XA9642968

XA9642968

IAEA-TECDOC-906

Designing nuclear power plants for improved operation and maintenance

IAEA

September 1996

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.

IAEA-TECDOC-906

Designing nuclear power plants for improved operation and maintenance

INTERNATIONAL ATOMIC ENERGY AGENCY IAEA

The originating Section of this publication in the IAEA was:

Nuclear Power Engineering Section
International Atomic Energy Agency
Wagramerstrasse 5
P.O. Box 100
A-1400 Vienna, Austria

DESIGNING NUCLEAR POWER PLANTS FOR IMPROVED OPERATION AND MAINTENANCE
IAEA, VIENNA, 1996
IAEA-TECDOC-906
ISSN 1011-4289

Printed by the IAEA in Austria
September 1996

FOREWORD

One of the lessons that the nuclear power industry has learned from its many years of experience is that a plant should be designed from the outset to make it readily operable and maintainable over its life. This includes providing standardization of components, designing equipment to minimize maintenance needs, designing to reduce occupational exposure to ionizing radiation, and designing to facilitate those maintenance needs that do exist. Such needs include activities to support inspection, test, repair, and replacement of equipment and systems over the plant life and assuring that adequate access, laydown space, tooling and services are provided as part of the basic plant design. It also includes consideration of the environment in which operation and maintenance activities are performed. Important aspects of operability and maintainability are human factors considerations. These include those aspects of the design which affect:

- monitoring, controlling and protection functions assigned to plant operators,

- monitoring and diagnostic functions performed by plant engineers and managers during normal, upset and emergency conditions, and

- inspection, on-line and off-line surveillance testing, preventive maintenance and corrective maintenance functions assigned to maintenance personnel.

The current IAEA programme in nuclear power implementation includes efforts to provide feedback to designers for better operability and maintainability of nuclear power plants. It is hoped that this publication will be useful to those organizations in Member States that are responsible for the design of new power plants or for upgrading existing designs.

The IAEA wishes to thank all those who took part in the preparation and review of this publication.

EDITORIAL NOTE

CONTENTS

1. INTRODUCTION

The purpose of this publication is to compile demonstrated, experience based design guidelines for improving the operability and maintainability of nuclear power plants. The guidelines are for use principally in the design of new nuclear power plants, but should also be useful in upgrading existing designs. The guidelines derive from the experience of operating and maintaining existing nuclear power plants as well as from the design of recent plants. In particular these guidelines are based on and consistent with both the EPRI Advanced Light Water Reactor Utility Requirements Document, Volume 1 [1], and the European Utility Requirements for LWR Nuclear Power Plants [2].

The target audience for this publication is those utilities in Member States that now operate or are planning to operate nuclear power plants. The report is also expected to be useful to designers, and in aiding communication between designers and utilities.

The selection of the guidelines was based, consistent with safety requirements, on reducing the cost of operating and maintaining nuclear power plants. Given that safety is a fundamental requirement in nuclear power plant operation, it is recognized that improvements in operability and maintainability will also improve safety. The guidelines encourage the implementation of design attributes and features chosen to:

- Improve plant availability – plant availability is a primary factor in determining electric production costs and is therefore critical to the success of any design. Particular emphasis is given in the guidelines to reducing the frequency and duration of planned and forced outages.

- Reduce direct and indirect costs – the guidelines encourage the implementation of operability and maintainability features which reduce:

    - labour costs for operation and maintenance
    - other maintenance costs (e.g. materials, spare parts, tools)
    - radiation dose related costs
    - logistics support costs (e.g. configuration management).

- Increase standardization and simplification – using standard and simplified systems, components and structures within and among nuclear power plants directly improves the ability of the plant operator to cost effectively operate and maintain one or more nuclear power plants. For example, operations and maintenance training is simplified and reduced, spare parts inventories are optimized and reduced, modular component replacement can be used to reduce forced outages and on-line maintenance, etc.

While the guidelines provide the greatest benefit when implemented in new designs, they can be used to identify areas for improvement in existing plants and as guidelines for the design of upgrades and retrofits to existing plants. Since upgrades and retrofits can be costly and can perturb already adequate approaches to operations and maintenance, the designer must pay particular attention to:

- The cost–benefit assessment of implementing design features encouraged by the guidelines. For example, the costs of implementing a new man–machine interface system (M–MIS) in an existing monitoring or control system can be difficult to estimate in the pre-project phase and have sometimes overrun estimates by an order of magnitude.

– Avoiding the introduction of unintended effects – using the above example, introducing a new M–MIS to an existing monitoring or control system perturbs the established training and procedures for interfacing with the system and can lead to operating errors. Errors can be potential or latent for weeks, months or years after the introduction of the new M–MIS.

An approach to implementing these guidelines is suggested in Section 8.

2. PLANT OPERABILITY GUIDELINES

The following guidelines relate to desirable design features and attributes which improve the operability of a nuclear power plant. These guidelines address how the plant operator interfaces with the physical plant, procedures and training as well as design considerations intended to reduce the frequency and duration of forced and planned outages. A design which conforms to these guidelines will be (relatively) more resistant to and tolerant of operator error as well as have (relatively) fewer and shorter planned and forced outages. Therefore, such a plant will enjoy higher availability and lower production costs.

2.1. PLANT CHARACTERISTICS

2.1.1. Overall availability

An overall availability target for the design should be established and the plant should be designed to achieve that target. The target should consider, as a minimum:

- Experience with similar designs
- Site characteristics including external events
- Economic analysis of the target cost of producing electricity and competitive positioning relative to other indigenous sources of power
- Outage duration and fuel cycle length
- Cost effective implementation of on-line maintenance capability
- Safety considerations
- Grid requirements, especially any manuevering requirements
- Plant size
- All relevant regulatory requirements for that design, especially required periodic inspection.

2.1.2. Planned outage duration and frequency

Targets for planned outage frequency and duration should be set consistent with the overall availability target and the plant should be designed to achieve that target. Since availability is very dependent on outage length, the design outage should be divided into logical phases with target durations established for each phase. The plant systems and components should be designed to cost-effectively achieve those targets. The targets should consider as a minimum:

- Experience with similar designs
- Fuel cycle length (if applicable)
- Pre-outage accessibility to outage work areas, especially adjacent to the containment equipment hatch and inside the containment
- Plant tests and inspections, especially major ones
- Maintenance requirements
- Provision in the design for pre-outage preparation and work, especially accessibility (e.g. removable fuel handling equipment controllers, crane and hoist checkout).

