GIF/RSWG/2021/001

Basis for the Safety Approach for Design & Assessment of Generation IV Nuclear Systems

Revision 2

July 2021

Prepared by:

The Risk and Safety Working Group
of the Generation IV International Forum

Printed by the OECD Nuclear Energy Agency for the Generation IV International Forum (GIF)

DISCLAIMER

This report was prepared by the Risk and Safety Working Group of the Generation IV International Forum (GIF). Neither GIF nor any of its members, nor any GIF member‘s national government agency or employee thereof, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by GIF or its members, or any agency of a GIF member’s national government. The views and opinions of authors expressed therein do not necessarily state or reflect those of GIF or its members, or any agency of a GIF member’s national government.

TABLE OF CONTENTS

Executive Summary

2008 version of this document was the first major work product of the Generation IV International Forum (GIF) Risk and Safety Working Group (RSWG). Ten years after its publication, an update of the 2008 version was requested by the GIF Policy Group to reflect the experience gained from development and application of the Integrated Safety Assessment Methodology (ISAM) and to consider the lessons from the Fukushima Dai-ichi accident as articulated in the new requirements issued by various international organizations such as the IAEA, OECD, EC, and WENRA. This report provides a high-level summary of the safety related achievements of the past ten years to supplement the objectives, principles, and attributes discussed in the original report to continue guiding the ongoing R&D activities.

The RSWG was formed to promote a consistent and effective approach to assuring the safety of Generation IV nuclear energy systems. The six Generation IV reactor concepts that have been selected by the GIF members present a diverse set of design and safety characteristics. A number of these characteristics are significantly different from those presented by the earlier generations of light water reactors. The overall success of the Generation IV program depends on, among other factors, the ability to develop, demonstrate, and deploy advanced system designs that exhibit excellent safety characteristics. While the RSWG recognizes the excellent safety record of nuclear power plants currently operating in most GIF member countries, it believes that progress in knowledge and technologies, and a coherent safety approach, hold the promise of making Generation IV energy systems even safer and simpler than this current generation of plants.

The Generation IV research and development program is guided by the recently updated GIF IV Technology Roadmap (Ref. [1]) which identified three specific safety goals for Generation IV systems:

1. *Generation IV nuclear energy systems operations will excel in safety and reliability.*
2. *Generation IV nuclear energy systems will have a very low likelihood and degree of reactor core damage.*
3. *Generation IV nuclear energy systems will eliminate the need for offsite emergency response*.

Since its inception, the RSWG focused on defining the attributes that are most likely to help meet these Generation IV safety goals and identifying methodological advances that might be necessary to achieve these goals. This has been done consistently with the work of IAEA. Important findings and recommendations of the RSWG presented in this document include:

- **Generation IV Safety Philosophy**
  - Opportunities exist to further improve on nuclear power's already excellent safety record in most countries. As a starting point, the RSWG recognizes that the level of safety that has been attained by the vast majority of operating nuclear power plants (Generation II) in most countries of the world is already very good. In parallel, the quantitative safety objectives applicable to the reactors of the third generation (e.g. AP1000 and EPR) are very ambitious and assure an improved level of protection reducing the level of risk in a demonstrable way. For Generation III reactors, the lessons learnt from the Fukushima accident has been taken into account. These lessons must also be considered at the design stage for Generation IV reactors. Considering the already ambitious Generation-III safety objectives as the reference, Generation-IV reactor systems will excel in safety, with improved safety design and more robust safety

demonstration. Further safety improvements for Generation IV systems are possible through progress in knowledge and technologies and the application of a cohesive safety philosophy early in the design process. It is worthwhile and achievable to further improve what is already a very safe source of clean and reliable energy. Such improvements will, in particular, address the way to achieve the level of safety through the implementation of a safety that will be **"*built-in*"** to the fundamental design rather than **"*added on*"** to the system architecture.

- Quantitative probabilistic objectives. The probabilistic objective of severe accident prevention for the Generation III pressurized water reactors is 10^{-5} per year. An additional prescriptive reduction of severe accident frequency for Generation IV systems[1] is not justified and could even be counterproductive. The current probabilistic objectives are already ambitious and reach the limits in terms of representativeness and confidence. Indeed, the hardening of the probabilistic objectives for the already highly unlikely events could increase the complexity of the installation and its operation, thus reducing its safety on a daily basis, for a marginal gain in terms of severe accident probability. This probabilistic objective can be used for comparative purposes, but it should not be used as an absolute value for acceptance of the design. For Generation IV reactors, for which a limited experience feedback is available, the safety demonstration will rely primarily on deterministic methods to cover the levels of defence-in-depth and to extend the prevention and mitigation of the severe accidents. Probabilistic methods, when relevant, will provide additional insights.

- Potential safety improvements should simultaneously be based on several elements. These include the notion of "optimal risk reduction" (i.e. ALARP); the adoption of ambitious safety objectives that will drive the research required to attain those objectives; the application of innovative technologies; an emphasis of accident prevention backed up by mitigation; the search for robust safety architecture; and, finally the requirement for the improvement of the safety demonstration's robustness. For all these items, technical requirements should be considered only if they can bring a real and demonstrable benefit. The report represents a preliminary step for the definition and the motivation of such requirements.

- The diversity of the Generation IV systems and the need for a consistent approach applicable for the design and the assessment of these systems justify re-examination of the traditional safety approach. Such an updated approach must simultaneously answer key criteria such as: Agreement with current and foreseen future regulations; ability to demonstrate the full implementation of defence in depth; allowing for a plants' design and assessment which will exhibit both deterministic practices and probabilistic objectives over an broad spectrum of design conditions, including severe plant conditions; handling internal and external hazards so as to achieve, as much as possible,

[1] A severe accident is defined in IAEA Safety Glossary as an "accident more severe than a design basis accident and involving significant core degradation." Similar definitions also exist in national regulations: For example, NRC defines it as "an accident in which substantial damage is done to the reactor core whether or not there are serious offsite consequences." Even though the term includes the cases with core melt conditions within the context of Generation III water-cooled reactors and some Generation IV SFR, GFR, LFR and SCWR designs, the concept of severe accident for Generation IV reactors in general, and for the MSR and VHTR systems in particular, is yet to be more explicitly defined. In order to avoid the potential automatic association of severe accidents with accidents leading to a core melt (especially when it is not applicable), the terms "severe accident" and "severe plant conditions" are used interchangeably throughout this report.

the coherency with the approach adopted for internal events; improving the safety demonstration for the domains where gaps still exist in the current state of art.

- The principle of "defence in depth" has served the nuclear power industry well, and it must be preserved in the design of Generation IV systems. Defence in depth is the key to achieve safety robustness, thereby helping to ensure that Generation IV systems do not exhibit any particularly dominant risk vulnerability. To meet these objectives, the defence in depth should be implemented in a way that it is exhaustive, progressive, tolerant, forgiving and well-balanced. Details about these characteristics of effective defence in depth are provided within the report.

- The Generation IV design process should be driven by a "risk-informed" approach (i.e. considering both deterministic and probabilistic methods). Indeed, the RSWG believes that safety and economics of Generation IV designs can be positively impacted by formally adopting, in addition to the deterministic approach, the use of PSA techniques and complementary tools as drivers throughout the design process.

- For Generation IV systems, in addition to prototyping and demonstration, modelling and simulation should play a large role in the design and the assessment. Making use of sophisticated modelling tools and techniques and advanced computing power, modelling and simulation is increasingly being used in the design and evaluation of complex technologies. Prototyping and demonstration systems are expensive and contribute to the long lead time associated with the development of new technologies. Making increased use of modelling and simulation can provide a means of more thoroughly evaluating a candidate design, thereby reducing uncertainties, and improving safety. By focusing attention on those aspects of the design that are most critical to plant safety, development costs are reduced and safety is enhanced.

➢ **Design and assessment of innovative systems**

- The Design Basis for Generation 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 represent, with a high degree of confidence, the range of physical events that could conceivably challenge the plant safety. For accidents other than a severe accident, the design aims to ensure that the radiological consequences shall not lead to the need to implement measures to protect populations. In the case of severe accident, the objective is to have very low releases such that no off-site measures are necessary. If measures are nevertheless necessary, they shall be limited in time and space with sufficient grace period for their implementation. Even temporary evacuation of populations should not be necessary and only sheltering, limited in time and space, shall be envisaged. Accidents likely to lead to very large off-site radioactive releases, or with kinetics that would not allow for the timely implementation of necessary measures to protect populations, shall be rendered physically impossible or, failing that, extremely unlikely with a high degree of confidence so that they can be considered as practically eliminated. 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 internal events and external hazards in a consistent way, factoring in the treatment of physical protection issues along with associated uncertainties.

- Objectives and practices for the design improvements. To efficiently set up these practices, four complementary ways may be followed by the designer: 1) Critical and systematic examination and consideration of the feedback from the past experience; 2) rationalization of the design approach by the deliberate adoption of the ALARP principle based on a cost-benefit analysis; and 3) implementation of the concept of defence in depth in a manner that is demonstrably exhaustive, progressive, tolerant, forgiving and well-balanced. Finally, special attention should be given to the treatment of the severe plant conditions through provisions of measures that help managing such conditions.

- Achievement of the safety demonstration's robustness. This rests on the ability of the designer and the developer to be exhaustive in the recognition of risks stemming from phenomena considered in the design. Whenever possible, plant design features based on natural phenomena and physical properties of materials should be relied on to demonstrate, in an "intuitive" manner, the ability of the plant to prevent the accident progression with an adequate degree of confidence, an understanding of the associated uncertainties and provision of sufficient margins, and the minimization of impact on workers and public.

- Practical assessment tools to support the design and evaluation activities. Among the conventional tools such as PIRT, probabilistic, deterministic, and phenomenological assessments, the Objective Provision Tree and the notion of Line of Protection which allow schematizing the whole safety architecture are suggested as part of the process to help the plant design and evaluation.

➢ **Activities Achieved Since 2008 and the Fukushima Daiichi Accident**

The work to improve the safety of nuclear installations is a continuously evolving process. Since the publication of the RSWG's Basic Safety Approach (BSA) in 2008 and the Fukushima accident in 2011, the international organizations with regulatory oversight function have reviewed the safety standards to ensure their continued improvement. Specific activities were launched to integrate the lessons learned and provide new requirements/recommendations applicable to operation of existing reactors as well as assessment of future nuclear installations. Significant emphasis was on the management of the severe accidents and the ability to handle the external hazards, all leading to re-examination of:

- External hazards and their uncertainty,
- Robustness of the electrical systems and ultimate heat sink,
- Independence of prevention/mitigation measures in different levels of defence in depth,
- Common-cause and common-mode failures,
- Protection of spent fuel in storage locations,
- Considerations for multi-unit sites and other nuclear/non-nuclear facilities,
- Improved emergency management systems.

Another key milestone for the activities of the RSWG since the publication of the BSA was the 2011 document describing the Integrated Safety Assessment Methodology (ISAM). The ISAM is intended to support the achievement of "built-in" safety by supporting development of the

safety architecture and framework from the earliest design stages. The ISAM is a "toolkit" consisting of elements that help to answer different safety-related questions and provide important safety perspective throughout the design cycle by using the interim analysis results to actively shape the direction of the design process. The expected result is the improvement of safety, the reduction of capital costs and the reduction of the time needed for the technology development and deployment.

- **Future activities of the RSWG**

The future activities of the RSWG will focus on proposing technology-specific safety design criteria and guidelines, implementation of the integrated safety assessment methodologies for specific design tracks, and necessary crosscutting safety related R&D. Generation IV safety goals, objectives, and requirements generally conform with IAEA standards (e.g. the IAEA SSR series). The design guidelines for Generation IV systems that specify recommendations on how to comply with the safety requirements are also expected to be fairly consistent with the approach used in IAEA guidelines for design of light-water reactors (e.g. the IAEA SSG series) with targeted design-specific modifications.

Concerning the RSWG's relationships with the developers and the designers, it is expected that the definition of a common agreed safety approach outlined in this report will provide essential insights for safety related R&D. Strong interactions will be maintained with the System Steering Committees (SSCs) in order to help check the pertinence of the R&D already defined within the System Research Plans, to help identify complementary themes & items and to provide consultative support to the safety related system assessment. Interaction with Proliferation Resistance and Physical Protection Working Group (PR&PP) should continue to further facilitate integrated consideration of safety, proliferation resistance and physical protection goals.

Chapter I: Introduction

I.1 Background

More than 50 years of experience with operating nuclear power plants provide evidence that nuclear technology has a potential to play a key role in the future by providing a means of supplying the world with a safe, proliferation-resistant, and economic source of energy. Based on this long term vision, fourteen countries (Argentina, Australia, Brazil, Canada, China, Euratom, France, Japan, Republic of Korea, Russian Federation, Republic of South Africa, Switzerland, the United Kingdom, and the United States) have joined the Generation IV International Forum (GIF) with the aim to organize and coordinate international collaboration on research and development (R&D) for the fourth generation of nuclear energy systems. The Generation IV reactors will represent new solutions to the world's future energy and environment challenges while allowing continued economic development and growth throughout the world.

