRAMME FOR COMPUTER CAPABILITIES

The previous section described the investigations that can be carried out and the responses that should be provided by the plant if the plant has an excellent programme for computer capabilities. The attributes of an excellent programme for computer capabilities discussed in the previous section are collected here in the form of a summary list to assist further in evaluating a specific plant's computer capability programme. An excellent computer capability programme should have the following:

Excellence in objectives and bases

- Computer applications are in use to enhance the safe operation of the plant and to increase the efficiency of work.
- Objectives of computer capabilities clearly defined.
- Correct definitions for classification of computer applications established.
- Management and end-users are satisfied with how the objectives for computer capabilities are met.

Excellence in quality assurance

- A Computer Quality Assurance Programme established, documented and in use.
- Responsibilities and organization clearly defined and established.
- Documentation for operating, maintaining and use of computer systems established and in use. Originals of procedures stored in a safe and secure storage area.
- Emergency recovery routines established and documented.
- Manual back-up routines in case of computer failure established, documented and tested.
- Back-up routines for secondary memories established, documented and tested. Back-up copies stored in safe and secure storage area.
- Software quality assurance programme including coding methods and tools for software maintenance established, documented and in use.
- Programme in use including routines and procedures for managing modifications in software as well as in hardware.
- A security programme established defining clearly who has access to the software as well as the hardware.

Excellence in administrative control

- Clearly documented administrative responsibilities identifying functions, responsible organizations and individuals, and communication interface.

- Individuals who understand and communicate their responsibilities, which are consistent with those documented, and who adopt an appropriate attitude to safety.

Excellence in experience feedback

- Clearly documented routines for feedback of experience from end-users.

- Clearly documented routines for feedback of experience from regulatory bodies and/or institutions.

- Participation in formal or informal users' groups. Personnel attending national and international meetings in the field of computer capabilities.

Excellence in maintenance activities

- Ability to have access to well-trained technicians and training facilities supplied by vendor or appropriate institution.

- Spare parts agreement and/or facilities for storing of spares.

- Access to test system or development system for testing spare parts, and for training purposes.

- Assurance by agreement or equivalent to software knowledge from vendor or institution. This includes access to trained and qualified personnel as well as training facilities for plant's own personnel.

Excellence in effectiveness measurements

- Availability measurements performed and documented.

- Performance tests performed and documented.

- Diagnostics established for evaluation of availability trends and performance tests performed.

- Specific time limits for the retention of records, and a basis for setting these.

- Significant records stored in a safe and secure storage area.

- Long-term (five to ten year) planning of developments, improvements and maintenance of software and hardware established and accepted by management.

Excellence in the treatment of human errors

- Personnel exhibit frankness in identifying and recording human errors that can occur.

Excellence in auditing the programme for computer capabilities

- Audit process in place to audit periodically the overall programme and individual aspects of the programme.

- Audit process in place to audit how the computer quality assurance programme is followed by organization and individuals.

Excellence in personnel

- Personnel well qualified.

- Programme in place to maintain qualification and motivation.

- Personnel exhibits a positive attitude to safety, wanting to understand safety implications and wanting to be personally active in ensuring safety.

6. SPECIAL FEATURES TO CONSIDER WHEN REVIEWING THE CAPABILITIES OF THE PLANT PROCESS COMPUTER SYSTEM

The capability of the process computer system in use at a nuclear power plant is important to the safe and effective operation of the plant. Listed below are features and applications which, as a part of that capability, support these objectives. Some of the listed applications and features may not be applicable due to the type of reactor in use.

o Basic Functions

- Operator communication
- Sequence of events recorder
- Alarm annunciation
- Logging
- Post mortem review
- Limit checking
- Self checking

o General Functions

- Production report functions
- Measurement of operating time of special equipment
- Transient recording of parameters affecting the reactor vessel
- Supervision of plant unit status
- Recording of plant unit operation times
- Safety system testing
- Redundant input validity checking
- Automatic checking of points for safe unit shut down
- Automatic surveillance testing of time for valve closing

o Core Supervision Functions

- Neutron flux display
- Core performance calculation
- Detector calibration

- Reactor Supervision Functions

  - Safety Parameter Display System (SPDS)
  - Control rod manoeuvering and monitoring
  - Calculations of reactor thermal power
  - Safety Analysis Function (SAS)
  - Containment gas analysis
  - Xenon concentration monitoring
  - Neutron flux calibration (PRM)
  - Calculation of dryout and thermal margins
  - Presentation of operating point (BWR plants only)
  - Reactor coolant water quality monitoring
  - Surveillance of reactor vessel heating

- Turbine Supervision Functions

  - Turbine performance monitoring
  - Pre-heater performance monitoring
  - Condenser performance monitoring

GLOSSARY

An extensive glossary exists in the IAEA Manual on Quality Assurance for Computer Software Related to the Safety of Nuclear Power Plants (Technical Reports Series No. 282).

For better understanding of the previous text, additional explanations are given for a selected number of expressions.

Availability

The term availability means the time or percentage of time which the computer system is operable and available to perform its functions. There must be a clear definition of the parts of the system or applications which must not be operable although the system as a whole is declared operable and available. For example: part of the data acquisition system may be down but the system may still be regarded as operable. Accounting as an administrative application may not be working but the system may still be regarded as operable.

Back-up

The term back-up means a back-up copy, 'bit by bit', of a secondary memory i.e. disks or tape which could at any time, by manual action, replace the disk or tape which is currently running on the system. The reason for making back-up copies is that programs and data on secondary memories may be destroyed when hardware or software failure occurs. There should preferably be two types of back-up copies: one or more for operating purposes and one or more for safe keeping. The last should be stored separately from the computer premises and in a fire proof area.

Computer application

Specific function performed within a computer system.

Computer capabilities

An expression for the overall framework where computers are utilized. Within this framework several different computer systems and computer applications may exist.

Computer system

A functional unit consisting of one or more interconnected computers and associated software. (See IAEA Manual on Quality Assurance for Computer Software Related to the Safety of Nuclear Power Plants.)

Computer Quality Assurance Programme

The total activities established and implemented to assure quality together constitutes the quality assurance programme.

These activities are of two basic types: programmatic and work-oriented.

The programmatic activities are administrative in nature and include for example the establishment of the programme, and its management throughout the pre-study, specification, design, purchase, construction, commissioning, operation, maintenance and modification phases for a computer system.

For a computer system it is the proper combination of these two types of activity, programmatic and work-oriented, that constitutes an appropriate quality assurance programme.

Efficiency

How well a specific computer application or a computer system performs its specified task. The performance may be measured with reference to quality measurements like: Availability, Correctness, Timing, Clarity, Readibility, Maintainability etc.

Annexes

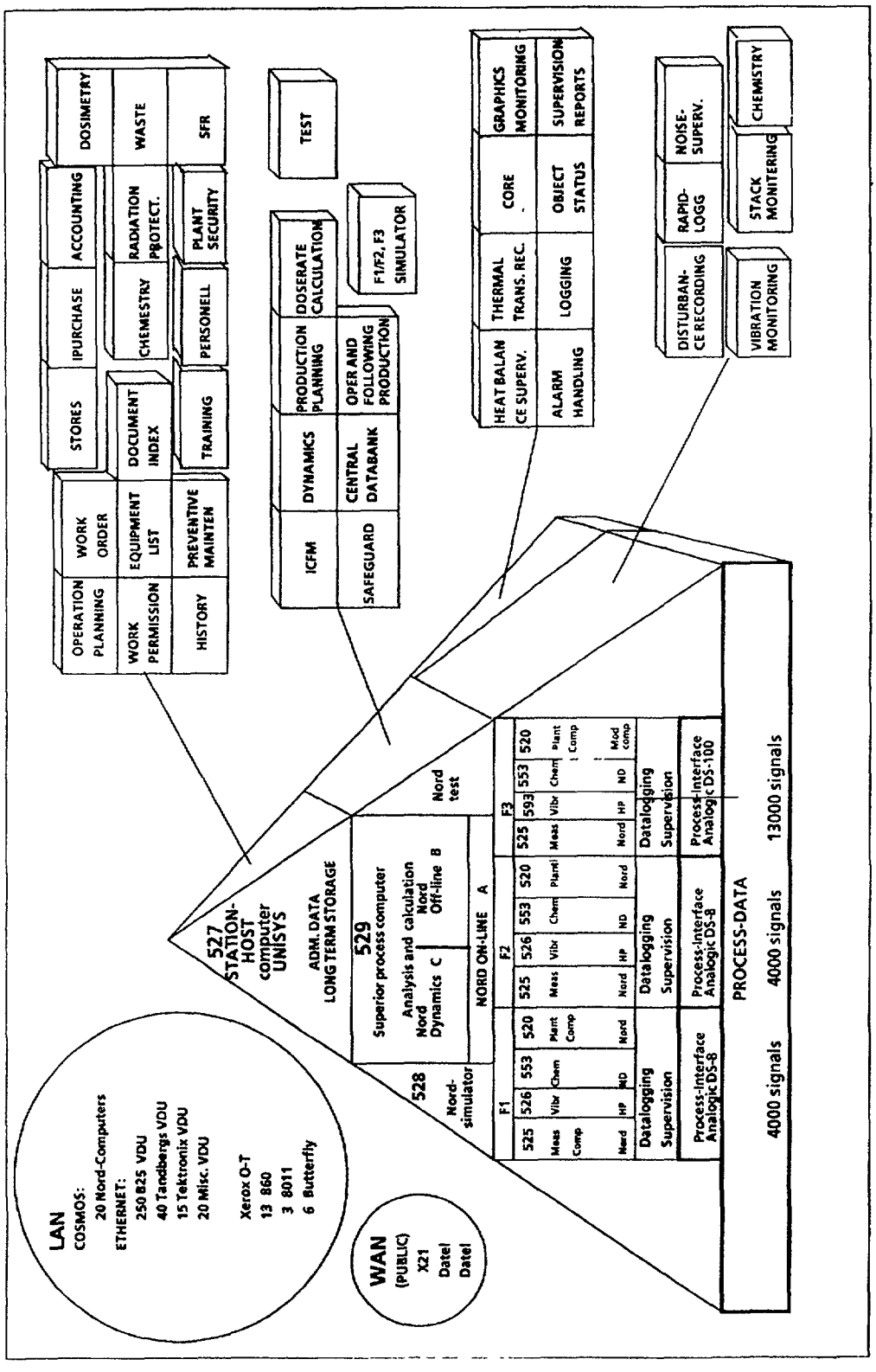
EXAMPLES DEMONSTRATING PARTICULAR ASPECTS OF THE UTILIZATION OF COMPUTER CAPABILITIES IN NUCLEAR POWER PLANTS