2.1.3. Forced outage duration and frequency

Since both safety and availability are impacted by forced outages, the design should cost effectively reduce the frequency and duration of forced outages, considering, as a minimum:

- Grid tolerance of forced shutdowns
- Design features which prevent unnecessary reactor shutdowns, such as runbacks, limitation systems, load rejection without reactor trip, partial loss of coolant flow capability
- Ability of the design to recover to power operation in minimum time
- Systematic analysis of forced outage experience feedback
- Careful design of relevant plant operating procedures and technical specifications
- Cost effective diagnostic features designed to determine the cause of the forced outage.

2.1.4. Overall occupational radiation exposure

A target should be set for the average annual collective dose from occupational radiation exposure and the plant should be designed to achieve that target (see Section 6).

2.1.5. Choice of number of trains/channels

The selection of the number of equipment trains and I/C channels for safety related and non-safety related systems should consider:

- Capital, operating and maintenance costs
- Flexibility in achieving the design planned outage length
- Safety system performance (e.g. elimination of cross connects, independence of systems)
- Plant operability while shutdown with emphasis on shutdown risk considerations
- The ability to test and inspect safety and non-safety I/C and fluid/mechanical systems at power
- System availability achieved through component and/or train redundancy
- Single failure proof design of non-safety fluid/mechanical and control systems which have a significant impact on availability
- Simplification of the design (e.g. design of relief and safety valves).

2.1.6. Operating experience feedback

The design process should include and incorporate the output of a systematic operating experience feedback programme which evaluates the operating history of similar and other designs and makes specific recommendations to improve the design.

2.1.7. Special plant configurations

The plant should be designed to be effectively and safely operated in required special operating modes (e.g. reduced water inventory/mid-loop operations), which have been necessary to simplify operation and meet availability goals.

2.2. MANOEUVERING AND TRANSIENT RESPONSE

2.2.1. Plant startup

The plant should be designed to be capable of startup from cold shutdown to full power within a target duration consistent with the availability targets of the design. Areas for design improvement are:

- Physics testing
- Safety system tests
- System leak and hydrostatic tests
- Permissible heatup and pressurization rates
- Achievement of desired chemistry conditions.

2.2.2. Plant upset and emergency response

The design of the plant should consider features which yield forgiving plant responses to upset and emergency conditions. Such ease of operation will positively influence return to power and therefore, plant availability. A forgiving design should include such features as:

- A minimal need for operator action in mitigating and recovering from upset events
- Ability to sustain load rejection (including loss of grid) without reactor trip
- Sufficient margin between relief and safety valve setpoints and normal operating pressure to minimize lifting
- Gradual plant response to upset events (e.g. sizing of coolant volume relative to power to yield a gradual response to upsets and emergencies).

2.2.3. Load follow and manoeuvering

The design should accommodate manoeuvering and load follow transients including:

- Grid requirements
- Load cycle frequency
- Power reduction/increase rates
- Minimum load follow power level and time at that level
- Core characteristics (e.g. xenon transients)

- Automated control system for load follow response
- Capacity and capability of auxiliary systems (e.g. waste water recovery)
- Ability to operate auxiliary systems from the control room
- Provisions to adjust setpoints for special operating conditions (e.g. N-1 loop operation, reactor stretchout/coastdown).

2.2.4. Grace period for normal actions

For safety considerations and operability in upset and emergency conditions, the design of the plant shall be such that manual actions for upset and emergency conditions are required no sooner than:

- 30 minutes for control room actions
- 1 hour for actions outside the control room
- 6 hours for the use of portable equipment
- 3 days for the use of heavy equipment.

2.2.5. Unplanned automatic trips

The plant should be designed to limit the number of unplanned automatic plant trips to less than one per year. Such design should consider at least:

- Reliability and fault tolerance of control and actuation systems
- Reducing required testing of actuation systems and other systems capable of causing a trip (e.g. automated self-testing)
- Increased operating margin to setpoints of actuation systems
- Lockouts, permissives and other features which minimize or mitigate operator error capable of producing a trip
- Design features which avoid trips such as limitation system, runbacks, and load rejection capability.

2.3. OPERABILITY: TESTS AND INSPECTIONS

2.3.1. Major tests and inspections

Tests and inspections requiring considerable preparations or which can only be performed during outages should be designed such that:

- The frequency and duration of the major test/inspections are consistent with the overall availability goal and with the outage frequency and duration guidelines for the maximum planned interval between outages
- The tests/inspections require the least preparation to the extent feasible
- The tests/inspections are simplified to the extent feasible
- Tests/inspections requiring abnormal plant configurations should be avoided.

2.3.2. Tests/inspections at power

The plant should be designed to permit the maximum amount of tests/inspections while at power. If on-line maintenance is a design intent, then the design considerations below should support post maintenance testing. To facilitate such a design, consideration should be given to:

- Permanently installed radiation shielding at frequent test/inspection locations
- Permanently installed test/inspection features such as full flow bypass lines for pumps, component redundancy, systems isolation and draindown capability, and full flow valve stroking capability
- Provisions for system accessibility (e.g. doors, stairs, platforms, routing through low radiation zones, etc.)
- Periodic testing should be designed to leave as is the negative impact on affected component life
- I/C systems, and in particular safety systems, should incorporate automated on-line self-testing to the extent practical
- To the extent practical, reducing the need for periodic testing by designing systems so that the safety and normal operating configurations are identical, thereby minimizing the need for tesing different configurations
- To the extent practical, design plant I/C systems to permit diagnosis down to the component level while at power without requiring plant power reduction
- Periodic testing should be conducted so as not compromise the safety function of that train.

2.3.3. Temporary test/inspection installations

The plant should be designed to avoid the need for temporary test connections, scaffolding, blind flanges, jumper cables, spool pieces, etc. to perform tests and inspections. If needed, a simple and positive means of identifying the presence of temporary installations should be provided.

2.4. MAN–MACHINE INTERFACE SYSTEMS (M–MIS)

The M–MIS refers to all instrumentation and control systems provided as part of a design that perform requisite monitoring, control, display and protection functions associated with all modes of plant operation as well as off-normal, emergency, and accident conditions.

2.4.1. M–MIS design process

The M–MIS design process should be fully integrated with the overall plant design process; the M–MIS design should begin early in the design process with input from a multi-disciplinary team consisting of operations, maintenance, design and human factors experts. It should use state-of-the-art design techniques to achieve an optimum, cost-effective M–MIS, including:

- Function and task analysis (e.g. level of automation)
- Ergonomic and human factors guidelines
- System availability and reliability analysis
- Static and dynamic simulation as well as other forms of verification and validation.

It has proven useful when designing a new generation of plant and M–MIS to complete the construction of a full scope control room simulator during the design process to permit adequate validation of the M–MIS. High fidelity simulation has proven to be effective in validating backfits as well.

