IAEA Services Series No. 5

DSRS guidelines

Reference document for the
IAEA Design Safety Review Services

INTERNATIONAL ATOMIC ENERGY AGENCY

March 1999

IAEA SAFETY RELATED PUBLICATIONS

IAEA SAFETY STANDARDS

Under the terms of Article III of its Statute, the IAEA is authorized to establish standards of safety for protection against ionizing radiation and to provide for the application of these standards to peaceful nuclear activities.

The regulatory related publications by means of which the IAEA establishes safety standards and measures are issued in the **IAEA Safety Standards Series**. This series covers nuclear safety, radiation safety, transport safety and waste safety, and also general safety (that is, of relevance in two or more of the four areas), and the categories within it are **Safety Fundamentals**, **Safety Requirements** and **Safety Guides.**

- **Safety Fundamentals** (silver lettering) present basic objectives, concepts and principles of safety and protection in the development and application of atomic energy for peaceful purposes.

- **Safety Requirements** (red lettering) establish the requirements that must be met to ensure safety. These requirements, which are expressed as 'shall' statements, are governed by the objectives and principles presented in the Safety Fundamentals.

- **Safety Guides** (green lettering) recommend actions, conditions or procedures for meeting safety requirements. Recommendations in Safety Guides are expressed as 'should' statements, with the implication that it is necessary to take the measures recommended or equivalent alternative measures to comply with the requirements.

The IAEA's safety standards are not legally binding on Member States but may be adopted by them, at their own discretion, for use in national regulations in respect of their own activities. The standards are binding on the IAEA for application in relation to its own operations and to operations assisted by the IAEA.

OTHER SAFETY RELATED PUBLICATIONS

Under the terms of Articles III and VIII.C of its Statute, the IAEA makes available and fosters the exchange of information relating to peaceful nuclear activities and serves as an intermediary among its members for this purpose.

Reports on safety and protection in nuclear activities are issued in other series, in particular the **IAEA Safety Reports Series**, as informational publications. Safety Reports may describe good practices and give practical examples and detailed methods that can be used to meet safety requirements. They do not establish requirements or make recommendations.

Other IAEA series that include safety related sales publications are the **Technical Reports Series,** the **Radiological Assessment Reports Series** and the **INSAG Series**. The IAEA also issues reports on radiological accidents and other special sales publications. Unpriced safety related publications are issued in the **TECDOC Series**, the **Provisional Safety Standards Series**, the **Training Course Series,** the **IAEA Services Series** and the **Computer Manual Series**, and as **Practical Radiation Safety and Protection Manuals**.

IAEA Services Series No. 5

DSRS guidelines

Reference document for the
IAEA Design Safety Review Services

INTERNATIONAL ATOMIC ENERGY AGENCY

March 1999

The originating Section of this publication in the IAEA was:

Engineering Safety Section
International Atomic Energy Agency
Wagramer Strasse 5
P.O. Box 100
A-1400 Vienna, Austria

DSRS GUIDELINES
REFERENCE DOCUMENT FOR THE
IAEA DESIGN SAFETY REVIEW SERVICES
IAEA, VIENNA, 1999
IAEA-SVS-05

Printed by the IAEA in Austria
March 1999

FOREWORD

The Engineering Safety Section of the Safety of Nuclear Installations Division of the IAEA performs safety services in the design area for new and operating nuclear facilities. Some of these services are in specific areas such as seismic safety and fire safety of nuclear power plants. In particular, seismic safety review services (also covering other external events) have been performed systematically for the past ten years. Other services have also been carried out but more infrequently and on an ad hoc basis. Services will be starting in two other areas which have gaining more importance in recent years; these are ageing and software important to safety.

The present publication covers the more general topic of a design safety review of a nuclear power plant. With the publication of this report it is intended to make Member States aware of the possibility of a service through which they can have a better appreciation of the overall design of a facility or one which is already in operation. It includes a generic and procedural part followed by a technical part corresponding to different systems of a nuclear power plant. In the latter, the topics which have already been covered by other more specific services (such as seismic, fire, ageing and software important to safety) have been intentionally left out.

This publication is intended to be used mainly in the preparation and execution of a design review service by the IAEA and to provide information to potential recipients of the service regarding the effort involved and the topics that can be covered. It is also expected to be useful if Member States decide to conduct such reviews themselves either through regulatory authorities or as part self assessment activities by plant management. The IAEA officer responsible for this publication was A. Guerpinar of the Division of Nuclear Installation Safety.

EDITORIAL NOTE

In preparing this publication for press, staff of the IAEA have made up the pages from the original manuscript(s). The views expressed do not necessarily reflect those of the IAEA, the governments of the nominating Member States or the nominating organizations.

Throughout the text names of Member States are retained as they were when the text was compiled.

The use 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 names of specific companies or products (whether or not indicated as registered) does not imply any intention to infringe proprietary rights, nor should it be construed as an endorsement or recommendation on the part of the IAEA.

CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

The IAEA provides Design Safety Review Services (DSRS) as an element of its regular, extrabudgetary and technical assistance programmes to assess the safety of nuclear facilities. Reviews are conducted in response to requests from Member States, with whom the scope, objectives and technical disciplines to be covered by the review are agreed and as a part of an overall project existing in the interested country for assessing the safety of the nuclear facility.

DSRS are provided to Member States during any of the major stages of the licensing process, i.e. during facility design, construction and commissioning phases as well as during operation phase. Regardless of the phase of facility development or operation, the main purpose of a DSRS mission is to provide assistance to Member States with respect to implementation of IAEA requirements and Safety Guides and standards of international practice to ensure consistent and uniform assessments of safety.

1.2. PURPOSE, SCOPE AND STRUCTURE OF THIS PUBLICATION

The primary purpose of this publication is to provide guidance for planning and conducting a DSRS mission The guidance is primarily intended for use when the IAEA is invited by a Member State to perform this service. However it is expected to be useful to Member States themselves for planning and performing design reviews by their national authorities, as well as for internal reviews by utilities that operate nuclear power plants (NPPs) or by NPP management. The guidance is intended to provide assurance that a DSRS will be adequately planned and successfully implemented. The contents of the publication should not limit a DSRS design review at any particular site, however, as site or facility specific safety issues may require special procedures or consideration.

The scope of this publication covers plant design safety reviews of issues other than those involved with earthquakes and corresponding structural issues, with fires, with software important to safety and with ageing. These four specific fields are covered by specific IAEA Services Series, since they are the object of frequent requests of assistance to IAEA.

This publication presents a general procedural framework for reviews and a sample of technical recommendations on requirements and issues to be checked for safety related systems. Issues proposed for a check are discussed in Appendix I and a typical list of safety related systems is included as Appendix II. The safety related systems of Appendix II have been grouped as shown in Appendix I, following the structure of Ref. [1], in order to favour a more integrated review of plant design.

A design review is a multi-disciplinary review of the design of a nuclear power plant, based on the available documentation and discussions with the organizations involved with the design, construction and operation of the plant. It is carried out by a group of international experts under IAEA co-ordination. Its objective is to provide to the requesting Member State an independent review and assessment of the plant design and to make recommendations on additional analysis or plant modifications to be carried out in order to enhance nuclear safety.

The scope of the review can be tailored for each specific case in order to address specific areas of review which are considered as presenting potential safety issues. It is recognized that the review is intrinsically based on IAEA Requirements and Safety Guides as well as the experience of the participating experts.

1.3. OBJECTIVES OF DSRS MISSIONS

The objectives of DSRS missions are as follows:

(a) To assist Member States, as specified in the preparatory agreements between them and IAEA, with their application of IAEA safety requirements and recommendations in accordance with NUSS safety requirements and guides, of suitable standards of international practice and of pertinent national regulatory requirements, in order to ensure a systematic, consistent and uniform assessment of safety;

(b) To provide thorough and adequate reviews and evaluations of identified design safety issues.

1.4. SCOPE OF DSRS MISSIONS

DSRS missions can be viewed in two broad categories for the purpose of defining their scope and implementation.

(a) During design and construction phases

A DSRS mission performed during the design and construction phase typically, focuses on general adherence to governing safety guides and criteria; implementation of the design criteria, analysis methodologies, construction practices, quality assurance and control procedures. etc.

(b) During the operational phase

A DSRS mission performed after design and construction of the facility may be requested because:

- questions have been raised by the country's regulator, the design organization or other outside consultants about the current design of the nuclear power plant,
- a significant number of independent design changes have been made to the nuclear power plant over time,
- lessons learned from the operating experience at other facilities indicate that a design review of selected structures, systems or components would be beneficial,
- of the change in the perception of an internal or external hazard,
- regulatory changes have been instituted which require a re-evaluation of the site, facility design or procedures.

TABLE I. SCOPE OF DSRS MISSIONS

Site selection and characterization	**Design and construction**	**Post-construction**
Review work plans and technical procedures for site selection or site investigations.	Evaluate implementation of site monitoring or investigations recommended by previous missions.	Review the re-evaluation of design basis values or beyond design basis values for a specific external or internal event.
Review site selection and site investigations to determine design bases values for all external events.	Review implementation of design requirements and design guides.	Review the safety assessment of the plant in light of updated safety requirements.
Review the design capabilities of the perspective NPP design organization.	Evaluate and discuss identified safety issues.	Review work plans and technical procedures for plant safety assessments.
Review organizational structure to manage the project and QA plan.	Review organizational structure, QA plan and its implementation during the design and construction phase..	Review evaluations of capacity of structures, systems and components of existing plants.
		Follow-up previous mission reviews and implementation of recommended safety enhancement actions.

1.5. PRINCIPAL PARTICIPANTS IN DSRS MISSIONS

The participants in DSRS missions are determined by the scope of the mission. Principal participants are the IAEA review team and counterpart host government, utility nuclear facility team leader and discipline professionals as summarized in Table II. The IAEA team leader is an IAEA staff member. The counterpart team leader may be from the host government regulatory authority or the host utility. The number of team discipline professionals and the areas of discipline expertise will be dictated by the mission scope. Typically overlapping expertise will be sought for the IAEA review team in order to provide redundancy in the review of the subject matter. Technical participants on the host side also will be dictated by the scope of technical issues to be reviewed during the mission. Technical participants on the host side should have participated in the plant design evaluations and should have overlapping expertise to assure complete, in-depth coverage of the scope of safety issues to be reviewed during the mission.

TABLE II. PRINCIPAL PARTICIPANTS IN DSRS

IAEA review team	**In-country counterpart**
Team leader (IAEA staff member)	Regulatory authority, utility, NPP management contact as appropriate for the mission scope.
Discipline professionals as required by scope of mission (most appropriate professional expertise worldwide).	Plant design personnel as required by the scope of mission. Technical professionals involved in nuclear facility design, construction, commissioning, or re-evaluation activities are drawn from many organizations, including: - national institutes - universities - consulting professionals - utility personnel - engineering design organization.

1.6. ELEMENTS OF DSRS MISSIONS

A DSRS mission has three primary elements: preparation for the mission, conduct of the mission, and reporting. Regardless of the scope of the mission or the specific safety issues being reviewed, realization of a successful mission requires equal care in the execution of each of the elements mentioned above as described in Sections 2, 3 and 5 of this publication.

1.7. CONDUCT OF DSRS MISSIONS

While details of the conduct of DSRS will vary depending on the mission scope, they should include the following steps:

(a) review of written material;

(b) technical exchanges with counterpart discipline professionals;

(c) direct on-site observations/evaluations;

(d) discussions of evaluations and preliminary conclusions and recommendations with counterpart personnel;

(e) preparation of the draft mission report.

Technical discipline members of the IAEA review team are expected to thoroughly cover their respective discipline materials in enough detail and depth to reach independent conclusions about the adequacy of design parameters, design procedures or safety criteria used. Typically this will require review of written material supplied by the host utility, technical exchanges with discipline counterparts and direct observation of site data, including a site visit, or direct observation of the facility design work or as-built conditions. A substantial part of the review time will be spent reviewing procedures and practices used, including drawings and work plans and implementation. Consequently, the review team

should be familiar with the IAEA NUSS requirements and guides and users manuals relevant to the scope of the mission (see Section 4). If necessary to gain sufficient facts to reach an independent safety evaluation, more than one iteration through one or more elements of a document review, technical exchange or direct data evaluation should be made.

The final product of a DSRS mission is the mission report, which is specifically discussed in Section 5 of this publication. A draft report will be prepared during the mission and will be presented to the in-country counterpart at the closing meeting before the review team leaves the country. The chapters on Technical Session Findings and Conclusions and Recommendations are the highest priority portions of this draft report. The findings should address weaknesses identified by the review in enough detail to document the specific concern with sufficient facts to make the concern fully understandable. Similarly, good practices should be documented for the benefit of future reviews. Conclusions should be clearly stated. Recommendations should be unambiguously formulated, clearly stated and based on the identified weaknesses. Each specific recommendation should identify actions needed to remedy identified weaknesses.

After the performance of the mission the draft report will be reviewed and finalized. After completion and final editorial clearance the mission report is subjected to the IAEA internal approval clearance procedure.

2. PREPARATION FOR DSRS MISSIONS

2.1. SCOPE OF THE MISSION

The scope of the mission is defined by the IAEA team leader and in-country counterpart. The scope of the review mission dictates all elements of the mission execution: he technical discipline composition of the review team, the reference material to be provided prior to the mission and during the mission, the technical discipline composition of the in-country counterpart specialists, the extent of the site visit and facility walk downs, and so on. The scope should be clearly stated and unambiguous and should be clearly reflected in the mission agenda.

2.2. PARTICIPANTS OF THE REVIEW MISSION

The participants in the review mission are the IAEA review team and its in-country counterparts.

The IAEA review team is composed of a team leader, who is always an IAEA staff member, and the discipline professionals. The IAEA review team is a multi-disciplinary team of individuals with expertise in the required engineering and scientific disciplines, as defined by the mission scope and required for the review. The following should be taken into account:

(a) Team members should be independent of the in-country organizations. In addition to the extent possible, team members should not be from countries or organizations contractually involved in the project in order to avoid potential conflicts of interest.

(b) Team members should overlap in expertise, to the extent possible, to provide redundancy, a broad range of views and experience, and concurrence of opinions on review issues. Diversity of experience of the team members is advantageous to the review.

(c) The IAEA review team should remain intact, until the subject review is completed, to provide continuity and efficiency for subsequent missions to the same site/facility.

In-country counterparts include the nuclear regulatory authority; management, engineering, and operations representation from the utility or owner/operator of the plant; government institutions that provided support for the design or for the mission evaluation; and consultants and contractors that performed or participated in the work or subject to be reviewed. The in-country counterparts could also include consultants and contractors from outside the host country engaged by the regulator, the utility, plant owner/operator, or other in-country participants.

2.3. IAEA TEAM LEADER RESPONSIBILITIES

The IAEA team leader will establish all required technical and logistical liaison contacts with the in-country counterpart as officially indicated in the formal request from the Member State. These contacts may be with the regulatory authority, with the utility, or with the nuclear facility management as appropriate for the scope of the review mission. the team leader and the in-country counterpart will establish the mission scope and objectives. This may be accomplished through written/oral communication or a meeting.

