Western European
WENRA
Nuclear Regulators Association

Report

Western European
WENRA RHWG
Nuclear Regulators Association

Report
Safety of new NPP designs

Study by Reactor Harmonization Working Group RHWG
March 2013

Table of Content
Safety of new NPP designs

-

01
Introduction

One of the objectives of the Western European Nuclear Regulators' Association (WENRA), as stated in its terms of reference, is to develop a harmonized approach to nuclear safety and radiation protection and their regulation.

A significant contribution to this objective was the publication, in 2006[1], of a report on harmonization of reactor safety in WENRA countries. This report addresses the nuclear power plants (NPPs) that were in operation at that time in those countries; it includes about 300 "Reference Levels"[2].

Since then, the construction of new nuclear power plants has begun or is being envisaged in several European countries. Hence, it was considered timely for WENRA to develop the safety objectives for new nuclear power plants. A report "Safety objectives for new power reactors – study by RHWG – December 2009" and "WENRA statement on safety objectives for new nuclear power plants – November 2010" have been published by WENRA (www.wenra.org). The statement includes seven safety objectives, which are the basis for further harmonization work of WENRA. Based on these safety objectives, WENRA decided to develop common positions on selected key safety issues for the design of new nuclear power plants.

This report sets out the common positions established by the Reactor Harmonization Working Group (RHWG) of WENRA on the selected key safety issues. The work was initiated and also a major part of the work was carried out before the TEPCO Fukushima Dai-ichi accident. Therefore, the report discusses also some considerations based on the major lessons from the Fukushima Dai-ichi accident, especially concerning the design of new nuclear power plants, and how they are covered in the new reactor safety objectives and the common positions.

Within the WENRA Safety Objectives for New Nuclear Power Plants the words "reasonably practicable" or "reasonably achievable" are used. In this report the words Reasonably Practicable are used in terms of reducing risk as low as *reasonably practicable* or improving safety as far as *reasonably practicable*. The concept of *reasonable practicability* is directly analogous to the ALARA principle applied in radiological protection, but it is broader in that it applies to all aspects of nuclear safety. In many cases adopting practices recognized as good practices in the nuclear field will be sufficient to show achievement of what is "reasonably practicable".

[1] Harmonization of Reactor Safety in WENRA countries, report by RHWG, January 2006

[2] These "Reference Levels" were updated in January 2008

For some design expectations in this report, ”reasonable practicability” should be taken to mean that, in addition to meeting the normal requirements of good practice in engineering, further safety or risk reduction measures for the design or operation of the facility should be sought and that these measures should be implemented unless the utility is able to demonstrate that the efforts to implement the proposed measures are grossly disproportionate to the safety benefit they would confer.

This study presents WENRA safety expectations for the design of new NPPs. These expectations are defined in addition to the recent design requirements presented in international texts such as the ones presented in IAEA SSR-2/1 which also covers other fields to ensure safety at the design stage[3].

[3] As stated in IAEA SSR-2/1, the safety of a nuclear power plant is ensured by means of proper site selection, design, construction and commissioning, and the evaluation of these, followed by proper management, operation and maintenance of the plant. In a later phase, appropriate transition to decommissioning is required.

02
WENRA safety objectives for new nuclear power plants

The WENRA safety objectives for new nuclear power plants were developed on the basis of a systematic review of the Fundamental Safety Principles (SF-1 document issued 2006 by the IAEA). Grounding the safety objectives on the fundamental safety principles has been explained in the December 2009 study by the RHWG. The WENRA Objectives O1-O7 cover the following areas:

O1. Normal operation, abnormal events and prevention of accidents

O2. Accidents without core melt

O3. Accidents with core melt

O4. Independence between all levels of Defence-in-Depth

O5. Safety and security interfaces

O6. Radiation protection and waste management

O7. Leadership and management for safety

The safety objectives address new civil nuclear power plant projects. However, these objectives should also be used as a reference to help identify reasonably practicable safety improvements for “deferred plants” and existing plants during Periodic Safety Reviews.

The safety objectives are formulated in a qualitative manner to drive design enhancements for new plants with the aim of obtaining a higher safety level than that expected from existing plants. For instance, to be able to comply with the qualitative criteria proposed in Objective O3 “Accidents with core melt”, confinement features should be designed to cope with core melt accidents, even in the long term.

The WENRA safety objectives call for an extension of the safety demonstration for new plants, consistent with reinforcement of Defence-in-Depth. Some situations that are considered as “beyond design” for existing plants, such as multiple failures conditions and core melt accidents, are taken into account in the design of new plants.

WENRA considers that these safety objectives reflect the current state of the art in nuclear safety and can be implemented at the design stage using the latest available industrial technology of nuclear power plants. However, since nuclear safety and what is considered adequate protection can never be static, these safety objectives may be subject to further evolution reflecting the need to strive for continuous improvement.

WENRA expects new nuclear power plants to be designed, sited, constructed, commissioned and operated in line with these objectives.

The WENRA statement on safety objectives for new nuclear power plants is included in Annex 1.

03
Selected key safety issues

The WENRA safety objectives are by nature high level and even when the WENRA statement was published in November 2010 it was recognized that supplementing them with some more detailed common positions on selected issues would help to clarify the meaning. The safety issues where common positions have been developed were chosen on the basis that they were particularly relevant to the expectations for new reactors in comparison with existing reactors. The topics were selected so that they would be relevant for the design of new reactors, constitute an entity and also to make it possible to complete the work by the end of 2012, taking into account the resources of the RHWG.

Objective O4 “Independence between all levels of Defence-in-Depth” seeks enhancement of the effectiveness of the independence between all levels, to provide as far as reasonably practicable an overall reinforcement of Defence-in-Depth. **Position 1** presents WENRA’s Defence-in-Depth approach, describing WENRA’s expectation that multiple failure events and core melt accidents should be considered in the design of new nuclear power plants. **Position 2** presents the expectations on the independence between different levels of Defence-in-Depth. **Position 3** describes methodology for identification of multiple failure events that should be considered in the design, the related design expectations and the associated safety demonstration.

Objective O4 also mentions strengthening of each Defence-in-Depth level separately. This is achieved by the application of redundancy, diversity and separation principles within one level of Defence-in-Depth. According to safety objective O2 “Accidents without core melt”, the core damage frequency should be reduced as far as reasonably achievable, taking into account all types of credible hazards and failures and credible combinations of failures.

Objective O3 “Accidents with core melt” requires that for accidents with core melt that have not been practically eliminated, design provisions have to be taken so that only limited protective measures in area and time are needed for the public and that sufficient time is available to implement these measures. **Position 4** presents the design provisions to deal with core melt accidents and an interpretation of what limited protective measures could mean in practice.

Objective O3 states also that accidents with core melt which would lead to early or large releases have to be practically eliminated. **Position 5** presents a discussion on means for practical elimination, gives examples of typical LWR accident sequences that could be considered for practical elimination and expectations for the safety demonstration.

Objective O2 “Accidents without core melt” requires providing due consideration to siting and design to reduce the impact of external hazards and malevolent acts. **Position 6** describes the expectations for how external hazards should be considered in the design of new NPPs and **Position 7** deals with design expectations concerning an intentional crash of a commercial aircraft on a NPP. Airplane crash is an example of the safety and security interface, which is discussed in Objective O5 “Safety and security interfaces”.

03.1 Position 1: Defence-in-Depth approach for new nuclear power plants

Introduction

The primary means of preventing accidents in a nuclear power plant and mitigating the consequences of accidents is the application of the concept of Defence-in-Depth (DiD)[4]. This concept should be applied to all safety related activities, whether organizational, behavioural or design related, and whether in full power, low power or various shutdown states. This is to ensure that all safety related activities are subject to independent layers of provisions, so that if a failure were to occur, it would compensated for or corrected by appropriate measures. Application of the concept of Defence-in-Depth throughout design and operation provides protection against anticipated operational occurrences and accidents, including those resulting from equipment failure or human induced events within the plant, and against consequences of events that originate outside the plant.

Therefore, Defence-in-Depth is a key concept of the safety objectives established by WENRA for new nuclear power plants. In particular, these safety objectives call for an extension of the safety demonstration for new plants, in consistence with the reinforcement of the Defence-in-Depth approach. Thus the DiD concept should be strengthened in all its relevant principles. In addition to the reinforcement of each level of the DiD concept and the improvement of the independence between the levels of DiD (as stated in the WENRA safety objectives), this also means that the principle of multiple and independent barriers should be applied for each significant source of radioactive material. It shall also be ensured that the DiD capabilities intended in the design are reflected in the as-built and as-operated plant and are maintained throughout the plant life time.

Some situations that are considered as “beyond design” for existing plants, such as multiple failure events and core melt accidents, are considered in the design of new plants. As a consequence, it has been considered useful to refine this approach which remains consistent with the IAEA SF-1 document.

This section focuses primarily on the proposal to refine the structure of the DiD levels. Other DiD related topics, i.e. the “Independence of Defence-in-Depth levels”, “Multiple failure events” and “Provisions to mitigate core melt and radiological consequences” are addressed in separate sections.

Historical development of the Defence-in-Depth as regards currently operating reactors

The concept of “Defence-in-Depth” has been introduced in the field of nuclear safety in the early 1970s. This concept was gradually refined to constitute an increasingly effective approach combining both prevention of a wide range of postulated incidents and accidents and mitigation of their consequences. Incidents and accidents were postulated on the basis of single initiating events selected according to the order of magnitude of their frequency, estimated from general industrial experience.

[4] According to the IAEA safety glossary, this concept is depicted as a hierarchical deployment of different levels of divers equipment and procedures to prevent the escalation of anticipated operational occurrences and to maintain the effectiveness of physical barriers placed between a radiation source or radioactive materials and workers, members of the public or the environment, in operational states and, for some barriers, in accident conditions.

The definitions of the different levels of DiD were set as to mirror escalation from normal operation to accident so that if one level fails, a higher level comes into force. This does not mean that the situations considered in one level are systematically resulting from a failure of systems/features associated to the previous level of defence. The different levels of DiD were set as to cover the different situations that need to be considered in the design and operation of the plant. The approach was intended to provide robust means to ensure the fulfilment of each of the fundamental safety functions[5] of:

(1) Control of reactivity;
(2) Removal of heat from the reactor and from the fuel store;
(3) Confinement of radioactive material, shielding against radiation, as well as limitation of accidental radioactive releases.