- The capacity (e.g. number of work positions) of the M–MIS should support accomplishing special plant activities and configurations (e.g. startup testing, on-line maintenance) such that the activities can be completed within the design durations.

2.4.2. M–MIS information structure

The information provided at each (main control room and local) M–MIS should generally be structured hierarchically, with flexibility to restructure the hierarchy according to plant modes (e.g. startup, refuelling, operation). The information provided to the operator should support the functions and tasks. The highest level of the hierarchy should display information (discrete parameters and assembled/calculated information) which indicates the status and/or trend of important plant functions. References [3] and [4] provide additional information on M–MIS information structure.

2.4.3. Automated M–MIS functions

As a minimum, M–MIS (main control room and local) should be designed to automatically:

- Validate the information provided to the operator
- Identify to the operator deviation (consistent with plant mode) from expected status, trends and parameter values via alarms, messages, diagrammatic presentations, coding and other means
- Detect and display problems within the M–MIS
- Store key parameters during transients for subsequent analysis
- Provide the operator with directly usable information which does not require calculation, interpolation, or inference for its use in operator tasks
- Evaluate testing and test data of fluid/mechanical and I/C systems.

Special consideration should be given to automating control functions such as operation of the refuelling machine, plant heatup and cooldown, and response to upset and emergency conditions.

2.4.4. M–MIS diagnostic function

The information provided by any M–MIS, should be consistent with the functions to be accomplished at that M–MIS (main control room and local) and should be designed to assist the operator in detecting, diagnosing and correcting unexpected or off normal process, component, system and plant events.

2.4.5. M–MIS location, sizing and access

M–MIS locations (main control room and local) should be designed to accommodate and provide access for the anticipated number of operating, maintenance and other personnel for all modes of plant operation. Sufficient information and control stations should be provided at each M–MIS location to support the division of responsibilities among personnel.

The location of the main control room should be selected to support all of the operations functions outside the control room (e.g. firebrigade) as well as to support interfacing with other plant staff. Required access to the main operating area should be limited by providing other adjoining work spaces for interfacing with plant staff. Access security provisions for the M–MIS (main control room and local) should provide the security function while not inhibiting access during normal or emergency conditions.

2.4.6. M–MIS graceful degradation

The M–MIS should be designed to degrade gracefully. Graceful degradation refers to design features which:

- Isolate failures in the system to prevent propagation
- Provide alternative means of control or sources of information in the event of failure in the primary means
- Provide inherent backup to maintain control and information
- Permit rapid system restoration following failure.

2.4.7. Communication system

An integrated, comprehensive and reliable communication system should be designed to provide plant wide and offsite communications for all modes of plant operation. Design of the communication system should consider separation of operational and administrative functions. The communications system should provide reliable communications (visual and audible) for high noise locations. Special consideration should be given to the capacity and reliability of on-site and off-site communications systems to be used in emergency conditions. Special consideration should also be given to personnel communication in confined spaces and in protective clothing.

2.4.8. M–MIS Environment

The working environment surrounding M–MIS locations should be designed such that environmentally induced operator stress, fatigue and error are minimized. Design considerations should include at least:

- Lighting
- Air temperature and humidity
- Noise
- Standing/seated station ergonomics
- Communications apparatus.

2.4.9. M–MIS post accident environment

Essential M–MIS locations should be designed for post-accident habitability, including the following considerations:

- Radiation
- Contamination
- Steam, smoke, toxic gas
- Access from one M–MIS location to another.

2.4.10. M–MIS alarm scheme

The M–MIS alarms should be designed to inform the operator of deviations from expected conditions for a given plant mode. The design should incorporate such features as:

- Prioritization of alarms
- Operating mode dependence of alarms
- Reduced number of alarms relative to existing designs
- Alarm patterns which assist in diagnosis
- Validated alarm input to prevent spurious alarms
- Indication of plant and equipment status which is distinguishable from the alarms.

2.4.11. M–MIS for special operating modes

The M–MIS should be designed to accommodate special plant operating modes (e.g. reduced water inventory, mid-loop).

2.5. PROCEDURES AND TECHNICAL SPECIFICATIONS

2.5.1. Comprehensive and complete procedures and technical specifications

Procedures should be provided for all operations and maintenance activities (for all modes of plant operation) which are comprised of more than three or four actions. Each procedure and technical specification should be complete and unambiguous, requiring the operator or the maintainer to use a minimum number of procedures or technical specifications at a time and to use information from the M–MIS directly without calculation, interpolation or inference. For example, plant state oriented emergency procedures have been found to reduce the number of procedures required to address events.

2.5.2. Procedures, technical specifications and human factors

Procedures and technical specifications should be developed concurrent with the M–MIS. The goal is to provide a M–MIS and procedures and technical specifications which support each other. The format style and presentation of procedures and technical specifications should observe human factor guidelines.

2.5.3. Planned and forced outage duration and technical specifications

Plant design and technical specifications should be coordinated to support safety and outage performance goals duration. Consideration should be given to:

- Number of trains required to be operable
- Number of I/C channels required to be operable
- Allowed periods of system/component unavailability are consistent with mean times to repair.

3. INFORMATION MANAGEMENT SYSTEM

The information management system (IMS) refers to the systems used to store, present, and manage all information in the power plant (other than that in the M–MIS) that is used to support operations, maintenance, administration, purchasing, security, etc. The lack of such systems and their subsequent development in existing designs has been very expensive and has led to errors in operation and maintenance. The systematic development of such systems in new designs will improve operability and maintainability and, therefore, reduce production costs.

3.1. IMS FUNCTIONS

The IMS should be designed to acquire, store, update, display, output and manipulate information throughout the plant at appropriate locations, and according to the roles and responsibilities of personnel accessing the system. One essential function of the IMS would be to facilitate configuration management of the plant (see Section 4).

3.2. IMS INFORMATION CONTENTS

The IMS should contain essential information related to at least the following:

- Procedures and technical specifications (operating procedures may be in the M–MIS)
- Work management and equipment tagging
- Design basis information
- Technical manuals, drawings, specifications
- Licensing and analytical methods and documentation
- Material management and purchasing
- Operations and maintenance planning
- Plant parameter and equipment operation/maintenance history
- Radiation protection (e.g. dose management, dosimetry).

3.3. IMS HUMAN FACTORS

The IMS information structure and access and the input/output hardware and software should be designed in accordance with human factors principles to ensure efficient, error free access to the IMS on demand.

