ETSON

EUROPEAN
TECHNICAL SAFETY
ORGANISATIONS
NETWORK

TECHNICAL SAFETY ASSESSMENT GUIDE

SAFETY FLUID SYSTEMS

ETSON/2015-001 March 2015

FOREWORD

Since the beginning of EUROSAFE initiative (1999), IRSN, GRS and Bel V (former AVN) have pursued the objective to advance the harmonisation of nuclear safety in Europe by comparing their safety assessment methodologies. Based on a long standing experience of more than 40 years, in spite of different national nuclear safety regulatory backgrounds, they have developed practical methods to perform safety assessments that presented sufficient similarities to encourage them to persevere in building a collection of common best practices. The first version of their common Safety Assessment Guide was thus approved in 2004.

The general Safety Assessment Guide (SAG), and its specialized guides, the Technical Safety Assessment Guides (TSAG), have been written by the members of the European Technical Safety Organisations Network with progressive improvements brought by the new members of ETSON.

The SAG provides general principles such as safety assessment objectives or transparency and traceability of the process, and describes the general process for performing the safety assessment of nuclear installations. The goal of this SAG is to set down the harmonized methodology applied by ETSON organisations to ensure a common quality of safety assessment and to develop higher confidence in delivered safety assessments.

The TSAG series consists of specialized guides dedicated to specific technical domains of importance to the safety of nuclear installations. They provide an overview of the available practical knowledge gained by Technical Safety Organisations (TSO) in conducting safety assessments covering these main technical issues (use of operating experience feedback, assessment of human and organisational factors, prevention of severe accidents, probabilistic safety assessment, etc.).

Each guide published by ETSON is updated according to the extension of experience gained as well as to the new requirements in nuclear safety.

The Technical Safety Assessment Guides present the common views and practices of ETSON members:

- Bel V - Belgium
- GRS - Germany
- IRSN - France
- VTT - Finland
- CV Rez - Czech Republic
- LEI - Lithuania
- VUJE - Slovakia
- PSI - Switzerland
- JSI - Slovenia
- INRNE-BAS - Bulgaria

With the contribution of ETSON associated members:

- SSTC - Ukraine
- NRA - Japan
- SEC NRS - Russia

CONTENTS

1 SCOPE

This Technical Safety Assessment Guide (TSAG) is intended for/addressed to engineers working in Technical Safety Organisations related to safety authorities regarding nuclear installations and describes the process of performing a safety assessment concerning a (part of a) safety fluid system.

This TSAG has the purpose of addressing safety assessments of systems for both new and existing reactors.

When a system is being mentioned in this guide, all redundancies of that system are considered.

A safety fluid system is defined as starting from its source and ending at the injection point. Closed loop systems are considered entirely.

The TSAG will take into consideration only fluid systems necessary for design basis accidents (Defense in Depth - DiD level 3 for existing plants or 3a for new plants - see Report "Safety of new NPP designs"; WENRA; March 2013). All safety related auxiliary fluid systems are also included in the scope of this TSAG. Ventilation systems are included as well; these systems share a lot of similarities and make use of the same principles during the assessment process. Fluid systems required in DBA concerning the spent fuel pool are addressed as well.

I&C and electrical systems are not included; they are out of scope for this guide. Systems that are considered as exclusively taking part in Radioactive Waste Management are excluded.

2 INTRODUCTION

Reviewing and assessing the various safety related issues raised by nuclear activities to determine whether the activities comply with the applicable safety objectives and requirements is one of the principal prerequisites to achieve and maintain a high level of safety in nuclear activities.

The purpose of this guide is to provide guidance to Technical Safety Organisations (TSO) on reviewing and assessing safety questions raised in nuclear activities with regard to safety fluid systems.

The principal objective of a safety assessment is to determine whether the operator's submissions demonstrate compliance with the stipulated safety objectives or requirements.

3 DEFINITIONS

Safety system

System important to safety, provided to ensure the safe shutdown of the reactor or the residual heat removal from the core, or to limit the consequences of anticipated operational occurrences and design basis accidents. Components of safety systems may be provided solely to perform safety functions or may perform safety functions in some plant operational states and non-safety functions in other operational states.

Safety function

Combined action of a set of technical features to perform a certain task during a certain plant condition.

Active failure

An active failure is a malfunction, excluding passive failures, of a component that relies on mechanical movement to complete its intended function upon demand.