The first examples of the Generation IV nuclear energy systems (demonstrators or prototypes) are already being deployed in some GIF member states. In order to get a favorable public perception, they will have to compete economically with other sources of energy, while satisfactorily addressing nuclear safety, waste management, and proliferation resistance issues. Because of that, the Generation IV systems introduce substantial innovative technologies compared to current plants and these changes will have to be accommodated within the regulatory framework to support their licensing.

As described in its charter and subsequent policy statements, the GIF is led by the Policy Group (PG) that is responsible for the overall framework, policy formation and for interactions with third parties. An Experts Group (EC) is advising the Policy Group on R&D strategy, priorities and methodology, and on evaluating research plans for each Generation IV system. Under the Policy Group, there are six System Steering Committees (SSC) to implement the research and development for each Generation IV reactor concept selected in the GIF IV Technology Road Map (Ref. [1]), with participation by GIF Members interested in contributing to collaborative R&D. Each SSC plans and integrates R&D projects contributing to the design of a given system. Since January 2005, the OECD's Nuclear Energy Agency has been providing Technical Secretariat support for the GIF. The GIF governance structure is illustrated in Fig. I.1.

The GIF charter envisions the safety, reliability, physical protection and proliferation-resistance among the essential priorities in the development of next-generation systems. Accordingly, the Policy Group has recognized the need to establish Methodology Working Groups with the aim to address more specifically approaches to be adapted to safety, economics, physical protection and proliferation resistance in the context of R&D planning, in particular[2]:

- the Risk and Safety Working Group (RSWG),
- the Economic Methodology Working Group (EMWG), and
- the Proliferation Resistance & Physical Protection Working Group (PR&PPWG).

[2] In 2020, the Education and Training Task Force is also elevated to a Working Group status

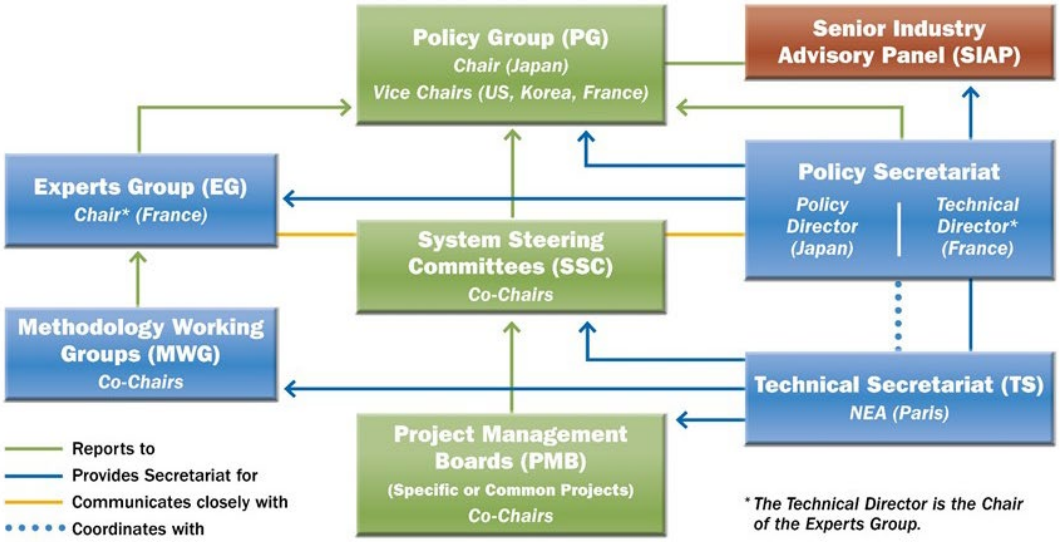


Fig. I.1—Generation IV International Forum (GIF) governance structure

The primary objective of the RSWG is the implementation of a harmonized approach on safety, and to address risk and regulatory issues in development of the next generation systems. To this end, the RSWG focuses particularly on proposing safety goals and evaluation methodology as well as advising and assisting the Experts Group and Policy Group on interactions with the nuclear safety regulatory community, and other relevant stakeholders including IAEA and OECD/NEA's Working Group on Advanced Reactor Safety (WGSAR). Concerning the relationships with the developers and the designers, functional interfaces with the System Steering Committees (SSCs) have been established in order to help check the pertinence of the R&D already defined within the System Research Plans, to help identify complementary themes and items, and to provide consultative support to the safety related system assessment.

In parallel, the PR&PP Working Group's goal is to develop an improve evaluation methodology to assess Generation IV nuclear energy systems with respect to PR&PP. Following its charter, the RSWG interacts with the PR&PP Working Group to assure a mutual understanding of safety, security and safeguard priorities and their implementation in both the PR&PPWG and RSWG evaluation methodologies.

I.2 Objectives of the report

The primary objective of this report is to discuss GIF safety goals, safety principles and evaluation methodology of the next generation systems. It is intended to motivate the need for an innovative safety approach and provide the foundations for such an approach with support of RSWG's integrated safety assessment methodology.

In the aftermath of Fukushima Dai-Ichi accident, the new mission for developers of Generation IV reactors is to identify areas for enhancement, achieve their implementation, and demonstrate their effectiveness. The approach proposed in this updated report remains to be strengthening the implementation of defence in depth, increasing the robustness and transparency of the safety demonstration, and continually improving the safety culture. In qualitative terms, this approach can be fulfilled through assuring the independence of the DiD levels, better defining the allowable off-site response measures to keep radioactivity releases limited in time and in

area, demonstration of the design robustness against cliff edge effects, practical elimination of event or sequences that could lead to early or large releases, and making the safety architecture exhaustive, progressive, tolerant, forgiving and balanced. In quantitative terms, tightening of risk space and probabilistic targets is recommended for the prevention and management of severe accidents, consideration of natural hazards exceeding the design basis, and treatment of the events, conditions or sequences that are practically eliminated.

I.3 Scope and Structure of the Report

This report contains integrated considerations of RSWG to achieve and demonstrate the improved safety potential of future reactor systems. It emphasizes the need for a technology neutral approach capable of addressing the issues of all the Generation IV systems, i.e. for their design and their assessment. In Chapter II, the purpose of the RSWG is discussed along with the major elements of RSWG Terms of Reference, objectives and goals. It also includes discussion of the membership of the RSWG, interfaces with other GIF IV bodies, in particular with the Policy Group, and other external organizations.

Chapter III proposes a Generation IV safety philosophy. It recalls and discusses the key safety goals as contained in the GIF IV Technology Roadmap, in particular the need for excellent operational safety and reliability, very low likelihood and degree of reactor core damage, and reduced (or eliminated) technical needs for off-site emergency response. The potential for safety improvements and the need for an innovative approach for design and assessment of GIF IV systems is emphasised. Main safety principles and characteristics that are desirable for Generation IV designs, such as defence in depth, risk informed design, reduced reliance on human actions to mitigate off-normal conditions, etc., are identified and commented.

Practical steps for the design and the assessment of innovative systems are commented in Chapter IV. The introductory part briefly summarises and discusses the major Generation IV concepts. The key point is on how differences between Generation IV systems and current designs result in a need to re-examine approaches to safety. Relevant differences between the current and historical approaches to safety, compared to new approaches needed for Generation IV designs are also mentioned, including discussion of the concept of minimization or elimination of some accident scenarios, of the safety margins concept as a response to uncertainties, etc.

In Chapter V, an overview of RSWG's Integrated Safety Assessment Methodology is provided with brief description of its components that include, qualitative safety features review, phenomena identification and ranking table, objective provision tree, and deterministic, phenomenological, and probabilistic safety assessments.

In Chapter VI future activities of the RSWG are presented such as further revisions of the objectives, the principles, and the tools presented in this document to achieve a technology neutral general framework for the Generation IV assessment, the test and the demonstration of the applicability of the framework, and finally the proposal of necessary crosscutting safety related R&D. The possible interactions with the System Steering Committees (SSCs) are also discussed.

In appendices, additional considerations are given to the concept of optimal risk reduction (ALARP), an improved implementation of defence-in-depth principle, and concepts of the Objective Provision Tree (OPT) and the Line of Protection (LOP), the principle of "practical

elimination" including considerations of the attributes and characteristics of the selected technological systems as they affect issues associated with safety. In addition, a concept of safety margins and uncertainties, examples of application of OPT and PSA methodologies and R&D for the homogenization of the safety architecture's design and assessment design & assessment methodologies, in particular their content and implementation, severe plant conditions management, and safety and reliability for systems implementing specific processes are also briefly discussed.

While the scope of the RSWG includes the entire nuclear fuel cycle, this report deals only with reactor technology. Issues associated with non-reactor facilities and processes are not addressed here and will be addressed in future RSWG work and documents. Similarly, apart from some consideration of commonalities, this report does not deal with PR& PP issues in GIF reactor systems as the PR&PPWG is preparing its own documents addressing these issues.

Chapter II: Risk and Safety Working Group Charter and Objectives

II.1 The GIF Risk and Safety Working Group

The RSWG is comprised of representatives nominated by the GIF member states. The RSWG also includes experts from SSCs, PR&PP working group, and external organizations such as IAEA as resource for advice and resolution of specific tasks. The RSWG currently has three co-chairs nominated by the representatives and approved by the PG. The co-chairs are responsible for organizing work and preparing reports or presentations summarizing RSWG advices and recommendations.

According the Terms of Reference, the RSWG meets at least annually, but in recent practice it is twice per year. The interface to the SSCs is assured through assignment of each co-chair to two specific SSCs. One of the co-chairs participates in meetings of the EG and PG to inform them on current RSWG activities, its strategic views and advises on the approach to safety and risk issues related to next generation systems. The co-chairs also maintain an active interface with the IAEA (which participates as an observer in the RSWG), and other international organizations such as WGSAR that focuses on regulation of the Generation IV systems.

II.2 RSWG Terms of Reference

The revised RSWG Terms of Reference (December 2014) specify the following RSWG scope of work:

- *Continue the development of white papers on the application of ISAM in collaboration with the six reactor System Steering Committees (SSCs) focusing on the safety aspects.*
- *Implement the safety assessment on six systems to review and identify the main safety advantages and challenges with the aim of providing a snapshot of the major safety concerns.*
- *Continue to monitor and interpret the lessons learnt from TEPCO's Fukushima Daiichi Nuclear Power Plants accident and to evaluate those lessons for their applicability and implications for Gen IV systems.*
- *In the longer term, the activities and work of the RSWG will also include the following:*
- *Identify and promote a common and consistent risk-informed approach to safety in the design of Gen IV systems by:*
    - *proposing safety principles, objectives and attributes based on the Gen IV safety goals to guide R&D plans;*
    - *proposing a technology-neutral general framework of technical safety criteria and assessment methodologies;*
    - *testing and demonstrating the applicability of the framework and assessment methodologies;*
    - *proposing necessary crosscutting safety related R&D.*
- *Provide consultative support on matters related to safety to SSCs and other Gen IV entities which develop specific concepts and designs;*

- *Advise the EG and the PG on the application of the safety approach for Gen IV systems;*
- *Promote development of a Gen IV safety database;*
- *Interact with the PR&PP Working Group to assure a mutual understanding of safety priorities and their implementation in PRPP and RSWG evaluation methodologies;*
- *Undertake appropriate interactions with regulators, IAEA and relevant stakeholders, primarily for the purpose of understanding and communicating regulatory insights to the Gen IV development;*
- *Report annually to the EG on status and progress of the activities including the work plan for the following years.*

Concerning the relationships with the developers and the designers (i.e. the SSCs, including the System Integration & Assessment (SI&A) Projects and the other PMBs), it is expected that the availability of a common agreed safety approach will provide essential insights on the Generation IV R&D. Strong interactions have to be implemented with the SSCs, SI&A & PMBs in order to check the pertinence of the R&D already defined within the system research plans, to identify complementary themes & items and to help system assessment.

Concerning the interactions with the regulators, it is worth noting that the initial PG dialogue with senior nuclear safety regulators has highlighted the potential benefits of early exchanges and mutual understanding regarding safety goals adopted for R&D plans. In particular, a need has been identified to explore the potential of risk-informed, technology-neutral regulatory approaches to licensing of advanced designs. Also, with the further development of system R&D plans, a need emerges for clarifying standards to be adopted for quality management, as well as to define the relationship of quality assurance (QA) with safety goals.