Once the scope is defined, the team leader will recruit the needed discipline professionals and establish the schedule of events and meeting agenda. The team leader will provide the in-country counterpart with the proposed schedule of events leading up to the review mission.

Transmission of detailed reference material for IAEA team review before arriving on-site is an essential part of this schedule. A safety analysis report or equivalent documentation should be included. Detailed reference material to be reviewed should be received at the IAEA at least one month in advance of the mission.

The team leader will provide the in-country counterpart with the logistical requirements for the site visit and facility walk-down, if appropriate. The team leader will review the reference material submitted by the in-country counterparts for completeness and adequacy and distribute the material to the review team members prior to the mission.

2.4. IN-COUNTRY COUNTERPART RESPONSIBILITIES

The in-country counterpart will carry out the logistics for the mission including transmittal of the reference material, establishing the arrangements for the mission (hotel, meeting rooms, access to the site and facility, participation of engineering and scientific discipline personnel to support the on-site review, transportation, secretarial services, and so on), and contacts with the plant owner/operator. The in-country counterpart will provide the requested reference material according to the previously agreed upon schedule, i.e. at least one month in advance of the meeting.

2.5. IAEA REVIEW TEAM RESPONSIBILITIES

IAEA review team members will familiarize themselves with the reference material in advance of the mission. In addition, team members are expected to perform a background review of appropriate published material for their individual responsibilities on the mission.

Each team member is responsible for the preparation, writing and reviewing of the specific section of the mission report dealing with the subject under his responsibility. He will also be asked to review the report on other closely related subjects to ensure consistency and good integration between all disciplines reviewed. The completion and review of the draft report after the mission is also a task to be performed by the team members.

2.6. GUIDELINES AND CRITERIA FOR THE REVIEW

The guidelines and criteria for performing the review are mainly those established in the IAEA NUSS publications, in terms of reference (TOR) prepared specifically for the project, in guides or practice of the member state (country), in well documented international practice and other relevant information. The Requirements and Safety Guides of the IAEA Nuclear Safety Standards (NUSS) programme are the main basis for the review. Additional codes and standards, specific to a nuclear power plant type, may be used in the studies. Some modifications of these reference codes and standards may be required for the specific condition in the country of consideration. Within the scope of a mission, the IAEA NUSS Safety Requirements, Standards and Safety Practices are applicable.

3. CONDUCT OF THE MISSION

3.1. ELEMENTS OF THE MISSION

Section 1.6 presented the elements of the mission, the conduct of which can be further elaborated as follows:

- Review of reference material submitted in advance;
- Review of written material on-site;
- Technical exchanges with counterpart personnel;
- Direct on-site and in-facility observations and evaluations;
- Discussion of evaluations, preliminary conclusions, and recommendations;
- Draft report submitted to the in-country counterparts.

The mission duration is typically two weeks which is divided, e.g. into a day and a half day of orientation and general introductions; eight days of technical exchanges between the IAEA team and the in-country counterparts and on-site and in-facility evaluations; one day of report writing; and one-half day of concluding meetings.

Each aspect of the conduct of the mission requires documentation. A detailed list of all written material reviewed should be maintained, especially those items which form the bases

of judgements made and conclusions drawn. Reports, drawings, maps, photographs, published papers, and so on should be identified by their unique identifiers for reference. Dates of documents and accurate revision numbers should be noted since, typically, they may be in an on-going state of revision. In addition to identification of the reviewed items, a summary of the level of detail of the review of each item should be documented. Documentation of written material can easily take the form of a matrix or spread-sheet with notations for review detail.

Documentation of meetings and technical exchanges should be maintained for inclusion of salient items in the draft report. This documentation should identify all in-country discipline professionals with whom discussions were held, specifically identifying their respective contributions.

The draft report should follow the outline presented in Section 5. It is essential that the significant observations, conclusions, and recommendations of the mission are documented in the draft report prior to completion of the in-country part of the mission so that the in-country counterparts can review their substance and provide clarifying or dissenting views. It is important to provide clear recommendations concerning future actions necessary to resolve deficiencies.

3.2. FACILITY WALKDOWN: DESIGN REVIEWS

During the mission, a facility walk down or in-plant review should be performed. The purposes of the walk down are the following:

- review in-plant features presented in the reference material and discussed in the opening days of the mission;
- assess typical structures, equipment, components, and distribution systems and their installations for known vulnerabilities as determined from other assessments (see Appendix I);
- assess the as-is condition of structures, systems, and components, for known vulnerabilities;
- assess the as-is conditions of structures, systems and components to verify the accuracy of drawings and procedures.

A preliminary reconnaissance walk down is generally followed by more specific walk downs to determine the general design and layout of structures, systems and components for each system identified in Appendix I. These walk downs are not intended to replicate the extensive walk downs to be performed later but are intended to provide an overview of the facility consistent with the mission’s scope and objectives.

Documentation of the mission walk down is to be performed by field notes, photographs, annotated drawings for as-built conditions, etc. A summary of these items is contained in the final report; text or appendices.

The facility walk down is a task for which an overlap in the review team’s technical expertise is desirable. Issues arise during the walk down which require the judgement of the

team and independent views are helpful. In fact, during these walk downs, teams of two or more qualified engineers are desirable to provide redundancy in the evaluation process.

Required in-country counterpart support for the walk down includes general logistics (scheduling of plant support including systems and operating expertise, access to equipment, access to generally restricted areas, etc.) and the ability to respond to specific questions during the mission by scheduling the availability of plant engineering and operational support personnel.

Adequate preparation for the facility walk down is essential for its success. The IAEA team leader and the in-country counterpart should co-ordinate the activity prior to the mission kick-off meeting and confirm during the first days of the mission the arrangements to assure its success.

3.3. DETAILED SCOPE OF THE DESIGN REVIEW

The design review will be conducted in two general areas: general design review and plant systems design review. The general design review will evaluate: safety classifications, general design basis, safety analysis, design verification, system and component reliability, provisions for in-service test, maintenance and inspection, equipment qualification, ageing, human factors and other design considerations. The plant systems design review will focus on the following five areas: reactor core, reactor coolant system and reactor coolant auxiliary systems, containment systems, instrumentation-control and protection systems, emergency power systems, and fuel handling and storage. See Appendix I for the detailed review guidelines.

4. REVIEW OF ORGANIZATIONAL AND QUALITY ASSURANCE ASPECTS

4.1. GENERALITIES

A quality assurance programme is considered to be an essential aspect of management of all phases of development and operation of a nuclear facility. IAEA Member States should have in place the necessary framework for the safety regulation of nuclear facilities. To assist Member State organizations responsible for nuclear facility projects in establishing and implementing their quality assurance programme, the IAEA has developed a Code of Practice [2] and fourteen Safety Guides.

DSRS team members should be familiar with these documents. During an DSRS mission team members will review relevant aspects of the quality assurance programme and its implementation. The following elements of the programme may be evaluated as they apply to the disciplines being reviewed within the scope of the review mission.

- quality assurance plan;
- procedures and work plans;
- document and records management;

– technical documentation approval procedures;

– independent verification methods and procedures.

4.2. QUALITY ASSURANCE PROGRAMME

The organization having overall responsibility for a nuclear facility is responsible for establishing and implementing an overall QA programme. Typically, the DSRS team leader interacting with the in-country counterpart will determine whether an acceptable QA programme has been established for the nuclear facility to be reviewed. The QA programme should be consistent with the requirements of IAEA Code 50-C-QA and should be documented in a programme description. Procedures and work plans are integral parts for an acceptable QA plan.

The DSRS team will review the facilities QA procedures covering those activities within the scope of the review mission to ensure that they are consistent with the IAEA's guidelines and are described in a clear and logical sequence.

Work plans implement QA procedures in the planning and conduct of specific activities or tasks. Typically, plans constitute detailed descriptions of technical tasks and include work flow charts, schedules and other descriptive material linking the task to other related work activities and tasks. The DSRS team will review relevant QA work plans to ensure they properly reflect the ongoing design or design modification work..

The QA Plan for a nuclear facility project establishes procedures for approval of technical documentation of completed work. For each study element or task the procedures require the responsible manager to designate, as part of the work study plan, qualified individuals to review the reported results of the work. The reviewed reports together with resolution of review comments are then submitted to the responsible manager for final evaluation and approval. The DSRS review team will determine whether technical publication approval procedures consistent with IAEA's guidelines have been implemented for the studies reviewed by the mission.

4.3. SAFETY CULTURE

Safety culture is that assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, nuclear plant safety issues receive the attention warranted by their significance.

Reference [3] presents a complete treatment of the subject, including an Appendix containing a long list of safety culture indicators, like the following: "Do staff routinely read and understand reports on operating experience?". The list is subdivided into four sections: Government and its Organizations, Operating Organization, Research Organizations and Design Organizations.

It is here suggested that the review team submits the pertinent indicator-questions included in INSAG-4 to the plant and design staff, in order to detect where a possibility of improvement might exist in the practice of safety culture. It is indeed believed that a progress in this field may compensate for possible inadequacies of plant designs conceived to old

standards, which may be difficult to fix by a backfitting action. A word of warning seems however in order here concerning the INSAG-4 indicator-question list. It has indeed to be appreciated that the list is very extensive and detailed and that some of the suggested questions could be neglected or reworded in view of previous answers obtained.

5. REPORT FORMAT

The final report serves as the formal documentation of the DSRS mission. The report is provided to the in-country counterparts at the concluding meeting in draft form to solicit comments and corrections.

The general layout of the report and the contents of each section are as follows:

SUMMARY

A one to two page executive summary is the first section. The executive summary should summarize the important aspects of the mission with emphasis on its Findings, Conclusions, and Recommendations;

INTRODUCTION: BACKGROUND AND OBJECTIVES

The Introduction should present the background material for the mission including any previous missions related to this site and facility. The objectives of the mission should be clearly stated;

CONDUCT OF THE MISSION

This section provides the details of the mission including schedule (day by day itinerary including meeting subjects, on-site visit and facility walk down, if appropriate, etc.), locations, participants, detailed scope of the mission, and a summary of the reference material provided in advance of the mission;

TECHNICAL SESSION FINDINGS

Findings are statements of the issues and their review within the scope of the mission. An appropriate format for the Findings section would include a general introductory section followed by, for each issue being considered:

(i) Summary of the specific objectives for the issue;

(ii) Background including a summary of previous reviews (open items, recommended actions, on-site visits, etc.);

(iii) List of reference material reviewed during the mission;

(iv) Summary of the studies and results presented to the IAEA review team during the mission;

(v) Summary of IAEA and other reference documents related to the findings; and

(vi) Summary of discussions and remarks including the positions of the in-country counterparts as they relate to the issue under consideration.

The findings should be clearly numbered for ease of future reference.

CONCLUSIONS

Conclusions state the observations of the IAEA review team with regard to the scope of the mission and the information provided by the in-country counterparts. In the conclusions section, the IAEA review team states their opinion as to whether the facility meets the criteria to which the review is being performed.

RECOMMENDATIONS

Recommendations present action items to the in-country team necessary to be performed to meet the review criteria.

Appendix I

DESIGN REVIEW GUIDELINES

I.1. GENERAL DESIGN REVIEW GUIDELINES

This portion of the design review mission is dedicated to the review of general design issues and programs at the nuclear power plant. The intent is to determine if the facility has been designed and has the necessary programmes in place to maintain that design, in order to provide a reasonable assurance that the plant will operate safely.

Requirements and review guidelines

The IAEA safety requirements for design are identified in Ref. [1].

I.1.1. Design management and organization

- The design management process has adequate internal checks to ensure that the systems, structures and components of a nuclear power plant have the appropriate characteristics, specifications and material composition such that the plant can operate safely with accident prevention and protection of site personnel and the public as the prime goal.
- During the design process, consideration was given to the requirements of the operating organization. These requirements took into account all operational aspects which include the capabilities of the personnel who will eventually operate the plant. The design organization has supplied adequate safety design information and recommended practices for incorporation into the plant operating procedures.
- The design management processes have taken account the results of deterministic and complementary probabilistic safety analysis, so that an iterative process takes place which ensures that due consideration has been given to the prevention of accidents and mitigation of their consequences.
- The design management processes have taken account the lessons learned from industry operating experience and from research. The design organization has a valid process for the review and incorporation of lessons learned from nuclear power industry operational experiences and from research.

I.1.2. Safety classifications

- All structures, systems and components (including software for instrumentation and control) which form all or part of a safety group, have been carefully identified and classified on the basis of their function and significance with regard to safety.
- The methodology for classifying the safety significance of a structure, system or component is based on a mixture of deterministic and complementary probabilistic methods. This methodology should take into account: the consequences of failure, the probability that the item will be required, the time following a postulated initiating event (PIE) at which, or during which, the item will be required to operate.

I.1.3. General design basis

- The design basis specifies the necessary capabilities of the plant to cope with a specified range of operational states and accident conditions within the defined radiation protection requirements.

- The plant conditions have been identified and grouped into a limited number of categories according to their probability of occurrence and potential radiological consequences.

- The design process includes consideration for safe normal operation of the nuclear power plant by establishing a set of requirements and limitations for operation. These requirements and limitations should include: constraints on process variables and other important parameters; safety system settings, and requirements for maintenance, testing and inspection of the plant.

- The plant design recognizes that challenges to all levels of defense may occur and that design measures have been provided to ensure that the safety functions are accomplished.

- The design has addressed the potential for accident conditions to occur also during low power and shutdown states, such as startup, refueling, maintenance, etc. when safety system availability may be reduced, and that appropriate limitations on safety system unavailability have been identified.

- The engineering design rules for systems and components are specified and comply with the appropriate accepted national standard engineering practices.

- A set of design limits consistent with the key physical parameters, is specified for each plant condition category, taking account of the likelihood of occurrence of each credible PIE and the potential consequences of the safety design requirements not being met.

- The nuclear power plant is designed to operate safely within a defined range of parameters (e.g. pressure, temperature, power) and assuming the availability of a minimum set of specified back-up facilities (e.g. auxiliary feedwater capacity and emergency power supply). The design considers the response of the plant to a wide range of events, and will allow safe operation or shutdown, if required, without the necessity of invoking provisions beyond the first, or at the most the second, echelon of defense.

- Protection system provisions include the means to initiate automatically the operation of the necessary safety systems, to prevent progression to a more severe condition which may threaten the next barrier. The protection system also allows manual initiation of automatic protection sequences, should the operator deem it necessary.

- The design accounts for required operator actions necessary to place the plant into a stable long term shutdown condition.

- Equipment required during the recovery processes has been placed at the optimal location to ensure its ready availability and the environmental conditions at the location have been considered during the accident conditions.

- Consideration has been given to severe accident sequences so that preventive or mitigative measures can be identified (Ref. [4], paras AA5, AA6).