Next page(s) left blank

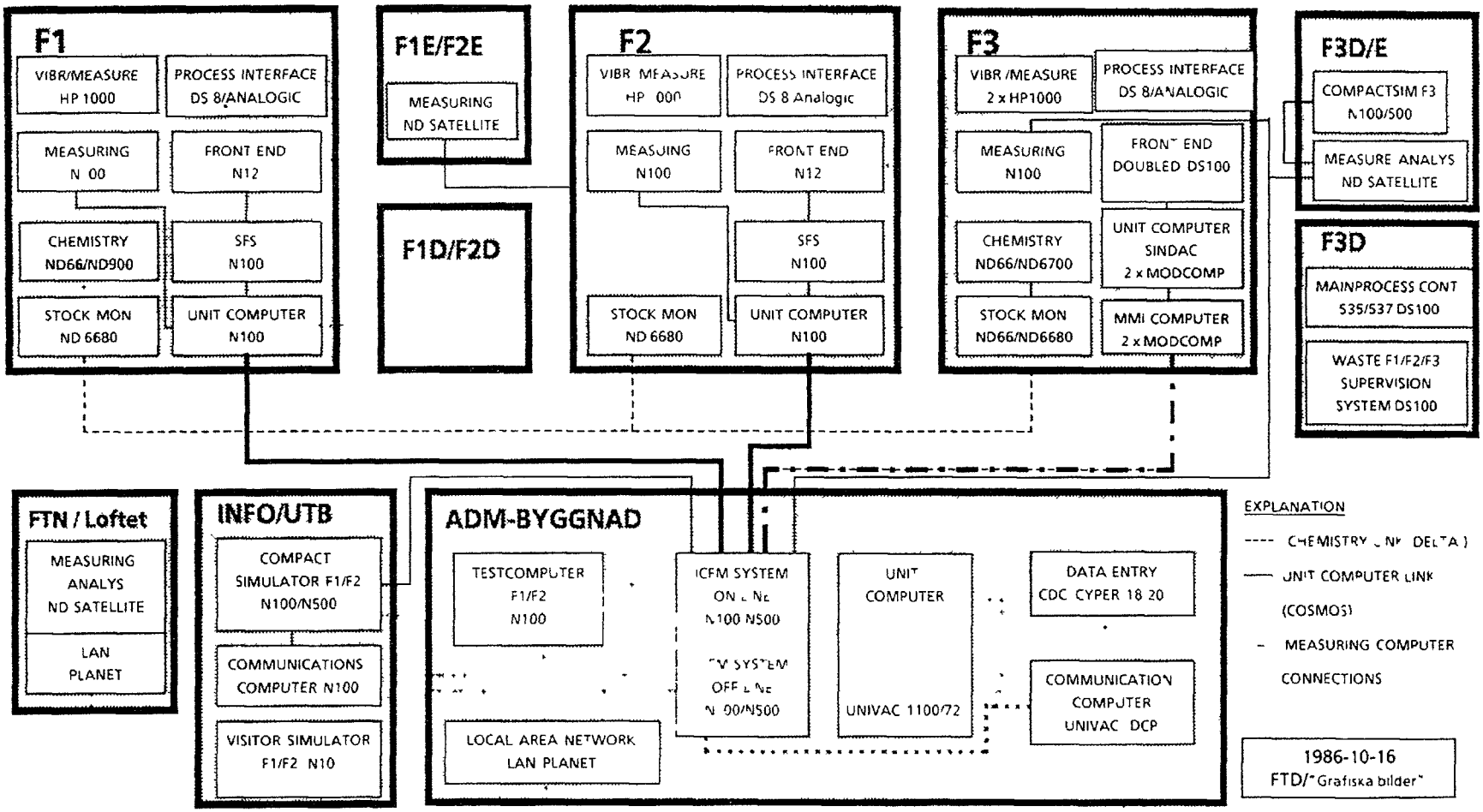
Annex 1

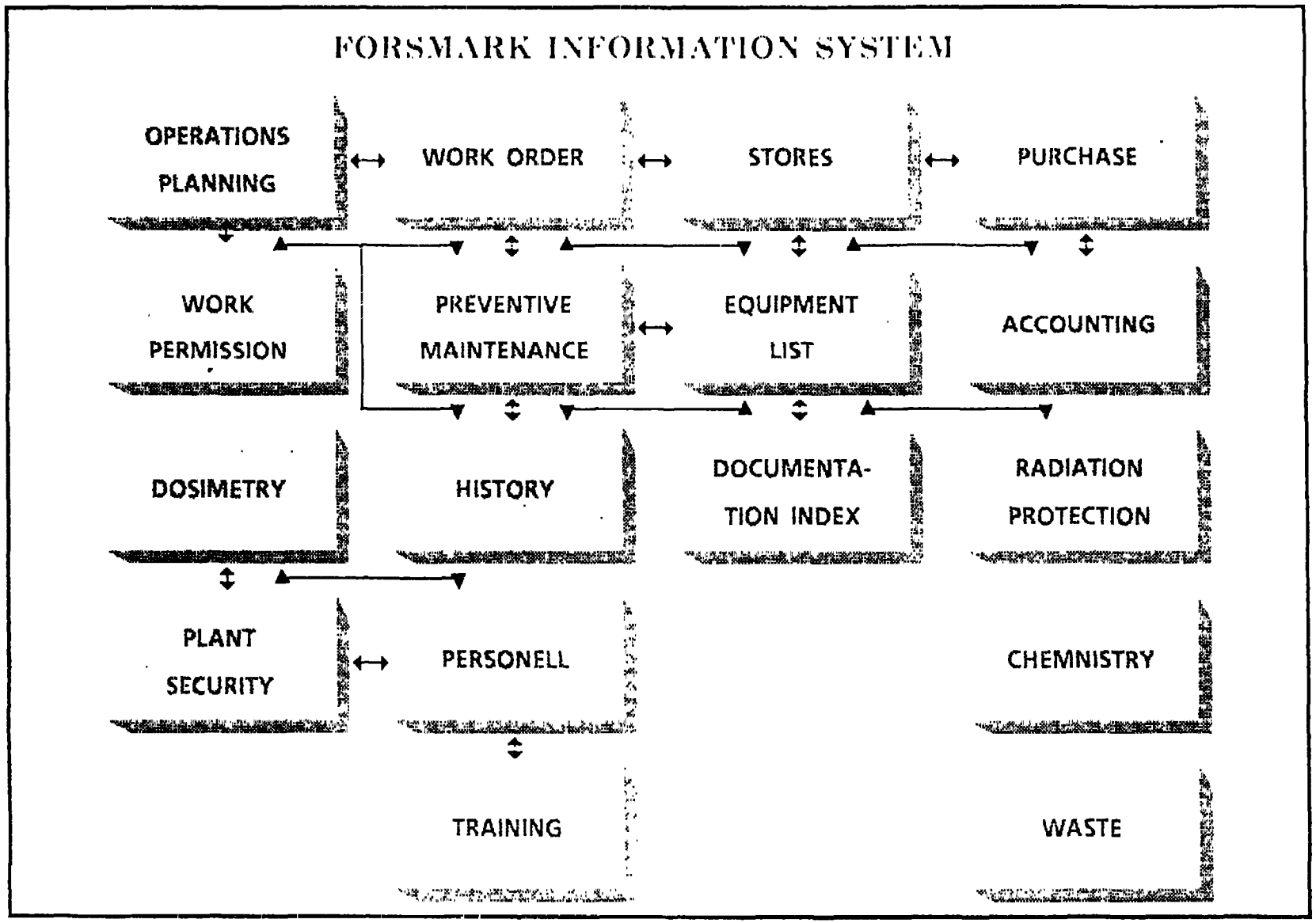
UTILIZATION OF COMPUTER CAPABILITIES AT A NUCLEAR POWER PLANT

(Used by Forsmark Nuclear Power Plant, Sweden)

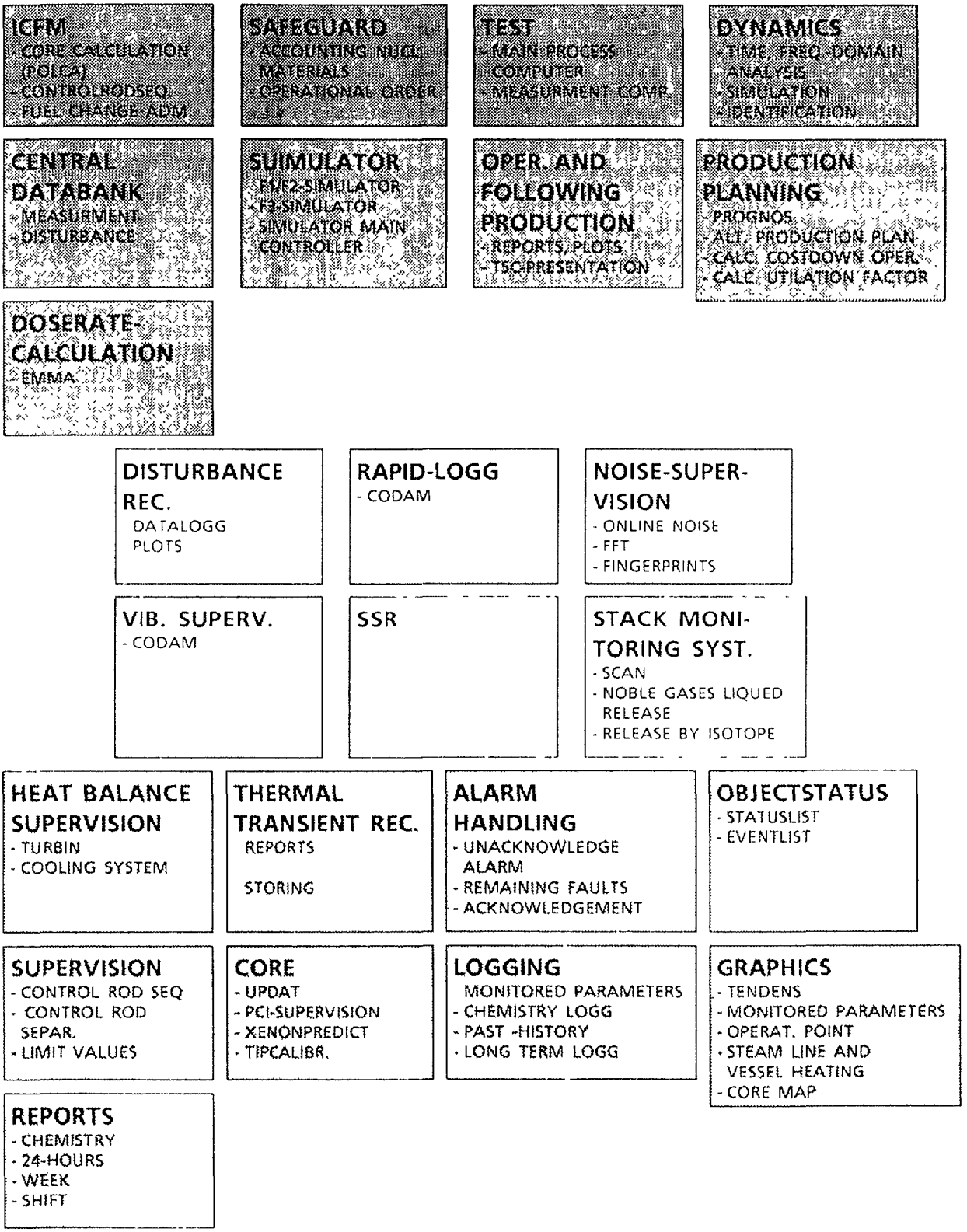


FORSMARK POWER PLANT - COMPUTER SYSTEM




FORSMARK INFORMATION SYSTEM
OPERATIONS PLANNING
WORK ORDER
STORES
PURCHASE
WORK PERMISSION
PREVENTIVE MAINTENANCE
EQUIPMENT LIST
ACCOUNTING
DOSIMETRY
HISTORY
DOCUMENTA-TION INDEX
RADIATION PROTECTION
PLANT SECURITY
PERSONELL
CHEMNISTRY
TRAINING
WASTE

FORSMARK PROCESS FUNCTIONS



LEVEL 1 ADMINISTRATIVE DATA PROCESSING

- MAINTENANCE SYSTEM
  - equipment
  - PM
  - spare parts
  - history
  - work order

- OPERATION
  - operations planning
  - work permission

- MANAGEMENT SYSTEM
  - stores
  - purchase
  - accounting
  - training
  - personnel

- WASTE

- CHEMISTRY

- RADIATION PROTECTION/DOSIMETRY

- ADMISSION

- ARCHIVE/DOCUMENTATION

LEVEL 2 CALCULATIONS

- ICFM (in core fuel management)
  - core calculation
  - burnup following
  - generation of control rod sequence
  - reports, plots, operational data display
  - fuel change administration

- SAFE GUARD
  - accounting of nuclear material
  - operational orders for fuel handling

- PRODUCTION PLANNING

- TURBINE FOLLOWING

- ONLINE CORE CALCULATION

- TEST COMPUTER

- SIMULATION, IDENTIFICATION, FREG. ANALYSIS

- DOSERATE-CALCULATION

- SIMULATORS
  - F1/F2
  - F3
  - cccc (to optimise controllers)

- SPECTRAL ANALYSIS

LEVEL 3

MAINCOME

- SUPERVISION
  - core supervision
  - limit checking
  - control rod supervision
  - oper.point
  - PCI

- ALARM HANDLING AND LOGGING

- LOGGING
  - on event
  - regular interval

- PRESENTATION
  - trend
  - reports
  - operational data

- TRANSIENT RECORDING (thermal)

- XENON PRED

- LPRM-CALIBR.

COMPUTERS FOR SPECIAL PURPOSE

- SUPERVISION
  - turbine vibrations
  - feedwater pump vibration

- DISTURBANCE RECORDER

- OUTLINE NOISE ANALYSIS

- GRAPHIC PRESENTATION

- CHEMICAL ANALYSIS
  - stack monitoring system
  - noble gases and liquid release
  - release by isotope

Annex 2

A COMPUTER QUALITY ASSURANCE PROGRAMME
(excerpts)

(Used by Forsmark Nuclear Power Plant, Sweden)

VATTENFALL

Sid 1(55)

Kl.-nr 3172

FORSMARKSVERKET

Titel
FORSMARK - SOFTWARE QUALITY ASSURANCE FOR COMPUTERSYSTEMS AT FORSMARK

Art PF_ INSTRUKTION		Nr 428:1	
Block PF		QAM-nr 4.4	☐ Verifieras
Giltig/datum 1986-11-01			
Ersätter			
Sökord för register Kvalitetssäkring	Författare Sjöstrand, Johansson, Mattsson, Lindholm		Ansv kontor FTD
Hänvisning till följande dok	Kontrollerad/Tagit del cFT LQ cFT		
O/T 860 X / O/T 8011 / Delvis / Kontor/Sign FTD-Sjö/Giv	Fastställd cKF		

Summary

This computer quality assurance instruction guide all activities regarding software for technical and administrative computer systems at Forsmark.

The instruction is adopted to routines valid at Forsmark and to the procedures in use at the Computer department of Forsmark.

The instruction guide the following activities:

- Time and resource planing
- Project planning for modifications
- Software maintenance
- Documentation
- Test procedures and control
- Software standards and regulations

Program library and work library, methods and tools are adopted to the needs for the computer department.
Procedures and methods for security and quality assurance for back-up of both data and program code are included.

The chapter for security contains only a referens to the general security handbook for computer systems issued by the head-office of the Swedish State Power Board.