In the early stage, the concept of Defence-in-Depth included three levels:

Levels of defence in depth	Objective	Essential means	Associated plant condition categories (for explanation - not part of original table)
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation	Normal operation
Level 2	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance features	Anticipated operational occurrences
Level 3	Control of accident within the design basis	Engineered safety features and accident procedures	Design basis accidents (postulated single initiating events)

[5] IAEA SSR-2/1

Then, the concept of Defence-in-Depth for the current operating reactors was further developed to take into account severe plant conditions that were not explicitly addressed in the original design (hence called “beyond design conditions”), in particular lessons learned from the development of probabilistic safety assessment and from the Three Mile Island accident (USA 1979) which led to a severe core melt accident and from the Chernobyl accident (Ukrainian Republic of USSR 1986). These developments led to two additional levels in DiD (see INSAG 10 – 1996):

Levels of defence in depth	Objective	Essential means	Associated plant condition categories (for explanation - not part of original table)
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation	Normal operation
Level 2	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance features	Anticipated operational occurrences
Level 3	Control of accident within the design basis	Engineered safety features and accident procedures	Design basis accidents (postulated single initiating events)
Level 4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents	Complementary measures and accident management	Multiple failures Severe accidents
Level 5	Mitigation of radiological consequences of significant releases of radioactive material	Off-site emergency response	

New reactor designs and associated evolution of the Defence-in-Depth levels

Rationale for an evolution of DiD levels

For new reactor designs, there is a clear expectation to address in the original design what was often "beyond design" for the previous generation of reactors, such as multiple failure events and core melt accidents, called Design Extension Conditions in IAEA SSR-2/1. This is a major evolution in the range of situations considered in the initial design to prevent accidents, control them and mitigate their consequences, and in the corresponding design features of the plant. It implies that the meaning of "beyond design basis accident" is not the same for existing reactors and for new reactors. Several scenarios that are considered beyond design basis for most existing reactors are now included from the beginning in the design for new reactors (postulated multiple failure events and core melt accidents).

In the DiD approach, the objectives of the different levels of defence are mainly defined as successive steps in the protection against the escalation of accident situations.

The phenomena involved in accidents with core/fuel melt (severe accidents) differ radically from those which do not involve a core melt. Therefore core melt accidents should be treated on a specific level of Defence-in-Depth.

In addition, for new reactors, design features that aim at preventing a core melt condition and that are credited in the safety demonstration should not belong to the same level of defence as the design features that aim at controlling a core melt accident that was not prevented. However, should a core melt accident occur, all plant equipment still available may be used.

The question has been discussed by RHWG whether for multiple failure events, a new level of defence should be defined, because safety systems which are needed to control postulated single initiating events are postulated to fail and thus another level of defence should take over. However, the single initiating events and multiple failure events are two complementary approaches that share the same objective: controlling accidents to prevent their escalation to core melt conditions.

Hence, at this stage of the discussion, it has been proposed to treat the multiple failure events as part of the 3rd level of DiD, but with a clear distinction between means and conditions (sub-levels 3.a and 3.b).

The scope of the related safety demonstration has to cover all risks induced by the nuclear fuel, including all fuel storage locations, as well as the risks induced by other relevant radioactive materials.

Refined structure of the levels of DiD

The refined structure of the levels of DiD proposed by RHWG is as follows:

Levels of defence in depth	Objective	Essential means	Radiological consequences	Associated plant condition categories
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation, control of main plant parameters inside defined limits	No off-site radiological impact (bounded by regulatory operating limits for discharge)	Normal operation
Level 2	Control of abnormal operation and failures	Control and limiting systems and other surveillance features		Anticipated operational occurrences
Level 3 (1) 3.a	Control of accident to limit radiological releases and prevent escalation to core melt conditions (2)	Reactor protection system, safety systems, accident procedures	No off-site radiological impact or only minor radiological impact (4)	Postulated single initiating events
3.b		Additional safety features(3), accident procedures		Postulated multiple failure events
Level 4	Control of accidents with core melt to limit off-site releases	Complementary safety features(3) to mitigate core melt, Management of accidents with core melt (severe accidents)	Off-site radiological impact may imply limited protective measures in area and time	Postulated core melt accidents (short and long term)
Level 5	Mitigation of radiological consequences of significant releases of radioactive material	Off-site emergency response Intervention levels	Off site radiological impact necessitating protective measures(5)	-

(1) Even though no new safety level of defence is suggested, a clear distinction between means and conditions for sub-levels 3.a and 3.b is lined out. The postulated multiple failure events are considered as a part of the Design Extension Conditions in IAEA SSR-2/1.

(2) Associated plant conditions being now considered at DiD level 3 are broader than those for existing reactors as they now include some of the accidents that were previously considered as "beyond design" (level 3.b). For level 3.b, analysis methods and boundary conditions, design and safety assessment rules may be developed according to a graded approach, also based on probabilistic insights. Best estimate methodology and less stringent rules than for level 3.a may be applied if ap-

propriately justified. However the maximum tolerable radiological consequences for multiple failure events (level 3.b) and for postulated single failure events (level 3.a) are bounded by Objective O2.

(3) The task and scope of the additional safety features of level 3.b are to control postulated common cause failure events as outlined in Section 3.3 on "Multiple failure events". An example for an additional safety feature is the additional emergency AC power supply equipment needed for the postulated common cause failure of the primary (non-diverse) emergency AC power sources.

The task and scope of the complementary safety features of level 4 are outlined in Section 3.4 on "Provisions to mitigate core melt and radiological consequences". An example for a complementary safety feature is the equipment needed to prevent the damage of the containment due to combustion of hydrogen released during the core melt accident.

(4) It should be noted that the tolerated consequences of Level 3.b differ from the requirements concerning Design Extension Conditions in IAEA SSR-2/1 that gives a common requirement for DEC: "for design extension conditions that cannot be practically eliminated, only protective measures that are of limited scope in terms of area and time shall be necessary".

(5) Level 5 of DiD is used for emergency preparedness planning purposes.

In each level of DiD, some situations need to be practically eliminated as it cannot be demonstrated that, should they occur, their radiological consequences would be tolerable. Situations that could lead to early or large releases of radioactive materials have to be practically eliminated (see Section 3.5 on "Practical elimination").

03.2 Position 2: Independence of the levels of Defence-in-Depth

Introduction

According to the 2010 WENRA "Statement on safety objectives for new nuclear power plants" WENRA expects new nuclear power plants to be designed, sited, constructed, commissioned and operated with the objective, among others, of "*enhancing the effectiveness of the independence between all levels of defence-in-depth, in particular through diversity provisions (in addition to the strengthening of each of these levels separately…), to provide as far as reasonably achievable, an overall reinforcement of defence-in-depth*." (Objective O4: "Independence between all levels of defence-in-depth").

This section focuses on the independence between systems, structures and components (SSCs) important to safety, allocated to different levels of Defence-in-Depth (DiD). It does not aim to address independence between SSCs important to safety within a level of defence-in-depth nor administrative/procedural aspects.

Furthermore, this section solely addresses those SSCs which are necessary to meet the acceptance criteria, related to the three fundamental safety functions, and the radiological goals defined at the different DiD levels according to WENRA safety objectives.

Definitions of key terms used in this section are given in the end. The levels of DiD which are referred to in this section are defined in Section 3.1 on Defence-in-Depth.

This section aims to give some guidance on how to enhance the effectiveness of the independence between the levels of DiD.

Independence between systems, structures and components (SSCs)

WENRA considers that independent SSCs for safety functions on different DiD levels shall possess both of the following characteristics:

- the ability to perform the required safety functions is unaffected by the operation or failure of other SSCs needed on other DiD levels;
- the ability to perform the required safety functions is unaffected by the occurrence of the effects resulting from the postulated initiating event, including internal and external hazards, for which they are required to function.[6]

As a consequence, the means to achieve independence between SSCs are adequate application of:

- diversity;
- physical separation, structural or by distance;
- functional isolation.

The following expectations on independence are related to the independence between SSCs as credited in the deterministic safety demonstration. If an accident was to occur, all available and effective equipment could obviously be used, including those not credited in the safety demonstration.

[6] Based on the IAEA safety glossary.

Basic safety expectations on the independence between different levels of DiD

(1) There shall be independence to the extent reasonably practicable between different levels of DiD so that failure of one level of DiD does not impair the defence in depth ensured by the other levels[7] involved in the protection against or mitigation of the event.

(2) The adequacy of the achieved independence shall be justified by an appropriate combination of deterministic and probabilistic safety analysis and engineering judgement.
For each postulated initiating event (starting with DiD level 2), the necessary SSCs should be identified and it shall be shown in the safety analysis that the SSCs credited in one level of DiD are adequately independent of SSCs credited in the other levels of DiD.[8]

(3) Appropriate attention shall be paid to the design of I&C, the reactor auxiliary and support systems (e. g. electrical power supply, cooling systems) and other potential cross cutting systems. The design of these systems shall be such as not to unduly compromise the independence of the SSCs they actuate, support or interact with.

Implementation of the basic safety expectations

In applying the above basic expectations, the following considerations shall be taken into account (some specific considerations are presented in the next section):

(1) SSCs fulfilling safety functions in case of postulated single initiating events (DiD level 3.a) or in postulated multiple failure events (DiD level 3.b) should be independent to the extent reasonably practicable from SSCs used in normal operation (level 1) and/or in anticipated operational occurrences (level 2). This independence is so that the failure of SSCs used in normal operation and/or in anticipated operational occurrences does not impair a safety function required in the situation of a postulated single initiating event or of a multiple failure event resulting from the escalation of such failures during normal operation or a level 2 event.

(2) SSCs fulfilling safety functions used in case of postulated single initiating events (DiD level 3.a) should be independent to the extent reasonably practicable from additional safety features used in case of postulated multiple failure events (DiD level 3.b). For the safety analyses of postulated multiple failure events, credit may be taken from SSCs used in case of postulated single initiating events as far as these SSCs are not postulated as unavailable and are not affected by the multiple failure event in question; SSCs specifically designed for fulfilling safety functions used in postulated multiple failure events should not be credited for level 3.a event analyses for the same scenario.