Passive failure

A passive failure is a failure of a component to maintain its structural integrity or the blockage of a process flow path.

4 THE SAFETY ASSESSMENT PROCESS OF SYSTEMS

4.1 PREPARATORY ACTIONS

This paragraph describes which preparatory actions should be performed before starting a safety assessment related to a fluid system.

After the preparatory actions, enough information should have been gathered to be able to assess the validity and completeness of the submitted file and the efficacy/efficiency/effectiveness of safety provisions made by the licensee considering any safety fluid system.

4.1.1 COMPLETENESS OF THE APPLICATION FILE/VERIFICATION OF THE APPLICATION FILE

The first step to be executed, when receiving such an application file, is the verification whether the provided information is complete, including references and graphics. The safety issues discussed in the application file should be clearly documented. If necessary, after the preparatory actions are executed, a meeting can be scheduled requesting confirmation of information or clarification. If the application file is considered to be complete, the next step of preparatory actions can be started: comprehension of the system.

4.1.2 COMPREHENSION OF THE SYSTEM

Whoever is executing the assessment should comprehend every aspect of the considered system. This can be done by gathering information from the Safety Analysis Report of the installation and the Technical Specifications of the system, as well as procedures, Piping & Instrumentation Diagrams and other documents. Information about prior assessments and experience feedback linked to the concerned system should be accessible.

4.1.3 IDENTIFICATION OF THE REGULATORY REQUIREMENTS, GENERAL SAFETY OBJECTIVES AND CODES/STANDARDS APPLICABLE TO THE SYSTEM

The regulatory requirements should be identified considering every part of the safety

fluid system including the safety related auxiliary systems.

The most recent applicable regulation is to be used. Gathering information concerning the history of regulatory requirements can prove to be useful. For units built before the issue of new regulatory requirements, the new requirements (or an equivalent) should be considered as a target objective.

In case of lack of national regulations, consulting internationally accepted regulatory requirements (IAEA, WENRA, etc.) may provide valuable guidance.

4.1.4
MILESTONES OF PAST ASSESSMENTS

Assessments previously performed on the same system or similar systems are to be taken into consideration. The recommendations made as a result of previous safety assessments should be studied as well as the resulting consequences and actions for the designer/operator.

Also, assessments performed for other similar NPP's may be taken into consideration to ensure consistent positions amongst the NPP's. Attention has to be paid to the existing positions for similar installations with similar systems subjected to the same regulations. If the executed safety assessment shows results that are different from former safety assessment, positions shall be justified.

4.2 PERFORMING THE SAFETY ASSESSMENT

4.2.1
METHODS FOR THE ANALYSIS

The safety demonstration of the design of systems mainly relies on deterministic studies. The functional and design requirements of the safety system and the associated design features are defined on the basis of all postulated plant conditions in which the safety system is required.

The safety assessment of the safety system is to provide the statement that the system has sufficient capability to fulfill its safety function in all the postulated situations.

Other cross-cutting issues should also be considered in the safety assessment of the system design, as they may generate expectations for the system design and operation:

- the insights of Probabilistic Safety Analyses (PSA), to complement the conventional deterministic studies (see §4.2.6.1);
- the operating experience analysis gained from the system or similar systems on existing installations (see §4.2.6.2).

The safety assessment should also take into account:

- design rules applicable to similar installations;
- the available current knowledge;
- possible research developments (e.g.: research activities on sumps clogging, etc.) notably in case of introduction of innovative design or features.

4.2.2
ROLE OF THE SYSTEM

A system can perform different functions as a whole, and also different components of the system may perform different functions. The reviewer shall clearly identify the different functions executed by the system or its different components.

4.2.2.1
Safety functions (directly or indirectly requiring the system)

A safety function can be performed by one or several systems. A safety system can

perform one or more safety functions. Some are more important than others. The different functions of the safety fluid system should be identified and if possible ranked by their safety significance.

Some functions are not safety related; it is recommended to mention them as well and keep them in mind, for reasons of completeness. The safety function of a system determines among others the safety classification (see §4.2.4), design requirements, required qualification, etc. If a system has more than one safety function, the system should be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety function that demands the highest classification.

The conditions that the system may have to face during any design basis accident have to be determined and analyzed. In order to fulfill its safety function, the system must be protected and/or qualified against those conditions. The conditions, to be taken into account, should be defined in regulatory documents.