Fast delgivning: F1, F2, F3, FT(UKN),

Övrig delgivning: FTD(30), FTQ(2), FTA, FTN, FTK, FXE, FXD, FP, FE, FS

1983-09 5000

OT860-FTI-Sjö/2

5627 •

TABLE OF CONTENTS

7. SOFTWARE STANDARDS AND REGULATIONS

7.1 Process computer systems and applications
7.2 Administrative computer systems and applications

8. TESTING

8.1 Test plans
8.2 Test procedures
8.3 Principles for tests
8.4 Test performance
8.5 Procedures for transfer of applications from test system to production systems

9. REVIEW AND CONTROL

9.1 Plan for control
9.2 Methods for evaluation

10. DATA REGISTRATION AND MODIFICATION ASSIGNMENTS

10.1 Assignment ordering routines
10.2 Work distribution
10.3 Preparation of assignments
10.4 Planning of assignments
10.5 Accomplishment of assignments
10.6 Closing of assignments at the computer department
10.7 Final closing of assignments

11. PROGRAM LIBRARY AND WORK LIBRARY

11.1 Process applications
11.2 Administrative applications
11.3 Back-up routines and procedures for handling and storage of media
11.4 Safety and security procedures for magnetic media and documentation

12. EXPERIENCE FEEDBACK AND FOLLOW-UP OF CORRECTIONS

13. CODING: METHODS AND TOOLS

14. SECURITY

15. MANAGEMENT OF VENDORS

Appendices (Number corresponds to refered chapter)

4.1 Time and resource planning - codes and example
4.2 Cost calculations for performance of modifications
4.3 Form for investment calculation of software or hardware modification
5.1 Example of analyses report and project report
5.2 System specification
7.1 Module head for process computer applications
8.1 Checklist for debugging of software
8.2 Test protocol for process computer applications
8.3 Test protocol for administrative computer applications
11.1 Program library for process computer applications
A. Test methods

Annex 3

A MAINTENANCE PROGRAMME FOR A PLANT PROCESS COMPUTER SYSTEM
(excerpts)

(Used by Forsmark Nuclear Power Plant, Sweden)

VATTENFALL

Sid 1(11)

FORSMARKSVERKET

Kl.-nr 76719

Titel

FORSMARK - MAINTENANCE ROUTINES FOR THE PLANT COMPUTER AT FORSMARK 3

Art	Nr	
KF-INSTRUKTION	342:1	
Block: F3	QAM-nr: 5.3.8	Verifieras
Giltig/datum: 1984-05-25		
Ersätter		

Sökord för register	Författare	Ansv kontor
Underhållsrutin	Olle Andersson	F3DA
Hänvisning till följande dok: KF-INSTRUKTION 624 och 157	Kontrollerad/Tagit del: F3D F3E FTI	
O/T 860:	O/T 8011: X	Delvis:	Kontor/Sign: FTI
Fastställd: cF3		

Summary

Administrative instruction for routine maintenance tasks and operation of the process plant computer system at Forsmark, unit 3

Contents

Appendixes

Fast delgivning: F3, FT, FAK1

Övrig delgivning: F3D, F3E, F3EC, F3P, FTI, FTR2, FTD, KFN/FTD, Elb/F3EC, PML/F3EC, 1 ex till datorhall F3

3. DATABASE MAINTENANCE

Database maintenance includes modifications, additions and up-dates in the database of the computer system as specified by the forms described in the C-documentation, folders C395 and C396. These forms are utilized to specify, e.g., point data, picture data, TTD data and data for applications.

All file generation should be carried out on the spare computer. After completed updating file generation is carried out, whereupon manual transfer follows. If the modification is approved, this will be done on the regular computer by selection in a special display. Then the spare computer is updated for consistency between the databases in the regular and spare computers. If the modification is not approved manual transfer is initiated once more. Then the modification has to be cancelled, whereupon the database again has the same contents as before the modification. A detailed procedure is available in UI (Maintenance Instructions) for the computer system and in C-documentation, folder 334.

4. PROGRAM MAINTENANCE

Program maintenance includes modifications, additions and updates in programs and modifications, additions and updates in the database, which are not specified on forms according to Section 3 above. Program source code, object modules and load modules are stored on discs or have to be fed in possibly from magnetic tape, when a modification is to be carried out. There are procedures in the C-documentation, folders C333 and C334. Checking of new program functions should be carried out on the spare computer, if possible.

5. OTHER MAINTENANCE TASKS

Everyone who works in the computer rooms has to look after good housekeeping. This means that there is paper in all printing units, that ribbons are changed when required, that printed lists are thrown away, if they are not going to be saved, that printed lists which are going to be saved are filed in folders and that folders are returned to their right places.

F3E is responsible for taking required FU actions concerning printer paper, ribbon changes etc. Further F3E is responsible for ensuring an adequate supply of magnetic tapes, paper and ribbons in the computer rooms.

Annex 4

QUALITY PROCEDURE FOR DEVELOPMENT, MAINTENANCE AND PROCUREMENT OF COMPUTER SOFTWARE

(excerpts)

(Used by Commonwealth Edison Company, United States of America)

INFORMATION ONLY

Commonwealth Edison Company

QUALITY ASSURANCE MANUAL

TITLE:	DESIGN CONTROL FOR OPERATIONS - DIGITAL COMPUTERS AND SOFTWARE	QUALITY PROCEDURE Q.P. NO. 3-54

1.0 PURPOSE

This Quality Procedure establishes standards and practices for the development, maintenance, and procurement of computer software.

2.0 SCOPE

This Quality Procedure applies to applications software that is:

2.1 safety-related,

2.2 used to perform controlled analyses,

2.3 used to verify station Technical Specification compliance, or

2.4 used to comply with regulatory requirements not contained in the Technical Specifications.

3.0 TABLE OF CONTENTS

5.0 REQUESTING SOFTWARE MAINTENANCE OR DEVELOPMENT

This section outlines the steps to be taken when requesting the development of new software, or the maintenance of existing software for both software problems and enhancements.

Responsibility		Action
Requestor	1.	Fill out and sign section 1 of the Software Activity Request (SAR) (QP 3-54, Form 1) with a description of the activities requested.
Requestor's Supervisor	2.	Examine the activities requested. Sign to indicate concurrence. Forward the form to the Site Administrator.
Site Administrator	3.a	Examine the activities requested.
	3.b	Check the appropriate box ("problem", "maintenance", or "development") at the top of the SAR.
	3.c	If the SAR pertains to a problem that cannot be confirmed, then resolve any user errors, misunderstandings, etc., with the requestor, and return the SAR form. No further action is necessary.
	3.d	Sign and date section 2 to approve activity request.
	3.e	Assign a sequential number to the SAR. Log the SAR number, a short description, the affected computer, and the date on which the SAR was initiated.
	3.f	Send the SAR form to the software owner for concurrence.

Responsibility		Action
	3.g	If the SAR is for a software problem, forward copy to site QA.
Software Owner	4.a	Sign and date section 2 to signify the confirmation of the problem and authorization to proceed with evaluation and resolution.
	4.b	For software problems determine the impact of the problem on plant operations, present work, and if required past work.
	4.c	If required, notify code users of software problems. 1
	4.d	If required, alert responsible personnel of the need to notify the NRC per 10CFR21, or 10CFR50.72, or 10CFR50.73.
	4.e	Assign an investigating department to examine the problem. Forward the SAR to the investigating department.
Investigator	5.a	Document the evaluation, the proposed resolution, and the affected sites. Identify the software items affected and fill out a Documentation Checklist (QP 3-54, Form 2) for documentation requiring development or modification. Attach the evaluation/proposed resolution and the Documentation Checklist to the SAR form.
	5.b	Sign and date section 3 of the SAR form.

Responsibility		Action
Investigator's Supervisor	6.	Review the evaluation/proposed resolution and Documentation Checklists. Sign section 3 of the SAR to indicate concurrence and to authorize the modification of baseline materials.
Investigator	7.a	Receive the software owner's permission to proceed with the work.
	7.b	Send copies of the SAR form and attachments to the site administrator at affected sites, and to the software owner.
Software Owner	8.a	Ensure that software baselines are revised or developed per section 6.0.
	8.b	Verify the completeness of the documentation package, and the results of software validation testing. If the documentation and validation testing of the software are acceptable, sign section 4 of the SAR form. Forward the form to the site administrator.
Site Administrator(s)	9.a	Verify the completeness of the documentation package by comparison against the Documentation Checklist.
	9.b	Install the software. Software installations at the generating stations shall be performed per section 7.0.
	9.c	If the documentation and testing of the software are acceptable, sign section 4 of the SAR form. Forward the SAR to the programming dept.

Responsibility	Action
Programming Dept.	10. File the SAR.

6.0 PERFORMING SOFTWARE MAINTENANCE OR DEVELOPMENT

This section outlines the steps to be followed for developing or maintaining software.

New software development shall require that all the documentation required by this section be prepared and reviewed, unless otherwise noted. For software maintenance, the documentation identified in the Documentation Checklist shall be modified by following the applicable steps of section 6.0. Modified software shall receive the same reviews as new software.

In certain situations plant operations shall require the modification of constants which are embedded in applications programs. It is not required that this modification be performed according to section 6.0, if site procedures exist to control this specific activity.

Responsibility	Action
Software Owner	1. As required by Appendix A, prepare a Functional Requirements Specification (FRS) for the proposed software maintenance or development. Submit the FRS to the programmer.
Programmer	2. Prepare, or revise, a Software Requirements Specification (SRS) according to Appendix B. Sign the cover sheet of the SRS.
Programmer's Supv.	3.a Review the SRS to assure that: 1. each requirement is complete, distinct, and verifiable; 2. there is sufficient detail to design the software; and 3. the SRS follows the prescribed documentation format in Appendix B.
	3.b Sign and date the SRS.

Responsibility		Action
Software Owner	4.a	Review the SRS against the FRS to ensure that it satisfies FRS requirements.
	4.b	Sign and date the SRS cover sheet. (This version of the SRS is now a controlled document.)
Programmer	5.a	Record the SRS revision number and date on the Documentation Checklist.
	5.b	Prepare or revise, per Appendix C, a Software Design Description (SDD) traceable to the SRS.
	5.c	Sign and date the SDD.
Programmer's Supv.	6.a	Review the SDD to verify that: 1.the requirements of the SRS have been satisfied; 2. design features can be traced to requirements in the SRS; and 3. the SDD adheres to the prescribed documentation format.
	6.b	Sign and date the SDD cover sheet. (This version of the SDD is now a controlled document.)

Responsibility	Action	
Programmer	7.a Record the SDD revision number and date on the Documentation Checklist.	
	7.b Develop test plans, and prepare or revise per Appendix D, the Software Verification and Validation Plan (SVVP).	
	7.c Sign and date the SVVP cover sheet.	
	7.d Implement the software in code.	
	7.e Collaborate with the software owner and develop test cases for software validation.	▶1
Programmer's Supv.	8.a Review the source code to verify that: 1. the design expressed in the SDD has been implemented; and 2. the source code meets required programming standards.	
	8.b Review the SVVP to assure that the requirements in the SRS will be thoroughly validated.	
	8.c Sign and date the SVVP.	
Software Owner	9.a Review the SVVP to assure that the requirements in the SRS will be thoroughly validated.	
	9.b Sign and date the SVVP. (This version of the SVVP is now a controlled document.)	
Programmer	10.a Perform software validation by execution of the test cases.	

Responsibility	Action	
	10.b Prepare a Software Verification and Validation Report (SVVR), per Appendix E.	
	10.c Sign and date the SVVR.	
Programmer's Supv.	11.a Review the SVVR to assure that verification and validation is thorough and acceptable.	
	11.b Sign and date the SVVR.	
Software Owner	12.a Review the SVVR for acceptability.	
	12.b Sign and date the SVVR. (This version of the SVVR is now a controlled document.)	
Programmer	13. Prepare user's documentation for the software per Appendix F.	
Software Owner	14.a Review user's documentation to assure that required aspects of code use have been explained.	
	14.b Sign and date the user's documentation. (This version of the user's documentation is now a controlled document.)	
Programmer	15. Record the revision numbers of the SVVP, SVVR, validated code, and user's documentation in the Documentation Checklist.	*2

7.0 SOFTWARE INSTALLATION ON GENERATING STATION COMPUTERS

This section outlines requirements for the installation of code on generating station computers, regardless of whether the code is installed temporarily for testing, or permanently for use. Software installations on generating station computer requires the approval of the station.

Responsibility		Action	
Programming Department	1.	Submit to the site administrator the following information:	
		a. The purpose of the software installation (testing, experiment, permanent installation, etc.)	
		b. The conditions required for, or resulting from, the software installation, e.g. possible effects on other programs, effects on plant operations, time duration of the effects, etc.	*1
		c. Documentation required by the Documentation Checklist.	
Site Administrator	2.a	Examine the supplied information for reasonableness and completeness.	
	2.b	Prepare and log a software installation form per station procedures. Record the work request number on the installation form.	
	2.c	Record the installation form number on the SAR.	
	2.d	Perform a 10CFR50.59 safety evaluation on the installation.	

Responsibility	Action	
	2.e. Review the information to verify installation conditions. Authorize installation.	
	2.f If the software can affect the Control Room operations, forward the installation form to the licensed shift supervisor for approval.	
Licensed Shift Supervisor	3. Examine plant, system, and/or equipment conditions for software installation. If acceptable, authorize the installation.	*1
Programmer / Site Administrator	4. Determine installation testing requirements and attach them to the installation form. Install the software and perform installation testing as required.	

8.0 SOFTWARE PROCUREMENT

The following sections provide requirements for software procurement.

Software procured as part of, or as a revision to, an integrated hardware package, may be tested as an integrated system when it has been determined by technical evaluation that the functional testing of the hardware package adequately validates the software. *1

Procured software shall be qualified for use per section 9.0.