(3) Complementary safety features specifically designed for fulfilling safety functions required in postulated core melt accidents (DiD level 4) should be independent to the extent reasonably practicable from the SSCs of the other levels of DiD.

---

[7] This should cover all plant states of the nuclear power plant.

[8] For future development designs a more systematic allocation of each SSC to one particular level of DiD, irrespective of the postulated initiating event, may provide a more robust demonstration of the independence between levels of DiD.

Specific considerations (examples on specific topics)

Emergency AC power supply

The emergency AC power supply belonging to DiD level 3.a may be used also in DiD level 2. An additional diverse emergency AC power supply shall be designed for DiD level 3.b because the common cause failure of the primary (non-diverse) emergency AC power sources is postulated. The emergency power supply on DiD Level 3.b may be also used for DiD level 4. The rationale for this is that additional independent on-site provisions are not likely to significantly increase the reliability of the emergency AC power supply. Lessons learnt from the Fukushima Dai-ichi accidents with regard to the supply of additional AC power supply provisions are addressed separately.

Separation of cables

Since principles of separation of cables already exist between the divisions of redundant systems and between safety and non-safety systems, it may not be reasonably practicable to introduce additional separation on the basis of levels of defence.

Reactor protection system (RPS) and other I&C aspects

The reactor protection system (RPS) shall be adequately independent from other I&C systems and must be functionally isolated from them. The RPS may have I&C functions on other DiD levels than 3, e.g. the scram system may be actuated by the RPS for specific DiD level 2 events. Diverse I&C means shall be designed for DiD level 3.b in case the common cause failure of the RPS has to be postulated.

Limitation and control systems (not the RPS) for the actuation of systems needed to handle level 2 events may be combined with I&C for normal operation.

Containment

On each level of defence there is a need for confinement as a safety function. This safety function may be accomplished for example by the use of the containment in combination with other SSCs. The containment is thus an example of a structure which is used on different levels of defence and for which it would not be reasonably practicable to require independence for different levels of Defence-in-Depth.

Reactor pressure vessel

The reactor pressure vessel in combination with other SSCs may be used to fulfil/accomplish several safety functions on several levels of DiD. For example, on DiD level 1 and 2 this may include removal and transfer of thermal energy from nuclear fuel during normal and abnormal operation. On DiD level 1, 2, 3 and 4 this may include the removal of residual heat from nuclear fuel to the ultimate heat sink and on level 1, 2, 3 and 4 this may also include the prevention of the dispersal of radioactive material. It would not be reasonably practicable to require independence for these different levels.

The list of specific considerations/examples shall give guidance on the implementation of the basic safety expectations and thus is not exhaustive.

Definitions

Functional isolation:

Prevention of influences from the mode of operation or failure of one circuit or system on

another.[9] Functional isolation shall refer to the isolation of inter-connected systems and sub-systems from one another so as to prevent propagation of failure or spurious signals from one system to another and it also includes electrical isolation and information flow isolation.

Fundamental safety function:
A safety function is a specific purpose that must be accomplished for safety. In a nuclear power plant there exist the following three fundamental safety functions (from IAEA SSR-2/1):

(1) Control of reactivity;
(2) Removal of heat from the reactor and from the fuel store;
(3) Confinement of radioactive material, shielding against radiation, as well as limitation of accidental radioactive releases.

Independence between systems, structures and components:
Independent systems, structures and components (SSCs) for safety functions on different DiD levels shall possess both of the following characteristics:

- the ability to perform the required safety functions is unaffected by the operation or failure of other SSCs needed on other DiD levels;
- the ability to perform the required safety functions is unaffected by the occurrence of the effects resulting from the postulated initiating event, including internal and external hazards, for which they are required to function. [9]

Means to achieve independence between SSCs are adequate application of:

- physical separation, structural or by distance;
- functional isolation;
- diversity.

Reactor protection system:
System that monitors and processes the variables relevant for safety and which, on reaching pre-set actuation limits, automatically initiates the necessary actions of safety systems for the control of DiD level 3 events, in order to prevent an unsafe or potentially unsafe condition. The reactor protection system encompasses all electrical and mechanical devices and circuitry, from sensors to actuation device input terminals. [9]

Systems, structures and components important to safety (SSCs):
A general term encompassing all the plant elements (items) of a facility or activity which contribute to protection and safety, except human factors.

- Structures are the passive elements: buildings, vessels, shielding, etc..
- A system comprises several components and/or structures, assembled in such a way as to perform a specific (active) function.
- A component is a discrete element of a system.
  Examples of components are wires, transistors, integrated circuits, motors, relays, solenoids, pipes, fittings, pumps, tanks and valves.

[9] Based on the IAEA safety glossary.

03.3 Position 3: Multiple failure Events

Introduction

Defence in depth (DiD) is a key element of the safety objectives established by WENRA for new nuclear power plants. In particular, these safety objectives call for an extension of the safety demonstration for new plants, in consistence with the reinforcement of the defence in depth. Some situations that are considered as "beyond design" for existing plants, such as e.g. multiple failure events, are to be considered in the design of new plants. As a consequence, it has been considered useful to refine this approach whilst remaining consistent with the IAEA SF-1 document (cf. with Section 3.1 on "Defence in depth approach for new nuclear power plants").

In this refined DiD concept for new reactors level of defence 3 consists of level 3.a and level 3.b. Both levels aim to "control of accidents to limit radiological releases and prevent escalation to core melt conditions". Level 3.a includes "Postulated single initiating events" and level 3.b includes "Selected multiple failure events including possible failure or inefficiency of safety systems involved in level 3.a".[10]

Level 3.b is related to Objective O2, "Accidents without core melt". According to Objective O2 it shall be ensured that accidents without core melt induce no off-site radiological impact or only minor radiological impact (in particular, no necessity of iodine prophylaxis, sheltering or evacuation). Design provisions considered in level 3.b for postulated multiple failures shall further decrease the frequency and/or mitigate consequences of sequences beyond those considered in the design basis for existing reactors so far, such as anticipated transients without scram (ATWS) or station black out (SBO) scenarios.

Scope

In a general sense, failure of safety or safety related system at a NPP may arise for different reasons. These failures could result due to

i) a single Postulated Initiating Event (PIE) with consequential failures;

ii) an external or internal hazard (e.g. earthquake, flooding, fire) affecting one or several safety (or safety related) systems;

iii) common cause failure for other reasons than a postulated hazard, affecting similar equipment in

   a. the same safety (or safety related) system, or

   b. several safety (or safety related) systems

iv) random failures that affect simultaneously several safety (or safety related) systems.

Failures resulting from a PIE (i) or a postulated hazard (ii) are part of the considered event and studied with the corresponding rules. This section deals with multiple failures resulting from common cause failures, affecting the same safety or safety related system (iii.a). Other common cause failures affecting different safety (or safety related) systems are not postulated.

[10] Level 3.b events are considered as a part of the Design Extension Conditions in IAEA SSR 2.1.

There should be other design provisions to prevent such failure modes. Combination of random failures that affect simultaneously several safety (or safety related) systems (iv) are not postulated deterministically from this approach, and should be considered in PSA.

Multiple failure events to be considered at the design stage are characterized as:

- a postulated common cause failure or inefficiency of all redundant trains of a safety system11 needed to fulfil a safety function necessary to cope with an anticipated operational occurrences (AOO) or a single PIE (see examples in Table 1), or
- a postulated common cause failure of a safety system or a safety related system needed to fulfil the fundamental safety functions in normal operation (see examples in Table 2).

Methodology of identification of multiple failure events

The identification of multiple failure events should start with a systematic deterministic approach based on a list of anticipated operational occurrences and postulated single initiating events.[12]

Safety (or safety related) systems to fulfil the related safety functions for these AOO and PIE have to be identified. Based on this a list of multiple failure events should be developed. Furthermore, a list of common cause failures of safety systems or safety related systems needed to fulfil the fundamental safety functions in normal operation should be compiled. This process is supported by PSA.

As a result an intermediate list should include:

- AOOs and a postulated common cause failure of redundant trains of a safety system;
- Single PIEs and a postulated common cause failure of redundant trains of a safety system;
- Complex or specific scenarios including common cause failures of safety systems or safety related systems needed to fulfil the fundamental safety functions in normal operation

The identification procedure shall be performed for any operational state and should include failures of spent fuel pool cooling.

Based on this, a selection of a reasonable number of limiting (bounding) cases, which present the greatest challenge to the acceptance criteria and which define the performance parame-

[11] IAEA safety glossary: ***safety system.*** A *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*.

Safety systems consist of the *protection system*, the *safety actuation systems* and the *safety system support features*. *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*.

[12] The approach may start at the beginning of the design with a reduced list based on engineering judgment and should be completed stepwise in parallel to the developing design approach.

ters for safety related equipment, should be made using experience feedback, engineering judgment and probabilistic assessment.

In choosing the multiple failure events to be addressed in the design, the following factors should be considered together:

- the frequency of the event;
- the grace time for necessary human actions;
- the margins to cliff edge effects; and
- the radiological or environmental consequences of the event (care should be taken to scenarios with containment bypass).

Any general cut-off frequency should be justified, considering in particular the overall core damage frequency (CDF) aimed at.

The identification process should lead to a list of postulated multiple failure events which have to be considered in the design.

Design expectations

While the postulated single initiating events analyses in combination with the single failure criteria usually gives credit on redundancy in design provisions of safety systems and of their support functions, addressing multiple failure events emphasizes diversity in the design provisions of the third level of DiD.

Safety assessments of the plant conditions resulting from the multiple failures selected by deriving them from the defined methodology shall be performed deterministically in order to design additional safety features that aim at preventing core damage conditions. “Accident procedures” shall be in place to define the management of the safety features and to give guidance on necessary human actions. The appropriateness of the foreseen additional design features has to be assessed by PSA modelling and results.

The expectations for the additional safety features and the associated systems which are foreseen to cope with such conditions on the level 3.b of the DiD concept do not have to be as stringent as for 3.a if appropriately justified. This justification may be based on probabilistic arguments, complemented by additional factors similar to those in the previous section. Systems designed to comply with these conditions should have sufficient redundancy of active components to reach adequate reliability.