A system must be able to fulfill its safety function in anticipated operational occurrences and design basis accidents (up to DiD level 3).

The compliance of the system to applicable regulations must be demonstrated by the licensee and verified by the TSO.

4.2.2.2
Field of application (Design basis accidents requiring the system)

After determining the different safety functions, one should investigate the field of application of each function and in which phase they intervene to maintain safe operation or to bring the nuclear power plant to safe state. The design basis accidents define the safety functions and their field of application. As mentioned in §3, only systems necessary to cope with design basis accidents are considered here.

As mentioned in §4.2.2.1, some safety systems perform also non-safety functions, when these are mentioned they should be complemented with their field of application for informational purposes. System characteristics related to non-safety functions may not endanger the fulfillment of a safety function.

4.2.2.3
The system regarding hazards

Assessment should be made concerning the function of the system regarding hazards. One should determine if the system has a safety role during the occurrence of a hazard.

The protection of a system against hazards is treated in §4.2.5.5.

4.2.3
FUNCTIONAL REQUIREMENTS

The assessment shall identify the functional requirements of the system. Functional requirements correspond to aptitudes/ capabilities that must be fulfilled by the system:

- the safety functions performed by the system;
- the situations during which these functions have to be performed;
- the required performances of the system.

4.2.4
CLASSIFICATION OF SAFETY FLUID SYSTEMS

The safety of a nuclear power plant is based on a reliable operation of both operational and safety-significant structures, systems and components (SSC).

The assessment shall check that the SSC are well-classified on the basis of their safety significance.

The safety significance is mainly determined by the system functions in normal operation, abnormal operation (e.g. transients AOO)

and design basis accidents. This means the functions performed by the equipment in the defence in depth concept. Safety significance is also attached to equipment that performs no safety tasks but whose failure can lead to damage of equipment, carrying out safety-related tasks in the defence in depth concept.

The reliability of SSC is substantially determined by a number of defined properties (redundancy, diversity, maintenance, testing, power supply, seismic classification, environmental conditions) and quality features. SSC that are in the same safety classes meet the same specifications and quality characteristics.

Safety systems are designed, manufactured, installed and then subsequently commissioned, operated and maintained to a level of quality commensurate with their classification.

Concerning classification, the following items shall be assessed by the reviewer:

- For classification of systems and components the following criteria could be taken into account:

  (i) the level of defence to which the system or component belongs;

  (ii) the consequence of failing to deliver the safety function;

  (iii) the extent to which the function is required, either directly or indirectly, to prevent, protect against or mitigate the consequences of initiating faults;

  (iv) the potential for a functional failure to initiate a fault or exacerbate the consequences of an existing fault;

  (v) likelihood that the function will be called upon.

- The classification shall be based primarily on deterministic criteria. Probabilistic methods might be applied complementary.

- The classification shall also take into account the applicable conventional and nuclear regulations for design and operation.

- Equipment that performs multiple functions of different safety classes shall be classified consistent with the function of the highest class (i.e. the one requiring the most conservative engineering design rules).

- Specified characteristics of a system or component established following the classification shall be ensured over the lifetime of the system or component.

- The classification of all safety-related equipment shall be summarized in the Safety Analysis Report or in a specific document.

- The classification shall be checked after system or plant modifications, or new safety analysis resulting in a new safety significance of a system or component.

- It shall be checked whether the redundancy of the system is consistent with the requirements related to its classification.

- It shall be checked whether the redundancy or the diversification of the system electrical power supply (diesel generators, batteries, etc.) is consistent with the requirements related to its classification.

- It shall be checked whether the system design responds to seismic requirements that are consistent with the system's classification

- Auxiliary systems for main systems should be classified according to their importance for the function of the main system.

- Failures in a system of lower class may not have a negative impact on systems of higher class.

4.2.5
DESIGN REQUIREMENTS

4.2.5.1
Single failure criterion

SINGLE FAILURE AND SINGLE FAILURE CRITERION DEFINITIONS

The single failure criterion (SFC) is a deterministic criterion in the safety system analysis. For a system on which the SFC is applied, it shall be checked that the system is capable of performing its function in the presence of any postulated single failure of one of its components.

SFC applies to each safety system or support systems needed to operate in DBA.