8.1 Safety-related and Regulatory-related

Safety-related or regulatory-related software shall be developed and managed according to an approved software quality assurance program. Potential vendors or sub-contractors of safety-related software have the option of adhering to their own Edison-approved Software QA program, or to the Commonwealth Edison program outlined in this procedure.

If the former option is chosen, vendors shall submit a copy of their software quality assurance program and procedures. Computer Services and Quality Assurance will review these procedures. If they are found to meet the intent of QP 3-54, they will be recommended for placement on the Quality Approved Bidders List as a software supplier, and if applicable, a software developer. This will be done in accordance with QP 4-51.

Once placed on the Quality Approved Bidders List, the vendor may supply software to Commonwealth Edison. This software shall be ordered with the following documentation or its equivalent; a Software Requirements Specification, a Software Design Description, Source Code Listing if required, User's documentation, and Software Verification and Validation Plans and Reports. Each document should include the content required by the applicable sections of QP 3-54, and shall be acceptable to Commonwealth Edison. *1

Existing software that was not developed under the requirements of this QP, and which does not have the supporting documentation required by this QP, may be obtained if a technical evaluation is performed per section 9.0.

Software developers and suppliers shall be required to promptly report any identified software problems to Commonwealth Edison as per the requirements of 10CFR21, unless otherwise agreed.

8.2 Commercial Grade

Software may be purchased commercial grade per the requirements of QP 4-51. Commercial grade software shall require that the vendor be on the Commercial Approved Bidders List. Commercial grade software shall be ordered with the documentation required by Appendices B through F, or equivalent documentation, if this documentation already exists and is available. A technical evaluation shall be performed for commercial grade software per section 9.0.

Annex 5

COMPUTER SOFTWARE ACTIVITY REQUEST PROCEDURE

(Used by Braidwood Nuclear Power Plant, United States of America)

BwAP 500-10
Revision 2

COMPUTER SOFTWARE ACTIVITY REQUEST PROCEDURE

A. STATEMENT OF APPLICABILITY

This procedure describes the method for reporting and documenting problems, requesting maintenance, enhancements or developement of computer software that affects the operation of the nuclear generating station as defined by Q.P. 3-54. For Non Q.P. 3-54 software the use of this procedure is discretionary. Q.P. 3-54 related software falls in the following areas.

1. Computer software that is used to verify station technical specification compliance.

2. Computer software that is used to comply with non technical specification regulatory requirements.

3. Computer software that is used for controlled analysis.

4. Computer software that is Safety Related.

B. REFERENCES

1. Q.P. 3-54, "Design Control for Operations-Digital Computers and Software".

2. Q.P. 3-54 Form 1, "Software Activity Request".

3. Q.P. 3-54 Form 2, "Documentation Checklist".

4. Q.P. 3-53, "Design Control for Operations-Controlled Analysis".

5. Q.P. 3-52, "Design Control for Operations - Plant Maintenance"

6. Q.P. 3-51 Attachment A, "Definition of a Modification and Phases of Testing"

7. IEEE/ANSI 729-1983, "Standard Glossary of Software Engineering Technology"

8. IEEE/ANSI 828-1983, "Standard for Software Configuration Management Plans"

9. IEEE/ANSI 829-1983, "Standard for Software Test Documentation"

10. IEEE/ANSI 830-1984, "Guide to Software Requirements Specifications"

11. IEEE 1033-1985, "IEEE Recommended Practice for Application of IEEE Standard 828 to Nuclear Power Generating Stations"

12. INPO Good Practice TS-407, "Computer Software Modification Controls"

13. BwAP 500-9, "Software Configuration Management"

14. BwAP 500-11, "Plant Computer Configuration Control"

15. BwAP 500-11T1, "Plant Computer Change/Installation Request"

16. BwAP 500-11T2, "Plant Computer Change/Installation Request Documentation Revision and Training Summary Checklist"

17. BwAP 500-11T4, "Plant Computer Change/Installation Request Engineering Synopsis"

18. BwAP 500-12, "Computer Software Documentation and Testing"

19. BwAP 500-12A1, "Recommended Outline for Functional Requirements Specification"

20. BwAP 500-12A2, "Recommended Outline for Software Requirements Specification"

21. BwAP 500-12A3, "Recommended Outline for Software Design Description"

22. BwAP 500-12A4, "Recommended Outline for Software Verification and Validation Plan"

23. BwAP 500-12A5, "Recommended Outline for Software Verification and Validation Report"

24. BwAP 500-12A6, "Recommended Outline for User's Documentation"

25. BwAP 500-14, "Computer Software Reviewed for Q.P. 3-54 Applicability"

26. BwAP 500-14T1, "Computer Software Review Checklist"

27. BwAP 1205-6, "Conduct of Safety Evaluations and 10CFR50.59 Review"

28. BwAP 1205-6T1, "10CFR50.59 Format for Safety Evaluation"

29. BwAP 1205-6T2, "10CFR50.59 Checklist for Facility Changes"

30. BwAP 1205-6T3, "Safety Evaluation Checklist/Worksheet"

C. DEFINITIONS

1 Baseline - A specification or product that has been formally reviewed and agreed upon, that thereafter serves as a basis for further development and that can only be changed through formal change control procedures.

2. Site Administrator - Department head (or designee) responsible for the configuration of the target computer.

3. Software - The portion of a computer system that is implemented in software, including design, test, and user documentation as well as the software code.

4. Software Code - One or more computer programs, or part of a computer program.

5. Software Maintenance - Modification of a previously operational executable code to correct faults, to improve performance or other attributes, or to adapt a product to a changed environment.

6. Software Owner - Department head (or designee) responsible for the technical content (not necessarily the source code) of the software.

7. Investigator - Person(s) assigned by the software owner to investigate the cause of a software problem.

D. MAIN BODY

1. Requesting Computer Software Activity

The requestor shall initiate a Software Activity Request (SAR), Q.P. 3-54 Form 1, providing the following information in section 1 of the form:

a. The plant site, computer system affected and the affected unit number.

b. A description of the request with as much information as possible. (Attach an additional sheet if necessary) If applicable attach a Functional Requirements Specification (FRS).

c. For new product development initiate a classification of the software per BwAP 500-14, Computer Software Review for Q.P. 3-54 Applicability.

The initiator and the initiator's supervisor sign and date the form and forward it to the appropriate Site Administrator for the affected computer. The appropriate Site Administrator for each computer system is defined in BwAP 500-14.

2. Review of problem by Site Administrator and Software Owner

a. The Site Administrator reviews the description provided at the top of the SAR and checks Problem, Maintenance, or Development . If the condition requires further investigation or if the affected software is not working per design check Problem. If the affected software is working per design but requires enhancement, check Maintenance. If resolution of the condition requires a new system then check Development.

b. The Site Administrator:

1) Logs the SAR and assigns a sequential log number.

2) Signs and Dates the form in Section 2.

3) If the software is previously unclassified initiate the classification of the software per BwAP 500-14 to determine Q.P. applicability, determination of the Software Owner and target machine Site Administrator.

4) Forwards the SAR to the Software Owner for review.

5) If the SAR is identified as a problem and is Q.P. 3-54 applicable, forward a copy of the SAR to the site Q.A. department.

6) If the software is QP 3-54 related install the change using a Nuclear Work Request (blanket) and log as required.

c. The Software Owner:

1) Sign and date the SAR signifying authorization to proceed with evaluation and resolution.

2) For software problems, determine the impact of the problem on plant operations, present and past work (If Required).

3) If required, alert responsible personnel of the need to notify the NRC per 10CFR21, 10CFR50.72, or 10CFR50.73.

4) If required, notify code users of the problem.

5) Assign the investigating/programming department and forward the SAR.

3. Programming Department Investigation and Resolution

a. The investigator(s) document the evaluation of the request and indicate a recommended resolution. Attach the evaluation to the SAR. On the SAR form in section 3:

1) If no correction is necessary, indicate this by writing "No Action Required".

2) Fill in the software identification number and revision of the affected software product(s).

3) Circle the affected target machine sites.

4) If it is determined that a previously approved software product baseline is to be modified, or a new product is to be developed, then initiate and attach Q.P. 3-54 Form 2, Documentation Checklist for each affected product. Indicate on the checklist the Software Product ID and revision, and the affected software items. Indicate on the SAR the Product ID's affected.

5) If the corrective action is to make a computer database change or to change non Q.P. 3-54 related software not requiring a documentation checklist, fill in "Other" on the SAR with the resolution.

b. The lead investigator signs and dates the SAR in section 3. The investigator's supervisor signs and dates the SAR in section 3 indicating concurrence with the evaluation/resolution and authorizes modification of the affected baseline materials if necessary.

c. Obtain concurrence from the Software Owner of the evaluation/resolution before proceeding with the necessary changes. Document this concurrence in Section 3 of the SAR. If no baseline materials are affected forward the SAR to the Software Owner. Skip to step 4.

d. The programming department performs software developement documentation and testing. If the programming department is located at the station this activity will be performed per BwAP 500-12, Computer Software Documentation and Testing, or other department specific procedures.

e. When work is complete, copies of the software package and the SAR is forwarded to the Software Owner, if required.

4. Review and Installation of Resolution

a. The Software Owner reviews the investigator's evaluation and corrective action. If software baseline materials are affected:

1) Ensure that baseline materials are revised or developed per Q.P. 3-54 standards.

2) Verify the completeness of the documentation package and the results of the software validation testing.

b. If acceptable, the Software Owner signs and dates the SAR in section 4 and forwards it to the Site Administrator.

c. If baseline materials are affected the Site Administrator verifies the completeness of the documentation package by comparison against the Documentation Checklist.

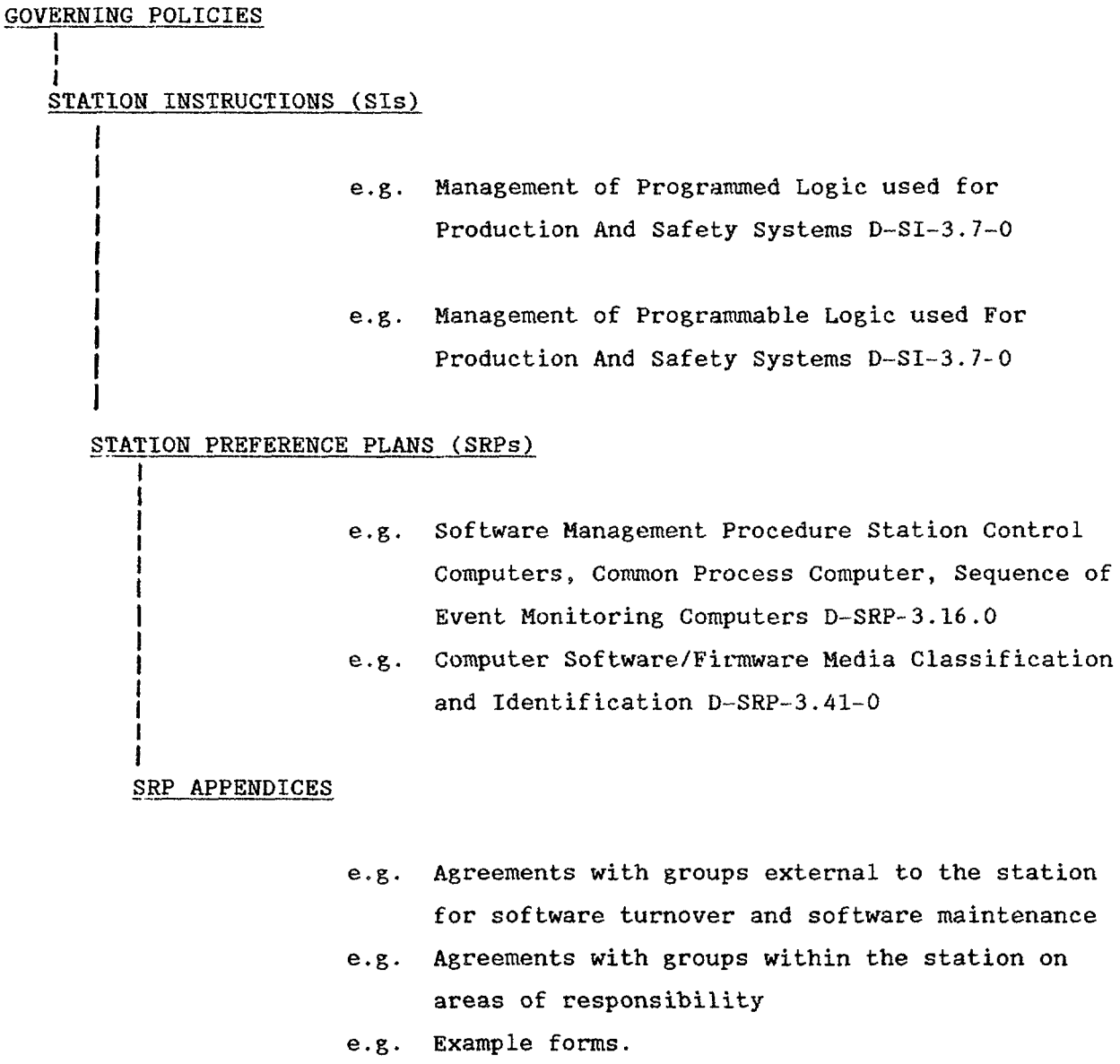
d. The Site Administrator or his designee installs the software change per the installation procedures for the applicable computer.

e. The Site Administrator signs and dates the SAR in section 4 and forwards the SAR to the programming department for filing.