3.4. IMS SPECIFIC CONTENT SELECTION

Certain analyses, such as reliability centered maintenance analyses, logistics support analyses, maintenance job and task analyses, outage planning, and other specific analyses should be used to select the nature and extent of the information to be contained in the IMS, with emphasis on including only essential information. A periodic review of the IMS contents should be conducted to delete unused or obsolete information and ensure the validity of the data. The frequency of the reviews will depend on the criticality of the information, e.g. procedures and technical specifications must be updated as changes are approved, whereas human resources information may be updated at regular intervals.

3.5. IMS ACCESS

Access to IMS information, especially the ability to alter IMS information, should be controlled by physical and software security measures to ensure the integrity and validity of the information.

3.6. IMS AVAILABILITY

The IMS (at least relevant portions) should be available as early in the plant design process as possible to ensure that design basis and design detail information are adequately captured to support plant construction, startup, operations and maintenance. IMS reliability should be such as to support plant availability goals.

4. MAINTENANCE AND MAINTAINABILITY GUIDELINES

4.1. INTRODUCTION

Maintainability is defined as those attributes and features of a nuclear power plant design which collectively improve the cost effectiveness of maintenance (e.g. by reducing the frequency, duration, labour, dose and costs of maintenance). Maintainability is a design consideration and results from decisions during conceptual and detailed design phases of a project, in the areas of layout, system design, and equipment specification and selection. Maintenance requirements should be identified based on a systematic analysis of the large experience base from existing plants to identify both positive experiences as well as causes of significant events and unplanned outages and incorporate appropriate features in the plant design.

4.2. PREVENTIVE AND PREDICTIVE MAINTENANCE

Preventive maintenance establishes maintenance activities on equipment independent of its actual condition, but based on past experience. Predictive maintenance (which is part of preventive maintenance) aims at considering the specific equipment condition (e.g. ageing, or deterioration) to anticipate repair or replacement needs. Preventive maintenance programmes should be based on appropriate inspection and maintenance codes.

Examples of such inspection and maintenance codes are ASME Section XI and the French RSEM.

Operating experience shows that a regularly scheduled programme for maintenance and routine inspections is instrumental for early detection of problems, and in keeping plant availability high by minimizing unscheduled maintenance.

Predictive maintenance should be based on equipment condition monitoring. To establish the predictive maintenance programme, consultation between the designer, operator and maintenance personnel should begin early in the design process and should be completed prior to commissioning. References [5] and [6] provide additional information on the use of reliability centered maintenance to establish preventive and predictive maintenance programmes.

4.3. CORRECTIVE MAINTENANCE

Corrective maintenance is that maintenance/repair work done upon failure of plant components. A proposed maintenance programme should be identified early in the design process based on consultation between the designer, the utility. This programme should identify those components for which preventive maintenance will be provided, as well as those components for which only corrective maintenance will be provided.

4.4. TEST, INSPECTION AND PREVENTIVE MAINTENANCE AT POWER

The plant should be designed to permit the maximum amount of preventive maintenance to be performed while at power. This will:

- Reduce the workload, and potentially the duration, of outages
- Permit better maintenance planning and preparation
- Allow for the use of the highest skilled personnel because of scheduling flexibility
- Reduce conflicts and interference among maintenance activities
- Reduce peaks in maintenance staffing needs.

To facilitate such a design, consideration should be given to:

- Permanently installed radiation shielding at frequent maintenance locations
- Permanently installed features such as full-flow bypass lines for pumps, component redundancy and system isolation and draindown capability
- Provisions for system accessibility (e.g. doors, stairs, platforms) that are routed through low radiation areas.

4.5. EQUIPMENT PERFORMANCE MONITORING SYSTEM

Provisions for using an equipment performance monitoring system should be made to provide information to ensure that the plant is maintained within design values throughout its life. The system should use permanent and/or portable devices to record the history of stressors (e.g. temperature, radiation, pressure, and vibration) in and around all systems, structures and components (SSC) whose ageing degradation or failure can have a significant adverse effect on safety, reliability, availability or maintenance cost.

The environment in and around SSC has been found to play an important role in reliable service life. A comprehensive record of the history of stresors could therefore contribute to plant life extension. This system should be implemented as part of the IMS described in Section 1.4.

4.6. PROVISION FOR REPLACEMENT OR EXCHANGE OF MAJOR COMPONENTS

Experience over the past two decades with commercial nuclear power throughout the world has shown the need for designs that facilitate the replacement of major components. Experience has also shown that detailed planning is required during the design phase, to assure that the plant arrangement and features can accommodate removal and replacement of components.

The plant arrangement should provide features to facilitate the replacement of all major plant components (e.g. steam generators, condensers, turbines, heat exchangers), or critical parts of these components, consistent with the plant design life. Excluded from this provision are the reactor vessel and its supports, and basic plant structures.

The design should accomodate major component exchange within the planned outage lengths (e.g. generator rotor, condenser water boxes, reactor coolant pump motors).

4.7. INSPECTION AND TESTING

4.7.1. Inspection

The inspection techniques used during manufacturing,and those used for in-service inspection during operation should be capable of achieving compatible and repeatable results.

Equipment procurement specifications should either provide the detailed inspection procedures to be used in both manufacturing and at the site, or should require that they be provided by the equipment supplier (with concurrence by the utility).

The design of the plant should consider the provision for inspection and should include access requirements for equipment and associated personnel, the space to operate that equipment, and needed services (such as containment penetrations).

4.7.2. Periodic testing

The plant design should cost-effectively provide the provision for periodic operability/performance tests to be performed at power, without interfering with normal operation, It should be possible to test systems/subsystems or instrument loops in as close to normal operating conditions as practical. Tests should simply and directly measure system design basis parameters. Only the items that cannot reasonably be tested at power should be tested during outages (see also Section 1.3.2).

4.7.3. Startup testing

Startup testing should verify that systems provide design capabilities, that equipment interlocks are performance tested, and that temporary installations are removed at the appropriate time. Also, included in these tests should be a means of capturing startup data that can benchmark system performance for future reference and comparison.

The plant design should include features to carry out pre-operational and startup testing. Needs for startup testing should be integrated with operational testing needs.

4.8. ADVANCED TECHNOLOGY

Advanced technology should be encouraged where there is a need to solve known problems or an opportunity for simplification, and where the advanced technology is proven, including the following:

- Diagnostic monitoring techniques for leak detection, vibration, and other potential problems to minimize the failure of critical SSC.

5. MAINTAINABILITY STUDIES AND LOGISTICS SUPPORT ANALYSIS

5.1. INTRODUCTION

Maintainability of NPPs has often not been adequately considered in the early design of a plant, or superseded by other considerations during the detailed design process. Planning of maintenance has often been performed by utility personnel before startup but well after a number of design decisions affecting maintenance have already been made.