ASSUMPTIONS FOR THE APPLICATION OF SFC TO SAFETY SYSTEMS (LEVEL 3 OF DEFENCE IN DEPTH)

Method:

- the compliance of a system with the single failure criterion shall be examined by successively applying to each component of the system or of auxiliary systems necessary for its operation a single failure and by checking, in each case, that the corresponding safety function is ensured;
- the assessment must verify that the single failure considered is independent of any other failures directly caused by the operating conditions under which the system must ensure its function. In particular, all failures resulting directly from an initiating event shall be considered as being part of the initiating event;
- furthermore, the compliance with the single failure criterion shall be verified for each of the operating conditions. This must be fully justified in the application file.

Active/passive failure:

- for mechanical safety systems conveying a fluid and fulfilling a safety function in a short term, an active single failure (failure of an active component) should be postulated;
- for mechanical systems conveying a fluid and fulfilling a safety mission in the long term, an active or a passive single failure should be postulated (only the most penalizing one). Passive failures should be defined by analysis of realistic failure mechanisms of the components, considering the different operating conditions and possible leakage;.
- it should be checked that the most penalizing failure is taken into account by the designer/operator. This must be fully justified in the application file.

Assumptions for passive failure (if postulated):

- the passive failure is considered in the long term period, usually after 24h following the occurrence of the postulated initiating event. For safety injection and containment heat removal systems, it may be postulated at the time of the switchover to the recirculation mode. In order to verify the robustness of the installation, sensitivity studies could be required to check that there would be no "cliff-edge effects" in case of a passive single failure in the short term (before 24h).

Exceptions to SFC:

- it can be acceptable that some single failures can be excluded when applying the single failure criterion for the design of systems if the exclusions are clearly justified by appropriate methods in connection with precise design and operation provisions, taking into account operational experience. Justifications should include an analysis of the consequences of the failure, using realistic assumptions.

IMPACT OF SFC AND MAINTENANCE ON THE REDUNDANCY OF THE SYSTEM

The effectiveness of the system redundancy may be reduced by random or intentional unavailabilities of the system.

For some reactors, regulations require (n+2) redundancy for the safety systems (where n is

the number of trains required to perform the safety function) in order to take into account the unavailability (e.g. for maintenance) of one train in addition to the application of SFC to another train. In such cases, it shall be checked that the system design fulfils this requirement.

The solution with (n+1) redundancy generates particular vigilance, constraints on the allowable duration of contingent unavailability and stringent limitations on scheduled unavailability of one redundancy during operating periods where the system is required for safety.

If the maintenance operations of the safety system are scheduled out of the periods when the system is required or if the nature of the preventive maintenance is such that the system can be restored to an operational state in due time which enables the necessary safety function in case of demand mode, then it is acceptable that the unavailability due to maintenance is not cumulated to the SFC.

If maintenance or testing operations are foreseen when the system is required to be available as a safety system, redundancy (n+1) is suitable if it can be demonstrated that another system is able to ensure adequate functional redundancy during these periods or that the duration of unavailability is short enough not to impair significantly the plant safety level or the system is automatically brought into operation mode.

4.2.5.2
System Diversity

It shall be checked that, as far as possible, the risk of common cause failures (CCF) is minimized. Specific attention shall be paid on systems ensuring safety functions for the most frequent initiators.

The risk of CCF (due to the design, the manufacturing, the maintenance, etc.) on identical or similar equipments within a system or in all systems performing the same safety function shall be examined to check the need for diversifying equipments.

Probabilistic safety analyses may be used to determine the adequate balance between redundancy and diversification.

4.2.5.3
Electrical supplies

Depending on their safety classification, the components of the system may need emergency power supply in case of loss of off-site power (LOOP) or station blackout (SBO).

The fail safe position of equipment in case of loss of electrical supply shall be assessed.

4.2.5.4
Equipment qualification

The objective of equipment qualification is to demonstrate the ability of the equipment to operate in all the postulated situations it is required and in the environmental conditions it is supposed to operate.

The assessment should focus on:

- the general qualification approach that will be used for all types of equipment (mechanical, electrical, etc.) inside and outside the reactor building;
- the identification of the conditions in which the system could operate: radiation, pressure, temperature, humidity, dust, vibrations, seismic loads and also the chemical conditions and the duration of operation in these conditions;
- the means to demonstrate that the qualification will be ensured during the life of the plant. Ageing of the equipment during their operating time will be considered. See §4.2.8.1

4.2.5.5
Protection against hazards (internal, external)

The design requirements of the system or parts of the systems regarding all hazards (including postulated combination of hazards) considered in the design shall be clearly specified by the designer.

