An Integrated Safety Assessment Methodology (ISAM) for Generation IV Nuclear Systems

Risk and Safety Working Group (RSWG)

Version 1.1 – June 2011

The content of this RSWG report was presented in a workshop with the six GIF – Systems Steering Committees held on 12-13 April 2010 in Petten. A first version of this report was then distributed for comments and suggestions from the GIF - Expert Group and the GIF – Systems Steering Committees on 18 June 2010.

This revised version takes into account comments received from the GIF Expert Group and GIF – Systems Steering Committees on the first version. This version was approved at the 14th RSWG meeting (11 April 2011) for being forwarded to the GIF – Expert Group

Moreover, even endorsed, the document does not engage the designers. The latter are clearly unloaded of any commitment with regard to the practices, the principles and objectives as they are suggested by the RSWG."

PREFACE REGARDING THE 11 MARCH 2011 JAPANESE EARTHQUAKE AND ACCIDENT AT THE FUKUSHIMA DAIICHI NUCLEAR POWER STATION

On 11 March 2011, a magnitude 9.0 earthquake and several large aftershocks struck the country of Japan, causing massive destruction, widespread loss of life, and extensive human suffering. This earthquake, the largest ever recorded in Japan, along with the resulting tsunami, caused severe damage to the Fukushima Daiichi nuclear power site. Although many details and the full consequences associated with this catastrophe will not be known for some time, it is known that significant core damage occurred in three of the Fukushima Daiichi reactors, resulting in widespread radioactive contamination.

A number of detailed analyses and "lessons learned" investigations will be performed in the months and years to come. It is highly likely that the results of some of these analyses may have implications for the development and deployment of Generation IV nuclear systems. It is also likely that some of these analyses may have implications for how to ensure that the scope and depth of Generation IV safety assessments are carried out in a sufficiently robust way as to understand system vulnerabilities under a very broad range of accident conditions, including some that might formerly have been deemed so unlikely as to preclude their consideration. Without the benefit of such detailed analyses, at the time of publication of this document, it is too early to know how safety philosophies and assessment methods including the Integrated Safety Assessment Methodology will need to be modified or updated based on lessons that will be learned from the Fukushima experience. In our future program of work, the Generation IV Risk and Safety Working Group intends to closely monitor events at the Fukushima site, as well as lessons learned from those events, in order evaluate how those lessons can best shape our approach to assessing and ensuring the safety of Generation IV systems. Future updates to this Integrated Safety Assessment Methodology document will include consideration of those lessons and findings.

Risk and Safety Working Group
June 2011

Table of contents

Executive Summary 7

1. Introduction 11
1.1 - The Role of an Integrated Safety Assessment Methodology 11
1.2 - Attributes of an Effective Safety Assessment Methodology 11
1.3 - Human Factors Considerations 13
1.4 - ISAM Overview 13
1.4.1 Qualitative Safety Features Review (QSR) 14
1.4.2 Phenomena Identification and Ranking Table (PIRT) 15
1.4.3 Objective Provision Tree (OPT) 15
1.4.4 Deterministic and Phenomenological Analyses (DPA) 16
1.4.5 Probabilistic Safety Analysis (PSA) 16
1.4.6 Integration of ISAM Elements 17
1.5 - Resources Required to Implement ISAM 18

2. Elements of an Integrated Safety Assessment Methodology (ISAM) 21
2.1 - Qualitative Safety Features Review (QSR) 21
2.1.1 - Introduction 21
2.1.2 - The elaboration of the qualitative recommendations for the assessment 21
2.1.3 - Guidelines for the design and the assessment 22
2.1.4 - Defence in Depth (DiD) implementation 24
2.1.5 - Safety recommendations 25
2.1.6 - Qualitative Safety Features Review (QSR) 26
2.1.7 - Conclusions on the QSR 26
2.2 - Phenomena Identification and Ranking Tables 28
2.2.1 - Introduction 28
2.2.2 - Description of PIRT 28
2.2.3 – The Individual Steps Used in PIRT 28
2.2.4 - Anticipated Results 29
2.2.5 - Anticipated Issues 30
2.2.6. - Conclusions on the PIRT 31
2.3 - Objective Provision Trees for assessment of adequacy of Defence-in Depth (DiD) 33
2.3.1 – Introduction 33
2.3.2 - Description of OPT 33
2.3.3 - Major inputs and outputs of OPT 38
2.3.4 - Anticipated Results and Applications 38
2.3.5 - Recognized or Anticipated Issues 39
2.4 - Application of Deterministic and Phenomenological Analyses (DPA) 40
2.4.1 – Brief description of DPA 40
2.4.2 - Major inputs and outputs 42
2.4.3 - Recognized or Anticipated Issues 43
2.5 - Probabilistic Safety Assessment 44
2.5.1 Introduction 44
2.5.2 Description 44
2.5.3 Developing PSAs for Generation IV Nuclear Systems 45
2.5.4. PSA Relationship to Other ISAM Elements 47
2.5.5. Scope and Quality (Details on this subject are provided in Appendix 6) 48
2.5.6 Treatment of Uncertainties (Details on this subject are provided within the Appendix 6) 49

3. Example of application of ISAM methodology to JSFR 51
3.1 – Introduction 51
3.2 – Applicability of PIRT to JSFR safety design work 51
3.3 – Applicability of OPT to JSFR (see Appendix 7) 52
3.4 – Applicability of DPA to JSFR DHRS (see Appendix 7) 53

3.5 – Applicability of PSA to JSFR DHRS (see Appendix 7) 55
3.6 – Summary 56

Annex - Glossary of main terms used in the Report 57

Appendix 1 – Reminder of the safety objectives and approach 63

Appendix 2 – QSR Tables of Technical recommendations 65

Appendix 3 – Phenomena Identification and Ranking Tables - Details 94
A3.1 - Introduction 94
A3.2 - Description of PIRT 94
A3.2.1 The Objective and Usefulness of the Task 94
A3.2.2 The Individual Steps in the Activity 95
A3.2.3. - Conclusions on the PIRT 101

Appendix 4 – Objective Provision Trees for assessment of adequacy of Defence-in Depth (DiD) 102

Appendix 5 – Deterministic Safety Analysis - Task individual steps 106

Appendix 6 – PSA Scope, Quality and Treatment of Uncertainties 109

Appendix 7 – Details of example of application of PIRT, OPT, DPA and PSA to JSFR 113
A7.1 JSFR plant and its design specifications 113
A7.2 Outline of self-actuated shutdown system (SASS) 113
A7.3 PIRT application result 114
A7.4 Alternative representation of OPT 115
A7.5 Details of the application of DPA and PSA to DHRS of JSFR 115

Executive Summary

A principal focus of the Generation IV (Gen IV) International Forum's Risk and Safety Working Group charter is the development and demonstration of an integrated methodology that can be used to evaluate and document the safety of Gen IV nuclear systems. A first RSWG report issued in 2008 presented the "*Basis for the Safety Approach for Design & Assessment of Generation IV Nuclear Systems*". Following its mandate RSWG has prepared this new document that describes a methodology, called the Integrated Safety Assessment Methodology (ISAM), for use throughout the Gen IV technology development cycle.

Early generations of nuclear technology generally applied system safety analysis techniques to relatively mature designs. In many cases, reactors were fully designed, built, and operating before methods that are today recognized as system safety analysis tools were applied to identify and evaluate safety vulnerabilities associated with these systems. The result, in many instances, was addition of design "backfits" developed to reduce safety vulnerabilities discovered through operating experience or through analysis. For Gen IV nuclear systems, the ISAM is intended to support achievement of safety that is "built-in" rather than "added on" by influencing the direction of the concept and design development from its earliest stages. The ISAM is perhaps best thought of as a "tool kit" consisting of elements that help to answer different safety-related questions and help provide important safety perspective at various stages of design development. The value of the toolkit is that it uses interim analysis results to actively shape the direction of the design. The expected result is to improve safety, reduce capital costs and reduce the time required for the technology development cycle. It is envisioned that the ISAM will be used in three principal ways:

- The ISAM is intended for use throughout the concept development and design phases with insights derived from the ISAM serving to influence the course of the design evolution. In this application of the methodology, the ISAM is used to develop a more detailed understanding of safety related design vulnerabilities, and resulting contributions to risk. Based on this detailed understanding of safety vulnerabilities, new safety provisions or design improvements can be identified, developed, and implemented relatively early.
- Selected elements of the methodology will be applied at various points throughout the design evolution to yield an objective understanding of risk contributors, safety margins, effectiveness of safety-related design provisions, sources and impacts of uncertainties, and other safety-related issues that are important to decision makers.
- The ISAM can be applied in the late stages of design maturity to measure the level of safety and risk associated with a given design relative to safety objectives or licensing criteria. In this way, the ISAM will allow evaluation of a particular Gen IV concept or design relative to various potentially applicable safety metrics or "figures of merit." This *post facto* application of the ISAM will be especially useful for decision makers and regulators who require objective measures of safety for licensing purposes, or to support certain late-stage design selection decisions.

The methodology is NOT intended to dictate design requirements, to dictate compliance with quantitative safety goals, or to constrain designers in any other way. The sole intent is to provide a useful methodology that contributes to the attainment of Generation IV safety objectives, that yields useful insights into the nature of safety and risk of Generation IV systems, and that permits meaningful evaluations of Generation IV concepts with respect to safety.

<u>Toward achievement of Generation IV Safety Goals</u>

Advanced technologies, together with a safety approach driven by insights derived from an integrated safety assessment methodology, hold the promise of making Gen IV energy systems even safer than the current generation of nuclear plants.

Although the ISAM is essentially a PSA-based safety assessment methodology for Gen IV systems, the strength of the ISAM is that it offers tools that are tailored to answering specific types of questions at various stages of design development. The elements of the methodology complement and support one another in a way that contributes to a much more complete understanding of the range of safety issues. The diversity of analysis tools that comprise the ISAM help to ensure that the assessment of Generation IV system safety will be complete and robust. It is anticipated that using the elements of the ISAM in an integrated way will result in optimizing safety, reducing technology development cycle time, reducing development costs, and facilitating licensing of Gen IV systems.

ISAM Overview

The ISAM consists of five distinct analytical tools. It is intended that each tool be used to answer specific kinds of safety-related questions in differing degrees of detail, and at different stages of design maturity. By providing specific tools to examine relevant safety issues at different points in the design evolution, the ISAM as a whole offers the flexibility to allow a graded approach to the analysis of technical issues of varying complexity and importance. The methodology is well integrated, as evidenced by the fact that the results of each analysis tool support or relate to inputs or outputs of other tools. Although individual analytical tools can be selected for individual and exclusive use, the full value of the integrated methodology is derived from using each tool, in an iterative fashion and in combination with the others, throughout the development cycle.

Figure 1 shows the overall task flow of the ISAM and indicates which tools are intended for use in each phase of Generation IV system technology development.

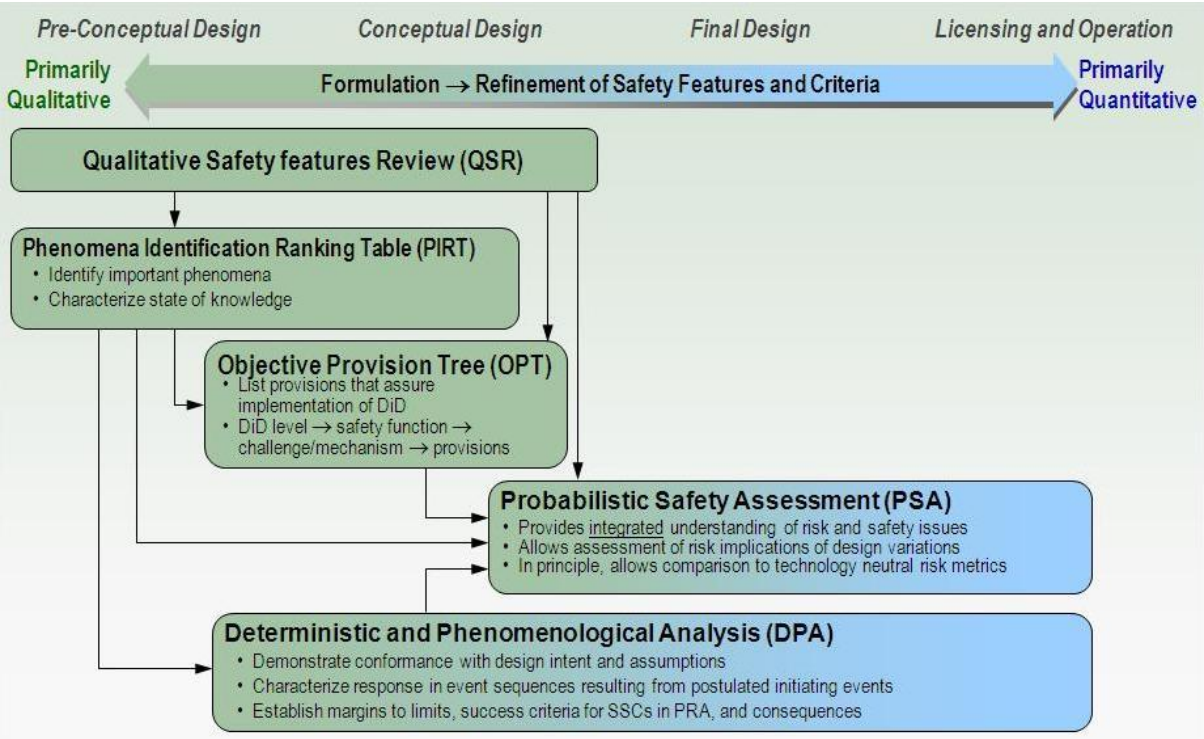


Figure 1 Proposed GIF Integrated Safety assessment Methodology (ISAM) Task Flow

Each of the analysis tools that is part of the ISAM is briefly described here:

- *Qualitative Safety Features Review (QSR)*

The Qualitative Safety Features Review (QSR) is a new tool that provides a systematic means of

ensuring and documenting that the evolving Gen IV system concept of design incorporates the desirable safety-related attributes and characteristics that are identified and discussed in the RSWG's first report entitled, "Basis for the Safety Approach for Design and Assessment of Generation IV Nuclear Systems", as well as in other references (e.g., the INPRO Safety methodology). The QSR provides a useful means of shaping designers' approaches to their work to help ensure that safety truly is "built-in, not added-onto" since the early phases of the design of Gen IV systems. Using a structured template to guide the process, concept and design developers are prompted to consider, for their respective systems, how the attributes of "defence in depth", high safety reliability, minimization of sensitivity to human error, and other important safety characteristics might best be incorporated. The QSR also serves as a useful preparatory step for other elements of the ISAM by promoting a richer understanding of the developing design in terms of safety issues or vulnerabilities that will be analyzed in more depth in those other analytical steps.

- *Phenomena Identification and Ranking Table (PIRT)*

The Phenomena Identification and Ranking Table (PIRT) is a technique that has been widely applied in both nuclear and non-nuclear applications. As applied to Gen IV nuclear systems, the PIRT is used to identify a spectrum of safety-related phenomena or scenarios that could affect those systems, and to rank order those phenomena or scenarios on the basis of their importance (often related to their potential consequences), and the state of knowledge related to associated phenomena (i.e., sources and magnitudes of phenomenological uncertainties).

The PIRT is used initially in the pre-conceptual design phase of a system's development, and is applied iteratively throughout the development process. In the early stages of design development, it is intended that PIRT be used in a rather general way to identify safety phenomena that are potentially relevant to the particular design, and to rank the relative importance of those phenomena. The results can be used to: (1) prioritize confirmatory research activities to address the safety-significant issues, (2) inform decisions regarding the development of independent and confirmatory analytical tools for safety analysis, (3) assist in defining test data needs for the validation and verification of analytical tools and codes, and (4) provide insights for the review of safety analysis and supporting data bases. The PIRT can be focused on very general issues, or on highly specific design issues, depending on the need, and relative to the stage of design development.

The method relies heavily on expert elicitation, but provides a discipline for identifying those issues that will undergo more rigorous analysis using the other tools that comprise the ISAM. As such, the PIRT forms an input to both the Objective Provision Tree (OPT) analyses, and the Probabilistic Safety Analysis (PSA). The PIRT is particularly helpful in defining the course of accident sequences, and defining safety system success criteria. The PIRT is essential in helping to identify areas in which additional research may be helpful to reduce uncertainties.

- *Objective Provision Tree (OPT)*

The Objective Provision Tree (OPT) is a relatively new analytical tool that is enjoying increasing use. The International Atomic Energy Agency (IAEA) has been a particularly influential developer and proponent of this analysis tool. The purpose of the OPT is to ensure and document the provision of essential "lines of protection" to ensure successful prevention, control or mitigation of phenomena that could potentially damage the nuclear system. There is a natural interface between the OPT and the PIRT in that the PIRT identifies phenomena and issues that could potentially be important to safety, and the OPT focuses on identifying design provisions intended to prevent, control, or mitigate the consequences of those phenomena.

The OPT can be applied early in the pre-conceptual design phase, and iteratively through conceptual design. The OPT is an entirely qualitative analysis method and as such, its purpose is to inform the design process and to help structure inputs that will eventually make their way into the PSA. The OPT can be extremely useful in helping to focus and structure the analyst's identification and understanding of possible initiators and mechanisms of abnormal conditions, accident

phenomenology, success criteria, and related issues. It will help identify effective design provisions for prevention and mitigation of phenomena that challenge the safety of Gen IV systems. The possibility to use the OPT to help harmonizing the safety and the security approach is under assessment in close connection with the Proliferation resistance & Physical Protection (PRPP) group.

- *Deterministic and Phenomenological Analyses (DPA)*

Classical deterministic and phenomenological analyses, including thermal-hydraulic analyses, computational fluid dynamics (CFD) analyses, reactor physics analyses, accident simulation, materials behaviour models, structural analysis models, and other similar analysis tools collectively constitute a vital part of the overall Gen IV ISAM. These traditional deterministic analyses will be used as needed to understand a wide range of safety issues that guide concept and design development, and will form inputs into the PSA. These analyses typically involve the use of familiar deterministic safety analysis codes. It is anticipated that DPA will be used from the late portion of the pre-conceptual design phase through ultimate licensing and regulation of the Generation IV system.

- *Probabilistic Safety Analysis (PSA)*

Probabilistic Safety Analysis (PSA) is a widely accepted, integrative method that is rigorous, disciplined, and systematic, and therefore it forms the principal basis of the ISAM. PSA can only be meaningfully applied to a design that has reached a sufficient level of maturity and detail. Thus, PSA is performed, and iterated beginning in the late pre-conceptual design phase, and continuing through to the final design stages. In fact, as the concept of the "living PSA" (one that is frequently updated to reflect changes in design, system configuration, and operating procedures) is becoming increasingly accepted, the RSWG advocates the idea of applying PSA at the earliest practical point in the design process, and continuing to use it as a key decision tool throughout the life of the plant or system. Although the other elements of the ISAM have significant value as stand-alone analysis methods, their value is enhanced by the fact that they serve as useful tools in helping to prepare for and to shape the PSA once the design has matured to a point where the PSA can be successfully applied.

Fundamentally, the PSA provides a structured means of identifying the answers to three basic questions related to the safety of Gen IV systems. These are:

- What can go wrong?
- How likely is it that it goes wrong?
- What are the consequences when it does go wrong?

The centrepiece of the ISAM is a "full scope" PSA that considers both internal and external events, and models potential accident phenomena from the hypothetical occurrence of an initiating event through the point at which accident progression is either arrested, or offsite consequences are realized.

One of the key strengths of the PSA is that it facilitates a systematic understanding of the uncertainties relating to the safety (or risk) of a Gen IV system. Uncertainties arise from a number of sources. The traditional response to these safety-related uncertainties has been the provision of additional "safety margin" in the design, often based largely on "engineering judgment," to provide assurance that in the event of any accident, severe loss of control and/or damage will not occur. Adding such safety margins is, of course, expensive, and may also lead to an inappropriate focus on some aspects of design and operation to the detriment of other issues that may, in fact, be more important to safety. By facilitating a disciplined, systematic understanding of the sources and magnitudes of safety-related uncertainties, the PSA will play a key role in helping to ensure that cost and safety issues are more optimally balanced.

1. Introduction

1.1 - The Role of an Integrated Safety Assessment Methodology

In accordance with its Terms of Reference, the primary objective of the Gen IV International Forum's (GIF) Risk and Safety Working Group is to "*promote a consistent approach on safety, risk, and regulatory issues between Generation IV systems.*" Central to meeting this objective is the articulation of a methodology that can be used to assess the safety of Gen IV systems. The RSWG's first report ("*Basis for Safety Philosophy of Generation IV Nuclear Systems*", [1.1]) discussed GIF safety goals and safety principles as well as the basis for the evaluation methodology of the next generation systems; it has provided a set of general findings and recommendations endorsed by the GIF Policy Group and the Expert Group; a brief review on the RSWG safety objectives and approach is given in Appendix 1.

This report describes the suggested safety assessment methodology, tentatively called the Gen IV Nuclear Systems Integrated Safety Assessment Methodology (ISAM).

It is envisioned that the ISAM will be used in three principal ways:

- **Influence the course of the design evolution**
  The ISAM is intended for use throughout the concept development and design phases with insights derived from the ISAM serving to actively contribute to and influence the course of the design evolution. In this application, the ISAM is used to develop a more detailed understanding of safety related design vulnerabilities, and resulting contributions to risk. Based on this detailed understanding of safety features and the identification of safety vulnerabilities, new safety provisions or other design improvements can be introduced relatively early on.

- **Support risk and safety comparisons**
  The methodology can be applied at any point in the design evolution from the conceptual development phase through the final design phase to support risk and safety comparisons of various nuclear system concepts and designs. In this application within a design concept, the methodology can form an input to "down-select" and formulate decisions requiring a systematic and comparative understanding of safety issues predicated on a common analytical framework.

- **Qualitatively and quantitatively measure the level of safety and risk**
  ISAM provides both the possibility to measure the quantitative level of safety achieved as well as an indication of how far and how consistently the recommendations related to the qualitative safety (good practices, transparency, safety demonstration robustness, etc.) are met. The ISAM can be applied throughout the design process to measure the level and quality of safety and risk associated with a given design relative to a specified safety objective or licensing criterion. In the late stages of design maturity the ISAM will allow evaluation of a particular Gen IV concept or design relative to various potentially applicable safety metrics or "figures of merit". This *post facto* application of the ISAM might be especially useful for regulators and other decision makers who require objective measures of safety for licensing purposes, or to support certain late-stage design selection decisions.

It is specifically NOT intended that the ISAM methodology be used to dictate design requirements, to dictate compliance with quantitative safety goals, or to constrain designers in any other way. The sole intent is to provide a methodical approach that contributes to the attainment of Gen IV safety objectives, that yields valuable insights into the nature of safety and risk of Gen IV systems, and that permits meaningful comparison of the safety of Gen IV concepts.

1.2 - Attributes of an Effective Safety Assessment Methodology

A useful safety assessment methodology for Gen IV nuclear systems must incorporate a number of important attributes. In defining the methodology recommended for use in developing Gen IV nuclear

systems, the RSWG has sought to ensure that these attributes are reflected and incorporated in the methodology. These attributes include generic characteristics applicable for all the systems, specific characteristics when applied to a given system or characteristics to be fulfilled when the methodology is applied for the inter-comparison of different systems. These attributes are the following:

- ***Generic characteristics***
  - The methodology should help improving the discussions and exchanges between designers, analysts and regulators.
  - The methodology should consist of, or be largely based on existing tools that are widely accepted for their validity. Thus, the methodology should minimize the need for developing new tools and lengthy validation.
  - Nevertheless, if justified, new tools may be needed to address :
    - Specific issues which characterize the innovative systems (e.g., increased use of inherent safety features and/or passive systems);
    - Specific recommendations considered as relevant to ensure an increased level of safety (e.g., to address specific severe accidents recommendations such as the concept of "practical elimination" [1.1]);
    - Specific recommendations considered as relevant to help improve the robustness of the demonstration (e.g., the mastering of the uncertainties [1.1]);
  - The methodology must be comprehensive, understandable, user-friendly, effective and efficient.
  - The methodology must allow for the integration of a diverse range of multidisciplinary inputs including those that are principally qualitative and those that are principally quantitative in nature.
  - Based on the desirability of offering a graded approach to technical issues of varying complexity and importance, characteristics such as practicality and flexibility must be reflected in the methodology.
  - To the extent that is appropriate, the methodology shall be consistent with relevant guidance and documentation including the RSWG Safety Philosophy document [1.1], the PR&PP methodology [1.2], and other work including the US NRC NUREG-1860 [1.3], the IAEA TECDOC-1570 [1.4], INPRO [1.5] and others.
  - The methodology must primarily and actively contribute to the development of designs that fulfil the safety objectives of Gen IV systems.
- ***Characteristics applicable to the implementation of a given system***
  - Throughout the development process, the safety assessment methodology must help designers understand safety related design vulnerabilities, and how alternative design solutions can reduce or eliminate those vulnerabilities. In order to successfully fulfil this role, the methodology must yield information about which aspects of design contribute the most to the reduction of risk associated with that concept or design. Thus, the methodology must serve to do more than just quantitatively measure overall safety after the design is complete.
  - For a given concept, the methodology
    - must help and support the comparisons of potential alternative design options.
    - must yield information that allows comparison of a concept or design relative to established safety metrics or "figures of merit."
    - must yield a mix of both qualitative and quantitative information that will support eventual licensing and regulatory processes.

- Importantly, the methodology must provide information that permits an understanding of the level of uncertainty associated with the measured level of safety, as well as an understanding of the sources of that uncertainty.
- Based largely, but not exclusively, on a systematic understanding of sources and magnitudes of uncertainties, the methodology must help identify areas that need additional research, data collection, and improved analytical models.

➢ ***Characteristics applicable to the inter comparison of different systems***

- The methodology must allow meaningful comparisons of the nature of risk between different Gen IV system concepts and designs. For example, the methodology will be useful in comparing risks associated with the Liquid Metal Fast Reactor concepts (LFR, SFR) and those reactors cooled by gas (GFR; VHTR).

1.3 - Human Factors Considerations

Human factors issues are likely to be more subtle and complex in Gen IV nuclear systems than have been encountered to date. These issues will arise from the increased use of advanced technology, the novelty of human interactions with such technology, coupled with a lack of design experience and empirical data of human factors in advanced systems. An important element of ISAM is therefore the transparency and analysis of the human-based safety claims in order to fully understand and substantiate the human contribution to safety and overall reliance of Gen IV nuclear systems on human reliability.

Human factors considerations within the ISAM are best served through the process of Human Factors Integration (HFI) incorporating Human Reliability Assessment (HRA) good practices such as those advocated in the NUREG good practice guide [NUREG 1792]. HFI aligns well with the integrated principles and processes of ISAM. It provides a good practice organising framework and management strategy to help ensure that all relevant HF issues, activities and standards are identified and addressed in a timely manner throughout an evolving design. This will enable the comprehensiveness and importance of human factors to be identified for each stage of the design such that human reliability claims and knowledge can be adequately accommodated and ultimately transferred into the subsequent operating regime. HFI will provide the means of successfully informing the QSR, PIRT and OPT activities, and will also ensure that correct analytical tools and techniques are applied in a proportionate manner to support the DPA and PSA. This should ensure that the human-based safety aspects of the design‘s defence-in-depth are substantiated and the impact on overall system reliability and risk is objectively defined and understood.

Human factors integration within ISAM cannot be underestimated given that many human-based risk contributors could easily be overlooked for advanced technology and for the increasing focus on the design and use of automation. It is likely that Gen IV nuclear systems will shift the importance or balance of human failure analysis to the operator’s cognitive state (e.g., decision making) and to human error in design, construction, maintenance, testing and calibration.

Contemporary HRA techniques underpinned with task analysis that is focused more on cognition and context will be necessary to identify human errors and their origins and mechanisms. Specific issues likely to need more consideration than has been done for existing nuclear systems, are the dynamic evolution of an operator’s mental model when interacting with advanced systems. Performance influencing factors such as automation-induced dependency and issues associated with this e.g., boredom, vigilance detriment, situational awareness, diligence, competence and violations will need careful consideration and mitigation through both the design and operational support in Gen IV nuclear systems.

1.4 - ISAM Overview

The ISAM provides an integrated set of tools that satisfies the list of desired attributes outlined above. It offers a Risk Informed approach in which qualitative and quantitative, deterministic and probabilistic insights are made available to support the designer throughout the design process.

The integrated methodology consists of five distinct analytical tools, or "elements." These include:

- Qualitative Safety Features Review (QSR)
- Phenomena Identification and Ranking Table (PIRT)
- Objective Provision Tree (OPT)
- Deterministic and Phenomenological Analyses (DPA)
- Probabilistic Safety Analysis (PSA)

It is intended that each element be used to answer specific safety-related questions with different degrees of detail[1] and at different stages of design maturity. By providing specific tools to examine relevant safety issues at different points in the design evolution, the ISAM, as a whole, offers the flexibility to allow a graded approach to the analysis of technical issues of varying complexity and importance. The methodology is well integrated, as evidenced by the fact that the results of each analysis tool support or relate to inputs or outputs of other tools. Although individual analytical elements can be selected for individual and exclusive use, the full value of the integrated methodology is derived from the complementary use of all elements in an iterative fashion throughout the development cycle. Figure 1 shows a flow diagram depicting 1) the major analytical elements of the methodology, 2) the interrelationships between the elements, and 3) the stages of the design evolution at which each of the elements is applicable.

Each element of the methodology is briefly described hereafter. More complete information on each of the elements is presented in later chapters of this document.

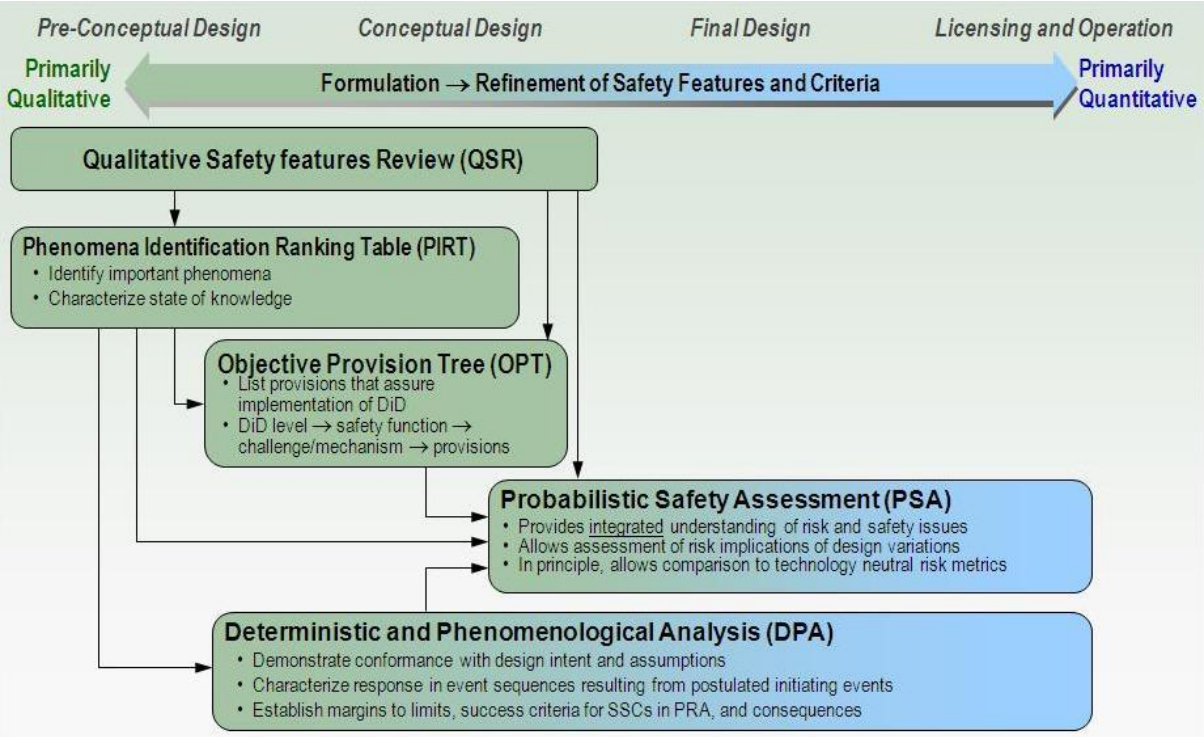


Figure 1 Proposed GIF Integrated Safety assessment Methodology (ISAM) Task Flow

1.4.1 Qualitative Safety Features Review (QSR)

The Qualitative Safety Features Review is a new tool that provides a systematic means of ensuring and documenting that the evolving Gen IV system concept of design incorporates the desirable safety-related attributes and characteristics that are identified and discussed in the RSWG's first report [1.1].

[1] E.g., in correlation with the available resources

It is believed that the QSR provides a useful means of shaping designers' approaches to their work to help ensure that safety is "built-in, not added-on" through the early phases of the design of Gen IV systems. Using a structured template to guide the process, concept and design developers are prompted to consider, for their respective systems, how the attributes of "defence in depth", such as transparency, high reliability, minimization of sensitivity to human error, and other important safety characteristics[2], might best be incorporated. The QSR is not regarded as a tool that allows an analyst to determine whether or not a developing concept is "good enough," but rather, provides a measure of discipline to help ensure that certain desirable characteristics are incorporated into the design in its earliest phases. The QSR also serves as a useful preparatory step for other elements of the ISAM by promoting a richer understanding of the developing design in terms of safety characteristics, i.e., assets or vulnerabilities that will be analyzed in more depth in those other analytical steps.

1.4.2 Phenomena Identification and Ranking Table (PIRT)

PIRT is a process based largely on expert elicitation. The process involves selecting hardware (i.e., nuclear plant), selecting an accident scenario, and then identifying all plausible phenomena impacting on the outcome of the accident. Each phenomenon is then ranked in order of relative importance and its state of knowledge. The PIRT provides a structured means of identifying and analyzing a wide variety of off-normal scenarios that potentially challenge the viability of complex technological systems. The PIRT methodology brings into focus the phenomena that dominate, while identifying all plausible effects to demonstrate completeness.

The PIRT is used initially in the pre-conceptual design phase of a system's development, and is applied iteratively throughout the development process. It is to be used as an early "screening" tool to identify, categorize, and characterize phenomena and issues that are potentially important to risk and safety of a Gen IV system. The PIRT can be focused on very general issues, or on highly specific design issues, depending on the need. The method relies heavily on expert elicitation, but provides a discipline for identifying those issues that will require more rigorous analysis using the other tools that comprise the ISAM. As such, the PIRT forms an input to both the Objective Provision Tree (OPT) analyses, and the Probabilistic Safety Analysis (PSA) in identifying mechanisms and initiating events that will challenge the safety functions. Furthermore, in the case of the PSA, the PIRT is particularly helpful in defining the course of accident sequences. The PIRT is also useful in helping to identify areas in which additional research may be helpful to reduce uncertainties.

1.4.3 Objective Provision Tree (OPT)

The Objective Provision Tree is a relatively new analytical tool. It provides an exhaustive overview of the safety related architecture and allows the identification, for each level of the defence in depth, of all provisions[3] that contribute to the achievement of safety functions as well as their mutual interrelations. The International Atomic Energy Agency (IAEA) has been a particularly influential developer and proponent of this analysis tool. The purpose of the OPT is to ensure and document the implementation of essential "lines of protection" to ensure successful prevention, control or mitigation of phenomena that could potentially damage the nuclear system. It introduces a new and exhaustive vision of the safety architecture allowing identification, for each level of the defence in depth, of all provisions that contribute to the achievement of safety functions and their mutual interrelations.

There is a natural interface between the OPT and the PIRT in that the PIRT identifies phenomena and issues that could potentially be important to safety, and the OPT focuses on identifying design provisions intended to prevent, control or mitigate those phenomena. Simultaneously, the OPT can help identify new safety challenging mechanisms with possible feedbacks in terms of requirements for further PIRT analysis.

[2] E.g., Cf. Ref. 1.1: "*the defence in depth should be implemented in a way which is exhaustive, progressive, tolerant, forgiving and well-balanced*."

[3] Provisions: – inherent characteristics, technical options and organizational measures – selected for the design, the construction, the operation including the shut down and the dismantling, which are taken to prevent accidents or limit their effects.

The OPT should be applied early in the pre-conceptual design phase, and iteratively through conceptual design. The OPT is basically a qualitative analysis tool and as such, its purpose is to facilitate the design process and to help structure inputs that will eventually make their way into the PSA. The OPT can be extremely useful in focusing and structuring the analyst's understanding of safety concerns, accident sequence phenomenology, accident sequence success criteria, and related issues. It will help define effective design elements (e.g., requested performances and reliability) for the implemented provisions.

1.4.4 Deterministic and Phenomenological Analyses (DPA)

Within the context of the recommended risk informed approach, the deterministic and phenomenological analyses, which include thermal-hydraulic analyses, computational fluid dynamics (CFD) analyses, reactor physics analyses, accident simulation, materials behaviour models and structural analysis models, collectively constitute a vital part of the overall Gen IV ISAM. These analyses will be used as needed to understand and quantify the safety issues that must guide concept and design development, and their results will form inputs needed for a credible PSA. These analyses typically involve the use of familiar deterministic safety analysis codes. It is anticipated that DPA will be systematically used from the late portion of the pre-conceptual design phase through ultimate licensing and regulation of the Gen IV system.

1.4.5 Probabilistic Safety Analysis (PSA)

PSA has been widely used in a variety of nuclear and non-nuclear applications since the early 1970s; it provides a structured means of identifying the answers to three basic questions related to safety. These are:

- What can go wrong?
- How likely is it they can go wrong?
- What are the consequences if they do go wrong?

As a widely accepted, integrative method that is rigorous, disciplined, and systematic, PSA forms the principal basis of the ISAM. PSA can only be meaningfully applied to a design that has reached a sufficient level of maturity and detail. Thus, PSA is to be performed, and iterated, beginning in the late pre-conceptual design phase, and continuing through the final design stages addressing licensing and regulation concerns. In fact, as the concept of the "living PSA" (one that is frequently updated to reflect changes in design, system configuration, and operating procedures) is becoming increasingly accepted, the RSWG is advocating the idea of applying PSA at the earliest practical point in the design process, and continuing to use it as a key decision tool throughout the life of the plant or system. Moreover it is important to consider the PSA not only for the results corresponding to the conventional levels 1, 2 and 3[4] but also for the indications that are obtained at the intermediate stages, e.g., before core degradation.

Although the other elements of the ISAM have significant value as stand-alone analysis methods, to a significant degree, their value is enhanced by the fact that they serve as useful tools in helping to prepare for, and to shape, the PSA once the design has matured to a point where the PSA can be successfully applied.

The centrepiece of the ISAM is a "full scope" PSA that considers both internal and external events and models potential accident phenomena from the hypothetical occurrence of an initiating event through the point at which accident progression is arrested and the onsite and offsite consequences duly assessed.