Annex 6

HIERARCHY OF GOVERNING POLICIES AND PROCEDURES FOR COMPUTER SOFTWARE

(Used by Darlington Nuclear Generating Station,
United States of America)



Annex 7

CHANGE CONTROL PROCEDURE FOR SYSTEM, EQUIPMENT AND COMPUTER SOFTWARE
(excerpts)

(Used by Darlington Nuclear Generating Station, United States of America)

820084 rev 84 04 **Darlington NGS 'A'**	function: Station Reference Plan	system: Planning	unit: 9	sci
title: D-SRP-3.05				

DARLINGTON NUCLEAR GENERATING STATION 'A'

STATION REFERENCE PLAN

D-SRP-3.05-3

CHANGE CONTROL PROCEDURE

prepared/revised by	verified by	approved by	rev	page
K.A. Meagher	D. McQuade	H.L. Austman	3	1 of 42
date 88-09-21	date 21 Oct 88.	date 24 Oct 88		3:05:3

1.0 GOVERNING POLICY

Station Instruction D-SI-2.5 'Change Control'.

2.0 SCOPE

All permanent changes to DNGS'A' systems, equipment and computer software shall take place in accordance with this SRP. All changes to licensing documents and all operational changes shall also take place in accordance with this SRP.

Temporary changes are not covered by this procedure. See D-SRP-1.4 'Jumper Control'.

Adherence to this plan is essential to ensure that:

1. changes are reviewed and approved by the appropriate authority,
2. interested parties both internal and external to the Station are informed of changes,
3. the status of all changes is readily available,
4. adequate records of the implementation of the changes are readily available, and
5. documentation is complete and in agreement with field installation.

2.1 DEFINITIONS AND ACRONYMS

As-built	A discrepancy between actual field systems, equipment or process computer software and the design documentation. In the Operations environment, as-builts can occur in the following circumstances: 1. An ECN may be installed differently from the specifications in the ECN Package. 2. Field installation may be discovered which differs from the design documentation because of an earlier failure to update the documentation. 3. The field installation agrees with the design documentation but the system does not work as intended due to an oversight. Corrected by Minor Change Procedure.

BSP	Business Section Procedure: a written procedure for use by the Business Section.
Change	Any addition to, deletion from or modification to: systems, equipment, process computer software, operational instructions and licensing documents.
CMP	Control Maintenance Procedure: a written procedure for use of Control Maintenance.
CND	Change Notice of Deviation form: a form used by Construction to get design documentation updated by DED.
Computer Group	A group within the technical unit which is responsible for making computer changes.
Computer Package (not paper only)	Drawings and documents related to a change of process computer software. The contents of these packages are specified in Computer related station reference Plans.
DED	Darlington Engineering Division: The division of Ontario Hydro responsible for the design of DNGS'A'.
Design Change	Any change that alters design intent or requires revision of design documents.
Design Documentation	Any official document or drawing produced by DED which describes the design of DNGS'A' systems, equipment or computer software.
Control Maintenance Documentation Group	A group within Control Maintenance which is responsible for documenting wiring changes.
ECN	Engineering Change Notice: A package of design documents prepared by DED to cover an engineered change. Also referred to as an ECN Package.
ECN-AM (refer to Appendices D and E)	ECN Allocation Memo: A form prepared by DED to present a summary of the design work required to cover the change. The ECN-AM gives an estimate of engineering manpower and also identifies the sub ECN Packages.
ECN Procedure	The procedure by which engineered changes are controlled so that work can be executed in accordance with the governing principles.
ECN Start Date	A date set three months (six weeks for wiring changes) prior to turnover after which all engineered changes must be done via an ECN. An ECN Start Date list based on agreed turnover dates will be issued by DED at least every three months.

Engineered Change	A change to the design of DNGS'A' systems, equipment or software for which design assistance was sought by the responsible DNGS'A' Superintendent.
EWR (refer to Appendix C)	External Work Request form: A form used to request work (and estimates) from organizations other than DNGS'A' operations. The expenditure limit and the charge number are specified on the form.
Licensing Documents	Documents used to in the submission for our Operating License.
Materials	E type: Those materials ordered by DED usually as part of an ECN. These materials are normally received on site by Construction Stores. C type: Those materials ordered and stocked by Construction Stores. X type: Those materials ordered by Operations.
Minor Change	A station engineered change of a minor correctional nature to systems, equipment or computer software intended to ensure system performance as per the design intent.
Minor Change Package	A package of marked up design documents used to install a Minor Change. Within the Minor Change Package, there will generally be a Mechanical Package prepared by the System Engineer, a Wiring Package prepared by the Control Maintenance Documentation Group and/or a Computer Package prepared by the Computer Group.
Minor Change Procedure (refer to section 3.3)	The procedure by which Minor Changes are controlled so that work can be executed in accordance with the governing principles.
MMS	Material Management System: The computer system used to control material data.
Operational Changes	Changes to the way the station is operated which affect the conditions of our operating license.
Operating Commitment	An Operating Commitment is any parameter or event extracted from licensing documentation and placed under the administrative control of Operations because changes to it would significantly impact on Public Safety. Operating Commitments are maintained in the Operating Commitments database.
Operating Documentation	The documents produced by Operations to facilitate operation of the station and to provide training to station personnel. They include Operating Manuals, Flowsheets, Training Manuals, Operating Memos, etc.

Originator	Anyone, inside or outside the department who identifies the need for a change. Usually this will be the System 'Engineer'.
Parent DR	The Deficiency Report on which the originator or System 'Engineer' describes the deficiency with the system, equipment or computer software which a change is required. A Parent DR is required for all changes.
Proposed Change (refer to Appendix A)	This form documents the reason for the change and the expected cost. The form is routed to designated internal and external parties for review and comment.
Request for Documentation Update Form (refer to Appendix B)	This form is used to request revision of design documents. Separate Request for Documentation Update forms will be issued for mechanical changes, for wiring changes and process computer changes. Before the in-service date of the last unit, DED will cover the cost of document revisions; after that, a blanket EWR will be issued periodically to cover the cost of having these revisions made. NOTES: 1. Please put system name in the first line of 'description of service.' 2. Please indicate on the second line of the 'description of service': the units to which this revision will be made as a Minor Change and to which units it applies as a normal drawing revision.
SRL	System Routing List: A computerized printout of wiring routine and terminal information used mainly by Control Maintenance.
Sub DR	Any DR written to have work done which is directly related to implementing the change identified by the Parent DR.
System 'Engineer'	That member of the DNGS'A' Technical/ Commissioning Unit to whom the Technical/ Commissioning Superintendent has delegated the technical responsibility for the system. This is usually the person specified in the SCI responsibility list.
TSP	Technical Section Procedure: A written procedure used by the Technical Unit.
Wiring Package	Drawings and documents related to a wiring change.
WMS	Work Management System: A computer system used to keep track of work at DNGS'A'.

3.0 PROCEDURES

3.1 RESPONSIBILITIES

The following is a general description of the stake holders' responsibilities in permanent changes at DNGS'A'. The detailed responsibilities and activities associated with permanent change procedures are specified in sections 3.2, 3.3 and 3.4 of this SRP.

Changes to licensing documents and operational changes are discussed in section 3.5 'Requirements for AECB Approval of Changes'.

1. Operations are responsible for:

   a. obtaining approval in principles for all changes,

   b. implementing and documenting all changes,

   c. returning installation confirmation and as-built information to DED for all changes, and

   d. ensuring that the change is consistent with licensing documents.

   e. obtaining AECB approval as required for changes after the Operating License is issued.

2. Construction is responsible for:

   a. preparing the Installation Package, liaising with DED, installing and turning over a change when requested to do so by Operations

   b. providing qualified personnel to assist the Production Section to install a change when requested to do so

   c. conveying to Operations, documentation that adequately reflects the field condition and the status of any completed or incompleted change, which they have been requested to execute by Operations, and to cooperate with the Operations Planning Section concerning the scheduling of such activities.

3. Darlington Engineering is responsible for:

   a. designing and engineering changes as requested by Operations

   b. securing design approvals (except AECB approvals after the Operating License has been issued), and

   c. updating and reissuing design documents altered as a result of the change.

4. The Technical and Commissioning Sections are responsible for administration of the Change Control Procedure.

5. The System 'Engineer' is responsible for ensuring that a complete Change Package is prepared for every change: PCs, EWRs, Work

Plans, etc. He shall also ensure that the operating and training documentation is revised/prepared and issued and that any required retraining is arranged.

The System 'Engineer' is also responsible for getting mechanical documentation revised to accurately reflect the change.

6. The System 'Engineer's' Supervisor is responsible for verifying that all technical activities required to implement a change are completed.

7. The Technical or Commissioning Superintendent is responsible for ensuring that the change meets the station needs and is consistent with licensing documents, and that the technical work is performed and verified by competent personnel. He is also responsible for verification of the PC (see exception noted in section 3.3 paragraph 2 of this SRP).

8. The Maintenance Superintendent is responsible for ensuring the change is installed in the field by competent personnel.

9. The Technical Manager is responsible for reviewing all PCs and EWRs to ensure adequate control of new project work.

10. The Production Manager is responsible for authorization (except for Minor Changes not requiring AECB approval) and execution of all field work associated with a change.

11. The Station Manager is responsible for approving all PCs and ensuring that appropriate approval or information requirements are identified (see exception noted in section 3.3 paragraph 2 of this SRP). He is also responsible for approving ECN-AMs for category 1 and 2 EWRs.

12. The Production Section is responsible for the performance and documentation of the field work necessary to implement a change. The documentation shall include all completed Work Plans marked up with pertinent information and the associated work reports.

13. The Control Maintenance Documentation Group is responsible for ensuring that the electrical and I&C documentation accurately reflects the change. The CM Documentation Group prepares Work Packages, as requested by the System 'Engineer' and marks up drawings to show changes to the Wiring Package. The CM Documentation Group also forwards Electrical and I&C Change Completion documentation to Darlington Engineering.

14. The Planning Section is responsible for monitoring the preparation for the change, scheduling the execution of the field work and monitoring/reporting the status of the change.

15. The Training Section is responsible for ensuring that station staff receive any training resulting from the change, as authorized by the Production Manager.

16. The Business Section is responsible for:

    a. the distribution and filing of documents pertaining to change,

    b. the cost and variance monitoring and reporting of a change,

    c. the procurement and availability of materials

3.2 CHANGE CONTROL OVERALL PROCEDURE

The overall procedure for controlling changes at DNGS'A' is outlined in Figure 1. This flowchart is meant to guide the reader to the correct detailed procedure to follow when making a permanent change to a system, equipment or process computer software on or after the ECN start date.

Changes to licensing documents and operational changes are discussed in section 3.5 'Requirements for AECB Approval'.

Changes identified before the ECN start date that can be installed before the turnover date will be handled by CND drawing revision. (If the change is to be handled by CND drawing revision, the Design Package and materials must be available at site before the ECN start date.)

If the change cannot be installed by the turnover date, these procedures in this SRP must be followed.

A description of the steps in the Figure 1 is given in the correspondingly numbered paragraphs below. This procedure shall be completed before the ECN or Minor Change procedure is started.

1. When any deficiency is identified which requires a change to correct, a Deficiency Report shall be issued to the Technical Section. This DR is the initiating or 'Parent DR'. If the originator of the Parent DR is not a member of the DNGS'A' department, the System 'Engineer' must raise the Parent DR.

2. The System 'Engineer' shall investigate the problem and formulate a proposed solution. He/she shall then contact the System Design Engineer at DED and discuss the problem, the solution and the appropriate procedure to use to implement the change. If the minor change procedure is to be followed, the System 'Engineer' (operations) shall follow-up the discussion with a memo (speedy) or telex to the Senior Design Engineer with a copy to the System Design Engineer.

   The System 'Engineer' shall then present his findings and recommend to his Superintendent a draft solution (with alternatives) and the proposed procedure to implement the solution. The decision rules for his recommending the appropriate change procedure shall be those outlined in paragraphs 3 and 4 below.

   Further discussions with DED shall take place as appropriate.

3. The Technical/Commissioning Superintendent shall decide if the change requires assistance from DED (engineered change). After considering the recommendations of the System 'Engineer', he shall make this decision based on the following decision rules:

   a. Is the design intent altered?

   b. Is any engineering analysis required?

   If the answer to either of these questions is yes, the ECN Procedure shall be used to implement the change. Also see exceptions to Minor Change Procedure noted in paragraph 6 below.

4. If this is not an engineered change, the Technical/Commissioning Superintendent shall determine if any design documentation will require revision as a result of the change. The Minor Change

Procedure shall be used to implement changes which will require revision of any design document.

If this is not an engineered change and revisions to design documents will not be made as a result of the change, the change can be made by normal Work Package procedures. Such a change is not considered to be a design change.

5. Changes which are not design changes can be made via normal Work Package Procedure with the consent of the responsible Technical Superintendent. In these cases, the System 'Engineer' will raise a Sub DR to the appropriate Production Work Group to correct the problem. These Sub DRs shall be verified by the responsible Technical/Commissioning Superintendent.

   When the change is made satisfactory to the System 'Engineer', he will sign off the Parent DR.