II.3 RSWG meetings

The scope of the RSWG work is demanding and involve difficult questions like “how safe is safe enough”. While recognizing that the answer to this question is of the responsibility of the national safety authorities, the discussions lead to a number of other issues such as:

- the content of a cohesive safety philosophy applicable to all the Generation IV systems,
- the objectives and the ways to meet the potential safety improvements,
- the basic principles of an approach applicable to the design and the assessment of innovative systems including the ways to assess the adequacy of the defence in depth to address the treatment of severe plant conditions,
- the role of passive design features, and
- the possible role of available design and safety assessment methodologies and the need for developing innovative indicators and tools.

The following chapters detail the results of the discussions and indicate the RSWG’s suggestions.

Other issues are still open for discussion and resolution, e.g.:

- a common understanding of undesirable end states (for example core melt) for different reactor systems and their practical elimination,
- an agreed way for the integration of the security and safeguard considerations,

- an agreed approach to address internal and external hazards in a consistent way,
- an agreed and detailed complementary use of deterministic and probabilistic assessment methods,
- the identification of specific rules for the detailed design and the assessment of the design extension conditions that could lead to severe plant conditions, and
- the identification of a clear path forward on how to define QA standards.

The development of advanced safety assessment methodologies (e.g. risk-informed approach), is an evolving process and currently being pursued in collaborations with WGSAR.

Chapter III: Generation IV Safety Philosophy

III.1 Goals for Generation IV

As part of the recently updated Generation IV Technology Roadmap (Ref.[1]), representatives of the Generation IV International Forum developed general goals for future nuclear energy systems. Eight goals for Generation IV were defined in the four broad areas of sustainability, economics, safety and reliability, and proliferation resistance and physical protection:

- Resource utilization
- Waste minimization
- Reduced life-cycle costs
- Reduced risk to capital investments
- Improved operational safety and reliability
- Reduced likelihood and degree of core damage
- Elimination of the need for off-site emergency response
- Enhanced proliferation resistance and physical protection

Among these goals, improved safety and reliability is recognized as an essential priority in the development and operation of nuclear energy systems. Nuclear energy systems must be designed so that during normal operation or anticipated transients, the safety margins are adequate, accidents are prevented, and off-normal situations do not deteriorate into severe plant conditions.

Safety and reliability of the future generation of reactor designs are addressed in the Technology Roadmap by following specific goals:

1. **Generation IV nuclear energy systems will excel in operational safety and reliability.** The focus of this goal applies to safety and reliability during normal operation of all facilities employed in the nuclear fuel cycle, and thus, deals with the relatively likely kinds of operational events that set the forced outage rate, determine worker safety, and result in routine emissions that could affect workers or the public.

2. **Generation IV nuclear energy systems will have a very low likelihood and degree of reactor core damage.** This goal calls for design features that create high confidence that the possibility of core damage accidents will be very small for Generation IV reactors. The goal deals with both minimizing the frequency of initiating events, and introducing design provisions to ensure that the plants can successfully control and mitigate the consequences of accidents causing core damage. For accidents that do not lead to a severe accident, the design aims to ensure that the radiological consequences shall not lead to the need to implement measures to protect populations.

3. **Generation IV nuclear energy systems will eliminate the need for offsite emergency response.** It is desirable that Generation IV systems demonstrate, with high confidence, the capability of the safety architecture to manage and mitigate the consequences of severe plant conditions so that any potential releases of radiation will be small and have only insignificant public health consequences. Two cases have to be considered to fulfil this ambitious objective:

a. In the case of a severe accident, the objective is to have very low releases such that no off-site measures are necessary. If measures are nevertheless necessary (e.g., restrictions on consumption on a crop), they shall be limited in time and space with sufficient time for their implementation. Even temporary evacuation of populations should not be necessary and only sheltering, limited in time and space, shall be envisaged.
b. Accidents likely to lead to very large off-site radioactive releases, or with kinetics that would not allow for the timely implementation of necessary measures to protect populations, shall be rendered physically impossible or, failing that, extremely unlikely with a high degree of confidence (practical elimination).

To this purpose it is interesting to point out that Generation IV goals are defined as *"to stimulate the search for innovative nuclear energy systems both for the reactors and the fuel cycle installations and it will serve to motivate and guide the R&D on Generation IV systems as collaborative efforts get underway."* These goals continue the past trend and seek simplified designs that are safe, and further reduce the potential for severe plant conditions and minimize their consequences. The achievement of these ambitious goals cannot rely only upon technical improvements, but will also require systematic consideration of human performance as a major contributor to the plant availability, reliability, inspectability, and maintainability.

Since the proliferation resistance and physical protection are also essential priorities in the expanding role of nuclear energy systems, identifying safety and security interfaces and establishing common design principles/features that improve both the plant safety and security are also a common RSWG and PR&PP working group goals.

III.2 A Cohesive Safety Philosophy

As a starting point, the RSWG recognizes that the level of safety that has been attained by the vast majority of operating nuclear power plants in most countries is already very good. Moreover, the safety objectives applicable to the reactors of the third generation (e.g. AP1000 and EPR) are already very ambitious and guarantee a very high level of protection reducing the level of risk in a demonstrable way.

Further, the nuclear industry and regulators have shown themselves to be very effective in incorporating operating experience that has been gained through decades of operations. While much of the experience that has been gained in nearly 50 years of commercial reactor design and operation will be very helpful in ensuring the safety of Generation IV technology, most of that experience is applicable specifically, but not exclusively, to light water reactor technology. The diversity of technologies that represent Generation IV systems require new thinking and new methods, using a proven staged approach. The RSWG believes that, through advanced technology and the early application of a cohesive safety philosophy, it is worthwhile and achievable to further improve on what is already a very safe source of clean and reliable energy. Although measurable safety improvements might be achieved in a number of different ways, the RSWG believes that one of the most important fundamental means lies in the concept of safety that is "built-in, not added-on." By this, we mean that Generation IV designs are developed from the earliest stages in a way that is guided by insights that are derived, e.g., from PSA and other formal safety assessment methods. The result is a robust design, free of dominant vulnerabilities, and for which no safety-related "add-ons" are necessary to achieve a

desired level of safety.

More so than it has been done for the existing plants (Generation II and III), for the Generation IV it will be necessary to further develop and apply analysis methods that will allow designers to anticipate the wide range of operational challenges that might occur in a plant, and to design for that range of events. The process for identification of the risks that can challenge the fundamental safety functions must be comprehensive and exhaustive. **Reliance on the definition of a bounding accident scenario will no longer be a recommended practice for future reactors.** Rather, the specification of a range of different types of design basis accidents and design extension condition will be the preferred approach. The identification of these scenarios, retained to design and size the safety architecture provisions, must be as exhaustive as possible: the lack in the exhaustiveness of the scenarios being covered by the notion of envelope situations and, more generally, by the full implementation of the defence in depth principles.

The RSWG believes that an optimally effective approach to ensuring the safety of Generation IV nuclear facilities and systems must be based on a well-developed safety philosophy that applies to both design and operation. Such a safety philosophy must be much more than just a collection of prescriptive design requirements. In fact, it is preferred that the safety philosophy not be prescriptive in nature at all, but rather should articulate the desired objectives and principles applicable to achieve a safe Generation IV design.

The safety philosophy must set forth an integrated set of principles that are derived from an explicit understanding of the safety outcomes that must be achieved, and the good practices that will help to achieve those outcomes over a full range of potential operational challenges to which the facility might be subjected during its operating life.

A significant body of good work that articulates much good thinking about safety philosophy already exists. Notable examples include work performed and documented by the IAEA, various national regulatory bodies, and others. The RSWG recognized early on that it would not be necessary to recreate all of this work, but rather, to draw upon it to the extent possible in formulating a safety philosophy that could be applied to Generation IV reactors. The purpose of this chapter is to present the thoughts of the RSWG as they relate to the articulation of such a safety philosophy.

III.3 Potential for Safety Improvements

One of the most difficult questions associated with the safety of any complex technology that has the potential, although very small, for being the source of accidents that might result in significant loss or damage, is the question of "how safe is safe enough." The RSWG devoted considerable time to the discussion of this topic. Some of that discussion focused on the question of whether or not Generation IV power plant designs should be encouraged or required to meet specific quantitative safety goals. Ultimately, the RSWG came to the conclusion that setting quantitative safety goals, particularly as conditions for licensing, is the domain of regulatory organizations in the respective GIF countries. Thus, the RSWG prefers not to set forth any further specific quantitative recommendation on this matter.

It is proposed that the probabilistic objective of core melt accident prevention is kept identical to that retained for the Generation III pressurized water reactors (i.e., 10^{-5} per year). An additional prescriptive reduction of core damage frequency is not justified and could even be

counterproductive. Indeed, the current probabilistic objectives are already ambitious and reach the limits in terms of representativeness and confidence. In fact, the hardening of the probabilistic objectives for the already highly unlikely events could increase the complexity of the installation and its operation, thus reducing its safety on a daily basis, for a marginal gain in terms of severe accident probability.

This probabilistic objective can be used for comparative purposes, but it should not be used as an absolute value for acceptance of the design. For Generation IV reactors, for which a limited experience feedback is available, the safety demonstration will rely primarily on deterministic methods to cover the levels of defence in depth and to extend the prevention and mitigation of the core melt accidents. Probabilistic methods, when relevant, will provide additional insights.

As a fundamental tenet, the RSWG believes that safety must be designed into Generation IV technology rather than added onto a basic, mature design through the addition of engineered safety features or backfits intended to reduce vulnerabilities that should have been recognized and eliminated in earlier phases of the design. Potential safety improvements, beyond those already incorporated in existing nuclear power plants, should simultaneously include consideration of the following elements: the notion of "optimal risk reduction" (ALARP); the consideration of ambitious objectives; incorporation of innovative technologies; an emphasis on prevention backed up by mitigation; the search for robust safety architecture; and finally, the requirement for the improvement of safety demonstration's robustness.

- **The concept of "optimal risk reduction"** (ALARP[3])
  The concept of "optimal risk reduction" is one that should be reflected in the design and operation of Generation IV systems. By this the RSWG means that the level of risk should be reduced to the extent that is possible in a way that is consistent with available technology, cost-benefit analyses, and other considerations that define what level of safety is both "reasonable" and "achievable." Integration of credible and reliable insights derived from probabilistic safety analysis throughout the design process is the key to doing this effectively. The Appendix 1 discusses further the "domain of risk" and the concept of "optimal risk reduction".

- **The consideration of ambitious objectives**
  The consideration of ambitious goals for safety improvement, even if qualitative, is essential to stimulate research that will result in an even higher level of safety than already exists in operating nuclear power plants. On the other side, as already indicated, when compared with Generation II concepts, the safety objectives applicable to the reactors of the third generation are already very ambitious and guarantee a very high level of protection reducing the level of risk in a demonstrable way, perhaps by about an order of magnitude. The RSWG considers that these objectives can be kept – as a minimum - for the Generation IV systems. The RSWG believes however that, by exploiting progress in knowledge and technologies, further improvements are both achievable and desirable in the Generation IV technology. Meanwhile, it is agreed that searching for further improvement is nevertheless justified by the opportunity of looking for innovative systems, but that complementary requirements are to be considered only if they can bring a real and demonstrable benefit.

[3] ALARP stands for "As Low As Reasonably Practicable", and is a term often used in the milieu of safety-critical and high-integrity systems. The ALARP principle is that the residual risk shall be as low as reasonably practicable.

- **The opportunity brought by the innovative technologies**
  Advanced technology holds the promise of significantly reducing the level of risk associated with each new Generation IV plant. Consciously selecting Generation IV concepts, and taking full advantage of the safety characteristics brought by progressing knowledge and advanced technology, is consistent with the ALARP principle, and should be an explicit goal of Generation IV. As an overall goal, it may be feasible to consider significantly increase the number of operating reactors around the world without significantly increasing the currently negligible level of societal risk incurred by exposure to this technology.

- **The emphasis on prevention backed up by mitigation**
  Focusing on the principles that will result in further improvements in reactor safety should be preferred over achieving a significant reduction in a selected fundamental risk metric. For example, it may be more desirable to effectively eliminate accident sequences that might have the potential for offsite releases of radionuclides than it is to make substantial improvements in containment performance.

- **The search for robust safety architecture**
  The objective is the implementation of a robust safety related architecture which merges the full set of 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. Looking for the robustness of this architecture means that there would be an effort for the implementation of the needed provisions following and fully fitting the principles of the defence in depth (DiD). The latter is recognized as a fundamental principle the application of which has to be improved by, e.g.: the consideration of the internal initiators and the external hazards in a consistent way; the implementation of provisions with a logic which answers the notion of independent and successive DiD levels; the consideration of the physical protection issues; the consideration of “severe plant conditions”; the integration of the notion of "practical elimination" which will require adequate demonstration.