– Design activities have considered the following: important event sequences that may lead to severe accidents, potential design changes which could either reduce the likelihood of these events or would mitigate the consequences, plant design capabilities, including the possible use of some systems beyond their originally intended function and normal operating conditions and the use of additional temporary systems to return the anticipated accident condition to a controlled state.

I.1.4. Defence in depth [5]

The design process should incorporate the principle of defence in depth to ensure that multiple levels of protection are provided. The following requirements should be adhered to:

– Systems are conservatively designed, constructed and operated in accordance with appropriate quality levels and engineering practice.

– The design provides multiple physical barriers to the release of radioactive material to the environment.

– Provisions were made in design to prevent operational occurrences from escalating into accident conditions.

– Provisions were made to allow other systems to act to control the consequences of accident conditions and to bring about stable and acceptable conditions.

– The design provides for the supplementing of the control of the plant by automatic activation of safety systems and by operator actions.

– The design provides for equipment and procedures to back up accident prevention measures, to control the course, and limit the consequences of accidents.

– In addition, the safety design objectives listed in Section 3.1 of Ref. [6] should be reviewed.

I.1.5. Safety analysis

– A safety analysis of the plant design, applying deterministic and complementary probabilistic analysis methodologies has been performed to establish and confirm the design basis for the items important to safety and to ensure that the overall plant design is capable of meeting the prescribed and acceptable limits for radiation doses and releases for each plant condition category. A description of the deterministic and probabilistic analysis requirements is identified in Section 4.4.1 of Ref. [1] and in Ref. [4] (paras GL3, GL4, AA2, AA3, IH6).

– The applicability of the analysis methods and degree of conservatism used have been verified.

– The safety analysis of the plant design is regularly updated as a result of significant changes in plant configuration, operating experience and, more in general, knowledge advancements.

I.1.6. Design verification

The design organization has implemented a programme of design verification to ensure that the design delivered for fabrication and construction and built during construction meets the safety requirements set out at the beginning of the design process. Details of an acceptable design verification process are given in Section 4.5 of Ref. [1].

I.1.7. System and component reliability

- The potential for common mode and common cause failures in safety systems, structures and components has been considered.
- The single failure criterion has been applied to each safety group incorporated in the plant design..
- Spurious actions have been considered as one mode of failure.
- Non-compliances with the single failure criterion have been justified.
- The principle of failure to safety (fail-safe) has been incorporated into the design of systems and components important to safety for the nuclear power plant.
- Auxiliary services necessary to maintain a safe state of the plant (e.g. electricity, cooling water, compressed air or other gases, means of lubrication, etc.) are considered as part of the system important to safety.

I.1.8. Provisions for in-service test, maintenance and inspection

- The design of structures, systems and components important to safety has considered calibration, testing, maintenance, inspection and monitoring with respect to their functional capability during the life of the nuclear power plant.
- The design ensures that reasonable on-line maintenance and testing of systems important to safety can be conducted without the need to shut down the plant.

I.1.9. Equipment qualification (Ref. [4], para. GL2)

- Equipment is designed and programmatically maintained to be capable of meeting, throughout its operational life, the requirements for performing safety functions while subject to the environmental conditions (e.g. vibration, temperature, pressure, jet impingement, radiation, humidity) existing at the time of need.
- To the extent possible, equipment expected to operate during severe accidents (e.g. certain instrumentation) can, with reasonable confidence, achieve the design intent.

I.1.10. Ageing (Ref. [4], para. GL2)

The design provides appropriate conservatism for all safety related structures, systems, and components to take into account relevant ageing mechanisms and potential age related degradation.

I.1.11. Human factors

The design has considered plant layout, operational, maintenance and inspection procedures, in order to facilitate the interface between the operating personnel and the plant.

- The working areas and working environment of the site personnel have been designed in accordance with accepted ergonomic principles.
- There has been a systematic consideration of human factors and the human–machine interface included in the design process at an early stage.
- The human–machine interface has been designed to provide the operators with comprehensive, but easily managed information, compatible with required decision and action times.
- The human–machine interface has been considered also in the design of the supplementary control room.
- When the nuclear power plant information display and controls were designed, the operator was considered to have dual roles: that of a systems manager, including accident management, and that of an equipment operator.
- The design aims to promote the success of operator actions in the light of the time available, the expected physical environment, and psychological pressure.

I.1.12. Configuration management

Within the general framework of the quality assurance programme, a configuration management programme should exist. Configuration management refers to the effective control of the plant's as-built configuration and operation to ensure compliance with approved and accepted design bases. Configuration management of the plant should identify and document the physical and functional characteristics of the plant's structures, systems, components, and computer software, and ensure that changes to the documented characteristics are properly developed, assessed, approved, issued, implemented, verified, recorded, and incorporated into the plant's controlled documentation. The configuration management programme should meet the following provisions:

- The plant design bases are identified, validated, and documented.
- Systems, structures, and components required to be maintained within the configuration management programme are identified. Appropriate documentation and/or computer databases exist to document these items and link them to the design bases.
- A change control process exists which ensures that physical and operational changes meet the design bases, are properly executed, and are incorporated into plant documentation in a timely manner.
- The plant maintains a document control process which ensures current plant configuration is reflected in appropriate controlled documents (i.e. drawings, procedures, reports, tables, etc.), and ensures that documents are properly approved before use, released and distributed to appropriate personnel, updated in a timely manner, and tracked pursuant to revision level and approval status.

– The management information system for configuration management, either manual or automated, should ensure that versions of information in different documents or databases are consistent, prevent unauthorized changes to information, clearly identify authority and responsibility for data maintenance, and make data and information easily available to those who need it.

I.1.13. Other design considerations

– For multi-reactor sites, structures, systems and components important to safety are normally not shared between two or more nuclear power reactors. If structures, systems and components important to safety are shared between two or more nuclear reactors, it has been demonstrated that all safety requirements are met for all reactors.

– All nuclear power plant systems that may contain fissionable or radioactive materials have been designed to ensure adequate safety in operational states and in accident conditions.

– If the nuclear power plant is coupled with district heating and/or water desalination units, it has been designed to prevent transport of radioactivity from the nuclear plant to the desalination or district heating unit during normal operation and accident conditions.

– Structures, systems and components important to safety have been designed and located to minimize, consistent with other safety requirements, the probability and effects of fires and explosions caused by internal events. External events are outside the scope of this review.

– Non-combustible or fire retardant and heat resistant materials have been used wherever practicable throughout the plant, particularly in locations such as the containment and control room.

– Internal floods and missiles (Ref. [4], para. IH9) generated within the plant boundary have been considered in the design of the nuclear power plant.

– The nuclear power plant design has a sufficient number of simple, and clearly and durably marked, safe escape routes with reliable emergency lighting and other building services essential to the safe use of these routes.

– Suitable alarm systems and means of communication have been provided so that all persons present in the plant can be warned and instructed even under accident conditions.

– Communications necessary for safety, both within the nuclear power plant and to the outside, are assured at all times.

– The nuclear power plant’s design has considered a permanently controlled access to guard against unauthorized entry of persons and goods to the plant.

– The nuclear power plants design has considered restricting unauthorized access to, or interference for any reason, with safety structures, systems and components.

– Systems which have a significant probability to be required to operate simultaneously have had their interactions, such as effects from physical or electrical connection, environmental conditions, or component failures, evaluated.

– The design of the nuclear power plant has accounted for grid-plant interactions in relation to the required reliability of the power supply to the plant systems important to safety (Ref. [4], para. AA7).

– At the design stage, special consideration was given to the incorporation of features which will facilitate the decommissioning and dismantling of the plant.

I.2. PLANT SYSTEMS DESIGN REVIEW GUIDELINES

This section includes design review guidelines for the reactor core, reactor coolant system and associated systems, containment systems, instrumentation and control/protection systems, emergency power systems and fuel handling and storage systems. For each area there is a discussion of the requirements and review guidelines for each system. In addition, issues for each area have summarized from Ref. [4]. Each of these issues should be reviewed and considered as appropriate while performing the design review. It is important to note that these issues are only for LWRs, issues for other reactor designs have not been discussed in these guidelines.

I.2.1. Reactor core

Requirements and review guidelines

A more detailed list of requirements is included in Refs [1, 7]. A list of the main items to be checked is included here for convenience; some additional elements have been added:

General requirements

Radioactive materials should be confined within the fuel matrix and the fuel cladding to the maximum possible extent; indeed, the fuel matrix and cladding are the first two physical barriers in a defence in depth scheme:

– A basic safety design intent is to assure, as far as practicable, reactivity behaviour characteristics of the core which are favourable to safety, e.g. the power coefficient of reactivity should never be positive.

– Reactor core components and associated structures should be designed taking into account safety functions to be achieved during and following accident conditions, e.g. reactor shutdown, emergency core cooling and long term stable cooling.

Basic neutronic and thermalhydraulic design

The combination of inherent reactor neutronic characteristics, thermohydraulic characteristics and the control system capability should be sufficient to provide adequate regulation of the reactor power for all operational states.

– The reactor should be capable of being shut down and held subcritical under operational states and accident conditions.

- Adequate provision for cooling the core under operational states and accident conditions should be made and cooling effectiveness should be proven by analysis or experiment.
- Assessments of the core power distribution, especially peak channel power and peak linear heat rating, should be performed on an iterative basis during the design for representative operational states to provide bases for: (a) operational limits and conditions; and (b) operating procedures which would ensure compliance with design limits, including core design parameters, throughout reactor core life.
- Appropriate instrumentation and control means should be provided so that parameters indicative of core conditions including fuel element integrity can be monitored and core conditions adjusted safely to ensure that design limits are not exceeded during operational states.
- The design of the core should take into account the fact that it is desirable to achieve a low demand on the control system for maintaining axial, radial and local power distributions within the limits stipulated for normal operation.
- Analytical models, data and computer codes used in the neutronic and thermohydraulic design of the core should be based on adequate experiments or measurements applicable to the conditions expected.
- Thermohydraulic design limits on such parameters as minimum critical power ratio, minimum departure from nucleate boiling ratio, local cladding temperature and fuel temperature should be set such that sufficient margins exist during operational states to keep fuel failures to an acceptably low value.
- Appropriate monitoring instrumentation should be provided for assessing the state of the core during accident conditions.

Considerations for mechanical design

- The fuel elements and assemblies should be designed to ensure that the cladding remains leak tight for operational states, as far as is practicable.
- Structural integrity should be ensured, so that the core can be safely controlled, shut down and cooled under operational states and accident conditions.
- All core and associated components should be designed to be compatible with each other under the effects of irradiation, chemical and physical processes and static and dynamic mechanical loads, including thermal stress, existing during operational states and accident conditions.
- Means should be provided for safe handling of core components to ensure their integrity during transport, storage, installation and refueling operations.
- Means, preferably physical, should be provided to inhibit the incorrect location in the core of any components important to safety, e.g. fuel assemblies and reactivity control or shutdown devices.
- Uncontrolled movement of reactivity control devices should be prevented.
- High quality design and fabrication should be ensured by the establishment and implementation of satisfactory quality assurance procedures.

– The design of the core, other reactor internals and the reactor cooling system should minimize the chance of any obstruction of the coolant flow which could lead to core damage during any operational state.

Fuel elements and assemblies

The following aspects should be included in the review:

– Effects of changing pellet thermal conductance and pellet-cladding resistance with service time.
– Cladding overpressurization due to production of fission gases and its consequences in normal operation and in accidents.
– Effects of burnup on metallurgical clad properties, geometrical stability, power distribution (plutonium), reactivity and coefficients of reactivity.
– Pellet-cladding interactions during power transients.
– Effects of burnable poison on reactivity coefficients and gas production.
– Hydrogen embrittlement of zircaloy cladding, also as a consequence of moisture inside the cladding.
– Absence of critical heat flux in normal conditions.
– Impairment of the free movement of control-safety rods due to fuel deformations due to irradiation or vibrations.

Reactivity control means

The following aspects should be included in the review:

– Limitation of reactivity worth of any single reactivity control device in order not to exceed limits in case of accidental device ejection.
– Prevention of precipitation and of deposition of soluble poisons.

Core monitoring system

The following aspects should be included in the review:

– Monitoring of power level, distribution and temporal variation, of coolant and moderator, of reactivity control means.
– Monitoring of failed fuel.

Reactor shutdown means

The following aspects should be included in the review:

– Reactor subcriticality in any state, assuming one device inoperable (stuck rod).
– Two diverse shutdown systems required.

– In order to have subcriticality in the long term, operator action may be required (absorber movement due to maintenance or refueling operations are to be taken into account).

– Simple, reliable and possibly fail-safe systems.

– Absorber depletion with service and generation of gas.

– Chemical attack.

– Structural deformations of shutdown devices and of core structures and its effect on shutdown time delay.

Core support structures and reactor internals

Special care should be exercised to avoid fluid induced vibrations: long cylinders and long rods or pieces of pipes are particularly sensitive to these phenomena; in case of uncontrolled vibrations, structural breaks may happen, which might endanger core and shutdown capability and reactor pressure boundary integrity (metal pieces may concentrate in specific places and result in the erosion of the pressure boundary wall).

Core management

– Safety parameters affecting fuel utilization. Reactivity, fuel and clad temperatures, peaking factors are not directly measurable: the core operation has therefore to be closely followed by the use of instruments and of calculations.

– A complete core safety report should be prepared at each refueling.

Qualification and testing

– Initial qualification of equipment and its result

– Initial and periodic inspections

– Quality assurance in design, manufacture and operation.

Specific issues

Inadvertent boron dilution under low power and shutdown conditions (Ref. [4], para. RC 1; Ref. [8], para. RC 1)

Operational experience and probabilistic safety analyses have indicated that inadvertent boron dilution at lower power and shutdown conditions can occur. A slow dilution might be due to leakage of fresh water into the primary system and its consequences could be handled by the reactor protection system. Boron concentration is frequently monitored by samples and continuously by boron meters located in the primary circuit. On the contrary, a large and quick insertion of fresh water in the system (due, e.g. to the start up of a pump at low power or shutdown in conditions of unbalanced boron concentration among the various loops) could give rise to prompt criticality and to fuel damage. Measures taken to prevent or

to mitigate such events range from the installation of additional interlocks, additional and/or improved instrumentation to the improvement of operating instructions.

Slow and unreliable insertion of control rods (Ref. [4], para. RC 2)

This phenomenon has happened many times in various reactors and is due to various causes, such as: bowing of fuel elements due to excessive retaining spring force, wear due to incorrect tolerances, degraded drive mechanisms, irradiation induced deformations of fuel bundles. The phenomenon severity ranges from the complete blockage of a control rod to the slow fall of some rods. Remedial actions include replacement of hold down springs, more frequent testing, avoiding placement of highly irradiated bundles in control rod positions.

Power oscillations in BWR (Ref. [4], para. RC 3)

Power oscillations have been observed at various BWRs. Both stable and divergent oscillations are possible. The oscillations are caused by the reactor entering in a power-flow rate region capable of sustaining them. Remedial actions consisted in more stringent limits in the operating region of the reactor and in the installation of automatic suppression systems based on control rods.