[4] Cf. IAEA Glossary: *Three levels of probabilistic safety assessment are generally recognized. Level 1 comprises the assessment of plant failures leading to determination of the frequency of core damage. Level 2 includes the assessment of containment response, leading, together with Level 1 results, to the determination of frequencies of failure of the containment and release to the environment of a given percentage of the reactor core's inventory of radionuclides. Level 3 includes the assessment of off-site consequences, leading, together with the results of Level 2 analysis, to estimates of public risks.*

1.4.6 Integration of ISAM Elements

As discussed above, and elsewhere in this document, the ISAM is best thought of as a tool kit of useful analysis tools for Gen IV systems. The elements that comprise the ISAM are intentionally diverse. Some are primarily qualitative, others quantitative. Some are probabilistic, others deterministic. Some are inductive, others deductive. Some focus on high-level issues such as systemic response to various phenomena, others focus on more detailed issues. This diversity helps to provide a richer, more complete, and more robust understanding of risk and safety issues than would otherwise be possible through a more limited kind of assessment methodology. The RSWG strongly believes that using all of the elements of the ISAM in an integrated way will improve and optimize all aspects in which safety is implemented, will reduce technology development cycle time, will reduce development costs, and will facilitate the licensing of Gen IV systems. Consistent with this idea of an "integrated toolkit," it is intended that designers have total flexibility to determine the best ways in which to apply ISAM for their developing designs. That said, some general guidance regarding ISAM may be helpful, and can be summarised as follows:

a) The QSR is used throughout the Gen IV system development process to help provide guidance to designers which on the one hand helps ensure that the attributes and characteristics that are most important to safety are actually considered and, as far as feasible, incorporated into the developing concepts and on the other, identify possible safety vulnerabilities that will be addressed with higher priority.

b) In the early phases of the pre-conceptual design stage, the PIRT is applied to help identify specific issues and phenomena that may be important to a particular concept. The PIRT provides a structured way to identify and rank these issues and phenomena, and to inform the developing design concept in its earliest phases.

c) Based on an understanding of the phenomena and issues highlighted in the PIRT, the OPT is used through conceptual design development to ensure and document that the developing design incorporates adequate "lines of protection" (number and quality). These provisions perform prevention, control and mitigation functions relative to those phenomena and issues and ensure that the whole safety architecture fully meets the defence in depth objectives and principles.

d) Deterministic and phenomenological analyses are performed throughout the design process to investigate discrete safety issues, to check the correct implementation of basic deterministic principles such as the single failure criterion or the needed diversification and segregation and to form inputs that will be incorporated into the PSA.

e) Finally the PSA is the synergistic/integrative framework in which both deterministic and probabilistic models are brought together to develop a detailed understanding of what kinds of accident sequences might occur, the relative frequencies of those sequences, how those accidents would progress and what the consequences of those accident sequences could be. The PSA requires as inputs, uncertainty distributions on input parameter values. By propagating those uncertainties through the risk models, the PSA yields answers that both take into account, and display the impacts of, those uncertainties. It is the PSA that will directly allow a detailed understanding of the aspects of design and operation that are most important to plant risk, and it is the PSA that will permit the assessment (qualitative and quantitative) of the improvements during the Gen IV concepts development.

It should be understood that the different elements of ISAM are not of equal interest and the same can be said for the successive steps in developing a new design: pre-conceptual design, conceptual design, final design and licensing & operation. The different elements of the ISAM methodology are expected to be used through successive steps from purely qualitative to a more and more quantitative analysis as shown in the following table.

Development stage	QSR	PIRT	OPT	DPA	PSA
Selection of a reactor type	X	X	X		
Definition of high safety issues	X	X	X		
Definition of safety provisions		X	X	X	
Definition of safety systems initial design			X	X	X
Definition of safety systems final design			X	X	X

Although limited scope trial applications of the ISAM have already occurred, and have demonstrated the usefulness of the methodology, more detailed and realistic trial applications are expected to occur in coming years, and will help define appropriate means of application and integration.

1.5 - Resources Required to Implement ISAM

It is anticipated that prior to application of the ISAM, Gen IV System Steering Committees and other developers of Gen IV nuclear systems will, ideally, wish to have information regarding the levels of effort, time to completion, and types of expertise that must be invested in completing each of the analysis elements of the recommended safety assessment methodology. Unfortunately, due to a relative lack of experience with some of the elements of the ISAM, and a complete lack of experience in application of the fully integrated methodology, no definitive estimates of resource requirements for ISAM application exist at the present time. However, the RSWG believes it is important to present a few relevant thoughts regarding this question as a part of this methodology document.

Beginning with careful consideration of the desirable attributes that the Gen IV safety assessment methodology should exhibit, the ISAM is intended to offer a practical, efficient, and validated approach to design and assessment of Generation IV nuclear systems. The development of the ISAM specifically sought to avoid the need for new or complex tools, and thus sought to minimize the need to master new or unfamiliar analysis methods as a part of Generation IV system development.

The ISAM offers an integrated set of analysis tools that will efficiently provide safety-related answers and perspectives that must be developed by system designers in any case, *with or without ISAM*. Thus, it is intended that the ISAM does not create any additional "burden" on system design teams, but rather, that it provides an efficient means of addressing the kinds of safety issues that would have to be addressed anyway but – likely - in a much less efficient *ad hoc* way. Further it is expected that, by using ISAM elements throughout the design process, insights from ISAM analyses actively contribute to the design evolution resulting in enhanced safety, reduced technology cycle development times, optimized R&D support and, eventually, reduced capital costs. It is believed, therefore, that while the ISAM will certainly require the expenditure of resources to implement, it offers significant potential for net cost savings over the entire technology development effort for Generation IV nuclear systems.

It should also be noted that some elements of the ISAM, particularly the PSA and deterministic analyses, are very likely to be required by national regulators as a part of the licensing process. While licensing is outside the scope of the Generation IV system development effort, the deployment of Generation IV systems will be facilitated by early interactions with regulators in which those interactions are guided by the discipline and formality of the structured, systematic, validated and harmonized safety assessment approach offered by the ISAM. Again, the result will be further net savings of both time and money.

Perhaps a more significant issue in terms of implementing the ISAM is identifying and obtaining the expertise necessary to apply the methodology, and the actual integration of that expertise as a part of the overall design effort. It is true that most designers do not have experience with the analysis tools

that comprise the ISAM thus often it will be necessary to bring in specialists who do have that expertise. While the specifics will differ from one situation to another, here are the RSWG's early recommendations regarding who might best perform each element of the ISAM:

Qualitative Safety Features Review – Check list provided and updated by the RSWG; applied by the system design team, and eventually reviewed by RSWG

Phenomena Identification and Ranking Table – Facilitated by an experienced practitioner of PIRT, with expert teams comprised of system designers and supplemented by outside experts as required. Review and comment by RSWG as required.

Objective Provision Tree – Led by an experienced practitioner of OPT, with involvement by system designers. Review and comment by RSWG as desired.

Deterministic and Phenomenological Analyses – Performed by the system design team, and supplemented by outside experts as required.

Probabilistic Safety Assessment – Performed by team of outside specialists with recognized expertise in the discipline. Supported by system designers as necessary.

References to Section 1

[1.1] *Basis for the Safety Approach for Design & Assessment of Generation IV Nuclear Systems – RSWG Report, January 2009*

[1.2] *Evaluation Methodology for Proliferation Resistance and Physical Protection of Generation IV Nuclear Energy Systems - GIF/PRPPWG/2006/005 - Revision 5 - November 2006*

[1.3] *Feasibility Study for a Risk-Informed and Performance-Based Regulatory Structure for Future Plant Licensing - Main Report - US NRC NUREG 1860, December 2007*

[1.4] *Proposal for a Technology-Neutral Safety Approach for New Reactor Designs - IAEA TECDOC 1570, September 2007*

[1.5] *Guidance for the Application of an Assessment Methodology for Innovative Nuclear Energy Systems - INPRO Manual for the area of Safety of Nuclear Reactors; Volume 8 of the Final Report of Phase 1 of INPRO – IAEA, December 2007*

2. Elements of an Integrated Safety Assessment Methodology (ISAM)

Within the following sections the objectives, the scope and the content of each of the ISAM elements are described. When needed, further details are provided within the appendix.

2.1 - Qualitative Safety Features Review (QSR)

QSR is defined as the identification of safety related recommendations or foreseen characteristics helpful for a standard qualitative safety assessment

2.1.1 - Introduction

The basic idea is to provide the designer with a check list summarizing the good practices and recommendations which can be useful to verify that the design details are coherent with the recommendations which are available from different sources (Regulators, IAEA, RSWG), and applicable to the future nuclear systems[5].

For this Qualitative Safety Features Review (QSR) the check list is, structured following the principle of the defence in depth, and includes a comprehensive set of qualitative recommendations or foreseen characteristics and features. The list will help the designer to qualitatively assess the design options identifying strong characteristics or safety vulnerabilities. If several options are available it will allow safety objectives to be met and will guarantee at best the correspondence of the final result with the principles and the "good practices" suggested, among others, by the RSWG and endorsed by the GIF PG/EG.

The main objective of this section is to explain the logic for the identification of these recommendations, foreseen characteristics and features necessary for the preparation of this check list.

Based on the levels of Defence in Depth, and taking into account the recommendations formulated by the RSWG as well as from other reference documents (e.g., the IAEA standards, the INSAG, INPRO guidelines), these recommendations are obtained using a top-down functional approach, i.e., the contents of the various levels of the defence in depth (“prevention”, “control”, “protection”, “management of the severe accidents”) are translated into recommendations or foreseen characteristics and features applicable to any design.

Each of these recommendations / characteristics (Class 1) are detailed as far as feasible (i.e., step by step) with a technology neutral logic (Class 2 ⇨ Class N) to obtain a set of specific recommendations (“check list”) applicable to a given technology. This check list forms the basis for the ***Qualitative Safety Features Review (QSR)***

2.1.2 - The elaboration of the qualitative recommendations for the assessment

The reference [2.1.1] defines the attributes that are most likely to help meet the Generation IV safety goals, and identify the methodological advances that have to be achieved and demonstrated to do that. Apart from reference [2.1.1] it is recognized that a further step is necessary to make its content directly usable by the Gen IV Systems Steering Committees (& the System Integration & Assessment Management Boards (MB), as well as other Projects MBs).

The objectives, principles, guidelines presented within the reference [2.1.1] are translated into interim safety related recommendations usable by the designer to perform the qualitative safety assessment. The identification of such recommendations has to be done following a standard, understandable and

[5] The approach is analogous to the one adopted by the IAEA with its set of safety series organized in three levels: *Fundamentals*, *Safety standards*, *Guides*. The main difference is, first of all, the synthetic presentation – i.e., through a check list – and secondly the direct correlation with the levels of the defence in depth. The latter is justified by the objective to give to the designer an instrument to verify easily and concretely the correspondence with the principles of the defence in depth.

transparent integrated approach. The main goal of this section is to suggest such a pragmatic approach for the identification of the recommendations and/or foreseen characteristics and features.

The latter have been grouped in four classes according to the scheme below:

- Class 1 – Generic & Technology neutral (i.e., applicable to all the technologies implemented by the innovative systems)
  - Class 2 – Detailed & Technology neutral
    - *Class 3 – Detailed & Technology neutral but applicable to a given safety function*
      - *Class 4 – Detailed, applicable to a given safety function, and technology specific, i.e., applicable to a given reactor technology.*

Following this scheme a comprehensive "check list" is established[6] for the different levels of the defence in depth, for the different safety functions and could be developed for the different concept technologies.

Knowing the system/option characteristics it is then possible to qualitatively compare such characteristics with the recommendations to achieve the requested assessment.

2.1.3 - Guidelines for the design and the assessment

As indicated above, the recommendations used for the qualitative safety assessment of the systems/provisions, i.e., the QSR check list, have to be consistent with all the available guidelines (IAEA; RSWG; others).

2.1.3.1 - Available technical guide-lines from the IAEA

Several IAEA references are essential to derive the applicable guidelines [2.1.2-2.1.7].

To meet the safety objectives, these references describe and set up "***Fundamental safety principles***" [2.1.2], "***Basic safety principles"*** [2.1.3-2.1.7] as well as "***Specific safety principles***" [2.1.4-2.1.7]; the latter address all the concerns related to the nuclear plant design, operation and decommissioning: *⬩ Siting; ⬩ Design; ⬩ Manufacturing and construction; ⬩ Commissioning; ⬩ Operation; ⬩ Accident management; ⬩ Emergency preparedness.* Examples provided by the reference [2.1.4] give details applicable on the *Design process*, *General features*, as well as *Specific features.* Several of these principles are directly usable to work out and set up the set of assessment recommendations for the plants and their provisions.

The reference [2.1.5] recommends the adoption of some complementary generic principles that are useful for working out assessment recommendations and foreseen characteristics and features, as for example (without hierarchy):

---

[6] Below the example of a set of recommendations (in *italic*) applicable to the 1st level of the defence in depth (Prevention), for the Decay Heat Removal safety function, and applicable to a given technology (e.g., the sodium cooled) for which the natural convection can bring an essential contribution.

1st level of the defence in depth: Prevention

- Class 1 – Generic & Technology neutral:
  - ***Work out and set up a simplified plant design***
- Class 2 – Detailed & Technology neutral:
  - ***Work out and set up a simplified thermo-hydraulic design***
- Class 3 – Detailed & Technology neutral but applicable to a given safety function*:*
  - ***Simplify the thermo-hydraulic for the DHR under abnormal conditions***
- *– Class 4 –* Detailed, applicable to a given safety function, technology specific:
  - ***Allow the DHR through the easy natural convection starting and operation***

Following this example, the assessment of different possible options for internals will score positively those which will allow implementing easily the natural convection while the options for which the natural convection would be more difficult to establish and/or less effective and /or associated to larger uncertainties will be scored less favourably.

1) *The plant design should be extended to include the operating and maintenance procedures required for it.*
2) *Design should avoid complexity.*
3) *Plants should be designed to be "user friendly".*
4) *Design should further reduce dependence on early operator action.*
5) *The design of the system provided to ensure confinement of radioactive materials after a postulated accident should take into account the values of pressure and temperature encountered in severe accident analysis.*
6) *Accidents that would be large contributors to risk should be designed out or should be reduced in probability and/or consequences.*
7) *The plant should be adequately protected by design against sabotage and conventional armed attack.*
8) *Design features should reduce the uncertainty in the results of probabilistic safety analysis.*
9) *Consideration should be given to passive safety features.*

Obviously each of these recommendations needs corresponding metrics that will be used to compare and classify the different options. For some of them specific instruments are already suggested and if needed, should be developed (e.g., "*Index of complexity*" [2.1.8] for items 2, 3 and 4 above; living "*on line simplified PSA*" (Section 2.5) for items 4, 6 and 9 above; etc.); in any case a consistent effort is needed to cover the full set.

2.1.3.2 - Available technical guide-lines from the RSWG

For the Design and assessment of innovative systems the reference [2.1.1] explicitly recognizes that:

- *The Design Basis for Gen IV energy systems should cover the full range of safety significant conditions. The historical notion of a single bounding design basis accident must be replaced by a "spectrum" of possible accidents that, while of low probability, represents with high confidence the range of physical events that could conceivably challenge the plant.*
- *Specific efforts should be made for demonstrating the "practical elimination" of initiators, sequences or phenomena associated with the extremely low residual risk. Among other considerations, these efforts should be based on the experience in the implementation of this concept for latest designs, specific R&D and engineering judgement.*
- *Updated safety analysis methods should be applied to examine the full range of safety-significant issues. As part of an adequate treatment of the full spectrum of design conditions including the domain of severe plant conditions, these updated methods must, for example, consider all internal events and all hazards in a homogeneous way and the treatment of physical protection issues as well as of new sources of uncertainty.*
- *Objectives and practices for the design improvement are identified within the report* ([2.1.1] NDR). *To efficiently set up these practices, three complementary ways may be followed by the designer: 1) critical and systematic examination and consideration of the feedback experience; 2) rationalization of the design approach by the deliberate adoption of the ALARP principle on a cost benefit basis[7]; and 3) implementation of the concept of defence in depth in a manner that is demonstrably exhaustive[8], progressive[9], tolerant[10], forgiving[11] and*

[7] i.e., taking into account that there has to be gross disproportion before the safety improvement is not adopted.

[8] An exhaustive defence, the identification of the scenarios to be retained to design and size the safety architecture provisions must be as exhaustive as possible. It has to be noted that, coherently with the defence-in-depth principle possible lacks of exhaustiveness are compensated by consideration of enveloping situations which are taken into account independently of their expected occurrence frequency

well-balanced[12]*. Finally, special attention should emphasise the treatment of the severe plant conditions through provisions of measures that help managing such conditions.*

- *For these new concepts, the achievement of the robust safety demonstration rests on the capacity of the designer and the developer to be exhaustive in the recognition of risks stemming from phenomena considered for the design. Whenever possible, plant design features based on natural phenomena and physical properties of materials should be used to demonstrate, in an "intuitive" manner*[13]*, the ability of the plant to arrest the accident progression. This should be with an adequate degree of confidence, an understanding of the associated uncertainties and provision of sufficient margins, and the minimization of impacts on workers and the public.*
- *Practical instruments are suggested for use by the designers to support the design activity as well as the assessment activities. Among others, the Objective Provision Tree and the notion of Line of Protection will allow the whole safety architecture to be structured and presented in a scheme. The availability of this systematic representation of the safety architecture may help the plant design and assessment as well as to improve transparency.*

The recommendations used for the qualitative safety assessment of the systems/provisions, i.e., the QSR check list, have to be consistent with all the available guidelines (IAEA; RSWG; others).

2.1.4 - Defence in Depth (DiD) implementation

As stated above, the design effort must be coherent with the DiD approach through the adoption of three generic goals: prevention, control and mitigation. The "practical elimination" of initiators, sequences or phenomena associated with the extremely low residual risk is the natural outcome in the achievement of these goals. These goals can be expanded to obtain the five levels of the DiD [2.1.5], [2.1.6].

The improvement of the DiD justifies a specific effort to implement better prevention of incidents and accidents and to ease the management of all the abnormal situations (levels 1 to 3) while looking for systematically feasible consequence mitigation (levels 4 and 5).

It is important to note that through the fourth and fifth levels, the DiD approach requires an ultimate demonstration of the plant safety, taking into account, as a matter of routine, the possibility for plant degradation (severe plant conditions or "severe accidents"). Several reasons motivate the full integration of this recommendation:

(i) to cover the possible lack of exhaustiveness of the selected deterministic sequences,

(ii) to demonstrate the aptness of the concept for mitigating severe accidents,

(iii) to demonstrate the avoidance, by design, of any cliff edge effect[14].

Such reasons have to be considered in elaborating the recommendations associated with these DiD levels.

---

[9] A graduated, progressive defence; without that, "short" sequences can happen for which, downstream from the initiator, the failure of a particular provision entails a major increase, in terms of consequences, without any possibility of restoring safe conditions at an intermediate stage.

[10] A tolerant defence: no small deviation of the physical parameters outside, the expected ranges, can lead to severe consequences (i.e., rejection of "cliff edge effects").

[11] A forgiving defence, which guarantee the availability of a sufficient grace period and the possibility of repair during accidental situations

[12] A balanced or homogeneous defence, i.e.,: no sequence participates in an excessive and unbalanced manner to the global frequency of the damaged plant states

[13] "*Intuitive*" means that, due to the inherent plant characteristics, the designer will be able to anticipate and describe the sequences while guaranteeing the identification/management of the uncertainties.

[14] The Cliff edge is a discontinuity in the relationship between the frequencies and the consequences that defines the risk : *Risk = frequency x consequences*. It is characterized by a small change ***for the frequency of occurrence*** that leads to a large increase in the consequences

2.1.5 - Safety recommendations

The section 2.1.3 above recalls some generic recommendations and the technical guidelines that must be taken into account for future nuclear plants. Starting from the Defence in Depth levels, all these indications are integrated and developed following a functional analysis approach[15].

The approach consists of developing qualitative contents at various levels of defence in depth. Starting from the indications provided, for example, within the INSAG 10, the objective is to give indications useful to the designer about generic notions such as "prevention", "control", "protection", "management of the severe accidents". The latter are translated into recommendations applicable to the design through:

- the generic recommendations for the evaluation of the main plant design options;
- the specific recommendations for the evaluation of the safety provisions (systems, structures, components, others).

This development is shown in table A2.1a of Appendix 2 to obtain the first set of recommendations which are then detailed within the tables which follow: Table A2.1b & A2.1c. This development is relatively subjective and it is important to discuss it and, if need be, to correct and/or to complete the supplied list. Figure 2 resumes the global approach.

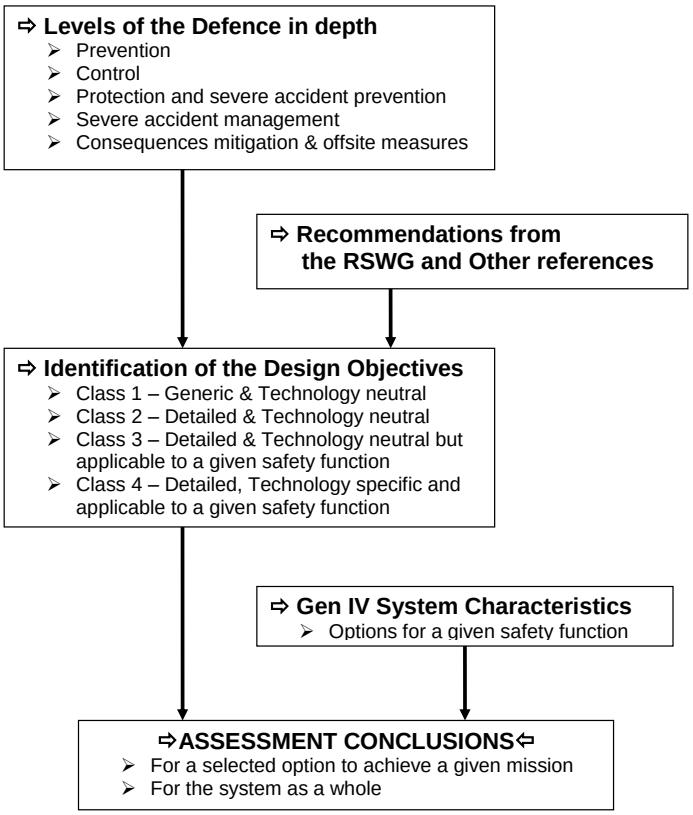


Figure 2: Approach to establish the Safety Recommendations/Characteristic (class 1 to 4) and to achieve the Qualitative Safety Review (QSR)

[15] This approach, currently used for the "value analysis", details generic recommendations (*What is necessary*) suggesting more and more detailed technical solutions (*How it can be realized*).

After the *Generic & Technology neutral recommendations* (i.e., top level: class 1 (⇨)) applicable to the future reactors (table A2.1a), the identified *Detailed & Technology neutral recommendations* (class 2 (•)) are still generic and apply to all safety related design options (table A2.1b). A further step is presented on table A2.1c.

As an example, the methodology is applied to the decay heat removal function identifying the *Detailed & Technology neutral recommendations applicable to a given safety function* (class 3 (∗)) applicable to the corresponding provisions (table A2.1c).

These tables are provided by the RSWG to help the designer to identify weak points and characteristics of a given option. Whilst the main objective of the section is to present the methodology, the recommendations listed on table A2.1 (A2.1a ⇨ A2.1c) are **open for discussion** to improve their coherence versus the claimed goals.

2.1.6 - Qualitative Safety Features Review (QSR)

Following the logic presented within the Figure 2, the system and option characteristics and features are compared to the check list's items. The options' characteristics can be rated as **"favorable" (⇧)**, **"unfavorable" (⇩)** or **neutral (⇔)** to satisfy or meet each specific recommendation of the check list. For a given option, "favorable" rating will be used to support its implementation while the identification of "unfavourable" rate will either be used to discard its selection or to motivate further R&D effort to reduce the identified drawbacks.

Perfectly in line with the Gen IV philosophy, such results are essential to identify, motivate and prioritise the R&D efforts that support the design activities and to motivate the selection among different options if several are available.

2.1.7 - Conclusions on the QSR

On the one hand, generic recommendations are already available for future nuclear plants and can provide guidelines directly applicable for the design.

On the other, the defence in depth approach remains the reference. Its effective implementation allows all of the levels to be addressed (prevention, protection, mitigation) with the objective to achieve an exhaustive, progressive, tolerant, forgiving and well-balanced defence.

The development of the DiD levels following a functional approach, that systematically integrates the available guidelines (*What is necessary ↔ How it can be realized*), allows the identification of a series of technical recommendations or desirable features applicable for the assessment of future nuclear plants. The development can be pursued to define the recommendations and foreseen characteristics and features needed for the evaluation of the provisions related to a safety function, i.e., the full set of plant options.

The corresponding check list is worked out within the Appendix 2 and as a matter of example an assessment grid useful for a qualitative analysis of design options for the Decay Heat Removal safety function is provided.

A similar approach can easily be applied to the evaluation of the design options for other important safety functions e.g., Reactivity Control and Fission Products Confinement. A further development needed for the detailed application to a given reactor technology is currently considered to be beyond the scope of this report. Such development is feasible should it be required by the SSCs (*Class 4 – Recommendations Detailed, applicable to a given safety function, but technology specific*).

It is important to point out that the results of this assessment can be extremely helpful to identify, motivate and prioritise the R & D efforts that support the system design activities.

In conclusion it is worth recalling that, within the context of the Gen IV activities, as for all the works of the RSWG, these tools are suggested by the group and have to be endorsed by the designers.

References to Section 2.1

[2.1.1] *RSWG : Basis for the Safety Approach for Design & Assessment of Generation IV Nuclear Systems January 2009*

[2.1.2] *Fundamental Safety Principles; IAEA Safety Fundamentals No. SF-1*

[2.1.3] *Safety of Nuclear power plants - Design; IAEA Safety Standards Series No. NS-R-1*

[2.1.4] *Basic Safety Principles for Nuclear Power Plants; IAEA Safety Series n°75-INSAG3 rev.1 – INSAG 12*

[2.1.5] *The Safety of Nuclear Power; IAEA Safety Series n°75-INSAG5*

[2.1.6] *Defence-in-Depth in Nuclear Safety - INSAG10 - IAEA*

[2.1.7] *INPRO Manual for the area of Safety of Nuclear Reactors; Volume 8 of the Final Report of Phase 1 of INPRO*

[2.1.8] *Principle of an operational complexity index for the characterization of the human factor relevance of future reactors concepts ; Bernard PAPIN – Enlarged Halden Program Group Sandefjord, Norway, 2004*

2.2 - Phenomena Identification and Ranking Tables

2.2.1 - Introduction

One of the assessment tools that has been successfully used and accepted as valid for the evaluation of reactor systems is the technique of Phenomena Identification and Ranking Table (PIRT). The US NRC and its contractors developed the PIRT process in 1989 as part of the Code Scaling, Applicability and Uncertainty effort [2.2.1, 2.2.2]. The PIRT is a proven formalized subjective decision-making tool, which is exhaustive, defendable, and auditable. It allows the evaluation of a concept or design by following the response of a key measurable parameter, called the "Figure-of-Merit" (FOM), chosen by a panel of experts. The technique helps to systematically identify system and component vulnerabilities and generate a ranked table identifying relative contributions to safety and risk. One of the distinct advantages of the technique is to identify the knowledge level in the phenomena, which helps identify the gaps in knowledge areas requiring additional research and data collection.

2.2.2 - Description of PIRT

The objective of the PIRT technique is to identify and rank phenomena in order of most effect on the selected Figure-of-Merit (FOM) (cf. Table 1 below). The FOM is defined as the primary criterion or the variable that is used for the determination of relative importance of each phenomenon influencing the plant behaviour. While ranking the phenomena, the adequacy of the available knowledge and the uncertainties are also assessed and documented (cf. Table 2 below). The underlying philosophy is that in complex and coupled physical systems some phenomena are more important than others during an event sequence affecting the safety of a reactor system.

Rank	***Definition***	***Application Outcomes***
High (H)	*Phenomenon has controlling impact on figure-of-merit*	*Experimental simulation and analytical modelling with a high degree of accuracy is critical*
Medium (M)	*Phenomenon has moderate impact on figure-of-merit*	*Experimental simulation and/or analytical modelling with a moderate degree of accuracy is required*
Low (L)	*Phenomenon has low impact on figure-of-merit*	*Modelling must be present only to preserve functional dependencies.*
Insignificant (I)	*Phenomenon has no, or insignificant impact on figure-of-merit*	*Modelling must be present only if functional dependencies are required.*

Table 1: Most Often Used Phenomena Ranking Scales

Rank	***Meaning***
4	*Fully known, small uncertainty*
3	*Known, moderate uncertainty*
2	*Partially known, large uncertainty*
1	*Very limited knowledge, uncertainty cannot be characterized.*

Table 2: Most Often Used Knowledge Based Ranking Scales

2.2.3 – The Individual Steps Used in PIRT

The PIRT exercise involves a panel with expertise spanning the various disciplines involved in safety and risk assessment of the problem defined by the scope.

The PIRT process can only be applied to a scenario in a reactor concept or design. It should identify, recognize, and qualify the relative importance of all relevant phenomena with the associated rationales through a nine-step process. These steps are given in Figure 3 and described in detail within the Appendix 3.

Step 1: Define the Issue
- **Step 2**: Define the Specific Objective
  - **Step 3**: Obtain Database Information
    - **Step 4**: Define Hardware and Scenario
      - **Step 5**: Establish the Figure of Merit
        - **Step 6**: Identify Phenomena
          - **Step 7**: Rank Importance
            - **Step 8**: Assess Knowledge
              - **Step 9**: Document

Figure 3: Nine-Step PIRT Process

2.2.4 - Anticipated Results

The advantage of the PIRT process is that it can be applied to conceptual designs as well as more mature designs. Information can be obtained on analytical tools used to simulate accident scenarios as well as behaviour of hardware during accident scenarios. This flexibility of PIRT allows design evaluations to proceed at any stage as long as a need is identified and the cost of performing the evaluation can be justified. The design features can be prioritized with respect to the way a reactor responds to phenomena arising from the accident scenario. The screening of plausible phenomena, to determine those that dominate the plant response, ensures sufficient and efficient analysis.

The PIRT process provides a prioritized list of phenomena, the adequacy of the knowledge and the associated uncertainties important to an accident scenario for a given reactor concept or design. This allows gaps to be defined that then need to be filled by a priority R&D effort (Figure 4).

Knowledge Base Gap Determination				
Adequacy of knowledge	Rank of Phenomenon			
	H	M	L	I
(4) Fully known; small uncertainty				
(3) Known; moderate uncertainty				
(2) Partially known; large uncertainty	GAP	GAP		
(1) Very limited knowledge; uncertainty cannot be characterized	GAP	GAP	GAP	

Figure 4: Gaps identification

Another graphic representation of PIRT outcomes is given in Figure 5. For a given phenomena, the PIRT process through expert elicitation identifies the region of high importance (in green horizontal space) and the region of high knowledge uncertainty (in yellow vertical space). The top right hand corner is the region of high importance and high uncertainty. When this space is identified and required R&D is completed, the space at the right-hand corner moves horizontally towards a region of low knowledge uncertainty, as shown by the horizontal arrow. In some instances, the importance of the phenomenon identified by the region on right hand corner could diminish, relative to other phenomena, as a result of the R&D undertaken to address that phenomenon. When such diminishing of importance occurs, the arrow in Figure 5 would point diagonally towards the origin.

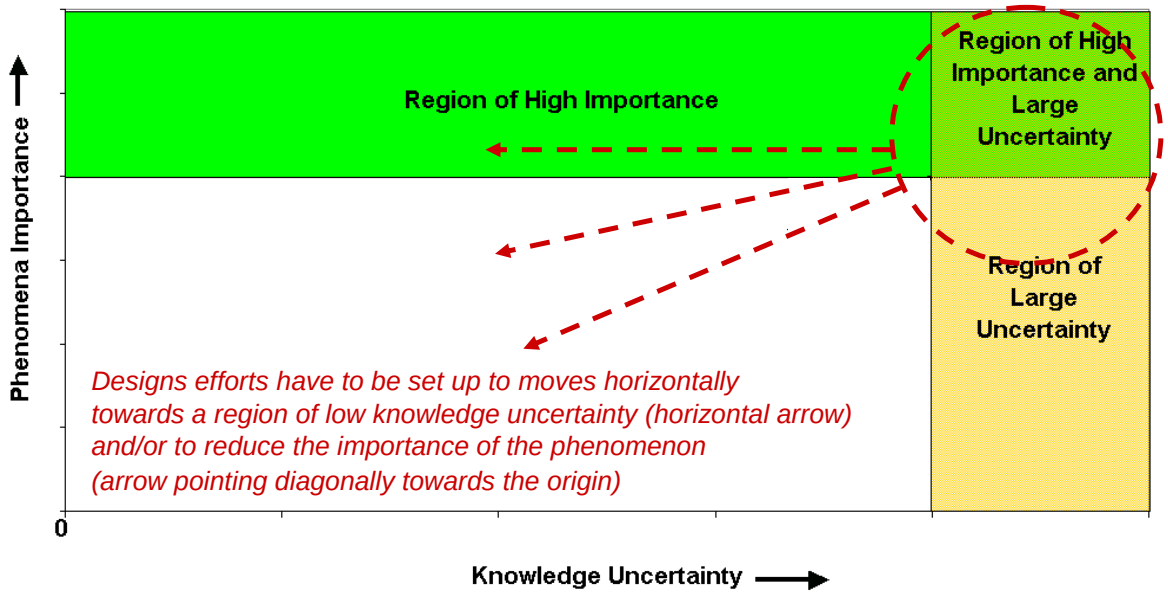


Figure 5: The Pictorial Representation of PIRT Outcome

The design can be shaped through iterative PIRTs by identifying open key issues (or phenomena) and the required R&D activities such as separate effects and integrated tests, supporting analytical solutions, modelling and code development.

PIRT technique has been used in a number of different applications such as adequacy of new designs [2.2.3-2.2.10], code development and applications for reactor safety applications [2.2.2], uncertainty analysis of computer codes [2.2.11-2.2.12], and severe accident phenomena [2.2.13]. In all of these cases, there were instances of inadequate and incomplete data. In instances where only partial data and information was available, the nature of the PIRT was declared preliminary. The PIRT technique has been used as a guide for planning cost-effective experimental programs [2.2.13] and for code development efforts [2.2.9].

2.2.5 - Anticipated Issues

While PIRT has several advantages, there are issues that need careful assessment before a panel is convened. The process can have resource penalties if the sponsor does not carefully weigh the panel dynamics and compatibility. Independence of panel members and depth of their expertise on the subject matter are significant contributors to the success of the deliberations. Independence means members without vested interest in an outcome.

The success of PIRT depends on the specificity of the scope definition. The usefulness of PIRT tends to increase with the degree of specificity to its objectives [2.2.2]. A vaguely defined PIRT could incur significant cost as the panel attempts to define the scope in collaboration with the sponsor. The PIRT sponsors need to have a clear understanding of what they need to determine from the PIRT technique and be pragmatic about the outcome. If the scope definition requires extensive analysis and computer simulations, the sponsor should factor in the cost of analysis, and provide the resources and analytical support prior to the panel deliberations.

The principle sources of uncertainty during the PIRT process arise from the adequacy of information provided to the panel, especially if the reactor design is relatively new and panel members do not know the functionality of systems and components. The second source of uncertainty arises from the use of inadequate and unqualified analytical tools to improve the understanding of event sequence and component behaviour during perturbed conditions. This uncertainty can be eliminated if decisions are made on back of the envelope bounding calculations rather than using unqualified tools. The third uncertainty may arise due to the subjectivity of the ranking process. This uncertainty can be

eliminated by carefully selecting the panel members from diverse backgrounds and on the strength of their past subject matter accomplishments.

2.2.6. - Conclusions on the PIRT

The capabilities of Gen IV systems in terms of public risk aversion and safety margin enhancement can be assessed using the Phenomena Identification and Ranking Table (PIRT) Technique. The tool has been used previously as a design assist tool to assess new reactor concepts. The tool has also been used in the assessment of safety analysis and regulatory compliance.

PIRT technique has proven to be a practical and flexible technique allowing a systematic and graded approach to technical issues of varying complexity and importance. The technique is able to systematically identify system and component vulnerabilities and generate a ranked table identifying relative contributions to safety and risk using a simple nine-step process. The technique can also incorporate uncertainties in the assessment and characterize them explicitly. One of the distinct advantages of the technique is to identify the knowledge level in the phenomena, which helps identify the gaps in knowledge areas requiring additional research and data collection.

References to Section 2.2:

[2.2.1] *Boyack, B. et al., "Quantifying Reactor Safety Margins: Application of Code Scaling, Applicability, and Uncertainty Evaluation Methodology to a Large-Break, Loss-of-Coolant Accident," U.S. Nuclear Regulatory Commission Report, NUREG/CR-5249, December 1989.*

[2.2.2] *Wilson, G.E. and Boyack, B.E., "The role of the PIRT process in experiments, code development and code applications associated with reactor safety analysis," Nuclear Engineering and Design, Vol. 186, pp. 23-37, 1998.*

[2.2.3] *Larson, T.K., Moody, F.J., Wilson, G.E., Brown, W.L., Frepoli, C., Hartz, J., Woods, B.G., and Oriani; L. "IRIS Small Break LOCA Phenomena Identification and Ranking Table (PIRT)," Nuclear Engineering and Design, Vol. 237, No6, pp. 618-626, 2007.*

[2.2.4] *S.J. Ball and S.E. Fisher, "Next Generation Nuclear Plant Phenomena Identification and Ranking Tables (PIRTs) (NUREG/CR-6944) Volumes 1 to 6, USNRC, March 2008.*

[2.2.5] *N. K. Popov, H. Sills, A. Abdul-Razzak, "Development of Phenomena Identification and Ranking Tables for the Advanced CANDU Reactor," Nuclear Technology, Vol. 158, No. 1, pp. 2-17, April 2007.*

[2.2.6] *R.B. Vilim, W.D. Pointer, T.Y.C. Wei, "Prioritization of VHTR System Modeling Needs Based on Phenomena Identification, Ranking and Sensitivity Studies," Nuclear Engineering Division, Argonne National Laboratory, ANL-GenIV-071, April 2006.*

[2.2.7] *D. J. Diamond, "Experience Using Phenomena Identification and Ranking Technique (PIRT) for Nuclear Analysis," Presented at PHYSOR-2006 Topical Meeting, Vancouver, British Columbia, Canada, September 10-14, Also available as 2006BNL-76750-2006-CP, ES&T Department / NEIS Division, Brookhaven National Laboratory, P.O. Box 5000,Upton, NY 11973-5000.*

[2.2.8] *U.S. Rohatgi, H.S. Cheng, H.J. Khan, K.W. Wulff, "Preliminary Phenomena Identification and Ranking Tables (PIRT) for SBWR start-up stability," Nuclear Regulatory Commission, Washington, NUREG/CR-6474; Also available as Div. of Systems Technology; Brookhaven National Lab., Upton, USA, BNL-NUREG-52504, March 1997.*

[2.2.9] *J. H. Song, B. D. Chung, J. J. Jeong, W. P. Baek, S. Y. Lee, C. J. Choi, C. S. Lee, S. J. Lee, K. S. Um, H. G. Kim, and Y. S. Bang, "Phenomena Identification and Ranking Table for the*

APR-1400 Main Steam Line Break," Journal of the Korean Nuclear Society, Volume 36, Number 5, pp. 388-402, October, 2004.

[2.2.10] *H.E. Sills, et al., "PIRT Efforts in Support of ACR-700 Computer Code Validation," 25th Annual Conference of the Canadian Nuclear Society, Toronto, Ontario, Canada, June 6-9, 2004.*

[2.2.11] *R.K. Ratnayake, et al., "Identification and Ranking of Phenomena Leading to Peak Cladding Temperatures in Boiling Water Reactors During Large Break Loss of Coolant Accident Transients," Proceeding s of ICONE10, 10th International Conference on Nuclear Engineering, Arlington, VA, April 14-18, 2002.*

[2.2.12] *M.P. Gol-Mohamad, M. Modarres, and A. Mosleh, "Modified Phenomena Identification and Ranking Table (PIRT) For Uncertainty Analysis," Proceeding s of ICONE14, 14th International Conference on Nuclear Engineering, Miami, FL, July 17-20, 2006.*

[2.2.13] *D. Magallon, et al., "European Expert Network for the Reduction of Uncertainties in Severe Accident Safety Issues (EURSAFE)," Nuclear Engineering and Design, Vol. 235, pp. 309-346, 2005.*

2.3 - Objective Provision Trees for assessment of adequacy of Defence-in Depth (DiD)

2.3.1 – Introduction

Application of the concept of defence in depth in the design of a plant provides a series of defence levels aimed at preventing severe plant conditions and ensuring appropriate protection in the case that prevention fails. This strategy has been proven to be effective in compensating for equipment and human failures, both potential and actual.

In this context, the key objective of the RSWG is to provide tools which allow the designer to materialize the levels of the DiD; this seems interesting to guide the construction of innovative safety architectures[16], and to work out instruments which will allow a better demonstration of the robustness of the result.

To implement and assess the adequacy of the DiD for NPPs several approaches and methods have been used. Works performed under the aegis of the IAEA suggest the use of a systematic approach for making an inventory of the Defence in Depth capabilities of a plant [2.3.1] through development of Objective Provision Trees (OPT) [2.3.2] specifying design provisions at each level of defence. RSWG elaborated further on the methodology and propose the implementation of OPT in an iterative manner in the development of the design concepts of the Gen IV systems from the very beginning.