- **Extremely Reliable Plant Systems**

  High reliability of plant systems may be achievable in a number of different ways. Some of these potentially include use of new materials, improved maintenance practices, on-line condition monitoring and prognostics, among others. Of particular promise in terms of improving reliability, is the increased use of “passive design features” and other inherently safe design provisions, such as gravity, natural convection, conduction, negative reactivity feedback, thermal inertia, and other intrinsic physical processes. The ultimate expression of safety philosophy in Generation IV designs would be the reactor systems that exhibit “fail safe behaviour” in their design. The conviction of the RSWG is that, while achieving such a level of passive and inherent safety may be very challenging, the implementation of passive and inherent safety provisions remains a desirable goal from a safety point of view if it is proved successful in efficiency, reliability, availability and balance between cost and productivity.

- **Reduced Reliance on Human Intervention**
  Generation IV designs should represent a significant step forward in terms of being

increasingly "error tolerant" and in terms of providing the means by which the operator's job becomes simpler and less involved, especially during critical phases of responding to off-normal conditions. It is expected that some of the Generation IV systems will exhibit more advanced instrumentation and control technology than currently operating plants do. This instrumentation and control will be important to the success of these specific Generation IV systems for a number of reasons such as reduced operating and capital costs, and overall improved plant availability. For other Generation IV systems that do not require reliance on advanced instrumentation and control technology, inherent and passive safety features will result in reduced reliance on human intervention in the event of a safety challenge to the plant. Through improved plant automation and/or reliance on inherent/passive design features, Generation IV systems could seek to minimize the need for human actions during critical phases of postulated accident conditions, but would also provide a long grace period and allow the trained operators to intervene in situations in which their unique cognitive abilities and creativity may be beneficial. In short, Generation IV systems would seek to retain the most positive aspects of the human-machine interface, but to minimize the possibility for human errors.

- **The requirement for the improvement of safety demonstration's robustness**
  The implementation of a "robust" demonstration rests on the designer and the developer to assure the capability of the plant to successfully respond to a broad range of hypothetical challenges without a realistic threat of releasing radionuclides to the environment. Thus, designers are required – as far as feasible – to master the exhaustiveness in addressing the risk generated by the process and the plant and in selecting the phenomena (events, situations) to be considered in the design of the Generation IV systems. The latter has to be done for the various stages of their life. The adequate treatment of these events and situations, through technical solutions and through organization, has to be proved bringing the confidence in the selected options. In particular, this is based on the search for options able to ensure a favourable intuitive plant behaviours. This has to be, as far as possible, based on natural phenomena; the analyst could so guarantee the progression with an adequate degree of confidence, the mastery of the associated uncertainties or the consideration of sufficient margins and the minimization of the impact of the human factor.

III.4 Re-examination of the Approach to Safety

In parallel with the potential for safety improvements through the consideration of the elements as they are described within the previous section, there is a need to re-examine the approach which, as suggested in Ref. [2], fit with other criteria, in particular:

"The fundamental objective of the safety approach is to provide, through the identification of a comprehensive set of technology-neutral requirements, the process used by designers, operating organizations, and regulators in the design, construction, operation and safety assessment of innovative reactors to ensure nuclear safety."

A set of characteristics (or principles) are proposed to determine whether the safety approach has met its purpose. The main characteristics of the safety approach should be:

- **Risk-informed.** A complementary approach should be used that combines both

deterministic and probabilistic information into the decision making process[4].

- **Understandable, traceable, and reproducible**. The criteria and guidance developed as part of this approach should have a clearly stated basis, and therefore, each step of the process should be identified and clearly described.
- **Defensible**. Whenever possible, known technology should be used to develop the technical basis so that necessary assumptions and approximations and their impacts are known and understood.
- **Flexible**. New information, knowledge, research results etc., should be incorporated, in an efficient and effective manner, by appropriate changes and modifications to the safety approach, the technical bases and the safety requirements.
- **Performance-based**. Where justified, the safety approach, technical bases, and safety requirements should be goal setting and performance based to the extent practical, rather than being prescriptive.

Moreover, the details of this innovative approach have to be defined keeping the coherence with the following criteria:

- agreement with current and the - foreseen - future regulations,
- ability to prove the full implementation of the defence in depth: prevention, detection and control of the abnormal situations, mastery of the accidents, management of severe plant conditions and mitigation of their consequences, and potential off-site measures,
- allowing for the installation's design / analysis to manage simultaneously deterministic practices and probabilistic objectives
- ability to handle internal and external hazards so as to achieve, as much as possible, the coherency with the approach adopted for internal events, i.e. in guaranteeing a common global treatment,
- allowing to improve the safety demonstration for the domains where gaps still exist in the current state of art, and
- allowing the demonstration of the achievement of a level of safety equivalent or even better with regard to the current Generation III systems.

The adoption of these criteria should, on one hand, guarantee that all the Generation IV designs will answer a set of coherent principles and, on the other hand, will help defining the necessary crosscut and specific R&D to validate the choice of the innovative options selected for these designs. Ultimately, such an approach allows guaranteeing that the Generation IV systems which meet these technology neutral safety requirements are suitable for setting up the discussions with the regulators for licensing.

III.5 Lessons learnt from the Fukushima accident

In 2011 the accident of Fukushima Daiichi represented a solution of continuity for the work of safety improvement. Immediately after the accident specific activities were launched with the objective to synthetize the lessons learned and to provide indications (requirements and recommendations) applicable for the updating of nuclear installations in operation and / or for

[4] The term "Risk-informed" is linked to the USA practice and the understanding can be different in other GIF countries. For the moment it seems interesting not to be excessively restrictive. The basic idea is to build a safety approach based on analysis of risks where the probabilistic insights are used to assess the credibility of these risks while keeping the Defence in Depth as foundation to build the safety architecture.

the design and the assessment of future nuclear installations. Significant changes concern, in particular, the management of the severe accidents and the taking into account of natural hazards of external origin.

The natural external hazards considered in the design have to be adequately defined. Additionally, the combination of hazards has also to be assessed (e.g., combination of earthquake and flooding). Then, the consequences of more severe natural external hazards has to be assessed in a design extension domain. The Fukushima accident has shown that, because of the occurrence of external hazard with a magnitude beyond the one considered in the design basis, multiple failures may occur inside a given plant, or simultaneously in different plants located in the nuclear site, or outside the nuclear site.

For natural external hazards in the design extension domain, sufficient design margins should be provided to prevent a cliff-edge effect in terms of off-site radiological consequences. The installation must be autonomous for a period compatible with the time required for the implementation of the intervention means, in particular with regard to its electricity supply. It should be taken into account that natural hazards may simultaneously affect reactors and storage locations of the entire site.

The main issues to make the plant more robust in regard to natural hazards are as follows:

- Ensure the presence of sufficient design margins on the equipment needed to avoid the cliff-edge effects in terms of off-site radiological consequences, for natural hazards more severe than those taken into account in the design reference domain of the plant;
- Develop a significant autonomy of the installation, with regard to the duration necessary for intervention;
- Develop the provisions allowing the implementation of internal or external emergency measures on the degraded plant.

In general, for Generation IV reactors, the objectives are similar to those of Generation III reactors. These lessons are taken into account from the early stages of design, with due considerations for the specificities of the concept (e.g., by enhancing passive capabilities). Several of these activities are still underway but intermediate results are available. The lessons learned from the accident include:

- Re-examination of external hazards to consider that some events, in particular the natural hazards, cannot be defined precisely and that has to be considered in the design of future reactors;
- Robustness of the electrical systems and ultimate heat sink;
- Independence of prevention/mitigation measures in DiD levels;
- Increased emphasis on common cause and common mode failures;
- Protection of spent fuel in storage pools;
- Multi-unit sites and other nuclear/non-nuclear facilities;
- Accident management and control;
- Improved off-site emergency response;
- Improved safety culture.

The top-tier safety objectives (IAEA, BSA) were confirmed but the implementation of the (material and immaterial) safety provisions, to achieve the safety objectives, have been better

detailed, and the required demonstration process of the safety level has been revised to ensure greater robustness. Despite the different sources, the key messages derived from the analysis of the contributions of the different international organizations and regulatory organizations are perfectly consistent. These key messages can be structured following a set of main themes:

- Strengthening the prevention of unacceptable radiological consequences to the public and the environment;
- Avoidance of long term off site contamination through severe accident mitigation;
- Prevention of severe accident through strengthening the plant design basis;
- Scope of the safety assessment;
- Scope of the safety analysis;
- Assessment of defence in depth;
- Maintenance of the safety assessment.
- Periodic safety review;
- Emergency preparedness;
- Accident management;
- Knowledge on internal and external hazards;
- Feedback from operating experience;
- Continued safety research;
- Harmonization safety–security.

These themes have been developed and, as needed, completed, indicating the correspondence with the content of the different references. It is interesting to point out that the integration and the synthesis of the inputs provided by the different international organizations appears to be more exhaustive than the indications provided, singularly, by these organizations. Table 1 summarizes the mutual interdependence between the different items; it appears that six main topics can help to resume the whole set of essential insights.

Essential Top Tier Recommendations and Requirements – Synthesis	**Complementary requirements**			
1. ***Strengthening the prevention of unacceptable radiological consequences to the public and the environment***	• *Emergency preparedness*	*Feedback from operating experience* •	Continued safety research •	Harmonization safety - security •
2. Avoidance of long term off site contamination through severe accident mitigation - (Severe accident mitigation)	• *Accident management*			
3. Prevention of severe accident through strengthening the plant design basis	• *Fire safety*			
4. Scope of the safety assessment,				
5. Scope of the safety analysis				
6. Assessment of defence in depth	• *Maintenance of the safety assessment;* • *Periodic safety review*			

Table 1: Synthesis for the recommendations and requirements for safety approach update

III.6 Main Safety Principles for Generation IV Systems

The principles that should define an effective safety basis for Generation IV systems are, in part, based on effective practices and lessons learned from the current generation of nuclear power plants, and in part from deliberative thinking about the nature of Generation IV concepts and the special considerations that may be applicable to them. Much of the work of the RSWG has been focused on identifying these principles and discussing the ways in which these principles may be applicable to the various Generation IV concepts. It should be emphasized that this is a work in progress, and as Generation IV conceptual designs continue to evolve, the specifics of how these principles should apply themselves in the various concepts similarly evolve. The important principles that the RSWG believes must be embodied in Generation IV technology include those discussed below.

III.6.1 Defence in Depth (DiD)

The concept of defence in depth is one that seems to be universally accepted as the most basic and most effective safety principle of all. It is clear that the concept of defence in depth must remain central to the safety basis of Generation IV systems. Much has been written about the concept of defence in depth (Ref. [3]), and no attempt to exhaustively discuss the topic will be made here. However, some important points about the concept and its applicability to Generation IV systems are recalled in order to fix a commonly agreed RSWG vision.

The concept of defence in depth is recognized worldwide as an effective way of ensuring the safety of nuclear power plants and other nuclear facilities. The concept has been defined in a number of different ways. Common to all definitions, however, is the notion that a safe design involves overlapping layers of safety and multiple barriers, such that if one safety provision should fail, another will be available to prevent unacceptable damage from occurring. The idea of defence in depth is manifested in various ways in modern nuclear power plants. Some of these familiar ways include redundancy and diversity in design, intentional safety margin or "over-design" of certain plant features, multiple barriers that perform mitigative functions for different phases of a postulated accident progression, and others.

Fundamentally, defence in depth is a rational response to uncertainties associated with the design construction and operation of a nuclear power plant. Limited uncertainties exist on many levels, even for nuclear power plant designs that have operated for many years. Just a few of these uncertainties include those associated with initiating event frequencies, safety system reliability, human factor, accident phenomenology, containment performance under various conditions, etc. Since nuclear power plant accidents are very rare events, empirical uncertainties exist about how the plant and its safety architecture will actually respond to certain challenges. In part, because of those uncertainties, overlapping levels of safety intentionally provide margin in addition to that which is likely to be needed to respond to a plant upset.

The idea of defence in depth begins with an emphasis on prevention of off-normal conditions that, if not appropriately detected, controlled and mitigated, might initiate a chain of events that would lead to an outcome that is unacceptable from a safety point of view. Various plant design features constitute this "prevention level" of defence. Recognizing that prevention may not eliminate all possible initiating events, a "control, management and mitigation levels" of

defence are fulfilled by plant provisions (e.g. safety systems) that respond to operational challenges in a way that will, with high reliability, arrest the progression of any possible accident sequence.

In some respects, Generation IV designs will present significant new perspectives to the implementation of defence in depth principles. The variety of coolants, fuels and materials, control schemes, core physics, and other aspects of plant design that are represented by the different Generation IV concepts means that defence in depth will be expressed and implemented differently for each concept. However, the basic principle of defence in depth will have to be reflected in each design.

In this context, one specific challenge for Generation IV systems is to develop an approach to defence in depth that is both consistent with the successful practices that have been used in operating reactors, and that makes use of the improved analytical methods to cost-effectively optimize the value of the concept. For Generation IV systems, the goal will be to apply defence in depth in a manner that explicitly takes into consideration uncertainties based on their systematic assessment. The ideal outcome will be a design that optimizes both capital costs and safety by applying defence in depth where it will have the desired effect, but not to "over-design" in a way that adds to cost but not safety.