These requirements could be linked to:

- the role of the system in the prevention of hazards (example: the risk of explosion of a tank): the system shall be considered as a potential origin of hazard;
- the role of the system in the limitation of the consequences of hazards (example: fire extinguishing system);
- the protection of the system against hazards including consequential failures of initiating events.

The assessment shall ensure that the design of the system meets these requirements.

Specific attention shall be paid on hazards that need long term operation of systems (system reliability, sufficient water or fuel reserves, etc.).

System design regarding hazards shall be checked by assessing each hazard.

4.2.5.6
Location (system and its components) – Physical separation

The location of the system and its components shall be examined regarding:

- the requirements of spatial or physical separation because of the risk of CCF due to hazards;
- the function of safety systems shall not be endangered by systems used in normal operation or other systems executing the same safety functions;
- the need of accessibility to the equipment in case of accident;
- the radiation protection: the location of the system and its equipment shall limit the radiation dose received by the workers.

4.2.6
OTHER SAFETY ISSUES TO TAKE INTO ACCOUNT IN THE ASSESSMENT

4.2.6.1
PSA insights

The safety demonstration of the design of systems mainly relies on deterministic studies.

Nevertheless, PSA is used as a complementary useful tool in the safety assessment process for the systems design, among other applications.

Indeed, PSA may provide useful insights for the verification of the sufficiency and suitability of the systems design, especially in terms of systems redundancy and diversification.

In practice, the use of PSA during the safety assessment of the design of fluid systems can be useful to:

- estimate the overall importance (contribution to the core melt frequency) of the system;
- estimate the most important risk contributions within the system (components failures, human errors, common cause failures, functional dependencies, etc.), evaluate the reliability of the system;
- identify and evaluate the risk due to common cause failures, within the system and beyond system boundaries (support systems, etc.);
- evaluate the impact of systems/components unavailability due to maintenance.

In a more global context, the PSA should be used to:

- verify the balanced design of reactor safety related to the absence of scenarios having a predominant contribution to the frequency of core damage;
- contribute to the analysis of the sufficient diversification of the safety systems and functions;

- evaluate the influence of shared support and auxiliary systems.

4.2.6.2
Operating experience feedback

During the assessment, it shall be verified that the design of the system solves problems or weaknesses that have been identified on similar systems on existing plants on the basis of national and international Operating Experience Feedback (OEF).

4.2.6.3
System reliability (Reliability Analyses)

Reliability analyses provide quantitative information regarding the functional reliability of safety fluid systems during its respective intended uses. These reliability analyses may be used, together with deterministic criteria, when assessing the safety fluid systems to verify whether the safety concept is balanced.

Reference may be made to reliability analyses already carried out for comparable systems in other plants.

4.2.6.4
System requirements for the practical elimination of situations

In addition to the safety function that the safety system shall fulfill for the different design basis conditions in which it is required (e.g.: injection of borated water into the Reactor Coolant System by the safety injection system in case of Loss of coolant accident), the system may play a role in the safety demonstration for particular situations that must be "practically eliminated" (e.g.: role of some components, such as safety injection check valves on the injection lines, in accidental sequences with direct containment bypass).

It should be determined if the system may cause such a situation or is involved in the "practical elimination" of such situations.

4.2.6.5
Defence in depth

For new reactors, it shall be checked that the WENRA requirements for new nuclear power plants (Report "Safety of new NPP designs"; WENRA; March 2013) are fulfilled. In particular for system design, it shall be verified whether the requirements such as those issued in Position 2 regarding the independence of the levels of defense-in-depth are fulfilled.

4.2.7
SYSTEM OPERATION

The operation, maintenance and testing of fluid systems has to be in accordance with the design requirements. The fluid systems must be able to fulfill their functions continuously (e.g. ventilation) or on demand (e.g. emergency core cooling).

4.2.7.1
Configuration

All components of fluid systems are to be arranged such that they can operate, be tested and be kept in a proper state. For power operation, tests and maintenance, various system configurations are possible. The various modes of fluid systems operation in different plant conditions (start-up, power, outage), operating instructions and procedures have to be clearly described and documented.

Outages, maintenance, repairs or tests typically require changes in system configurations. Some tasks require strict isolation of components or systems. Particular attention should be given to situations when isolated components (mechanical, electrical, control) are put into operation.