Loss of thermal margin caused by channel box bow (Ref. [4], para.. RC 4)

Bowing of fuel boxes in a BWR has caused local neutron peaking and fuel rod burnout. The box in question was at its second cycle in the reactor. Remedial actions have consisted in limiting the life of the fuel boxes and in taking into account such a bowing in the thermal-hydraulic calculations.

Accident response of high-burnup fuel (Ref. [4], para. RC 5)

On the basis of recent transient tests with high burnup fuel, it has to be expected that fuel ruptures might happen for lower values of specific enthalpy at high burnup. A higher release of fission products during transients and accidents might ensue. This issue is still under study and a conservative attitude is justified.

Fuel cladding corrosion and fretting (Ref. [4], para. RC 6)

During refuelling tests, some fuel rods damaged by fretting and corrosion were found. Apparently the phenomenon was peculiar to the particular reactor and position in core. The subject is under study and its generic significance for safety is questionable.

Insufficient subcriticality monitoring at shutdown (Ref. [8], para. RC 3)

Some reactors do not use a neutron source to monitor neutron flux at shutdown. Therefore, the degree of subcriticality may be uncertain. In this case a new measuring system should be installed.

I.2.2. Coolant system and associated systems (RCS and RCAS)

Requirements and review guidelines

The system design requirements for the reactor coolant system (RCS) and reactor coolant associated systems (RCAS) are identified in Refs [1, 9, 10].

Each of the major components of the RCS (reactor vessel, reactor coolant pumps, pressurizer (including heaters and spray nozzles), pressure relief and safety valves, steam generators, and the pressure boundary) and the RCAS (emergency core cooling, residual heat removal, chemical and inventory control, steam, feedwater, service water, component cooling water, and ultimate heat sink) have been designed with the following considerations:

RCS postulated initiating events (PIE)

- Review the plant's listing of reactor coolant system PIEs and the analysis for each.
- PIEs that could have a significant influence on the RCS design include: pipe breaks, heat exchanger tube failures, internal missiles, fires and pump failures. The methodology for plant response analysis PIEs is described in Ref. [11].

RCS design basis

- Review the listing of the system performance requirements for the RCS and RCAS components.
- Review the listing of codes and standards used for the design of the major RCS and RCAS components.
- Review analysis identifying the limiting condition for which each RCS and RCAS component has been designed.

Material selection for RCS structures and components

The design process for the selection of RCS component materials considers the following:

- chemical compatibility with the coolant
- compatibility with adjoining materials
- strength, creep and fatigue properties
- corrosion and erosion resistance properties
- irradiation damage effects
- ductility characteristics
- fracture toughness
- ease of fabrication, weldability
- activation characteristics (type of radiation, impurity contents, half-lives)
- behaviour during PIEs (e.g. metal/water reaction).

Layout — Radiological protection and component accessibility

The layout and equipment accessibility of the RCS and RCAS components should allow inspection, maintenance and repair while keeping the exposure of site personnel as low as reasonably achievable. Additional guidelines on plant layout are provided in Ref. [12].

Protection against the consequences of pipe failure

A detailed discussion and review guidance regarding pipe failure criteria, assessment of pipe failure consequences and protection against pipe failure consequences are listed in Section 3.9 of Ref. [6].

Overpressure protection

- All pressure containing components of the RCS and RCAS are protected against overpressure that exceeds design specifications by an integrated overpressure protection system which includes: instrumentation and control systems that are designed in accordance with Ref. [13], pressure relief valves, safety valves, and a reactor protection system that is designed in accordance with Ref. [14].
- Additional discussion and review guidance on overpressure protection is listed in Section 3.10 of Ref. [6].

Instrumentation and control (I&C)

- The operator has adequate instrumentation and control to be able to determine if abnormal RCS conditions exist, RCS operating parameters are approaching approved operational limits, a safety function related to the RCS needs to be performed, the RCS safety systems are ready to perform their safety function or they are in the process of carrying out their safety function, and whether or not the safety function has been accomplished.
- Appropriate monitoring equipment for the detection of leaks should be provided.
- General guidance on review of instrumentation and controls is provided in Section 2.4 of this appendix.

Reactor coolant activity

- Design measures have been taken to reduce the sources of radiation associated with the reactor coolant system activity in order to keep the radiological consequences as low as reasonably achievable.
- The selection of materials, maintenance of fuel cladding integrity and leaktightness, and reactor coolant chemistry control were taken into account during the original design.
- Provisions have been made for purification of the RCS during normal operation.
- RCS decontamination piping, if provided, has not become a location for unacceptable sources of radioactive sludge and debris.

– The design has considered the potential effects of the radiolysis of water and possible accumulation of combustible mixtures in high points in the primary circuit.

Interface requirements

– Interface requirements, both physical and performance related, are specified in the design to ensure compatibility between the RCS, RCAS, and supporting systems. Supporting systems include heating, ventilation, and air-conditioning (HVAC), service water, component cooling water, condenser, compressed air and other systems required for the operation of the RCS and RCAS. The interface requirements should include, but not be limited to, those for flow rates, loadings, response times and heat transfer capabilities. Supporting systems should be subjected to the design requirements consistent with the design requirement of the systems they support. Therefore, each supporting system should be designed in accordance with the same safety class, seismic classification, separation, redundancy and environmental qualification as the applicable RCS or RCAS system or component.

– Systems or portions of systems of different safety classes should be connected through appropriate interface devices. Their function should not cause either loss of safety function of the higher class system or escape of radioactivity. Each interface device should have the same safety class as the higher safety class to which it is connected.

– Interfaces between RCAS and those structures not included in the RCAS should be specified for design considerations. Typical interface requirements include:

  - design loading conditions,
  - temperature of the structures and components must be within acceptable limits,
  - in-service inspection requirements,
  - supports anchored directly to the containment should be designed to prevent loosening with possible subsequent loss of containment leaktightness; they should also be designed to allow periodic testing of the containment,
  - clearance between piping and pipe whip restraints should be as small as possible to reduce the energy impact.

Provisions for inspection, testing and maintenance

– Portions of the RCS important to safety are designed to be tested, maintained, and inspected for functional capability. The specified inspection and test methods should not call for performance capabilities beyond established techniques.

– Testing simulates as closely as practicable the conditions under which the safety functions will be provided.

– Inspection intervals, methods, locations, and acceptance criteria ensure timely detection and correction of any deterioration or ageing that might preclude components from performing their design function.

Integrity of major pressure retaining components

- Reactor pressure vessels should be constructed of materials with appropriate properties such as ductility and toughness, and conservative stress limits should be used. The design should account for all base and cyclic loads expected to occur during the lifetime of the plant.
- Steam generator tube design should take into account all the cycles of maximum stress expected to occur during operational states and accident conditions. The steam generator tube design should permit examination over the entire length of the tubes. Tube support components and the method for connecting the tubes to the supports should not cause damage or cracking of tube walls.
- Additional guidance is provided in Ref. [6].

Requirements and review guidelines for reactor coolant and associated systems (RCAS)

Emergency core cooling

- The design should include adequate cooling for a sufficient time for the entire spectrum of accidents and failures considered in the plant design.
- The design should incorporate backup electrical power, redundancy, diversity, separation, and consider single failure criterion.
- Pump intakes should be protected against clogging due to debris and should be designed to prevent cavitation. NPSH calculations should use conservative data.
- If borated water is used, the design ensures that boron deposition is avoided (i.e. by switching over to hot leg injection after 12 hours).
- For BWRs, the control rod cooling system is capable of providing a backup cooling function in emergencies.

Residual heat removal

- The system should be capable of removing the residual heat from the core at a rate that ensures design limits for the fuel and the RCS pressure boundary are not exceeded.
- Provision for isolation from the RCS should be included, and overpressure protection should be guaranteed.
- The design should incorporate backup electrical power, redundancy, diversity, separation, and consider single failure criterion.

Chemical and inventory control

- The system should have adequate capacity to ensure the inventory and pressure of the RCS are maintained within design limits for all operational states and anticipated transients.
- Adequate instrumentation should be provided to monitor volumetric changes, leakage and water level.

- The system should maintain chemical conditions and remove impurities and suspended solids to keep the RCS within specified limits, minimize deposition of crud, and protect against corrosion.
- Provision should be made to remove activated corrosion and fission products leaking from the fuel.
- Degassing devices should be provided when needed to meet prescribed limits.
- If chemical reactivity control is used, the system should meet the requirements set forth in Ref. [10].
- Backup electrical power, redundancy, diversity, separation, and consider single failure criterion should be considered commensurate with the functions of the specific component.

Steam and feedwater

- The system is designed to maintain heat transfer from the RCS at a rate that will maintain the reactor core within design limits for all operational states and transients.
- Backup feedwater capability is provided in case the normal feedwater system is unavailable.
- The feedwater system is designed and controlled to prevent steam generator overfill.
- The steam generator overpressure system is designed for potential steam generator tube rupture such that primary water is not discharge from the safety or relief valves.
- Backup electrical power, redundancy, diversity, separation, and consider single failure criterion should be considered commensurate with the specific functions of the component. The backup feedwater system is specifically designed for reliability.

Ultimate heat sink

- The type of ultimate heat sink selected should be based on site-related natural phenomena (e.g. earthquake, flooding, extreme weather, volcanic activity, etc.), external man-induced events (e.g. aircraft crash, explosion, vehicle impact, loss of off-site power, etc.), and internal plant events (e.g. fire, pipe rupture, internal flooding, etc.).
- The design should take into account the following heat loads: reactor core decay heat, spent fuel decay, stored heat, heat rejected from items important to safety, and other accident-related heat loads (e.g. chemical reactions).
- For multi-reactor sites, active components should generally not be shared. If they are, the design should be capable of dealing with accident conditions in one reactor while maintaining safe shutdown of the remaining reactors.
- The design should incorporate backup electrical power, diversity, separation, and consider single failure criterion.
- Additional guidance is provided in Ref. [15].

RCS pump seal injection

The reactor coolant pump seal injection system is designed with appropriate backup electrical power, redundancy, diversity, separation, and considers single failure criterion

Specific issues

The following RCS and RCAS issues have been identified and should be reviewed and considered as appropriate while performing the design review. Each of these issues are discussed in detail in Ref. [4].

Overpressure protection of the RPV at solid conditions and at low temperatures (Ref. [4], para. PC 1)

Reactor coolant system safety and relief valves when used to perform their safety functions such as mitigation of a steam generator tube rupture accident or cold overpressure protection, may have to fulfil their function in water flow conditions that they may not have been designed for. Using these valves that are not qualified for water flow to limit RCS pressure in water solid conditions could lead to a loss of coolant accident. The majority of events have occurred during startup or shutdown conditions at low reactor vessel temperatures. The primary approach to prevent these events to provide additional spring loaded safety valves and to limit the number of high pressure safety injection pumps available at low temperatures.

Adequacy of the isolation of low pressure systems connected to the reactor coolant pressure boundary (Ref. [4], para. PC 2)

Isolation valves between the reactor coolant system and the low pressure interfacing systems may not adequately protect against overpressurization of the low pressure systems if they are leaking or are inadvertently opened. The failure of RCS isolation valves, including check valves, could result in a loss of coolant accident and containment bypass. Several accidents have been reported where failures in RHR or ECCS check valves have resulted in opening of pressure relief valves or the bypass of primary coolant to the refueling water storage tank.

Reactor coolant pump seal failures (Ref. [4], para. PC 3)

Reactor coolant pump seal failures can challenge the makeup capabilities of nuclear power plants. In PWRs, this can occur during station blackout conditions. A loss of seal injection flow may damage the pump seal and lead to a LOCA condition. A typical solution to this issue is to backup up the seal water cooling pumps with emergency power from an electrical diesel generator.

Safety, relief and block valve reliability — primary system (Ref. [4], para. PC 4)

If a safety valve on the primary circuit should fail to close in connection with a safety transient, the transient could result in a small break LOCA. The risk of a safety value not closing after actuation is high at some nuclear power plants if the valve has not been qualified

for steam/water flow. Pilot operated relief valves (PORVs) are involved in the mitigation of some accidents and as such their insufficient reliability could impair the fulfilment of safety functions.

Safety, relief and block valve reliability — secondary system (Ref. [4], para. PC 5)

A primary to secondary leak such as a multiple tube failure in a steam generator could result in overfilling a steam generator. Water could enter the steam lines and reach the safety and relief valves. The lack of qualification of these secondary circuit valves to operate with water or water-steam mixture can lead to their inability to close after actuation. This event is serious because of the potential release of effluent directly to the environment.

Spring-actuated safety and relief valve reliability (Ref. [4], para. PC 6)

Inoperable pressure relief valves or incorrect pressure settings can significantly increase the risk of overpressurization of the reactor vessel or the steam generators. In addition, relief valves that open prematurely can initiate unnecessary plant transients. It is important to verify the facility's maintenance, calibration and testing capabilities. The facility's quality assurance programme should ensure that the pressure relief valves are installed correctly, properly set and are equipped with the proper springs.

Water hammer in the feedwater line (Ref. [4], para. PC 7)

It is critical that the plant design consider the possible impact of water hammer events on plant systems. Various water hammer events have occurred in feedwater piping or steam generator feedrings. The damage is primarily to pipe hangers and restraints, however, several incidents have resulted in piping and valve damage.

Steam generator overfill (Ref. [4], para. PC 8)

Operational experience at PWRs has resulted in operational procedures and designs which prevent the possible overfill of steam generators. The concerns are: increased weight and potential seismic loads placed on the steam lines, increased potential for water hammer, potential of a secondary safety valve sticking open, and the potential tube rupture in certain steam generator designs.

Emergency core cooling system sump screen adequacy (Ref. [4], para. SS 1)

The containment sumps are designed to collect primary circuit water after a LOCA in order to recirculate the water for the second phase of the accident. The sump openings are covered with screens to prevent debris from returning to the suction of the ECCS pumps. There is a potential for thermal insulation in containment to block the flow of water through the sumps to the suction of the ECCS pumps. Therefore, it is important that the design of thermal insulation for equipment and piping in containment and the design of the sump screens take into consideration this possibility of sump blockage. It is also important that the facility have a good containment housekeeping procedure to ensure that loose debris that could result in clogging of the sump screens is removed from containment prior to startup.

Emergency core cooling water storage tank and suction line integrity (Ref. [4], para. SS 2)

WWER-1000 plants have a ECCS water storage tank which also serves as the containment sump. The tank is located under the containment. Each of the three safety system trains has a single suction line from the tank to the ECCS and spray pumps. The suction line is equipped with one containment isolation valve. If there is a passive failure in the tank or in any of the three suction lines between the tank and the isolation valves it could lead to inadequate cooling capability during an accident. To mitigate the consequences of such an accident the facility should have increased non-destructive testing of the vital piping and isolation valves in these lines. The accident analysis should adequately address the potential consequences of the design issues of these systems on WWER-1000s.