Given this framework, PSA is recognized as an effective means of identifying accident scenarios that could occur for a particular design and, with the associated assessment tools, as effective means to quantitatively assessing the weight of the uncertainties associated with various aspects of those scenarios. The PSA and the associated tools will also be used to assess the effectiveness of design features and their interaction that may be proposed to provide defence in depth in response to those uncertainties. The setting of a quantitative safety goal stated in probabilistic terms, i.e., frequency limits for consequence levels, enables probabilistic considerations, including success criteria, to be factored into the implementation of defence in depth.

The deterministic and probabilistic considerations are therefore integrated into the comprehensive implementation of defence in depth. The notions of "deterministic success criteria" and "probabilistic success criteria" are suggested to help in providing design provisions to fulfil the requested missions in each DiD level. The performance of these provisions have to be defined in terms of physical performance and required reliability; Depending on their safety significance, these provisions will then have to be adequately safety classified. The final goal of this process is the optimization of the whole safety related architecture in terms of performance, reliability and cost.

The proposals for considering the simultaneous contribution of deterministic approach and probabilistic assessment is detailed and discussed in Appendix 2. The whole process has to remain compatible with the notion of a risk-informed design that incorporates formally developed risk insights from the earliest stages of the design, as discussed later (Section III.5.2).

Other complementary and essential characteristics that help improving the safety level, ensuring the effectiveness of the defence in depth concept, optimising the risk-informed implementation and easing the safety demonstration are:

- An exhaustive defence; i.e., the process for identification of the risks, which leans on the fundamental safety functions, should look for exhaustiveness. Any potential oversight should be compensated by consideration of enveloping situations which are taken into

account independent of their expected occurrence frequency (single failure criterion, margins, postulated combinations, etc.).

- A gradual, progressive defence; without that, "short" sequences can happen for which, downstream from the initiator, the failure of a particular provision entails a major jump in consequences without an opportunity of restoring safe conditions at an intermediate stage[5].
- A tolerant defence; no small deviation of the physical parameters outside the expected range can lead to severe consequences (i.e. rejection of "cliff edge effects").
- A forgiving defence, which guarantee the availability of a sufficient grace period and the possibility of repair during accidental situations.
- 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 (i.e., avoidance of dominant risk contributors).

The application of these principles are expected to lead to an improved safety architecture based on a "simple" design and uncomplicated and reliable operation and robust response in accidental situations.

If well implemented, the concept of defence in depth will allow Generation IV systems to successfully respond to a variety of operational challenges, some of which might not even have been fully anticipated in the design. It should be a goal of Generation IV systems to create designs that exhibit a great deal of robustness in terms of their ability to cope with a wide variety of operational challenges or deviations from normal operation.[6]

In conclusion, the DiD is judged to be the most adequate principle to bring in a convincing and irrefutable way, the proof that the safety demonstration and the architecture of the innovative concepts (i.e. thus having limited feedback experience) have reached the objectives defined for the Generation IV systems.

III.6.2 Risk-Informed Design

Probabilistic safety assessment has become a highly sophisticated tool to identify potential accident scenarios and quantitatively estimate their probabilities of occurrence in a defined time period. When combined with an estimate for the consequences associated with postulated accidents, PSA can also provide risk insights. Along with the traditional deterministic methods, this methodology has come to be widely accepted as one of the bases for ensuring the safety of nuclear power (and increasingly other technologies as well) around the world.

Until recently, PSA was primarily applied after the design was finalized, or even after the plant was built. Applied in this post facto way, PSA was essentially used as a means of measuring the level of risk associated with an operating facility. With the development current

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

[6] To be more specific, it is preferable to develop a design for which the total risk is made up of a larger number of small frequency scenarios than to have that risk dominated by one or two higher frequency scenarios. It is possible to imagine two different designs with the same likelihood of core damage or other risk metric, but with vastly different characteristics in terms of the number and nature of scenarios that make up that total risk. It is generally accepted that an effective design will seek to eliminate any dominant vulnerabilities even when the total plant risk is very low. Designs that exhibit no dominant vulnerabilities reflect the desirable characteristic of balance.

evolutionary plants (Generation III), however, the value of PSA as an important contributor for the design process is recognized. Simultaneously, limitations have to be kept in mind, especially when the PSA techniques are applied to innovative concepts characterized by large uncertainties, lack of reliable data and lack of precise knowledge about provisions, degradation and failure.

Having said that it is recognized that both safety and economics of Generation IV designs can be positively impacted by formally adopting the use of PSA techniques as a design driver throughout the design process to check the meeting of the whole set of objectives and criteria defined for safety architecture of the Generation IV systems (Section III 5.1). Ideally these techniques will be applied from the earliest phases of Generation IV plant design. During the earlier conceptual phases of the design, the associated PSA models will be simple and conceptual as well. These models, however, will be used as a major input to influence the direction of the Generation IV design as it matures and becomes more detailed. As the design evolves, so too, will the PSA model. In this iterative way, the maturing PSA model will both reflect and drive the maturation of the plant design. Substantial potential exists to use this approach to optimize plant safety and capital costs by focusing safety features where they will do the most good, and by eliminating design elements that are unnecessary or marginal to safety.

Nevertheless as a complement to all these considerations, there is general consensus that, when applied to an innovative design, the PSA is a useful, but not sufficient, tool to assess the meeting of the complementary objectives defined for the DiD in future systems: Exhaustiveness, progressiveness, tolerant, forgiveness, balanced, simplicity. Other specific tools such as the Objective Provision Tree (OPT) and the notion of Line of Protection (LOP) can also be used to supplement PSA and help the designer check how the concept fit with the full set of suggested criteria for the DiD improvement while preparing the right implementation of the simplified PSA.

III.6.3 Simulation, Prototyping, and Demonstration

Making use of sophisticated modelling tools and techniques and advanced computing power, modelling and simulation is increasingly being used in the design and evaluation of complex technologies. Prototyping and demonstration systems are expensive and contribute to the long lead time associated with the development of new technologies. Making increased use of modelling and simulation can provide a means of more thoroughly evaluating a candidate design, thereby reducing uncertainties, and improving safety. By focusing attention on those aspects of the design that are most critical to plant safety, development cost is reduced and safety is enhanced, leaving testing and prototyping being used primarily as late-stage verifications of the final design.

The uses of PSA to drive Generation IV design is really just one application of this idea. Similar benefits can also be derived by modelling and simulation applied to reactor physics, thermal hydraulics, fuel performance, materials behaviour, and a number of other issues that are central to reactor design and development.

While modelling and simulation should be used extensively in the development of Generation IV designs, used appropriately, prototyping and demonstration facilities will be needed as well. The overall aim of using modelling and simulation and prototyping is to reduce uncertainties in the design so that resources can be focused where they will be most effective and so the operating plant will be unburdened by unnecessary requirements and regulation. Modelling and

simulation can be an effective way to identify those design ideas that are most promising and to eliminate those that are not. Ultimately, however, the most convincing means of further reducing uncertainties in those concepts that are near actual deployment may be to demonstrate their viability in carefully designed experiments with prototypes. Some have gone so far as to suggest the idea of "licensing by test." In this approach to licensing, experiments in prototypes would be used to demonstrate to the satisfaction of a licensing authority the ability of a design to cope with an assortment of design basis challenges. Each regulatory body will, of course, define their own protocols. It is the recommendation of the RSWG, however, that an effective mix of modelling, simulation, prototyping, and demonstrations can be highly effective in reducing development and deployment time, improving safety, reducing uncertainties, and reducing costs.

Finally, it is important to point out the fact that separate effects test facilities have to be available for tools development and validation and that some integral test facilities will likely be needed to achieve the tools qualification.

Chapter IV: Design and assessment of innovative systems

IV.1. Current plant experience

The design of current evolutionary plants (Generation III) is based on past experience without putting into question the major principles established for the safety architecture. Their safety is mainly achieved in a deterministic way. The probabilistic methods are also employed to identify the conditions to be addressed and the provisions implemented to cope with them. The major sources for the identification of challenges and suitable provisions are current licensing practices and feedback from operational experience.

An ambitious level of safety is aimed and reached for these plants essentially through the extension of the design basis including the consideration of the severe plant conditions in the design. A complement to this approach is the adoption and the robust implementation of the principle of "practical elimination." During the design process, when the risk associated with an initiating event, a sequence or a situation is assessed as unacceptable, further specific provisions are implemented:

- if possible, the initiating event, the sequence or the situation is considered among the plant conditions addressed and managed by the design;
- otherwise the initiating event, the sequence or the situation is practically eliminated by showing, with a robust demonstration, that the corresponding risk is reduced to a level that it can be excluded from the plant states considered in the design.

The latter are considered as the Residual Risk (RR) events (see Section IV.3.5 and Appendix 4).

The plant conditions that are considered in the design are conventionally subdivided into two categories:

- Design Basis Conditions (DBC)[7]
- Design Extension Conditions (DEC)[8].

The deterministic approach has been implemented for past and current plants for design and analysis purposes mainly related to the DBC based on conservative engineering rules and conservative assessment techniques. As a complement to this deterministic approach, probabilistic insights are considered for the DBC through the sub-categorization of initiating events in separate categories roughly defined by frequency ranges; this categorization leads to consideration of accidents with frequency of occurrence higher than about 10^{-4} per reactor year. Several categories are conventionally defined, and allowable consequences are specified for each of these categories by national regulators.

The probabilistic approach is based upon the systematic consideration and combination of initiating events – each with their own frequency of occurrence – and the failure frequencies of the provisions set-up to cope with these events. The results from probabilistic analyses, generally obtained with realistic conditions and best estimate data, are applied for DEC safety assessment to check the adequate protection against the most unlikely events and sequences. Specific attention has to be focused on hazards that are conventionally treated separately

[7] Design Basis Conditions (DBC): Normal Operation, Incident and Accident Conditions (i.e. design basis accidents) of internal origin for which the plant is designed according to established design criteria and conservative methodology.
[8] 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.

(internal and external hazards like fires, flood or earthquakes); this has to be done considering that looking for an improved robustness of the safety demonstration means, among others, to search for a more coherent approach to the treatment of these hazards when compared with the treatment adopted for internal events.

IV.2. Generation IV systems: A need for re-examining the safety approach

The Appendix 5 shows the main characteristics of the Generation IV systems. The systems selected by GIF shows a large variety of technologies as well as issues and options to address their unique safety characteristics. This variety justifies the implementation of a re-examined safety approach for their design and assessment. Chapter III recalls the general safety objectives, the principles the designs have to satisfy, and the good practices the designers have to implement. The rationale being the establishment of technology neutral safety requirements applicable to the design of all Generation IV systems, the key elements of the potential for safety improvement and the top tier characteristic for an updated "risk informed" approach (i.e. considering both deterministic and probabilistic methods) is justified. Ultimately such an approach can assure that the Generation IV systems meeting these technology neutral safety requirements are suitable for deployment.

IV.3. Design of innovative systems

IV.3.1 Objectives and ways for the design improvement

The desired characteristics of an adequate safety approach for the Generation IV systems are risk-informed; understandable, traceable, and reproducible; defensible; flexible; and performance-based. Complementary criteria are: Agreement with current and the - foreseen - future regulations; full implementation of the defence in depth; capability to manage simultaneously deterministic practices and probabilistic objectives; handling of hazards and of internal events guaranteeing a common global treatment; safety demonstration for the domains where gaps still exist in the current state of art; capability to demonstrate the achievement of a level of safety equivalent or even better with regard to the current systems.

As discussed in Chapter III, the important “boundary conditions” (principles, objectives and criteria) that define an effective “safety basis” for Generation IV systems are also defined as follows: The concept of defence in depth, recognized as an effective way of ensuring the safety of nuclear power plants and other nuclear facilities; complementary objectives for the whole defence (exhaustive, progressive, tolerant, forgiving, balanced) the meeting of which has to lead to an architecture leaning, as much as possible, on a "simple" design and uncomplicated conditions of exploitation in normal and accidental situations; the notion of “risk informed” approach with the complementary role of the PSA and of the complementary tools as the OPT and others (such as LOP); the role of inherent and passive provisions and the conditions for their acceptability: successful in efficiency, reliability, availability and balancing cost and productivity; the role of human factor looking for retaining the most positive contributions, while minimizing the less positive aspects.

For design purposes all these inputs can be summarized as follows:

- full implementation of the defence in depth (i.e. all the levels have to be considered) consideration of the hazards according to the most recent bases and knowledge (PSA, event analysis, combinations with internal events);
- consideration of "physical protection" concerns;

- minimization of the impacts linked to the radioprotection and the environment (effluents & waste); consideration of the actions for the decommissioning;
- implementation of provisions (inherent, passive or active, procedures) dedicated to the robustness of the architecture;
- robustness of the safety demonstration.