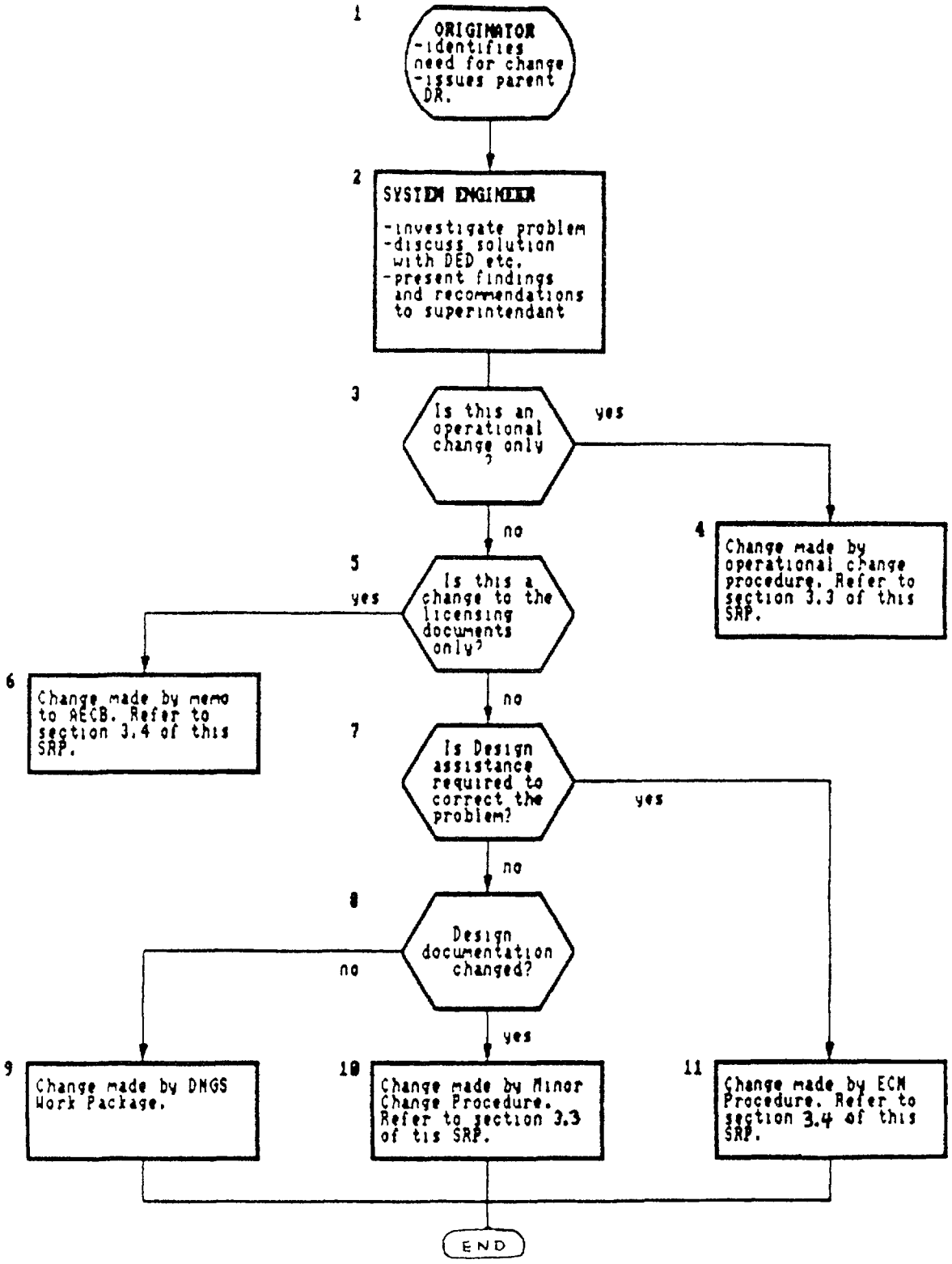


Figure 1. Overall Change Control Procedure

6. The Minor Change Procedure is used to make minor design changes which are meant to ensure the system performs as per the design intent. The Minor Change Procedure does not apply to changes to design intent, changes to special safety systems after unit 2 criticality or to changes involving design ordered 'E' type materials. Refer to section 3.3 of this SRP for a detailed description of this procedure.

7. The ECN Procedure is used to make engineered changes. All approved changes to the design intent of a system, equipment or process computer software after the ECN start date shall be implemented via this procedure. Refer to section 3.4 of this SRP for a detailed description of the ECN procedure.

Annex 8

COMPUTERIZED EVALUATION SYSTEM FOR NUCLEAR EQUIPMENT RELIABILITY

(Used by Kansai Electric Power Company, Inc., Japan)

NUCLEAR EQUIPMENT RELIABILITY EVALUATION SYSTEM

The Kansai Electric Power Co., Inc.

Nuclear Power Operations Department

CONTENTS

1. Objectives of Reliability Evaluation System

Objectives: To ensure the continued stable safe operation of nuclear power plants and to improve the availability.

The following are crucial to achieve these objectives:

(1) Prevention of similar accidents or failures happened before.

(2) Prevention of possible accidents or failures in nuclear power plants.

(3) Rapid and appropriate recovery actions in the case of accidents or failures.

It is necessary to continuously grasp problems in design and manufacturing of equipment, aging degradation and others, utilizing them in the improvement of system components or the inspection and maintenance. Therefore, the system has developed to meet the needs for a computerized systematic classification of the increased trouble information, operating records, and maintenance records with the operating years, as well as the quantitative analysis to obtain information required for improvement. (See Fig. 1)

2. Details of Reliability Evaluation System Development Process

We have conducted the construction and the operation of nuclear power plants as a pioneer in nuclear power generation; however, main actions taken till 1979 or 1980 were separate measures against initial failures, and the systematic evaluation for the increased maintenance and failure information on equipment was not satisfactorily performed. Detailed measures against failures and their development into other plants were also insufficient.

From 1980, we started to review a system which would be

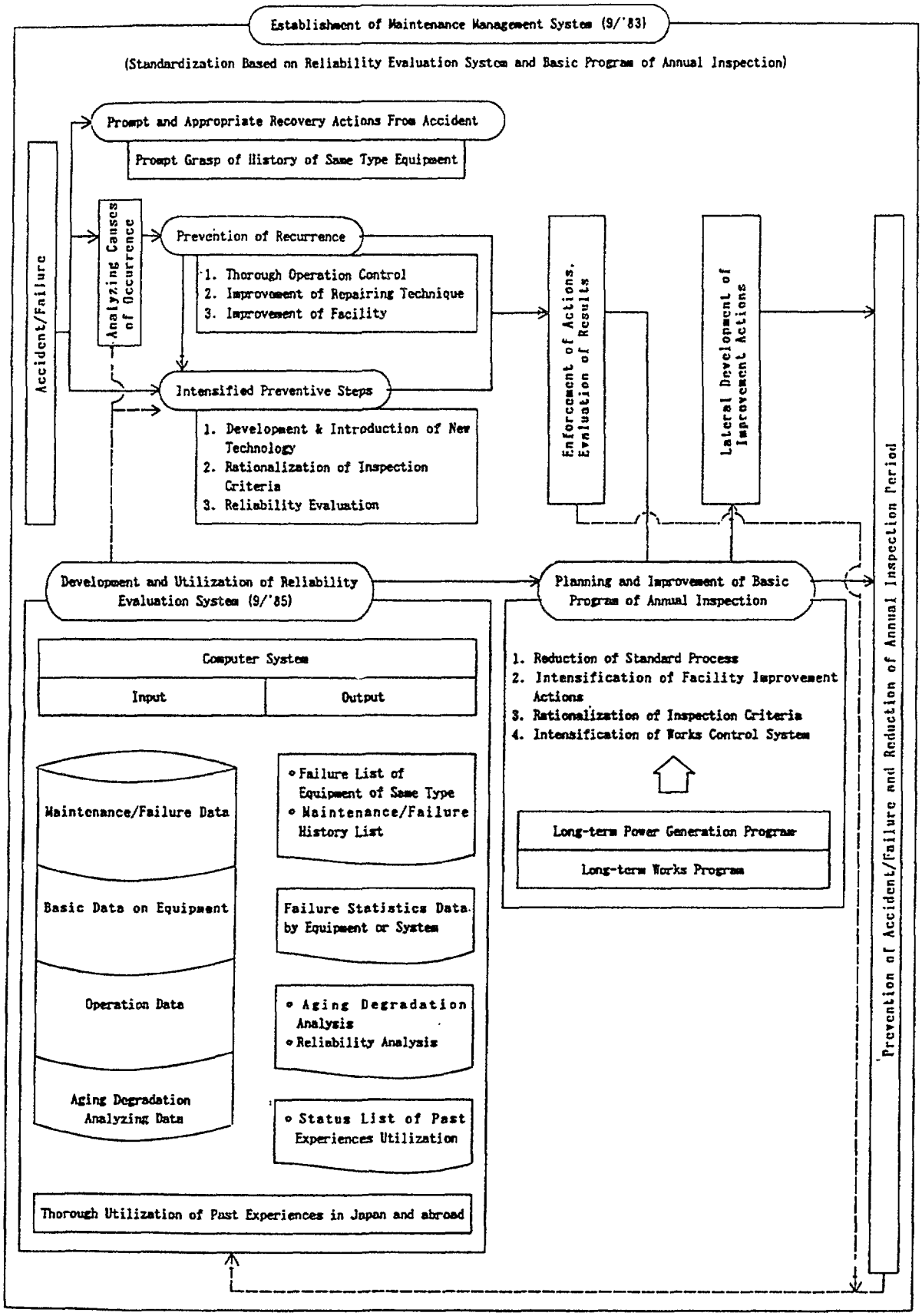


Fig. 1 Reliability Evaluation System in Maintenance Management

available for the earlier countermeasures against potential failures and enhancing equipment reliability, such as preventive maintenance, by numerically and diversely analyzing the maintenance/failure data. The review resulted in the full-scale operation of the computer-aided data base and the utilization system (the computer-aided Reliability Evaluation System) from 1984.

3. Outline of Reliability Evaluation System

The computer-aided Reliability Evaluation System consists of four sub-systems; data storage system, statistics system, retrieval system and analysis system. It is designed to allow the stored data to be input and output in the interactive on-line system at power stations, Fukui Nuclear Power District Office or the Headquarters. The System features the capability to process the information in Chinese characters to the utmost for meeting the user needs, which leads to the increased information and the frequent utilization of the system.

Though the data stored is limited to the KEPCO's for the time being, it covers the system data and the plant and equipment operating data as well as the maintenance data (during both operation and outage). (See Fig. 2)

4. Reliability Evaluation System Input Data

The data processed by the Reliability Evaluation System is largely divided as follows:

(1) Maintenance/Failure Data; involves the equipment maintenance and failure records, including the Work Orders, the Slips for Failures Found during Annual Inspection, the Report on Troubles, the Reports on Improvements and the Annual Inspection Work Records.

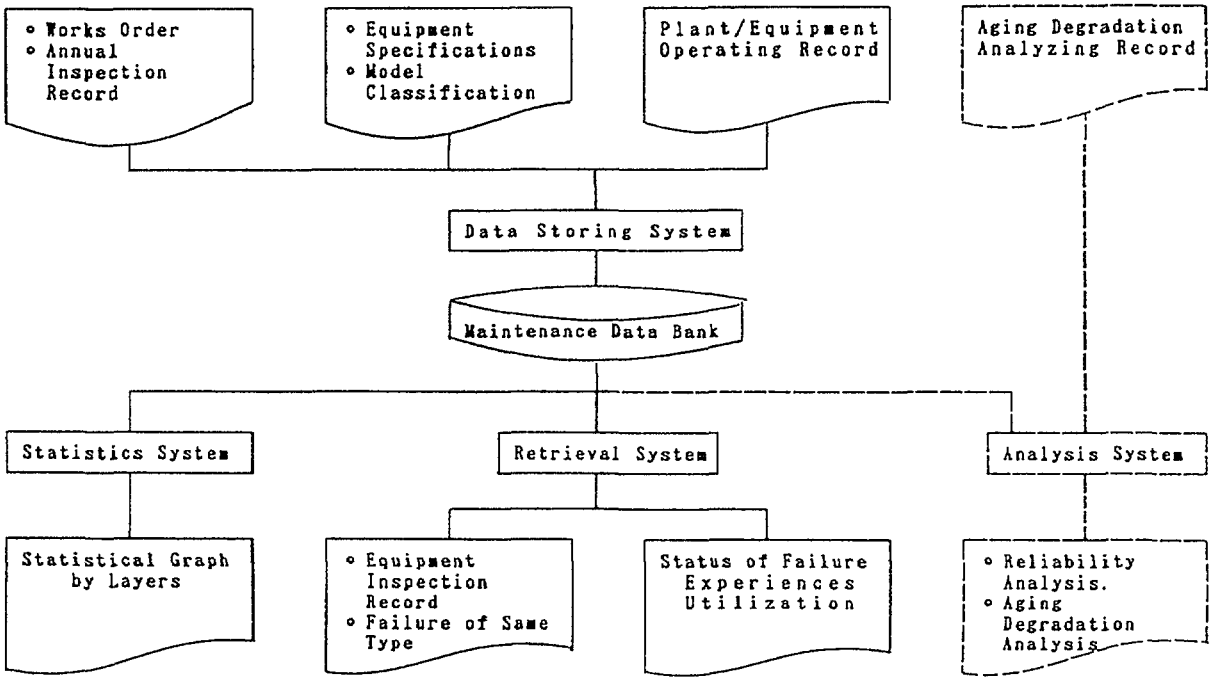


Fig. 2 Outline of Reliability Evaluation System

(2) Basic Data on Equipment; involves the basic specifications such as the models, manufacturers and design values.