It is believed that applying the OPT in an iterative process will help designers to identify all measures and provisions needed to sketch the design safety architecture, having identified and addressed all potential hazards posed by the plant. Contrary to the experience from the past, when the assessment of the systematic application of DiD of the existing plants resulted in many safety backfits, it is expected that for Gen IV, the application of OPT at a very early stage will allow safety to be built-in the design concepts. This work has to be done in relationship with the technological development of the design concepts taking into account that the application of the OPT will support also the identification of all potential hazards and possible initiating events and disturbances to be considered in the design, which for innovative concepts may not be an easy task. It is important to note that, for the identification of the initiating events, OPT is accomplishing the same functional and analytical objectives as a Failure Mode and Effect Analyses (FMEA), Hazard and Operability Study (HAZOP) or any other methodology used for this purpose. An essential difference, however between the OPT and the FMEA is that the former helps to build the skeleton of the safety architecture according to the principles of defence in depth while the latter does not support explicitly such a process. If applied in a complementary manner to OPT however, FMEA could help to verify that all possible interactions between provisions are properly taken into account and no significant initiating events identified by the OPT are overlooked. From this point of view FMEA is complementary to the OPT for it is involved in the establishment of DiD only to identify corrective measures at different levels - prevention, control, mitigation of - but not necessarily to build a safety architecture.

2.3.2 - Description of OPT

The Objective Provision Tree (OPT) is a practical tool [2.3.3] which should be applied on line to design and/or to assess the structure of the safety architecture of innovative Nuclear Power Plants (NPPs) coherently with the DiD philosophy [2.3.4]. This is done through visual presentation and a systematic inventory of the NPP prevention/control/mitigation capabilities, i.e., the systematic identification of the provisions that participate to the safety mission's achievement. Its use requires a minimal knowledge of the installation characteristics and phenomenology, and the associated risks.

[16] Conventional architectures (e.g., for the Gen III LWR) are built in an evolutionary manner with improvements which can be important but not necessarily radical compared to the previous design; for the innovative systems, the increasing role of new and original provisions (e.g., more intrinsic safety characteristics, passive systems, etc.) justify the search for instruments which will allow the designer to prove that all the safety principles are correctly addressed even if this is done with innovative solutions.

The OPT method aids design development and its safety assessment by integrating, in a preliminary and macroscopic way, concerns of performance of the provisions and their reliability, without waiting for detailed PSA models to be developed. It allows the designer to make sure that:

- the provisions required at each level of the defence in depth and for each plausible challenge to the safety function, exist and are correctly implemented (i.e., without controversial interactions) and
- singularly, these provisions can meet the design performance requirements (physical performance of provisions and their reliability). The final proof of this single capability to meet the requirements is obviously supported by specific deterministic assessment.

The quantitative assessment remains to be done with a tool such as PSA which is able to consider and quantify the whole behaviour of the safety architecture for the full set of selected initiating events, sequences and plant conditions.

On the basis of the process under examination and the phenomenology involved under an installation's abnormal situations, the OPT method provides a top-down method with a tree structure which:

- for each level of DiD (normally level 1 to 5),
- and for each safety objective/function (in general, control of reactivity, removal of heat from the fuel, and confinement of radioactive materials),

identifies:

- the possible challenges to the safety functions
- the plausible mechanisms which can materialize these challenges
- the provided provision(s) to prevent, control or mitigate the consequences of the challenges/mechanisms,

All this is expressed through a hierarchical structure of relationships in the form of a tree.

The OPT method is an approach expressed through a number of trees, and, in general, there are three levels of structures which form the logic framework of this method.

1) List of safety functions and relevant DiD level to be assessed by OPT: The implementation of DiD philosophy should be assessed for all the related safety functions for each relevant DiD level, thus this list indicates the total number of the OPTs for all safety functions and all DiD levels.
2) Hierarchy structure: A hierarchy structure expressed as a tree, from the top level of "DiD level ⇨ safety functions" to the lowest level until the "elemental structure (challenge ⇨ mechanism ⇨provisions)."
3) Elemental structure: The lowest part of the tree, showing "provision(s)" foreseen against specified "challenge/mechanism."

The hierarchy structure of OPT expresses the process of deducing safety-deteriorating mechanisms and provisions to cope with these mechanisms, starting from the DiD level and safety objective at the upper part of the tree. Normally, the hierarchy structure of an OPT consists of the following levels from the top to the bottom (see Fig.6):

- *Level of DiD* — *level 1 to 5*
- *Objectives and Barriers* — *to be achieved and to be protected*
- *Safety Function* — *to be maintained (to be performed successfully)*
- *Challenge* — *to cope with (e.g., disruption of heat transfer path)*
- *Mechanism* — *to be prevented or controlled (e.g., loss of coolant)*
- *Provision* — *to be implemented to prevent and/or control mechanisms.*

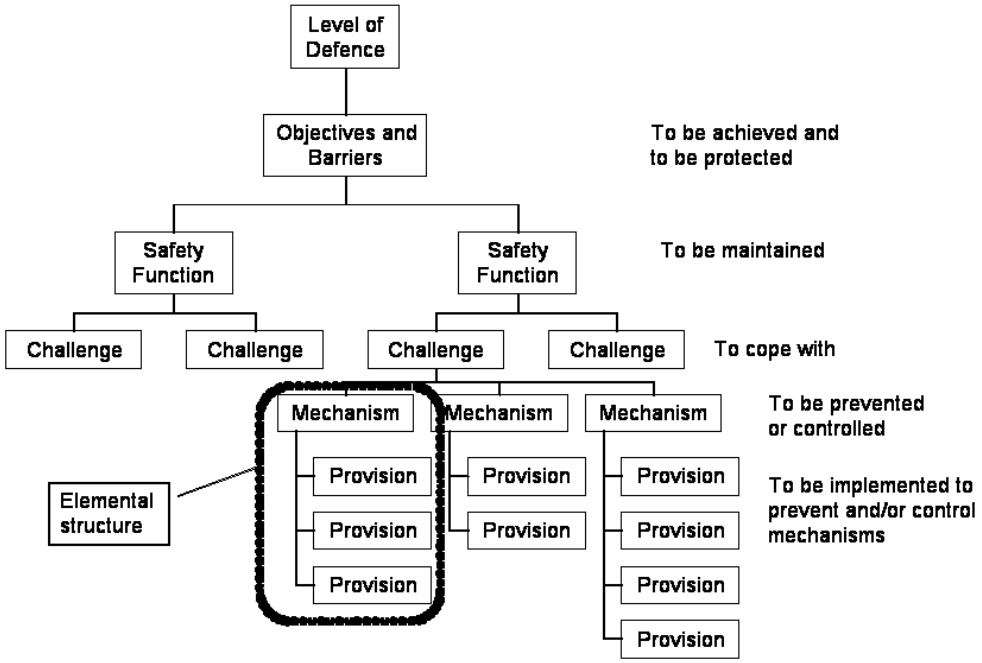


Fig. 6 Hierarchy Structure of OPT

The elemental part of the OPT structure exists at the lowest part of the tree (see Fig. 7). This structure addresses a specific mechanism that could deteriorate safety function, and identifies the set of provisions that is designed to work jointly to prevent or control the mechanism and its potential consequences. The provision will be single or plural, and include hardware, engineered systems, passive or inherent features, operator's actions, administrative procedures, and so on. If plural provisions are implemented and all of them are expected to work simultaneously or sequentially (in other word, "AND logic") to achieve the mission, those provisions are placed in a vertical manner and connected with a vertical line. For a given level of the DiD and a given safety function, such a set of provisions is called as a Line of Protection (LOP).

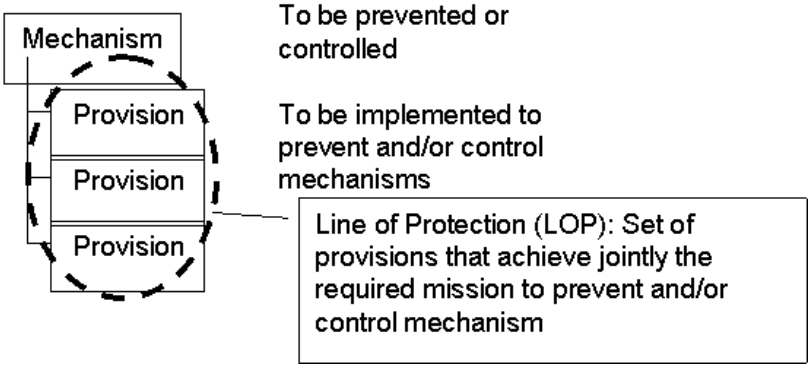


Fig. 7 Elemental structure of OPT

A LOP is a "*coherent combination of provisions*", sufficient to assure the required safety function. LOP effectiveness is characterized by its physical performances[17], its reliability[18] and the degree of independence vis-à-vis other LOPs[19]. The requirements concerning physical performances and

[17] I.e.,: the capability to keep the plant's physical parameters within the allowed ranges.
[18] Finally the probability to correctly achieve the requested mission.
[19] Following one of the key principles of the DiD the failure of a given level (i.e.,: the failure of the provisions which materialize the level) shall not affect the capability of the following level to fully achieve the requested mission.

reliability, i.e., the mission's success criteria, depend on plant conditions (which are going to evolve during the accident) and on the level of defence in depth to which the LOP is required to operate.

The LOP as a "*coherent combination of provisions*" acts as a single element i.e., a single chain with several links. The knowledge of its composition allows the pertinence of its design to be checked in terms of performance and reliability as a whole, identifying the possible weak "links" of the LOP chain. The identification of such weak links can be of prime importance for the designer to prioritize the effort needed to ensure that the final set of provisions is as homogeneous as is feasible from a reliability point of view.

2.3.2.1 - Objective of the OPT

The objective of constructing the OPT is to help designers to ensure that Defence in Depth philosophy is or has been applied in a systematic, comprehensive and adequate manner from the very beginning of the design process.

The iterative implementation of this task at different design stages allows the designer to successively elaborate design details which demonstrate unambiguously the consistency with the DiD principles. The final objective remains the verification that the safety architecture guarantees a DiD which is *exhaustive, balanced, progressive, tolerant and forgiving*. The availability of the OPT can contribute to this objective at least for the *exhaustive*, the *tolerant* and the *forgiving* aspects, the performances of the provisions being defined consequently.

The availability of the OPT will also help produce well structured and defendable evidence on DiD application when comparing different design options or discussing safety matters with safety authorities and regulators.

Moreover, for the qualitative assessment, the availability of an exhaustive overview of the safety architecture, allows the possible interactions between provisions to be checked to insure that no contradictory missions are allocated to these provisions. Following this logic, it is worth noting that the OPT, if its use is extrapolated to organize the "security provisions", could be useful to help harmonizing the safety and security approaches; this can be done checking that provisions for safety are not in contradiction with the security requirements and vice-versa.

Finally the availability of such a comprehensive vision of the safety architecture has to be seen as an essential input for an exhaustive PSA that will be in charge of quantitatively assessing characteristics of the plant such as the degrees of "*balanced*" and "*progressive*" safety.

2.3.2.2 - Individual steps of OPT (see Appendix 4 for details)

The OPT construction process begins with some crucial steps performed by the design and/or research organization.

2.3.2.2.1- Team setting and defining the analytical scope

The best application of the OPT methodology [2.3.5] showed that it is very important that all of the staff involved in the exercise have the same understanding of the key elements, terminology used and scope of the assessment.

After initial training, it is recommended to start the exercise by the development of an OPT for a given level of defence in depth and given objective and safety function by each of the working teams. Based on the comparison and mutual verification of the performed work, a common understanding of the methodology shall be developed which is needed for its further consistent application.

2.3.2.2.2 - Data gathering

Second step shall be the collection of design, research and safety assessment documentation that may be needed to develop the OPTs. At this particular stage consideration shall be given to the available

design and/or safety analyses associated with different safety issues and phenomena. It should be ensured that the documentation of all phenomena identified by previously developed Phenomena Identification and Ranking Table (PIRT) exercise are available to the OPT team. It is evident, however that in the process of OPT's development, there might be some need for extra information.

2.3.2.2.3 - Development of the OPTs

The construction and development of the OPTs shall start with consideration of the three fundamental safety functions: reactivity control, fuel heat removal and confinement of radioactive materials and shall cover at least levels 1 to 4 of the DiD.

The set of possible challenges has to be identified for all given objectives as expressed for example in terms of acceptable achievement of safety functions i.e., the mission's success criteria. At each level of defence, the set of possible challenges[20] has to be identified (e.g., for the safety function "*reactivity control*", the challenge could be "*insertion of unallowable positive reactivity*"), and all root mechanisms[21] leading to the challenges have to be specified (e.g., for the example above, the "*control rod withdrawal*").

Eventually, to the extent possible, the comprehensive list of safety provisions that contribute to preventing the mechanism from taking place, is described and illustrated in the form of "objective provisions trees"[22].

At the pre-conceptual and conceptual design stages, concurrent alternatives may exist and it is up to the designers to select the best one, keeping in mind the need to achieve exhaustive, tolerant, forgiving, balanced and progressive DiD by means of robust, reliable and as simple as possible design solutions. Attention shall be paid to those design items that may form part of different lines of protection and may raise conflicts among the different missions during implementation.

With the evolution of the design and development of detailed design solutions, the designer/assessor shall be able to apply the OPT method to assess the design provisions for more specific safety functions or principles [2.3.6] derived from the fundamental safety functions. An example of a detailed subdivision of the three fundamental safety functions for light water type of reactors is provided in Appendix 4.

An example of OPTs developed for one of the three fundamental safety functions and level 3 of DiD for Japanese Sodium Cooled Fast Reactor [2.3.5] is provided in Figure 9 (Chap. 3.3). A more comprehensive example of application to the HTR concept is given by the reference [2.3.3].

2.3.2.2..4 - Documentation of the results

Along with the graphical development of the OPT, it is suggested to complement this process with development of an excel file which will allow and give some unique numbering for each of the branches and/or elements of the OPTs, thus allowing better link between graphical trees and the provisions documentation.

In addition to the graphical/ Excel representation of the OPTs, it is of high importance to document all information which was used when identifying each set of safety provisions and when judging on its adequacy.

[20] Challenges: generalized mechanisms, processes or circumstances (conditions) that may impact the intended performance of safety functions; a set of mechanisms have consequences which are similar in nature.

[21] Mechanism: specific reasons, processes or situations whose consequences might create challenges to the performance of safety functions.

[22] Objective provisions tree: graphical presentation, for each of the specific safety principles belonging to the five levels of in depth, of the following elements from top to bottom: (1) objective of the level; (2) relevant safety functions; (3) identified challenges; (4) constitutive mechanisms for each of the challenges; (5) list of provisions in design and operation preventing the mechanism to occur.

2.3.3 - Major inputs and outputs of OPT

To complete this OPT task, the designers need to have available the general design documentation and any information relevant to the boundary conditions and reliability performance parameters of design for safety critical equipment. Any safety and reliability analyses available at different stages of the design evolution should be used. The input on major phenomena and their ranking as output of PIRT, if available, is obviously essential.

As an output of this task comprehensive information will be available on:

- What are the sets of provisions needed to ensure that all identified safety functions are maintained – this will include identification of individual sets of provisions, judgment on their reliability and selection of the best design options, if several sets of provisions can provide similar degree of safety.
- Graphical representation of the safety related design architecture that will be very useful in the development of Probabilistic Safety Assessment (PSA) models. In addition, the reliability data and expert judgments collected within this task will provide valuable input for PSA model quantifications.
- Graphical representation of the design architecture that will be very useful in development of deterministic Accident Analyses (AA). The OPTs, in particular the "Challenges and Mechanisms" part, will help to determine the list of Postulated Initiating Events (PIEs) to be addressed in AA.
- Systematically identified design provisions and topics which need further research/ and development and experiments to judge on their adequacy or not with regards to the design safety objective
- How well the reactor system design applies the DiD principles and whether the applied DiD is exhaustive, tolerant and forgiving; as indicated above, the "balanced" and the "progressive" aspects will be quantitatively assessed by the implementation of the complete PSA.
- The availability of the OPT will also help produce well structured and defendable evidence on DiD application when discussing safety matters with safety authorities.

2.3.3.1 - Stages of the design evolution to complete OPT

The OPT methodology for assessment of DiD application may be applied at any stage of design evolution. As indicated above this analysis supports the designers in identifying that adequate safety provisions exists at any design stage and, if needed, indicates how to implement complementary provisions. It is evident, however, that applying OPT methodology in a general way at an early conceptual stage and increasing the level of details of the OPTs along with the evolution of the design feature is the preferred option.

2.3.3.2 - Relationships between OPT task and other tasks for safety assessment

As indicated above the OPT task, in providing the comprehensive view of the plant's safety architecture, ideally fits in the safety assessment process between preparation of PIRT and development and quantification of reactor design specific PSA models.

The OPT development could also help in identifying new mechanisms specifically related to given provisions and providing feedback on the PIRT stage cannot be excluded.

2.3.4 - Anticipated Results and Applications

As already indicated, creation of OPTs is an iterative process. After it is first applied, results of requested experiments, design changes, sensitivity studies, or other results from simulations may require revisions to the original OPTs and associated documentation. However, the value of the OPTs development process lies not in absolute accuracy at a point in time, but in its rational guidance in allocation of limited research resources to a complex research process and justifiable demonstration of the adequacy of DiD for any reactor system.

During the conceptual phase, the results of OPT construction have potential to guide further research efforts needed to ensure that DiD is exhaustive, tolerant and forgiving by means of robust, reliable and simple design solutions. The full consistency with the recommendations for balanced and progressive safety will be guaranteed by the PSA.

2.3.5 - Recognized or Anticipated Issues

2.3.5.1 - Uncertainties

The major sources of uncertainties for this task are associated with the availability of scientific and engineering evidence of the effectiveness of the selected safety provisions (i.e., their physical performances and expected reliability). For the innovative designs, it might be expected that available operational test data are inadequate to support the judgments on the reliability of the innovative solutions. It is expected to start the evaluation with qualitative expert judgements that eventually, with the evolution of the design solutions and progressive research and development, will be replaced with quantitative measures.

Having said that, the designer must be aware that the analysis of these uncertainties would also help select among the different possible options. Moreover, the consciousness about these uncertainties becomes the rationale for further R&D effort, fitting perfectly with the GIF approach.

2.3.5.2 – Needs for flexibility

Difficulties in terms of applicability may arise. The designer is faced with situations for which it will be difficult to identify the one to one correspondence between the levels of defence in depth and different provisions. Flexibility is essential but this does not question the foundations of the approach. In Annex A4b the problem is addressed and solutions are proposed.

References to Section 2.3:

[2.3.1] *Assessment of Defence in Depth for Nuclear Power Plants, Safety Reports Series No 46, IAEA, Vienna (2005)*

[2.3.2] *Proposal for a Technology-Neutral Safety Approach for New Reactor Designs, IAEA TECDOC 1570, Vienna (2007)*

[2.3.3] *Considerations in the Development of Safety Requirements for Innovative Reactors: Application to Modular High Temperature Gas Cooled Reactors, IAEA TECDOC 1366, Vienna (2003).*

[2.3.4] *Defence in Depth in Nuclear Safety, INSAG-10, A report by the International Nuclear Safety Advisory Group, IAEA, Vienna (1996)*

[2.3.5] *Findings from pilot use of the OPT methodology for JSFR, H. Niwa, S. Kubo, JAEA, Presentation given at the 4th GIF RSWG Meeting, Paris (26-28 April, 2006)*

[2.3.6] *Safety of Nuclear Power Plants: Design, IAEA Safety Standard Series, Safety Requirements No. NS-R-1, IAEA, Vienna (2000).*

2.4 - Application of Deterministic and Phenomenological Analyses (DPA)

2.4.1 – Brief description of DPA

2.4.1.1 - Nature of the Task

Although the ISAM emphasizes PSA as its central element, traditional deterministic analyses of thermal-hydraulics, reactor physics, severe accident behaviour, structural response, and a great many other issues remain a vital part of the safety evaluation of Gen IV systems. Indeed, by definition, a complete PSA must include many inputs that are primarily derived from deterministic analyses. [2.4.1].

On the one hand the conventional "*deterministic approach*" where the safety analysis is uniquely based on deterministic assessment and the adoption of conventional rules and, on the other, a "*risk based approach*" where all the design would be supported and demonstrated only through probabilistic demonstration. Considering the evolution of the safety approach, the former seems today insufficient because new tools are available (e.g., PSA) and it seems essential to exploit their contribution, and the latter is certainly inadequate for the degree of experience feedback does not allow the demonstration only on probabilistic insights.

This "risk informed" methodology, looking for and considering simultaneously deterministic and probabilistic insights, suggests that the use of Objective Provision Tree and Probabilistic Safety Assessment (given in the next section) as main tools to evaluate in a systematic way the implementation of Defence in Depth principle to achieve the plant design safety should be kept. Deterministic assessments, including engineering evaluations, consideration of human factor[23] and 'traditional" deterministic safety analysis are needed to support the application of OPT and PSA.

Deterministic safety analyses, in this context, are first of all needed to evaluate the adequacy of the chosen provisions (combined in lines of protection in the OPT) to fulfil their expected functions and establish "success criteria" for the System, Structures and Components modelled in the PSA. Deterministic analyses are also needed to determine the consequences in terms of "acceptability or not" of different event sequences modelled in the PSA.

In case of deterministic assessment, which supports PSA, it is preferable to use best estimate computer codes and best estimate analyses for the corresponding accidents and sequences analyses. Sensitivity analyses shall be performed to establish margins to limits and to cover imprecision in actual parameters at the design stage. The computer programmes, analytical methods and plant models used in the deterministic analysis shall be verified and validated, and adequate consideration shall be given to uncertainties. Experiments, also driven by PIRT exercises, shall be conducted to support deterministic model validations as well as accident sequence outcomes assessment.

> Nota bene: *Discussing the deterministic assessment one must be aware that, as anticipated above, this can be requested within the context of a conventional and self standing "deterministic approach" where only a given set of pre-determined event and sequences are selected and analyzed. In this case the sequences will be assessed implementing specific rules to address the uncertainties concerns; for the so called "design basis" conservative approach will be privileged while for the design extension conditions (former "beyond design basis") "best estimate" approach will be preferred.*

It is clear, that at a later stage, and in particular during the licensing phase, a full scope of deterministic safety analysis may be needed to demonstrate that the plant as designed is capable of meeting any prescribed limits for radioactive releases and acceptable limits for potential radiation doses for each category of plant states [2.4.2]. This type of analyses will include [2.4.3]:

[23] The consideration of human factor within the deterministic approach will be achieved considering explicitly the grace delay as "decoupling factor" between, on one side, the needed physical performances of the safety architecture and, on the other side, the potential for the operator to interact with the installation's behavior

1) confirmation that operational limits and conditions are in compliance with the assumptions and intent of the design for normal operation of the plant;
2) identification of PIEs inherent to the plant design.
3) analysis and evaluation of event sequences that result from PIEs;
4) comparison of the results of the analysis with radiological acceptance criteria and design limits;
5) confirmation of the design basis;
6) demonstration that the management of anticipated operational occurrences and design basis accidents and severe plant conditions is possible by automatic response of safety systems in combination with prescribed actions of the operator (with a sufficient grace period[24]).

2.4.1.2 - Objective of the task

The objective of this task is to provide the quantitative insights that are needed to support the achievement of the PSA. The integration of deterministic and probabilistic safety analyses will allow the designer to assess the adequacy in terms of physical performance of the designed LOPs for each level of Defence in Depth (DiD). The integration of deterministic results within the PSA will also allow the degree of achievement of safety architecture characteristics such as "exhaustive", "progressive", "tolerant", "forgiving" and "well-balanced" [2.4.1] to be assessed and quantified. The iterative use of this task at different design stages will allow a review and possibly a modification of the design details in order to verify the adequate application of DiD in the final reactor system design.

2.4.1.3 - Task individual steps

Performing a deterministic analysis is a complex task, which places significant requirements on analysts. These requirements usually include knowledge of the dominant physical phenomena and associated computer code(s) used in the analysis. Deterministic safety analysis also called "accident analysis" is performed in several steps. These steps need not always be sequential; some can be carried out in parallel. Different kinds of activities are performed within each step. A general flow chart illustrating this procedure is shown in Figure 8. The main activities are briefly summarized within the Appendix 5 [2.4.4]:

[24] Grace period: the period of time during which a safety function is ensured in an event with no necessity for action by personnel. The grace period might be achieved by means of the automation of actuations, the adoption of passive systems or the inherent characteristics of a material, or by any combination of these (IAEA safety glossary).

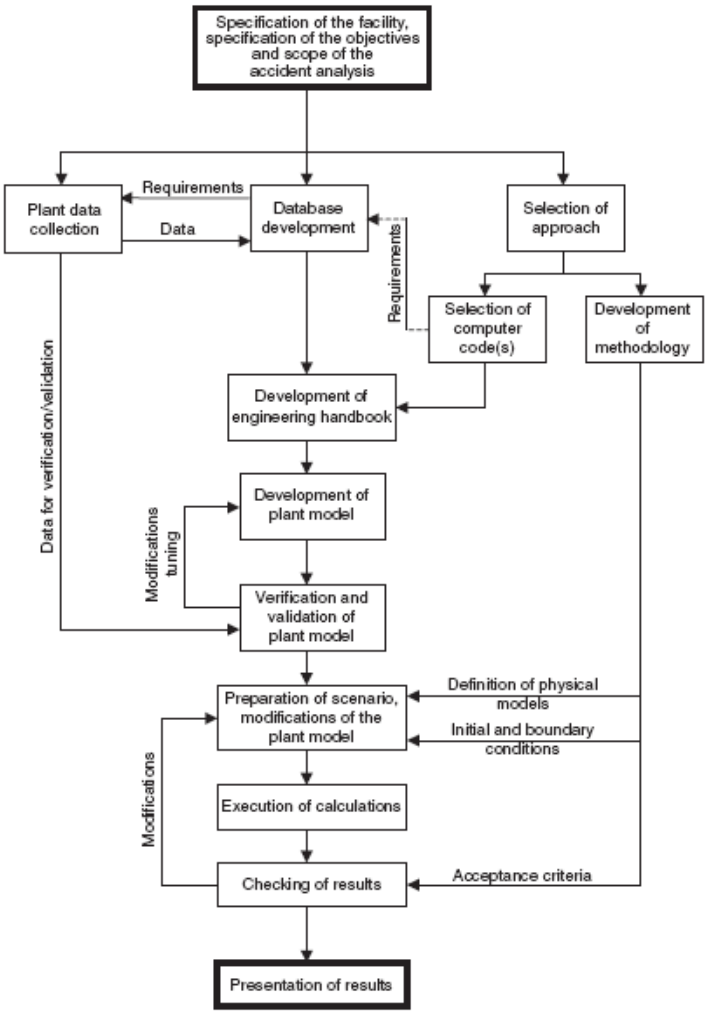


Figure 8: Main steps in the deterministic analysis.

2.4.2 - Major inputs and outputs

Inputs and outputs of the deterministic safety analysis are obviously strongly related to the results expected from the PSA for a given accidental sequence.

An accident sequence is the combination of an initiating event and hardware and human failures (provisions/LOP failure) that can potentially lead to undesirable consequences. The subsequential possible stages of an accidental sequence follow the logic of the DiD where the failure of a given level (i.e., of the corresponding LOP) is controlled and managed by the following level (i.e., by the corresponding LOP).

The deterministic analysis is implemented to quantitatively and mechanistically describe the sequence and, considering the physical performances of relevant LOPs, to assess the consequences at each stage of the sequence until unacceptable conditions occur.

To execute a deterministic analysis, analysts need to have available all design documentation and any information relevant to the initial and boundary conditions and physical performance of the relevant LOP and the corresponding provisions. Any safety/reliability analyses available at different stages of the design evolution should also be used. The input coming from PIRT on major phenomena and their ranking shall also be useful to evaluate the level of conservatism to apply on certain assumptions.

As output, this task will provide the:

1) confirmation that design provisions forming each line of protection can adequately perform their expected functions;

2) determination of the "success criteria" to be required for the physical performance of the system, structures and components (provisions/LOP), modelled in the PSA together with a clear definition of the consequences at each stage of the sequence included in the PSA.

2.4.2.1 - Deterministic analyses at the different stages of the design evolution

Linked to PSA itself, the corresponding accident analysis can be performed at any stage of the design, for example, at conceptual or early design stage, at the final design stage or during the design licensing phase. However it is recommended to associate them to the design process from the conceptual stage in order to have a continuous safety assessment of the reactor design. Accident analyses for various stages differ mainly in the level of knowledge of the layout and characteristics of the plant systems.

2.4.2.2 - Relationships between deterministic analyses task and other tasks for safety assessment

The relationship between PIRT, OPT, PSA and deterministic analysis is established within the iterative process to review the adequacy of the measures taken to implement the Defence in Depth philosophy. In particular the deterministic analysis, together with PSA, provides a means to evaluate the efficiency of the provisions defined in the different LOP to ensure that the relevant safety functions are respected and all important phenomena are considered.

2.4.2.3 - Anticipated Results and Applications:

As already indicated, the deterministic analysis within the framework of a risk informed approach shall provide together with PSA a comprehensive view of the overall safety of the plant for the whole range of the event probability-consequence spectrum. The risk informed approach will be integrated in the design to assess its safety and compliance with the Defence in Depth principles.

2.4.3 - Recognized or Anticipated Issues

The major limitations and constraints associated with this task are to be found in the availability of scientific and engineering evidence on the qualification of the models, correlations and methods adopted in the analysis.

For innovative designs it is reasonable to expect that insufficient operational or experimental data are available to support the validation of the computational tools used. The use of passive systems, new materials, new physics, all contribute to the uncertainty in the results.

It is expected to start the analysis with some conservative assumptions based on expert judgments, which will be removed eventually with the development of the design solutions and progress in research. At this stage PIRT applications represent a valuable means to minimise those conservative assumptions and to define a structured research programme.

References to Section 2.4:

[2.4.1] *Basis for the Safety Approach for Design & Assessment of Generation IV Nuclear Systems, RSWG Report January 2009.*

[2.4.2] *Safety Assessment and Verification for Nuclear Power Plants, IAEA Safety Guide No. NS-G-1.2, IAEA, Vienna (2001)*

[2.4.3] *Deterministic Safety Analysis for Nuclear Power Plants, IAEA Draft Safety Guide DS 395 draft 8, IAEA, Vienna (2008).*

[2.4.4] *Accident Analysis for Nuclear Power Plants, IAEA Safety Report Series No. 23, IAEA, Vienna (2002).*

[2.4.5] *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants. Chap 15 Accident Analysis, NUREG-0800, USNRC. March 2007*

2.5 - Probabilistic Safety Assessment

2.5.1 Introduction

The recommended RSWG methodology for evaluating the safety of Gen IV nuclear systems includes elements that are deterministic, probabilistic, qualitative and quantitative. They attempt to reflect a Risk Informed approach and this is why the methodology is structured with the objective to achieve a Probabilistic Safety Analysis (PSA). This section describes PSA, and discusses its role in the development, design, licensing, and operation of Gen IV nuclear systems.

2.5.2 Description

PSA is a rigorous, systematic, and comprehensive tool for identifying and estimating the likelihoods of sequences of events that can result in the loss or damage related to the design and operation of complex engineered systems. Also known as Probabilistic Risk Assessment (PRA), PSA has been widely practiced in the nuclear power field since its first major application in the WASH-1400 Reactor Safety Study published in 1975.

The essential construct underlying PSA is the potential interaction between technological **hazards**, potential **challenges** that create possibilities for those hazards to cause loss or damage, and the effectiveness or reliability of **safety provisions** that are provided in a system design to prevent or mitigate the potential loss or damage. It is the interaction between these variables that gives rise to the level of **risk** associated with a particular technology or design. In general, it can be observed that risk is directly proportional to the magnitude of the hazard and the frequency of challenges, and inversely proportional to the reliability of safety provisions, associated with a given technology. The level of risk is conventionally expressed by measures that describe both the frequency and the consequences of certain sequences of events that result in loss or damage.

PSA is a means of systematically answering three important questions relating to the risk and safety of a complex system. These are:

- What can go wrong? That is, what kind of upset conditions (states of disequilibrium) can possibly arise in a given system that could, if not successfully controlled and mitigated, lead to adverse consequences?
- What is the frequency of events, or combinations of events, that, if not controlled and mitigated, have the potential to lead to adverse consequences?
- What are the frequencies of the various adverse consequences that are potentially associated with the technology or system?

Collectively, these three questions are sometimes referred to as the "risk triplet." In answering these three basic questions, it is necessary to develop analytical results at a number of intermediate levels, each of which is useful in better understanding the risks and safety issues associated with the system.

Historically, PSA has sometimes been thought of as an "alternative" form of safety analysis differentiated from the more traditional "deterministic" methods such as thermal-hydraulic modelling, structural mechanics, reactor physics, and the like. More correctly, however, PSA should be thought of as a type of safety analysis that integrates all relevant information about the safety and risks of a system. This information will include knowledge about the physics associated with system design and operation, as well as information about the frequency of reactor transients or loss of coolant events, component failure rates, potential human errors, and a great many other issues, as well as expressing the level of uncertainty inherent in this information. Thus, PSA should not be thought of as an alternative to deterministic analysis, but rather as an integrated framework that incorporates deterministic analysis as one type of information, along with all other kinds of information available regarding the system as it relates to safety. The aim of PSA is to integrate all known information about the system to systematically identify what can go wrong, how likely it is that they can go wrong, and what the resulting consequences are likely to be.

2.5.3 Developing PSAs for Generation IV Nuclear Systems

As mentioned previously, PSA has been widely applied in the nuclear power field since the late 1970's. Many references and examples detailing how to perform a PSA exist elsewhere, so no attempt to define or prescribe how to perform a PSA will be offered here.

As applied to Gen IV systems, the principal role of the PSA is to provide the analytical framework in which to systematically:

1) identify a complete set of accident sequences,
2) estimate the frequencies of those sequences, and
3) provide a full account of the attendant uncertainties.

The RSWG envisions that PSA should be used throughout the Gen IV system development cycle. As a general principle, the complexity and level of detail of the analysis will increase as the system design evolves. Specific applications of the PSA results will be associated with each stage of design development. At a high level, the PSA will be of significant value in three major phases of Gen IV technology development. These are the design and design selection stage, the licensing stage, and the operational stage.

2.5.3.1 PSA in the Design Stage

Too often in the past, PSA has been used essentially "after the fact" in the nuclear power plant design process. That is, PSA has been used principally to measure the level of risk associated with a design *only after the design is already quite mature, often after the plant is actually licensed and operating.* Although development and application of PSA in this late stage of technology development certainly has proven value, much greater value can be realized by applying PSA from the earliest stages of the design, and using insights derived from the PSA to drive the design based on an understanding of safety vulnerabilities and their potential for risk reduction.

Even in the earliest stages of conceptual design, simple PSA models can be useful in understanding how a design can be vulnerable to certain failures. As the design matures, based in part on an understanding of those vulnerabilities, the complexity of the PSA should also mature to yield more detailed insights into safety and risk issues associated with the design.

PSA may also be used to help understand differences in the level of safety associated with various candidate options within a Gen IV concept. Thus, PSA can serve as a basis for selecting the designs that optimally meet certain selection criteria in which safety is a prominent consideration. Examples might include selecting a design that offers the lowest level of public risk, selecting a design that offers the highest level of safety for a given level of cost, balancing price per kilowatt against measured level of public risk. Obviously, the use of PSA results in making such selections or decisions requires a thorough understanding of how the results were developed and what they mean. As in all aspects of PSA, a detailed understanding of uncertainty issues may be particularly important. See Section 2.5.6, below, for additional discussion of uncertainties.

Finally it is important to consider the PSA not only for the results that correspond to the conventional levels 1, 2 and 3 (cf. § 2.5.5 for details) but also for the indications that are obtained at the intermediate stages, i.e., before the core degradation. These indications are essential to check the meeting of objectives for the DiD such as progressiveness, tolerant, forgiving and well-balanced.

A particularly important use of PSA during the design process is in the area of defining and developing design features that offer appropriate levels of safety margin. Safety margin is, of course, one element of defence in depth, and represents, by definition, "something more than what is needed to perform some important safety function." Safety margin is the prudent response to uncertainty. Examples include all the spectra of physical parameters essential to guarantee the plant safety i.e., the neutronics, themal-hydraulics, and mechanics.

Minimal cut sets and quantitative importance measures are particularly useful to understand aspects of design and operation that are contributing most to risk metrics of concern and that, consequently, hold most potential for risk reduction through improved design features.

2.5.3.2 PSA in Licensing

PSA is used extensively by nuclear regulators around the world as a key input to the process of certifying, licensing, and regulating nuclear power plants. Regulators widely recognize the value that this rigorous and comprehensive technique has in developing insights into the safety issues that are important in this realm. Because PSA has become such an important part of the licensing process, the RSWG believes that the development of a detailed PSA, that has both evolved along with the design and contributed to the development of that design, will be a particularly powerful tool in communicating with national nuclear regulatory bodies throughout the licensing phase. By making PSA an integral part of the development of Gen IV systems, a thorough understanding of all aspects of design safety exists, and can be expressed in terms that will facilitate effective interaction with national regulators.

2.5.3.3 PSA in Plant Operation

In the day-to-day operation of existing nuclear power plants throughout the world, PSA is used in a great many ways to improve plant safety, manage plant operations, and facilitate interactions with regulators. Examples include the use of risk models in on-line risk monitors, using risk insights in equipment configuration management, managing on-line maintenance, in-service testing, defining appropriate compensatory measures, and many others.

Because the PSA has been used throughout the design and licensing phases of current reactors, the technique is fully mature and available to support decision making and management during the operation phase. However PSA application to operating Gen IV systems will need collection of data relevant to new features to be implement before it can be fully operational.

2.5.3.4 Appropriate Risk Metrics

Given the diversity of different Gen IV reactor concepts, the traditional risk metrics that have been used widely for light water reactors will no longer be applicable or meaningful. For example, the traditional measure of core damage frequency (CDF) that has been widely used for light water reactors has no meaning for the Gen IV Molten Salt Reactor. It should be noted that no single risk metric will be perfect for all decisions or applications. The selection of specific risk metrics must be tailored to the decision or application under consideration. Further, chosen risk metrics must be applicable to the range of Gen IV concepts to permit comparisons. In the design phase, selected risk metrics may be used primarily to support down-selection decisions among competing alternative options, to make informed judgments about provision of safety margins, or to establish the overall level of safety relative to known benchmarks such as risk measures associated with the current generation of nuclear power plants. During the licensing phase, national regulators will likely evaluate whether or not a candidate design applying for licence or certification meets the overall risk and safety objective adopted by that particular regulator[25]. It is expected that individual national nuclear regulatory bodies will be specific in identifying and defining risk metrics that will be used in the licensing process for Gen IV systems. It is important to note here that the definition and utilization of risk metrics by regulators may differ somewhat from the needs of designers as they develop and evaluate the safety of Gen IV systems.

When applicable, the traditional measures of CDF and Large Early Release Frequency (LERF) remain extremely useful for many purposes but, for example, the first one could be generalized to be applicable to all the concepts (i.e., including the MSR) and to all the possible severe accident strategies including those that would exclude the explicit consideration of whole core melting. “Core

[25] For example, in its Advanced Reactor Policy Statement, the US Nuclear Regulatory Commission has stated that advanced reactors must be, at a minimum, as safe as those nuclear power plants that are currently licensed in the US. The NRC has also expressed its expectations in its 1986 Safety Goal Policy Statement.

damage" could be generalized with terms such as "undesirable event with significant source term mobilization". On the other hand the LERF has to be disconnected from the notion of tight containment.

However, the principal nominal risk metric that should be used for comparing Gen IV concepts and designs, identifying potential safety improvements, measuring compliance with established safety goals, and evaluating the appropriate amount of safety margin provided by a given design is the **frequency-consequence curve** (so called Farmer's curve)[26].

The x-axis of the F-C curve represents, for example, dose (Rem or Sievert) at the site boundary, and the y-axis represents frequency per reactor year. Both axes are plotted on a logarithmic scale.

As a technology-neutral risk metric, the F-C curve permits meaningful "bottom line" comparisons of risks associated with various Gen IV concepts and designs. It is also consistent with the overall Gen IV safety objective which looks for the elimination of the need for any offsite evacuation in the event of a reactor accident. Although every PSA develops intermediate-level results that are useful for many applications, the use of the F-C curve as described permits evaluation and comparison in a way that is independent of specific features of a Gen IV concept[27].