To achieve these improvements, four complementary ways may be followed by the designer:

1) Critical examination and consideration of the feedback experience:
   - identification of the crosscut domains which have the potential for improvements: hazards; human factor; digital I&C and software reliability analysis;
   - items specific to each technology (e.g.: Na - water reaction, sodium fires, etc. for the sodium technology) including all the stages of the cycle of life of the systems.

2) Rationalization of the design approach by the deliberate adoption of the ALARP principle (optimal risk reduction) applicable to the full spectrum of design conditions, i.e.: the implementation of innovative provisions looking for further risk reduction (prevention of the initiators and consequences mitigation) on a cost-benefit basis. Application of ALARP should also consider adoption of provisions that represent relevant good practice (which could, for example, help transfer safety provisions across different Generation IV reactor technologies)

3) Reinforced treatment of the severe plant conditions (degraded situations defined on a case by case basis for each concept):
   - identification of provisions for the prevention of the severe plant conditions, i.e. to make highly improbable all the sequences susceptible to lead to unbearable releases in the environment
   - according to the fourth level of the defence in depth, severe plant conditions have to be considered, especially 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) Improvement in the defence in depth implementation, as discussed in Section III.5.1, to achieve an exhaustive defence, a progressive defence; a tolerant defence; a forgiving defence; a well-balanced defence. The application of these principles has to lead to an architecture leaning, as much as possible, on a "simple" design and uncomplicated conditions of exploitation (operation and maintenance) in normal and accidental situations.

IV.3.2. The steps for the design

For innovative systems, the design would be iterative. Around the “reactor process”, which design and performances are defined to fulfil the basic requirements (power level, ranges of operating temperatures, efficiency, potential for fissile creation, potential for waste

management, etc.), a safety related architecture[9] is build up to insure the operability, the availability and the safety of the system (Fig. IV.1).

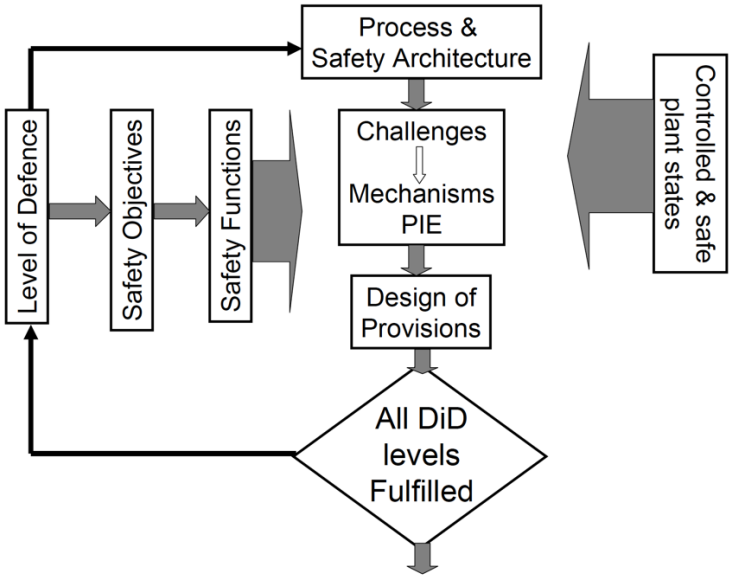


Fig. IV.1– Iterative process for the construction of the safety architecture

Starting from the different safety functions (left side of the Figure IV.1) challenges and mechanisms (initiating events) are identified using for example the Objective Provision Tree (see Appendix 3), to define the conditions the system has to deal with (postulated initiating events - PIE). The implementation of specific provisions to address these postulated initiating events, leads to complementary conditions (possible provisions' failures) that have, in turn, to be considered.

In parallel, the definition of the controlled and safe plant states (which have to be achieved after each abnormal condition) allows defining the missions which are requested and so giving the needed inputs for the provisions' design (right side of the Figure IV.1)). Step by step, for all the level of the defence in depth, all the plausible system's conditions have to be addressed and the needed provisions identified and designed. As a complement to the treatment of these internal events, an improved coherence with the treatment addressing internal and external hazards has to be looked for.

Finally, it is worth recalling that, in regards to severe plant conditions, the organization of the safety design and demonstration, in particular concerning the consideration or the exclusion of given initiators or situations, has to meet the generic objective that states that (see Section IV.1) "single initiating events should be "dealt with" or "excluded"", i.e. :

- For those "dealt with", the proof that the plant can deal with design extension conditions is achieved with specific rules (e.g. best estimate);

- Beside the events taken into account for the design, a limited number of initiators, sequences or situations are "practically eliminated" by showing, with a robust

[9] Recall on Safety architecture: *The full set of 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 the effects.*

demonstration that, through the implementation of specific provisions, the corresponding risk is made, in fine, acceptable. In this case, the initiator, the sequence or the situation are no longer considered for the safety analysis and rejected within the Residual Risk (RR) (see Section IV.3.5 and Appendix 4).

As discussed above (Section IV.1), for current plants the major sources for the identification and selection of safety challenges are current licensing practices and operational experience feedback. The set of initiating events and conditions implemented for current plants (essentially LWR) does not necessarily apply to future systems. Conventional initiators, as for example, the "double ended guillotine break" or the "control rod ejection" as "design basis accidents", are not necessarily applicable to plants with different layouts (integral concepts; internal control rod mechanisms) and different operating conditions (reactor cooling system operating at atmospheric pressure). The experience feedback being not available for these future systems, alternative methods have to be implemented to correctly identify such initiators and conditions, despite their frequency/probability.

Chapter III introduces the principles for new instruments to help this identification, namely the Objective Provision Tree and the notion of Line of Protection (see Appendix 3). Once the architecture defined and represented through the OPT, the mechanisms, as identified, do represent the exhaustive set of plausible initiating events. Concerning these tools it is worth noting that the basic difference with the conventional methods as the FMEA (Failure Modes and Effects Analysis), HACCL (Hazards Analysis Critical Control List) and others, is the explicit link between these initiating events and the corresponding provisions, with the defence in depth and its levels; this can help assessing the coherence of the design with the principles of the defence in depth. Still coherently with this logic, another essential advantage related to this link is represented by the possibility to easily consider, for the design of these provisions, the proper operating and boundary conditions (e. g. the environmental conditions during severe plant conditions).

To help the initiating events/conditions identification and categorization, and following the suggested risk informed approach (i.e. considering both deterministic and probabilistic methods) applicable to future systems, the idea is to create a more explicit link between the defence in depth and the different event categories: DBC, DEC and RR.

A rough approach to connect the two first families of conditions with the principles of the DiD leads to consideration of the DBC as being addressed by the levels 1 to 3 of the DiD (cf. the INSAG 10 terminology in Ref. [3]: *Prevention of abnormal operation and failures > Control of abnormal operation and detection of failures > Control of accidents within the design basis*), and consideration of the DEC as being connected with the level 4 of the DiD (cf. the INSAG 10 terminology: *Prevention of abnormal operation and failures > Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents*). These links allow the definition of probabilistic objectives; the latter being related to the reliability performances which are requested for the provisions implemented to address the single DiD levels.

The link between the Residual Risk and the defence in depth is implicitly generated by the failure of its fourth level which, as indicated by the definition of the RR, has to be eliminated by design or practically eliminated.

Within the following sections indications and guidelines are suggested on how to address DBC,

DEC and RR for future systems. The implementation of these guidelines could have strong feedback on the R&D effort which has to be set up for each of the Generation IV systems.

It is important to point out that the completeness and the coherence of the R&D plans for the different Generation IV systems should be assessed versus these guidelines; this is why it is extremely important to achieve the proactive consensus within the RSWG and the endorsement at the GIF level.

IV.3.3. Design Basis Conditions

The three first levels of the defence in depth convey the principle of prevention, detection and control of accidents. After the design phase, detailed analysis and assessment of the safety architecture are required to ensure that all challenges and mechanisms are correctly addressed and the corresponding objectives are met. In other words, the objective is to ensure that, in any design basis conditions, sufficient barriers remain effective to meet the radiological objectives with the due reliability, i.e. to keep the system within the tolerable risk space as discussed in Chapter III, and to ensure the "optimal risk reduction" (ALARP; see also Appendix 1).

Following the risk informed objectives, the design and the assessment have to combine deterministic and probabilistic insights considering simultaneously deterministic and probabilistic assessment techniques and success criteria. In parallel, the OPT implementation allows guaranteeing that all the provisions which participate to the achievement of safety missions are correctly considered.

For each level of the defence in depth and for each safety function the identification of challenges and mechanisms through the OPT, allows setting up a comprehensive deterministic approach. The plant designer should recognise that challenges to safety functions may occur at any reactor state, and this for all levels of defence; design provisions of different nature (engineered systems, characteristics, etc.) are to be implemented to ensure that the safety functions are accomplished and that the safety objectives and acceptance criteria can be met. The design, with specific rules, of these provisions, to insure the requested physical performances, is also a deterministic contribution. Content and details of these rules (Single Failure Criterion, Aggravating failure, combinations, etc.) has to be further discussed.

The comprehensive identification of initiating events and the following analysis to assess their potential consequences, allow identifying the set of representative postulated initiating events that is retained for the final safety assessment.

Still during the design of the provisions, the consideration of reliability objectives to cope with the probabilistic success criteria of each level of defence, represent the probabilistic contribution. Moreover, the notion of Line of Protection (cf. Appendix 3), which allows merging the contribution of several provision to achieve a common mission, asks for specific probabilistic support to insure that the reliability objectives are effectively met, for a given level of the defence in depth, by the LOP as a whole (i.e. jointly by all the provisions of the LOP).

The design architecture will so be established satisfying both deterministic and probabilistic success criteria for the representative plant conditions; once achieved, such safety architecture will be ready to be verified through both deterministic assessment and probabilistic safety assessment. This will be done considering a full list of internal conditions and conventional

rules for safety analysis.

In case of hazards, the main risks are the initiation of events and the unacceptable degradation of the provisions implemented for the management of these events. For Generation IV reactors/systems the layout and the design of these provisions shall minimize the sensitivity to and the consequences from hazards. The designer will implement an approach similar to that adopted for the reactors of the third generation with an improved exhaustiveness in the range of hazards considered, in the levels of severity and in the combinations of the considered hazards. The latter will be defined and characterized in the same way for all the systems of the fourth generation. As a generic objective it will be necessary to design the installation so that internal and external hazards are not dominant contributors to the radiological releases.

In this context the OPT is considered as a preparatory step for the development of a PSA model used for final verification that the probabilistic safety criteria are met for the design as a whole. The meeting of complementary requirements (a*s far as possible, an exhaustive, progressive, tolerant, forgiving, balanced and simple defence*) will also be checked.

IV.3.4. Design Extension Conditions

In addition to the design which fulfils the objectives of the Design Basis Conditions, and coherently with the 4^{th} level of the defence in depth, a number of Design Extension Conditions (DEC) are considered to complete the design of the plant to assure, with a sufficient degree of confidence, that their consequences are considered in the design.

The DECs shall be selected by the designer – in relation with the design - with the basic aim of addressing all the significant phenomenology and meeting the objective of keeping the plant within the tolerable risk space, even for extremely low probable events and sequences, and to prove the robustness of the confinement function. The global probability objective to meet the threshold of radiological releases requiring significant protective measures of the populations (in terms of extent or of duration), is suggested to be 10^{-6} per reactor year, as a guideline.

In order to mitigate the consequences of the events under DEC category, the designer should identify the need to introduce additional provisions or the need to supplement some already present provisions. The consideration of these design extension conditions would allow the designer to define the appropriate boundary conditions for the design of such provisions.

The design extension concept makes use of probabilistic methods as one way of identifying where DEC provisions shall be implemented, together with engineering judgement and other specific criteria. For current plants, once the relevant sequences have been selected, the assessment is done on a realistic basis, and makes use of best estimate accident analysis; claims for use of non-safety grade equipment can be made.

For future systems, the consideration of DEC should make use of best estimate methodologies; sound engineering practices are required. Specific rules have to be agreed for the detailed design and the assessment. They have to address, amongst the others, the following items:

- Possible operator actions and needed grace delay time;
- Qualification of provisions: required demonstration of capability of performing required actions and survivability;
- Degree of independence of provision needed to mitigate a severe accident versus those provided to fulfil DBC requirements (this item is directly linked to the independence

between the different levels of the defence in depth);
- Possible role of low safety classified or non-classified provisions, including the possible use of some provision beyond their initially intended DBC capability, to bring the plant to a controlled state or to mitigate the consequences of a severe accident;
- Role of PSA evaluation to justify the need for diversified equipment.