According to Section 3.2 on the “Independence of Defence-in-Depth Levels”, systems, structures and components (SSCs) fulfilling safety functions used in case of postulated single initiating events (DiD level 3.a) should be independent to the extent reasonably practicable from additional safety features used in case of postulated multiple failure events (DiD level 3.b). For the safety analyses of postulated multiple failure events, credit may be taken from SSCs used in case of postulated single initiating events as far as these SSCs are not postulated as unavailable and are not affected by the multiple failure event in question. SSCs specifically designed for fulfilling safety functions used in postulated multiple failure events should not be credited for level 3.a event analyses for the same scenario.

Safety demonstration

For the additional safety features on level 3.b of the DiD concept it shall be shown that under the assumption of the postulated multiple failures first a controlled state[13] and later on a safe state14 is reached and the radiological criteria of O2 “No off-site radiological impact or only minor radiological impact” will be fulfilled analogue to the requirement on level 3.a.

Once a controlled state is reached emphasis shall be paid to achieve a safe state in which the fundamental safety functions can be ensured and stably maintained for long time.

For the technical safety demonstration, acceptance criteria should be:

- reaching core sub-criticality quickly and maintaining it after;
- no or only limited fuel damage and ensuring of a coolable core geometry;
- prevention of energetic dispersal of fuel;
- limiting the pressure in the reactor coolant pressure boundary below a justified value;
- maintaining the fuel in the spent fuel pool covered with coolant with sufficient margin and ensuring that potential boiling conditions will not preclude potential necessarily access by personnel to perform accident procedures.

For level 3.b, analysis methods and boundary conditions, design and safety assessment rules may be developed according to a graded approach, also based on probabilistic insights. Best estimate methodology and less stringent rules than for level 3.a may be applied if appropriately justified. However the maximum tolerable radiological consequences for multiple failure events (level 3.b) and for postulated single failure events (level 3.a) are bounded by Objective O2.

Examples of multiple failure scenarios

Some examples of multiple failure scenarios are given below. Plant specific lists of multiple failure scenarios may include these examples but probably will not be limited to it. The examples are:

[13] IAEA SSR-2.1: Plant state, following an *anticipated operational occurrence* or accident conditions, in which the fundamental safety functions can be ensured and which can be maintained for a time sufficient to implement provisions to reach a *safe state*.

[14] IAEA SSR-2.1: Plant state, following an *anticipated operational occurrence* or accident conditions, in which the reactor is subcritical and the fundamental safety functions can be ensured and stably maintained for long time.

Table 1. Examples of postulated common cause failures of safety systems needed to fulfil a safety function necessary to cope with an AOO or a single PIE.

Denotation	Postulated Initiating Event	Loss of a safety system
LOCA	Small LOCA	Medium head safety injection
	Small LOCA	Low head safety injection
Station blackout	Loss of off-site power	Emergency power supply
Total loss of feed water	Loss of main feed water	Emergency feed water supply
ATWS	Anticipated Transient	Fast shutdown

Table 2. Examples of postulated common cause failures of safety systems needed to fulfil the fundamental safety functions in normal operation

Denotation	Initiating condition	Loss of a system
Loss of RHR	*normal operation*	Residual heat removal
Loss of UHS	*normal operation*	Ultimate heat sink
Loss of CCW/ECW	*normal operation*	Component cooling water / essential cooling water
Loss of spent fuel pool cooling	*normal operation*	Spent fuel pool cooling

03.4 Position 4: Provisions to mitigate core melt and radiological consequences

Introduction

WENRA has issued safety objectives for new reactors including Objective O3 "Accidents with core melt":

> *reducing potential radioactive releases to the environment from accidents with core melt[15], also in the long term[16], by following the qualitative criteria below:*
>
> - *accidents with core melt which would lead to early[17] or large[18] releases have to be practically eliminated[19];*
> - *for accidents with core melt that have not been practically eliminated, design provisions have to be taken so that only limited protective measures in area and time are needed for the public (no permanent relocation, no need for emergency evacuation outside the immediate vicinity of the plant, limited sheltering, no long term restrictions in food consumption) and that sufficient time is available to implement these measures.*

Design provisions to deal with accidents with core melt

The goal behind Objective O3 is that the nuclear power plants have to be designed in such a way that even in case of an accident with core melt *only limited protective measures in area and time are needed for the public and that sufficient time is available to implement these measures*. Any reasonably achievable solution which would further reduce the radiation doses of workers or the population or environmental consequences should be implemented.

In such an accident, the reactor containment structure is the main barrier for protecting the environment from the radioactive materials. Thus, it is essential to maintain the integrity of this barrier throughout the course of such an accident. In addition to the containment structure there have to be complementary safety features included in the design of the plant and procedures implemented to mitigate the consequences of core melt accidents. Consequently, the containment and the core melt management systems have to be designed to comply with Objective O3 and to keep radioactive releases during the severe accident conditions starting from all operational states as low as reasonably practicable. Any event resulting in a situation where Objective O3 is not fulfilled is considered a failure of the containment function.

---

[15] *Core melt accidents (severe accidents) have to be considered when the core is in the reactor, but also when the whole core or a large part of the core is unloaded and stored in the fuel pool. It has to be shown that such accident scenarios are either practically eliminated or prevented and mitigated.*

[16] *Long term: considering the time over which the safety functions need to be maintained. It could be months or years, depending on the accident scenario.* This definition is different from the long term restrictions in food consumption, which is interpreted in the last section of this appendix.

[17] *Early releases: situations that would require off-site emergency measures but with insufficient time to implement them.*

[18] *Large releases: situations that would require protective measures for the public that could not be limited in area or time.*

[19] *In this context, the possibility of certain conditions occurring is considered to have been practically eliminated if it is physically impossible for the conditions to occur or if the conditions can be considered with a high degree of confidence to be extremely unlikely to arise (from IAEA SSR 2.1).* Section 3.5 deals with the issue "Practical elimination" in more detail.

Provisions have to be taken to prevent accidents which would require protective actions for the public that could not be considered as limited in area and time (large release) and also to prevent accidents which would require protective actions for the public for which there would not be sufficient time to implement these measures (early release). These provisions have to make such accidents physically impossible to occur or to make it possible to consider with high degree of confidence that they are extremely unlikely to arise. Section 3.5 on "Practical Elimination" discusses this topic including examples of containment bypass and fuel melt sequences in the spent fuel pools.

In order to reliably maintain the containment barrier:

- Complementary safety features (DiD level 4) specifically designed for fulfilling safety functions required in postulated core melt accidents shall be independent to the extent reasonably practicable from the SSCs of the other levels of DiD. Independence of DiD levels is discussed in Section 3.2;
- Complementary safety features specifically designed for fulfilling safety functions required in postulated core melt accidents shall be safety classified and adequately qualified for the core melt accident environmental conditions for the time frame for which they are required to operate;
- The systems and components necessary for ensuring the containment function in a core melt accident shall have reliability commensurate with the function that they are required to fulfil. This may require redundancy of the active parts;
- It shall be possible to reduce containment pressure in a controlled manner in a long term taking into account the impact of non-condensable gases;
- If a containment venting system is included in the design, the safety margins in containment dimensioning shall be such that it should not be needed in the early phases[20] of the core melt accident, to deal with the containment pressure due to the non-condensable gases accumulating in the containment;
- Containment heat removal during core melt accidents shall be ensured. If included in the design, the containment venting system shall not be designed as the principal means of removing the decay heat from the containment;
- The strength of the containment including the access openings, penetrations and isolation valves shall be high enough to withstand, with sufficient margins to consider uncertainties, static and dynamic loads during core melt accidents that have not been practically eliminated (pressure, temperature, radiation, missile impacts, reaction forces). There shall be appropriate provisions to prevent the damage of the containment due to combustion of hydrogen;

In order to reduce the release of radioactive substances:

- there shall be provisions to reduce the amount of fission products in the containment atmosphere in case of the core melt accident;
- there shall be provisions to reduce the pressure inside the containment;

[20] Early phase is considered to last until the amount of radioactive material in the containment atmosphere has decreased significantly.

- if a containment venting system is included in the design to reduce the containment pressure in a core melt accident, it shall have a filtering capability;
- the containment penetrations should be surrounded by secondary structures to collect the potential leakages from the containment.

Any instrumentation required to decide on countermeasures shall be included in the design. This instrumentation shall be safety classified, adequately qualified for environmental conditions and it shall have reliability commensurate with the function that it is required to fulfil.

Analysis methodology

To show that the safety objective is reached, two complementary approaches are needed: deterministic and probabilistic. The following deals with scenarios that are not practically eliminated from the design point of view. The topic of practical elimination is discussed in Section 3.5 in more detail.

Deterministic analyses shall cover core melt scenarios starting from all operational states. Postulated core melt accidents are typically considered with realistic assumptions and best estimate methodologies. Adequate methods have to be utilised in order to show the robustness and reliability of the approach. On-site and off-site radiological consequences shall be analysed using stated and justified assumptions. Any possible influence from and on other nuclear facilities in the vicinity of the plant shall be analysed.

The probabilistic safety assessment (PSA) is complementary to the deterministic analyses. Comprehensive level 2 PSA of sufficient scope shall be carried out to demonstrate that the containment function can be shown to be reliable to meet Objective O3. PSA shall also be used to demonstrate that the selection of accident sequences for deterministic calculations is adequate for the design of severe accident provisions.

Intervention levels

These protective measures of sheltering, iodine prophylaxis, evacuation, and permanent relocation are associated with Generic Intervention Levels, which are used for emergency preparedness planning in the 5th level of the defence in depth. Such intervention levels have already been enforced by EU members in their national regulation to comply with Directive 96/29/Euratom - 13 may 1996 – article 50.2., and are consistent with the ICRP recommendations and IAEA GS-R-2. However, the intervention levels are not fully harmonised between European countries and there are some quantitative differences. Maximum admissible levels are set for food marketing in Europe.