The availability of SSC depend on their reliability and maintainability but also on the availability of associated logistic means.

The objectives of maintainability studies are to predict the quantitative maintainability characteristics of equipment, to identify requirements for certain features or changes to design to improve maintainability and to guide design decisions. They also provide guidance for design support activities and maintainability checklists for design criteria and design reviews.

The following guidelines are based on methodologies such as RAM (reliability, availability and maintainability), RCM (reliability centered maintenance) and operating experience. It is recognized that maintainability studies are not mandatory to develop a maintenance program, and also that such studies should be selectively applied to plant SSC based on their expected cost-effectiveness.

5.2. RELIABILITY, AVAILABILITY AND MAINTAINABILITY STUDIES (RAM)

The purpose of these studies is to ensure optimum performance and reliability of plant equipment. The results of these studies (e.g. mean time between failures [MTBF], and mean time to repair [MTTR]) should be used to plan predictive, preventive and corrective maintenance programmes.

5.3. RELIABILITY CENTERED MAINTENANCE STUDIES (RCM)

A reliability centered maintenance programme is one where predictive, preventive and corrective maintenance requirements are determined based upon achievement of a system/plant reliability goals in the most cost-effective manner. Elements for establishing a maintenance programme should be provided by the designer to ensure optimum performance of the plant. These elements will allow maintenance programmes to be implemented based on RCM principles.

5.4. MAINTENANCE TASK ANALYSIS AND LOGISTICS SUPPORT ANALYSIS

In order to ensure adequate maintainability, designers should plan and initiate development or acquisition of maintenance logistics support in terms of spare parts, maintenance instructions, special equipment and tools, workshops, training of maintenance personnel.

In the Annex a logic diagram explains the different tasks of the maintainability and logistics support studies.

5.5. ASPECTS OF THE LOGISTICS SUPPORT ANALYSIS

5.5.1. Organization

The organization of plant personnel should be determined based upon the planned operation and maintenance activities. In this way the organization will be sized and structured to allow effective control and accomplishment of all operation and maintenance related activities.

5.5.2. Training

The technical data and requirements should be available to the operator for training and qualifying staff prior to plant startup.

5.5.3. Spare parts supply and storage

A list of recommended spare parts based on the logistics support analysis, the RCM analysis and the operating experience of current plants should be provided.

Experience from NPPs demonstrates the need for a spare part management system to facilitate identification and location of spares, as well as to maintain the desired inventory of spares. The system should be integrated with the IMS, if possible.

5.5.4. Maintenance facility, repair shop

Well equipped repair shops designed for maintenance of mechanical, electrical and instrument equipment should be accessible from all work areas during plant operation, taking into account that work on equipment contaminated with radioactive material should be strictly separated from clean work areas.

5.5.5. Documentation

A list of documents and a definition for each of these documents, including their hierarchy, should be established as early as possible.

An identification system should be applied to documents from all project participants for baseline documents, change control documents and support activity documents and record. The system should allow the retention of the equipment suppliers own identification system.

A documentation management system should be used during design, construction, startup, and operation, so that documentation can be maintained and updated.

The documentation management system should be capable of storing, controlling and accessing relevant records and other information for design, construction, test, startup, operation and maintenance from the design basis to the "as-built" configuration of the plant. Physical facilities should be provided to allow easy storage, retrieval, maintenance and management of documents.

The management of plant documents should be integrated, if possible in IMS.

5.5.6. Configuration management

Configuration management ensures that plant information (e.g. drawings specifications) correctly represents the approved design basis, and the physical plant itself (e.g. pumps, valves, wiring). During the life of the plant as changes are made this equality relationship must be preserved.

The IMS should help to facilitate configuration management.

5.6. LOGISTICS SUPPORT DATABASE

The logistics support database should support the IMS. In the Annex a logic diagram shows how this data is integrated in the logistics studies.

The fields of this database should be jointly defined as early as possible. A standard should be used to build this database, and to preserve the ability of information systems to communicate and exchange information.

5.7. LOGISTICS SUPPORT ANALYSIS REPORTS

The LSA computerized data system should be built to produce logistics support analysis reports to be used to aid in the execution of the maintenance programme.

6. RADIATION EXPOSURE

6.1. INTRODUCTION

Design features described in this section are aimed at:

- optimizing radiation protection (the magnitude of individual doses, the number of people exposed and the likelihood of incurring exposures should be kept as low as reasonably achievable),
- restricting individual radiation exposure not to exceed any relevant dose limits, and
- achieving targets for collective dose from occupational radiation exposure over the life of the plant.

6.1.1. Individual dose

Principles of radiation protection are developed by the International Commission on Radiological Protection (ICRP). Based on these principles International Basic Safety Standards for Protection against Ionizing Radiation and for the Safety of Radiation Sources (BSS), jointly sponsored by FAO, IAEA, ILO, OECD/NEA, PAHO and WHO, were issued in 1996. These Standards specify individual dose limits for occupational exposure.

6.1.2. Collective dose

The collective dose from occupational exposure should be as low as reasonably achievable. A target for annual collective dose should be set at the beginning of the design for use in designing equipment and installation.

6.2. BASIC GUIDELINES

Specific design features should be provided in the plant to reduce individual doses, and to meet the specified collective dose target.

Considerations include:

- Material selection, especially those subject to radiation, or in contact with the reactor coolant (e.g. selecting cobalt free hardfacing)
- Design and proper installation of water treatment to allow high quality chemistry standards
- Adequate permanent shielding for both gamma and neutron radiation, augmented with temporary shielding when necessary
- Design of components to facilitate cleaning and chemical decontamination to reduce exposure during maintenance
- Application of robotics for cleanup, maintenance and inspection tasks (see Section 5.4)
- design of equipment in modules for rapid disassembly, for standard exchange, inspection or maintenance
- Zero leakage fuel and zero leakage control rods (less than one manufacturing defect per 10 000 units)
- Plant layout to permit personnel movement through the plant without exposure to radiation sources
- Plant layout to assure radioactive components are adequately shielded from normal work areas and nearby components
- Avoiding the spread of contamination (e.g. ventilation systems, barriers and inter-zonal monitors)
- Systems for remote handling of contaminated resins and filters including packaging for waste disposal
- Instrumentation and devices to conduct testing and inspection remotely, particularly in high radiation areas
- Design features to prevent the introduction of inpurities and foreign material into the plant system.

6.3. ROBOTICS FOR INSPECTION AND REPAIR OPERATIONS

A robotics applications analysis should be performed during the design phase to identify candidate activities for use of robotics equipment to reduce radiation doses.