Although the F-C curve provides a technology-neutral basis for making comparisons and assessment of safety relative to an offsite risk metric, some of the intermediate results of the PSA will provide useful or essential information to developers and designers. The RSWG will investigate the applicability of potential technology-neutral intermediate risk metrics such as "frequency of fuel barrier breach," "frequency of environmental barrier breach," and others. These two prospective measures, respectively, are closely correlated with the notions of Level 1 and Level 2 PSA, but are potentially able to be applied in a more technology-neutral way.

At an even more detailed level, developers and designers will find that both the qualitative and the quantitative information represented by individual accident sequence characterizations and frequency estimates, as well as the minimal cut sets that comprise each accident sequence, provides essential information that is useful in understanding the level of risk associated with a particular design. The use of quantitative importance measures that are commonly used in PSA will allow the developer or designer to easily evaluate how the sensitivity of risk results to specific events. Two such commonly used quantitative importance measures include "Risk Reduction Worth" (RRW, cf. Glossary) and "Risk Achievement Worth." (RAW, cf. Glossary)

Finally, as indicated above, PSA will bring an essential contribution to check the meeting of safety objectives such as "progressive", "tolerant", "forgiving" and "well-balanced".

2.5.4. PSA Relationship to Other ISAM Elements

As the "centrepiece" of the ISAM, PSA shares interfaces with each of the other elements. Because the PSA provides a comprehensive framework that includes consideration of many diverse bits of knowledge and data about a system, PIRT and OPT serve primarily as early screening tools that increase knowledge of the system, drive the design evolution, and form inputs that are useful in performing the integrated PSA. Relationships and interfaces between the PSA and the other elements of the ISAM are described below.

2.5.4.1 Phenomena Identification and Ranking Table (PIRT)

In the earliest stages of concept development, PIRT serves as a screening tool to identify phenomena that may be important to system safety. In later stages of development, PIRT can be focused on a more detailed level. The relationships between PIRT and PSA include:

[26] See, for example, discussion on Sections 3 and 6 within the NUREG 1860.

[27] For example, comparing CDF for the MSR versus that of a reactor using a traditional metal-clad fuel form is meaningless. Similarly LERF for a design that does not employ a traditional containment has no meaning. However, for purposes of both establishing the safety basis of the reactor and licensing it, offsite consequences, measured in a consistent way, seems like a reasonable measure.

- Identification of initiating events
- Identification of accident sequence classes and specific sequence types
- Identification of specific phenomena and safety issues that will be more deeply analyzed in the PSA
- Phenomena that have the potential to cut across system boundaries, or to affect multiple systems/provisions
- Vulnerabilities to, and potential effects of, certain external events and other "macro events" affecting multiple systems/provisions

2.5.4.2 Objective Provision Tree (OPT)

The Objective Provision Tree is developed early in the design evolution as a means of analyzing and documenting the implementation of design provisions that perform essential safety functions. It is an important tool for understanding the ways in which the developing design provides Defence in Depth, as well as the ways in which the Lines of Protection that prevent, control or mitigate certain types of challenges to the integrity of the plant, are constructed and their performances, both from physical point of view, as well as from reliability point of view, are guaranteed.

The OPT will help the PSA stage :

- Defining the system success criteria for the mitigation of selected initiating events and accident classes
- Identifying the safety provisions to be modelled in the PSA
- Identifying the potential common cause failure events
- Identifying the phenomena that have the potential to cut across system boundaries, or to affect multiple systems/provisions
- Identifying for a given provision possible conflicting implementation for different level of defence (lack of independency between the levels) or, under a given level of defence, for different mechanisms[28].

2.5.4.3 Deterministic Analyses

Deterministic methods have long been used in nuclear safety, licensing, and regulation. Common applications include modelling thermal-hydraulic behaviour, neutronics, reactor physics, structural mechanics, fate and transport of materials, dose-consequence phenomena. The contribution of the deterministic studies remains essential to correctly quantify the different steps of the safety assessment. (Section 2.4).

2.5.5. Scope and Quality (Details on this subject are provided in Appendix 6)

Nuclear power plant PSAs are often defined in terms of three different "levels" depending on the scope of the analysis and the nature of results that are developed. The distinction is a useful one, and can likely be largely preserved, perhaps with slight adaptation, for Gen IV systems.

Following the international practice, three levels of PSA are considered [2.5.6]:

Level 1: the assessment of plant failure leading to the determination of "core damage frequency" (Section 2.5.3.4 concerning the possible evolution of the terminology)

Level 2: The assessment of containment response leading, together with level 1 results, to the determination of containment release frequency.

Level 3: The assessment of off-site consequences leading, together with the results of Level 2 analysis, to estimate the public risk.

[28] "Conflicting implementation" means that the achievement of a given mission will affect the capability of the provision to correctly achieve other missions that could be requested simultaneously.

Based, in part on the discussion of appropriate risk metrics and other considerations, it is anticipated that a PSA that will yield all of the benefits, and fulfil all the roles that are desirable for Gen IV systems will have to include the following scope and attributes (see Appendix 6 for details):

- The accident sequence modelling must be performed for the entire range of initiating event types that are credible for a given reactor concept, and that could potentially result in an unwanted radiological exposure at the site boundary. The diversity of Gen IV design concepts necessitates broadening the scope of the analysis to encompass a potentially much wider spectrum of events and sequences in particular organizing the systematic search and the exploitation of the "*intermediate results of the PSA"*.
- Include consideration of both internal and external events as both contribute to the risk.
- A rigorous analytical treatment of uncertainties is essential. A conservative bias is called for so as to avoid underestimating the magnitude of uncertainties in PSA input parameters.
- State of the art methods for the analysis of human behaviour that can initiate or otherwise influence (negatively and positively) how the course of postulated accident sequences should be applied.
- Be performed to what has customarily been defined to be Level 3.

Because the PSA will play a much larger role in the design and licensing of Gen IV systems than ever before the need for transparency, quality, and completeness cannot be overstated (see Appendix 6 for details):

- A rigorous quality assurance program should be established prior to initiating the PSA, and the analysis must be conducted in accordance with its provisions.
- From the outset, the PSA must analyze a broad spectrum of potential challenges to the plant.
- The PSA must be led and performed by acknowledged experts in the field of PSA.
- There are a number of international consensus standards that have been established, or are under development to ensure the quality of PSA. PSAs for Gen IV systems should be performed in accordance with these standards.
- Modelling methods and codes used in the PSA must be "state of the art" and generally accepted by major international regulatory bodies, professional societies, or other recognized arbiters of technical validity.
- The PSA should be reviewed by a team of independent experts

2.5.6 Treatment of Uncertainties (Details on this subject are provided within the Appendix 6)

The topic of uncertainties in PSA is one that has attracted a lot of attention, and has even created controversy about how "dependable" PSA results are, and thus, how useful those results are in making decisions regarding design, licensing, regulation, and operation of nuclear power plants. It is important to recognize from the outset, however, that while the topic is an important one, for the most part *PSA does not create new sources of uncertainty. It merely displays and characterizes uncertainties that are inherent in the inputs and thus the output, of the models that comprise the PSA.* In other words, the PSA is displaying uncertainties that exist in any case, but which might otherwise not be specifically identified, propagated, or reflected in the results of analyses.

Uncertainties in PSA arise from many sources. These include:

- Inability to precisely specify initial or boundary conditions
- Incomplete or sparse data on failure rates, initiating event frequencies, human error rates, etc.
- An incomplete understanding of some phenomena expected during both normal operations and off-normal conditions
- The use of assumptions in developing PSA models
- Limitations in the modelling methods that are used in PSA.

Details about the treatment of uncertainties through the PSA are provided within the Appendix 6.

Reference to Section 2.5

[2.5.1] *US NRC "Feasibility Study for a Risk-informed and Performance-Based Regulatory Structure for Future Plant Licensing (NUREG 1860)." December 2007.*

[2.5.2] *IAEA "Proposal for a Technology-Neutral Safety Approach for New Reactor Designs (TECDOC-1570)." September 2007.*

[2.5.3] *US NRC "Commission Policy Statement on the Regulation of Advanced Nuclear Power Plants (59 FR 35461). 1994. UPDATED NOVEMBER 2008*

[2.5.4] *IAEA "Determining the Quality of Probabilistic Safety Assessment (PSA) for Applications in Nuclear Power Plants ((TECDOC-1511)." July 2006.*

[2.5.5] *Nuclear Energy Institute "A Risk-Informed, Performance-Based Regulatory Framework for Power Reactors (NEI-02-02)." May 2002.*

[2.5.6] *Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants – IAEA Safety Standards – Specific Safety Guide SSG-3, 2010*

3. Example of application of ISAM methodology to JSFR

3.1 – Introduction

In order to obtain better understanding of the methods described in Chapter 2 of this report, this chapter describes an example of preliminary application of PIRT, OPT, DPA and PSA to the Japanese Sodium-cooled Fast Reactor (JSFR) system, which is being developed as one of the Gen IV reactor systems [3.1],[3.2]. In the JSFR system as shown in Appendix 7, there are major innovative safety features to be evaluated as follows:

- Passive reactor shutdown system (i.e., Self-Actuated Shutdown System (SASS) shown in Appendix 7),
- Passive decay heat removal system (i.e., natural circulation of sodium coolant and natural air flow at the air cooler),
- Leak tight backup structures in the sodium cooling systems (i.e., guard vessels and guard pipes in the primary cooling system, enclosures in the secondary cooling systems which include both the decay heat removal system (DHRS) and the main heat transport system),
- Double wall heat transfer tubes in the steam generators and the air coolers of the DHRS, and
- In-vessel retention against typical core disruptive accidents (i.e., ULOF, UTOP) by pursuing the re-criticality free for eliminating severe re-criticality and in-vessel core debris cooling.

3.2 – Applicability of PIRT to JSFR safety design work

It is recognized that PIRT could be helpful in demonstrating adequacy of analysis models and parameters that are used in DPA, which is necessary for defining success criteria of level-1 PSA. In particular, PIRT could be useful in identifying and considering important factors or phenomena affecting the safe shutdown that is led by innovative passive safety features (e.g., reactor shutdown by SASS, decay heat removal by natural circulation) upon accidents. JAEA performed preliminary application of PIRT to examine the reactor safe shutdown by means of SASS, during an unprotected loss of flow (ULOF) accident, where the term of “unprotected” means “with a failure of conventional reactor shutdown system”. SASS is installed above the core and it holds the control rods above the core in normal operation. Once the core outlet temperature rises abnormally, SASS loses the holding force due to its inherent characteristics without actuation of any instrumentation and control devices and the control rods are inserted into the reactor core.

Following the individual step described in Chapter 2, PIRT of reactor shutdown by SASS upon the ULOF accident was conducted as shown below.

1) The issue was defined as identifying the priority R&D issues related to innovative safety features specific to JSFR.
2) The specific objectives were defined as identifying phenomena and factors having a significant impact on reactor safe shutdown by means of SASS, in order to confirm effectiveness of SASS, that is expected to be actuated under beyond DBA conditions.
3) Database information was obtained e.g., R&D results concerning the holding force that is dependent upon the temperature of the main device constituting SASS, design specifications of SASS, design information about neutronics and thermal/hydraulics characteristics of reactor and primary heat transport systems (PHTS).
4) Hardware and scenario were defined as follows:
   i. Hardware: SASS in the backup reactor shutdown system (BRSS), reactor, reactor power control system (RPCS) and PHTS.
   ii. Postulated scenario: a ULOF (unprotected loss of flow) accident.
5) The figure of merit was defined as the maximum temperature of core coolant, which represents the safety criterion of preventing severe core damage under the ULOF accident condition.

6) Phenomena to be considered were identified i.e., phenomena, characteristics and state variables that affect maximum temperature of core coolant upon ULOF accident, by experts who are familiar with accident and thermal/hydraulics analyses and SASS.
7) The importance ranking was rated by considering sensitivities of uncertainty included in each phenomenon in terms of the maximum core coolant temperature upon the ULOF accident. The ranking scales defined in Table 1 were applied.
8) The knowledge level was assessed at the two different time points (i.e., before starting SASS R&D and at present) by considering whether we have sufficient knowledge to simulate precisely the identified individual phenomena and state variables. The knowledge level ranking scales defined in Table 2 were applied.

The PIRT preliminary application result is provided in Appendix 7.

3.3 – Applicability of OPT to JSFR (see Appendix 7)

Following the individual step described in Chapter 2, the OPT of JSFR safety features were developed as shown below.

1) The objectives were defined as assessing the structure of safety architecture of the JSFR in a systematic, comprehensive and adequate manner based on the defence-in-depth philosophy.
2) The design, research and safety assessment documentation were collected.
3) OPTs were developed by considering the three fundamental safety functions and the levels 1 to 4 of the defence-in-depth.
4) The developed OPT was illustrated in a tree structure and also expressed in a different representation with unique numbering as shown in Appendix 7.

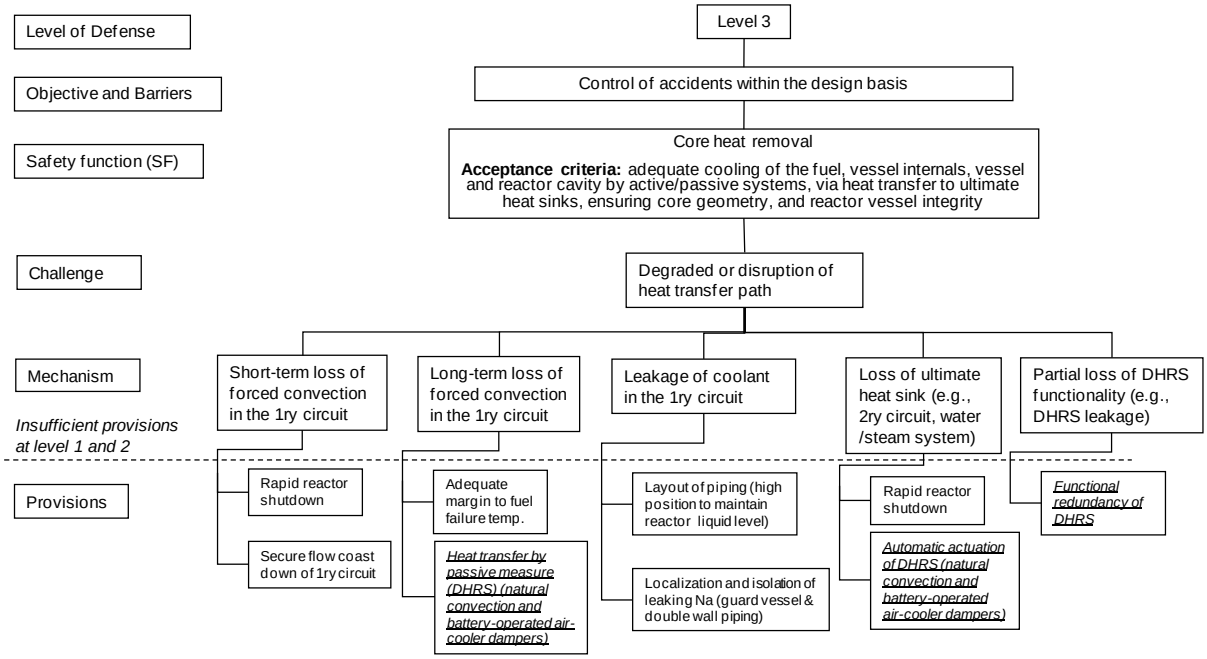


Figure 9: Example of OPT developed for JSFR safety function 2 (core heat removal) at level 3 of defence in depth

As shown in Figure 9, OPT is the organized structure of safety-related provisions based on the defence-in-depth philosophy. In particular, the provisions that are expressed with italic letters and underlined in Figure 9 are characterized with the safety design features and recommendations of decay heat removal function as shown below.

- DHRS should have capability of long-term decay heat removal without forced circulation of the primary heat transport system (PHTS) sodium coolant.
- When loss of ultimate heat sink such as SHTS, main feedwater system, main steam system, etc., occurs in normal reactor operation, the ultimate heat sink should be switched to DHRS (i.e., PRACS and DRACS) automatically following the reactor scram.
- Even assuming complete loss of function in a single train of DHRS, DHRS should have sufficient decay heat removal capability.

In the process of developing the PSA model, these features became key inputs to specify plant responses upon the initiating event and success criteria of DHRS during the decay heat removal operation. In addition, adequacy in meeting the requirements was confirmed by conducting DPA associated with the decay heat removal function.

The outline of DHRS in JSFR is briefly described. The JSFR is equipped with three trains of reactor auxiliary cooling systems for decay heat removal so that the decay heat can be removed only by way of the decay heat removal system. One of them is the DRACS that is directly connected to the reactor vessel, and the others are the PRACS that is connected to the primary cooling system. These trains are operated in a fully passive condition (i.e., natural circulation of sodium coolant and natural air flow at the heat sink).

The success criterion depends on the cooling time period after reactor shutdown as the decay heat decreases with time. Within the 24h period, two out of three trains are required, and after the 24h period the success criterion is relaxed to the level that at least one out of three trains of DHRS provide sufficient cooling capacity. The design improvement will be discussed in Section 3.5.

3.4 – Applicability of DPA to JSFR DHRS (see Appendix 7)

Following the individual step described in Section 3.2, DPA of DHRS was conducted as shown below.

1) Facility, objectives and scope of the analysis were specified:
   i. Target system is the DHRS in JSFR.
   ii. Objective is to determine the consequences in terms of "success or failure" of different event sequences modelled in the PSA.
   iii. Scope was specified to the analysis of decay heat removal characteristics upon the typical accident with reactor scram.
2) Approach was selected: i.e., best estimate analyses using best estimate code to cope with innovative safety features (i.e., natural circulation).
3) A computer code in the category "(c) thermo-hydraulic codes" was selected: i.e., one-dimensional flow network code that has been developed and used for sodium-cooled fast reactors.
4) Methodology of the accident analysis is as follows:
   i. Physical model to be applied is a one-dimensional flow network model.
   ii. Examples of initial and boundary conditions are initial transient power history in a short time, no heat loss from the system, conservative inlet air temperature at the air cooler, no heat exchange at the SG tubes.
   iii. Acceptance criteria (specific to PSA) are defined as maintaining core coolable geometry: i.e.,
      - Coolant boundary temperature: ≤ 650 ºC (tentatively)
      - Core coolant temperature: ≤ 900 ºC (tentatively)
5) Data for analysis were collected, which is associated with the plant systems operating characteristics (e.g., heat balance), neutronics, thermal and hydraulics characteristics (e.g., reactivity coefficients, material properties), design specifications of systems and components (e.g., geometry).
6) A database containing the above data was developed and has been updated corresponding to progress of the design work.

7) The engineering handbook was developed, which describes how to convert the data included in the above database into input of the analysis code.
8) The plant model was developed.
9) The models and methods in the analysis code were applied, which are equivalent to those of the code already verified and validated that was used in the safety evaluation of the prototype sodium-cooled fast reactor "Monju".
10) As a basic scenario the reactor scram followed by the DHRS operation was supposed. Systems and components available were determined, corresponding to the accident sequence that was developed in the event trees of the level-1 PSA of JSFR by considering the key information obtained from the OPT. No modification of the plant model was needed as the check of the result in step 12.
11) The calculation was executed by following the code manual.
12) The analysis results were checked using the supervisory review by performing some sensitivity analyses.
13) The analysis results were presented as shown in Figure 10.

Figure 10 indicates that a successful accident sequence developed in the event trees results in the reactor coolant boundary integrity representing core integrity being maintained. In addition, the accident consequence of the other sequences was regarded conservatively as core damage by considering uncertainty. Thus, DPA serves as a determination of success criteria in the level-1 PSA model. It is for future work to implement sensitivity analyses to establish margins to the limits and to cover imprecision in actual parameters at the design stage.

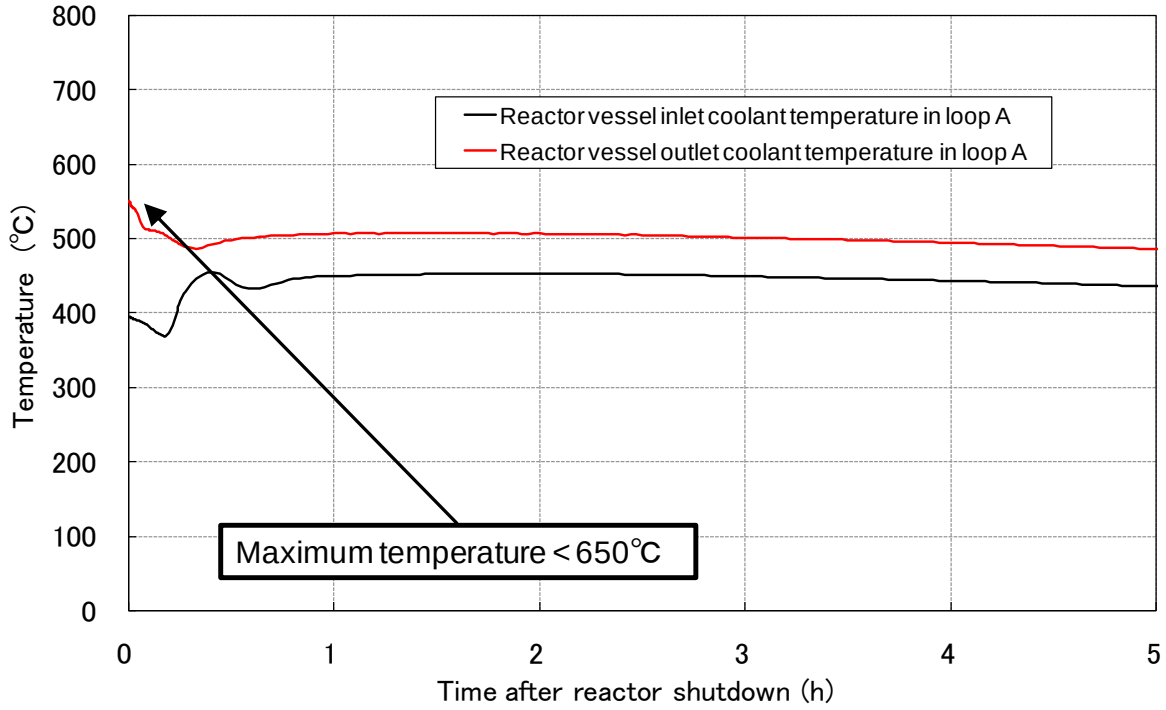


Figure 10: Example of DPA results:
Passive cooling scenario by using DRACS & PRACS-A with a single air cooler damper failure

3.5 – Applicability of PSA to JSFR DHRS (see Appendix 7)

The scope of PSA was focussed on the level-1 PSA related to internal initiators and specific to decay heat removal after successful reactor shutdown. PSA was conducted following the steps below.

1) Initiating events were identified and categorized, based on the plant design information and using master logic diagram method.
2) The mitigation systems were defined and the event trees (ET) were developed, based on the plant design specifications linked with the key information that was obtained from the OPTs and on the DPA results.
3) The fault trees (FT) were developed, based on the system design information with some assumptions related to support systems.
4) Common cause failures (CCF) of major active failure modes of redundant components were considered e.g., damper failure to open, battery failure to supply electricity to damper drivers.
5) Human error in operator's recovery action was considered.
6) The component failure rate was estimated, based on the CORDS for sodium-fluid components and on the domestic LWR reliability data.
7) The occurrence frequency of the initiating events was quantified, based on the failure rate and the operating experiences of nuclear reactor systems (i.e., sodium-cooled fast reactors, LWRs).
8) CCF parameters and human error probability were determined, based on the methodology used in LWR PSA.
9) Quantification of the accident sequences with combining ET and FT was executed.

Contributors to the protected loss of heat sink (PLOHS) frequency were broken down by time phases with different success criteria. The dominant contributor is loss of two out of three trains of DHRS within 24h after reactor shutdown. Obviously this is because the success criterion is different after the 24h period. If the designer enhances the heat removal capacity of a single train of DHRS in this time period so as to become less-demanding success criteria, there is potential to reduce at most 99% of the total PLOHS frequency. Based on this information, the designer and analyst examined the possibility of introducing non-safety-related blowers at the air cooler inlet to enhance PRACS and DRACS capability with consideration of both lower cost increase and significant safety improvement. By conducting additional DPA, it was confirmed that the consequence of the decay heat removal scenario with sodium natural circulation and forced-air flow by using DRACS alone would be adequate for maintaining the reactor coolant boundary integrity. In addition, the PSA with design improvement showed quantitatively that introduction of the air cooler blowers in both PRACS and DRACS can reduce significantly the PLOHS frequency; i.e., improve the reliability of decay heat removal.

There are some uncertainty issues in the PSA. In order to address the issue that cumulative component operating time is still short, compared with the target reliability level, and further effort will be made to collect the empirical reliability data for sodium-cooled fast reactors. In order to minimize the uncertainty due to shortage of such empirical reliability data, the margin to the safety target is ensured by introducing redundancy and diversity in the core cooling measures.

The second issue is related to epistemic uncertainty due to the fact that the component to be considered is a new type even if empirical reliability data of a similar type are available. Reliability and safety performance of new type of components would be tested and demonstrated to some extent in the research and development process of those components, although the operating time would be limited. Sensitivity of the uncertainty in the reliability of new components needs to be examined.

Phenomenological uncertainty associated with the passive cooling is not assessed explicitly yet. Sensitivity of the uncertainty in DPA will be analyzed and if the sensitivity is significant, the uncertainty will be quantified (e.g., with the Monte Carlo calculation based on the evaluation of the response surface and uncertainty in individual analysis parameters).

3.6 – Summary

Following the method described in Chapter 2, preliminary application of PIRT, OPT, DPA and PSA to the JSFR system was examined. It can be noted that those four tools are useful to show the adequacy of safety-related design and R&D activities of JSFR.

- PIRT provided a framework to confirm the appropriateness for key R&D studies.
- OPT organized a structure of safety-related provisions based on the defence-in-depth philosophy.
- DPA provided key information for the success criteria to be defined in the PSA model.
- PSA provided the quantitative assessment of the level of safety and provided useful information for the system design improvement.

References to Section 3

[3.1] *R. Nakai and K. Kurisaka, JAEA, "Applicability of PIRT, OPT, DPA and PSA to Japanese Sodium-cooled Fast Reactor (JSFR)", Presentation given at the 10th GIF RSWG Meeting, Brookhaven (4-5 May, 2009).*

[3.2] *K. Kurisaka and Y. Shimakawa, "Application of Integrated Safety Assessment Methodology (ISAM) to Japanese Sodium-cooled Fast Reactor (JSFR)", Proceedings of ICAPP'10, San Diego, CA, USA, June 13-17, 2010.*

Annex - Glossary of main terms used in the Report

Accident scenario	A postulated or assumed set of conditions and/or events. Most commonly used in analysis or assessment to represent possible future conditions and/or events to be modelled, such as possible accidents at a nuclear facility. A scenario may represent the conditions at a single point in time or a single event, or a time history of conditions and/or events (including processes).
Accident	Any unintended event, including operating errors, equipment failures and other mishaps, the consequences or potential consequences of which are not negligible from the point of view of protection or safety.
Analysis	Often used interchangeably with assessment, especially in more specific terms such as 'safety analysis'. In general, however, analysis suggests the process and result of a study aimed at understanding the subject of the analysis, while assessment may also include determinations or judgements of acceptability. Analysis is also often associated with the use of a specific technique. Hence, one or more forms of analysis may be used in assessment.
Best estimate	The point estimate of a parameter utilized in a computation which is not biased by conservatism or optimism. Generally, the mean value of a parameter is considered to be the best estimate.
Beyond design basis accident	Accident conditions more severe than a design basis accident.
Challenges	Generalized mechanisms, processes or circumstances (conditions) that may impact the intended performance of safety functions; a set of mechanisms have consequences which are similar in nature.
Core damage frequency	Term used in probabilistic risk assessment (PRA) that indicates the likelihood of an accident that would cause damage to a nuclear reactor core.
Defence in depth	A hierarchical deployment of different levels of diverse 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 material and workers, members of the public or the environment, in operational states and, for some barriers, in accident conditions. The objectives of defence in depth are: (a) To compensate for potential human and component failures; (b) To maintain the effectiveness of the barriers by averting damage to the facility and to the barriers themselves; (c) To protect workers, members of the public and the environment from harm in accident conditions in the event that these barriers are not fully effective.
Design basis accident	Accident conditions against which a facility is designed according to established design criteria, and for which the damage to the fuel and the release of radioactive material are kept within authorized limits.
Design basis	The range of conditions and events taken explicitly into account in the design of a facility, according to established criteria, such that the facility can withstand them without exceeding authorized limits by the planned operation of safety systems.

Design	The process and the result of developing a concept, detailed plans, supporting calculations and specifications for a facility and its parts.
Deterministic analysis	Analysis that uses single numerical values (taken to have a probability of 1) for key parameters, leading to a single value for the result. In nuclear safety, for example, this implies focusing on accident types, releases and consequences, without considering the probabilities of different event sequences. Typically used with either 'best estimate' or 'conservative' values, based on expert judgement and knowledge of the phenomena being modelled.
Engineered safety	Engineered systems, structures or components that make their use acceptable without undue risk with provisions to prevent, mitigate, or contain potential accidents. Although an objective in their design is to make them highly reliable, they remain in principle subject to failure (however low the probability of such failure), unlike inherent safety characteristics[29].
Figure of merit	A quantity used to characterize the performance of a component, system or method, relative to its alternatives.
Grace period	The period of time during which a safety function is ensured in an event with no necessity for action by personnel. The grace period might be achieved by means of the automation of actuations, the adoption of passive systems or the inherent characteristics of a material, or by any combination of these.
Graded approach	For a system of control, such as a regulatory system or a safety system, a process or method in which the stringency of the control measures and conditions to be applied is commensurate, to the extent practicable, with the likelihood and possible consequences of, and the level of risk associated with, a loss of control. A method in which: (1) The significance and complexity of a product or service are determined; (2) The potential impacts of the product or service on health, safety, security, the environment, and the achieving of quality and the organization's objectives are determined; (3) The consequences if a product fails or if a service is carried out incorrectly are taken into account.
Human error	Human error is an imbalance between what the situation requires, what the person intends, and what the person does.
Inherent safety feature	Fundamental property of a design concept that results from the basic choices in the materials used or in other aspects of the design which assures that a particular potential hazard can not become a safety concern in any way. This feature represents conclusive, or deterministic safety, not probabilistic safety[30].
Inherent Safety	The achievement of safety through the elimination or exclusion of inherent hazards through the fundamental conceptual design choices made for the nuclear plant.
Large early release frequency	The likelihood of a radioactivity release from the containment which is both large and early. Large is defined as involving the rapid, unscrubbed release of airborne fission products to the

[29] This statement from the IAEA glossary is debatable for the effective "reliability" of inherent features can be affected by environmental conditions. This concern is addressed by the discussions which are underway on the reliability of "passive systems" and "inherent features".
[30] Same comment as above (foot note N° 29)

	environment. Early is defined as occurring before the effective implementation of the off-site emergency response and protective actions.
Licensing basis/criteria	A set of regulatory requirements applicable to a nuclear installation.
Limit	The value of a quantity used in certain specified activities or circumstances that must not be exceeded. The term limit should only be used for a criterion that must not be exceeded, e.g., where exceeding the limit would cause some form of legal sanction to be invoked. Criteria used for other purposes — e.g., to indicate a need for closer investigation or a review of procedures, or as a threshold for reporting to a regulatory body — should be described using other terms, such as reference level.
Line of Protection	Set of related and consistent provisions that collectively perform or achieve a desired safety-related function, role, or outcome.
Mechanism	Specific reasons, processes or situations whose consequences might create challenges to the performance of safety functions.
Minimal cut set	A cut set is said to be a minimal cut set if, when any basic event is removed from the set, the remaining events collectively are no longer a cut set.
Mitigation	An immediate action taken by the operator or other party to reduce the potential for conditions to develop that would result in exposure or a release of radioactive material requiring emergency actions on or off the site; or to mitigate source conditions that may result in exposure or a release of radioactive material requiring emergency actions on or off the site.
Objective Provision Tree	Graphical presentation, for each of the specific safety principles belonging to the five levels of in depth, of the following elements from top to bottom: (1) objective of the level; (2) relevant safety functions; (3) identified challenges; (4) constitutive mechanisms for each of the challenges; (5) list of provisions in design and operation preventing the mechanism to occur.
Passive feature	A feature that does not depend on an external input such as actuation, mechanical movement or supply of power.
Phenomenon	A phenomenon is any event that is observable, however commonplace it might be, even if it requires the use of instrumentation to observe it.
Probabilistic analysis	Often taken to be synonymous with stochastic analysis. Stochastic conveys directly the idea of randomness (or at least apparent randomness), whereas probabilistic is directly related to probabilities, and hence only indirectly concerned with randomness. Therefore, a natural event or process might more correctly be described as stochastic (as in stochastic effect), whereas probabilistic would be more appropriate for describing a mathematical analysis of stochastic events or processes and their consequences (such an analysis would, strictly, only be stochastic if the analytical method itself included an element of randomness, e.g., Monte Carlo analysis).
Probabilistic safety assessment	PSA is a rigorous, systematic, and comprehensive tool for identifying and estimating the likelihoods of sequences of events

	that can result in the loss or damage related to the design and operation of complex engineered systems. Three levels of probabilistic safety assessment are generally recognized. Level 1 comprises the assessment of plant failures leading to determination of the frequency of core damage. Level 2 includes the assessment of containment response, leading, together with Level 1 results, to the determination of frequencies of failure of the containment and release to the environment of a given percentage of the reactor core's inventory of radionuclides. Level 3 includes the assessment of off-site consequences, leading, together with the results of Level 2 analysis, to estimates of public risks.
Provisions	Inherent characteristics, technical options and organisational measures – selected for the design, the construction, the operation including the shut down and the dismantling, which are taken to prevent the accidents or limit their effects.
Risk achievement worth	Risk Achievement Worth (RAW) of a modeled plant feature (usually a component, train, or system) is the increase in risk if the feature is assumed to be failed at all times. It is expressed in terms of the ratio of the risk with the feature failed to the baseline risk level.
Risk informed	A "risk-informed" decision-making is a philosophy whereby risk insights are considered together with other factors to establish requirements that better focus the attention on design and operational issues commensurate with their importance to health and safety. It enhances the traditional approach by: (a) allowing explicit consideration of a broader set of potential challenges to safety, (b) providing a logical means for prioritizing these challenges based on risk significance, operating experience, and/or engineering judgment, (c) facilitating consideration of a broader set of resources to defend against these challenges, (d) explicitly identifying and quantifying sources of uncertainty in the analysis, and (e) leading to better decision-making by providing a means to test the sensitivity of the results to key assumptions.
Risk matrix	A table used in risk analysis in which rows show the risks and columns show their likelihood (probability) of occurrence and their impact.
Risk reduction worth	Risk Reduction Worth (RRW) of a modeled plant feature is the decrease in risk if the feature is assumed to be perfectly reliable. It is expressed in terms of the ratio of the baseline risk level to the risk with the feature guaranteed to succeed.
Risk triplet	The three questions, "What can go wrong?", "How likely is it?" and "What are the consequences?" are referred to as the risk triplet.
Risk	A multiattribute quantity expressing hazard, danger or chance of harmful or injurious consequences associated with actual or potential exposures. It relates to quantities such as the probability that specific deleterious consequences may arise and the magnitude and character of such consequences.
Safety function	A specific purpose that must be accomplished for safety.

Safety margin	The margin required to ensure safety of an engineered system and typically the margin of safety is the strength of the material minus the anticipated stress.
Safety requirements	The design of a nuclear power plant is expected to meet three general safety requirements: (a) The capability to safely shut down the reactor and maintain it in a safe shutdown condition during and after appropriate operational states and accident conditions; (b) The capability to remove residual heat from the reactor core after shutdown, and during and after appropriate operational states and accident conditions; (c) The capability to reduce the potential for the release of radioactive material and to ensure that any releases are within prescribed limits during and after operational states and within acceptable limits during and after design basis accidents.
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.
Source term	The radiological source term for a given accident sequence or release category consists of the release fractions for various radionuclide groups (expressed as fractions of initial core inventory), and the timing, elevation, and energy of the release.
Synergistic assessment	The assessment of a combined, correlated or synergistic action of a group of units or faculties that exceeds the sum of the individual effects; increased effectiveness, achievement, etc., produced as a result of combined action or cooperation.
Uncertainty	An estimate of the uncertainties and error bounds of the quantities involved in, and the results from, the solution of a problem.

References for the Glossary:

1. *Safety Related Terms for Advanced Nuclear Plants*, IAEA-TECDOC 626, International Atomic Energy Agency, September 1991
2. IAEA Safety Glossary Terminology Used in Nuclear Safety and Radiation Protection, 2007 Edition, International Atomic Energy Agency, Vienna, 2007.

Appendix 1 – Reminder of the safety objectives and approach

A high safety level, at least as safe as gen III plants, is advocated for future power plants.

The approach promoted by the RSWG can be summarized as follows:

1) *High priority shall be given to the effort to identify, as comprehensively as feasible, plausible abnormal situations (incident and accident),*
2) *High priority shall also be given to the prevention efforts to avoid these abnormal situations and showing how they are dealt with at as high a level as possible in the defence in depth.*
3) *Design effort for an easier management of abnormal situations (protection).*
4) *Design effort to take into account and to mitigate the consequences of severe accidents (mitigation).*
5) *In relation with the effort for the identification and the prevention (cf. items 1 & 2 above) specific efforts should be made for demonstrating the "practical elimination" of initiators, sequences or phenomena associated with residual risk.*[31]

To achieve the requested level of safety the RSWG recommend the implementation of a safety that will be "*built-in*" within the design rather than "*added on*" to the system architecture. This logic motivates the early integration of safety concerns within the design stages; an ad-hoc "on line" assessment methodology is a key contributor to meet this objective. The above recommendation is complemented by the RSWG's recommendation for the achievement of a robust safety demonstration.

The primary means of preventing the abnormal conditions and/or, controlling and mitigating the consequences of accidents is the implementation of "defence in depth" (DiD). This concept is applied to all safety activities, whether organizational, behavioural or design related, to ensure that they are subject to layers of overlapping provisions, so that if a failure were to occur, it would be detected and compensated for or corrected by appropriate measures. Application of the concept of defence in depth throughout design and operation is essential to provide a graded protection against a wide variety of transients, anticipated operational occurrences and accidents, including those resulting from equipment failure or human action within the plant, and events that originate outside the plant.

To meet the above objectives and still within the frame of a correct DiD implementation, it is essential to design the safety provisions and their architecture in order to achieve [A1.1]:

- *An exhaustive defence, i.e., the identification of the risks, which leans on the fundamental safety functions, should look for exhaustiveness; the identification of the corresponding scenarios to be retained to design and size the safety architecture provisions must be as exhaustive as possible.*
- *A graduated, progressive defence; without that, "short" sequences can happen for which, downstream from the initiator, the failure of a particular provision entails a major increase, in terms of consequences, without any possibility of restoring safe conditions at an intermediate stage*[32].
- *A tolerant defence: no small deviation of the physical parameters outside, the expected ranges, can lead to sharp increase of consequences. Minimization of the use of safety provision which belong to the protection level of the defence in depth.*
- *A forgiving defence, which guarantee the availability of a sufficient grace period and the possibility of repair and restoring during abnormal conditions.*
- *A balanced or homogeneous defence, i.e., no initiator or sequence participates in an excessive*

[31] These are initiators, sequences or situations which consequences should not be reasonably manageable and the design will not address their management. They have to be identified as such and specific effort has to be set up to prove their practical elimination.

[32] It is worth noting that graduate and progressive defence is an efficient means for investment protection.

and unbalanced manner to the global frequency of the damaged plant states.

The interest of the proposed design options (and so their evaluation) must be judged based on their coherence when compared to all of the above objectives.

Finally, it is worth noting that the correct implementation of the defence in depth is also the key to achieve safety robustness for, with several independent and efficient layers of protection, it will be easy to keep under control the uncertainties and their propagation.