In emergency preparedness planning, certain areas are defined around nuclear power plants for which arrangements are made for taking urgent protective actions of sheltering, evacuation, and iodine prophylaxis in case of an accident. IAEA GS-R-2 (2002) and GS-G-2.1 (2007) documents define the following zones:

(1) A precautionary action zone (PAZ, with the suggested radius of 3–5 km for reactors rated more than 1000 MW_{th}) is an area for which precautionary urgent protective action shall be taken before a release of radioactive material occurs or shortly after a release of radioactive material begins in order to reduce substantially the risk of severe deterministic health effects;
(2) An urgent protective action planning zone (UPZ, with the suggested radius of 5–30 km for reactors rated more than 1000 MW_{th}) is an area for which urgent protective action

shall be taken promptly in order to prevent stochastic effects and avert doses in accordance with international standards.

WENRA interpretation of limited protective measures

To achieve Objective O3, it is expected that the off-site radiological impact of accidents with core melt which are not practically eliminated only leads to limited protective measures in area and time (no permanent relocation, no long term restrictions in food consumption, no need for emergency evacuation outside the immediate vicinity of the plant, limited sheltering). Iodine prophylaxis is not mentioned in Objective O3 list of protective measures, but it shall also be limited in area and time. Sufficient time shall be available to implement these measures.

For the design stage of a nuclear power plant, to achieve Objective O3 on the 4th level of the defence in depth, the following interpretations of limited protective measures are provided (specified zones are not meant to be used for emergency preparedness planning):

(1) Immediate vicinity of the plant: For new reactors, the design should be such that the possible release of radioactive substances in a postulated core melt accident, based on the analysed consequences of the accident, will not initiate a need for emergency evacuation beyond the immediate vicinity of the plant. The design goal should aim at having a radius of this immediate vicinity zone towards the lower end of the suggested PAZ range i.e. 3 km (evacuation zone).

(2) Limited sheltering and iodine prophylaxis: For new reactors, the design goal should be such that the possible release of radioactive substances in a postulated core melt accident, based on the analysed consequences of the accident, will not initiate a need for sheltering and iodine prophylaxis beyond the zone towards the lower end of the suggested UPZ range i.e. 5 km (sheltering zone).

(3) No long-term restrictions in food consumption: This is interpreted so that after a postulated core melt accident, based on the analysed consequences of the accident, agricultural products beyond the sheltering zone should generally be consumable after the first year following the accident.

(4) Sufficient time: Sufficient time is interpreted so that protective measures should be initiated early enough. Especially the evacuation shall be carried out already when there is a threat of a significant radioactive release into the environment. Sufficient time to implement these protective measures is different for each measure and for each accident scenario and depends on the location of the reactor. Sufficient time for each measure shall be estimated and considered in the design of a reactor and during the site licensing.

Table 3 below summarises the interpretation of limited protective measures of evacuation, sheltering and iodine prophylaxis to be applied as goals in the design phase of new reactors. The zones for emergency preparedness planning, which take into account plant location and population living nearby, are usually larger because they are based on conservative approaches to protect people (for example, it could be assumed that some DiD level 4 provisions could partially fail).

Table 3. Design goals for areas where limited protective measures may be needed.

Measure	Evacuation zone	Sheltering zone	Beyond sheltering zone
Permanent relocation	No	No	No
Evacuation	May be needed	No	No
Sheltering	May be needed	May be needed	No
Iodine Prophylaxis	May be needed	May be needed	No

As for doses to the public or level of contamination to foodstuff, the definition of quantitative values associated to qualitative goals of Objective O3 is difficult since the analysis methodologies of radiological consequences might be based on different national regulations and practices including calculation models and hypothesis.

In addition to the design goals related to limited protective measures, ALARA principle shall be applied and any reasonably achievable measure which would further reduce the radiation doses of workers or the population or environmental consequences should be implemented.

03.5 Position 5: Practical elimination

Introduction

WENRA has issued safety objectives for new reactors including Objective O3 "Accidents with core melt":

- reducing potential radioactive releases to the environment from accidents with core melt, also in the long term, by following the qualitative criteria below:
  - accidents with core melt which would lead to early or large releases have to be practically eliminated;
  - for accidents with core melt that have not been practically eliminated, design provisions have to be taken so that only limited protective measures in area and time are needed for the public (no permanent relocation, no need for emergency evacuation outside the immediate vicinity of the plant, limited sheltering, no long term restrictions in food consumption) and that sufficient time is available to implement these measures.

Here the scope of "core melt" includes the nuclear fuel at fuel storage locations, as described in the WENRA publication on safety objectives: "Core melt accidents (severe accidents) have to be considered when the core is in the reactor, but also when the whole core or a large part of the core is unloaded and stored in the fuel pool. It has to be shown that such accident scenarios are either practically eliminated or prevented and mitigated". Here, "core melt" also includes severe degradation due to mechanisms other than melting, since radioactive releases can occur without melting (e.g. severe reactivity increase accidents).

Accident sequences that are practically eliminated have a very specific position in the Defence-in-Depth approach because provisions ensure that they are extremely unlikely to arise so that the mitigation of their consequences does not need to be included in the design. The justification of the "practical elimination" should be primarily based on design provisions where possible strengthened by operational provisions (e.g. adequately frequent inspections). All accident sequences which may lead to early or large radioactive releases must be practically eliminated.

An early release means a release that would require off-site emergency measures but with insufficient time to implement them. A large release means situations that would require protective measures for the public that could not be limited in area or time.

Means of Practical Elimination

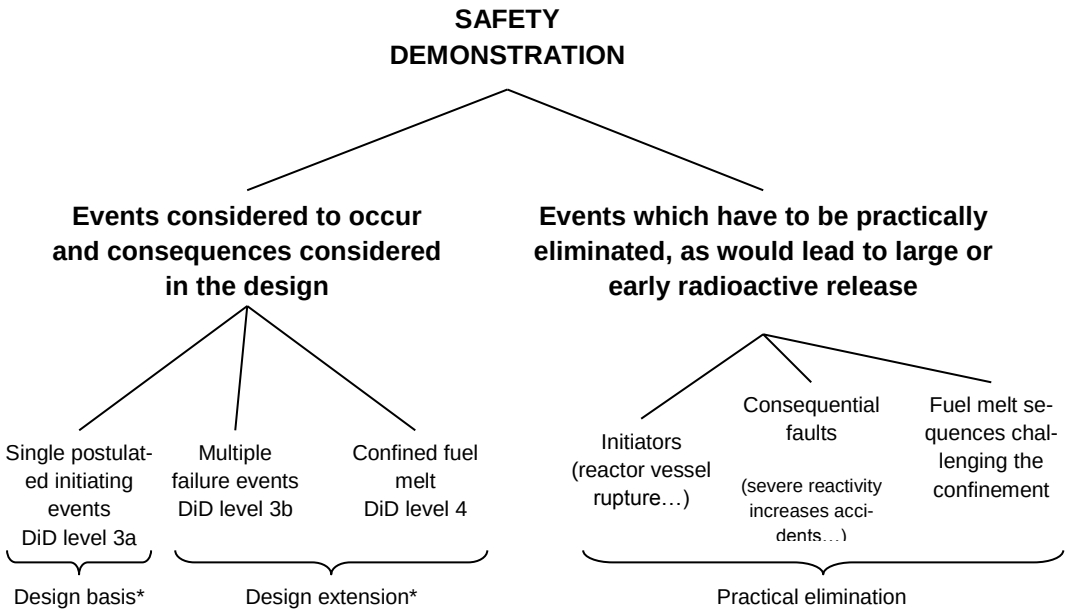
Accident sequences with a large or early release can be considered to have been practically eliminated:

(1) if it is physically impossible for the accident sequence to occur or
(2) if the accident sequence can be considered with a high degree of confidence to be extremely unlikely to arise (from IAEA SSR-2/1).

In each case the demonstration should show sufficient knowledge of the accident condition analysed and of the phenomena involved, substantiated by relevant evidence.

To minimize uncertainties and to increase the robustness of a plant's safety case, demonstration of practical elimination should preferably rely on the criterion of physical impossibility, rather than the second criterion (extreme unlikelihood with high confidence).

Accident sequences to be considered for Practical Elimination



* Comparable to IAEA SSR 2.1

Identification of accident sequences that have the potential to cause a large or early release should be based on deterministic analyses, supported by engineering judgment, and probabilistic assessment. These analysis approaches in the safety justification have to be adapted to each particular situation.

Important examples where consideration of severe accidents conditions should be aimed at practically eliminating large or early releases include those:

Unacceptable initiating faults:

- rupture of major pressure retaining components, e.g. reactor vessel.

Unacceptable consequential faults:

- large reactivity insertions directly leading to severe core degradation;
- internal hazard leading to severe core degradation (heavy load drops or internal flooding);
- fuel melt in an unconfined spent fuel pool situation[21].

[21] Also in confined spent fuel pool situations, fuel melt should be practically eliminated unless it can be demonstrated that there will be no large or early releases.

Fuel melt sequences challenging the confinement

- whilst at load that could damage the containment in an early phase as a result of direct containment heating, steam explosion or hydrogen detonation;
- whilst at load that could damage the containment in a late phase as a result of base mat melt-through or containment over pressurization;
- when in the shutdown state whilst the containment is open or severe accident mitigating measures are out of service;
- at all times when loss of confinement is caused by containment bypass, e.g. rupture of a steam generator tube, isolation valves are open or an interfacing system LOCA.

Different mechanisms and phenomena that could threaten the containment integrity during an accident with fuel melt, or due to the initiating event, have to be studied. It has to be shown that the failure of the containment function resulting from these events is practically eliminated. This requires reliability of the complementary safety features to manage the threats, as well as deterministic analyses of each mechanism and phenomenon, which need to be supported by adequate experimental results. Deterministic analyses are used to show that the containment function is fulfilled under design conditions of the containment including the expected conditions for the sequences which have not been practically eliminated, leading only to limited protective measures. Deterministic and probabilistic analyses are used to show that conditions leading to failure of the containment function due to physical phenomena or system failures are practically eliminated.

Deterministic analyses shall cover the expected course of severe accident scenarios. They are carried out with realistic assumptions and best estimate methodologies. Parameter variations have to be utilised in order to show the robustness and reliability of the approach. The probabilistic risk assessment is an essential supplement for the deterministic analyses. Analyses shall cover all the plant states (power operation, refuelling outages, maintenance, etc.) as well as different initiating event classes (internal events, fire, seismic events …).