Possible applications for robotics include:

- Ssteam generator inspection and maintenance
- Radwaste drum handling
- Fuel bundle sipping and inspection
- Refueling
- Vessel flange bolting/unbolting by multi-stud tensioner
- Ultrasonic test (UT) inspections and repairs of vessel internals
- UT inspections of pipes, welds, vessel and nuclear components.

Specific design features important to the effective functioning of robotics devices should be considered in the design of the plant.

6.4. ELECTROPOLISHING

The use of electropolishing surfaces should be considered in those areas of the plant where this treatment will cost effectively reduce the radiation dose to personnel during maintenance.

6.5. OTHER CONTAMINATION REDUCTION TECHNIQUES

The facility design should include other available means for reducing contamination in areas of the plant which may come into contact with radioactive fluid or materials. Such features include:

- Non-porous coatings for metal and concrete surfaces
- Drip trays
- Leakoff collection.

7. DESIGN STANDARDIZATION AND SIMPLIFICATION

Standardization and simplification are design biases which when broadly implemented produce a design with better operability and maintainability and reduced life cycle costs. The benefits of standardization and simplification are:

- Standard systems, structures and components (SSC) reduce operational complexity and training, spare parts inventory, maintenance force
- Simple designs are easier to operate
- Standard SSC require a reduced maintenance knowledge base
- Reduced regulatory uncertainty.

The following are key attributes of a design which is biased toward standardization and simplification:

- Where possible, a standard nuclear power plant design is implemented in a series of plants.
- Standard SSC are selected across plants and a plant across functions.
- SSC design is simplified, consistent with safety requirements, to minimize the number of components, needed to achieve plant functions.
- Nomenclature, labeling and coding is standardized through the plant to ensure a consistent set from conceptual design, through procurement, construction and operation. Vendors, operators, maintainers and designers should be able to readily identify any SSC by one unique label.
- Component selection and design is biased toward modularity and simplicity such that component repair is simplified and replaceability is enhanced.

8. IMPLEMENTATION OF OPERABILITY AND MAINTAINABILITY GUIDELINES

This section describes a process for using the operability and maintainability guidelines in this document in the design of new nuclear power plants or in the design of upgrades and retrofits in existing nuclear power plants. The process described integrates design, cost benefit, dose and availability considerations.

8.1. MAJOR FACTORS FOR CONSIDERATION

Experience in the nuclear industry has shown that major contributors to unavailability are, in order of importance:

- Planned outage length
- Forced outage unavailability
- Time to return to power following an outage
- Fuel cycle length and its impact on outage frequency.

When implementing these guidelines, particular attention should be paid to properly identify SSC parameters which relate to the major contributing factors to plant unavailability. These include SSC attributes such as mean time between failures and mean time to repair.

In addition, cost and dose factors must be considered. For example, for cost one considerations should include component cost, maintenance cost, cost of logistical support, and unavailability cost. For dose, one should consider maintenance methods and design methods for reducing radiation exposure attributable to the SCC.

Allocations for these considerations can be made on the basis of experience with identical or similar designs, or from analysis and expert opinion. For example, to meet an annual collective dose target, analysis and expert opinion can be used to identify those SSC (e.g. steam generators, reactor vessel and internals), which contribute to radiation exposure. Proportional partitioning of the new dose target based on analysis of operating experience or expert opinion can be used to allocate maintenance dose to the new SSC design. These allocations are then iterated through the functional analysis and design to verify their feasibility and to arrive at the SSC detailed design.

8.2. IMPLEMENTATION PROCESS

The process described below includes:

- Functional analysis of availability, maintenance costs, dose, etc., and
- Design activities.

These activities are actually iterative, such that if the outcome of a particular assessment is not acceptable from a cost, dose or availability point of view, the inputs to the assessment are reviewed to determine if allocation targets or the design should be changed.

These activities and their relationship are shown in Fig. 1.

The functional analysis takes as inputs the targets for dose, maintenance cost, outage contribution, and availability for the nuclear power plant SSC as well as experience feedback from operating plants. The targets are allocated from experience feedback and from functional analysis. From these inputs, the critical SSC are identified.

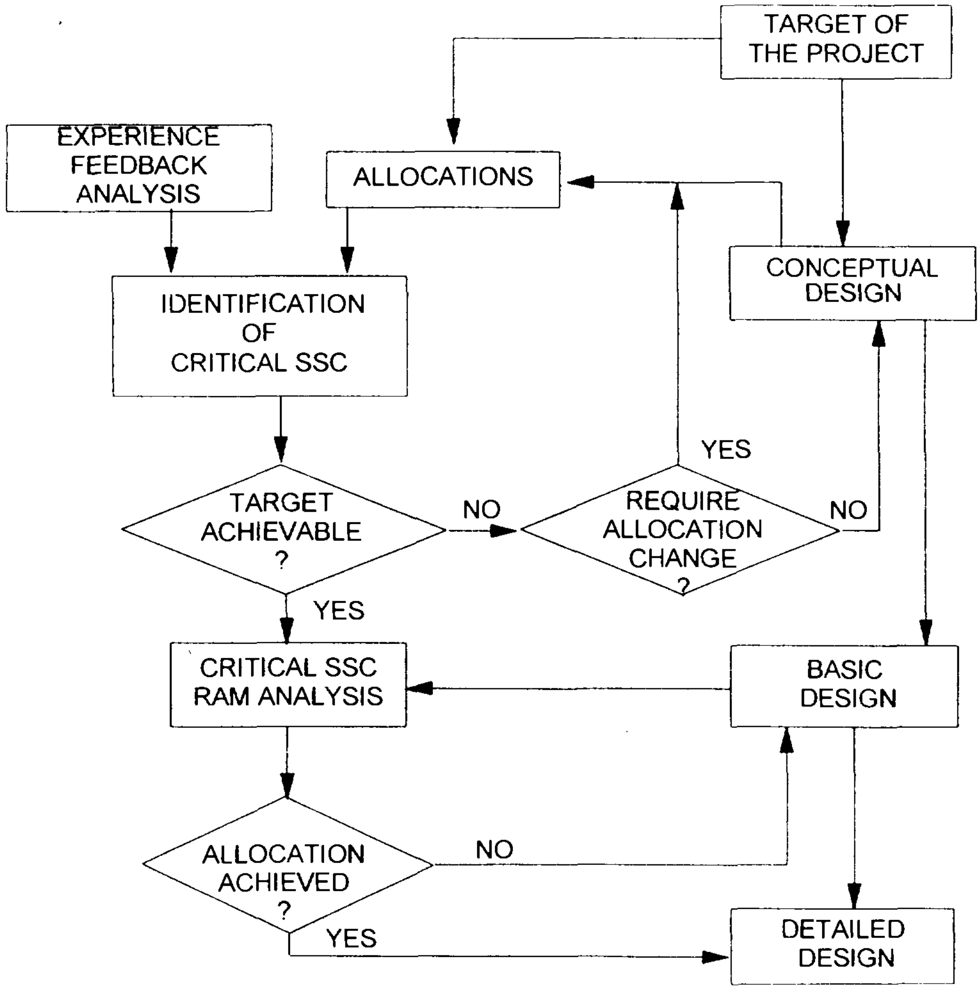


FIG. 1. Simplified implementation process.