ECCS heat exchanger integrity (Ref. [4], para. SS 3)

WWERs remove residual heat with heat exchangers that are cooled with service water. The service water supply is directly from a spray pond, lake or river, therefore , there is no closed loop intermediate cooling system. Use of these designs has the potential for excessive fouling of the heat exchanger and degradation of the piping. Tube ruptures in these heat exchangers can result in the addition of non-borated water to the primary circuit during shutdown conditions and contaminated water directly to the environment during normal operation or accident conditions. Various plant design changes have been made a facilities to help detect the presence of heat exchanger fouling. This issue should be considered in the facilities safety analysis.

Problems of emergency core cooling switchover to recirculation (Ref. [4], para. SS 4)

Switch over of the ECCS and containment spray pumps from the injection phase to the recirculation phase of an accident involves realignment of several valves and may be accomplished by manual, automatic or semi-automatic operations. The logic of these operations is designed to deal with the prevention of spurious operation and ensuring a high level of protection. A potential problem exists during switchover of the suction from the refueling water storage tank to the containment sumps. The problem is due to an inadequate suction pressure potentially resulting in pump damage during switchover. The facility’s safety analysis should satisfactorily address this issue and plant operating procedures should be clearly written to mitigate the possibility of this event.

Diversion of recirculation water (Ref. [4], para. SS 5)

This issue involves the potential hold-up of water required during the recirculation phase of an accident. If the volume of water held up in sumps, pools and canals is greater than the margin of excess water allotted in the re-circulation systems, containment cooling and/or reactor cooling could be lost during some LOCA events. A typical example of this problem is the situation where the refueling canal drain valves are left closed during operation resulting is a large volume of water that does not return to the containment sump.

Boron crystallization issues (Ref. [4], paras SS 6, SS 7 and CI 13)

There have been various incidents at PWRs involving the crystallization of boric acid on safety related pumps and piping. This is a particular problem at plants that have systems containing very highly concentrated boric acid that is used in some accident conditions. This

problem is especially prevalent on low alloy carbon steel components of the reactor pressure boundary.

There is also a concern of boron crystallization in the core during the recirculation phase of an accident. There is a potential of core flow blockage and of dilution of the recirculation coolant due to excessive boron crystallization. Therefore, during the recirculation phase there should be designed capabilities to switch the flow from the cold legs to the hot legs as necessary to reduce the potential for excessive boron crystallization.

Steam generator safety valve performance at low pressure (Ref. [4], para. SS 10)

WWER steam generators have two types of valves installed in their steam lines (2 safety valves and 1 relief valve). The relief valves are normally set from 74 to 1 bars and the safety valves are set from 84 to 40 bars. In the case of the WWER-440/213's the relief valve is located downstream of the main steam isolation valves (MSIV). There are some transients which require the use of safety valves at low pressure to cool the primary circuit. Therefore, the safety and relief valve design on these plants may not be adequate to deal with certain accidents that require long term cooling through the SG safety valves, if the relief valve is inoperable.

Thermal shock or fatigue caused by cold emergency feedwater supply to steam generators (Ref. [4], para. SS 11)

Several incidents have occurred due to the injection of cold feedwater in the steam generators resulting in thermal shock and subsequent damage to the feedwater piping or steam generators. These events are normally caused by actuation of the emergency feedwater system which is started only if AC power is not available for the auxiliary feedwater pumps. Damage to the steam generator internal structure and feedwater piping may result in coolant leakage. Even if provisions are made to cope with a limited number of thermal shocks, every provision should be made to reduce the number of these events.

Emergency feedwater system reliability (Ref. [4], para. SS 12)

Various studies have indicated that auxiliary feedwater systems (AFW) have a relatively high rate of failure. These are typical examples of potential AFW system failures: common-mode failure of AFW pump discharge valves, excessive delays in restarting AFW pump steam turbines and potential loss of flow due to feed or steam line breaks. The initiating events for a total loss of feedwater are plant-specific and should be clearly discussed in the facility's safety analysis. This event is potentially very serious and can significantly contribute to the core-melt frequency.

Overfill into the main steam lines in BWRs (Ref. [4], para. SS 14)

Degradation of the pressure relief capabilities is possible if water is introduced to the steam lines of BWRs. There are two possible solutions to this problem: verify the ability to reduce reactor pressure even if there is water in the steam lines or install qualified valves. If the steam lines are filled with water the risk of primary system overpressurization is significant.

Reliability of motor operated valves in safety systems (Ref. [4], para. SS 16)

Operating experience has proven that a number of safety related valves or valve operators have failed to operate on demand either during testing or during accident conditions. Gate valves have been particularly vulnerable to failures. The valve malfunction can be due to various causes including: improper switch settings, underestimating thrust/torque requirements, or overestimating motor actuator output. Test capability to represent design basis conditions in addition to preoperational, periodic and factory tests should be used to ensure that these valves will operate satisfactorily upon demand.

Reliability and mechanical failures of safety related check valves (Ref. [4], para. SS 17)

There have been a significant number of identified problems with safety related check valves that have resulted in decreased system reliability and unnecessary plant transients. In some cases check valve design has been inadequate resulting in failure of internal parts. In other incidents the design did not properly consider the sizing, installation and location for the system conditions under which the valve would be used. Malfunctioning safety related check valves could create unacceptable results during accidents and increase the risk associated with postulated core-melt accident sequences.

Need for assurance of ultimate heat sink (Ref. [4], para. SS 19)

The ultimate heat sink (river, lake, pond etc.) should be shown to be capable of dissipating the heat following normal and abnormal operating conditions. A significant number of events have resulted in degradation or complete loss of service water systems. These include: various fouling mechanisms, ice effects, flooding, single failures, multiple equipment failures and personnel errors. The initiating events are plant specific and should be clearly addressed in the facility's safety analysis. A complete loss of the service water/ultimate heat sink could potentially lead to a core-melt accident.

Reactor pressure vessel integrity (Ref. [4], para. CI1)

Tests on irradiated samples of reactor pressure vessels have indicated that the embrittlement of the ferritic steel could be more pronounced than previously thought, for a given degree of irradiation (fast neutron fluence). The safety relevance is enormous in the postulated cases of pressurised thermal shock (PTS) to be taken into consideration in the accident analyses. The failure of the vessel barrier will result in the failure of all of the reactor barriers. Remedial actions include: better material surveillance, reduced fluence (for new reactors), prevention of thermal shock (emergency core cooling water heating) and vessel annealing.

Asymmetric blowdown loads on reactor pressure vessel supports and internals (Ref. [4], para. CI 2)

Certain transient loads that could result from a postulated reactor coolant pipe rupture adjacent to the reactor vessel had been underestimated in the design analysis. Loads are lateral loads due to jet or reaction forces, differential pressures in the annulus between the vessel and

the reactor cavity and differential pressures across the core barrel. Consequently, the reactor vessel supports and internals may not have the margins of safety intended.

Analyses of the reactor pressure boundary using the leak before break (LBB) concept have shown that this phenomenon can be avoided by a timely shutdown of the reactor. In some cases, pipe motion restraints have been used at suitable locations in order to avoid ruptures which could cause the phenomenon.

Inconel 600 cracking (Ref. [4], para. CI 5)

Stress corrosion cracking was evidenced at various plants in control rod drive nozzles, pressurizer heater thermal sleeves and instrument nozzles. Remedial actions included replacement of parts (vessel heads) and augmented inspections.

Steam generator collector integrity (Ref. [4], para. CI 6)

WWER reactors have horizontal steam generators with hot and cold leg collectors. The steam generator tubes are connected to these collectors. Stress corrosion cracking in the bolted covers for these collectors has been identified as a significant degradation mechanism. The damage is possibly associated with the design of the cover seals which require a relatively high load. A large primary to secondary leak due to steam generator collector damage is not considered a DBA scenario, however, a large leak can impair the safety functions in case the BRU-A valve fails to close. This could lead to a containment bypass and leakage to the environment. The long term cooling of the core may be endangered.

Steam generator tube integrity (Ref. [4], para. CI 7)

PWR plants have observed degradation of the steam generator tubes that separate the primary from the secondary circuits. The main degradation mechanism has been identified as stress corrosion cracking, intergranular attack, denting and fretting. Degradation of steam generator tubing is detected by routine in-service inspection programmes during reactor outages.

Pipe cracks and feedwater nozzle cracking in BWRs (Ref. [4], para. CI 8)

BWRs have experienced pipe cracking in the heat affected zones of welds in the primary circuit piping. The cracks have occurred primarily in type 304 stainless steel. The main problem is recognized to be IGSCC of the austenitic stainless steel components that have made susceptible to this failure by being “sensitized”, either by post-weld heat treatment or by sensitization of a narrow heat affected zone near welds. A typical location for this problem is in the reactor vessel nozzles. Cracking of piping and feedwater nozzles threatens the integrity of the reactor pressure boundary.

Bolting degradation or bolting failures in the primary circuit (Ref. [4], para. CI 9)

Various failure and degradation has occurred that have adversely impacted the integrity of safety related bolts. Bolt degradation or failure could lead to the degradation or failure of safety related systems or to a loss of coolant accident. Primary circuit bolting should

be part of the in-service inspection programme at the plant. New designs should take into consideration the previous operating experience with existing bolting problems.

Cast stainless steel cracking (Ref. [4], para. CI 11)

Cast primary pump bodies in the primary and secondary circuits have been observed to have cracking problems. Cracking has been observed both inside and outside the casings. In some cases such cracking has also been observed in cast steel piping. The root cause of these cracking problems is due to the significant ferrite content of the piping material. Undetected cracks could lead to a loss of coolant accident or a failure of the effected component.

Loads not specified in the original design (Ref. [4], para. CI 12)

Piping connected to the RCS is subject to flow and thermal transients during normal operation of the plant. These transients involve repetitive thermal shocks, stresses and thermal stratification. Measurements during plant operations have indicated that the resulting loads may exceed fatigue and stress limits. For this reason the number of transients of various types should be tracked to ensure that transient limits, based on design assumptions, are not exceeded.

Steam and feedwater piping degradation (Ref. [4], para. CI 14)

Steam and feedwater piping is subject to degradation by corrosion, stress corrosion cracking, fatigue due to thermal stratification, water hammer and vibration. The piping material is usually carbon steel. Thermal stratification in feedwater piping can lead to significant stresses that may exceed design limits for fatigue.

Steam generator internals damage and plate cracking (Ref. [4], para. CI 15)

Several PWRs have experienced problems with steam generator internals. These problems were experienced with erosion/corrosion of the tube support plates and the wrapper barrel. Damage of the lateral supports in steam generators could affect the vibrational stability and the ability to sustain earthquake and LOCA loadings.

Solenoid valve reliability (Ref. [4], para. ES 9)

Solenoid operated valves (SOVs) are widely used in nuclear power plant safety systems as pilot valves. In this function these valves work with control system fluids, such as pneumatic or hydraulically operated isolation valves, and directly in fluid systems such as to vent the reactor head or to supply air to start the EDGs. Because the failure of SOVs can affect multiple valve functions in safety and non-safety systems, common mode failures of these valves could contribute significantly to risk.

I.2.3. Containment systems

Requirements and review guidelines

References [1] and [11] include a set of requirements to be checked during a design review of a containment system. Reference [1] includes problems from the generic consideration of severe accidents (to various degrees of severity according with the general assumptions of the specific design review); as an example, the problem of the preservation of the containment leak tightness besides that of the structural integrity and the survival of penetrations to severe accident environmental conditions are mentioned. In this connection, it is suggested to the review teams that a general position be initially developed concerning the degree of consideration to be given to beyond design (severe) accidents in the review.

One reasonable possibility is to look into the consequences of those severe accident phenomena that are important and most probable, once the assumption of a partial core melt has been made; these phenomena are: abundant hydrogen production and burning without detonations, consequent containment over pressurization, containment over pressurization due to malfunction of heat removal systems and possible existence of a direct passage from a containment bottom damaged by a molten core to the outside atmosphere. In many cases the ultimate structural capability of the containment structures goes well beyond design specifications and the containment integrity for many hours after the accident can be demonstrated with no plant backfitting; in other cases, backfitting provisions such as containment (filtered) venting devices have been implemented.

Accident management provisions are usually feasible in order to help plant operators to cope with such postulated severe accident situations.

Many safety experts believe that it is worthwhile to perform such a severe accident plant review, at least to have the plant operators well prepared in advance to take the most effective mitigating actions, even if no backfitting at all is implemented. In this sense it is also suggested here. In many cases, portable pieces of equipment for electric power supply or containment atmosphere cooling have been considered useful for severe accident management without major plant modifications.

In passing, it should be recalled here that much discussion went on in the past years concerning the possible detrimental consequences of pouring water over an overheated or molten core, either in the reactor vessel or in the containment floor; this problem was discussed at length in the framework of the Severe Accident Management (SESAM) Working Group, Committee for Safety of Nuclear Installations (CSNI), OECD. At last, in its concluding meeting (Niantic, Conn.,USA- Summer 1995) the group concluded with a clear statement in favour of the prevailing benefits of adding water to a damaged water reactor core. Water, therefore, should be supplied also to an overheated or molten core as soon as possible in order to quench it and stop the progress of containment damaging phenomena. The design review should also focus on the availability of emergency water in severe accident conditions.

Reference [9], even if a little older than Ref. [1], is considered applicable to containment design reviews.

For the convenience of the reader, a concise list of the requirements to be checked according to the above listed references has been included, with some comments and additions:

Coherence of the design basis for the containment system with postulated initiating events (PIE) and with safety performance specifications

The primary items to be checked include:

- pressure transient for containment envelope and systems
- temperature transient for containment envelope and systems
- differential pressure loadings for structures and equipment
- fluid jet impingement loads, pipe reaction loads, pipe impact loads and loads from internally generated missiles
- loads from external PIE (not specifically considered in this publication)
- radionuclide and hydrogen release to the containment
- environmental conditions (radiation levels, humidity, exposure to water and to its additives)
- combinations of the above listed parameters to be used as design conditions.

General design requirements

- Safety performance requirements (radionuclide releases in various conditions, ability to perform safety function during and after PIE)
- Reliability of structures and of subsystems, not necessarily expressed as reference numbers
- Qualification for postulated environmental conditions
- Maintainability
- Safety class
- Instrumentation and control in compliance with defense in depth concepts
- Power supplies
- Identification of containment parts and components
- Conditions to sharing of containment systems between various plants in multi-plant sites
- Recovery after accidents
- Decommissioning features.

Containment envelope and its extensions and appurtenances

- Resistance to pressure (positive and negative)/temperature
- Consistency with leakage requirements

- Differential pressures over internal containment structures
- Dynamic loads
- Consistency of coatings and thermal insulation materials with functional capability of filters and strainers (clogging)
- Reduction of the number of containment penetrations to the minimum
- At least two routes of egress from the containment.

Containment isolation

- Existence of adequate isolation systems on lines penetrating the containment according to applicable guides
- Existence of an adequate protection system for automatic isolation of containment penetrations.

Energy transfer and containment cooling

- Conservative consideration of energy transferred to the containment atmosphere for pressure/temperature calculations
- Adequacy of systems devoted to containment cooling in all specified plant conditions (including severe accidents as far as applicable) together with passive heat removal phenomena.