Accident sequences with core melt resulting from external hazards which would lead to early or large releases should be practically eliminated.

Safety demonstration

Demonstration of Practical Elimination via Physical Impossibility

Demonstration of physical impossibility, based on engineered provisions, can be difficult. Care must be taken to recognize that some claims for practical elimination may be based on assumptions (e.g. non-destructive testing, inspection) and those assumptions need to be acknowledged and addressed. For engineered provisions this can be done by excluding the certain feature from the design making further development of accident scenario impossible (accident sequence cut-off).

A very simple example of a physically impossible situation is the case of a 10 m high load drop to ground level which is not possible from a crane at ground level with a maximum lift height of 5m. Most cases however are not so simple to consider, but representative examples are:

- in the reactor core design negative reactivity feedback protects the plant against a self accelerating reactivity accident;
- eliminating from the design those component features and/or failures which may initiate specific accident sequences. For example designing the spent fuel pools in such a way that the coolant cannot escape the pools.

Demonstration of Practical Elimination as extremely unlikely with a high degree of confidence

(1) The degree of substantiation provided for a practical elimination demonstration should take account of the assessed frequency of the situation to be eliminated and of the degree of confidence in the assessed frequency (uncertainties associated with the data and methods shall be evaluated in order to underwrite the degree of confidence claimed). Appropriate sensitivity studies should be included to confirm that sufficient margin to cliff edge effects exist. For engineered provisions the practical elimination can be done for instance by providing substantial increase of the protective means reliability.

(2) Practical elimination of an accident sequence cannot be claimed solely based on compliance with a general cut-off probabilistic value. Even if the probability of an accident sequence is very low, any additional reasonably practicable design features, operational measures or accident management procedures to lower the risk further should be implemented.

(3) The most stringent requirements regarding the demonstration of practical elimination should apply in the case of an event/phenomenon which has the potential to lead directly to a severe accident, i.e. to pass from DiD level 1 to level 4. For example demonstration of practical elimination of a heterogeneous boron dilution fault would require a detailed substantiation. Good examples of such detailed substantiation already exist in the form of cases made to exclude reactor vessel failure.

(4) It must be ensured that the practical elimination provisions remain in place and valid throughout the plant lifetime. For example, in-service inspection and other periodic checks may be necessary.

(5) All codes and calculations must be validated against the specific phenomena in question and verified.

03.6 Position 6: External hazards

Introduction

This section provides a common position on the consideration of external hazards for new reactors. The purpose is to provide high level guidance on regulatory expectations on how external hazards should be considered in the design and siting of new reactors.

Here the external hazards of concern are those natural or man-made hazards to a site and facilities that originate externally to both the site and its processes, i.e. the licensee may have very little or no control over the initiating event. Malicious actions are not included in the scope of this study.

The assessment of natural external hazards requires knowledge of natural processes, along with plant and site layout. In contrast with almost all internal faults or hazards, external hazards may simultaneously affect the whole facility, including back up safety systems and non-safety systems alike. In addition, the potential for widespread failures and hindrances to human intervention may occur. For multi-facility sites this makes the generation of safety cases more complex and requires appropriate interface arrangements to deal with common equipment or services as well as potential domino effects.

Safety Expectations

The safety assessment for new reactors should demonstrate that threats from external hazards are either removed or minimised as far as reasonably practicable.

This may be done by showing that all relevant safety Structures, Systems and Components (SSCs)[22] required to cope with an external hazard are designed and adequately qualified to withstand the conditions related to that external hazards.

External Hazards considered in the *general design basis*[23] of the plant should not lead to a core melt accident (Objective O2 i.e. level 3 DiD).

Accident sequences with core melt resulting from external hazards which would lead to early or large releases should be practically eliminated (Objective O3 i.e. level 4 DiD). For that reason*, rare and severe external hazards*[24], which may be additional to the *general design basis*, unless screened out (see "Screening of External Hazards" below), need to be taken into account in the overall safety analysis.

For new reactors external hazards should be considered as an integral part of the design and the level of detail and analysis provided should be proportionate to the contribution to the overall risk.

---

[22] The words "all relevant safety Structures, Systems and Components (SSCs)" has the same meaning as "items important to safety" in IAEA's terminology.

[23] The *general design basis* is that used to define the events that have been taken into account in the design and associated design basis analysis

[24] Rare and severe external hazards are additional to the *general design basis*, and represent more challenging or less frequent events. This is a similar situation to that between Design Basis Conditions (DBC) and Design Extension Conditions (DEC); they need to be considered in the design but the analysis could be realistic rather than conservative.

Safety Demonstration

A number of stages are envisaged:

- Identification
- Screening
- Determination of hazard parameters
- Analysis

Identification of External Hazards

The first step in addressing the threats from external hazards is to identify those that are of relevance to the site and facility under consideration. Any identified external hazard that could affect a facility should be treated as an event that can give rise to possible initiating events.

The list of external hazards to be considered should be as complete as possible and include all of the hazards mentioned in the relevant IAEA sources[25]. These sources have been combined to produce a consistent and coherent list which is included in the end of this section. This generic list is a starting point and it is expected that it would be augmented by any site specific hazards not included. The overall demonstration should include justification that the list (generic + site specific) is complete and relevant to the local site.

Screening of External Hazards

Screening is used to select the External Hazards that should be analysed. The screening process should take as a starting point the complete list discussed in the previous section. Each external hazard on the list should be considered and selected for analysis if:

a. It is physically capable of posing a threat to nuclear safety, and
b. the frequency of occurrence of the external hazard is higher than pre-set criteria.

The pre-set frequency criteria may differ depending on the nature of the analysis that is to be undertaken. Typically for the *general design basis*, where the analysis will be done using traditional conservative methods, assumptions and data, the criterion will be higher than the frequency criteria used for analyses of *rare and severe external hazards* or PSA that could employ realistic, best estimate methods and data. Therefore the screening process may lead to separate, but compatible lists of external hazards for the range of analyses to be undertaken and there should be a clear and consistent rationale for the differences in the lists.

In all cases the pre-set frequency criteria used should be stated and justified taking into account the way the hazards are going to be analysed in the safety demonstration.

The degree of confidence of the estimated frequency of occurrence should be stated and justified taking into account the related uncertainties according to the state of knowledge.

The screening process should explicitly consider correlated events and combinations of events.

[25] See Safety Series Standards NS-R-3, NS-G-3.1, NS-G-3.3, NS-G-3.6, NS-G-1.5, NS-G-1.6 and relevant events in SSG-3 and SSG-18

Determination of hazard parameters

All of the candidate external hazards that are selected should be characterised in terms of their severity and/or magnitude and duration. The characterisation of the external hazard will depend on the type of analysis that is to be carried out and shall be conservative for the *general design basis* analysis and could be realistic/best estimate for *rare and severe external hazards* analysis and PSA. It should be noted that for external hazards PSA, a range of frequencies and associated hazard parameters is often required. All relevant characteristics need to be specified and the rationale for their selection justified. For some external hazards:

- the ability to forecast the magnitude and timing of the event, and the speed at which the event develops may be relevant and should be considered;
- several parameters could be relevant to characterize severity and/or magnitude.

Analysis Considerations

The external hazards analysis includes the design of SSCs which are relevant to ensuring that the fundamental safety functions are fulfilled, development of probabilistic models where necessary, and the consideration of *rare and severe external hazards*. The following should be considered when undertaking this analysis:

- Minimising the risk from external hazards by initial siting of the facility
- Designing plant layout to minimise impact of external hazards (this is particularly important for multi unit facilities – also where units are of different generation)
- Justification of the lists of identified external hazards
- Justification of any hazard screening
- Combinations of external hazards that can occur simultaneously or successively within a given period of time[26] including correlated hazards and those combinations which occur randomly
- Consideration of consequential events, such as fire or flooding following a seismic event
- External hazard induced multiple failure of safety systems and/or their support systems
- Cliff edge effects – where a small change in a parameter leads to a disproportionate increase in consequence.
- In addition to considering the impact of external hazards on the systems and components, the reliability of the buildings and structures responding to an external hazard should be taken into account.
- The PSA for external hazards should include consideration of building and structural reliability as well as system and component fragilities and should take account of the potential for human response to be affected by the external event.

[26] The given period of time means that subsequent hazards occur within the mission time of the induced fault sequence. The mission time is the time necessary to reach pre defined safe, stable condition and not an arbitrarily assumed value.

- Impact of climate change and other potential time related changes that might affect the site should be considered
- Consideration should also be given to the impact of external hazards on the ability to support (emergency services) the site damaged by that external event (relevant to DiD).
- The design of the plant should reflect the external hazards analyses. Similarly the operating and maintenance procedures as well as the training etc. should take account of the external hazards analyses.
- Care must be taken where the definition of the hazard levels is imprecise, and claims are made based on the accuracy of calculations which have an accumulation of assumptions and conservatisms (or lack of)
- A clear methodology is important, along with an understanding of the associated uncertainties, both epistemic and aleatory. This is particularly important where the work also supports numerical PSA based approaches and where it is used to screen out hazards.
- The use of generic fragilities should be treated with care, as failure mechanisms may not be similar for similar types of plant, despite appearances
- Large uncertainties in characterisation of the hazards, particularly those selected for *general design basis*, need to be addressed as part of "cliff edge" considerations and margin assessments
- Multiple unit sites may need additional consideration for common plant areas and mitigation

Standards and guides

The following documents provide appropriate information to guide detailed consideration of external hazards.