Continuing with the functional analysis, for each critical SSC, preliminary allocations are made for availability, outage contribution, maintenance cost, and dose. Using these allocations, preliminary design constraint input (e.g. mean time between failure, target maintenance dose, etc.) are given to the designer for incorporation. If the design cannot meet those constraints or is too costly, then an iteration to review the allocations and/or the conceptual design is made.

The allocations are passed to the SSC RAM assessment to determine if the allocations for reliability, availability and maintainability are met. If the allocations are met, they are passed to detailed design for implementation. If not, they are returned to basic design for re-evaluation. The aforementioned implementation process can also be applied to the existing plants for upgrades or improvements.

8.3. DESIGN PROCESS

The design process described in this section is not new. What is new (to the nuclear industry) is the introduction of iteration with allocations of specific attributes (e.g. availability, dose, maintenance cost, etc.) in the SSC design process. It is this feature of the process what contributes to achieving cost, dose and availability goals.

REFERENCES

[1] ELECTRIC POWER RESEARCH INSTITUTE, Advanced Light Water Reactor Utility Requirements Document, Volume 1, ALWR Policy and Summary Top-Tier Requirements, Palo Alto, CA (1990).

[2] EUROPEAN UTILITY REQUIREMENTS, European Utility Requirements for LWR Nuclear Power Plants, Volumes 1 and 2 – Revision A (1994).

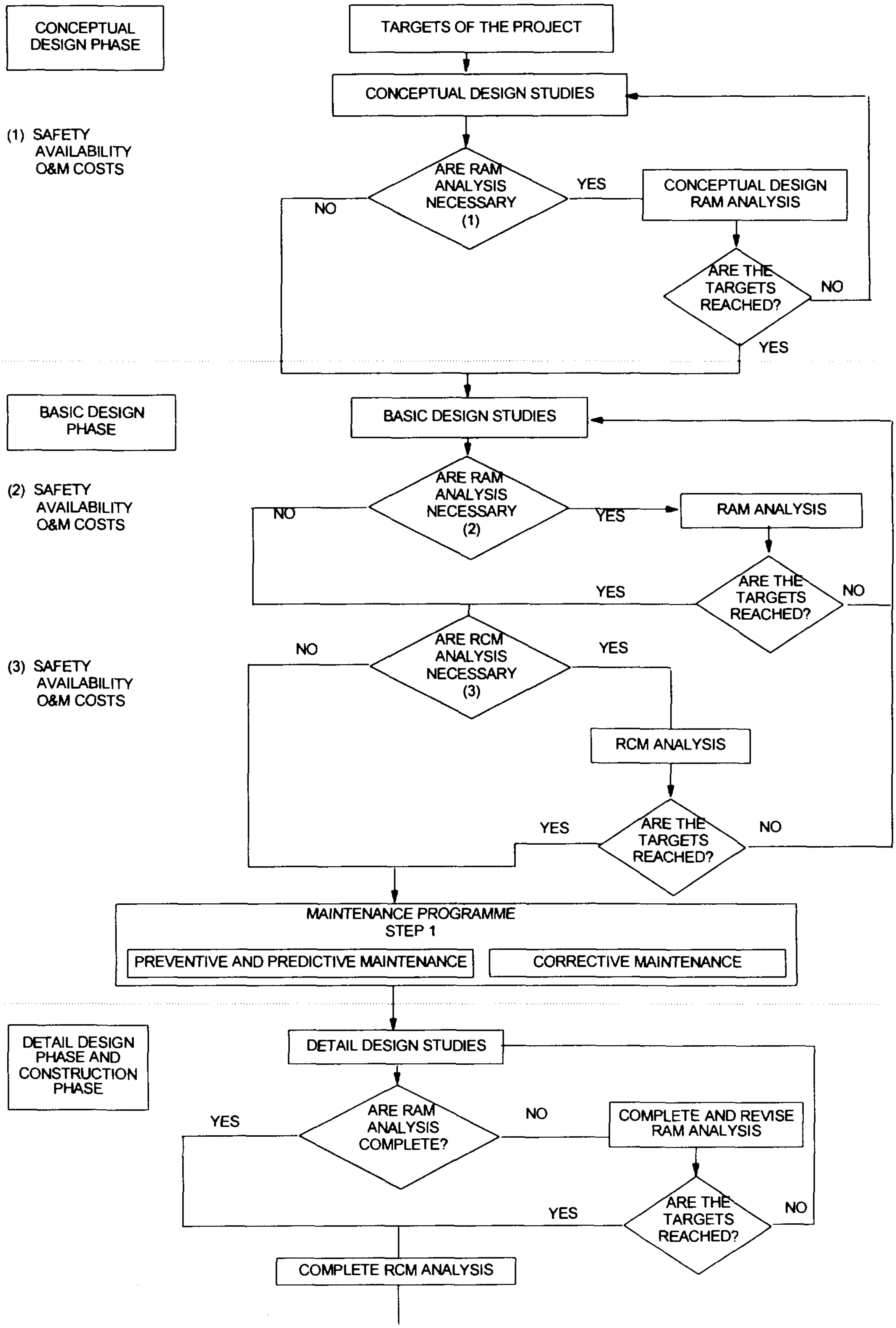
[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Computerization of Operation and Maintenance for Nuclear Power Plants, IAEA-TECDOC-808, Vienna (1995).