(3) Operation Data; involves the start-up/shutdown data of plants and the main rotating machines.

For the maintenance/failure data and the operation data, the new methods were introduced in 1983, and the data storage has begun since then. A part of these data were retroacted to 1980.

For the equipment data, major equipment among valves, pumps, tanks, heat exchangers has been already recorded. Preparation is under way to further extend the coverage of the data.

a. Work Order Data

The Work Order is a sheet issued every inspection/repair of failures during plant operation, surveillance test or periodic inspection. It contains both the coded information including the equipment concerned, purpose of the issue, conditionis of the failure found, actual date of start and completion of the work, and causes of the failure, and the description in Japanese such as the contents of the work (conditions of the failure) and the results (actions for the failure). This data

provides the basis for reliability evaluation of nuclear power plants which is the objective of the System.

b. Slips for Failures Found during Annual Inspection

It is issued when the failure event is found during the annual inspection. The contents and the nature of data are the same as those of the Work Order Data. This is a newly added sheet for the operation of the System.

c. Reports on Troubles

This is issued for repair works with high priority such as modification work. It provides the detailed information of the Work Orders and the Slip for Failures Found during Annual Inspection, including the detailed conditions and analyses of the causes.

d. Reports on Improvements

Based on the failures of other units, this sheet is issued for improvements of plant systems with high priority. Included in the report is data on the equipment concerned, and the reasons and contents of the improvement actions, constituting a part of the equipment records.

e. Annual Inspection Work Records

This is issued for every equipment in annual inspection. It includes data on the contents and results of the inspection, repairs, etc., constituting a part of the equipment records.

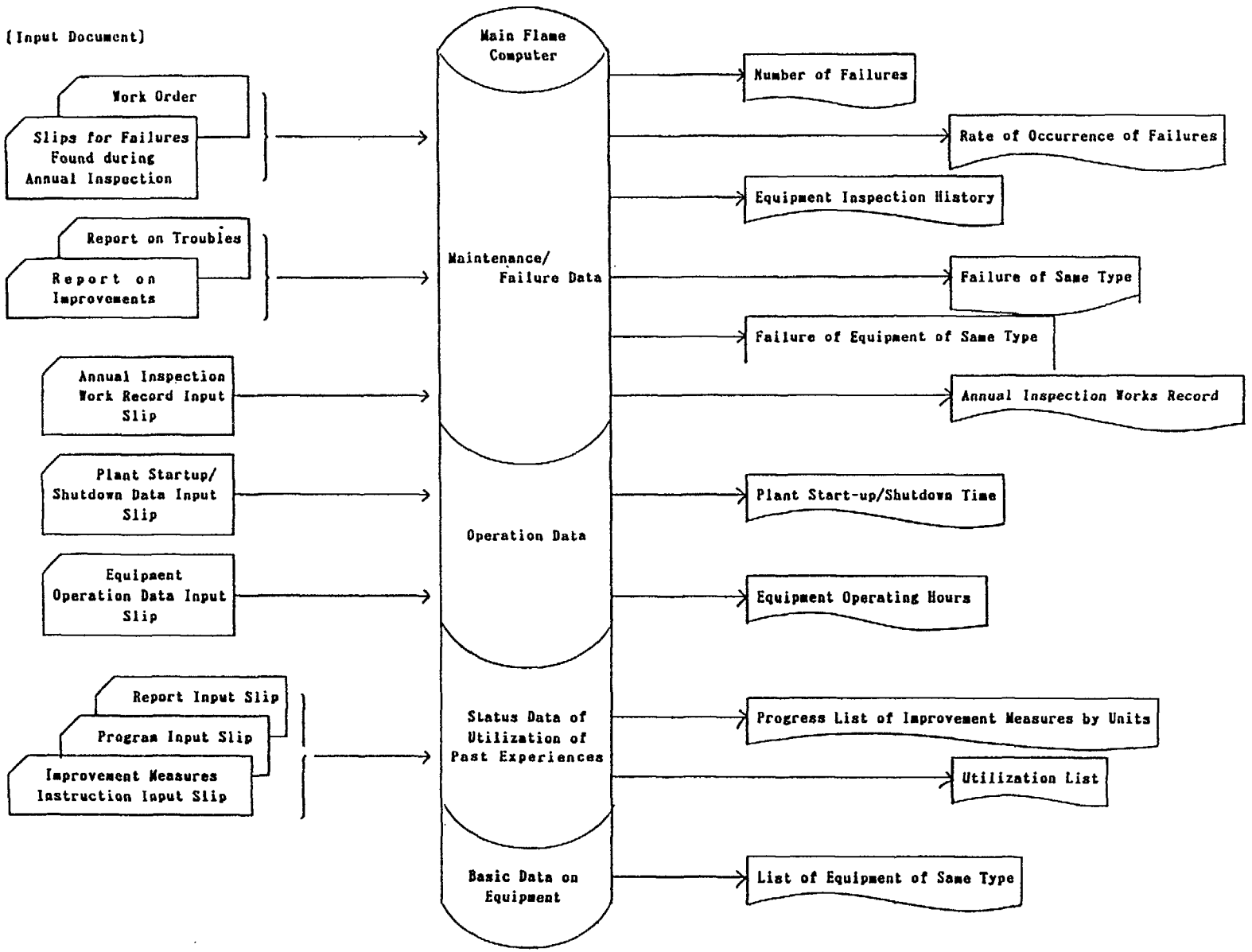
(See Table 4-1, 4-2)

Table 4-1 Input Items of Work Orders (Reports on Troubles)

1. File Number
2. Date of Issue
3. Purpose
4. Section concerned
5. Equipment Code
6. Issue of Safety Work Card
7. Necessity of Procedure
8. Name of Equipment *
9. Name of Works *
10. Contents of Works (Conditions of Trouble) *
11. Date of Occurrence (Found Date) of Trouble
12. Plant Conditions When Trouble Is Found
13. How Trouble Is Found
14. Failure Conditions When Trouble Is Found (1)
15. Failure Conditions When Trouble Is Found (2)
16. Failure Conditions When Trouble Is Found (3)
17. Emergency Level of Works
18. Started Date of Works
19. Completed Date of Works
20. Work Area
21. Results of Works (Actions against Troubles) *
22. Contents of Works
23. Work System
24. Contractor
25. Manday
26. Actual Work Hours
27. Exposure
28. Cause of Failure (1)
29. Cause of Failure (2)
30. Cause of Failure (3)
31. Influence on Plant
32. Radioactivity Release
33. Issue of Report on Troubles
34. Detailed Conditions of Trouble *
35. Emergency Actions *
36. Description of Cause *
37. Permanent Actions *
38. Direct Cause
39. Root Cause (1)
40. Root Cause (2)
41. Completed Date of Permanent Actions

* Input in Japanese (Chinese characters)

Table 4-2 Reliability Evaluation System Input/Output Data



5. Output Function of Reliability Evaluation System

5-1 Statistics System

It generates the Number List from the maintenance data stored, based on the coded classification such as equipment failures. It privedes the information utilized for the understanding and the analyses of failures of the equipment of the same type by manufacturers or by specifications in cooperation with the understanding of trends in failure occurrence, the analyses of factors of failure and the equipment data.

a. Number List; allows division for all coded items input. It can display a three-dementional matrix table and various graphs.

b. Rate of Occurrence List: directed to compare the equipment parameters rate with the equipment-related items in the Number List. It can display a three-dimentional matrix table and various graphs.

5-2 Retrieval System

It extracts the maintenance data stored based on the various conditions and displays the contents of the data, providing the following functions depending on the methods or the object of the extraction.

a. Inspection Record Retrieval: displays the failure and maintenance records of separate equipment by order of occurrence.

b. Failure of Same Type Retrieval: displays records of the failures by conditions, causes, etc.

c. Failure of Equipment of Same Type Retrieval: displays the records of the failures of the same equipment in other units.

d. Same Equipment Retrieval: displays the equipment whose manufacturer, design values, criteria, etc. are the same.

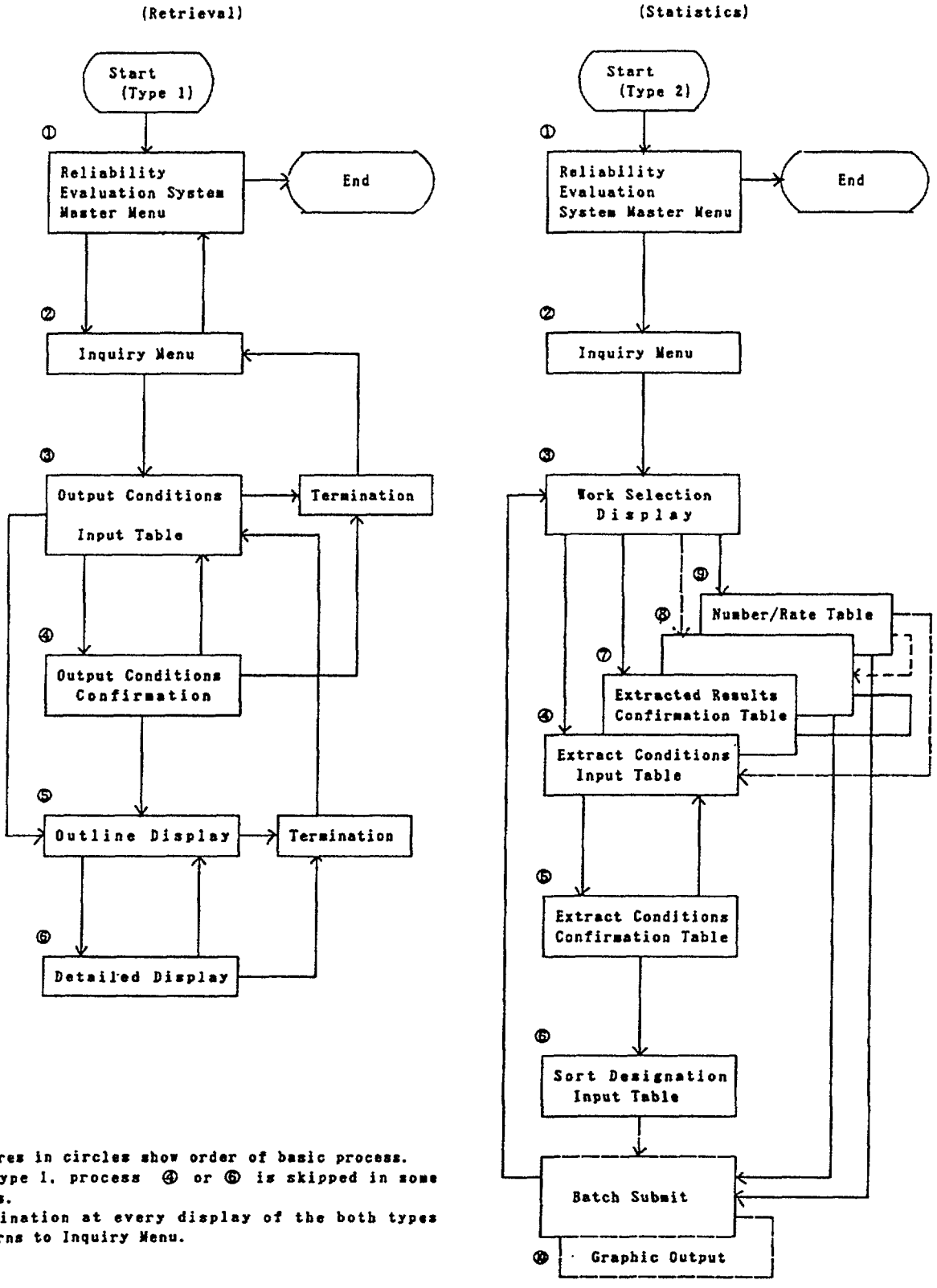
5-3 Analysis System

It provides the data necessary for analyzing the equipment reliability through the comprehensive evaluation and statistics on the stored maintenance/failure data, the equipment data and the operation data.

a. Reliability Analysis; intended for the mainly controlled equipment and computes the failure rate (λ), the mean time to repair (MTTR) and availability (A) of the equipment.

b. Weibull Analysis; components with the potential wear-out failure of important equipment are selected and their failure modes are also determined. Weibull distribution of failure history is then calculated for each component to determine its average life. Details of the data acquisition range will be decided in future.

Basic Process Pattern (On-line Inquiry)



Figures in circles show order of basic process.
In Type 1, process ④ or ⑤ is skipped in some works.
Termination at every display of the both types returns to Inquiry Menu.