It shall be checked that the safety fluid systems are designed such that non-destructive examinations of the components are possible if necessary.

4.2.7.2
Configurations actuation

Automatic actuation of safety fluid systems occurs when monitored physical parameters reach predetermined set points (pressure, temperature, neutron flux, etc.).

In many situations, manual operation of safety fluid systems is required. If manual actuation is the only way to start a system, it should be verified that there is adequate time available for the operator to perform the actuation. For an action outside the control room, It should be verified that the operator will be able to perform this action safely with respect to the environmental conditions.

4.2.7.3
Surveillance before and during operation

A surveillance program (monitoring, configuration checks, calibration, testing and inspections as far as possible during operation) should be established to ensure equipment availability and to detect abnormal conditions during plant operation.

The surveillance programs and procedures should cover mechanical or electrical components as well as software failures and deficiencies in procedures and potential sources for human errors.

COMMISSIONING TESTS

Commissioning tests are carried out to demonstrate the functional capability and operational availability of the safety fluid systems and thus fulfill one of the prerequisites for the commencement of the operation of the plant. Functional tests of the systems shall be as well carried out.

It will be verified that the tests are carried out such that the results enable conclusions to be drawn for the intended uses.

PERIODIC TESTS

Periodic functional tests are carried out to demonstrate that the tested components or the tested system are operationally available with respect to all the functions required of the system.

The assessment will check that the intervals between the periodic functional tests ensure reliability of the system and are specified in the technical specifications.

The following items should be as well verified:

1. the systems are designed such that periodic functional tests can be carried out safely;
2. the tests don't unacceptably restrict the availability of the systems needed for coping with incidents. Orders from the reactor protection system are given priority over the test schedule;
3. the periodic demonstration of operational availability is carried out as far as possible under conditions similar to those during incidents;
4. the instrumentation, control and power supply for the systems, required to cope with incidents is tested;
5. parameters, which help to provide information on the operational availability of the components and systems, are measured and documented.

MAINTENANCE

It will be verified that a maintenance program is defined for systems and components. All the maintenance work carried out shall be documented. Functional tests shall be carried out subsequent to maintenance work.

OPERATING TECHNICAL SPECIFICATIONS

During operation each NPP has to fulfill the conditions mentioned in their operating technical specifications. These specifications list all demands to be met to assure the function of a safety fluid system.

All the systems provided to cope with incidents and DBA are treated separately in the technical specifications.

It will be checked that the availability of the system is mentioned during all different modes of operation (power generation, hot shutdown, cold shutdown, etc.) and that each specification mentions what actions to take in case of unavailability of a system or a part of system (redundancy).

It will be verified that measures to verify the availability of the system are mentioned.

4.2.8 ADAPTABILITY TO FUTURE EVOLUTIONS

The main goal of this chapter is to provide guidance to Technical Safety Organisations on reviewing and assessing safety questions raised in nuclear activities with regard to safety fluid systems looking at the evolutions of a nuclear power plant. These possible evolutions of a NPP covers the ageing of structures and components, possible climate changes and decommissioning of NPP.

4.2.8.1 *Ageing of structures and components*

To maintain the plant safety it is very important to detect ageing effects on safety fluid systems (components).

During the safety assessment it is necessary to evaluate associated reductions in safety margins and if necessary verify that corrective actions are planned before loss of integrity or functional capability occurs. Thus, when performing the review of a system, it is necessary to check:

- are there specific aspects of this NPP (environmental conditions, use of different materials) related to ageing of structures and components of safety fluid systems?
- are the ageing issues for the safety fluid systems and its components clearly identified and documented throughout the plant's lifetime?

It shall be checked that analysis of ageing of structures and components of safety fluid systems includes:

- the list of structures and components of safety fluid systems of the plant that could be affected by ageing;
- the procedures and a monitoring process in order to detect degradation;
- effects of specific operation conditions on the structures and components of safety fluid systems (radiation level, vibrations, submerged conditions, radiation from hot surfaces, ventilation, unstable voltage, etc.) and mechanisms of degradation;
- appropriate consideration of the analysis of operating experience feedback with respect to ageing;
- a strategy for ageing management.

4.2.8.2 *Climate change*

The planned operating lifetime of a nuclear power plant is assumed to be up to several decades. Over such a period, it is expected that the global climate is likely to undergo changes, with regional variability. Climatic variability and climate change may have effects on the frequency and the severity of extreme meteorological and hydrological conditions.