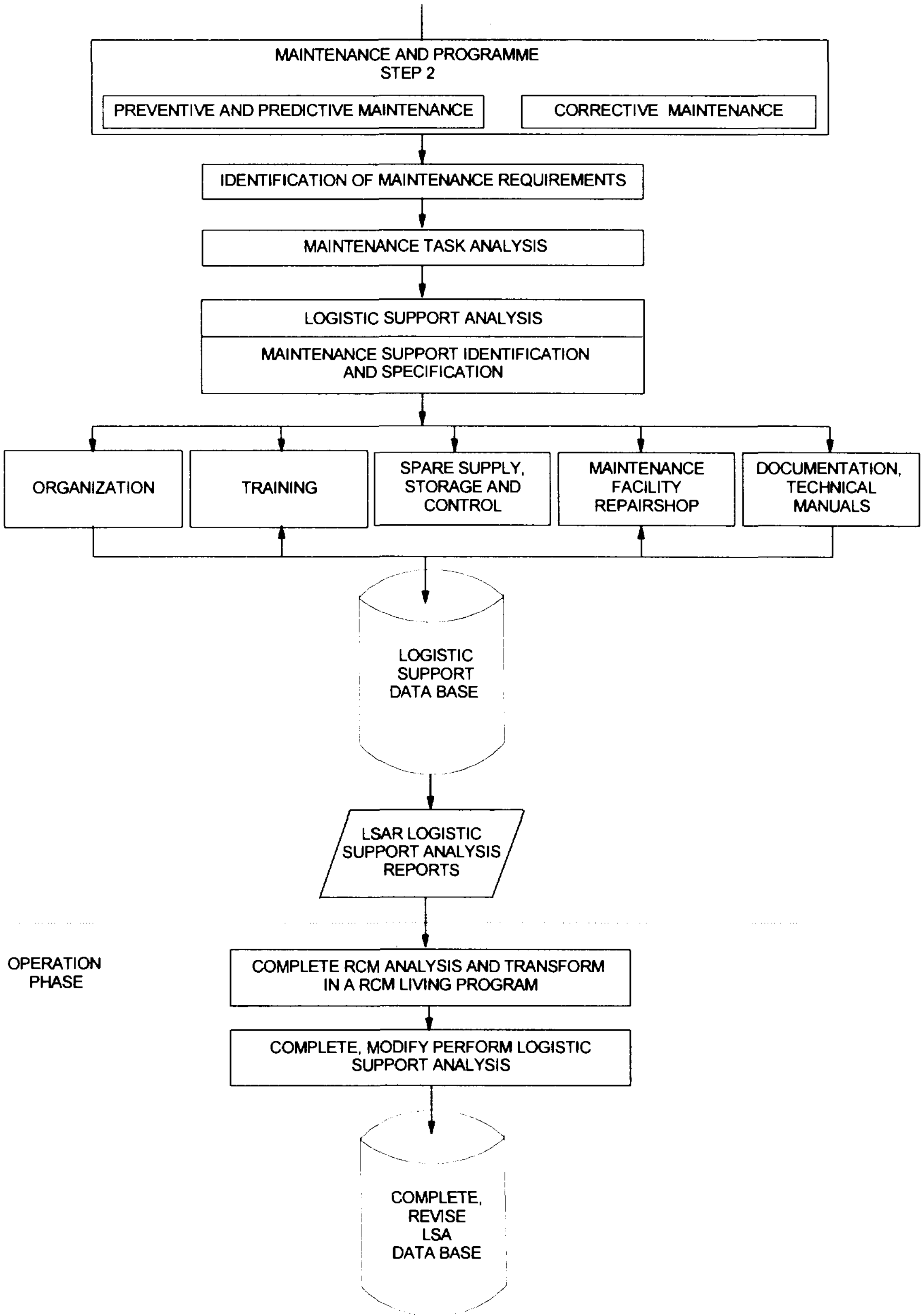
[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Control Room/Systems Design for Nuclear Power Plants, IAEA-TECDOC-812, Vienna (1995).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Related Maintenance in the Framework of the Reliability Centered Maintenance Concept, IAEA-TECDOC-658, Vienna (1992).

[6] DEGRAVE, C., MARTIN-ONRAET, M., Integrating Availability and Maintenance Objectives in Plant Design and Approach, The 3rd JSRE/ASRE Joint International Conference on Nuclear Engineering, Kyoto (1995).

Annex
INTEGRATION OF MAINTENANCE AND LOGISTICS SUPPORT DURING THE DESIGN OF AN NPP




MAINTENANCE AND PROGRAMME
STEP 2
PREVENTIVE AND PREDICTIVE MAINTENANCE
CORRECTIVE MAINTENANCE
IDENTIFICATION OF MAINTENANCE REQUIREMENTS
MAINTENANCE TASK ANALYSIS
LOGISTIC SUPPORT ANALYSIS
MAINTENANCE SUPPORT IDENTIFICATION AND SPECIFICATION
ORGANIZATION
TRAINING
SPARE SUPPLY, STORAGE AND CONTROL
MAINTENANCE FACILITY REPAIRSHOP
DOCUMENTATION, TECHNICAL MANUALS
LOGISTIC SUPPORT DATA BASE
LSAR LOGISTIC SUPPORT ANALYSIS REPORTS
OPERATION PHASE
COMPLETE RCM ANALYSIS AND TRANSFORM IN A RCM LIVING PROGRAM
COMPLETE, MODIFY PERFORM LOGISTIC SUPPORT ANALYSIS
COMPLETE, REVISE LSA DATA BASE

ABBREVIATIONS

ALARA	as low as reasonably achievable
BWR	boiling water reactor
HVAC	heating, ventilating, and air conditioning
HWR	heavy water reactor
IMS	information management system
LOCA	loss of coolant accident
LSA	logistics support analyses
LWR	light water reactor
M–MIS	man–machine interface system
MTBF	mean time between failures
MTTR	mean time to repair
O&M	operations and maintenance
QA	quality assurance
PWR	pressurized water reactor
RAM	reliability, availability and maintainability
RCS	reactor coolant system
RCM	reliability centered maintenance
RPV	reactor pressure vessel
SSC	system, structure and component

CONTRIBUTORS TO DRAFTING AND REVIEW

Churchill, B. (II)	Bruce B., Canada
Chang Zhang, Y. (II)	Guangdong Nuclear Power Plant, Republic of China
Kandel, J. (II)	DEPT/EPN Mission REP 2000, France
Martin-Onraet, M. (I, II)	EDF, France
Porchet, A. (II)	Framatome, France
Sturm, J. (II)	Neckar GmbH, Germany
Seo, Jong-Tae (II)	Korea Atomic Energy Research Institute, Republic of Korea
Korshunov, A.S. (II)	Atomenergoproekt, Russian Federation
Pearce, R. (I, II)	ABB/CENO, USA
Mazour, T. *Scientific Secretary* (I, II)	International Atomic Energy Agency
Cleveland, J. (II)	International Atomic Energy Agency
Rinejski, A. (II)	International Atomic Energy Agency

Consultants Meeting (I)
Vienna, Austria, 16–20 October 1995

Advisory Group Meeting (II)
Vienna, Austria, 20–24 November 1995

96-03163