Figure 5-1 Usage Flowchart of Reliability Evaluation System

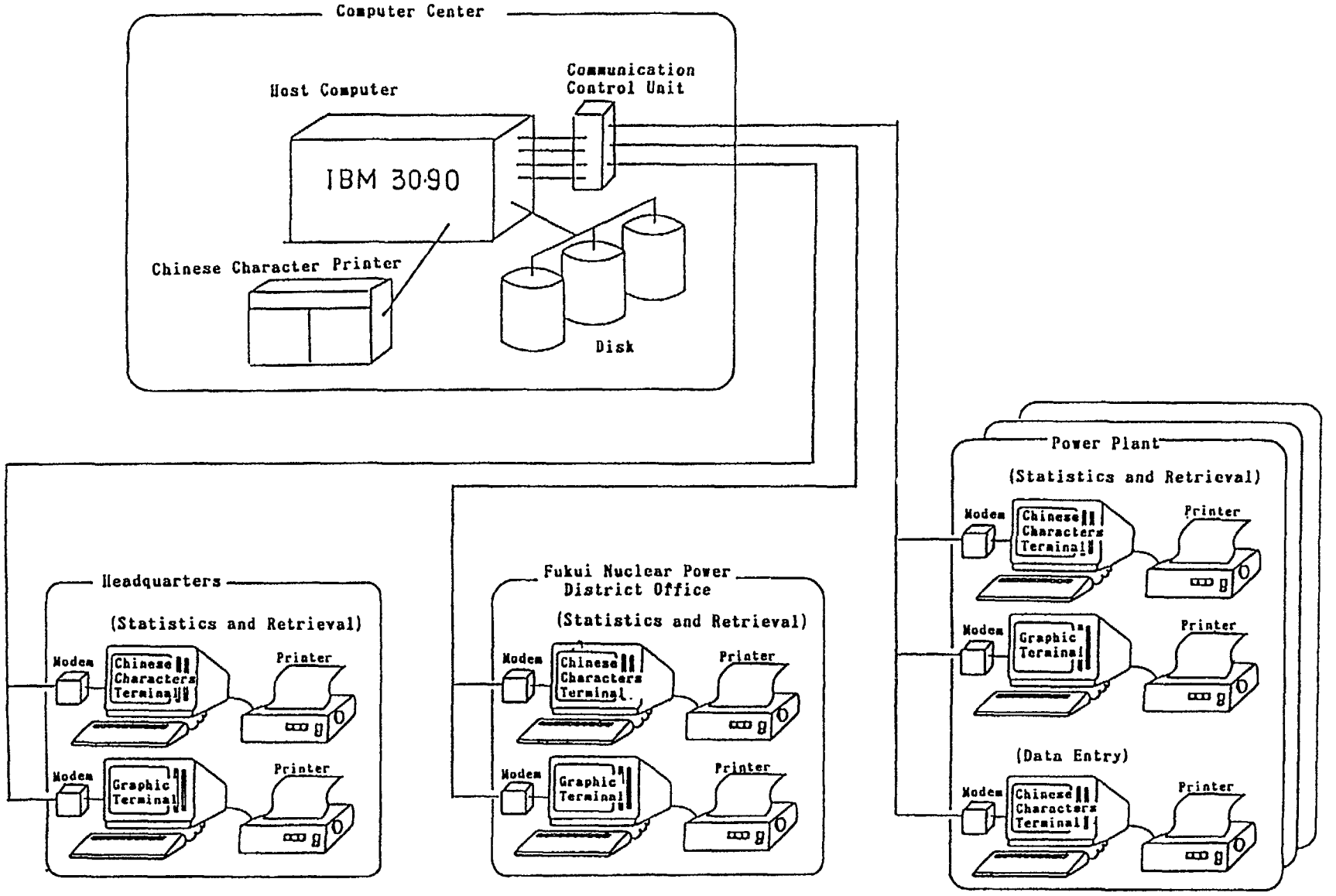


Fig. 5-2 System Hardware Configuration

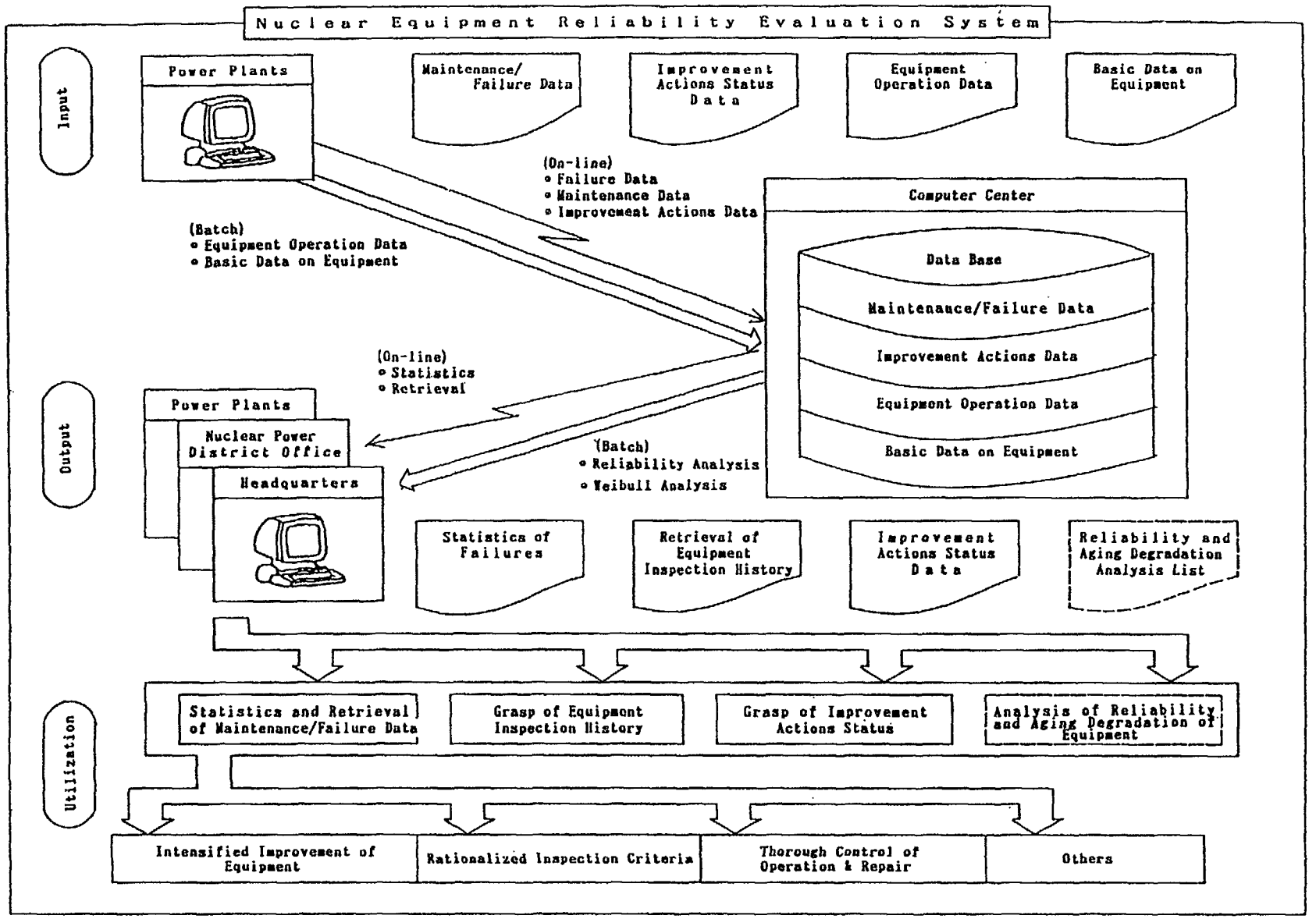
6. Utilization of Reliability Evaluation System

The system offers the statistics, retrieving and analyzing functions. The users can easily acquire the references required to solve the problems, optimizing a combination of these functions to meet a particular purpose.

For example, the overall trend of a failure is available by using the statistics function, which tells a weakpoint of the plant. The data for reliability evaluation and the technical review of the equipment are input to the system by the analyzing function to determine the ranges and items of examinations. Then the retrieving function provides the detailed information of failure, and inspection history and operating conditions of the equipment as the review material. If further information is needed, the related document will be available in link with the document filing system.

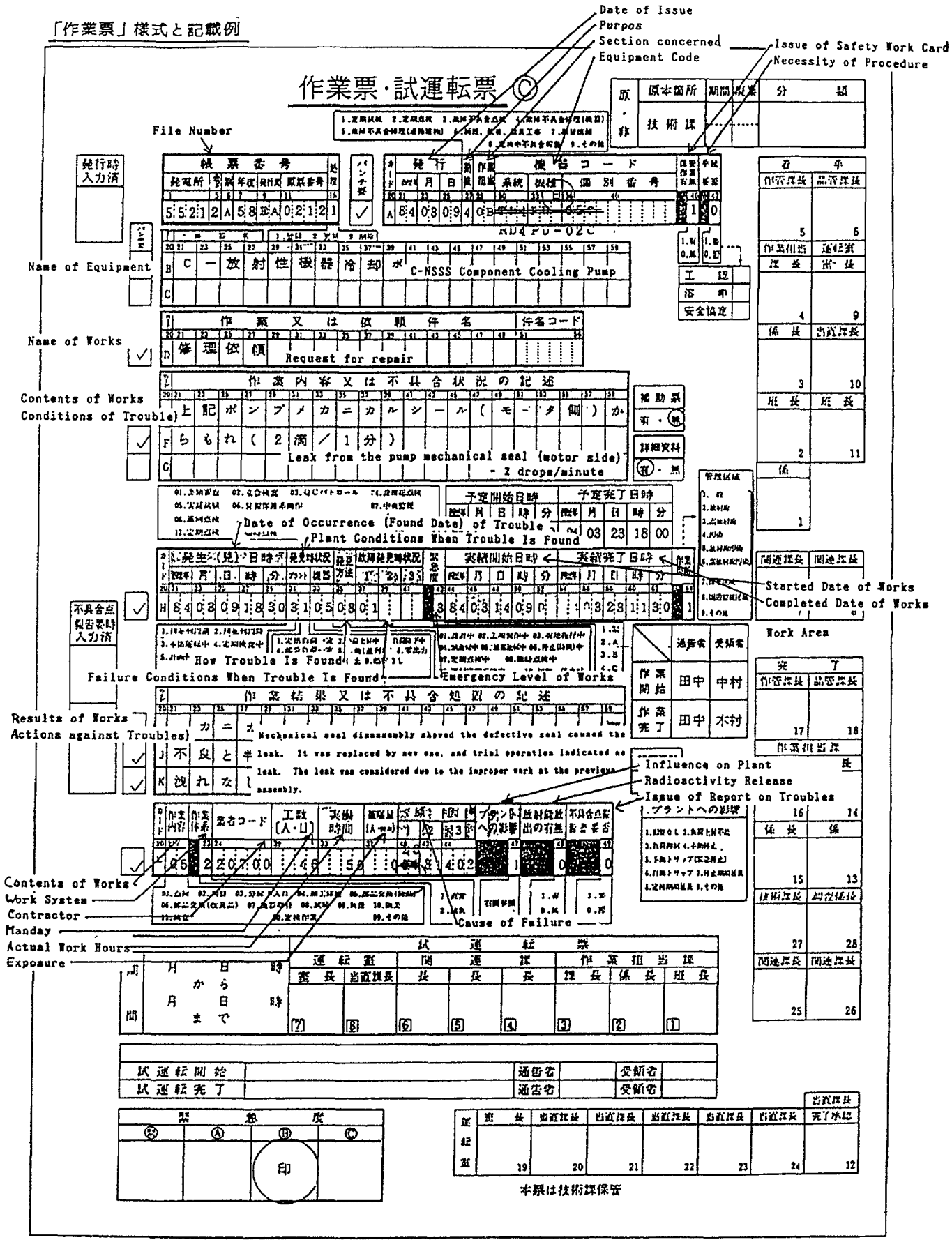
Based on the information acquired in this way, failure patterns and component life are calculated through technical reviews, determination of components which require corrective actions and of their failure modes, and Weibull analysis to plan and execute necessary actions.

Reference 1: System Outline



Reference 2: Work Order

「作業票」様式と記載例



Next page(s) left blank

LIST OF PARTICIPANTS

WORKING GROUP 3-7 APRIL 1989
ON
OSART GUIDANCE AND REFERENCE MATERIAL ON
COMPUTER CAPABILITIES

CANADA	J.E.S. Stevens	AECL, Toronto
FRANCE	J. Libmann	Institut de Protection et Sureté Nucléaire
FEDERAL REPUBLIC OF GERMANY	G. Grenz	Siemens AG KWU
GERMAN DEMOCRATIC REPUBLIC	F. Baldeweg	Institute for Nuclear Research
JAPAN	Y. Nishimura	The Kansai Electric Power Co., Inc.
	F. Sato	Nuclear Power Safety Information Research Centre
SWEDEN	O. Andersson	Forsmark Nuclear Power Plant
UNITED STATES OF AMERICA	N. Kretschmer (Chairman)	Braidwood Nuclear Power Plant
YUGOSLAVIA	Z. Reljic	Krsko Nuclear Power Plant
	M. Smolej	Krsko Nuclear Power Plant
IAEA	V. Solyany	Scientific Secretary, NENS
	C. Almeida	NENS
	L. Lederman	NENS

CONSULTANTS SERVICES
3-14 April 1989
OSART GUIDANCE AND REFERENCE MATERIAL
ON COMPUTER CAPABILITIES

SWEDEN	O. Andersson	Forsmark Nuclear Power Plant
UNITED STATES OF AMERICA	N. Kretschmer	Braidwood Nuclear Power Plant
IAEA	V. Solyany	Scientific Secretary, NENS