IV.3.5. Residual Risk

In terms of application of the defence in depth (DiD), it is worth noting that different provisions are implemented at different levels of the DiD. For example, the provisions for design, manufacturing and operation are implemented within the 1st level of the DiD (prevention). In parallel, the consideration of specific provisions implemented to master the management of an accidental situation are identified during the analysis of challenges /mechanisms matching with the 3rd level of the DiD. For DEC events, the provisions are identified within the framework of the 4th level of the DiD. In level 5 of DiD that covers residual risk events, the installation is assumed to be in a degraded situation (e.g. core melting), and the designer has sufficient provisions for the accident management and emergency response.

Most of the accident sequences are progressively dealt with by the provisions in Levels 2−4 of DiD through reliance on design measures for accident control, protection, mitigation. Situations that can lead to the severe plant conditions and for which it is not realistic to set up mitigation provisions should be "practically eliminated" to assure that they can be ruled out from the plant states considered in the design with a sufficient degree of confidence. For each of these scenarios, sufficient design and operation provisions have to be taken to design them out.

The Practical Elimination (PE) approach is implemented for a limited number of severe accident situations that can lead to an early or a large radioactive release if there are no realistic and demonstrable provisions to mitigate their consequences. The possibility of certain conditions may be considered to have been “practically eliminated” if they are physically impossible or if these conditions could be considered extremely unlikely with a high level of confidence.

For PWRs the list of situations to be practically eliminated is defined deterministically as a result of safety background and the discussions between the designers and the safety authorities. This is justified for the PWRs because designers know beforehand, due to large feedback experience, which initiators and situations they want to exclude/eliminate. The available safety background does help mastering the exhaustiveness of the approach. For the innovative concepts that lack this feedback experience, use of OPT can allow the search for the exhaustiveness and establish a means of communication between the designers themselves and between the designers and the safety authority.

The justification of “practical elimination” should be examined on a case-by-case basis, using deterministic considerations, complemented with a probabilistic assessment. Practical elimination of an accident situation cannot be claimed solely based on compliance with a general cut-off probabilistic value. The most stringent requirements regarding the demonstration of practical elimination should apply in the case of an event/phenomenon which has the potential to lead directly to a severe accident, i.e. to go through DiD level 1 to level 4. The practical elimination approach is more deeply described in Appendix 4.

IV.4. Assessment of innovative systems

The adequate selection of the design basis conditions, the use of enveloping and/or conservative assumptions, and the selection of suitable acceptance criteria provide confidence that the plant operation will not result in unacceptable damage, even in the eventuality of abnormal occurrences in the plant. In other words, the probability of unacceptable damage must be negligible even under the worst and highly improbable considered plant conditions with sufficient margins. These margins include room for insufficient knowledge and uncertainties associated with the design and operation of the plant.

Although the design assessment methodologies may vary from country to country or among different technologies, they have common elements that can be described as a set of conceptual steps where different types of safety margins can be identified (See Appendix 6). Once the architecture is built, the designer is required to prove that the safety operability, availability and safety objectives are met; this requires that the design assessment follows a process which is systematic, logical and auditable. A scheme to achieve such a process is proposed by the Ref. [2]; it is presented and described below (Fig.IV.2).

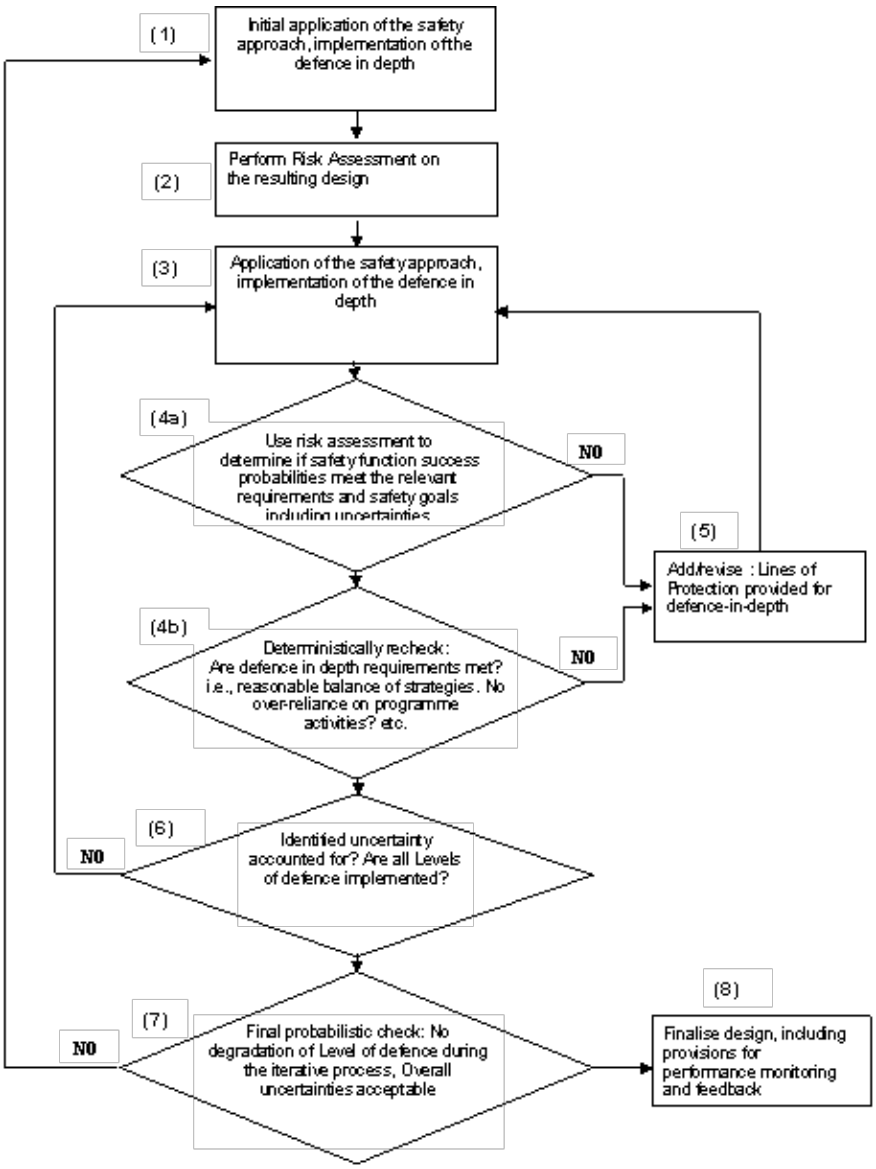


Fig. IV.2 – Design assessment: Process used to ensure that adequate defence in depth is achieved.

Stage(1) - Review of Levels of Defence

Once an initial design has been developed with preliminary implementation of the objective provision tree, the adequacy of the defence in depth measures can be systematically reviewed following the process indicated in Figure IV.2. The design to be reviewed is the basic reactor design that has been enhanced with the features needed to meet the challenges posed by the design basis, i.e. considering the specifications for normal operation, DBC and DEC. Provisions that will address the mechanisms and challenges have been identified and organized into LOPs. Further refining and completing the design so that it meets the deterministic and reliability targets of the overall safety goal, as well as determining what lines of protection are needed for each level of defence in order to meet the safety goal, is necessarily an iterative process. The identification of the postulated initiating event, the selection of sequences to be addressed, and sequences to be excluded by design (or practically eliminated), is an essential stage of this process. The means of terminating the corresponding sequences should also be specified and all the safe states for the plant defined.

Stage (2) - Risk Assessment

With the preliminary LOP architecture established, there will be sufficient information to allow the designer to perform an initial probabilistic safety assessment (PSA). The PSA considers all relevant postulated initiating events for the range of plant operating states required for the reactor concept being considered, e.g., full power/partial power operation, maintenance during operation, at power refuelling, shutdown conditions, etc. Appropriate uncertainty and sensitivity analyses should be conducted as part of the PSA process during this stage. The degree of simplification for the PSA process has to remain compatible with the design stage (pre-conceptual, conceptual, etc.).

Once agreed on the right degree of simplification, the level of PSA needed depends on the consequence metrics chosen for the safety goal representation. If the metrics are health effects, PSA Levels 1, 2 and 3 PSA are necessary. If other metrics are available for a particular reactor concept, which can be used as surrogates for the health effects, it may only be necessary to produce Levels 1&2 PSA analysis. For new plants design purpose PSA levels 1&2 will likely be largely sufficient.

Stage (3) - Identify Systems, Barriers, Phenomena, Actions to Provide Defence in Depth

From the results of the PSA the designer should investigate how well the quantitative goals for each level of defence have been met, as well as assessing the design against some qualitative principles that apply to defence in depth (e.g. a*n exhaustive, progressive, tolerant, forgiving, balanced and simple defence*). For each level of defence the assessments indicated in Stages (4a) and (4b) are carried out.

Stages (4a) [and (5)] - Review of LOP Reliability

The first part of the assessment is carried out by using the PSA results to determine if the LOPs have the required reliability to satisfy the frequency goals and associated consequences for the level of defence being examined. The demonstration of compliance with the reliability targets needs to account for uncertainties in the estimates of the reliabilities of systems, structures, components and operator actions used in the PSA. This inclusion of the uncertainties capable of being modelled in the safety assessment is an essential step. It is also possible that the risk assessment and this review will identify areas where success probabilities have been

significantly exceeded. In such cases the designer may consider modifying and/or deleting existing proposed LOPs. If any modifications have been made to the LOPs, another assessment of their reliability is then performed with an appropriately revised PSA. Once adequate reliability is established, the process proceeds to Stage (4b).

Stages (4b) [and (5)] - Review of Defence in Depth

In this part of the assessment the designer will verify that the fundamental principles of defence in depth have been met, for example: that there is a reasonable balance in the proposed methods of delivery of defence in depth; that there is no excessive reliance on a single system, unproven phenomena or on administrative processes; that there are no unrealistic operator actions required, etc. Complementary tools would be necessary to achieve this step (e.g. specific for human factor, the Index of Complexity, etc.).

Stage (5) – Review and Modify the Design

In this stage, the outputs first from Stage (4a) and then Stage (4b) are reviewed to confirm whether the reliability targets and defence in depth requirements have been met. If the reliability targets for the LOP have not been met the designer will need to modify existing LOPs and/or add new ones, thus enhancing the defence in depth and its reliability. Where the defence in depth principles have not been satisfactorily achieved the designer will need to review the design and modify it until the principles can be demonstrated as having been met. If modifications are made, the process has to return to Stage (3), to verify that the changes have not impacted on the reliability requirements. When the assessments of Stages (4a) and (4b) have produced satisfactory results, the process can proceed to Stage (6).

Stage (6) - Accounting for Uncertainty

Proper consideration of uncertainty is an essential part of the safety assessment. This is particularly important for innovative systems where the state of knowledge is not as advanced as for existing plants. At this stage an overall assessment of the level of defence being examined and its associated uncertainty is carried out to determine whether the identified uncertainties are adequately addressed, and the level of defence is adequately implemented. An appropriate method for dealing with uncertainties is the use of sensitivity analyses for uncertain parameters to determine their relative importance in the overall safety architecture; this approach has to rest on a sufficient knowledge of relevant phenomena and requires an adequate R&D effort. Any shortfalls in dealing with uncertainties will require further analysis and assessment with a return to Stage (3).

Stage (7) - Confirmation of Design Provisions

The whole process described above implicitly integrates the risk informed approach into the design. When all the levels of defence have been examined in the above manner, the final stage in this iterative process is a check to confirm that the design is exhaustive, balanced, and graduated, and meets the safety goals. It will also confirm that no particular level of defence has been degraded and that the overall treatment of uncertainties is acceptable. If any of these elements are not adequately demonstrated, then the designer will need to revisit the initial design concept (Stage 1). Once the requirements of Stage (7) have been met the designer will then be in a position to finalise the design (Stage 8).

Stage (8) - Finalisation of the Design

When all checks and assessments have been satisfactorily completed, the design can be

finalised with appropriate monitoring and feedback provisions. As the design develops in greater detail, further information may become available which challenges the assumptions, analyses or uncertainties used in the safety assessment. This process requires the designer to revisit the safety assessment, either after a significant change or periodically.

As part of this overall process the designer should assess scenarios that cover both DBC and DEC. For the latter, the designer can use the PSA to evaluate whether the likelihood of postulated events/sequences should be considered in Level 4 of the defence in depth, i.e. severe plant conditions, or if they can be considered as "practically eliminated".

As the above described process indicates, the development of acceptable designs for innovative reactors will be iterative, initially by the designer and ultimately with the regulator. As the design develops from conceptual to final, the designer will perform PSAs in greater detail during which a more robust design emerges.