Reference for Appendix 1

[A1.1] *Basis for the Safety Approach for Design & Assessment of Generation IV Nuclear Systems – RSWG Report, January 2009*

Appendix 2 – QSR Tables of Technical recommendations

TABLE A2.1a
CLASS 1 Technical Recommendations and Foreseen Characteristics and Features as function of the levels of the defence in depth
Applicable to all the future reactors

1. 1st level : PREVENTION : Prevention of abnormal operation and failures
1.1. ⇨Work out and set up a **design for the plant** (i.e., the reactor core, primary & secondary circuit and BOP), that will allow **simple procedures for the reactor operations and maintenance during normal conditions** (i.e., minimize process' complexity and avoid inherent instability; systematic consideration of human factors and the human–machine interface for operation and shut down[33])
1.2. ⇨Identify the **Postulated Initiating Events**, looking for exhaustiveness, including internal and external hazards considering all plausible plant conditions (operation and shut down); **minimize their frequency of occurrence**. *N.B. The analysis is organized first, listing the conventional PIE and, in a second step, reasoning through the safety functions. This allows a crossed vision of the assets and the drawbacks of the concept*
1.3. ⇨ In building the **safety architecture avoid by design** (prevent & practically eliminate) **the initiators, sequences or situations that can lead to unacceptable consequences and early chemical, toxic or radioactive releases (***including cliff edge effect).* *N.B.: Practical elimination shall be supported by specific demonstration.*
1.4. ⇨Work out and set up a **design for the process** (inherent plant's response) which allow for simple reactor management under abnormal, accidental and severe accident conditions and that that will **inherently minimise the PIE consequences** (tolerant and forgiving design for the process and the safety architecture). *N.B. As for the previous set of recommendations, the analysis is organized first, listing the conventional PIE and, in a second step, reasoning through the safety functions. This allows a crossed vision of the assets and the drawbacks of the concept*
1.5. ⇨Work out and set up a **design for the safety architecture** (OPT / LOP / provisions) that will allow **simple procedures for the reactor operations inspection**[34] **and maintenance under abnormal conditions** (i.e., minimize process' complexity[35] and avoid inherent instability; systematic consideration of human factors and the human–machine interface for operation and shut down) *N.B. The recommendation is considered here within the 1st level of the DiD but it is detailed within the section 2.4 (2nd level of the DiD)*
1.6. ⇨Work out and set up a **design for the safety architecture** (LOP / provisions) which allow for **simple accidental intervention procedures and repair under accidental conditions** (consideration of human factor) *N.B. The recommendation is considered here within the 1st level of the DiD but it is detailed within the section 3.5 (3rd level of the DiD)*
1.7. ⇨Work out and set up a **design for the safety architecture** (OPT / LOP / provisions) which allow for **simple, progressive, tolerant, forgiving and balanced reactor's behaviour/management under accidental conditions** *N.B. The recommendation is considered here within the 1st level of the DiD but it is detailed within the sections 1.10 and 3.4 (3rd level of the DiD)*
1.8. ⇨Work out and set up a **design for the safety architecture** (LOP / provisions) which allow **for**

[33] *Insights from INPRO criterion CR 1.7.2 can be useful to address this concern*
[34] *from INPRO methodology BP1 – CR 1.1.3*
[35] The notion of simplification relates to the safety architecture; it answers the specific INSAG requirement for reducing or avoiding complexity in comparison with current technologies; practically speaking this can justify looking for 'operator friendly' concept aimed at limiting the effects of human errors for example by limiting the operating constraints bearing on the operators. If needed specific indicators for complexity could be developed. This notion is also essential to reduce uncertainties. It is worth noting that looking for the simplification of the safety architecture remains compatible with the implementation of sophisticated single provisions.

simple, management of the severe plant conditions progress and the mitigation of their consequences *N.B. The recommendation is considered here within the 1st level of the DiD but it is detailed within the section 4.1 (4th level of the DiD)*
1.9. ⇨Select options which provide **confidence in innovation**[36]
1.10. ⇨Integrate the **principles of the defence in depth** within the whole safety architecture for an **exhaustive, progressive, tolerant, forgiving and well-balanced defence** *N.B. The item addresses generic recommendations for the architecture. It is complemented by recommendations addressing the design of the provisions within the 3.4 (3rd level of the DiD)*
1.11. ⇨Work out and set up a safety architecture which **minimise the potential for Common Modes**
1.12. ⇨Work out and set up a design that integrate **inherent security and proliferation resistance**[37] *To be defined coherently with the recommendation of the PR&PP*
1.13. ⇨Once the safety architecture available, qualify as needed the LOP provisions, both from physical performances point of view (i.e., the capability to achieve the mission) and from reliability point of view (i.e., the capability to achieve the mission with the requested reliability)
1.14. ⇨**Minimize the personnel exposure** (on site releases) during normal operation, decommissioning and dismantling – ALARA
1.15. ⇨**Minimize the risk for environment contamination** (off site radioactive material release) during normal operation, decommissioning and dismantling - ALARA
1.16. ⇨**Minimize the personnel exposure under abnormal, accidental and severe accident conditions** - ALARA (operation and shut down)
1.17. ⇨A **reduced-scale pilot plant or large-scale demonstration facility** should be built for reactors and/or fuel cycle processes, which represent a major departure from existing operating experience[38]
1.18. ⇨**Uncertainties and sensitivities identified and appropriately dealt with?** [39]

[36] *from INPRO methodology BP2 – CR 2.1.4*
[37] *from INPRO methodology BP1 – CR 1.8*
[38] *from INPRO methodology BP4 – CR 4.3*
[39] *from INPRO methodology BP4 – CR 4.4.2*

TABLE A2.1a (Cont)
CLASS 1 Technical Recommendations and Foreseen Characteristics and Features
as function of the levels of the defence in depth
Applicable to all the future reactors

2. ★ 2nd level :CONTROL : control of abnormal operations and detection of failures-
2.1. ⇨Implement a **layer of inherent or extrinsic provisions**, so that if a failure of the previous layer occurs (PIE, 1st level of the DiD), it would be detected and, if possible, managed by appropriate measures to keep the plant in safe conditions without soliciting the safety provisions which belong to the follow levels of the DiD
2.2. ⇨**Minimise the uncertainties** about the plant conditions under abnormal conditions
2.3. ⇨Work out and set up a design with simple and efficient inherent behaviour[40] under abnormal conditions (tolerant and forgiving design for the process and the safety architecture; avoid inherent instabilities) *(For recall → must / can be realised at the prevention level; cf. 1.4)*
2.4. ⇨Work out and set up a design for the safety architecture (OPT / LOP / provisions) that will allow **simple procedures for the reactor operations inspection and maintenance under abnormal conditions** (i.e., minimize process' complexity and avoid inherent instability; systematic consideration of human factors and the human–machine interface for operation and shut down[41]) *N.B. The recommendation is first considered at the 1.5 (1st level of the DiD) but it is detailed in this section 2.4*
2.5. ⇨Defining the abnormal conditions to be assessed, **take into account possible aggravating situations** (coherently with the PIE category)
2.6. ⇨Minimize the **personnel exposure under abnormal conditions** - ALARA Minimise the radioactive potential for injuries under abnormal conditions (operation and shut down) *(For recall → must / can be realised at the prevention level; cf. 1.16)*

[40] "*Simple plant inherent behaviour*" means that the sequences can be described without large uncertainties.
[41] *Insights from INPRO criterion CR 1.7.2 can be useful to address this concern*

TABLE A2.1a (Cont)
CLASS 1 Technical Recommendations and Foreseen Characteristics and Features
as function of the levels of the defence in depth
Applicable to all the future reactors

3. ★3rd level : PROTECTION : Control of accident within the design basis and prevention of severe plant conditions
3.1. ⇨Implement a **layer of provisions, so that if a failure of the previous layer(s) occurs, it would be detected and managed by appropriate measures** to meet the objectives of the design basis accidents domain while preventing the severe plant conditions. Minimize the frequency of occurrence of severe plant conditions (core degradation)
3.2. ⇨**Minimise the uncertainties about the plant conditions under accidental conditions** (operation and shut down)
3.3. ⇨Work out and set up a **design for the process** (inherent response) **which allow for simple reactor management under abnormal, accidental and severe accident conditions and that that will inherently minimise the PIE consequences**. *N.B. The analysis concerning the inherent characteristics of the plant is addressed at the first level of the DiD (1.2 for the PIE frequency of occurrence & 1.4 for the inherent minimization of the PIE consequences). The objective and the scope of the recommendations at this third level of the DiD are to insure that the engineered provisions, and finally the LOPs, are correctly sized to answer the requested missions.* *Below the analysis is organized first, listing the conventional third category PIE and, in a second step, reasoning through the safety functions.* *N.B. Normally, the Cat 2 initiating faults do not challenge the third level of the DiD and are managed by the first and second level of the DiD. As well, the Design Extension Conditions belong to the 4th level of the DiD*
3.4. ⇨Work out and set up a design for the **safety architecture** (LOP / provisions) **which allow for simple, progressive, tolerant, forgiving and balanced reactor's behaviour/management under accidental conditions** *N.B. The analysis concerning the generic characteristics of the plant architecture is addressed at the first level of the DiD (cf. 1.101). The objective and the scope of the recommendations at this third level of the DiD are to insure that the engineered provisions, and finally the LOPs, are correctly sized to answer the requested missions.*
3.5. ⇨Work out and set up a design for the **safety architecture** (LOP / provisions) **which allow for simple accidental intervention procedures and repair under accidental conditions** (consideration of human factor[42]) *N.B. The recommendation is first considered at the 1.6 (1st level of the DiD) but it is detailed in this section 3.5*
3.6. ⇨Work out and set up a safety architecture which minimize the **potential for Common Modes** (mutual aggressions, internal or external hazards) *N.B. The recommendation is considered and detailed at the 1.11 (1st level of the DiD) for the whole safety architecture; it is detailed in this section 3.6 focusing on the recommendation for the LOP design, especially concerning the requested reliability*
3.7. ⇨In defining the accidental sequence to be assessed, take into account **possible aggravating situations** (coherently with the PIE category))
3.8. ⇨Number of **confinement barriers maintained**[43]
3.9. ⇨**Minimize the personnel exposure** (including on site release) under accidental conditions[44] – ALARA ***(For recall → must / can be realised at the prevention level; cf. 1.16)***
3.10. ⇨**Minimize the risk for the environment contamination** (off site release) under abnormal and accidental conditions (without core degradation) – ALARA

[42] *Insights from INPRO criterion CR 1.7.2 can be useful to address this concern*
[43] *from INPRO methodology BP1 – CR 1.3.4*
[44] *from INPRO methodology BP3 – CR 3.1.1*

TABLE A2.1a (Cont)
CLASS 1 Technical Recommendations and Foreseen Characteristics and Features
as function of the levels of the defence in depth
Applicable to all the future reactors

4. **★ 4th level : SEVERE ACCIDENT MANAGEMENT- accident management including the confinement protection** ***N.B*** *The safety approach, coherently with the fourth level of the defence in depth, is completed by the consideration of plant conditions with more or less important core degradation (if need be, until the whole core melting) and the implementation of provisions which aim at making the risk acceptable. This is why the designer has to select and take into account the severe plant conditions configurations to be considered within the basis for the design of the safety architecture (i.e., the set of conditions considered for the design of the single provisions/LOP). Analogously the designer should prevent & practically eliminate the initiators, sequences or situations that can lead to unacceptable consequences and early releases. Finally he should reject the risk for the cliff edge effect. In conclusion :*
• *according to the fourth level of the defence in depth, some representative severe plant conditions have to be considered, in particular to demonstrate the effectiveness of the safety architecture and to prove the robustness of the confinement*
• *a limited number of initiators, sequences or situations, for which it is not realistic to set up provisions for mitigation, or to assure, with a sufficient degree of confidence, that their consequences would be mastered, will be eliminated by design or "practically eliminated" implementing specific provisions which guarantee their rejection within the Residual Risk (RR)*
4.1. ⇨Implement a layer of provisions/LOP, so that if a failure of the previous layer(s) occurs, the severe plant condition will be detected, managed and mitigated by appropriate measures and its consequences duly mitigated
4.2. **Minimise the uncertainties about the plant conditions under accidental conditions** (operation and shut down)
4.3. ⇨Work out and set up a design for the safety architecture (LOP / provisions) which allow **for simple management of the severe plant conditions progress and the mitigation of their consequences** *N.B. The analysis concerning the inherent characteristics of the plant is addressed at the first level of the DiD (1.2 for the PIE frequency of occurrence & 1.4 for the inherent minimization of the PIE consequences). The objective and the scope of the recommendations at this fourth level of the DiD are to insure that the engineered provisions, and finally the LOPs, are correctly sized to answer the requested missions. Below the analysis is organized first, listing the conventional Design extension Conditions and, in a second step, reasoning through the safety functions*.
4.4. ⇨Avoid major release of radioactive materials into the environment[45] : A major release of radioactivity should be prevented for all practical purposes, so that innovative systems would not need relocation or evacuation measures outside the plant site, apart from those generic emergency measures developed for any industrial facility used for similar purpose
4.5. ⇨Minimize the personnel exposure (on site accidental release) under accidental conditions[46] - ALARA *(For recall → must / can be realised at the prevention level; cf. 1.16)*
4.6. ⇨Minimise the offsite accidental release during the severe plant conditions
4.6.1. Conceive the containment provisions in order to keep the containment capabilities compatible with the objective to guarantee that:
5. ★ 5th level : CONSEQUENCES MITIGATION - Mitigation of radiological consequences of significant releases of radioactive materials
5.1. ⇨Delay the offsite release
5.2. ⇨Minimise the offsite radioactive release
5.3. ⇨Control the offsite release (release point and monitoring)
5.4. ⇨Provide relevant and reliable information for off-site management

[45] *from INPRO methodology BP1 – CR 1.5.1*
[46] *from INPRO methodology BP3 – CR 3.1.1*

TABLE A2.1b
CLASS 2 Detailed technical Recommendations and Foreseen Characteristics and Features as function of the levels of the defence in depth.
Applicable to all the future reactors

1. 1st level : PREVENTION : Prevention of abnormal operation and failures
1.1. ⇨Work out and set up a **design for the plant** (i.e., the reactor core, primary & secondary circuit and BOP), that will allow **simple procedures for the reactor operations and maintenance during normal conditions** (i.e., minimize process' complexity and avoid inherent instability; systematic consideration of human factors and the human–machine interface for operation and shut down)
1.1.1. Elaborate and set up a simple neutronic design (core & internals)
1.1.2. Elaborate and set up a simple plant's thermo hydraulic design
1.1.3. Elaborate and set up a plant's simple thermo-mechanic design
1.1.4. Elaborate and set up a simple plant's Instrumentation & Control (I&C) system
1.1.5. Elaborate and set up a simple plant layout (primary & secondary side and BOP) allowing accessibility for ISI&R
1.1.6. Minimize the uncertainties about the operational plant conditions
1.1.7. Improve the quality of the information (operational data)
1.1.8. Improve the man-machine interface
1.1.9. Adapt the man-machine interface to the future user (human and organizational factors)
1.2. ⇨Identify the **Postulated Initiating Events**, looking for exhaustiveness, including internal and external hazards considering all plausible plant conditions (operation and shut down); **minimize their frequency of occurrence**. *N.B. The analysis is organized first, listing the conventional PIE and, in a second step, reasoning through the safety functions. This allows a crossed vision of the assets and the drawbacks of the concept*
1.2.1. Category 2 Initiating faults
1.2.2. Category 3 Initiating faults
1.2.3. Category 4 Initiating faults
1.2.4. Design extension conditions (*Limiting events* in the EFR terminology; e.g., leakage of main and safety vessel)
1.2.5. Design extension conditions (*Beyond design Plant States* in the EFR terminology; e.g., CDA without loss of roof leaktightness)
1.2.6. Event eliminated by design or practically eliminated (*Events needing demonstration of Classification in the Residual Risk* (cf. 1.3 below)
1.2.7. PIE which affect the safety function "reactivity control"
1.2.8. PIE which affect the safety function "heat removal"
1.2.9. PIE which affect the safety function "confinement of radioactive materials"
1.3. ⇨ In building the **safety architecture avoid by design** (prevent & practically eliminate) **the initiators, sequences or situations that can lead to unacceptable consequences and early chemical, toxic or radioactive releases (***including cliff edge effect)*. *N.B.: Practical elimination shall be supported by specific demonstration.*
1.3.1. Prevent & practically eliminate initiators, sequences or situations which lead to the loss of reactivity control for which it is not realistic to set up provisions for mitigation.
1.3.2. Prevent & practically eliminate initiators, sequences or situations which lead to the loss of heat removal control for which it is not realistic to set up provisions for mitigation.
1.3.3. Prevent & practically eliminate initiators, sequences or situations which lead to the loss of radioactive material confinement control for which it is not realistic to set up provisions for mitigation.
1.4. ⇨Work out and set up a **design for the process** (inherent plant's response) which allow for simple reactor management under abnormal, accidental and severe accident conditions and that that will **inherently minimise the PIE consequences** (tolerant and forgiving design for the process and the safety architecture). *N.B. As for the previous set of recommendations, the analysis is organized first, listing the conventional PIE and, in a second step, reasoning through the safety functions. This allows a crossed vision of the assets and the drawbacks of the concept*
1.4.1. Category 2 Initiating faults

1.4.2. Category 3 Initiating faults
1.4.3. Category 4 Initiating faults
1.4.4. Design extension conditions (*Limiting events* in the EFR terminology)
1.4.5. Design extension conditions (*Beyond design Plant States* in the EFR terminology)
1.4.6. PIE which affect the safety function "reactivity control" - Inherent behaviour, physical margins and slow kinetics after PIE which affect the safety function "reactivity control"
1.4.7. PIE which affect the safety function "heat removal" - Inherent behaviour, physical margins and slow kinetics after PIE which affect the safety function "heat removal"
1.4.8. PIE which affect the safety function "confinement of radioactive materials" - Inherent behaviour, physical margins and slow kinetics after PIE which affect the safety function "confinement of radioactive materials"
1.5. ⇨Work out and set up a **design for the safety architecture** (OPT / LOP / provisions) that will allow **simple procedures for the reactor operations inspection and maintenance under abnormal conditions** (i.e., minimize process' complexity and avoid inherent instability; systematic consideration of human factors and the human–machine interface for operation and shut down) *N.B. The recommendation is considered here within the 1st level of the DiD but it is detailed within the section 2.4 (2nd level of the DiD)*
1.6. ⇨Work out and set up a **design for the safety architecture** (LOP / provisions) which allow for **simple accidental intervention procedures and repair under accidental conditions** (consideration of human factor) *N.B. The recommendation is considered here within the 1st level of the DiD but it is detailed within the section 3.5 (3rd level of the DiD)*
1.7. ⇨Work out and set up a **design for the safety architecture** (OPT / LOP / provisions) which allow for **simple, progressive, tolerant, forgiving and balanced reactor's behaviour/management under accidental conditions** *N.B. The recommendation is considered here within the 1st level of the DiD but it is detailed within the sections 1.10 and 3.4 (3rd level of the DiD)*
1.8. ⇨Work out and set up a **design for the safety architecture** (LOP / provisions) which allow **for simple, management of the severe plant conditions progress and the mitigation of their consequences** *N.B. The recommendation is considered here within the 1st level of the DiD but it is detailed within the section 4.1 (4th level of the DiD)*
1.9. ⇨Select options which provide **confidence in innovation**
1.9.1. Detect, study and model new phenomena as well as scaling considerations within experimental and analytical work
1.9.2. Undertake adequate efforts to evaluate and assess the reliability of new passive components or systems
1.10. ⇨Integrate the **principles of the defence in depth** within the whole safety architecture for an **exhaustive, progressive, tolerant, forgiving and well-balanced defence** *N.B. The item addresses generic recommendations for the architecture. It is complemented by recommendations addressing the design of the provisions within the 3.4 (3rd level of the DiD)*
1.10.1. Take care to the exhaustive character of the implemented defence
1.10.2. Take care to the progressive character of the implemented defence
1.10.3. Take care to the tolerant character of the implemented defence
1.10.4. Take care to the forgiving character of the implemented defence
1.10.5. Take care to the balanced character of the implemented defence
1.11. ⇨Work out and set up a safety architecture which **minimise the potential for Common Modes**
1.11.1. Separate and diversify the provisions which achieve the same safety mission at different levels of the DiD
1.11.2. Minimise the potential for flooding
1.11.3. Minimise the potential for fires
1.11.4. Minimise the Common Mode sensitivity to human induced hazards (physical protection)
1.11.5. Protect the LOP provisions against the potential hazards generated by the abnormal conditions
1.12. ⇨Work out and set up a design that integrate **inherent security and proliferation resistance**

To be defined coherently with the recommendation of the PR&PP
1.13. ⇨Once the safety architecture available, qualify as needed the LOP provisions, both from physical performances point of view (i.e., the capability to achieve the mission) and from reliability point of view (i.e., the capability to achieve the mission with the requested reliability)
1.13.1. Work out and set up a LOP design consistent with codes and standards
1.13.2. Qualify the LOP provisions to the representative boundary conditions (i.e., all the plausible situations during which the provision is supposed to operate).
1.13.3. Qualify the LOP provisions to the single failure criterion if requested
1.13.4. Qualify the LOP provisions for the earthquake
1.13.5. Qualify the LOP provisions for other external hazards (physical protection)
1.14. ⇨**Minimize the personnel exposure** (on site releases) during normal operation, decommissioning and dismantling – ALARA
1.14.1. Strengthen the first barrier
1.14.2. Strengthen the second barrier
1.14.3. Strengthen the third barrier
1.14.4. Minimise the contact dose
1.14.5. Minimise the implementation of materials which are activated by the plant operation
1.14.6. Limit the length of circuits which carry activated fluid
1.14.7. Minimise the maintenance times for normal conditions
1.14.8. Minimize the need for access to, or transit through, radiological zones
1.14.9. Innovative designs should be maintenance-friendly through careful layout, reliable equipment, and availability of maintenance procedures electronically at the work-face to guide the maintainer
1.15. ⇨**Minimize the risk for environment contamination** (off site radioactive material release) during normal operation, decommissioning and dismantling - ALARA
1.15.1. Simplify the chemistry of the primary circuit coolant
1.15.2. Minimize the self - generation of radioactive waste
1.15.3. Minimize the corrosion phenomenon
1.15.4. Ensure the good materials behaviour under irradiation
1.16. ⇨**Minimize the personnel exposure under abnormal, accidental and severe accident conditions** - ALARA (operation and shut down)
1.16.1. Minimize the time for the intervention & repair under abnormal conditions
1.16.2. Strengthen the first barrier
1.16.3. Strengthen the second barrier
1.16.4. Strengthen the third barrier
1.16.5. Innovative designs and the safety provisions implemented for the accidental conditions (3^{rd} level of the DiD) should allow repair-friendly through careful layout, reliable equipment, and availability of repair procedures electronically at the work-face to guide the repairer
1.16.6. Safety provisions implemented to materialize the 4^{th} level of the DiD, should be able to control severe accident scenarios and mitigate their consequences in a way that do not require or minimize the operator exposure.
1.17. ⇨A **reduced-scale pilot plant or large-scale demonstration facility** should be built for reactors and/or fuel cycle processes, which represent a major departure from existing operating experience
1.17.1. In case of high degree of novelty a small scale facility should be specified, built, operated, and lessons learned documented.
1.17.2. In case of low degree of novelty provide rationale for bypassing pilot plant.
1.18. ⇨**Uncertainties and sensitivities identified and appropriately dealt with?**
1.18.1. Provide evidence that a thorough analysis of uncertainties including complementary sensitivity studies has been performed. Three classes of uncertainties are identified:
1.18.1.1. Parameter (data) uncertainty, like initiating event frequencies, component failure rates, human error probabilities, etc.;
1.18.1.2. Model uncertainty associated with phenomenological models of the physical-chemical processes and related assumptions;
1.18.1.3. Completeness uncertainties reflect limitations of the scope or truncation effects.

TABLE A2.1b (cont)
CLASS 2 Detailed technical Recommendations and Foreseen Characteristics and Features as function of the levels of the defence in depth.
Applicable to all the future reactors

2. ★ 2nd level :CONTROL : control of abnormal operations and detection of failures-
2.1. ⇨Implement a **layer of inherent or extrinsic provisions**, so that if a failure of the previous layer occurs (PIE, 1st level of the DiD), it would be detected and, if possible, managed by appropriate measures to keep the plant in safe conditions without soliciting the safety provisions which belong to the follow levels of the DiD
2.1.1. Implement provisions to detect the Postulated Initiating Events (abnormal conditions) :
2.1.1.1. Category 2 Initiating faults
2.1.1.2. Category 3 Initiating faults
2.1.1.3. Category 4 Initiating faults
2.1.1.4. Design extension conditions (*Limiting events* in the EFR terminology)
2.1.1.5. Design extension conditions (*Beyond design Plant States* in the EFR terminology
2.1.1.6. PIE which affect the safety function "reactivity control"
2.1.1.7. PIE which affect the safety function "heat removal"
2.1.1.8. PIE which affect the safety function "confinement of radioactive materials"
2.2. ⇨**Minimise the uncertainties** about the plant conditions under abnormal conditions
2.2.1. Implement a design that inherently simplify the abnormal sequences (intrinsically stable behaviour)
2.2.2. Implement an adequate instrumentation (for automatic and manual intervention)
2.3. ⇨Work out and set up a design with simple and efficient inherent behaviour under abnormal conditions (tolerant and forgiving design for the process and the safety architecture[47]; avoid inherent instabilities) *(For recall → must / can be realised at the prevention level; cf. 1.4)*
2.4. ⇨Work out and set up a design for the safety architecture (OPT / LOP / provisions) that will allow **simple procedures for the reactor operations inspection and maintenance under abnormal conditions** (i.e., minimize process' complexity and avoid inherent instability; systematic consideration of human factors and the human–machine interface for operation and shut down) *N.B. The recommendation is first considered at the 1.5 (1st level of the DiD) but it is detailed in this section 2.4*
2.4.1. Improve the quality of the available information (operation data; In Service Inspection - ISI)
2.4.2. Simplify and automatize the procedures for the plant operation under abnormal conditions.
2.4.3. Simplify and automatize the procedures for the plant inspection, maintenance and repair
2.4.4. Minimize the needs for use of safety provision which belong to the protection level of the defence in depth
2.5. ⇨Defining the abnormal conditions to be assessed, **take into account possible aggravating situations** (coherently with the PIE category)
2.5.1. Minimize the potential consequences of aggravating situations
2.5.2. Take into account the unavailability for maintenance of corrective functions
2.5.3. Take into account the PIE with cumulative failures
2.6. ⇨Minimize the **personnel exposure under abnormal conditions**[48] - ALARA Minimise the radioactive potential for injuries under abnormal conditions (operation and shut down) *(For recall → must / can be realised at the prevention level; cf. 1.16)*

[47] No small deviation of the physical parameters, outside the expected ranges, can lead to severe consequences ; appropriate grace period and the possibility of repair and restoring during abnormal conditions

[48] This recommendation can likely be associated to the one within the 3rd level of the DiD considering together "abnormal and accidental conditions".

TABLE A2.1b (cont)
CLASS 2 Detailed technical Recommendations and Foreseen Characteristics and Features as function of the levels of the defence in depth.
Applicable to all the future reactors

3. ★3rd level : PROTECTION : Control of accident within the design basis and prevention of severe plant conditions
3.1. ⇨Implement a **layer of provisions, so that if a failure of the previous layer(s) occurs, it would be detected and managed by appropriate measures** to meet the objectives of the design basis accidents domain while preventing the severe plant conditions. Minimize the frequency of occurrence of severe plant conditions (core degradation)
3.1.1. Implement, through ad-hoc provisions, an adequate functional redundancy, for all the safety functions, to cope with the failure of the previous levels of the defence in depth.
3.1.2. Insure the availability and the reliability of the provisions which belong to the 3rd level of the Defence in depth
3.1.3. Implement an adequate instrumentation to follow the status of the plant (for automatic and manual intervention; cf. 2.1 & 3.2.1)
3.2. ⇨**Minimise the uncertainties about the plant conditions under accidental conditions** (operation and shut down)
3.2.1. Implement an adequate instrumentation to follow the status of the plant (for automatic and manual intervention)
3.2.2. Implement a design that simplify the accidental sequences (cf. also 1.4)
3.2.3. Protect the LOP provisions against the potential hazards generated by the accidental conditions
3.3. ⇨Work out and set up a **design for the process** (inherent response) **which allow for simple reactor management under abnormal, accidental and severe accident conditions and that that will inherently minimise the PIE consequences**. *N.B. The analysis concerning the inherent characteristics of the plant is addressed at the first level of the DiD (1.2 for the PIE frequency of occurrence & 1.4 for the inherent minimization of the PIE consequences). The objective and the scope of the recommendations at this third level of the DiD are to insure that the engineered provisions, and finally the LOPs, are correctly sized to answer the requested missions.* *Below the analysis is organized first, listing the conventional third category PIE and, in a second step, reasoning through the safety functions.* *N.B. Normally, the Cat 2 initiating faults do not challenge the third level of the DiD and are managed by the first and second level of the DiD. As well, the Design Extension Conditions belong to the 4th level of the DiD*
3.3.1. Category 3 Initiating faults
3.3.2. Category 4 Initiating faults
3.3.3. Independent LOPs for the accidental sequences which follow PIEs which affect the safety function “reactivity control”
3.3.4. Independent LOPs for the accidental sequences which follow PIEs which affect the safety function “heat removal”
3.3.5. Independent LOPs for the accidental sequences which follow PIEs which affect the safety function “confinement of radioactive materials”
3.3.6. Minimize the possibilities for “short” sequences (i.e., the failure of a provision entails a major increase of consequences, without any possibility of restoring safe conditions at an intermediate stage)
3.3.7. Ensure appropriate physical margins
3.3.8. Ensure appropriate grace period and the possibility of repair and restoring during accidental conditions
3.4. ⇨Work out and set up a design for the **safety architecture** (LOP / provisions) **which allow for simple, progressive, tolerant, forgiving and balanced reactor’s behaviour/management under accidental conditions** *N.B. The analysis concerning the generic characteristics of the plant architecture is addressed at the first level of the DiD (cf. 1.101). The objective and the scope of the recommendations at this third level of the DiD are to insure that the engineered provisions, and finally the LOPs, are*

correctly sized to answer the requested missions.
3.4.1. Independent LOPs for the accidental sequences which follow PIEs which affect the safety function "reactivity control"
3.4.2. Independent LOPs for the accidental sequences which follow PIEs which affect the safety function "heat removal"
3.4.2.1. Sequences initiated by the loss of primary coolant flow
3.4.2.2. Sequences initiated by a leakage of primary coolant
3.4.2.3. Sequences initiated by the degradation of the normal heat removal path
3.4.2.4. Sequences initiated by loss heat sink
3.4.3. Independent LOPs for the accidental sequences which follow PIEs which affect the safety function "confinement of radioactive materials"
3.4.3.1. Sequences initiated by barriers leakages (fuel, primary confinement, secondary confinement)
3.4.4. Minimize the possibilities for "short" sequences (i.e., the failure of a provision entails a major increase of consequences, without any possibility of restoring safe conditions at an intermediate stage)
3.4.5. Ensure appropriate physical margins
3.4.6. Ensure appropriate grace period and the possibility of repair and restoring during accidental conditions
3.4.7. Ensure that no initiator or sequence contributes in an excessive and unbalanced manner to the global frequency of the damaged plant states
3.5. ⇨Work out and set up a design for the **safety architecture** (LOP / provisions) **which allow for simple accidental intervention procedures and repair under accidental conditions** (consideration of human factor) *N.B. The recommendation is first considered at the 1.6 (1st level of the DiD) but it is detailed in this section 3.5*
3.5.1. Implement a design that inherently simplify the accidental sequences
3.5.2. Ensure an adequate information (accidental situation)
3.5.3. Simplify and automatize the procedures for the accident management
3.5.4. Simplify and automatize the procedures for the plant inspection, and repair
3.6. ⇨Work out and set up a safety architecture which minimize the **potential for Common Modes** (mutual aggressions, internal or external hazards) *N.B. The recommendation is considered and detailed at the 1.11 (1st level of the DiD) for the whole safety architecture; it is detailed in this section 3.6 focusing on the recommendation for the LOP design, especially concerning the requested reliability*
3.6.1. In designing the LOPs content and layout, provide provisions' separation and diversification in order to guarantee the requested reliability
3.7. ⇨In defining the accidental sequence to be assessed, take into account **possible aggravating situations** (coherently with the PIE category))
3.7.1. Take into account the possibility for aggravating failure
3.7.2. Take into account the unavailability for maintenance of corrective functions
3.7.3. Take into account the accidental sequences with cumulative provisions failures (complex sequences)
3.8. ⇨Number of **confinement barriers maintained**
3.8.1. The design of engineered safety features should deterministically provide for continued integrity at least of one barrier (containing the radioactive material) following any design basis accident
3.9. ⇨**Minimize the personnel exposure** (including on site release) under accidental conditions – ALARA ***(For recall → must / can be realised at the prevention level; cf. 1.16)***
3.10. ⇨**Minimize the risk for the environment contamination** (off site release) under abnormal and accidental conditions (without core degradation) – ALARA
3.10.1. Conceive the plant looking for the guarantee that plants would be so safe that there would be no technical justification for an emergency plan involving evacuation of the nearby population

TABLE A2.1b (cont)
CLASS 2 Detailed technical Recommendations and Foreseen Characteristics and Features as function of the levels of the defence in depth.
Applicable to all the future reactors

4. **★ 4th level : SEVERE ACCIDENT MANAGEMENT- accident management including the confinement protection** ***N.B*** *The safety approach, coherently with the fourth level of the defence in depth, is completed by the consideration of plant conditions with more or less important core degradation (if need be, until the whole core melting) and the implementation of provisions which aim at making the risk acceptable. This is why the designer has to select and take into account the severe plant conditions configurations to be considered within the basis for the design of the safety architecture (i.e., the set of conditions considered for the design of the single provisions/LOP). Analogously the designer should prevent & practically eliminate the initiators, sequences or situations that can lead to unacceptable consequences and early releases. Finally he should reject the risk for the cliff edge effect. In conclusion :*
• *according to the fourth level of the defence in depth, some representative severe plant conditions have to be considered, in particular to demonstrate the effectiveness of the safety architecture and to prove the robustness of the confinement*
• *a limited number of initiators, sequences or situations, for which it is not realistic to set up provisions for mitigation, or to assure, with a sufficient degree of confidence, that their consequences would be mastered, will be eliminated by design or "practically eliminated" implementing specific provisions which guarantee their rejection within the Residual Risk (RR)*
4.1. ⇨Implement a layer of provisions/LOP, so that if a failure of the previous layer(s) occurs, the severe plant condition will be detected, managed and mitigated by appropriate measures and its consequences duly mitigated
4.1.1. Implement a design that inherently simplify the severe accident sequences (cf. 1.4)
4.1.2. To cope with the failure of the previous levels of the defence in depth, ensure the safety function accomplishment under severe accident conditions implementing, through ad-hoc provisions, an adequate functional redundancy, for all the safety functions.
4.2. **Minimise the uncertainties about the plant conditions under accidental conditions** (operation and shut down)
4.2.1. Implement an adequate instrumentation to follow the status of the plant (for automatic and manual intervention)
4.2.2. Implement a design that simplify the accidental sequences (cf.1.4)
4.2.3. Allow the implementation of procedures for the plant inspection following severe accidental conditions
4.2.4. Protect the LOP provisions against the potential hazards generated by the severe plant conditions (pressure, temperature, etc.)
4.3. ⇨Work out and set up a design for the safety architecture (LOP / provisions) which allow **for simple management of the severe plant conditions progress and the mitigation of their consequences** *N.B. The analysis concerning the inherent characteristics of the plant is addressed at the first level of the DiD (1.2 for the PIE frequency of occurrence & 1.4 for the inherent minimization of the PIE consequences). The objective and the scope of the recommendations at this fourth level of the DiD are to insure that the engineered provisions, and finally the LOPs, are correctly sized to answer the requested missions.* *Below the analysis is organized first, listing the conventional Design extension Conditions and, in a second step, reasoning through the safety functions*.
4.3.1. Design extension conditions (*Limiting events* in the EFR terminology)
4.3.2. Design extension conditions (*Beyond design Plant States* in the EFR terminology)
4.3.3. Independent LOPs for Design Extension Conditions which require the safety function "reactivity control"
4.3.4. Independent LOPs for Design Extension Conditions which require the safety function "heat removal"
4.3.5. Independent LOPs for Design extension conditions which require the safety function

"confinement of radioactive materials"
4.3.6. Ensure appropriate physical margins
4.3.7. Simplify and automatize the procedures for the severe accident management
4.3.8. Improve the grace delay
4.4. ⇨Avoid major release of radioactive materials into the environment: A major release of radioactivity should be prevented for all practical purposes, so that innovative systems would not need relocation or evacuation measures outside the plant site, apart from those generic emergency measures developed for any industrial facility used for similar purpose
4.4.1. Safety provisions should be able to control severe accident scenarios and mitigate their consequences, so as to prevent containment failure. Control and mitigation should address all threats (internal and external). Thus innovative designs should show that:
4.4.1.1. The likelihood of a large release is so small that off-site emergency measures, while they may reduce the consequences thereof, do not lead to a significant reduction in risk; or
4.4.1.2. A large release could be excluded by design for all practical purposes, e.g., through use of inherent safety characteristics.
4.5. ⇨Minimize the personnel exposure (on site accidental release) under accidental conditions-ALARA *(For recall → must / can be realised at the prevention level; cf. 1.16)*
4.6. ⇨Minimise the offsite accidental release during the severe plant conditions
4.6.1. Conceive the containment provisions in order to keep the containment capabilities compatible with the objective to guarantee that:
4.6.1.1. the likelihood of a large release is so small that off-site emergency measures, while they may reduce the consequences thereof, do not lead to a significant reduction in risk; or
4.6.1.2. a large release is excluded by design for all practical purposes
4.6.2. Conceive in order to need only very limited protective measures in area and in time
5. ★ 5th level : CONSEQUENCES MITIGATION - Mitigation of radiological consequences of significant releases of radioactive materials
5.1. ⇨Delay the offsite release
5.2. ⇨Minimise the offsite radioactive release
5.3. ⇨Control the offsite release (release point and monitoring)
5.4. ⇨Provide relevant and reliable information for off-site management

TABLE A21 c
CLASS 3 : Detailed & Technology neutral recommendations applicable to a given safety function
(*) Recommendations applicable to the decay heat removal (DHR) safety function

1. 1st level : PREVENTION : Prevention of abnormal operation and failures
1.1. ⇨Work out and set up a **design for the plant** (i.e., the reactor core, primary & secondary circuit and BOP), that will allow **simple procedures for the reactor operations and maintenance during normal conditions** (i.e., minimize process' complexity and avoid inherent instability; systematic consideration of human factors and the human–machine interface for operation and shut down)
1.1.1. Elaborate and set up a simple neutronic design (core & internals)
1.1.2. Elaborate and set up a simple plant's thermo hydraulic design
1.1.2.1. Simplify the thermo hydraulic for the normal operating conditions (heat removal at nominal operating conditions and during nominal operational transients) – Primary (vessel internals) and Secondary side
1.1.2.2. Simplify the thermo hydraulic for the normal DHR
1.1.2.3. Simplify the thermo hydraulic for the safety DHR
1.1.2.4. Separate the normal operating DHR function from the safety DHR
1.1.2.5. Increase the range covered by normal DHR systems (forced convection, natural convection)
1.1.2.6. Minimize the number of components per system
1.1.2.7. Standardize the components among normal operating DHR and safeguard DHR
1.1.3. Elaborate and set up a plant's simple thermo-mechanic design
1.1.3.1. Simplify the primary vessel internals from mechanical point of view
1.1.3.1.1. Leaktightness
1.1.3.1.2. Corrosion
1.1.3.1.3. Defaults and cracks propagation
1.1.3.1.4. Vibrations
1.1.3.2. Minimize the number of systems connected to the primary circuit
1.1.3.3. Minimize the impact of transients
1.1.3.3.1. Minimise the thermo mechanical loads during operational transients
1.1.3.3.2. Minimise the thermo mechanical loads during abnormal and accidental transients
1.1.3.4. Minimize the number of components per system
1.1.4. Elaborate and set up a simple plant's Instrumentation & Control (I&C) system
1.1.5. Elaborate and set up a simple plant layout (primary & secondary side and BOP) allowing accessibility for ISI&R
1.1.6. Minimize the uncertainties about the operational plant conditions
1.1.7. Improve the quality of the information (operational data)
1.1.7.1. Implement adequate control on systems behaviour and status
1.1.8. Improve the man-machine interface
1.1.9. Adapt the man-machine interface to the future user (human and organizational factors)
1.1.9.1. Simplify and automatize as needed and justified the procedures for the operation
1.1.9.2. Simplify and automatize as needed and justified the procedures for the inspection
1.1.9.3. Simplify and automatize as needed and justified the procedures for the maintenance and preventive repair
1.2. ⇨Identify the **Postulated Initiating Events**, looking for exhaustiveness, including internal and external hazards considering all plausible plant conditions (operation and shut down); **minimize their frequency of occurrence**. *N.B. The analysis is organized first, listing the conventional PIE and, in a second step, reasoning through the safety functions. This allows a crossed vision of the assets and the drawbacks of the concept*
1.2.1. Category 2 Initiating faults
1.2.1.1. LOOSP <1 hour
1.2.1.2. Inadvertent reduction of primary pump