(1) IAEA Safety Standards Site Evaluation for Nuclear Installations Safety Requirements No. NS-R-3

(2) IAEA Safety Guide - External Events Excluding Earthquakes in the Design of Nuclear Power Plants - Safety Guide No. NS-G-1.5

(3) IAEA Safety Guide - Seismic Design and Qualification for Nuclear Power Plants Safety Guide Safety - Standards Series No. NS-G-1.6

(4) IAEA SSG 9 Specific safety guide: Seismic Hazards in Site Evaluation for Nuclear Installations. Aug 2010

(5) IAEA Safety Guide - Geotechnical Aspects of Site Evaluation and Foundations for Nuclear Power Plants Safety Guide - Safety Standards Series No. NS-G-3.6

(6) IAEA SSG-18 Meteorological and Hydrological Hazards in Site Evaluation for Nuclear Installations. (replaces NS-G-3.4 and NS-G-3.5)

(7) IAEA Safety Guide NSG 3.1 External Human induced events in site evaluation

(8) IAEA Safety Guide NSG 3.3 Evaluation of Seismic Hazards for Nuclear Power Plant

(9) IAEA SSG 3 Development and Application of Level 1 PSA for Nuclear Power Plants

(10) IAEA SSR-2/1 Safety of Nuclear Power Plants: Design

Generic list of External Hazards

Category	Hazard
Seismotectonic	Ground motion
	Long period ground motion
	Liquefaction
	Dynamic compaction
	Tsunami
	Volcano (includes other effects than seismic)
	Meteorite (includes other effects than seismic)
Flooding	Extreme Rainfall (note links to other meteorological phenomena)
	Tidal Effects
	Storm Surge
	Seiche
	Tsunami
	Dam Failure
	Watercourse containment failure
	Wind generated waves
Meteorological	High Wind (Tornado, Hurricane, Cyclone Typhoon) and wind blown debris
	Extreme Drought
	Extremes of Air Temperature
	Extremes of Ground Temperature
	Extremes of Sea (or river) Temperature
	Lightning
	Snow (snow pack and snow melt)
	Icing
	Hail
	Humidity
	Air pressure
	Sandstorm, dust storm
	Saltspray/saltstorm
	Snow avalanche
	Waterspouts
	Ice flows / Frazil
	Mist/Fog
	Solar flares
Man Made	Accidental Aircraft Impact
	Gas Clouds (toxic, asphyxiates, flammables)

Category	Hazard
	Liquid Releases (flammables, toxic, radioactive)
	Fires
	Explosions (blast waves, missiles)
	Missiles (turbines, bottles BLEVE)
	Structural Failure
	Transport (road, sea, rail)
	Electromagnetic Interference
	Pipelines (Gas, Oil, Water)
	Vibrations
	Space Debris
	Flotsam/ Jetsam
	Log jam
	Pollution (ground or water course)
	Electrical Eddy currents into ground
	Military Activity (Accidental)
	Residual artefacts from previous use (i.e. munitions)
Biological	Seaweed
	Fish
	Jellyfish
	Marine growth
	Crustaceans, molluscs (shrimps, clams, mussels, shells)
	Birds
Infestation	Airborne swarms
	Infestation by rodents and other animals
Geological	Settlement
	Ground heave
	Mining (inactive or active)
	Caverns/ natural cavities
	Groundwater
	Leeching
	Contaminated land
	Landslides
	Radon
	Fissures
	Faults
	Soluble Rocks
	Unstable Soils (quick clays etc.)
	Permafrost

03.7 Position 7: Intentional crash of a commercial airplane

Introduction

Accidental crashes of airplanes have been considered in the design of reactors for several decades. However, according to the estimated frequencies of crashes, only crashes of small airplanes and/or military airplanes were generally taken into account. After the September 11th, 2001 attack, the consequences of an intentional crash of a commercial airplane were then considered.

Despite measures taken to prevent the intentional crash of a commercial airplane[27], this event should be considered in the design of new reactors.

This event is considered by WENRA as a very significant example of the expectations regarding the improvement of the interface between safety and security issues, as stated in Objective O5.

Expected safety level

The general expectation is that such a crash should not lead to core melt and therefore not cause more than a minor radiological impact as stated in Objective O2. Nevertheless, in this specific situation, it is recognized that releases of radioactive materials could exceed those considered in other events not involving core melt. However, the consequences of this specific situation should remain within Objective O2.

Safety functions required to bring and maintain the plant in a safe state after such a crash shall be designed and protected adequately.

In particular, the following shall be ensured:

- Reactivity control, including reactor scram;
- Residual heat removal (including in the long term) from the core in the vessel and the fuel pool in order to exclude core or fuel melt;
- Confinement of radioactive materials, consistent with radiological consequences of Objective O2.

Key aspects of the safety demonstration which is expected from the licensees

Direct and indirect effects of the airplane crash shall be considered, in particular:

- effects of direct and secondary impacts on mechanical resistance of safety structures and systems required to bring and maintain the plant in a safe state after airplane crash;
- effects of vibrations on safety structures and systems required to bring and maintain the plant in a safe state after airplane crash;
- effects of combustion and/or explosion of airplane fuel on the integrity of the necessary structures and on the systems required to bring and maintain the plant in a safe state after airplane crash.

[27] Characterized by load/time curves.

Buildings or appropriate part of the buildings containing nuclear fuel and housing key safety functions should be designed to prevent airplane fuel from entering them. Fires caused by airplane fuel shall be assessed as different kinds of fire ball and pool fire combinations. Other consequential fires due to the airplane crash shall be addressed.

A realistic approach can be followed, using best estimate material properties and state-of-the-art analytical methods. Realistic failure criteria could be used. In addition it is not necessary to consider other coincident failure of plant and equipment. Sensitivity analysis shall be performed to confirm sufficient margin to cliff edge effects.

The effect of the event on the ability of plant personnel and off-site services to fulfil necessary actions shall be taken into account.

04
Lessons Learnt from the Fukushima Dai-ichi accident

A severe accident involving several units took place in Japan at Fukushima Dai-ichi nuclear power plant in March 2011. Even though in-depth analysis of this accident has not yet been completed, some items could be highlighted. The immediate cause of the accident was an earthquake followed by a tsunami coupled with inadequate provisions for tsunamis in the original design. Opportunities to improve protection against a tsunami were not adequately taken, which could have been possible for example as part of the PSR process.

Safety culture and organisational factors, including decision making capabilities, contributed to the inadequate protection of the plants and to the difficulties in accident management.

As a consequence of the tsunami, essential safety functions were lost at the plant, leading to core damage in three units and subsequently to considerable radioactive releases.

The Fukushima Dai-ichi accident demonstrates the importance of properly implementing the Defence-in-Depth principle to ensure safety, getting the design basis for external hazards right, providing adequate protection against external hazards and the need to ensuring strong PSR process together with independent regulatory body to drive it. The accident also confirmed the need to have comprehensive safety analysis using both deterministic and probabilistic methods in a complementary manner to provide as full coverage of all safety factors as possible. In the safety assessment specific considerations are needed for multi-unit sites and to address long term aspects.

The Fukushima Dai-ichi accident also demonstrates the importance of adequate on-site resources that are adequately qualified against external hazards and the effects of core melt accidents.

An important lesson from the accident was the importance of a control room and emergency response centre adequately protected against external hazards. Another key lesson was the need to attend to cooling and integrity of spent fuel pools as well as for the reactors. Siting has design implications, in particular in terms of securing sufficient diverse electrical and cooling supplies.

In general, one has to bear in mind that the specific nature of individual events and challenges can never be completely taken into account in design and operation of a nuclear power plant (or indeed any other industrial facility). However, a robust design based on DiD with sizeable safety margins and diverse means for delivering fundamental safety functions as well as comprehensive operator response plans will help to protect against the unanticipated.

Several studies have already been performed concerning the accident and detailed technical studies are still in progress in Japan and elsewhere. In the following conclusions on some es-

sential safety issues based on or reinforced by the lessons learnt from Fukushima Dai-ichi accident are presented, in relation with the positions detailed in Chapter 3.

04.1 External hazards

The Fukushima Dai-ichi accident has reinforced the need to undertake a comprehensive analysis of all external hazards as part of the design process for new nuclear power stations, and periodic safety reviews. In common with other parts of the safety demonstration, the external hazard analysis should cover all areas with significant amounts of radioactive material on the power station.

The Fukushima Dai-ichi accident has highlighted the need to take account of rare and severe hazards. External hazards are comprehensively considered in **Position 6**.

04.2 Reliability of safety functions

Lessons from the Fukushima Dai-ichi accident show the importance of proper implementation of the Defence-in-Depth (DiD) concept and a need for adequate protection of the plants against rare and severe external hazards.

External hazards are comprehensively considered in **Position 6**.

The defence in depth approach, independence of the levels of defence in depth, and multiple failure events are comprehensively considered in **Positions 1, 2 and 3**.

Decay heat removal

The nuclear power plant shall have arrangements to enable the decay heat removal in rare and severe hazards (**Position 6**). For this situation, protection of necessary electrical power supplies has to be ensured. Consistently with the DiD approach of **Position 1**, loss of the primary ultimate heat sink or access to it should be considered in the design. The primary and alternative means for decay heat removal in an emergency should function independently.

Ensuring the energy supply

Where safety functions of NPPs rely on AC power, diverse emergency AC power supply shall be required as a part of DiD sub-level 3.b additional safety features to cope with common cause failures of the primary emergency electrical power supply (**Positions 2 and 3**). Other actions for increasing the reliability of electrical power supply at NPPs deal with enhanced provisions of long term fuel and lubricating oil reserves for all emergency power units at the site and ensuring possibilities to use mobile power supply units. Adequate battery capacity shall be secured. This requires appropriate capacity of some critical batteries and may require improving possibilities to re-charge them.

The correct fail-safe position of safety related equipment in case of loss of energy supply needs to be considered in the design taking into account potential conflicting demands on this equipment.

04.3 Accidents with core melt

The Fukushima Dai-ichi accident confirms that accidents with core melt need to be considered in the design of NPPs. Complementary safety features (as defined in **Position 2**) which ensure the adequate integrity of the containment in case of an accident leading to a core melt need to be included in the design, as discussed in **Position 4**. Robust complementary safety features (DiD level 4) specifically designed for fulfilling safety functions required in postulated

core melt accidents should be independent to the extent reasonably practicable from the SSCs of the other levels of DiD, as discussed in **Position 2** and **Position 4**. Accidents with core melt which would lead to early or large releases should be practically eliminated. Analyses shall cover all the plant states (power operation, refueling, outages, maintenance etc.) as well as different initiating event classes (internal events, fire, seismic events, ...), as discussed in **Position 5**.

Essential design principles related to the Fukushima Dai-ichi accident deal with having a filtering capability for the containment venting if any, containment ultimate pressure strength and hydrogen management, also discussed in **Position 4**.