Radionuclide management

- Conservative calculation of amount of radionuclides released to the containment
- Check of survivability of essential safety equipment inside or near the containment system
- Adequacy of systems devoted to radioactivity removal.

Combustible gas control features

- Conservative estimate of hydrogen generated in the containment during an accident
- Adequacy of systems designed for hydrogen recombination/burning in a safe way.

Test and inspection

- Adequacy of the performed initial leak rate test
- Adequacy of the performance of periodic leakage tests (both local and integral)
- Existence of a complete record of test results including both "as found" and "as left" test results
- Identification of some systematic trends and corrective action taken.

Quality assurance and documentation

– Existence of a quality assurance plan which includes the containment system and its implementation.

Specific issues

Some containment issues to be considered in a design review are listed in Refs [4, 8].

A list of the main issues mentioned in these three references is presented here for the convenience of the reader, together with some additional comments:

Containment or confinement leakage from engineered safety feature (ESF) systems during an accident (Ref. [4], para. SS 9)

This issue was evidenced in the TMI accident, where radioactive products leaked from some of the reactor and containment auxiliary systems extending outside the containment building (reactor makeup and letdown system, containment sump purging system). It is worthwhile to check the possibility of these leakage paths during all of the postulated accidents, including some consideration of severe accidents. Remedial measures adopted by various countries include:

– increase of the leak tightness of buildings housing the safety systems outside the containment building;

– possibility to transfer highly radioactive leakages following an accident back into the reactor building;

– periodic tests of leakages between safety systems and their auxiliary systems.

Small break LOCA and containment bypass due to rupture of tubes between primary and secondary sides of primary system component heat exchangers

This event could take place in a WWER-1000 for breaks in the cooling circuit of primary pumps or in the primary letdown cooling heat exchanger. Backfitting modifications suggested are the installation of rupture disk in the secondary side of the involved circuits, discharging into the containment (besides other automatic valve isolation systems).

For prestressed concrete containment structures, sufficiency of instrumented tendons

Instrumented tendons should be more than a few percent of the total.

Dynamic loads due to condensation in suppression pools (Ref. [4], paras CS 1 and CS 2)

Containment systems based on pressure suppression (e.g. WWER-440/213 and BWR) have to be verified for resistance to dynamic pressure/underpressure loads during the condensation of the steam in case of accidents. Cases of containment damage have been recorded in operating experience, during various kinds of containment testing. Research results are also available.

Remedial actions can be taken in most cases, should a problem be identified. Quasi-static pressure loads on the containment structure following a LOCA may also exceed the structural capability of the containment if not correctly taken into consideration in the original design: real cases of this kind have been identified.

I.2.4. Instrumentation and control (I&C) protection systems

Requirements and review guidelines

A complete list of requirements is included in Refs [1, 16, 12]. Some of these requirements will be dealt with in the following:

General requirements

Instrumentation and recording equipment should be provided to ensure that essential information is available to monitor the course of design basis accidents and the status of essential equipment, and for predicting, as far as is necessary for safety, the locations and quantities of radioactive materials possibly escaping from their design locations. The instrumentation should be adequate to provide information as far as practicable about the status of the plant during severe accidents and for decisions during accident management.

Appropriate and reliable controls should be provided to maintain these variables within specified operating ranges.

Safety-related I&C systems normally include:

(1) Systems used to monitor or maintain plant parameters within:

  (i) Operational limits important to safety (e.g. coolant temperature or pressure control),

  (ii) Limits assumed as initial conditions in the safety analysis (e.g. reactor power limit control).

(2) Systems that may be utilized in the operation of safety systems, e.g. for testing the protection system.

(3) Systems used to detect and measure reactor coolant system leakage.

(4) Systems used to monitor the status of safety systems, e.g. those that monitor safety of safety channels, defects in pipes valves or pumps of safety systems.

(5) Systems used for accident monitoring and assessment, e.g. those which monitor and record, as necessary, containment pressure, containment radioactivity, reactor core cooling, radioactive releases to the environment and meteorological data.

(6) Other specific I&C applications important to safety, e.g. communication systems, fire detection and suppression, access control.

(7) Systems whose malfunction or failure could place a demand upon safety systems, e.g. pressurizer relief control, reactivity control.

(8) Systems whose malfunction or failure could cause a release of radioactive materials to the public and for which no safety system is provided, e.g. those that control waste management and spent fuel cooling.

(9) Systems which monitor or control plant environmental conditions that are necessary for proper functioning of plant equipment important to safety and habitability.

(10) Systems, other than safety systems, that perform functions important to the prevention, termination or mitigation of anticipated operational occurrences or accident conditions, e.g. reactor power setback systems.

(11) Systems, other than safety systems, that perform functions important to the maintenance of safe shutdown, e.g. provisions for computing the margin of criticality.

(12) Systems that monitor or control natural or man-made external phenomena that could adversely affect safety, e.g. seismic monitors (not specifically considered in this publication, see Section 2).

(13) Support systems for the above listed functions (e.g. emergency power systems, compressed air systems).

The order of the above list does not imply any gradation of importance to safety of these systems.

A plant protection system should be provided to:

(1) initiate automatically the operation of appropriate systems including, as necessary, the reactor shutdown systems in order to ensure that specified design limits are not exceeded as a result of anticipated operational occurrences;

(2) sense accident conditions and to initiate the operation of systems required to mitigate the consequences of such accidents within the design basis;

(3) be capable of overriding unsafe actions of the control system; and

(4) help, to the extent practicable, to mitigate the consequences of severe accidents.

Both instrumentation and control and protection systems components should be classified according to a logical safety classification system, as required by Section I.1.2 of this Appendix. Connected systems whose failure could jeopardise the operability of a specific safety related system, should be classified in the same class as the safety related system itself. Instrumentation, control and protection systems are relevant subjects for the implementation of the overall quality system of the plant.

These systems are qualified to operate under the environmental conditions to be expected after an accident for the needed service duration. Some systems may need to stay operable also after a severe accident (see Section I.1.8 of this Appendix).

Reliability and testability

The instrument, control and protection systems are designed for functional reliability and periodic testability commensurate with the functions to be performed. Design techniques, such as testability including a self-checking capability where necessary, fail-safe behaviour, redundancy, functional diversity and diversity in component design or principles of operation,

are used to the extent practical to prevent loss of a protection function. Features designed into the protection system should be sufficient at least to ensure that:

(1) no single failure results in loss of protection function;

(2) removal from service of any component or channels does not result in loss of required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated.

The protection system is designed to ensure that the effects of normal operation, anticipated operational occurrences and design basis accidents on redundant channels do not result in loss of its function.

Unless adequate reliability is obtained by some other means, the protection system is designed to permit periodic testing of its functioning when the reactor is in operation, including the possibility of testing channels independently to determine failures and losses of redundancy that may have occurred. The design should permit all of the three aspects of functionality (sensor, logic and final actuator) to be tested during operation.

There are a number of postulated failure causes that could affect protection system equipment and that need to be considered in the design of the system. The types of failures include random, common cause, cascading and analytical (resulting from inadequate or erroneous safety analyses). Numerous corrective techniques are available to reduce the likelihood or to alleviate the effects of these failures. Combination of these techniques may be required since any one technique is generally limited in its effectiveness. Table 1 of Ref. [4] provides representative examples of these failure causes and possible corrective techniques.

Use of computer-based systems

When the design is such that a safety system is dependent upon the reliable performance of a computer-based system, appropriate standards and practices for the development and testing of the computer hardware and software are established and implemented throughout the system life cycle, and in particular the software development cycle. In the present state of the art, the reliability of a computer based system cannot be predicted from the design process, nor tailored by the design process. For the hardware part of the system the confidence level can be assessed by using quantitative techniques; however, for software, only qualitative assessment is generally thought to be possible.

The level of reliability required is demonstrated by a comprehensive verification strategy which uses a variety of complementary means (including an effective regime of analysis and testing) at each phase of the process development in the framework of an appropriate quality assurance programme.

The level of reliability assumed in the safety analysis for the computer based system should be established on the basis of a conservative evaluation of the data from operational performance of identical systems used in similar applications.

Where a computer-based system is intended to be used in a protection system, the following requirements specifically apply:

(1) The highest standards and practices for the hardware and software are applied;

(2) the whole development process, including testing and commissioning, is properly documented and reviewable;

(3) as long as the computer-based system, in particular the software, has not been proven safe with a high level of confidence, a separate, “hard-wired”, back-up system is provided for the most critical functions;

(4) according to the extent and capability of the back-up system, and in order to confirm the confidence in the computer-based system reliability, the need for an assessment of the computer-based system by expert personnel independent from the designers and suppliers should be considered.

Separation of protection and control systems

Interference between the protection system and the control systems is prevented by avoiding interconnections or by suitable functional isolation. If signals are used in common by both the protection system and any control system, appropriate separation (e.g. by adequate decoupling and electrical isolators) is ensured. All safety requirements of Sections 2.4.1.1, 2.4.1.2 and 2.4.1.3 are met.

Electrical isolators include fiber-optic and photo-electric couplers, transformer-modulator isolators, current transformers, amplifiers, circuit breakers and relays. Isolators used are designed to prevent the maximum credible fault in the non-safety side of the isolator from degrading the performance of the safety side of it in an unacceptable measure.

Moreover, the protection system should be immune from adverse interactions with other plant systems; in particular the possibility of electromagnetic induction, electrostatic pickup, short circuits, open circuits and earthing faults should be taken into consideration during a design review.

Physical separation of the redundant portions of a safety system by distance, barriers or their combination in order to reduce the consequences of interactions or of area events such as fires should be also checked.

Control room

A control room (Section 4.9 of Ref. [13]) is provided from which the nuclear power plant can be safely operated in all its operational states and from which measures can be timely taken to maintain the plant in a safe state or to bring it back into such a state after the onset of plant design basis accidents and severe accidents. Room for additional people and equipment during emergencies should be provided Appropriate measures should be taken to safeguard the occupants of the control room against resulting hazards, such as undue radiation resulting from an accident condition, or toxic gases, which could jeopardize necessary operator actions.

The layout of the instrumentation and the mode of presentation of information provides the operating personnel with an adequate overall picture of the status and

performance of the nuclear power plant. Ergonomics are carefully taken into account in the control room design.

Devices are provided to give in an efficient way visual and if appropriate also audible indication of operating conditions and processes that have deviated from normal and could impair safety.

Supplementary control room

Sufficient instrumentation and control equipment is located, preferably at a single point which is physically and electrically separated from the control room, so that the reactor can be placed and maintained in a shut down state, residual heat removed, and the essential plant variables monitored should there be a loss of ability to perform these essential safety functions in the control room. Instrumentation and controls in the supplementary control room are in general a simplified version of the corresponding equipment in the main control room. Protection against internal and external events has, however, to be assured.

Automatic control

The automation of various safety actions is provided such that operator action is not necessary within a defined period of time from the onset of anticipated operational occurrences or design basis accidents and in addition, appropriate information is available to the operator to monitor the effect of the automatic actions**.**

Manual backup of the actuation of safety functions is also advisable; in this case, however, the number of safety system components common to both automatic and manual initiation should be kept to a minimum. It is advisable that such common components be limited to the actuation devices of the safety actuation system.

Manual initiation of safety actions may be used alone when it can be shown that acceptable limits will not be exceeded (see Section 2.3.2 of Ref. [14]).

Maintainability

The equipment is so designed that it facilitates surveillance and maintenance and, in case of failure, easy diagnosis and repair or replacement. Means provided for the maintenance of safety-related I&C systems is designed so that any effect on the safety of the plant is acceptable. Typical examples for such means are disconnection of one channel in a system with redundant channels and provisions for alternative manual actions.

To facilitate their maintenance, I&C systems, to the extent practicable, are located so as to minimize risks, in particular radiological doses, to operating personnel. Enough room is left surrounding the equipment to ensure that the maintenance staff can fulfil its task under normal working conditions. Attachment points are provided on nearby structures in order to make possible the installation of temporary supports for pieces of equipment to be maintained. Where practicable, equipment is not to be placed where there is a risk of high radiation level or where conditions of extreme temperature or humidity normally exist.

Alarms and communication systems

It has to be verified that appropriate visual or audible alarms be provided at suitable locations throughout the plant to warn on-site personnel and to enable them to take proper actions. Oral communications between the main control room, supplementary control points, technical support centre, emergency centre and other off-site emergency services are vital to safety, particularly under anticipated operational occurrences or accident conditions. Communications between such locations should be regarded as a highest category function and be provided with two, preferably diverse, communication links (e.g. self powered telephones, battery-operated telephones, speaking tubes, hand-held portable radios). These communication links should be routed in such a way that fires, electrical system failures and other applicable PIEs cannot incapacitate both systems simultaneously.

Spurious operation of the protection system

The primary requirement of the protection system should be to adequately carry out its specific protective task. However, spurious operation of this system should also be avoided also in order to eliminate unneeded stresses on the equipment. Too many spurious actuations may result from inadequate system characteristics or from inadequate set points. During the design review, the historical frequency of spurious actuations should be considered and evaluated.

Emergency control centre and related facilities

The following design requirements for the emergency control centre are also identified in Ref. [11]. The nuclear plant should have an on-site emergency control centre, separate from the plant control room and from the supplementary control room, to serve as a meeting point for emergency staff and as a centre for off-site communications. The emergency control centre design should include the following items:

– Important plant parameters such as reactor power, core temperatures, coolant system flows and temperatures, containment conditions, radioactivity release rates, meteorological conditions, etc. should be displayed.

– Reliable communication systems with the control room, supplementary control room, technical support centre, other important points in the plant, and off-site emergency organizations should be provided.

– Appropriate measures such as radiation monitoring, filtered ventilation, shielding, etc. should be included to protect occupants for a protracted time against hazards resulting from a severe accident.

– The emergency control centre should be provided with an appropriate backup power supply.

The plant should also have an on-site technical support centre near the control room as a meeting point for technical experts who provide plant management and technical support to operations personnel. The technical support centre should generally be designed to the same requirements as the emergency control centre.

Specific issues

Physical separation of instrument sensing lines for the reactor protection system (Ref. [4], para. IC 1)

One of the criteria commonly adopted for the plant protection system is that, the protection system equipment (for example interconnecting wiring, components, modules etc.) should be identified distinctively as being in the protection system. The identification should distinguish between redundant portions of the protection system".

In some cases, separation of redundant divisions of mechanical instrument sensing lines used for the protection system has not been carried out.

In some WWER reactors, some parts of the primary instrumentation use a common tap to the component to which it is connected. These parameters may be used in important control systems or in the protection system. Failure of the common tap will cause failure of all instruments connected to it and may result in actuation or non-actuation of one channel of the protection system. It is also a deviation from the Russian safety rule General Safety Regulations for NPPs.

A backfitting procedure, which makes it possible to weld additional taps to the vessel I&C nozzles has been developed in Russia (WWER-1000).