1.2.1.3. Etc. List to be completed
1.2.2. Category 3 Initiating faults
1.2.2.1. LOOSP >1 hour
1.2.2.2. Coast down of all primary pumps not due to the LOSSP
1.2.2.3. Etc. List to be completed
1.2.3. Category 4 Initiating faults
1.2.3.1. Loss of redundant systems (e.g., vault cooling circuits; roof cooling circuits; etc.)
1.2.3.2. Primary pump faults (pump seizure and shaft failure)
1.2.3.3. Missiles
1.2.3.4. Earthquake
1.2.3.5. Etc. List to be completed
1.2.4. Design extension conditions (*Limiting events* in the EFR terminology; e.g., leakage of main and safety vessel)
1.2.4.1. Leakage of main and safety vessel
1.2.4.2. Etc. List to be completed
1.2.5. Design extension conditions (*Beyond design Plant States* in the EFR terminology; e.g., CDA without loss of roof leaktightness)
1.2.5.1. CDA without loss of roof leaktightness
1.2.5.2. Etc. List to be completed
1.2.6. Event eliminated by design or practically eliminated (*Events needing demonstration of Classification in the Residual Risk* (cf. 1.3 below)
1.2.7. PIE which affect the safety function “reactivity control”
1.2.7.1. Inherent core reactivity changes (e.g., due to geometry changes)
1.2.7.2. Reactivity changes induced by events external to the core (e.g., Control rod withdrawal)
1.2.8. PIE which affect the safety function “heat removal”
1.2.8.1. Sequences initiated by the degradation of the normal heat removal path within the primary circuit
1.2.8.1.1. Sequences initiated by the loss of primary coolant flow
1.2.8.1.1.1. Set up a reliable primary fluid circulation (i.e., avoiding the possibility for uncontrolled bypasses)
1.2.8.1.1.2. Minimise the risk for normal flow disturbances (e.g., blockages)
1.2.8.1.1.3. Simplify the primary fluid path and set up the possibility for reliable natural convection
1.2.8.1.2. Sequences initiated by the leakage of primary coolant
1.2.8.1.2.1. Minimise the number of connections on primary circuit
1.2.8.1.2.2. Minimise the length of the pipes which carry primary fluid
1.2.8.1.2.3. Minimise the energy stored within the primary fluid (e.g., primary pressure)
1.2.8.1.2.4. Minimise the phenomena which, inducing abnormal stress and strains on the primary circuit, can increase the risk of its failure/leakage (e.g., those phenomenon which can induce corrosion)
1.2.8.1.3. Sequences initiated by physical modifications within the primary circuit (changes in conductivity, convection or radiation properties)
1.2.8.1.3.1. Provide the adequate means to keep the properties within allowable ranges
1.2.8.2. Sequences initiated by the degradation of the normal heat removal path downstream the primary circuit
1.2.8.2.1. Sequences initiated by the loss of secondary coolant flow
1.2.8.2.1.1. Set up a reliable secondary fluid circulation (i.e., avoiding the possibility for uncontrolled bypasses)
1.2.8.2.1.2. Minimise the risk for nominal flow disturbances (e.g., blockages)
1.2.8.2.1.3. Simplify the secondary fluid path and set up the possibility for reliable natural convection
1.2.8.2.2. Sequences initiated by the leakage of secondary coolant
1.2.8.2.2.1. Minimise the length of the pipes which carry secondary fluid

1.2.8.2.2.2. Minimise the energy stored within the secondary fluid (e.g., secondary pressure)
1.2.8.2.2.3. Minimise the phenomena which, inducing abnormal stress and strains on the secondary circuit, can increase the risk of its failure/leakage (e.g., those phenomenon which can induce corrosion)
1.2.8.2.3. Sequences initiated by physical modifications within the secondary circuit (changes in conductivity, convection or radiation properties)
1.2.8.2.3.1. Provide the adequate means (e.g., accessibility, measurements, etc.) to keep the properties within allowable ranges
1.2.8.3. Sequences initiated by loss heat sink
1.2.8.3.1. Provide reliable ultimate heat sink
1.2.9. PIE which affect the safety function "confinement of radioactive materials"
1.2.9.1. Sequences initiated by barriers leakages (fuel, primary confinement, secondary confinement)
1.3. ⇨ In building the **safety architecture avoid by design** (prevent & practically eliminate) **the initiators, sequences or situations that can lead to unacceptable consequences and early chemical, toxic or radioactive releases (***including cliff edge effect).* *N.B.: Practical elimination shall be supported by specific demonstration.*
1.3.1. Prevent & practically eliminate initiators, sequences or situations which lead to the loss of reactivity control for which it is not realistic to set up provisions for mitigation.
1.3.2. Prevent & practically eliminate initiators, sequences or situations which lead to the loss of heat removal control for which it is not realistic to set up provisions for mitigation.
1.3.2.1. Set up an ultimate DHR LOP capable to sustain the selected severe plant conditions
1.3.2.2. Set up sufficient DHR LOP (number and quality) to practically eliminate the total loss of the DHR.
1.3.3. Prevent & practically eliminate initiators, sequences or situations which lead to the loss of radioactive material confinement control for which it is not realistic to set up provisions for mitigation.
1.4. ⇨Work out and set up a **design for the process** (inherent plant's response) which allow for simple reactor management under abnormal, accidental and severe accident conditions and that that will **inherently minimise the PIE consequences** (tolerant and forgiving design for the process and the safety architecture). *N.B. As for the previous set of recommendations, the analysis is organized first, listing the conventional PIE and, in a second step, reasoning through the safety functions. This allows a crossed vision of the assets and the drawbacks of the concept*
1.4.1. Category 2 Initiating faults
1.4.1.1. LOOSP <1 hour
1.4.1.2. Inadvertent reduction of primary pump flow
1.4.1.3. Etc. List to be completed
1.4.2. Category 3 Initiating faults
1.4.2.1. LOOSP >1 hour
1.4.2.2. Coastdown of all primary pumps not due to the LOSSP
1.4.2.3. Etc. List to be completed
1.4.3. Category 4 Initiating faults
1.4.3.1. Loss of redundant systems (e.g., vault cooling circuits; roof cooling circuits; etc.)
1.4.3.2. Primary pump faults (pump seizure and shaft failure)
1.4.3.3. Missiles
1.4.3.4. Earthquake
1.4.3.5. Etc. List to be completed
1.4.4. Design extension conditions (*Limiting events* in the EFR terminology)
1.4.4.1. Leakage of main and safety vessel
1.4.4.2. List to be completed
1.4.5. Design extension conditions (*Beyond design Plant States* in the EFR terminology)
1.4.5.1. CDA without loss of roof leaktightness
1.4.5.2. List to be completed
1.4.6. PIE which affect the safety function "reactivity control" - Inherent behaviour, physical margins and slow kinetics after PIE which affect the safety function "reactivity control"

1.4.6.1. Inherent core reactivity changes (e.g., due to geometry changes)
1.4.6.2. Reactivity changes induced by events external to the core (e.g., Control rod withdrawal)
1.4.7. PIE which affect the safety function "heat removal" - Inherent behaviour, physical margins and slow kinetics after PIE which affect the safety function "heat removal"
1.4.7.1. Sequences initiated by the degradation of the normal heat removal path within the primary circuit
1.4.7.1.1. Sequences initiated by the loss of primary coolant flow
1.4.7.1.1.1. Foresee inertia in case of local blockage
1.4.7.1.1.2. Foresee an adequate inertia for the normal operation primary side circulation mode (e.g., pump inertia)
1.4.7.1.1.3. Foresee the natural convection behaviour on primary side
1.4.7.1.2. Sequences initiated by a leakage of primary coolant
1.4.7.1.2.1. Minimise the effects due to the loss of primary tightness
1.4.7.1.2.2. Ensure the DHR with reduced primary coolant inventory
1.4.7.1.3. Sequences initiated by physical modifications within the primary circuit (changes in conductivity, convection or radiation properties)
1.4.7.1.3.1. Provide the adequate means (e.g., accessibility, measurements, etc.) to restore the properties within allowable ranges
1.4.7.2. Sequences initiated by the degradation of the normal heat removal path downstream the primary circuit
1.4.7.2.1. Sequences initiated by the loss of secondary coolant flow
1.4.7.2.1.1. Foresee an adequate inertia for the operation secondary side circulation mode (e.g., pump inertia)
1.4.7.2.1.2. Foresee the natural convection behaviour on secondary side
1.4.7.2.2. Sequences initiated by the leakage of secondary coolant
1.4.7.2.2.1. Minimise the effects due to the loss of secondary tightness
1.4.7.2.2.2. Ensure the DHR with reduced primary coolant inventory
1.4.7.2.3. Sequences initiated by physical modifications within the primary circuit (changes in conductivity, convection or radiation properties)
1.4.7.2.3.1. Provide the adequate means (e.g., accessibility, measurements, etc.) to restore the properties within allowable ranges
1.4.7.2.4. Provide alternative paths for the DHR
1.4.7.3. Sequences initiated by loss heat sink
1.4.7.3.1. Foresee an adequate inertia to help keeping/restoring acceptable conditions
1.4.7.4. For each of above PIE ensure appropriate physical margins:
1.4.7.4.1. Improve the system efficiency
1.4.7.4.2. Increase the common range (overlapped domain) covered by redundant LOP belonging to different levels of the DiD,
1.4.7.5. For each of above PIE provide appropriate grace period :
1.4.7.5.1. Increase the process internal inertia; this inertia is considered as an integral part of the DHR/LOPs
1.4.7.5.2. Provide the passive access to adequate external inertia,
1.4.7.6. For each of above PIE provide the possibility of repair and restoring during abnormal conditions
1.4.8. PIE which affect the safety function "confinement of radioactive materials" - Inherent behaviour, physical margins and slow kinetics after PIE which affect the safety function "confinement of radioactive materials"
1.4.8.1. Sequences initiated by barriers leakages (fuel, primary confinement, secondary confinement)
1.5. ⇨Work out and set up a **design for the safety architecture** (OPT / LOP / provisions) that will allow **simple procedures for the reactor operations inspection and maintenance under abnormal conditions** (i.e., minimize process' complexity and avoid inherent instability; systematic consideration of human factors and the human–machine interface for operation and shut down) *N.B. The recommendation is considered here within the 1st level of the DiD but it is detailed*

within the section 2.4 (2nd level of the DiD)
1.6. ⇨Work out and set up a **design for the safety architecture** (LOP / provisions) which allow for **simple accidental intervention procedures and repair under accidental conditions** (consideration of human factor) *N.B. The recommendation is considered here within the 1st level of the DiD but it is detailed within the section 3.5 (3rd level of the DiD)*
1.7. ⇨Work out and set up a **design for the safety architecture** (OPT / LOP / provisions) which allow for **simple, progressive, tolerant, forgiving and balanced reactor's behaviour/management under accidental conditions** *N.B. The recommendation is considered here within the 1st level of the DiD but it is detailed within the sections 1.10 and 3.4 (3rd level of the DiD)*
1.8. ⇨Work out and set up a **design for the safety architecture** (LOP / provisions) which allow **for simple, management of the severe plant conditions progress and the mitigation of their consequences** *N.B. The recommendation is considered here within the 1st level of the DiD but it is detailed within the section 4.1 (4th level of the DiD)*
1.9. ⇨Select options which provide **confidence in innovation**
1.9.1. Detect, study and model new phenomena as well as scaling considerations within experimental and analytical work
1.9.2. Undertake adequate efforts to evaluate and assess the reliability of new passive components or systems
1.10. ⇨Integrate the **principles of the defence in depth** within the whole safety architecture for an **exhaustive, progressive, tolerant, forgiving and well-balanced defence** *N.B. The item addresses generic recommendations for the architecture. It is complemented by recommendations addressing the design of the provisions within the 3.4 (3rd level of the DiD)*
1.10.1. Take care to the exhaustive character of the implemented defence
1.10.1.1. For each plant condition (PC : PIE applied to an Initial plant status), implement an number of Lines of protection (LOP) coherent with the probabilistic objectives → (2a+b)
1.10.2. Take care to the progressive character of the implemented defence
1.10.2.1. Implement functional redundancies: independent LOP
1.10.3. Take care to the tolerant character of the implemented defence
1.10.3.1. Foresee control and limitation devices
1.10.3.2. Implement safety margins around the operational conditions
1.10.3.3. Minimize of the use of safety provisions which belong to the protection level of the defence in depth
1.10.4. Take care to the forgiving character of the implemented defence
1.10.4.1. Implement grace delay for the LOP intervention
1.10.5. Take care to the balanced character of the implemented defence
1.10.5.1. Implement an homogeneous number of LOP for each plant condition
1.11. ⇨Work out and set up a safety architecture which **minimise the potential for Common Modes**
1.11.1. Separate and diversify the provisions which achieve the same safety mission at different levels of the DiD
1.11.1.1. Diversify the components
1.11.1.2. Keep segregate the single loops
1.11.2. Minimise the potential for flooding
1.11.2.1. Put out of water the provisions important for safety
1.11.3. Minimise the potential for fires
1.11.3.1. Implement incombustible materials
1.11.4. Minimise the Common Mode sensitivity to human induced hazards (physical protection)
1.11.4.1. Minimize the possibility for simultaneous injuries to LOP provisions which will lead to the whole LOP failure
1.11.5. Protect the LOP provisions against the potential hazards generated by the abnormal conditions
1.11.5.1. Protect the provisions which belong to the second, third and fourth level of the DiD against hazards which characterize the accidental conditions (temperature, pressure,

etc.)
1.12. ⇨Work out and set up a design that integrate **inherent security and proliferation resistance** *To be defined coherently with the recommendation of the PR&PP*
1.13. ⇨Once the safety architecture available, qualify as needed the LOP provisions, both from physical performances point of view (i.e., the capability to achieve the mission) and from reliability point of view (i.e., the capability to achieve the mission with the requested reliability)
1.13.1. Work out and set up a LOP design consistent with codes and standards
1.13.2. Qualify the LOP provisions to the representative boundary conditions (i.e., all the plausible situations during which the provision is supposed to operate).
1.13.2.1. Qualify the materials for the planned function (performances)
1.13.2.2. Qualify the materials for the requested reliability
1.13.2.3. Qualify the materials for the requested availability
1.13.2.4. Qualify the materials for the expected environmental conditions
1.13.2.5. Plan the possibility for representative tests
1.13.2.6. Standardize the components among systems (improve the feedback experience)
1.13.3. Qualify the LOP provisions to the single failure criterion if requested
1.13.3.1. Take into account the Passive Single Failure criterion for the short term
1.13.4. Qualify the LOP provisions for the earthquake
1.13.4.1. Minimize the sensitivity of LOP provisions to earthquake
1.13.5. Qualify the LOP provisions for other external hazards (physical protection)
1.13.5.1. Minimize the sensitivity of LOP provisions to external hazards and aggressions
1.14. ⇨**Minimize the personnel exposure** (on site releases) during normal operation, decommissioning and dismantling – ALARA
1.14.1. Strengthen the first barrier
1.14.2. Strengthen the second barrier
1.14.2.1. Conceive the circuits connected to the primary
1.14.2.1.1. permanently → installed within the containment
1.14.2.1.2. temporarily → possibly outside the containment but isolable
1.14.2.2. Conceive the circuits connected to the secondary
1.14.2.2.1. designed to sustain the maximum injection pressure
1.14.2.2.2. in order to confine the discharge within the containment
1.14.3. Strengthen the third barrier
1.14.3.1. Limit the number of containment penetrations (building)
1.14.4. Minimise the contact dose
1.14.4.1. Minimize the corrosion phenomena and the radioactive products transport
1.14.5. Minimise the implementation of materials which are activated by the plant operation
1.14.6. Limit the length of circuits which carry activated fluid
1.14.6.1. Minimize the portions of circuits that carries primary coolant
1.14.7. Minimise the maintenance times for normal conditions
1.14.7.1. Improve the accessibility
1.14.7.2. Foresee equipments and robots
1.14.8. Minimize the need for access to, or transit through, radiological zones
1.14.9. Innovative designs should be maintenance-friendly through careful layout, reliable equipment, and availability of maintenance procedures electronically at the work-face to guide the maintainer
1.15. ⇨**Minimize the risk for environment contamination** (off site radioactive material release) during normal operation, decommissioning and dismantling - ALARA
1.15.1. Simplify the chemistry of the primary circuit coolant
1.15.2. Minimize the self - generation of radioactive waste
1.15.3. Minimize the corrosion phenomenon
1.15.4. Ensure the good materials behaviour under irradiation
1.16. ⇨**Minimize the personnel exposure under abnormal, accidental and severe accident conditions** - ALARA (operation and shut down)
1.16.1. Minimize the time for the intervention & repair under abnormal conditions
1.16.1.1. Improve the accessibility
1.16.1.2. Foresee equipments and robots

1.16.2. Strengthen the first barrier
1.16.3. Strengthen the second barrier
1.16.3.1. Conceive the circuits connected to the primary
1.16.3.1.1. permanently → installed within the containment
1.16.3.1.2. temporarily → possibly outside the containment but isolable
1.16.3.2. Conceive the circuits connected to the secondary
1.16.3.2.1. designed to sustain the maximum injection pressure
1.16.3.2.2. in order to confine the discharge within the containment
1.16.4. Strengthen the third barrier
1.16.4.1. Limit the number of containment penetrations (building)
1.16.5. Innovative designs and the safety provisions implemented for the accidental conditions (3rd level of the DiD) should allow repair-friendly through careful layout, reliable equipment, and availability of repair procedures electronically at the work-face to guide the repairer
1.16.6. Safety provisions implemented to materialize the 4th level of the DiD, should be able to control severe accident scenarios and mitigate their consequences in a way that do not require or minimize the operator exposure.
1.17. ⇨A **reduced-scale pilot plant or large-scale demonstration facility** should be built for reactors and/or fuel cycle processes, which represent a major departure from existing operating experience
1.17.1. In case of high degree of novelty a small scale facility should be specified, built, operated, and lessons learned documented.
1.17.2. In case of low degree of novelty provide rationale for bypassing pilot plant.
1.18. ⇨**Uncertainties and sensitivities identified and appropriately dealt with?**
1.18.1. Provide evidence that a thorough analysis of uncertainties including complementary sensitivity studies has been performed. Three classes of uncertainties are identified:
1.18.1.1. Parameter (data) uncertainty, like initiating event frequencies, component failure rates, human error probabilities, etc.,
1.18.1.2. Model uncertainty associated with phenomenological models of the physical-chemical processes and related assumptions,
1.18.1.3. Completeness uncertainties reflect limitations of the scope or truncation effects.

TABLE A21 c (cont)
CLASS 3 : Detailed & Technology neutral recommendations applicable to a given safety function
(*) Recommendations applicable to the decay heat removal (DHR) safety function

2. ★ 2nd level :CONTROL : control of abnormal operations and detection of failures-
2.1. ⇨Implement a **layer of inherent or extrinsic provisions**, so that if a failure of the previous layer occurs (PIE, 1st level of the DiD), it would be detected and, if possible, managed by appropriate measures to keep the plant in safe conditions without soliciting the safety provisions which belong to the follow levels of the DiD
2.1.1. Implement provisions to detect the Postulated Initiating Events (abnormal conditions) :
2.1.1.1. Category 2 Initiating faults
2.1.1.1.1. LOOSP <1 hour
2.1.1.1.2. Inadvertent reduction of primary pump
2.1.1.1.3. Etc. List to be completed
2.1.1.2. Category 3 Initiating faults
2.1.1.2.1. LOOSP >1 hour
2.1.1.2.2. Coast down of all primary pumps not due to the LOSSP
2.1.1.2.3. Etc. List to be completed
2.1.1.3. Category 4 Initiating faults
2.1.1.3.1. Loss of redundant systems (e.g., vault cooling circuits; roof cooling circuits; etc.)
2.1.1.3.2. Primary pump faults (pump seizure and shaft failure)
2.1.1.3.3. Missiles
2.1.1.3.4. Earthquake
2.1.1.3.5. Etc. List to be completed
2.1.1.4. Design extension conditions (*Limiting events* in the EFR terminology)
2.1.1.4.1. Leakage of main and safety vessel
2.1.1.4.2. Etc. List to be completed
2.1.1.5. Design extension conditions (*Beyond design Plant States* in the EFR terminology
2.1.1.5.1. CDA without loss of roof leaktightness
2.1.1.5.2. Etc. List to be completed
2.1.1.6. PIE which affect the safety function “reactivity control”
2.1.1.6.1. inherent core reactivity changes (e.g., due to geometry changes)
2.1.1.6.2. reactivity changes induced by events external to the core (e.g., Control rod withdrawal)
2.1.1.7. PIE which affect the safety function “heat removal”
2.1.1.7.1. Degradation of the normal heat removal path within the primary circuit
2.1.1.7.1.1. loss of primary coolant flow
2.1.1.7.1.2. leakage of primary coolant
2.1.1.7.2. Sequences initiated by the degradation of the normal heat removal path downstream the primary circuit
2.1.1.7.2.1. Sequences initiated by the loss of secondary coolant flow
2.1.1.7.2.2. Sequences initiated by the leakage of secondary coolant
2.1.1.7.3. Loss heat sink
2.1.1.8. PIE which affect the safety function “confinement of radioactive materials”
2.1.1.8.1. barriers leakages (fuel, primary confinement, secondary confinement)
2.2. ⇨**Minimise the uncertainties** about the plant conditions under abnormal conditions
2.2.1. Implement a design that inherently simplify the abnormal sequences (intrinsically stable behaviour)
2.2.1.1. Foresee the possibility for the natural convection within the primary circuit
2.2.1.2. Foresee the possibility for the natural convection within the secondary side
2.2.2. Implement an adequate instrumentation (for automatic and manual intervention)
2.2.2.1. Set up an instrumentation able to identify without ambiguity the system’s configurations
2.3. ⇨Work out and set up a design with simple and efficient inherent behaviour under abnormal conditions (tolerant and forgiving design for the process and the safety architecture; avoid

inherent instabilities) *(For recall → must / can be realised at the prevention level; cf. 1.4)*
2.4. ⇨Work out and set up a design for the safety architecture (OPT / LOP / provisions) that will allow **simple procedures for the reactor operations inspection and maintenance under abnormal conditions** (i.e., minimize process' complexity and avoid inherent instability; systematic consideration of human factors and the human–machine interface for operation and shut down) *N.B. The recommendation is first considered at the 1.5 (1st level of the DiD) but it is detailed in this section 2.4*
2.4.1. Improve the quality of the available information (operation data; In Service Inspection - ISI)
2.4.1.1. Implement adequate control on systems behaviour and status
2.4.2. Simplify and automatize the procedures for the plant operation under abnormal conditions.
2.4.2.1. Improve the man-machine interface
2.4.2.2. Limit the interactions among systems that perform the same function
2.4.2.3. Implement safety system automatization
2.4.3. Simplify and automatize the procedures for the plant inspection, maintenance and repair
2.4.3.1. Improve the accessibility
2.4.3.2. Foresee equipments and robots
2.4.4. Minimize the needs for use of safety provision which belong to the protection level of the defence in depth
2.5. ⇨Defining the abnormal conditions to be assessed, **take into account possible aggravating situations** (coherently with the PIE category)
2.5.1. Minimize the potential consequences of aggravating situations
2.5.2. Take into account the unavailability for maintenance of corrective functions
2.5.2.1. Foresee, as needed/justified, internal redundancy for the control DHR/LOP
2.5.3. Take into account the PIE with cumulative failures
2.5.3.1. Take into account the Plant Conditions (PC) with the Loss of Offsite Power
2.5.3.2. Take into account the PC with internal and external hazards
2.6. ⇨Minimize the **personnel exposure under abnormal conditions** - ALARA Minimise the radioactive potential for injuries under abnormal conditions (operation and shut down) *(For recall → must / can be realised at the prevention level; cf. 1.16)*

TABLE A21 c (cont)
CLASS 3 : Detailed & Technology neutral recommendations applicable to a given safety function
(*) Recommendations applicable to the decay heat removal (DHR) safety function

3. ★3rd level : PROTECTION : Control of accident within the design basis and prevention of severe plant conditions
3.1. ⇨Implement a **layer of provisions, so that if a failure of the previous layer(s) occurs, it would be detected and managed by appropriate measures** to meet the objectives of the design basis accidents domain while preventing the severe plant conditions. Minimize the frequency of occurrence of severe plant conditions (core degradation)
3.1.1. Implement, through ad-hoc provisions, an adequate functional redundancy, for all the safety functions, to cope with the failure of the previous levels of the defence in depth.
3.1.1.1. Implement, through ad-hoc provisions, an adequate functional redundancy, for the reactivity control.
3.1.1.2. Implement, through ad-hoc provisions, an adequate functional redundancy, for the heat removal.
3.1.1.2.1. Set up adequate DHR/LOP to provide the functional redundancy in case of failure of the previous levels of the DiD and to meet the safety objectives of the design basis accident domain
3.1.1.3. Implement, through ad-hoc provisions, an adequate functional redundancy, for the confinement of radioactive materials.
3.1.2. Insure the availability and the reliability of the provisions which belong to the 3rd level of the Defence in depth
3.1.2.1. For each possible plant conditions, the corresponding DHR/LOP has to show the due reliability in order to prevent, with high confidence, the loss of the DHR function which would lead to severe plant conditions
3.1.3. Implement an adequate instrumentation to follow the status of the plant (for automatic and manual intervention; cf. 2.1 & 3.2.1)
3.2. ⇨Minimise the uncertainties about the plant conditions under accidental conditions (operation and shut down)
3.2.1. Implement an adequate instrumentation to follow the status of the plant (for automatic and manual intervention)
3.2.1.1. Set up an instrumentation able to identify without ambiguity the system's configurations
3.2.2. Implement a design that simplify the accidental sequences (cf. also 1.4)
3.2.2.1. Provide a core design which help keeping coolable geometry during accidental condition
3.2.2.2. Foresee the possibility for the natural convection within the primary circuit
3.2.2.3. Foresee the possibility for the natural convection within the secondary side
3.2.3. Protect the LOP provisions against the potential hazards generated by the accidental conditions
3.2.3.1. Protect the provisions which belong to the third and fourth level of the DiD against hazards which characterize the accidental conditions (temperature, pressure, etc.)
3.3. ⇨Work out and set up a **design for the process** (inherent response) **which allow for simple reactor management under abnormal, accidental and severe accident conditions and that that will inherently minimise the PIE consequences**. *N.B. The analysis concerning the inherent characteristics of the plant is addressed at the first level of the DiD (1.2 for the PIE frequency of occurrence & 1.4 for the inherent minimization of the PIE consequences). The objective and the scope of the recommendations at this third level of the DiD are to insure that the engineered provisions, and finally the LOPs, are correctly sized to answer the requested missions.* *Below the analysis is organized first, listing the conventional third category PIE and, in a second step, reasoning through the safety functions.* *N.B. Normally, the Cat 2 initiating faults do not challenge the third level of the DiD and are managed by the first and second level of the DiD. As well, the Design Extension Conditions belong to the 4th level of the DiD.*

3.3.1. Category 3 Initiating faults
3.3.1.1. LOOSP >1 hour
3.3.1.2. Coastdown of all primary pumps not due to the LOSSP
3.3.1.3. List to be completed
3.3.2. Category 4 Initiating faults
3.3.2.1. Loss of redundant systems (e.g., vault cooling circuits; roof cooling circuits; etc.)
3.3.2.2. Primary pump faults (pump seizure and shaft failure)
3.3.2.3. Missiles
3.3.2.4. Earthquake
3.3.2.5. List to be completed
3.3.3. Independent LOPs for the accidental sequences which follow PIEs which affect the safety function "reactivity control"
3.3.3.1. Inherent core reactivity changes (e.g., due to geometry changes)
3.3.3.2. Reactivity changes induced by events external to the core (e.g., Control rod withdrawal)
3.3.4. Independent LOPs for the accidental sequences which follow PIEs which affect the safety function "heat removal"
3.3.4.1. Sequences initiated by the loss of primary coolant flow
3.3.4.1.1. Set up adequate protection DHR/LOP to provide the functional redundancy in case of failure of the previous levels of the DiD and to meet the safety objectives of the design basis accident domain
3.3.4.2. Sequences initiated by the degradation of the normal heat removal path including the sequences initiated by loss heat sink
3.3.4.2.1. As for 3.3.4.1.1
3.3.5. Independent LOPs for the accidental sequences which follow PIEs which affect the safety function "confinement of radioactive materials"
3.3.5.1. Sequences initiated by barriers leakages (fuel, primary confinement, secondary confinement)
3.3.6. Minimize the possibilities for "short" sequences (i.e., the failure of a provision entails a major increase of consequences, without any possibility of restoring safe conditions at an intermediate stage)
3.3.6.1. For each possible plant conditions, the corresponding DHR/LOP has to maintain, as far as feasible, the possibility to cope single provisions failure, repairing and restoring the capability to achieve the mission
3.3.7. Ensure appropriate physical margins
3.3.7.1. Improve the system efficiency
3.3.7.2. Increase the common range (overlapped domain) covered by redundant LOP belonging to different levels of the DiD
3.3.8. Ensure appropriate grace period and the possibility of repair and restoring during accidental conditions
3.4. ⇨Work out and set up a design for the **safety architecture** (LOP / provisions) **which allow for simple, progressive, tolerant, forgiving and balanced reactor's behaviour/management under accidental conditions** *N.B. The analysis concerning the generic characteristics of the plant architecture is addressed at the first level of the DiD (cf. 1.101). The objective and the scope of the recommendations at this third level of the DiD are to insure that the engineered provisions, and finally the LOPs, are correctly sized to answer the requested missions.*
3.4.1. Independent LOPs for the accidental sequences which follow PIEs which affect the safety function "reactivity control"
3.4.1.1. Inherent core reactivity changes (e.g., due to geometry changes)
3.4.1.2. Reactivity changes induced by events external to the core (e.g., Control rod withdrawal; gas through the core; etc.)
3.4.2. Independent LOPs for the accidental sequences which follow PIEs which affect the safety function "heat removal"
3.4.2.1. Sequences initiated by the loss of primary coolant flow
3.4.2.1.1. Set up adequate protection DHR/LOP to provide the functional redundancy

in case of failure of the previous levels of the DiD and to meet the safety objectives of the design basis accident domain
3.4.2.2. Sequences initiated by a leakage of primary coolant
3.4.2.2.1. Set up adequate protection DHR/LOP to provide the functional redundancy in case of failure of the previous levels of the DiD and to meet the safety objectives of the design basis accident domain
3.4.2.3. Sequences initiated by the degradation of the normal heat removal path
3.4.2.3.1. Set up adequate protection DHR/LOP to provide the functional redundancy in case of failure of the previous levels of the DiD and to meet the safety objectives of the design basis accident domain
3.4.2.4. Sequences initiated by loss heat sink
3.4.2.4.1. Set up adequate protection DHR/LOP to provide the functional redundancy in case of failure of the previous levels of the DiD and to meet the safety objectives of the design basis accident domain
3.4.3. Independent LOPs for the accidental sequences which follow PIEs which affect the safety function "confinement of radioactive materials"
3.4.3.1. Sequences initiated by barriers leakages (fuel, primary confinement, secondary confinement)
3.4.4. Minimize the possibilities for "short" sequences (i.e., the failure of a provision entails a major increase of consequences, without any possibility of restoring safe conditions at an intermediate stage)
3.4.4.1. For each possible plant conditions, the corresponding DHR/LOP has to maintain, as far as feasible, the possibility to cope with single provisions failure, repairing and restoring the capability to achieve the mission
3.4.5. Ensure appropriate physical margins
3.4.5.1. Increase the common range (overlapped domain) covered by redundant DHR/LOP belonging to different levels of the DiD
3.4.6. Ensure appropriate grace period and the possibility of repair and restoring during accidental conditions
3.4.6.1. Increase the process internal inertia; this inertia is considered as an integral part of the DHR/LOPs
3.4.6.2. Provide the passive access to adequate external inertia
3.4.7. Ensure that no initiator or sequence contributes in an excessive and unbalanced manner to the global frequency of the damaged plant states
3.5. ⇨Work out and set up a design for the **safety architecture** (LOP / provisions) **which allow for simple accidental intervention procedures and repair under accidental conditions** (consideration of human factor) *N.B. The recommendation is first considered at the 1.6 (1st level of the DiD) but it is detailed in this section 3.5*
3.5.1. Implement a design that inherently simplify the accidental sequences
3.5.1.1. Provide a core design which help keeping coolable geometry during accidental condition
3.5.1.2. Foresee the possibility for the natural convection within the primary circuit
3.5.1.3. Foresee the possibility for the natural convection within the secondary side
3.5.2. Ensure an adequate information (accidental situation)
3.5.2.1. Improve the quality of the available information about the plant status under accidental conditions (transient data; In Service Inspection - ISI). Set up an instrumentation able to identify without ambiguity the system's configurations
3.5.3. Simplify and automatize the procedures for the accident management
3.5.3.1. Improve the man-machine interface
3.5.3.2. Limit the interactions among systems that perform the same function
3.5.3.3. Implement safety system automatisation
3.5.4. Simplify and automatize the procedures for the plant inspection, and repair
3.5.4.1. Improve the accessibility
3.5.4.2. Foresee equipments and robots
3.6. ⇨Work out and set up a safety architecture which minimize the **potential for Common Modes**

(mutual aggressions, internal or external hazards) *N.B. The recommendation is considered and detailed at the 1.11 (1st level of the DiD) for the whole safety architecture; it is detailed in this section 3.6 focusing on the recommendation for the LOP design, especially concerning the requested reliability*
3.6.1. In designing the LOPs content and layout, provide provisions' separation and diversification in order to guarantee the requested reliability
3.6.1.1. Separate and diversify the protection DHR/LOP
3.6.1.2. Avoid any physical interaction between the systems in case of failure
3.7. ⇨In defining the accidental sequence to be assessed, take into account **possible aggravating situations** (coherently with the PIE category))
3.7.1. Take into account the possibility for aggravating failure
3.7.2. Take into account the unavailability for maintenance of corrective functions
3.7.2.1. Foresee, as needed/justified, internal redundancy for the protection DHR/LOP
3.7.3. Take into account the accidental sequences with cumulative provisions failures (complex sequences)
3.7.3.1. Provide provisions to address possible cumulative failures in order to meet the objectives of the design basis accidents domain.
3.8. ⇨Number of **confinement barriers maintained**
3.8.1. The design of engineered safety features should deterministically provide for continued integrity at least of one barrier (containing the radioactive material) following any design basis accident
3.9. ⇨**Minimize the personnel exposure** (including on site release) under accidental conditions – ALARA ***(For recall → must / can be realised at the prevention level; cf. 1.16)***
3.10. ⇨**Minimize the risk for the environment contamination** (off site release) under abnormal and accidental conditions (without core degradation) – ALARA
3.10.1. Conceive the plant looking for the guarantee that plants would be so safe that there would be no technical justification for an emergency plan involving evacuation of the nearby population
3.10.1.1.Strengthen the last barrier

TABLE A21 c (cont)
CLASS 3 : Detailed & Technology neutral recommendations applicable to a given safety function
(*) Recommendations applicable to the decay heat removal (DHR) safety function

4. ★ 4th level : SEVERE ACCIDENT MANAGEMENT- accident management including the confinement protection ***N.B*** *The safety approach, coherently with the fourth level of the defence in depth, is completed by the consideration of plant conditions with more or less important core degradation (if need be, until the whole core melting) and the implementation of provisions which aim at making the risk acceptable. This is why the designer has to select and take into account the severe plant conditions configurations to be considered within the basis for the design of the safety architecture (i.e., the set of conditions considered for the design of the single provisions/LOP). Analogously the designer should prevent & practically eliminate the initiators, sequences or situations that can lead to unacceptable consequences and early releases. Finally he should reject the risk for the cliff edge effect. In conclusion* :
• *according to the fourth level of the defence in depth, some representative severe plant conditions have to be considered, in particular to demonstrate the effectiveness of the safety architecture and to prove the robustness of the confinement*
• *a limited number of initiators, sequences or situations, for which it is not realistic to set up provisions for mitigation, or to assure, with a sufficient degree of confidence, that their consequences would be mastered, will be eliminated by design or "practically eliminated" implementing specific provisions which guarantee their rejection within the Residual Risk (RR)*
4.1. ⇨Implement a layer of provisions/LOP, so that if a failure of the previous layer(s) occurs, the severe plant condition will be detected, managed and mitigated by appropriate measures and its consequences duly mitigated
4.1.1. Implement a design that inherently simplify the severe accident sequences (cf. 1.4)
4.1.1.1. In case of core degradation provide a core relocation strategy which will help keeping coolable geometry during accidental condition, e.g., adequately spreading the core debris in case of significant core melting
4.1.1.2. Foresee the possibility for the natural convection within the primary circuit
4.1.1.3. Foresee the possibility for the natural convection within the secondary side
4.1.2. To cope with the failure of the previous levels of the defence in depth, ensure the safety function accomplishment under severe accident conditions implementing, through ad-hoc provisions, an adequate functional redundancy, for all the safety functions.
4.1.2.1. Implement, through ad-hoc provisions, an adequate functional redundancy, for the reactivity control (safety objective: Keep the degraded core subcritical on the long term) .
4.1.2.2. Implement, through ad-hoc provisions, an adequate functional redundancy, for the heat removal; i.e., set up adequate mitigation DHR/LOP to provide the functional redundancy in case of failure of the previous levels of the DiD and to meet the safety objectives (core coolability on the long term); Foresee the DHR with severe accident configurations
4.1.2.2.1. the possible degraded primary coolant inventory
4.1.2.2.1.1. Set up adequate (passive ?) ultimate DHR/LOP (including the heat sink) able to guarantee the coolability on the long term
4.1.2.2.2. the degraded core within the primary vessel
4.1.2.2.2.1. As for 4.1.2.2.1
4.1.2.2.3. fraction (if any) of the degraded core within the containment (core catcher)
4.1.2.2.3.1. As for 4.1.2.2.1
4.1.2.3. Implement, through ad-hoc provisions, an adequate functional redundancy, for the confinement of radioactive materials (safety objective: allowable releases).
4.2. **Minimise the uncertainties about the plant conditions under accidental conditions** (operation and shut down)
4.2.1. Implement an adequate instrumentation to follow the status of the plant (for automatic and manual intervention)
4.2.1.1. Set up an instrumentation able to identify without ambiguity the system's

configurations
4.2.2. Implement a design that simplify the accidental sequences (cf.1.4)
4.2.2.1. Provide a core design which help keeping coolable geometry during accidental condition
4.2.2.2. Foresee the possibility for the natural convection within the primary circuit
4.2.2.3. Foresee the possibility for the natural convection within the secondary side
4.2.3. Allow the implementation of procedures for the plant inspection following severe accidental conditions
4.2.3.1. Improve the accessibility
4.2.3.2. Foresee equipments and robots
4.2.4. Protect the LOP provisions against the potential hazards generated by the severe plant conditions (pressure, temperature, etc.)
4.2.4.1. Protect the provisions which belong to the fourth level of the DiD against the following hazards: presence of the degraded core, possible deflagrations, temperature, pressure, etc
4.3. ⇨Work out and set up a design for the safety architecture (LOP / provisions) which allow **for simple management of the severe plant conditions progress and the mitigation of their consequences** *N.B. The analysis concerning the inherent characteristics of the plant is addressed at the first level of the DiD (1.2 for the PIE frequency of occurrence & 1.4 for the inherent minimization of the PIE consequences). The objective and the scope of the recommendations at this fourth level of the DiD are to insure that the engineered provisions, and finally the LOPs, are correctly sized to answer the requested missions.* *Below the analysis is organized first, listing the conventional Design extension Conditions and, in a second step, reasoning through the safety functions*.
4.3.1. Design extension conditions (*Limiting events* in the EFR terminology)
4.3.1.1. Leakage of main and safety vessel
4.3.1.2. List to be completed
4.3.2. Design extension conditions (*Beyond design Plant States* in the EFR terminology)
4.3.2.1. CDA without loss of roof leaktightness
4.3.2.2. List to be completed
4.3.3. Independent LOPs for Design Extension Conditions which require the safety function "reactivity control"
4.3.4. Independent LOPs for Design Extension Conditions which require the safety function "heat removal"
4.3.5. Independent LOPs for Design extension conditions which require the safety function "confinement of radioactive materials"
4.3.6. Ensure appropriate physical margins
4.3.6.1. Improve the system efficiency
4.3.6.2. Increase the common range (overlapped domain) covered by redundant LOP belonging to different levels of the DiD
4.3.7. Simplify and automatize the procedures for the severe accident management
4.3.7.1. Improve the man-machine interface
4.3.7.2. Limit the interactions among systems that perform the same function
4.3.7.2.1. Independent LOPs for the management and the mitigation of severe plant conditions to :
4.3.7.2.1.1. keep the degraded core coolable on the long term;
4.3.7.2.1.2. keep the degraded core subcritical on the long term
4.3.7.3. Implement safety system automatization
4.3.8. Improve the grace delay
4.3.8.1. Implement an ultimate passive DHR for the corium cooling
4.4. ⇨Avoid major release of radioactive materials into the environment : A major release of radioactivity should be prevented for all practical purposes, so that innovative systems would not need relocation or evacuation measures outside the plant site, apart from those generic emergency measures developed for any industrial facility used for similar purpose
4.4.1. Safety provisions should be able to control severe accident scenarios and mitigate their

consequences, so as to prevent containment failure. Control and mitigation should address all threats (internal and external). Thus innovative designs should show that:
4.4.1.1. The likelihood of a large release is so small that off-site emergency measures, while they may reduce the consequences thereof, do not lead to a significant reduction in risk; or
4.4.1.2. A large release could be excluded by design for all practical purposes, e.g., through use of inherent safety characteristics.
4.5. ⇨Minimize the personnel exposure (on site accidental release) under accidental conditions- ALARA *(For recall → must / can be realised at the prevention level; cf. 1.16)*
4.6. ⇨Minimise the offsite accidental release during the severe plant conditions
4.6.1. Conceive the containment provisions in order to keep the containment capabilities compatible with the objective to guarantee that:
4.6.1.1. the likelihood of a large release is so small that off-site emergency measures, while they may reduce the consequences thereof, do not lead to a significant reduction in risk; or
4.6.1.2. a large release is excluded by design for all practical purposes
4.6.2. Conceive in order to need only very limited protective measures in area and in time
4.6.2.1. Qualify the last barrier to the selected severe plant conditions
5. ★ 5th level : CONSEQUENCES MITIGATION - Mitigation of radiological consequences of significant releases of radioactive materials
5.1. ⇨Delay the offsite release
5.2. ⇨Minimise the offsite radioactive release
5.3. ⇨Control the offsite release (release point and monitoring)
5.4. ⇨Provide relevant and reliable information for off-site management

Appendix 3 – Phenomena Identification and Ranking Tables - Details

A3.1 - Introduction

PIRT is a practical and flexible technique allowing a systematic and graded approach to technical issues of varying complexity and importance. The technique can also incorporate uncertainties in the assessment and characterize them explicitly. One of the distinct advantages of the technique is to identify the knowledge level in the phenomena, which helps identify the gaps in knowledge areas requiring additional research and data collection.