The need to manage large volumes of contaminated cooling water and filtered containment venting over longer periods of time should be included in the design and accident management considerations.

04.4 Spent fuel pools

The Fukushima Dai-ichi accident also highlighted the need for adequate safety and the design of spent fuel pools. This implies that single initiating events, multiple failure events (see **Position 3**), internal hazards as well as external hazards (see **Position 6**) should be properly addressed. In addition to having adequate instrumentation and control for the spent fuel pool, also under accident conditions, WENRA considers that both the defence in depth approach (see **Position 1**) and the practical elimination of accidents with early or large release (see **Position 5**) are fully applicable for fuel storage pools.

Once spent fuel in a pool is overheated, the further development is very difficult to assess. Thus the primary approach for spent fuel pools shall be to “practically eliminate” the possibility of extensive fuel damage due to mechanical, thermal or chemical effects. To achieve this it is essential to ensure the integrity of the spent fuel pools, and maintain sufficient water level in the pools. In addition, subcriticality of the fuel has to be ensured. The strategy to practically eliminate the fuel damages can take into account that time delays of spent fuel heating up in the case of loss of normal cooling systems usually are relatively long (unless the reactor core has been recently transferred into the pool). Practical elimination is discussed in **Position 5**.

The structural integrity of the spent fuel pools needs to be ensured, as needed to maintain sufficient water level in the pools in case of rare and severe external hazards.

04.5 Safety assessment

A strong periodic safety review (PSR) process is very important for continuous improvement of safety of nuclear power plants. In the event that PSR results indicate the need for improvement measures, it is vital that the measures are defined and implemented in an effective manner.

Long term accident mitigation measures should be considered in deterministic and probabilistic safety assessments and consideration given to the reliability and sustainability of the measures.

On multi-unit sites, the plant should be considered as a whole in safety assessments and interactions between different units need to be analysed. Hazards that may affect several units need to be identified and included in the analysis.

04.6 Emergency preparedness in design

The Fukushima Dai-ichi accident showed that events disrupting the regional infrastructure and affecting several units at the same site can have a significant adverse impact on the implementation of the required accident management actions.

The accessibility, functionability and habitability of the control room and of the emergency response centre have to be ensured. This will require adequate protection against rare and severe external hazards. Suitably shielded and protected spaces shall be provided to house necessary workers under postulated core melt accident conditions. The accessibility of local control points required for manual actions also has to be ensured.

The reliability and functionality of the on-site and off-site communication systems, equipment measuring releases, radiation levels and meteorological conditions need to be ensured, taking into account conditions related to rare and severe external hazards.

Annex 1
WENRA Statement on Safety Objectives for new Nuclear Power Plants, November 2010

Foreword

One of the objectives of WENRA, as stated in its terms of reference, is to develop a harmonized approach to nuclear safety and radiation protection issues and their regulation.

A significant contribution to this objective was the publication, in 2006[28], of a report on harmonization of reactor safety in WENRA countries. This report addresses the nuclear power plants that were in operation at that time in those countries; it includes about 300 "Reference Levels"[29].

Since then, the construction of new nuclear power plants has begun or is being envisaged in the short term in several European countries.

Hence, it has been considered timely for WENRA to define and express a common position on the safety objectives of new nuclear power plants, so that:

- new nuclear power plants to be licensed across Europe in the next years will be safer than the existing ones, especially through improvements of the design;
- regulators press for safety improvements in the same direction and ensure that these new plants will have high and comparable levels of safety;
- applicants take into account this common position when formulating their regulatory submissions.

A report "Safety objectives for new power reactors – study by RHWG – December 2009" has been published by WENRA in January 2010 for stakeholders' comments. Comments received were considered one by one either in establishing the present statement (e.g. comments on the safety objectives themselves) or as an input for the ongoing WENRA work related to new nuclear power plants. In particular, some clarifications were made to the safety objectives stated in the December 2009 study. These seven safety objectives in their final wording (November 2010), as decided by WENRA, are stated below. They will be the basis for further harmonization work.

Improving the protection of people and of the environment

[28] Harmonization of Reactor Safety in WENRA countries, report by RHWG, January 2006

[29] These "Reference Levels" were updated in January 2008

WENRA considers that the design of new nuclear power plants shall take into account the operating experience feedback, lessons learnt from accidents, developments in nuclear technology and improvement in safety assessment.

The safety objectives for new nuclear power plants have been defined on the basis of a systematic investigation of the Fundamental Safety Principles (SF-1 document issued 2006 by the IAEA). Grounding the safety objectives on the fundamental safety principles has been explained in the December 2009 study[30].

The safety objectives address new civil nuclear power plant projects. However, these objectives should be used as a reference for identifying reasonably practicable safety improvements for "deferred plants"[31] and existing plants during periodic safety reviews.

These safety objectives are formulated in a qualitative manner[32] to drive design enhancements for new plants with the aim of obtaining a higher safety level compared to existing plants. For instance,

- to be able to comply with the qualitative criteria proposed in following Objective O3, the confinement features should be designed to cope with core melt accidents, even in the long term;
- these safety objectives call for an extension of the safety demonstration for new plants, in consistence with the reinforcement of the defence in depth. Some situations that are considered as "beyond design" for existing plants, such as multiple failures conditions and core melt accidents, are considered in the design of new plants.

Based on these safety objectives, WENRA is currently developing positions on selected key issues for the design of new nuclear power plants.

WENRA considers that these safety objectives reflect the current state of the art in nuclear safety and can be implemented at the design stage using the latest available industrial technology of nuclear power plants.

However, since nuclear safety and what is considered adequate protection are not static entities, these safety objectives may be subject to further evolution. As technology and scientific knowledge advance, WENRA deems these safety objectives should be reviewed no later than 2020.

[30] In particular, in line with fundamental safety principle 5 "optimization of protection", the safety of new reactors will have to be improved as far as reasonably achievable starting from the design stage, taking into consideration the state of the art and by taking into account all circumstances of individual cases, as defined in SF-1, para. 3.23 (related objectives are O1 to O4 and O6)

[31] Plant project originally based on design similar to currently operating plants, the construction of which halted at some point in the past and is now being completed with more modern technology

[32] WENRA considered quantitative safety objectives but concluded that they would not be more informative than qualitative objectives with associated safety expectations. It was also recognized that the use of quantitative safety goals needs some prerequisites, such as the development of standardized methodologies. Furthermore, compliance with a numerical value may not be enough.

WENRA Safety Objectives for New Nuclear Power Plants

Compared to currently operating nuclear power plants, WENRA expects new nuclear power plants to be designed, sited, constructed, commissioned and operated with the objectives of:

O1. Normal operation, abnormal events and prevention of accidents

- reducing the frequencies of abnormal events by enhancing plant capability to stay within normal operation.
- reducing the potential for escalation to accident situations by enhancing plant capability to
  control abnormal events.

O2. Accidents without core melt

- ensuring that accidents without core melt induce[33] no off-site radiological impact or only minor radiological impact (in particular, no necessity of iodine prophylaxis, sheltering nor evacuation[34]).
- reducing, as far as reasonably achievable,
  - the core damage frequency taking into account all types of credible hazards and failures and credible combinations of events;
  - the releases of radioactive material from all sources.
- providing due consideration to siting and design to reduce the impact of external hazards and malevolent acts.

[33] In a deterministic and conservative approach with respect to the evaluation of radiological consequences.

[34] However, restriction of food consumption could be needed in some scenarios.

O3. Accidents with core melt

- reducing potential radioactive releases to the environment from accidents with core melt[35], also in the long term[36], by following the qualitative criteria below:
    - accidents with core melt which would lead to early[37] or large[38] releases have to be practically eliminated[39];
    - for accidents with core melt that have not been practically eliminated, design provisions have to be taken so that only limited protective measures in area and time are needed for the public (no permanent relocation, no need for emergency evacuation outside the immediate vicinity of the plant, limited sheltering, no long term restrictions in food consumption) and that sufficient time is available to implement these measures.

O4. Independence between all levels of defence-in-depth

- enhancing the effectiveness of the independence between all levels of defence-in-depth, in particular through diversity provisions (in addition to the strengthening of each of these levels separately as addressed in the previous three objectives), to provide as far as reasonably achievable an overall reinforcement of defence-in-depth.

O5. Safety and security interfaces

- ensuring that safety measures and security measures are designed and implemented in an integrated manner. Synergies between safety and security enhancements should be sought.

[35] For new plants, the scope of the safety demonstration has to cover all risks induced by the nuclear fuel, even when stored in the fuel pool. Hence, core melt accidents (severe accidents) have to be considered when the core is in the reactor, but also when the whole core or a large part of the core is unloaded and stored in the fuel pool. It has to be shown that such accident scenarios are either practically eliminated or prevented and mitigated.

[36] Long term: considering the time over which the safety functions need to be maintained. It could be months or years, depending on the accident scenario.

[37] Early releases: situations that would require off-site emergency measures but with insufficient time to implement them.

[38] Large releases: situations that would require protective measures for the public that could not be limited in area or time.

[39] In this context, the possibility of certain conditions occurring is considered to have been practically eliminated if it is physically impossible for the conditions to occur or if the conditions can be considered with a high degree of confidence to be extremely unlikely to arise (from IAEA NSG1.10).

O6. Radiation protection and waste management

- reducing as far as reasonably achievable by design provisions, for all operating states, decommissioning and dismantling activities:
    - individual and collective doses for workers;
    - radioactive discharges to the environment;
    - quantity and activity of radioactive waste.

O7. Leadership and management for safety

- ensuring effective management for safety from the design stage. This implies that the licensee:
    - establishes effective leadership and management for safety over the entire new plant project and has sufficient in house technical and financial re-sources to fulfil its prime responsibility in safety;
    - ensures that all other organizations involved in siting, design, construction, commissioning, operation and decommissioning of new plants demonstrate awareness among the staff of the nuclear safety issues associated with their work and their role in ensuring safety.

WENRA
WESTERN EUROPEAN NUCLEAR REGULATORS ASSOCIATION

RHWG
REACTOR HARMONISATION WORKING GROUP

WGWD
WORKING GROUP ON WASTE AND DECOMISSIONING