Inadequate electrical isolation of safety from non-safety related equipment ([4], para. IC 2)

Observations during SPDS (safety panel display system) evaluation tests found that for electrical transients below the maximum credible ones, a relatively high level of noise could pass through isolators. According to the amount of energy passed, damage of the safety component or an erroneous signal could occur. In one known case, a voltage transient generated by a power line fault caused a false indication of turbine trip which resulted in a spurious scram.

In one country (Republic of Korea) an appropriate error message is generated upon defective isolation and a diagnostic test is applied in order to isolate the cause of the error; fiber-optic devices are there used as isolators in this case. While this provision may not be sufficient to always solve the problem, it may how some degradation in isolator behaviour in a timely manner and so allow for early remedial actions. In the USA this problem has been the subject of Generic Issue N.142 since 1987.

A review of recorded failures does not reveal any incidents of system damage caused by isolation device challenge. However, based upon the potential design variations in future control systems resulting from application of computer technology, additional design and qualification test requirements for future plants are recommended.

Interference in I&C signal (Ref. [4], para. IC 3)

Electrical interference impacts between power cables or other components and instrumentation cables have been experienced in a number of plants. In one case a readjustment of the power cable eliminated the problem. In any case, additional grounding connections were installed. The original design of that plant did not consider the effects of

electromagnetic interference/radio frequency interference, heavy load switching transients and transients generated in the electrical and control systems due to external causes.

In many cases, the influence from power transients was considered already in the original design and instrument cables are fully separated from power cables and run on different cable trays; the possible impact of atmospheric phenomena like lightning was also considered .However, since the start of this decade (1990), when the problem of electrical interference was better focused, all important to safety equipment and the safe production of electricity have been in many plants checked regarding electromagnetic immunity and measures have been taken where the potential for the electromagnetic interference was high; the use of radio equipment is frequently forbidden in rooms (as I&C rooms) containing sensitive equipment. Industrial standards and regulatory documents have been produced on the subject.

I&C component reliability (Ref. [4], para. IC 4)

The I&C equipment of NPPs designed to previous standards is based on a technology that is known to present reliability problems: relay contact oxidation and low insulation resistance of wiring and of terminals are typical of this technology.

Operating experience has shown that I&C failure rate is relatively high and can cause power reduction. As the equipment gets older the amount of maintenance required to keep an acceptable status of I&C reliability will increase substantially. Moreover, old type components are not always offered by the market any more.

During a design review activity, pertinent operating experience should be carefully reviewed and, on the basis of this review, maintenance programmes should be evaluated. The market availability of replacement components should be considered. Upgrade and modernization of I&C should be recommended if necessary.

Lack of on-line testability (Ref. [4], para. IC 5)

The protection systems of some old plants do not provide for complete on-line testability (namely during plant operation). In practice, in many situations a combination of on-line partial tests with off-line test is adopted in such a way to adequately prove the operability of the system when required.

On-line tests by manual methods may cause errors and plant spurious trips. For this reason in some cases (e.g. France) automatic testers are implemented for periodic testing. In many countries (e.g. Slovakia) studies to replace existing RPS by new ones capable of self-testability are underway.

Reliability and safety basis for digital I&C conversions (Ref. [4], para. IC 6)

The adoption of digital technology in protection systems should be encouraged. In considering this issue during a design review, available standards and regulatory guidance documents should be taken into consideration.

Reliable ventilation of control room cabinets (Ref. [4], para. IC 7)

In the event of a failure in all the redundant trains of the HVAC systems in the control room the increase of temperature can lead in a short time to malfunctions of the electronic equipment in the control cabinets.

Failure of the redundant trains of the control room HVAC systems is not considered in the design basis.

However, probabilistic safety analyses usually do discover the criticality to risk of such systems. Not only control room cabinets are prone to this kind of common cause failure but also safety systems electric motor rooms and similar situations. Designers, if timely warned by the results of such an analysis or by some other means, have the possibility to take satisfactory remedial actions.

In many cases, remedial actions have been taken in operating plants. Examples are: the installation of independent closed-loop ventilation systems, the installation of humidifiers, the reduction of the normal control room temperature, procedures commanding the opening of the doors of all the control and protection cabinets to enable a natural ventilation to the electronic components and so on.

Human engineering of the control rooms (Ref. [4], para. IC 8)

This subject does not need an introduction demonstrating its importance after the many studies and other initiatives which followed the Three Mile Island accident. Yet many plants still exist where some elementary mistakes in control room arrangement are still present; examples are:

- The display of the plant is arranged by subsystems with an “active mimic” diagram of each subsystem shown with controls for pumps and valves in their appropriate functional position on the diagram; this type of organization has led to operational problems because the operator attention is focused on a specific item and he tends to disregard the interactions between the subsystems: an action that is taken at one point to solve one problem may create other problems in related subsystems;
- Indications of different types of process measurements, for example flow and pressure, are not distinguishable, except by the engraved legend: a more immediately understandable pictorial symbol should be provided;
- Control switches for pumps, valves, circuit breakers etc., all have handles of the same shape;
- The brilliance of the lights on these switches, indicating the operating status of the component, varies greatly, and in some cases it is difficult to determine which lamp is lit;
- Indicators that provide data that is important to the operator’s evaluation of the safety state of the plant are not differentiated from those used for normal operations;
- Some of the most valuable space on the control panel, that which is directly in front of the operator, is used for infrequent activities related to plant startup and surveillance testing.

Need for a safety parameter display system (Ref. [4], paras IC 9 and IC 12)

During a design review, the existence of a safety parameter display system (SPDS) has to be checked. This system is part of the information system important to safety which provides information for the safe operation of the plant during normal operation, anticipated transients and (in particular) during accidents.

The need for a dedicated SPDS was recognized after TMI and the majority of the plant owners world wide have retrofitted their plants with it. A variety of rather standardized designs is now available. When a technical support centre (TSC) for emergencies is present, the information displayed by the SPDS in the control room is also displayed in the TSC. Possible deficiencies in important information at some plants concern, by experience:

- Measuring scale of instruments extended well beyond the operating ranges (pressure, temperature, humidity, radiation field etc.);
- Qualified vessel level indication systems at PWRs;
- Adequate radiation monitoring of ventilation effluents.

Inadequacy of diagnostic systems for mechanical integrity (Ref. [4], paras IC 10 and IC 15)

A number of specific issues are referred to here, all concerned with early warning of possible loss of integrity of mechanical components:

- Primary pressure boundary leak detection
- Primary-to-secondary leak detection
- Component vibration monitoring and noise monitoring
- Monitoring of thermal loads in penetrations and nozzles.

In particular, it has to be noted that primary-to-secondary leak detection systems have had, in many cases, to be upgraded because the existing systems where not sensitive enough to timely detect steam generator tube degradations. Both volumetric activity of steam and activity of blowdown water may have to be measured. In a number of other cases, the measurement of the short-lived N-16 in the steam lines has given good results.

Reactor vessel head leak monitoring system (Ref. [4], para. IC 11)

This issue is rather specific to PWRs, where the vessel head hosts control rod drive mechanisms. Whatever solution is adopted for connection of the mechanisms to the vessel head, the possibility exists for leaks developing at junctions or even through cracks. Since the vessel head and the complex of control rod drive mechanisms are all enclosed in a thermal insulation composite envelope, the leak may stay undetected for a long time. Since in PWRs the primary water contains boric acid, external corrosion of mechanism housings and of vessel head may ensue.

This is not a theoretical possibility: in one case (USA) hundreds of kilograms of boric acid were found in the space between thermal insulation enclosure and vessel head during a refueling outage; in another (Russia), the vessel head had to be replaced.

Even if leakage and humidity monitoring systems are installed between head and external structure, experience indicates that they may not be sensitive enough.

During a design review, the existence of the requirement for suitable periodic tests of the pertinent leakage detection systems should be checked and the possible need for its upgrade studied.

Water chemistry control and monitoring equipment (primary and secondary)(Ref. [4], para. IC 13)

An accurate and possibly on-line chemical monitoring system is important to enable the operator to respond in time to deviations in the primary and secondary coolant water-chemical condition indices. Corrosion problems may arise from inadequacies in such a system. Chemical controls solely based on samples and laboratory analyses may not be timely enough to prevent damages due to deviations in coolant chemistry.

An on-line system should allow operators to:

- continuously control the coolant quality;
- make a timely diagnosis of the causes of water chemistry deviation during operation of the control system in on-line conditions with operator aid for elimination of the deviation causes;
- monitor automatically the corrosion conditions of structural materials;
- assess the residual service life of equipment components.

Adequacy of reactor vessel level instrumentation in BWRs (Ref. [4], para. IC 14)

In BWRs the water level in the vessel is a very important parameter for automatic actuation of critical safety functions (scram, reactor depressurization, emergency feedwater, ECCS). Water level measuring instruments generally use a reference leg which is constantly kept full of water through the action of an upper condensation chamber; the differential pressure between the bottom of the reference leg and the corresponding vessel position gives an indication of the vessel water level and serves as an input to the Reactor Protection System. Experience, however, indicates that incondensibles (radiolitic hydrogen + oxygen) may accumulate in the reference leg condensation chamber and dissolve in the reference leg water. This phenomenon, in case of decrease of reactor pressure, my cause gas bubbles to be formed in the reference leg: as a consequence, a higher level than real tends to be indicated by the instruments and a completely wrong picture of the situation is offered to the reactor protection system: one obvious consequence is the prevention of an automatic intervention of emergency water systems when needed. Various remedial actions have been proposed and adopted, such as:

- installation of recombination catalyzers in the condensation chamber in order to eliminate the incondensibles;
- installation of a diversified additional coolant level gauge;
- installation of a new type of degassing double condensation chamber;

- installation of a continuous reference leg backfill purging system which continuously injects water in the leg and purges any accumulated incondensibles (this system may, however, give rise to severe reactor transients in cases where the injection is made on the instrumentation side of a manual isolation valve and this valve is at a certain moment closed: reference leg overpressurization could occur indicating low-low water level in the vessel and initiating any emergency water injection available).

Establishment and surveillance of setpoints in instrumentation (Ref. [4], para. IC 16)

Many cases of wrong setpoints and of setpoint drift have been experienced. The methodology used in order to prevent this kind of situation should be carefully investigated during the design review. It is worth noting that a standard has been prepared in this connection by the Instrument Society of America (Draft F to ISA S67.04), which has been adopted by NRC.

Need for effective off-site communications in the emergency control centre ([4], para. EP 1)

As a result of TMI-2 accident, the need was recognized to substantially improve the ability to acquire data on plant conditions during emergency. Various schemes are implemented, whose description can be found in the references.

Need for technical support centre (Ref. [4], para. EP 3)

An established international practice calls for the availability of a room where current plant data and status are shown in order to enable technical experts to support the operators during the management of an event or accident. The room is separated from the control room. Various adopted solutions are described in the references.

Control room habitability (Ref. [4], para. ES 7)

Reviews of a number of plants have detected defects and deviations from present practice in control room habitability systems. Deficiencies in maintenance and testing, in design and installation and in availability of personnel knowledgeable in nuclear air-cleaning technology were detected.

Protection of personnel should be guaranteed in case of contamination of incoming air by radioactive and toxic substances. As a consequence, it should be possible to isolate the control room ventilation system from the main ventilation system. The emergency control room should also have a separate ventilation system. Various upgrades of the pertinent systems have been implemented in many plants.

Reliability of instrument air systems (Ref. [4], para. ES 8)

In a number of cases the instrument air system is not classified as a safety system since the fail safe principle is applied in safety functions dependent on its availability. However, a number of analyses have shown that the degradation of instrument air system can lead to failures in safety related systems, including possible common mode failures. Various remedial actions are possible at interested plants.

I.2.5. Emergency power systems

Requirements and review guidelines

The basic design function of the emergency power systems (EPS) is to provide the plant with necessary power in all relevant conditions within the design basis so that systems can perform their necessary safety functions and maintain the plant in a safe state.

- The EPS should provide power to safety systems for all anticipated operational occurrences and accident conditions , including any PIE coincidental with the loss of off-site power, to ensure radioactive releases are within acceptable limits.
- A primary design requirement for the EPS is high reliability. The system should be designed with backup electrical power, redundancy, diversity, separation, and consider single failure criterion commensurate with the functions of the specific component.
- If analysis shows the electrical grid supplying the plant has poor stability, design measures for improving stability should be considered.
- The most reliable transmission line available should supply power to the EPS.
- Appropriate breaker protection must be provided to isolate the plant from the grid during faults.
- Common cause failures should be accounted for in the design.
- The design bases should include items listed in Section 313 of Ref. [15].
- The EPS should be divided into independent, redundant divisions. Support such as room ventilation, cooling water, lubrication etc., should be assigned to the same EPS division as the safety system it is supporting.
- Equipment should be provided in the control room to monitor and control the EPS.
- Each reactor in a multi-reactor plant should have separate and independent EPS.
- For components that require an individual power supply, i.e. remote radiological monitors and meteorological equipment, communication systems, emergency lighting, etc., the power supply should be designed with appropriate capability, reliability, and testability.
- Appropriate grounding systems should be provided for lightening protection, system protection, and component protection.

AC power system and stand-by power system

- The AC power system should supply loads that allow a certain interruption of power supply during normal operation, anticipated operational occurrences, and accident conditions.
- Buses should be automatically disconnected from their power source if unacceptable voltage or frequency is detected.
- A stand-by electrical power system consisting of a fully independent electrical generating unit should be provided. All auxiliaries required to start and operate the unit, such as compressed air, stored fuel, oil and water, should be independently provided.

- The stand-by power system should have sufficient capacity under anticipated operational occurrences and accident conditions to start and supply all required safety loads. The design should account for necessary starting reliability, time required to start and accept loads, appropriate performance characteristics, adequate step load capability, and sufficient operability duration.
- The stand-by power system should not be used to supply the EPS on a continuous basis. Use of the stand-by system should be limited to the time necessary to recover the normal power supplies.
- When the stand-by power system is called upon to supply power to an EPS bus, that bus should be automatically disconnected from its normal supply.
- Means should be provided to periodically start and connect the stand-by system for test during normal plant operation.

DC power system

- The DC power system should supply, without interruption, DC loads, including control, monitoring and protection, switching, and auxiliary power, during normal operation, anticipated operational occurrences, and accident conditions.
- The DC system should normally be supplied from the AC system via battery chargers.
- A battery system should be provided to supply the DC system without interruption in case of loss of AC power to the battery charger.
- The battery should be maintained in a fully charged condition during normal operation.
- The battery charger should be capable of charging a fully discharged battery within an acceptable time frame while at the same time supplying the largest combined DC loads.
- Taking into account the most severe conditions expected (including station blackout), the battery should meet all required load demands and conditions until the stand-by power supply system can meet load demands.

Non-interruptible power system

- If safety loads require continuous AC power, such as protection and control systems, a non-interruptible power supply should be provided for these loads.
- The non-interruptible power supply should be divided into redundant divisions.
- Each division should consist of a supply from the DC power system, a AC–DC converter, and a distribution system.
- A backup supply from the AC bus of the same division with an automatic switchover device should also be provided.
- The non-interruptible power supply design should take into account the characteristics and requirements of the loads and interactions between the loads themselves.