The PIRT process has been previously used in new reactor designs. For example, a small break loss-of-coolant accident phenomena identification and ranking table project was successfully used in the International Reactor Innovative and Secure (IRIS) reactor. The IRIS plant conceptual design was completed in 2001 and the preliminary design is currently underway. By design, large primary penetrations of the reactor vessel or large loop piping were eliminated to prevent large break loss-of-coolant accidents. To test that the new reactor concept fulfils the promise of increased safety for small break loss-of-coolant accident, the PIRT technique was used. The primary objective of that PIRT project was to identify the relative importance of phenomena in response to small break loss-of-coolant accident in the IRIS reactor. The PIRT panel concluded that continued experimental data and analytical tool development is required in five different key areas [A3.1]. The identification of system vulnerabilities and the phenomena requiring additional R&D were identified due to expert elicitation that was possible in the PIRT process. Perhaps it is in recognition of the capability of PIRT technique in the assessment of new reactor concepts that USNRC has issued a six-volume treatise on the assessment of next generation of nuclear reactor concepts [A3.2] using PIRT. The PIRT process has also been successfully used in the assessment of other new reactor concepts [A3.3].

For complex systems, the PIRT technique is a versatile tool to identify areas where technology development is needed, where major challenges exist, and where uncertainties are large. The PIRT technique can consider importance of physical phenomena, conceptual model adequacy, verification and validation adequacy, and experimental adequacy. The application of PIRT technique would normally require some detailed knowledge of the system and components and is therefore extensively used in existing designs. PIRT technique has, however, been successfully used during pre-conceptual design phase, and iteratively thereafter, to identify, categorize, "screen", and characterize phenomena and issues that are potentially important to public risk and safety margins. The technique relies heavily on expert elicitation and it can be focused on general issues or on specific design questions, phenomenology, and temporal frames as needed.

A3.2 - Description of PIRT

The PIRT methodology brings into focus the phenomena that dominate an issue, while identifying all plausible effects to demonstrate completeness. The usefulness of PIRT technique lies in the ability to identify and rank, relatively quickly and cost effectively, all of the phenomena in a complex reactor system. The task that PIRT technique performs is recognizing the relative importance and the relative state of knowledge for the phenomena, with associated rationales. The benefit to using PIRT process is in the ability to focus the attention and resources efficiently to improve the state of knowledge of phenomena deemed poor, as budgets permit, one-at-a-time, starting from the most important to least important phenomena, when important phenomena are identified and their state of knowledge is assessed and ranked. In the following discussion, the PIRT process will be outlined and the essential steps required for a successful PIRT will be described.

A3.2.1 The Objective and Usefulness of the Task

The underlying philosophy is that in complex and coupled physical systems some phenomena are more important than others during an event sequence affecting the safety of a reactor system. The term phenomenon is defined as any empirically observable physical behaviour of a reactor system or component. The phenomenon can be a condition of a particular reactor/system/component, a physical or engineering approximation, a reactor parameter, or anything else that might influence the primary

evaluation criteria, the figure-of-merit. The final outcome of the PIRT process is a ranked list of phenomena and associated uncertainty in the knowledge level, which are germane to a particular subject, i.e., a very specific FOM.

The FOM is the criterion against which the relative importance of each phenomenon or processes in the plant behaviour is judged. The criterion selected can be a variable or a parameter that is affected by the performance of a reactor system or component. For example, the FOM for a large-break-loss-of-coolant accident PIRT could be the peak cladding temperature. All processes or phenomena affecting the peak cladding temperature can be assessed and ranked for their importance and relevance to have a direct impact on fuel cladding temperature. Similarly, the hydrogen generation, containment pressure, heat flux on the pressure vessel, etc. are some examples of possible FOM. In some instances the FOM are selected from primary regulatory limits [A3.4] set by regulatory agencies.

It is extremely important that all PIRT Panel members come to a common and clear understanding of the FOM and be familiar with how it will be used in the ranking. The characteristics of a well-defined FOM are that it is: (1) directly related to the issue(s) being addressed; (2) directly related to the phenomena expected to occur during the scenario; (3) easily comprehended, (4) explicit; (5) measurable, and (6) continuous (i.e., not a threshold effect).

Every component in the reactor concept or design needs to be examined in each reactor system. The components are assessed to identify the physical phenomena, physical processes and parameters that impact the FOM quantitatively. The phenomena are identified and ranked using Table 1 given in Section 2.2.2 for their importance to the FOM. The ranking identifies the most important phenomena for the FOM.

The second part of the PIRT process is to identify the level of knowledge available for the phenomena. An expert judgment is made based on thorough assessment of available analysis, literature and data. The adequacy of the knowledge and the uncertainty in the knowledge base is brought forth and listed using the Table 2 given in Section 2.2.2. The PIRT results would then identify the adequacy and applicability of existing experiments and analytic tools, and define the requirements for related experiments and analytic tools.

A3.2.2 The Individual Steps in the Activity

First and foremost task, following the decision to conduct a PIRT, is the selection of an expert panel. Typically an odd number of experts are assembled to avoid a tie in the expert ranking, if consensus was not forthcoming during deliberations. A group small enough to achieve consensus or agreement on judgments during deliberations, yet adequate to cover the required breadth of expertise, is required. The importance ranking assigned to phenomena is based on expert elicitation and consensus. The best PIRT accomplishments are made when breadth of expertise among panel covers relevant experiments, analytical experience, and plant operations.

The PIRT process is expected to identify, recognize, and qualify the relative importance of all relevant phenomena to the FOM with the associated rationales. It follows a nine-step process. These steps are shown in Figure 3, Section 2.2.3. The steps are described in the subsequent sections. It is imperative that an event scenario is selected for the assessment. The description of the reactor and the key systems and components that potentially respond to the selected scenario is then described followed by the scenario description.

Documentation of PIRT assessment is an essential final step. The qualifications, experience, and rationale for the selection of panel members are documented. The event scenario, the description of the reactor, key systems and components, and scenario description are also methodically documented. Finally, the PIRT process results and a summary are documented in a comprehensive report.

A3.2.2.1 - Define the Issue

The issues that are driving the need for a PIRT are defined in this step. The panel identifies the purpose and answers the question, "Why are we doing this PIRT and how will it be used?" For

example, the issue for the Risk and Safety Working Group (RSWG) is the comparison of safety margins of alternative Gen IV reactor designs and concepts against Gen IV safety goals with an expectation to identify areas for improvement and meet the goals including the application of ALARAP principle. The definition of the issue may evolve as a hierarchy starting with design or safety goals set by Gen IV programs (justified by federal regulations or other specific motivations) and descending to a consideration of key physical processes.

A3.2.2.2 - Define the specific objectives

The PIRT objectives are usually specified by the sponsoring agency. A clear statement of PIRT objectives is important because it defines the focus, content, and intended applications of the PIRT product. It is important to formulate and define in detail the specific problem that requires a resolution. While defining the objectives of PIRT, an assessment of available resources and the level of effort to be expended in the PIRT technique must be made. The PIRT effort can be tailored to the level of resource availability. The level of PIRT detail must also be assessed against the details required for the resolution of the problem. If the scope and the problem defined do not warrant highly detailed PIRT, a level of detail appropriate for the problem must be undertaken. The ability to have a flexible level of detail, depending on the resource availability and the problem requirement, is one of the strong desirable features of PIRT technique.

The PIRT objectives should include a description of the final products to be prepared with a view to answer the question, "What are we going to do about the issue?" Typically there are one primary and three adjunct objectives of PIRT [A3.4]. The primary objective has already been stated earlier, i.e., identifying the relative importance of systems, components, processes and phenomena in response to plant behaviour during a sequence of events. The adjunct objectives are to [A3.4]:

- Assess whether experimental data from integral and separate effects tests fully covers the range of plant physical behaviour
- Assess the capability and qualification of computer codes for modeling plant physical behaviour, and
- Identify, evaluate, and treat various contributors to uncertainties based on the appropriateness to plant physical behaviour to assess the overall uncertainty.

In terms of Gen IV reactor designs the objectives could be phrased as, "Do the Gen IV reactor systems demonstrate adequate knowledge level at "fully known with small uncertainties[49]" for phenomena ranked as "high" or "medium[50]"?". Depending on the availability of resources, level of details required to answer the objective question can be pursued, keeping in mind that PIRT development is an iterative process with significant feedback between various elements. Experience appears to indicate that highly design and scenario dependent PIRTs provide the most phenomenological information [A3.4]. For Gen IV systems, as design matures, more extensive PIRTs can be performed to obtain the desirable phenomenological information, whereas a preliminary PIRTs could provide a quick review of compliance to key goals.

A3.2.2.3 - Obtain the Necessary Database Information (Background)

The collection of background information is a vital step to the success of the PIRT process. The background information includes detailed system design description, accident sequence description and event table, and plant and experimental calculations. The contents of a state-of-the-art information database should also capture the relevant experimental and analytic knowledge relative to the physical processes and hardware for which the PIRT is being developed. Each panel member should review and become familiar with the information database and have a state-of-the-art understanding of factors affecting the defined problem to be tackled by the PIRT. To help the panel to reach a common understanding of the relevant data and factors, they should collectively review the collected state-of-the-art information.

[49] See Table 2 given in Section 2.2.2 for details
[50] See Table 1 given in Section 2.2.2 for details

The necessary information should include, but not be limited to, sensitivity studies, experimental data, analysis of experimental data, code simulations of experiments, and code simulations of plant behaviour of interest. Quick recap of relevant information can be provided through presentations made by subject matter specialists who may not be part of the PIRT panel. If simulations of cases are required, and if the problem addressed by the PIRT requires such inputs, they can be assigned to external analysts to provide the information required. All of the information reviewed and provided to the panel is documented and archived for subsequent review, if warranted.

The collective judgments reached by the panel require appropriate justification, and this justification is predominantly drawn from the collected state-of-the-art information. Specific information about plant design, response of the design to accident conditions, applicable experimental data and data reports, analytical tools and relevant analysis must be readily available to ensure the expert elicitation process progresses effectively and efficiently.

A3.2.2.4 - Hardware and Scenario Definition

In order to achieve the PIRT objectives defined in Step A3.2.2.1, a specific reactor concept or design and an event sequence must be selected along with plant hardware components, equipment and scenario for which the PIRT is conducted. Common sense must be applied to determine how far down the component hierarchy to proceed. It is necessary to establish the plant envelope where the PIRT will be applied. For example, a PIRT on large-break-loss-of-coolant-accidents can generally ignore containment if the study is confined to phenomena occurring within the pressure vessel boundary and the necessary boundary conditions can be applied to cover the absence of containment in the analysis. While for most of the plant designs, there are a number of active reactor systems common to all scenarios, there are also several scenario- and reactor-dependent systems or subsystems. Usually the details of the scenario-dependent systems define the plant envelope essential for the PIRT. For example, for a large-break LOCA scenario in a CANDU reactor, the primary heat transport pumps are included in the plant envelope, whereas in a station blackout scenario the primary heat transport pumps become redundant without power and therefore the PIRT process can exclude the pumps from the plant envelope. A good understanding and knowledge of all of the common and scenario-dependent systems for the various reactor designs are required to form an informed judgment of where to place the plant envelope during PIRT. An appropriate level of panel discussion is required, and a consensual agreement must be reached by the panel, to scope the plant envelope required to achieve the objectives of the PIRT without jeopardizing the validity of the PIRT results, while avoiding unnecessary level of details that may deter focus from key issues.

The relative importance of phenomena is dependent on scenario. Usually, but not always, the scenario is divided into phases. This is done because the importance of a phenomenon often varies during the course of a scenario. In addition, some system components may not be activated throughout the scenario. Experience obtained from previous PIRT efforts indicates that any consideration of multiple hardware configurations or scenarios impedes PIRT development. If assessments of multiple hardware configurations or scenarios are required, a follow-up PIRT ("delta" PIRT) to the alternative hardware configurations and scenarios can be assessed after the baseline PIRT is completed for a specified hardware and scenario.

The hardware and components should be partitioned as much as possible to help organize the ranking process. The partitioned components is equivalent to the 'provisions' described in Section 2.3 with Objective Provision Tree. A system level partitioning of hardware has the advantage to remove the system from the PIRT assessment if a particular system has no functional influence on the FOM. Typically the component hierarchy is developed from system, sub-system, and components. For example, in the PIRT assessing the water ingress scenario of VHTR system [A3.5], the system level partition included Reactor Vessel, Reactor Coolant Loop, Reactor Cavity Cooling System, and Shutdown Cooling Systems. The Reactor Vessel system consisted components such as Inlet Plenum, Riser, Top Plenum and Components, Core & Reflectors (Includes Bypass), Outlet Plenum and Components, and Lower Head. These components can further be subdivided to elementary level components, if required, depending on the level of details to be included in the PIRT.

A3.2.2.5 - Establish the Figure-of-Merit

The FOM is the primary evaluation criterion used to judge the relative importance of each phenomenon. The FOM must be identified before proceeding with the ranking portion of the PIRT effort. For example, the most important variable (i.e., the figure-of-merit) to safety of a reactor design during severe core damage accidents could be the fission product release that contributes to public dose. It is extremely important that all PIRT panel members come to a common and clear understanding of the chosen FOM and how it will be used in the ranking of phenomena. A well-defined FOM must be:

(1) Directly related to the issue(s) being addressed;
(2) Directly related to the phenomena expected to occur during the scenario;
(3) Easily comprehended,
(4) Explicit;
(5) Measurable, and
(6) Continuous (i.e., does not have a threshold effect).

For design basis accident scenarios, the FOM is generally derived from regulatory requirements. For beyond design basis accident scenarios, the FOM may be derived from regulatory or design goals, or from specific aspects of the accident progression.

A3.2.2.6 - Identify Phenomena

The phenomena are identified on the basis of collective expertise of the team members. The panel members rely on the background information described in Section A3.2.2.3. All plausible phenomena i.e., PIRT elements are identified in this step. A primary objective of this step is completeness. In addition to preparing the list of phenomena, precise definitions of each phenomenon should be developed and made available to the PIRT panel to ensure that panel members have a common understanding of each phenomenon. Within the context of a PIRT, the term "phenomenon" may encompass phenomena, processes, conditions, characteristics, and state variables.

In each PIRT effort, there is a phenomenological hierarchy beginning at the system level and proceeding in turn through the component level, local level, and so on. Each PIRT panel must determine the appropriate phenomenological levels to include in its list of identified phenomena. Insights into the levels to be included can often be derived by considering the data needs for analytic methods and the level at which data from experiments are collected. Usually, there is no need to proceed further down the phenomenological hierarchy than the level at which:

(a) Physical processes are modelled with analytic methods or

(b) Data, either direct or indirect, are acquired.

A3.2.2.7 - Importance Ranking

This is the most delicate step in the PIRT process. All of the previous steps prepare the panel members for this step. The quality of ranking is dependent upon the expertise of individual panel members, collective expertise of all panel members, the quality of the database informing the panel members, a correct and common understanding of the figure-of-merit, and the availability of time to discuss individual ranking and reach common consensus.

The PIRT process proceeds by ranking each phenomenon using some scoring criteria in order to help determine what is most important. A sample most often used ranking scale is given in Table 1 in Section 2.2.2. Each panel member records their ranking, the rationale for the ranking, and the supporting information to explain the ranking in Table A3.1. The individual phenomena rankings are then assembled during panel deliberations and an attempt is made to reach a common consensus on each of the phenomenon ranks if individual ranks differ among panel members. If a consensual rank is reached after deliberation, the importance-rank and the rationale are recorded for each phenomenon. If consensus is hard to reach, members vote on the phenomena, based on a prearranged voting rule, where the majority rank is recorded as the final rank while individual ranks and their rationale are recorded to retain the minority opinion in perspective.

Importance is ranked relative to the FOM adopted in Section A3.2.2.5. Several ranking scales have been used in the past. However, consistent application of the scale is equally important to the specifics of the scale. A word-based scale, e.g., High, Medium, Low or Inactive /Insignificant importance, has proven useful. Numerical scales, e.g., 1-5, have also been used. Outcomes are closely associated with the ranking process and the members of the PIRT panel should understand the outcomes as they embark on the ranking effort. For example, a phenomenon assigned an importance-rank of High must be simulated with a high degree of accuracy in both experiments and analysis tools while a phenomenon with an importance rank of Low requires significantly less accuracy in both experimental and analytic simulations.

Generally a word-based scale requires common consensus for ranking and therefore it is better suited for panels where good collaborative deliberations are possible. The numerical scales work well when common consensus is hard to achieve due to panel dynamics and voting is required for ranking. The numerical average of panel ranks is then used as the final rank.

A3.2.2.8 - Knowledge Assessment

The panel must distinguish between phenomena importance and knowledge assessments. A sample knowledge assessment ranking is scale is provided in Table 2 in Section 2.2.2. Detailed assessment rationales for the level of knowledge regarding each phenomenon and the supporting information yield the greatest long-term value.

As with importance ranking, several scales have been used in the past. Again, a consistent application of the scale is of equal importance as the specifics of the scale. A numerical scale, e.g., 1-4, which includes in its definitions a statement on uncertainty, has been used. A word-based scale, e.g., Known, Partially Known or Unknown, has also been used. By explicitly addressing uncertainty due to a lack of knowledge, an observed defect of earlier PIRT efforts has been addressed, namely, the tendency of PIRT panel members to assign high importance to a phenomenon for which panel members concluded that there was significantly less than full knowledge and understanding. A consistent outcome of PIRT efforts has been that phenomena found to be highly important relative to the FOM, but for which the knowledge level is insufficient, are carefully examined to determine if additional experiments or analytic efforts are warranted. The panel may also assess the importance of the effort needed to improve the knowledge base since these members would be competent to prioritise the R&D required.

Figure of Merit (FOM): Temperature Response of the Fuel Sheath		
# Sub-Scenario	Description of the Sub-Scenario	**Time Interval**
1	Early Blowdown Cooling	Time = 0 to ECC Injection
2	Late Blowdown Cooling/ECI/Refill	Time = ECI injection to Refill
3	Long Term Cooling	Time = Refill to Core Cooling

System	**Rank By Time Phase**			***Component***	**Rank By Time Phase**			**Process/ Phenomenon**	**Rank By Time Phase**		
	1	**2**	**3**		**1**	**2**	**3**		**1**	**2**	**3**
Emergency Cooling Injection (ECI)	M	**H**	M	**Injection Water Storage Tank**	L	**H**	L				
				Volume				Pressure	L	**H**	L
								Level	L	**H**	L
				Flow path				Flow – Pressure driven	L	**H**	L
				ECI Injection Valve	L	**H**	L				
				Flow path				Flow – Pressure driven	L	**H**	L
								Pressure drop (1-phase, 2-phase)	L	**H**	L
				ECI Piping	L	**H**	L				
				Flow path				Flow – Pressure driven	I	**H**	L
								Pressure drop (1-phase, 2-phase)	I	**H**	L
				Large Header Interconnect	M	**H**	M				
				Volume				Flashing	M	L	L
								Refill	L	**H**	L
				Flow path				Flow – Pressure driven	M	**H**	M
								Pressure drop (1-phase, 2-phase)	M	**H**	M
				Rupture Disc	I	**H**	L				
				Flow path				Change in path/state (open/close)	I	**H**	I
								Flow – pressure driven	I	**H**	L
								Pressure drop (1-phase, 2-phase)	I	**H**	L

Table A3.1 Format of Detailed PIRT Input Sheet [A3.6]

A3.2.2.9 - Documentation

A detailed and complete documentation is a key to successful implementation of a PIRT effort to make it as valuable as possible. The primary objective of this step is to provide sufficient coverage and depth that a knowledgeable reader can understand what was done (process) and the outcomes (results). The essential results to be documented are the phenomena considered and their associated definitions, the importance of each phenomena and associated rationale for the judgment of importance, the level of knowledge or uncertainty regarding each phenomenon and associated rationale, and the results and rationales for any assessments of extended applicability for the baseline PIRT. Other information may be included as determined by the panel or requested by the Sponsor[51].

A3.2.3. - Conclusions on the PIRT

The PIRT process has evolved from its initial development and application to code uncertainty assessments to its current description as a generalized process that can be used to support several important decision-making processes. PIRT is a forensic-style process based on the opinions of a panel of experts. The process involves selecting a nuclear plant, selecting an accident scenario, and then identifying all plausible phenomena impacting the outcome of the accident. Each phenomenon is then ranked in order of relative importance and its state of uncertainty in the knowledge. The PIRT is particularly helpful in defining the course of accident sequences, and defining safety system success criteria. The PIRT is essential in helping to identify areas in which additional research may be helpful to reduce uncertainties.

References for Appendix 3:

[A3.1.] *Larson, T.K., Moody, F.J., Wilson, G.E., Brown, W.L., Frepoli, C., Hartz, J., Woods, B.G., and Oriani; L. "IRIS Small Break LOCA Phenomena Identification and Ranking Table (PIRT)," Nuclear Engineering and Design, Vol. 237, No6, pp. 618-626, 2007.*

[A3.2] *S.J. Ball and S.E. Fisher, "Next Generation Nuclear Plant Phenomena Identification and Ranking Tables (PIRTs) (NUREG/CR-6944) Volumes 1 to 6, USNRC, March 2008.*

[A3.3] *N. K. Popov, H. Sills, A. Abdul-Razzak, "Development of Phenomena Identification and Ranking Tables for the Advanced CANDU Reactor," Nuclear Technology, Vol. 158, No. 1, pp. 2-17, April 2007.*

[A3.4] *Wilson, G.E. and Boyack, B.E., "The role of the PIRT process in experiments, code development and code applications associated with reactor safety analysis," Nuclear Engineering and Design, Vol. 186, pp. 23-37, 1998.*

[A3.5] *R.B. Vilim, W.D. Pointer, T.Y.C. Wei, "Prioritization of VHTR System Modeling Needs Based on Phenomena Identification, Ranking and Sensitivity Studies," Nuclear Engineering Division, Argonne National Laboratory, ANL-GenIV-071, April 2006.*

[A3.6] *D. Magallon, et al., "European Expert Network for the Reduction of Uncertainties in Severe Accident Safety Issues (EURSAFE)," Nuclear Engineering and Design, Vol. 235, pp. 309-346, 2005.*

[51] The Sponsor is the person requesting and funding the PIRT to resolve a specific problem

Appendix 4 – Objective Provision Trees for assessment of adequacy of Defence-in Depth (DiD)

The OPT construction process begins with some crucial steps performed by the design/ research organization.

A4.1.1 - Team setting and defining the analyses scope

First, the objectives of the exercise must be clearly stated, documented and understood by all the staff which will develop the OPTs. Test application of this methodology [A4.3] showed that it is very important that all of the staff involved in the exercise have the same understanding of the key elements, terminology used and scope of the assessment

After initial training, it is recommended to start the exercise by development of an OPT for a given level of defence in depth and given objective and safety function by each of the working teams. Based on the comparison and mutual verification of the performed work a common understanding of the methodology shall be developed which is needed for its further consistent application.

A4.1.2 - Data gathering

Second step shall be the collection of design, research and safety assessment documentation which may be needed to develop the OPTs. At this particular stage consideration shall be given to the available design/ safety analyses associated with different safety issues and phenomena. It should be made sure that the documentation on all phenomena identified by previously developed Phenomena Identification and Ranking Table (PIRT) exercise are available to the OPT team, too. It is evident, however that in the process of OPTs development there might be some need for extra information.

A4.1.3 - Development of the OPTs

The construction/ development of the OPTs shall start with consideration of the three fundamental safety functions: reactivity control, fuel heat removal and confinement of radioactive materials and shall cover at least levels 1 to 4 of the DiD.

For all given objectives (expressed for example in terms of acceptable achievement of safety functions : the mission's success criteria), at each level of defence, the set of possible challenges[52] has to be identified (e.g., for the safety function "*reactivity control*", the challenge could be "*insertion of unallowable positive reactivity*"), and all root mechanisms[53] leading to the challenges have to be specified (e.g., for the example above, the "*control rod withdrawal*").

Eventually, to the extent possible, the comprehensive list of safety provisions, which contribute to prevent that the mechanism takes place, is elaborated and illustrated in the form of "objective provisions trees"[54].

At the pre-conceptual and conceptual design stages concurrent alternatives may exist and it is up to the designers to select the best one keeping in mind the need to have exhaustive, tolerant, forgiving, balanced and progressive DiD by means of robust, reliable and as simple as possible design solutions. Attention shall be paid to those design items which may form part of different lines of protection and which implementation can raise conflicts among the different missions.

[52] Challenges: generalized mechanisms, processes or circumstances (conditions) that may impact the intended performance of safety functions; a set of mechanisms have consequences which are similar in nature.

[53] Mechanism: specific reasons, processes or situations whose consequences might create challenges to the performance of safety functions.

[54] Objective provisions tree: graphical presentation, for each of the specific safety principles belonging to the five levels of in depth, of the following elements from top to bottom: (1) objective of the level; (2) relevant safety functions; (3) identified challenges; (4) constitutive mechanisms for each of the challenges; (5) list of provisions in design and operation preventing the mechanism to occur.

With the evolution of the design and development of detailed design solutions the assessor shall be able to apply the OPT method to assess the design provisions for more specific safety functions or principles [A4.4] derived from the fundamental safety functions. An example of a detailed subdivision of the three fundamental safety functions for light water type of reactors is provided in [A4.5]:

1) *to prevent unacceptable reactivity transients;*
2) *to maintain the reactor in a safe shutdown condition after all shutdown actions;*
3) *to shut down the reactor as necessary to prevent anticipated operational occurrences from leading to design basis accidents and to shut down the reactor to mitigate the consequences of design basis accidents;*
4) *to maintain sufficient reactor coolant inventory for core cooling in and after accident conditions not involving the failure of the reactor coolant pressure boundary;*
5) *to maintain sufficient reactor coolant inventory for core cooling in and after all PIEs considered in the design basis;*
6) *to remove heat from the core1 after a failure of the reactor coolant pressure boundary in order to limit fuel damage;*
7) *to remove residual heat in appropriate operational states and accident conditions with the reactor coolant pressure boundary intact;*
8) *to transfer heat from other safety systems to the ultimate heat sink; to ensure necessary services (such as electrical, pneumatic, hydraulic power supplies, lubrication) as a support function for a safety system;*
9) *to maintain acceptable integrity of the cladding of the fuel in the reactor core;*
10) *to maintain the integrity of the reactor coolant pressure boundary;*
11) *to limit the release of radioactive material from the reactor containment in accident conditions and conditions following an accident;*
12) *to limit the radiation exposure of the public and site personnel in and following design basis accidents and selected severe accidents that release radioactive materials from sources outside the reactor containment;*
13) *to limit the discharge or release of radioactive waste and airborne radioactive materials to below prescribed limits in all operational states;*
14) *to maintain control of environmental conditions within the plant for the operation of safety systems and for habitability for personnel necessary to allow performance of operations important to safety;*
15) *to maintain control of radioactive releases from irradiated fuel transported or stored outside the reactor coolant system, but within the site, in all operational states;*
16) *to remove decay heat from irradiated fuel stored outside the reactor coolant system, but within the site;*
17) *to maintain sufficient subcriticality of fuel stored outside the reactor coolant system but within the site;*
18) *to prevent the failure or limit the consequences of failure of a structure, system or component whose failure would cause the impairment of a safety function.*

The applicability of these functions shall be checked and, if needed re-elaborated, for the respective GEN IV reactor system. Specific functions identified for the innovative systems shall be added where appropriate.

In the construction of the OPTs an expert judgment and supporting design evaluations shall be applied to identify for each DiD level and each function the corresponding challenges- mechanisms – provisions.

In addition, the designer shall demonstrate that there is not, within the architecture, provisions whose role and intervention, in situations where they are solicited, would be contradictory and detrimental to the proper behaviour of any other provisions as needed.

The description of the overall architecture so as to indicate accurately the role of each provision is the primary objective of the Objective Provisions Tree (OPT) methodology; in practice it allows to define

or identify for each provision, the conditions of its intervention, the required physical performance, as well as the reliability with which it must perform the required tasks.

It is important to note, however that certain flexibility might be needed in the implementation of the OPT methodology. It is important to emphasize that, due to the complexity of a nuclear facility, unambiguous description of the architecture and the one to one correspondence between the implemented provisions and the level of defence is probably not fully feasible nor, probably, desirable. In practice, the implementation of functional redundancy in the architecture, can lead to putting in place provisions which, although functionally redundant, and therefore capable to face the mutual failure, intervene simultaneously, guaranteeing the simultaneous coverage of two levels of defence in depth, e.g., the protection and control. This is the case, for example as regards the reactivity control, of shut down devices (e.g., control rods and shutdown rods, or even complementary shutdown systems) that can operate simultaneously by combining, in fact their action. The possible interchangeability between provisions for achieving the assigned mission has to be recognized by the OPT; in other words, the combination of provisions within the logic of the defence in depth should consider allowing this flexibility and, in preparing the OPT, this possible interchangeability should easily be shown.

In other cases the provisions intervene in sequence (i.e., one after the other) and truly redundant, and one can imagine, for example, absorber injection systems, other than rods, which would intervene in case of failure of previous systems (shut down rods). Under these conditions the allocation of a given provisions to a given level of the defence in depth is easier and unambiguous.

In terms of flexibility it is also important to consider the possibility that a provision can simultaneously perform tasks that relate several safety functions (e.g., the injection of borated water in a PWR, which participates in both reactivity control and decay of residual heat). Such a possibility can readily be seen through the OPT, by incorporating the provision into the trees for each of the safety functions. Note also that it is within each of these trees, that the designer will define the requirements for the function under consideration (e.g., for the example above: flow and boron concentration for the reactivity control and flow and temperature for the decay of residual power).

Regarding the "non desirable" character for the description of an unambiguous and "rigid" architecture, this is largely because one must consider the possible lack of completeness in the identification of situations; the designer must provide an architecture with the ability (flexibility) to cope with unexpected situations. For this the principle of “states approach” *(“approche par état” in French*) was developed; under these circumstances the provisions are not requested as part of a sequence clearly identified, but rather to address a situation that is defined by a set of given physical parameters and irrespective of upstream sequences.

Upon completion of the OPT it is therefore important, particularly in the treatment of degraded situations of installation (i.e., the fourth level of defence in depth), to consider, for the identification and design of provisions, the possibility of situations postulated on the basis of the representativeness of a set of physical parameters given and irrespective of the sequences that led to this situation.

An example of OPTs developed for the three fundamental safety functions and level 1 of DiD for Japanese Sodium Cooled Fast Reactor [A4.3] is provided in Appendix 3. An example of application to the HTR concept is given by the reference [A4.1].

For verification of the developed OPTs it is suggested to have different working teams crosschecking.

A4.1.4 - Documentation of the results

Along with the graphical development of the OPT it is suggested to complement this process with development of an excel file which will allow and give some unique numbering for each of the branches/ elements of the OPTs, thus allowing better link between graphical trees and provisions documentation. For example:

1. Level of Defence
1.1 Objective/Barriers

1.1.1 Safety Function
1.1.1.1 Challenge
1.1.1.1.1. Mechanism
1.1.1.1.1.1 Provision 1
1.1.1.1.1.2 Provision 2
1.1.1.1.1.3 Provision 3
……
1.1.1.1.1.n Provision n

The more complicated and more detailed the OPTs will become the better structuring of the documentation is needed and other means that excel sheets may be useful, too.

In addition to the graphical/ excel representation of the OPTs it is of high importance to document all information which was used when identifying each set of safety provisions and when judging on its adequacy. Data used to assess the reliability of provisions shall be documented as thorough as possible. This most probably will be the most difficult part of the implementation of OPT tool. On the other side, this is also when the most benefits from the application of this methodology will be experienced. If adequately developed, at the end of the OPTs constructions/ assessment, all sets of safety provisions for which good safety justification exists will be documented, as well as all design options where further research, development, experiments, expert judgments or alternative design solutions are needed. An appropriate data bases may be developed to support the documentation management.

References for Appendix 4:

[A4.1] Considerations in the Development of Safety Requirements for Innovative Reactors: Application to Modular High Temperature Gas Cooled Reactors, IAEA TECDOC 1366, Vienna (2003).

[A4.2] Defence in Depth in Nuclear Safety, INSAG-10, A report by the International Nuclear Safety Advisory Group, IAEA, Vienna (1996)

[A4.3] Findings from pilot use of the OPT methodology for JSFR, H. Niwa, S. Kubo, JAEA, Presentation given at the 4th GIF RSWG Meeting, Paris (26-28 April, 2006)

[A4.4] Safety of Nuclear Power Plants: Design, IAEA Safety Standard Series, Safety Requirements No. NS-R-1, IAEA, Vienna (2000).

[A4.5] Assessment of Defence in Depth for Nuclear Power Plants, Safety Reports Series No 46, IAEA, Vienna (2005)

[A4.6] Proposal for a Technology-Neutral Safety Approach for New Reactor Designs, IAEA TECDOC 1570, Vienna (2007)

Appendix 5 – Deterministic Safety Analysis - Task individual steps

Performing a deterministic analysis is a complex task, which places significant requirements on analysts. These requirements usually include knowledge of the dominant physical phenomena and associated computer code(s) used in the analysis. Deterministic safety analysis also called "accident analysis" is performed in several steps. These steps need not always be sequential; some can be carried out in parallel. Different kinds of activities are performed within each step. A general flow chart illustrating this procedure is shown in Figure A5.1. The main activities are briefly summarized below [Ref. 2.4.4 in section 2.4]:

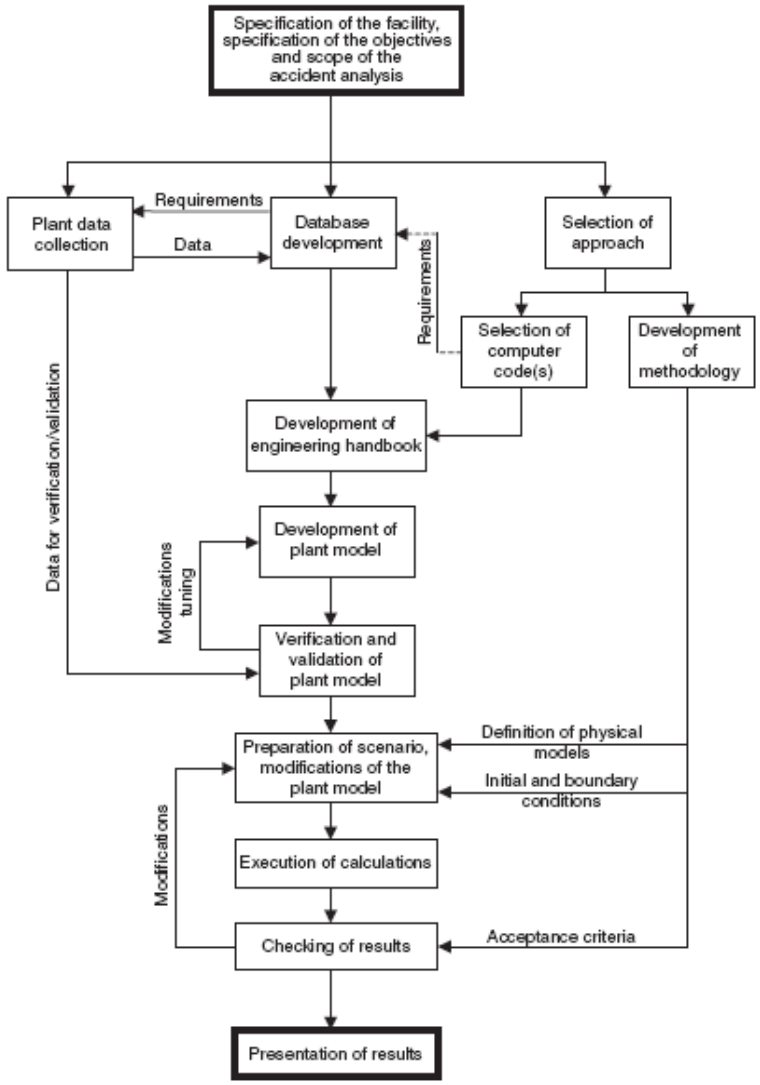


Figure A5.1. Main steps in the deterministic analysis.

A5.1 - Specification of the objectives of the analysis

Clear definition of the goals and scope of the analysis is a prerequisites for a successful performance. The spectrum of accident scenarios to be analysed for PSA is typically broader than that for licensing purposes. In a PSA, all plant operational states including shutdown modes are considered; events beyond the conventional design basis are taken into account; multiple failures and potential for common cause failures are also considered.

From the phenomenological point of view, due to this broader spectrum of situations, the analysis is more complicated because more complex thermo-hydraulic and core phenomena are considered. The complexity may be partially reduced when analysis is necessary to determine only whether severe

core damage has occurred without looking for the detailed description of the core degradation and of the extent of core damage. The objective of the analyses and the events sequences which need to be assessed by deterministic codes have to be determined based on the searched PSA level (level 1 ⇨ level 3).

A5.2 - Selection of the approach to be used

Probabilistic safety analysis typically uses a best estimate approach for evaluation of each individual scenario, i.e.,: best estimate computer codes and best estimate data for the corresponding accident analyses. For an innovative design, where there may be insufficient data to allow best estimate methods to be used, conservative assumptions shall be adopted, as needed.