Consequently, it should be verified that the variability of and changes in regional climate are considered, with account taken of uncertainties in the climate projections.

The regional climate change associated with global climate change may affect the change of hydrological and meteorological hazards. These hazards may affect the parameters of ultimate heat sink and the capacity of auxiliary systems and other systems, supporting the safety fluid systems (ventilation air cooling, etc.). It should be verified that adequate margins are taken into account to cope with climate change.

4.2.8.3 *Decommissioning*

The safety analysis should be performed for all stages of NPP during whole lifetime

of NPP, including decommissioning. During the decommissioning of NPP the safety analysis is an evaluation of the potential hazards associated with the implementation of the decommissioning activities and their potential consequences. In most cases the decommissioning of facilities is performed using a phased (step by step) approach. The nature of the decommissioning activities and the hazards they entail may differ for each phase.

The reviewing and safety assessment by Technical Safety Organisations should be conducted in accordance with relevant national regulations and international recommendations, and should be performed during the design phase of NPP for each phase of decommissioning (for the entire decommissioning period and taking into account the interrelation of the phases).

Since decommissioning of NPP's is inevitable, decommissioning should be evaluated during the design stage: it shall be verified that the designer describes how to facilitate the future dismantling operations.

Regarding safety fluid systems, it is necessary to take into account that the required safety systems are different for different decommissioning phases (e.g. including deferral periods). And the systems may perform different functions in different decommissioning phases. The safety fluid systems shall be in place to protect against or to mitigate the consequences of possible accidents during decommissioning.

Thus, performing the review and safety assessment is necessary to evaluate the suitability, sufficiency and reliability of these safety fluid systems for the entire duration of the lifetime of the plant.

4.2.9
ANALYSIS OF AUXILIARY SYSTEMS

The reliability of a safety function depends not only on the systems that participate directly to the function but also on the reliability of the auxiliary systems that are needed for the good operation of these systems.

For example;

- I&C;
- cooling systems;
- venting, heating and air-conditioning systems;
- electrical supply.

Therefore, the assessment should verify that functional requirements, design requirements (classification, SFC, redundancy, physical or spatial separation, etc.) of auxiliary systems are consistent with the requirements of the systems that it supports.

The design of auxiliary systems shall so be assessed in the same level of detail as the main systems. The consequences of the loss of auxiliary systems on the main system or on the safety function shall be examined. In that frame PSA could be useful.

5 USEFULL REFERENCES

CLASSIFICATION:

- IAEA SSG 30 - Safety Classification of Structures, Systems and Components in Nuclear Power Plants (May 2014).
- IAEA NS-G-1.9 Design of the Reactor Coolant System and Associated Systems in Nuclear Power Plants (September 2004).
- WENRA Reactor Safety Reference Levels (September 2014). Issue G: Safety Classification of Structures, Systems and Components.

DEFENSE IN DEPTH

- IAEA INSAG 10 "Defence in depth in nuclear safety" (1996).
- IAEA SSR-2/1: Safety of Nuclear Power Plants: Design.
- WENRA Reactor Safety Reference Levels (September 2014).
- WENRA Report "Safety of new NPP designs (March 2013).

SYSTEM OPERATION

- IAEA SSR-2/2 Safety of Nuclear Power Plants: Commissioning and Operation (July 2011).
- IAEA NS-G-2.14 Conduct of Operations at Nuclear Power Plants (August 2008).
- IAEA NS-G-2.6 Maintenance, Surveillance and In-service Inspection in Nuclear Power Plants (October 2002).
- IAEA-TECDOC-1335 Configuration management in nuclear power plants (January 2003).
- WENRA Issue K: Maintenance, in-service inspection and functional testing (January 2008).

ADAPTABILITY TO FUTURE EVOLUTION

- IAEA SSG-18 Meteorological and Hydrological Hazards in Site Evaluation for Nuclear Installations (November 2011).
- IAEA WS-G-5.2 Safety assessment for the decommissioning of facilities using radioactive material.
- WENRA Decommissioning safety reference levels report version 2.1 (March 2012).

ETSON

EUROPEAN
TECHNICAL SAFETY
ORGANISATIONS
NETWORK

ETSON SECRETARIAT - LEI
Breslaujos 3,
LT-44403 Kaunas, Lithuania
Phone: + 370 37 401926
www.etson.eu

Association n° W921001929