Distribution system

- Each distribution system should have sufficient capability to supply the required loads under all operating conditions and withstand the maximum credible overcurrent, under

plant fault and transient conditions, without damage or adverse effect on any of its components.

- The distribution system should be capable of switching loads and power supplies as needed.
- All main and branch circuits should be protected by overload, earth fault, short circuit, and other appropriate protective devices which should safeguard the main and branch circuits, buses, and cables from damage.
- Distribution system protective devices should be located in appropriate enclosures to protect them against the effects of PIEs.
- Distribution system protective devices should be co-ordinated so that only the faulted branch of the distribution system is isolated.
- Automatic connection between redundant divisions of the EPS should be avoided.

Controls

- Controls should normally be automatic, but backup manual controls should also be provided.
- Appropriate loads and all other power supplies should be automatically disconnected from the distribution system when the stand-by power system is required. A load sequencing program should automatically reconnect required loads to the distribution system after the stand-by system is connected.
- When the stand-by power distribution system is required, it should start and connect to the distribution system automatically.
- The EPS should automatically be synchronized to the normal power supply when the normal supply is being reinstated.
- Controls and redundant circuits for each division should be physically separated and electrically isolated from each other.

Buses and cables

- Buses and cables should be selected, rated, and qualified for their service and for environmental conditions, including post LOCA conditions for in-containment components, taking into account cumulative radiation effects and ageing.
- Buses and cables should be sufficiently fire retardant to prevent propagation of fires.
- Buses and cables should be rated for voltage, current, and temperature taking into account anticipated operational occurrences and accident conditions.
- Buses, cable trays, and their supports should be designed to withstand expected mechanical loads.
- Connectors, terminations, and splices should be selected and qualified for their applications and the in-service conditions expected throughout their design life.

– Control and instrumentation, low voltage, medium voltage, and high voltage cables should be physically separated or separated by barriers to prevent unacceptable influence on each other.

– Buses, cables, and wires for each division should be physically separated and electrically isolated from each other to prevent common cause failures. In addition, they should be protected from mechanical system, equipment, and structural failures, and from internal flooding such that a failure does not affect circuits or equipment of the other division.

– Containment electrical penetration assemblies should be rated and qualified for the expected service and environmental conditions expected throughout their design life. In addition, they should have the same physical separation and electrical isolations the cables to which they are connected.

Mechanical equipment

Mechanical Equipment includes all non-electrical equipment and components required for the EPS to fulfil its safety functions that generate electricity, pump water, compress air, position valves, operate instruments and controls, etc. Typical mechanical EPS equipment includes steam turbines, gas turbines, hydro turbines, diesel engines, and compressed gas vessels.

– Storage reservoirs for mechanical equipment should have a sufficient capacity of 'fuel' (e.g. pressurized nitrogen, pressurized air, fuel oil, etc.) so that the prime mover can operate for the time period needed to meet safety requirements.

– Automatic connection between redundant divisions of mechanical equipment should be avoided.

– Controls should be automatic, but backup manual controls should also be provided. Automatic controls should include switching to the emergency mode when required if being utilized in another mode, bypassing of normal operation protective devices when switching to emergency mode, and start of stand-by units.

– Sufficient mechanical equipment should be provided for complete control of each division of the EPS. The equipment and required instruments and controls should be physically separated and isolated by division.

Additional design requirements for the emergency power systems are identified in [1, 15, 11].

Specific issues

The following issues have been identified and should be reviewed and considered as appropriate while performing the design review. These issues are discussed in detail in [4].

Reliability of off-site power supply (Ref. [4], para. ES 1)

Off-site power supplies are required to be available to have sufficient capacity and capability to ensure that the fuel and reactor boundary are maintained within specified acceptable limits. The primary issues with off-site power source are: the reliability of the off-site power source as the preferred source, vulnerability of equipment to degraded voltage, and adequate design interfaces of the off-site and on-site power sources. External events could be a major source of off-site power disruption.

Diesel generator reliability (Ref. [4], para. ES 2)

Reliable emergency diesel generators (EDG) are required to provide power to all necessary safety systems in events which result in a loss of off-site power. The reliability of the starting capability of the EDGs has a high level of importance to reduce the core damage frequency. Therefore, improving the starting and running reliability of the EDGs will reduce the probability of events which could escalate into a core melt accident.

Scope of systems supplied by emergency on-site power (Ref. [4], para. ES 3)

Safety systems that are required to cope with design basis accidents are required to be powered by EDGs in the event of a loss of off-site power. WWER reactors have a significantly reduced number of systems that rely on the EDGs for emergency power. For those facilities that do not have EDG backup for all required safety related systems a thorough review of the safety analysis should be performed to determine how the plant intends to cope with issues such as: primary circuit makeup, auxiliary feedwater, control rod drive cooling, plant communications, pumping systems for filling the EDGs and the radiation control panel.

Breaker co-ordination to protect loads (Ref. [4], para. ES 4)

Circuit breaker co-ordination can limit the degradation of safety related systems during a fault condition on a system component. without breaker co-ordination, an electrical fault on one component, such as a motor or motor operated valve, could result in the loss of an entire motor control centre or switchgear bus. Generally the load breaker supplying component power will trip before the feeder breaker tips for the entire switchgear or bus.

Vulnerability of swingbus configurations (Ref. [4], para. ES 5)

Current international standards for power supply system design require physical separation between redundant safety functions. The use of swingbus electrical power supply configurations cannot provide for physical separation and, therefore, these designs do not meet international standards. Some plants in Japan, Sweden and the USA have swingbus configurations which have been modified to ensure their acceptability for physical separation.

Reliability of emergency DC supplies (Ref. [4], para. ES 6)

Batteries are the ultimate energy source in a nuclear power plant and are essential for station black out accident scenarios, therefore, they have to have adequate capacity and be highly reliable. International standards require significantly more discharge time than the 30 minutes that may be designed into some plants. In such cases, a thorough review of the safety analysis should be performed to determine how the plant intends to perform accident management actions after its discharge time has been exceeded.

Other battery issues to consider are: lack of a battery circuit monitor and ability of the battery system to withstand loads from external events.

Common cause failure of switchyard breakers

Nuclear power plant switchyards are normally protected against loss due to inadvertent actuation of fire protection trips. At one plant a small grass fire in the switchyard caused the

tripping of protective breakers. Therefore, the housekeeping in the switchyard area has to be maintained to ensure that such a common cause failure can be avoided.

I.2.6. Fuel handling and storage systems

Requirements and guidelines

A complete list of requirements is included in Ref. [11]. The unirradiated fuel storage facility at a NPP has to satisfy the following two main requirements:

- to prevent criticality even in case of accidental addition of a moderating agent (e.g. water or water spray);
- to allow for inspection of stored fuel elements and control rods.

The prevention of criticality is usually obtained by geometrically safe configurations or, more frequently, by the use of neutron absorbing material for the construction of the fuel rack structure. The irradiated fuel storage facility should satisfy the following safety requirements:

- To prevent criticality by physical means or engineering provisions, preferably by the use of geometrically safe configurations or by the use of neutron absorbing materials for the construction of the rack structure, even in case of optimum moderation;
- To provide for adequate heat removal in normal and accident conditions and, in particular, to be protected against design basis loss of cooling accidents;
- To permit inspection and testing of stored material and components important to safety;
- To prevent dropping of fuel during transit;
- To prevent unacceptable handling stresses on the fuel elements or fuel assemblies;
- To prevent the fall of heavy objects on stored fuel;
- To permit safe storage of defective fuel;
- To take adequate care of radiation protection hazards;
- To have means for controlling water contamination and water leaks;
- To have containment provisions such that an accidental damage to one or more fuel elements does nor generate undue hazard to population; normal operating conditions and special conditions during fuel or fuel cask movements have to be considered.

The stress on the assumption of optimum moderating conditions in the above listed requirements derives from the fact that the most critical condition for normal fuel arrangements is not the one in which the fuel storage is completely submerged by pure water: an optimum water “density” (water spray density or water level) does, indeed, usually exist. The reviewer has, therefore, to check the design assumptions, the status of the criticality prevention devices and the possibility of various forms and amounts of moderator in the fuel storage area.

Protection against the possible fall of heavy objects (fuel elements, fuel cask etc.) usually include a careful study of the movement path, the use of redundant brakes and crane cables, the physical limitation of the movement height or range, the use of load measuring devices and alarms. Possibilities of accidental loss of coolant from spent fuel pool should be reviewed.

Specific issues

The following fuel handling and storage systems issues have been identified and should be reviewed and considered while performing the design review: each of these issues is discussed in detail in Ref. [4].

Degradation of boron plates in fuel storage pools (Ref. [4] para. FS 1)

Two types of borated plates are used for fuel racks:

- Boraflex plates containing silica (USA) which may lose silica and boron carbide under gamma irradiation;
- Boral (France) plates which do not lose boron but swell upon irradiation.

The design review should check which kind of plate is used and which operational provision (periodic controls) are in place to guarantee against unacceptable degradation.

Potential for fuel pool drainage (Ref. [4], para. FS 2).

Operating experience shows that the accidental drainage of a spent fuel pool is a real danger in various situations. Inadequate maintenance practices, RHR misalignment, earthquake, stainless steel liner leaks, failure of piping systems, siphoning from permanent or temporary pipes or hoses, refueling water cavity seal failure are all real possibilities. A design review should consider this problem in the light of the applicable operating experience on the specific plant and elsewhere.

Damage to fuel during handling (Ref. [4], para. FS 3)

Mechanical failures of fuel grapples and of lifting devices or improper operation of such equipment have happened at times, although with no important consequences. Such possibilities should be considered in the review.

Appendix II

SAMPLE LIST OF SYSTEMS WITH A POTENTIAL IMPACT ON SAFETY

The following abbreviations are used to provide a direct correspondence between the list of nuclear power plant systems (below) and the system groups in Appendix I:

RC	reactor core
GL	general
IH	internal hazards
FS	fuel storage
SS	Safety systems
CI	Component integrity
RCS	reactor cooling system and associated systems
CS	containment system and associated systems
IC	instrumentation, control and protection systems
EPS	emergency power systems
FH	fuel handling and storage systems
ES	electrical and other support systems
EP	emergency preparedness (incl. physical protection)
PC	primary circuit and associated systems

List of systems

Reactor coolant system (RCS)
Emergency core cooling system (RCS)
Residual heat removal system (RCS)
Chemical and inventory control system (RCS)
Steam system (RCS)
Feedwater system (RCS)
Auxiliary feedwater system (RCS)
Condensate system (RCS)
Service water system (RCS)
Component cooling water system (RCS)
Containment cooling water system (CS)
Nuclear instrumentation systems (I&C/P)
Reactor protection system (I&C/P)
Control rod drive systems (RC)
Reactor core (RC)
Steam generator pressure and level control (I&C/P)
Heating, ventilation systems (I&C/P)
Air cooling systems (personnel and equipment) (I&C/P)
Containment systems (CS)
Containment combustible gas control system (CS)
Instrumentation and controls (I&C/P)
AC electrical systems (EPS)
DC electrical systems (EPS)
Emergency diesel generator systems (EPS)
Communications systems (EPS)
Emergency lighting system (EPS)

Emergency control room (I&C/P)
Turbine systems (EPS)
Electrical generator and associated cooling systems (EPS)
Pressurizer relief discharge systems (RCS)
Control room habitability system (I&C/P)
Fuel handling systems (FH)
Spent fuel storage systems (FH)
Compressed air systems (I&C/P)
Equipment and floor drain systems (RCS)
Fire protection systems (covered by other IAEA publications)
Waste management systems (liquid, gas & solid) (covered by other IAEA publications)
Process and effluent radiological monitoring and sampling systems (I&C/P)
Area and airborne radiation alarm systems (I&C/P)
Seismic instrumentation systems (covered by other IAEA publications)
Ultimate heat sink (RCS)
Leakage monitoring systems for water and steam (I&C/P)

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Code on the Safety of Nuclear Power Plants: Design, Safety Series No. 50-C-D (Rev.1), IAEA, Vienna (1988).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Quality Assurance for Safety in Nuclear Power Plants and other Nuclear Installations: Code and Safety Guides Q1–Q14, Safety Series No. 50-C/SG-Q, IAEA, Vienna (1996).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Culture: A Safety Report, Safety Series No. 75-INSAG-4, IAEA, Vienna (1991).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Generic Safety Issues for Nuclear Power Plants with Light Water Reactors and Measures taken for their Resolution, IAEA-TECDOC-1044, Vienna (1998).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Defence in Depth in Nuclear Safety, Safety Series No. 75-INSAG-10, IAEA, Vienna (1996).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of the Reactor Containment Systems in Nuclear Power Plants: A Safety Guide, Safety Series No. 50-SG-D12, IAEA, Vienna (1985).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Design for Reactor Core Safety in Nuclear Power Plants: A Safety Guide, Safety Series No. 50-SG-D14, IAEA, Vienna (1986).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Issues and their Ranking for WWER-1000 Model 230 Nuclear Power Plants, IAEA-EBP-WWER-05, Vienna (1996).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, General Design Safety Principles for Nuclear Power Plants: A Safety Guide, Safety Series No. 50-SG-D11, IAEA, Vienna (1986).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Reactor Coolant and Associated Systems in Nuclear Power Plants: A Safety Guide, Safety Series No. 50-SG-D13, IAEA, Vienna (1986).

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Fuel Handling and Storage Systems in Nuclear Power Plants: A Safety Guide, Safety Series No. 50-SG-D10, IAEA, Vienna (1984).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Related Instrumentation and Control Systems for Nuclear Power Plants: A Safety Guide, Safety Series No. 50-SG-D8, IAEA, Vienna (1984).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Emergency Power Systems at Nuclear Power Plants: A Safety Guide, Safety Series No. 50-SG-D7 (Rev.1), IAEA, Vienna (1991).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Fire Protection in Nuclear Power Plants: A Safety Guide, Safety Series No. 50-SG-D2 (Rev.1), IAEA, Vienna (1992).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Ultimate Heat Sink and Directly Associated Heat Transport Systems for Nuclear Power Plants: A Safety Guide, Safety Series No. 50-SG-D6, IAEA, Vienna (1981).

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Protection Systems and Related Features in Nuclear Power Plants: A Safety Guide, Safety Series No. 50-SG-D3, IAEA, Vienna (1980).

CONTRIBUTORS TO DRAFTING AND REVIEW

Cleary, J.	Pacific Northwest National Laboratory, Richland, Washington, United States of America
Couch, D.	Pacific Northwest National Laboratory, Richland, Washington, United States of America
Petrangeli, G.	ANPA, Rome, Italy
Guerpinar, A.	International Atomic Energy Agency

Consultants Meetings

Vienna, Austria: 30 June–4 July 1997,
1–5 December 1997, 4–8 May 1998