A5.3 - Selection of computer codes

Several computer codes are often used consecutively to analyze sequences which are often complex. Validation of the codes for intended applications is an essential precondition for their selection and implementation. Six categories of codes are requested for deterministic analysis:

(a) Reactor physics codes;
(b) Fuel behaviour codes;
(c) Thermo-hydraulic codes, including system codes, sub-channel codes, porous media codes and computational fluid dynamics (CFD) codes;
(d) Containment analysis codes, possibly also with features for the transport of radioactive materials;
(e) Atmospheric dispersion and dose codes;
(f) Structural analysis codes.

It is worth noting that the degree of uncertainties associated to the results of these categories can be very different. These uncertainties are related to both the codes themselves and to the boundary conditions which characterize the sequence under examination.

A5.4 - Methodology of the accident analysis

Several guidance documents are available concerning the execution of accident analyses [A5.5]. Those might be consulted for the implementation of this task.

A5.5 - Collection of data

Design information needs to be collected, checked and referenced at each stage of the accident analyses. For each stage of the accident analysis (pre-conceptual, conceptual and design stages), it is very important to have good track of the data used.

A5.6 - Database for the accident analysis

The starting point in the development of the plant specific plant model is the plant database. The reason for the development of the database is to collect, to formalize and reference in appropriate form all the data which are necessary in the analysis. The scope of the database depends on the intended field of applications It is practical to develop the database in code independent form. In Figure A5.1 the requirements on the database that depend on code selection are indicated with dashed lines.

A5.7 - Engineering handbook

An engineering handbook represents an intermediate step between the database and the input data "deck". A full description of how the plant data have been converted into an input data deck for a given computer code needs to be presented in this document. The database and the code user's manual are used for development of such a deck. The engineering handbook should allow a unique interpretation and reproducibility of the code input data deck. It is strongly recommended that an

independent review of the engineering handbook be performed; however such recommendation is requested at later stages of the design safety assessment.

A5.8 - Development of the plant model

On the basis of the engineering handbook, a plant model (often referred as input data deck) needs to be developed. The final product is the file in the format required by the computer code. The model consists of a general part describing the plant and a specific part describing the scenario of an accident. The basic recommendations from code manuals should be followed during the development of the plant model.

A5.9 - Verification and validation of the model

The input data need to be verified and validated in order to provide confidence that the modelling requirements have been fully met and that the performance and functionality are adequate. The verification process is part of quality control and related QA procedures. For innovative designs the need and scope of the verification and validation of the codes used shall be strongly linked to the scientific and engineering knowledge available at each design step for that specific reactor concept.

A5.10 - Preparation of the scenario

The scenario for the accident needs to be prepared after the verification process has been completed. Initial and boundary conditions need to be set in accordance with the methodology of the analysis. Input data for the definition of a postulated initiating event (e.g., break size and location) should be prepared. A choice from various optional code models (e.g., break flow model, heat transfer correlations) needs to be made. Simplified and conservative options may be used if specific models are not available.

A5.11 - Execution of the calculation

The calculation of the accident according to code requirements is performed and results are recorded in code output documents.

A5.12 - Checking of the results

Once the calculation has been completed, the results need to be checked through one or more of the following: supervisory review, independent calculations, comparison with a similar analysis, peer review and spot checking calculations for internal consistency. If necessary, corrections should be made to the input data deck and the calculation should be repeated. The limiting values of key parameters need to be estimated in order to check whether the acceptance criteria are met.

A5.13 - Presentation of the results

The results of the accident analysis need to be structured and presented in an appropriate way to provide a good understanding and interpretation of the course of the accident. Each case analysed needs to be clearly characterized by a description of the conditions and representative parameters of the process. In addition to other data, the results should include a set of key parameters as a function of the time needed to evaluate the status of the safety functions and the physical protective barriers. Finally, the presentation of the results needs to include conclusions concerning the achievement of the primary goals of the analysis, in particular as specified by the PSA model needs.

Appendix 6 – PSA Scope, Quality and Treatment of Uncertainties

A6.1 – PSA Scope and Quality

Nuclear power plant PSAs are often defined in terms of three different "levels" depending on the scope of the analysis and the nature of results that are developed. The distinction is a useful one, and can likely be largely preserved, perhaps with slight adaptation, for Generation IV systems.

Following the international practice, three levels of PSA are considered (Ref. [2.5.6-section 2.5]):

Level 1: The assessment of plant failure leading to the determination of "core damage frequency"

Level 2: The assessment of containment response leading; together with level 1 results, to the determination of containment release frequency.

Level 3: The assessment of off-site consequences leading, together with the results of Level 2 analysis, to estimate the public risk.

Level 1 PSA refers to the modelling of initiating events (transients and loss of coolant events) and safety system response. The phase of the accident progression that is considered is from the onset of the initiating event through the restoration of a safe, stable state, or the onset of core damage. The major results of a Level 1 PSA include an estimate of core damage frequency and estimates of the frequencies of individual accident sequences that collectively comprise that core damage frequency. Results are typically expressed as distributions describing the uncertainties inherent in the results. Because much of the phenomenology addressed in the Level 1 PSA is relatively well understood, the uncertainties in a Level 1 PSA are also relatively small. As discussed in Section 2.5, however, we would expect the magnitude of these uncertainties to increase for Generation IV nuclear systems.

Level 2 PSA includes everything described above for the Level 1 PSA, but extends the analysis to model what happens between the onset of core damage and the point in the accident progression where a safe, stable state is achieved (with a damaged core, but without release of radionuclides from the containment), or the point at which containment fails or is bypassed, and radionuclides are released to the environment. The major results of a Level 2 PSA include a probabilistic estimate of the magnitude, composition, timing, and energy of potential releases of radionuclides to the environment. Because some of this phenomenology is less well understood, uncertainties associated with Level 2 PSAs are larger than for Level 1 PSAs. Again, we would expect that the magnitude of these uncertainties will be even higher for Generation IV nuclear systems than for the fleet of currently operating reactors.

Level 3 PSA includes all of the analysis performed in Level 1 and Level 2 PSAs, and extends the analysis to model all that could happen between the release of radionuclides from the containment (or elsewhere) and the time that the ultimate offsite consequences of these hypothetical releases are experienced. Again, these analytical results are expressed probabilistically, and as a collection of possible scenarios, each with its own characteristics, consequences, frequencies, and uncertainties. Owing to the complexity and relative lack of experience with the issues modelled in the Level 3 PSA, the magnitude of uncertainties in the results of the Level 3 PSA are greater than for Level 1 and Level 2.

Based, in part on the discussion of appropriate risk metrics and other considerations, it is anticipated that a PSA that will yield all of the benefits, and fulfil all the roles that are desirable for Generation IV systems will have to include the following scope and attributes:

- The accident sequence modelling must be performed for the entire range of initiating event types that are credible for a given reactor concept, and that could potentially result in an unwanted radiological exposure at the site boundary. In most PSAs performed to date, the emphasis has been on analysis of formerly identified as "beyond design basis" accidents[55] –

[55] Coherently with the Ref.1, the plant conditions that are to be addressed for the design are conventionally subdivided into two categories (both are integral part of the design basis, i.e., they have to be considered for the design of the system architecture):

- Conditions included in the Design Basis Conditions (DBC): Normal Operation, Incident and Accident Conditions (i.e.,

those that have the potential of leading to severe core damage. The diversity of Generation IV design concepts necessitates broadening the scope of the analysis to encompass a potentially much wider spectrum of events and sequences in particular organizing the systematic search and the exploitation of the "*intermediate results of the PSA"*.

- Include consideration of both internal and external events as they are usually defined in PSA. External events analyzed must include seismic events, fires, floods, strong winds such as tornadoes and hurricanes, and other relevant natural and man-caused events that could credibly pose a challenge to the design. Because the nature, frequency, and severity of external events tends to be quite specific to a particular site, for the general purpose of evaluating the safety of a Generation IV concept or design it will likely be necessary to analyze external events relative to a hypothetical "reference site" for which bounding frequencies and severities (recurrence) of selected external events are postulated.
- A rigorous analytical treatment of uncertainties is essential. A conservative bias is called for to avoid underestimating the magnitude of uncertainties in PSA input parameters.
- State of the art methods for the analysis of human errors that can initiate or otherwise influence (negatively and positively) the course of postulated accident sequences should be applied.
- Be performed to what has customarily been defined to be Level 3 for light water reactors. That is, the scope of the analysis must include, at least at a screening level, modelling of all aspects of accident sequences from the postulated occurrence of an initiating event through the potential dose to an individual at the site boundary.

Because the PSA will play a much larger role in the design and licensing of Generation IV systems than ever before, the need for transparency, quality, and completeness cannot be overstated. While it may be tempting to make simplifying assumptions or take other "shortcuts," especially well in advance of the licensing process, such shortcuts are likely to result in errors, delays, increased costs, and perhaps reduced safety. To help ensure the quality and completeness of PSAs for Generation IV systems, the following recommendations are offered:

- A rigorous quality assurance program should be established prior to initiating the PSA, and the analysis must be conducted in accordance with its provisions.
- From the outset, the PSA must analyze a broad spectrum of potential challenges to the plant. This is in contrast to existing PSAs that have typically looked primarily at "beyond design basis" events (*cf. previous foot note*).
- The PSA must be led and performed by acknowledged experts in the field of PSA.
- There are a number of international consensus standards that have been established, or are under development to ensure the quality of PSA. PSAs for Generation IV systems should be performed in accordance with these standards. One such example is the American Society of Mechanical Engineers' "Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications (ASME RA-Sb 2005)."
- Modeling methods and codes used in the PSA must be "state of the art" and generally accepted by major international regulatory bodies, professional societies, or other recognized arbiters of technical validity.
- The PSA should be reviewed by a team of independent experts

---

design basis accidents) of internal origin for which the plant is designed according to established design criteria and conservative methodology.

- Conditions included in the Design Extension Conditions (DEC): A specific set of accident sequences that goes beyond design basis accidents, to be selected on deterministic and probabilistic basis and including: Complex Sequences, Severe plant conditions. Appropriate design rules and criteria are set for DEC, in general different from those for design basis accidents.

The terminology "Beyond design basis" is so replaced with DEC

A6.2 - PSA :Treatment of Uncertainties

The topic of uncertainties in PSA is one that has attracted a lot of attention, and has even created controversy about how "dependable" PSA results are, and thus, how useful those results are in making decisions regarding design, licensing, regulation, and operation of nuclear power plants. It is important to recognize from the outset, however, that while the topic is an important one, for the most part *PSA does not create new sources of uncertainty. It merely displays and characterizes uncertainties that are inherent in the inputs, and thus the outputs, of the models that comprise the PSA.* In other words, the PSA is displaying uncertainties that exist in any case, but which might otherwise not be specifically identified, propagated, or reflected in the results of analyses.

Uncertainties in PSA arise from many sources. These include:

- Inability to precisely specify initial or boundary conditions
- Incomplete or sparse data on failure rates, initiating event frequencies, human error rates, etc.
- An incomplete understanding of some phenomena expected during both normal operations and off-normal conditions
- The use of assumptions in developing PSA models
- Limitations in the modelling methods that are used in PSA

Even such elementary matters as estimating the failure probability of a particular type of component based on empirical data, or generically speaking the failure probability of a given provision, can be surprisingly difficult, and a source of uncertainty. Because Generation IV nuclear systems are likely to employ, at least to some degree, new materials, designs, fuel forms, coolants, operator interfaces, etc., it is very likely that the nature and magnitude of these kinds of uncertainties will be even larger in Generation IV systems than they are in the current fleet of operating nuclear power plants. One of the principal strengths of the PSA approach is its unique ability to formally account for those uncertainties in a disciplined way.

One widely accepted paradigm divides PSA uncertainties into two categories. "Aleatory uncertainty" (from the Latin *alea*) refers to random or stochastic phenomena, and is also called "random uncertainty or variability." The term "Epistemic uncertainty," on the other hand, derives from the Greek *episteme* which means "knowledge." Epistemic uncertainty is also called "state of knowledge uncertainty."

As a practical matter, for purposes of developing and evaluating Generation IV nuclear systems, it seems expedient and sufficient to differentiate between what we will call "data uncertainty" and "modelling uncertainty."

Data uncertainty refers to the aggregated uncertainty associated with the estimation of initiating event frequencies, component failure rates, and human error rates. Some of the sources of data uncertainty include issues of sample size, extrapolation from data for similar components in similar service, accounting for degraded performance states, observer error, and others. Generally, data uncertainty refers to the collective effect of sources of uncertainty that affect the analyst's ability to precisely estimate frequencies or probabilities of events.

Modelling uncertainty refers to the aggregated uncertainty that derives from modelling limitations, inability to precisely specify boundary conditions, incomplete understanding of physical processes, the use of assumptions in model development, etc. Generally, modelling uncertainty represents the affect of the analyst's inability to precisely understand and describe certain physical phenomena.

Appropriate treatment of data uncertainties for Generation IV systems should generally employ conventionally accepted means (e.g., Monte Carlo simulation for uncertainty propagation) with the additional expectations that the input probability density functions must sufficiently large as to reliably characterize the full uncertainty in the estimation of the underlying parameter.

Modelling uncertainties are best addressed through sensitivity studies. By varying selected aspects of how a particular issue is modelled, the analyst is able to determine how sensitive the overall risk model results are to various modelling issues and uncertainties. Modelling issues that have both large

uncertainties and large impacts on risk metrics of concern are candidates for further analysis or research and development.

When uncertainties are so large that they do not allow meaningful comparisons with established risk goals, other evaluative decision criteria, or among design alternatives, designers will have to choose between two possible courses. The first alternative is to introduce additional safety margin into the design. It will be necessary to provide enough additional safety margins to allow the designer to demonstrate that, even with large uncertainties, there is a very high degree of assurance that the design meets established safety goals. The other potential course is to recognize that uncertainty may be reduced through additional research and development.

Appendix 7 – Details of example of application of PIRT, OPT, DPA and PSA to JSFR

A7.1 JSFR plant and its design specifications

JSFR is a loop-type sodium-cooled fast reactor: i.e., primary pumps and intermediate heat exchangers (IHX) constituting two loops of PHTS are installed outside the reactor vessel as illustrated in Figure A7.1. The major design specifications are shown in Table A7.1. The thermal energy generated at the rated power of 3570MW heats up the primary coolant to 550 ºC at the reactor vessel outlet, then it is transferred to the secondary coolant with being heated to 520 ºC at the two IHXs. The main steam with temperature of 497 ºC and pressure of 19.2 MPa is generated at the two steam generators, and it rotates the turbine generator to produce the electric power output of 1500MW.

Table A7.1 Major design specifications of JSFR [A7.1]

Power output	1500MWe/3570MWt
Number of loops in PHTS	2
Primary coolant temperature	550ºC/395ºC
Primary coolant mass flow rate	1.8×10^{4} kg/s
Secondary coolant temperature	520ºC/335ºC
Main steam temperature and pressure	497ºC/19.2MPa

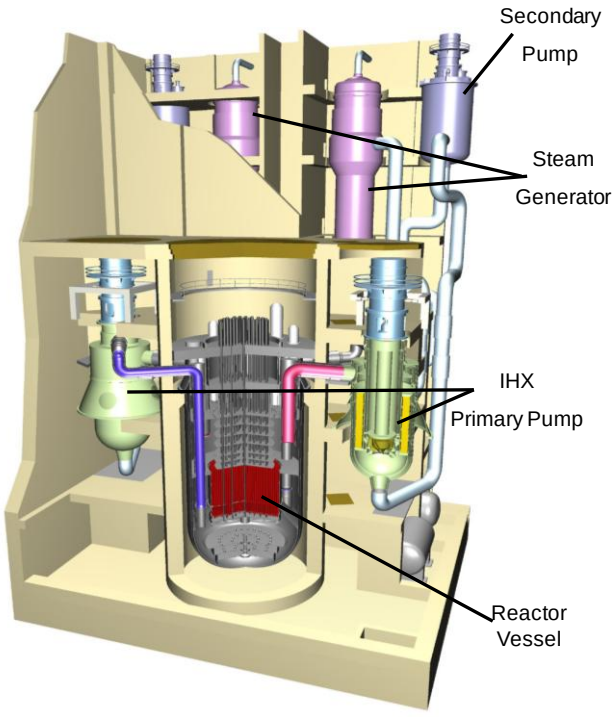


Figure A7.1 Schematic view of JSFR NSSS [A7.1]

A7.2 Outline of self-actuated shutdown system (SASS)

A self-actuated shutdown system (SASS, ref. A7.2) is a passive safety feature which inserts control rods by the gravity force, where the detachment of the rods would be achieved by the coolant temperature rise under anticipated transient without scram conditions. The self-actuated shutdown

feature of JSFR is achieved by the Curie point electromagnet using the temperature sensing alloy, which will lose magnetism at a predefined temperature. Figure A7.2 shows the fundamental structure of the Curie point electromagnet SASS. The Curie point electromagnet SASS consists of an electromagnet and an armature. The control rod is held by the magnetic force formed by the electromagnet. When the temperature of the sensing alloy embedded in the armature part of SASS exceeds the normal operation level in a certain extent, the magnetic resistance of a temperature sensing alloy increases and then the holding force is rapidly lost due to exceeding the Curie point. In a reactor case, when the temperature of the sensing alloy heated up by the increase of the coolant temperature under the ATWS conditions, the control rods would be detached and be inserted into the core by gravity force without any external driving force and/or actuation signals.

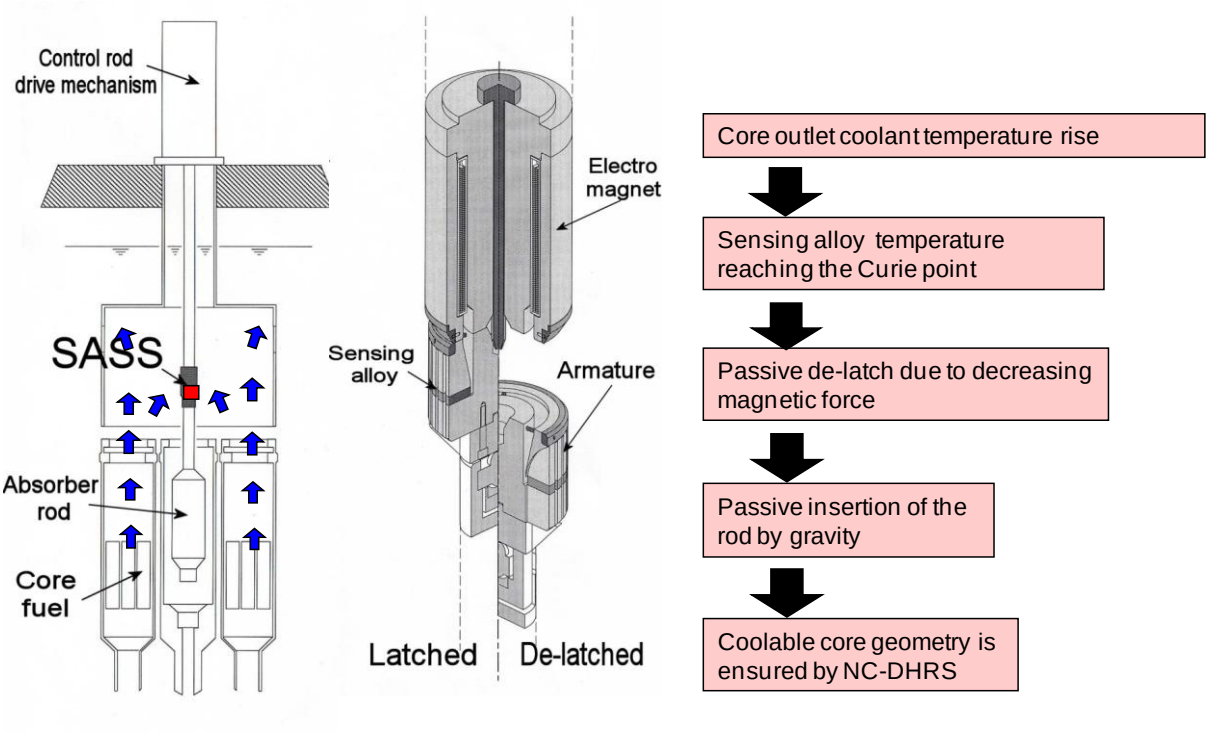


Figure A7.2 Outline of the Curie point electromagnet type of SASS [A7.3]

A7.3 PIRT application result

Table A7.2 shows the PIRT preliminary application result, which includes the key phenomena in evaluating the effectiveness of the SASS upon the ULOF accident. Comparison of the PIRT application results between the two different time points shows that the knowledge level of the key phenomena has been improved through the various experimental studies for the SASS research and development (R&D). PIRT can be helpful to identify needs for a key experimental study if it is conducted before addressing a new R&D issue.

Table A.7.2 Preliminary PIRT application result by two assessors A and B

System	Component	Phenomena/Characteristics/State variables	IR		KL_1		KL_2	
			A	B	A	B	A	B
BRSS	SASS	SASS actuation temperature	H	H	1	2	3	4
Reactor	Upper core region around SASS	Coolant transport delay time from core outlet to around SASS	H	H	3	2	3	3
		Time constant of temperature response delay from coolant around SASS to SASS device	M	M	1	2	3	3
	Reactor core	Core outlet temperature of the coolant that flows to around SASS	H	H	3	3	3	3
		Doppler reactivity coefficient	M	M	4	4	4	4
		Fuel temperature reactivity coefficient	L	M	4	3	4	3
		Fuel cladding temperature reactivity coefficient	M	M	4	4	4	4
		Coolant temperature reactivity coefficient	H	H	4	4	4	4
		Coolant flow rate halving time	H	H	4	4	4	4
		Power distribution	M	M	4	4	4	4
		Flow rate distribution among core assemblies	M	M	4	4	4	4
		Coolant temperature at the core inlet and outlet	L	L	4	4	4	4
		Fuel pin gap heat transfer coefficient	M	M	4	3	4	3
		Fuel pellet thermal conductivity	I	I	4	4	4	4
		Thermal material property of fuel cladding and coolant	I	I	4	4	4	4
RPCS	Temperature I&C	Coolant temperature to be used for reactor power control	M	L	4	4	4	4
PHTS	Pump	Pump rotating inertia	M	M	4	4	4	4
	-	Pressure loss in the reactor and PHTS	M	M	4	4	4	4

BRSS: Backup Reactor Shutdown System
RPCS: Reactor Power Control System
PHTS: Primary Heat Transport System
IR: Importance ranking
KL_1: Knowledge level before starting SASS R&D
KL_2: Knowledge level at present

A7.4 Alternative representation of OPT

OPT is usually drawn in a tree structure. Figure A7.3 is an alternative representation of OPT developed for JSFR safety function 2 at level 3 shown in Figure 9. This is a list style and compact expression. It is possible to construct and edit the tree structure without any specific drawing tool.

```
3.          Level 3 of defense
3.1         Control of accidents within the design basis
3.1.2       Core heat removal
3.1.2.1     Degraded or disruption of heat transfer path
3.1.2.1.1   Short-term loss of forced convection in the 1ry  circuit
3.1.2.1.1.1 Rapid reactor shutdown
3.1.2.1.1.2 Secure flow coast down to 1ry circuit
3.1.2.1.2   Long-term loss of forced convection in the 1ry  circuit
3.1.2.1.2.1 Adequate margin to fuel failure temp.
3.1.2.1.2.2 Heat transfer by passive measure(DHRS)(natural convection and battery-operated air-cooler dampers)
3.1.2.1.3   Leakage of coolant in the 1ry circuit (pipe break)
3.1.2.1.3.1 Layout of piping (high position to maintain reactor level)
3.1.2.1.3.2 Localization and isolation of leaking Na (GV & double wall piping)
3.1.2.1.4   Loss of ultimate heat sink (e.g., 2ry circuit, water/steam system)
3.1.2.1.4.1 Rapid reactor shutdown
3.1.2.1.4.2 Automatic actuation of DHRS (natural convection and battery-operated air-cooler dampers)
3.1.2.1.5   Partial loss of DHRS functionality (e.g., DHRS leakage)
3.1.2.1.5.1 Functional redundancy of DHRS
```

Figure A7.3 Example of a list style with unique numbering of OPT developed for JSFR safety function 2 at level 3

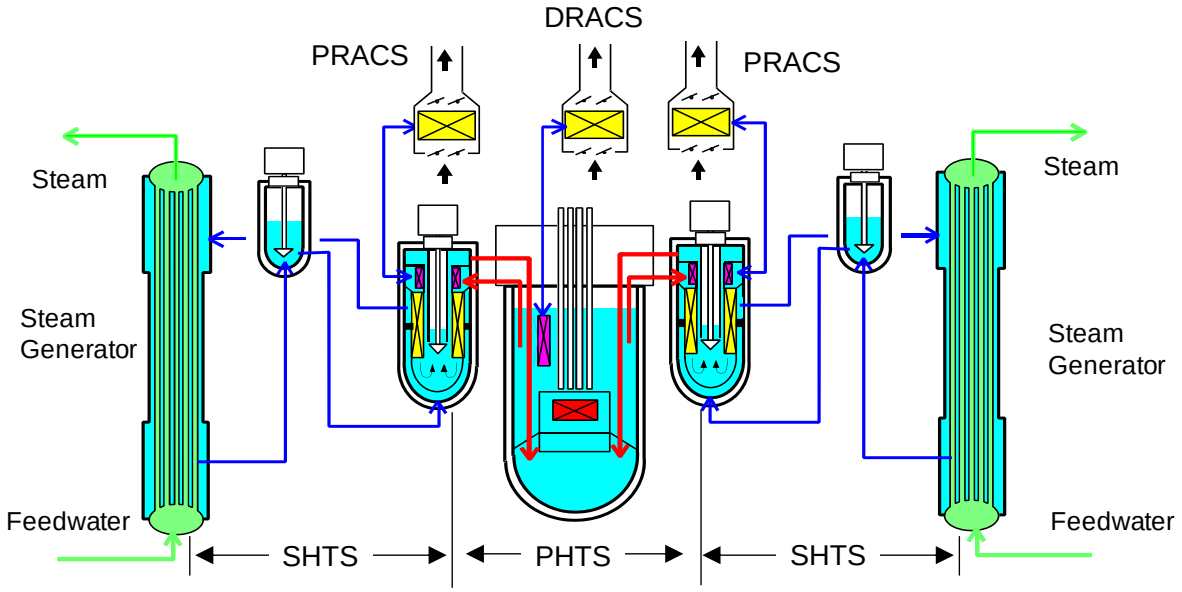
A7.5 Details of the application of DPA and PSA to DHRS of JSFR

The outline of DHRS in JSFR is briefly described. As shown in Figure A7.4, the JSFR is equipped with total three trains of reactor auxiliary cooling systems for decay heat removal so that the decay

heat can be removed only by way of the decay heat removal system. One of them is the DRACS that is directly connected to the reactor vessel, and the others are the PRACS that is connected to the PHTS. These trains are operated in a fully passive condition (i.e., natural circulation of sodium coolant and natural air flow at the heat sink).

DPA and PSA were conducted in a parallel way. In order both to determine postulated scenarios in DPA and to develop event trees in PSA, initiating events were identified and categorized, based on the plant design information and using master logic diagram method. The categorized initiating events are shown in Table A7.3. Then the mitigation systems were defined and the event trees were developed as shown in Figure A7.6, based on the plant design specifications linked with the key information that was obtained from the OPTs. The reactor scram followed by the DHRS operation was selected as the postulated scenario. Systems and components available were determined, corresponding to the successful accident sequence that was developed in the event trees. DPA was conducted by using the plant model shown in Figure A7.5. And then the end state in Figure A7.6, whether core integrity is maintained or not, was determined based on the DPA results.

Based on consideration of the JSFR PSA result, the designer/analyst examined possibility of introducing non-safety-related blowers at the air cooler inlet to enhance PRACS and DRACS capability with considering both less cost increase and significant safety improvement as shown in Figure A7.7. After additional DPA, it was confirmed that the consequence of the decay heat removal scenario with sodium natural circulation and forced-air flow by using DRACS alone becomes maintaining the reactor coolant boundary integrity as shown in Figure A7.8. The event tree was then updated as shown in Figure A7.9 by considering this design improvement. The updated PSA result shows quantitatively that introduction of the air cooler blowers in both PRACS and DRACS can reduce significantly the PLOHS frequency; i.e., improve the reliability of decay heat removal (see in detail Figure A7.10).



PRACS: Primary Reactor Auxiliary Cooling System
DRACS: Direct Reactor Auxiliary Cooling System
PHTS: Primary Heat Transport System
SHTS: Secondary Heat Transport System

Figure A7.4 Outline of decay heat removal system (DHRS)

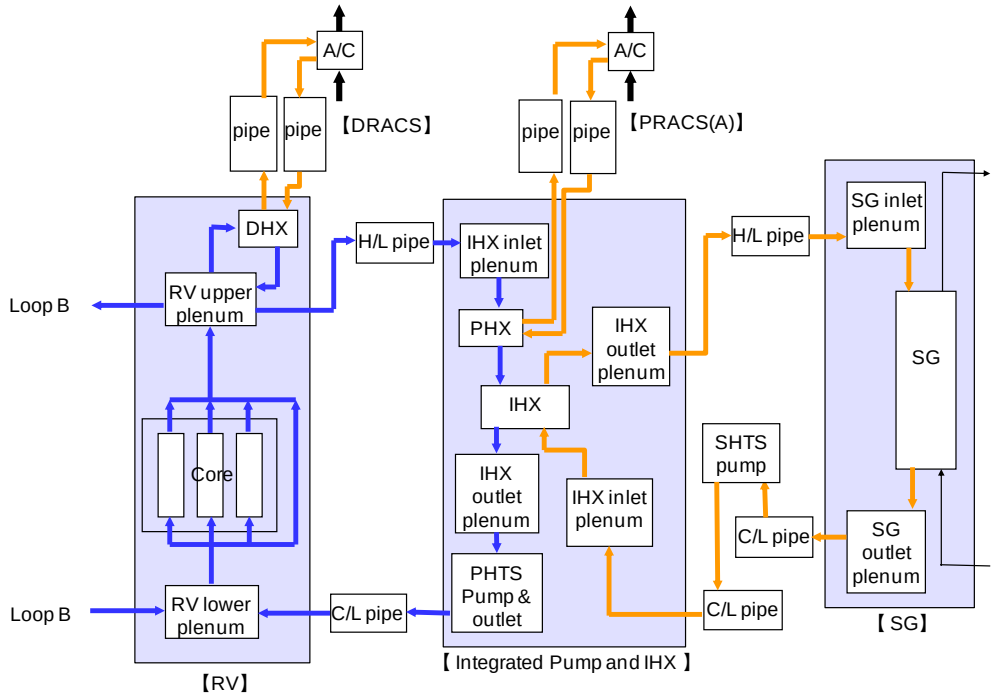


Figure A7.5 Example of the plant model for DPA of JSFR DHRS

Table A7.3 Categorization of initiating events for DHRS analysis

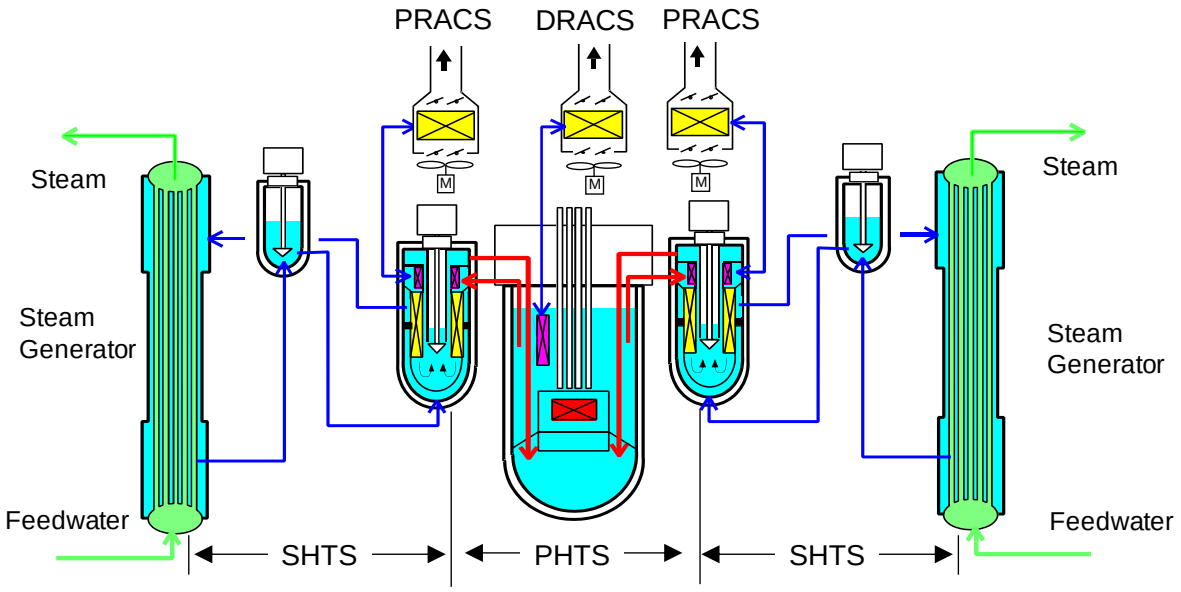
ID	Description	Examples	1 PRACS	DRACS	Electric power system
IC01	Reactor shutdown with all DHRS functions available	Positive reactivity insertion	○	○	○
IC02	Loss of forced circulation in one PHTS or SHTS	Primary pump stick	○	○	○
IC03	Sodium leakage inside the guard pipes/guard vessels in one PHTS	Sodium leakage inside the guard pipe in PHTS piping	△	○	○
IC04	Loss of circulation capability in DRACS	Sodium leakage within the enclosure in DRACS piping	○	×	○
IC05	Loss of off-site power	Loss of off-site power	○	○	△
IC06	Loss of main feedwater/steam line	Feedwater pump failure	○	○	○
IC07	Loss of circulation capability in one PRACS	Sodium leakage within the enclosure in PRACS piping	×	○	○

○: The initiating event does not affect the safety system.
△: The initiating event results in loss of redundancy in the safety system.
×: The initiating event results in complete loss of the safety system function.
Some accident management might be affected by IC02 and IC06.

Loss of circulation capability in PRACS-B	Reactor SCRAM	Passive cooling by using PRACS-A *	Passive cooling by using DRACS *	Seq. No.	Accident sequence	Core integrity	
IC07-B	RS	ANC	DNC			Before DPA	After DPA
Success ↑				1	/RS*/ANC*/DNC (Successful DBA scenario)	**Should be OK (1)**	OK
				2	/RS*/ANC*DNC (Passive cooling by using PRACS-A alone)	**Unknown (1)**	Damage
				3	/RS*ANC*/DNC (Passive cooling by using DRACS alone)	**Unknown (1)**	Damage
Failure ↓	This sequence is developed in detail in other event trees			4	/RS*ANC*DNC (Loss of all heat sink)	Damage	Damage
				5	-	-	-

*; This cooling mode relies only on the safety-related systems.
(1) Need to be confirmed by DPA

Figure A7.6 Typical event tree model in the JSFR Level-1 PSA



PRACS: Primary Reactor Auxiliary Cooling System
DRACS: Direct Reactor Auxiliary Cooling System
PHTS: Primary Heat Transport System
SHTS: Secondary Heat Transport System

Figure A7.7 Design improvement by introducing non-safety-related blowers at the air cooler inlet to enhance PRACS and DRACS capability

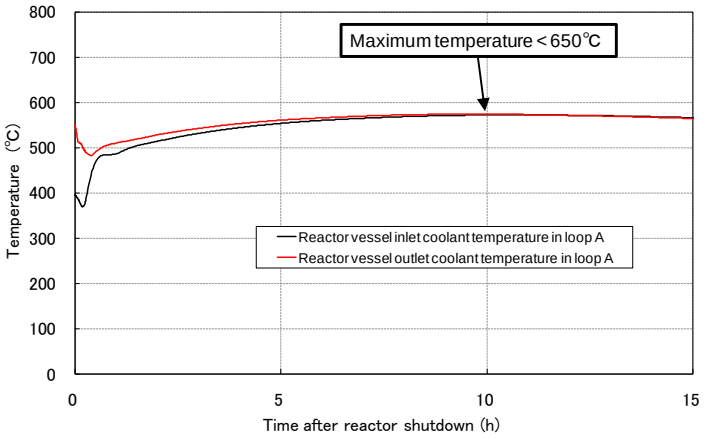


Figure A7.8 Additional DPA result: Forced-air flow with blower and sodium natural circulation cooling scenario by using DRACS alone

Loss of circulation capability in PRACS-B	Reactor SCRAM	Passive cooling by using PRACS-A *	Passive cooling by using DRACS *	Forced air flow cooling by using PRACS-A **	Forced air flow cooling by using DRACS **	Seq. No.	Accident sequence	Core integrity
IC07-B	RS	ANC	DNC	AFC	DFC			
						1	/ANC*/DNC (Successful DBA scenario)	OK
						2	/ANC*DNC*/AFC (**Forced air flow cooling by using PRACS-A alone**)	OK
						3	/ANC*DNC*AFC (Passive cooling by using PRACS-A alone)	Damage
Success ↑						4	ANC*/DNC*/DFC (**Forced air flow cooling by using DRACS alone**)	OK
						5	ANC*/DNC*DFC (Passive cooling by using DRACS alone)	Damage
						6	ANC*DNC (Loss of all heat sink)	Damage
Failure ↓	This sequence is developed in detail in other event trees					7	-	-

*; This cooling mode relies only on the safety-related systems.
**; This cooling mode relies not only on the safety-related systems but also on automatic actuation of the non-safety-related systems (i.e., air blower, electric power systems).

Figure A7.9 DHRS event tree model considering air cooler blower operation

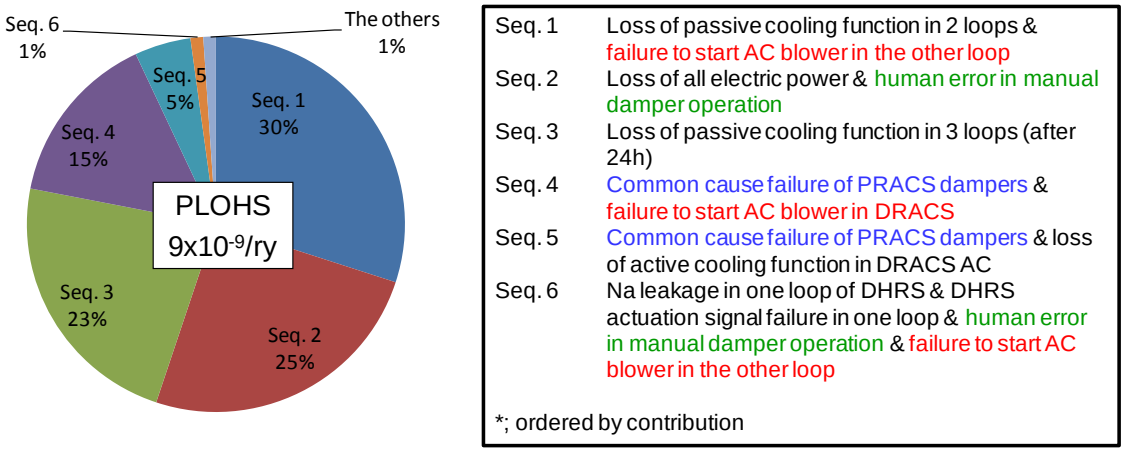


Figure A7.10 PSA result: Major contributors to PLOHS frequency broken down by combination of loss of mitigation systems

References A7

[A7.1] *Shoji Kotake, et al., "Development of Advanced Loop-Type Fast Reactor in Japan (1): Current Status of JSFR Development", paper 8226, Proceedings of ICAPP '08, Anaheim, CA USA, June 8-12, 2008.*

[A7.2] *Shigeyuki Nakanishi, et al., "Development of Advanced Loop-Type Fast Reactor in Japan (5): Adoption of Self-Actuated Shutdown System to JSFR", paper 8224, Proceedings of ICAPP '08, Anaheim, CA USA, June 8-12, 2008.*

[A7.3] *Ichimiya et al., "A Next Generation Sodium-Cooled Fast Reactor Concept and its R&D Program," Nucl. Eng. Technol., 39(3), 171-186(2007).*