Chapter V. RSWG's Integrated Safety Assessment Methodology

The RSWG issued the "Integrated Safety Assessment Methodology (ISAM)" in 2011 to assess and improve the safety architecture for Generation IV nuclear energy systems. Conceived as a design driver, ISAM toolkit components are intended to support the entire design process from a pre-conceptual stage to licensing stage. The ISAM includes five analytical tools: Qualitative Safety features Review (QSR), Phenomena Identification and Ranking Table (PIRT), Objective Provision Tree (OPT), Deterministic and Phenomenological Analyses (DPA), and Probabilistic Safety Assessment (PSA). Each tool is intended to answer specific safety-related questions with different levels of detail during various design stages. Often the output of each analysis tool supports preparation of input for other tools. Although each tool can be selected for individual and exclusive use, the full value of the integrated methodology is derived from using all tools, in an iterative fashion and in combination with the others, throughout the design process.

The chapter describes the ISAM toolkit components, their use in the system design, and how the inputs and outputs be combined with pilot examples of individual use of QSR, PIRT and OPT in combination with use of more conventional tools like DPA and PSA.

V.1. Overview of ISAM

The ISAM tools are intended to support a design process from early concept development to basic design and licensing. The use of ISAM provides early identification of safety related vulnerabilities and their contributions to risk during early stages of the concept development so that new design improvements can be identified, developed, and implemented relatively early. Each tool provides understanding of risk contributors, safety margins, effectiveness of safety-related design measures, and sources and impact of uncertainties. These pieces of information can then be used for decision making on design choices. The ISAM tools also help examine design maturity by measuring risks against safety objectives or by licensing criteria, including various potentially safety-related metrics or figures of merit, at a late design stage.

The ISAM consists of three qualitative and two quantitative distinct elemental tools that can be tailored to answer specific types of questions at various design stages. Each of the five analytical tools is used to answer specific safety-related questions with varying levels of detail at different stages of design maturity. The diversity of these tools and their integrated and iterative use are intended to ensure complete and robust design. Figure 1 shows an overall task flow of the ISAM and indicates which tools are intended to be used in what design stage of Gen-IV system development.

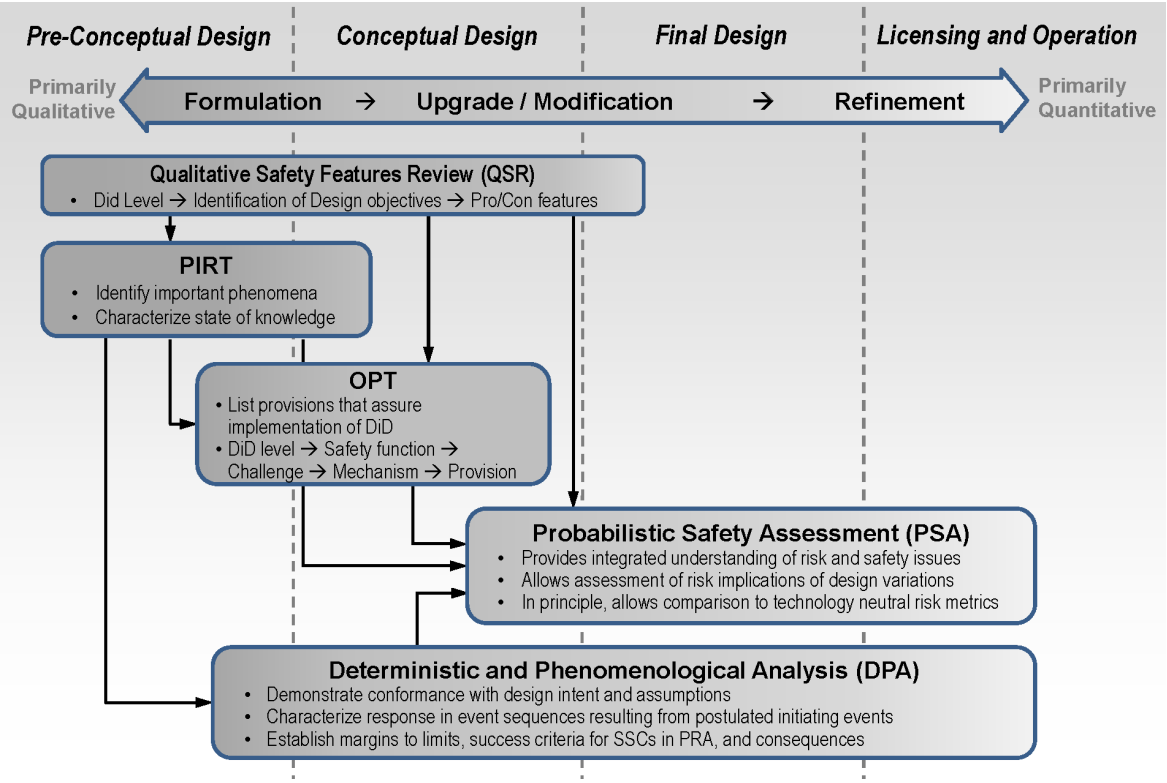


Figure 1: Task Flow of GIF Integrated Safety Assessment Methodology (ISAM) in Design Process

Qualitative Safety Features Review (QSR)

QSR is a relatively new tool to provide a systematic means of ensuring and documenting desirable or undesirable safety-related attributes and characteristics of a concept. It is a qualitative tool intended for use in pre-conceptual to conceptual design stages as a "checklist" approach to verify the safety features expected in the design. The use of a structured checklist template facilitates the design assessment with respect to fundamental safety functions to help the multidisciplinary development team consider and share their perspectives on important attributes such as application of defence in depth, achieving high reliability, minimization of sensitivity to human error, and other important safety characteristics that should be considered in the design. The QSR also serves as a useful preparatory step for the other ISAM tools by facilitating a multidisciplinary and comprehensive understanding of safety issues or vulnerabilities, which will be analysed in depth in latter steps through the use of other ISAM tools.

Phenomena Identification and Ranking Table (PIRT)

PIRT is a technique that has been widely used in both nuclear and non-nuclear applications. The PIRT is also a qualitative technique primarily used in a pre-conceptual design stage. It is used to identify a spectrum of safety-related phenomena or scenarios and to rank them in order of their importance (e.g. potential consequences) and the state of knowledge (i.e., causes and magnitudes of phenomenological uncertainties). The PIRT relies heavily on expert elicitation of knowledge and background information based on the output from the QSR in relation to safety features, potential risks, and trade-off had been identified. These QSR outputs are broken down into elemental or multiple phenomena, and the list of such phenomena is used as input for PIRT. The results from the PIRT can then be used to

- prioritize confirmatory research activities to address safety-significant issues;
- inform decisions on the development of analytical tools for safety analysis;
- assist in defining test data needs for validation and verification of analytical tools; and
- provide insights for the review of safety analysis and supporting databases.

The PIRT can focus on very general issues or on specific detailed design issues, depending on the need. It provides a systematic way of identifying technical issues that the developers face during the later design stages. As such, the PIRT forms input to both OPT and PSA. The issues identified in the PIRT and resolved in related research are also incorporated in the modelling used in the Deterministic and Phenomenological Analyses (DPA). In this context, the PIRT is particularly helpful in defining accident sequences and safety system success criteria. The PIRT is also essential to identify items to which additional research needs to reduce uncertainties.

Objective Provision Tree (OPT)

The Objective Provision Tree (OPT) is a relatively new analytical tool originally promoted by IAEA. It is also a qualitative tool intended for use in pre-conceptual to conceptual design stages. It ensures and documents provisions by using essential combination of multidisciplinary mechanisms so that phenomena that could potentially damage a nuclear system can be successfully prevented, controlled, or mitigated.

There is a natural interface between the OPT and the PIRT; the PIRT identifies phenomena and issues that could potentially challenge the safety function, while the OPT focuses on mechanisms that could arise from that challenge, and on design provisions to prevent, control, or mitigate its consequences. OPT formulates a "tree diagram" that contains mechanisms and corresponding provisions in relation to the foreseen challenge on specific safety functions. As such, the purpose of OPT in the ISAM is to inform designers the challenges (e.g. against maintaining core cooling) in a structural manner and to identify effective design provisions for prevention and mitigation of phenomena that pose challenges to the reactor safety. The OPT output is eventually fed into the PSA in formulation of fault trees and event trees including identification of possible accident initiators.

Deterministic and Phenomenological Analyses (DPA)

Traditional deterministic and phenomenological analyses collectively constitute an indispensable part of ISAM, including thermal-hydraulic analyses, computational fluid dynamics (CFD) analyses, reactor physics analyses, accident transient numerical simulation, materials behaviour models, and structural analysis models. These analyses are used as needed to understand a wide range of safety issues, and its output will form inputs to the PSA. By using a statistical approach related to the DPA, a number of output (e.g. peak temperatures during accident transients) form distribution of quantitative values, and the probability of the output go beyond or below a target value is obtained from the distribution. The results are used in the PSA as success/failure probability branch, for example. It is anticipated that DPA are performed from a late pre-conceptual design stage through licensing stage.

Probabilistic Safety Assessment (PSA)

The PSA provides a structured means to answer three questions: What can go wrong, how likely is it to occur, and what are the consequences? It is traditionally used to evaluate core damage frequency (CDF) and to present dominant accident sequences contributing to risks in

a licensing stage of a nuclear power plant. As part of ISAM, however, PSA primarily supports improved safety of the design via combination and iterative feedback with other ISAM tools. The PSA in the ISAM is performed from a late pre-conceptual design stage through the final design stage. Therefore, the PSA results are often updated to reflect changes in design and system configuration and these results, in return, influence the design process by contributing to key decisions and adopting new safety measures by studying the risk space. Although the other elements of the ISAM have significant value as stand-alone tools, their value is further enhanced by being integrated with PSA as the design proceeds towards licensing. As the centrepiece of the ISAM, PSA also facilitates a systematic understanding of uncertainties related to risk. Uncertainties arise from a number of causes and accommodated in a design through additional safety margin. Leaving a big safety margins is, of course, expensive, and it may also lead to an inappropriate focus on some specific aspects of the design instead of other more important, dominant risk contributors. The PSA can provide systematic understanding of sources and a range of safety-related uncertainties to help the developers achieve an optimized design considering safety, reliability and economic factors.

V.2. Integration of ISAM Tools

The QSR can be performed by system design teams and reviewed by external experts during any design phase, although it is most suitable from pre-conceptual to final design stages to ensure that the general design characteristics including safety features can be extended and potential vulnerabilities are identified/addressed during the subsequent design stages. Possible issues identified and documented via the QSR are covered in PIRT, OPT, and PSA.

The PIRT if facilitated by subject matter experts (system designers and external experts). It is typically employed from a pre-conceptual to conceptual design stages to identify specific issues and phenomena that may be important to a particular concept, by using the output from the QSR. The PIRT output is documented and used as input to OPT and PSA. PIRT output also informs the numerical modelling and associated R&D for DPA.

The OPT is employed from pre-conceptual to conceptual design stages to ensure that the design incorporates adequate provisions. It is led by system designers and reviewed by external experts. It is typically based on pro/con features obtained from the QSR and the understanding of the phenomena and issues that have been highlighted in the PIRT. The output obtained from an OPT is documented and used in PSA to formulate fault and event trees and to identify postulated initiating events.

The DPA are performed throughout all design stages to investigate safety issues and confirm consistent implementation of deterministic approach such as the application of a single failure criterion or required redundancy and diversity of SSCs. In an early design stage, numerical models that had been identified to be newly developed by using the PIRT need to be included in the computer models used in DPA. The PSA requires input from the OPT to formulate fault and event trees, and from the DPA to justify success or failure criteria. It is performed by a team of internal event and external hazard specialists with recognized expertise in PSA.

Sample applications of the ISAM are included in the RSWG's Guidance Document of ISAM issued in 2014. In recent years, the ISAM has been applied in the design process of six Gen-IV reactor systems, and the results of the pilot application are summarized in white papers as self-assessments reported by six system steering committees to provide guidance on improving safety features and upgrading safety related system design.

REFERENCES

[1] Technology Roadmap Update for Generation IV Nuclear Energy Systems, https://www.gen-4.org/gif/upload/docs/application/pdf/2014-03/gif-tru2014.pdf, January 2014.

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

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

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

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

[6] Basic Safety Principles for Nuclear Power Plants, 75-INSAG-3 Rev.1, INSAG-12, A report by the International Nuclear Safety Advisory Group, IAEA, Vienna (1999)

[7] K. Kurisaka: Probabilistic Safety Assessment of Japanese Sodium-cooled Fast Reactor in Conceptual Design Stage, 15th Pacific Basin Nuclear Conf. Sydney, Australia, 15-20 Oct. 2006

[8] Evaluation Methodology for Proliferation Resistance and Physical Protection of Generation IV Nuclear Energy Systems, Revision 5, September 30, 2006, Prepared by The Proliferation Resistance and Physical Protection Evaluation Methodology Expert Group of the Generation IV International Forum

[9] 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)

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

[11] Safety of Nuclear Power Plants: Operation, IAEA Safety Standards Series, Safety Requirements No. NS-R-2, IAEA, Vienna (2000)

[12] Safety Margins Action Plan - Final report, NEA/SEN/SIN/SMAP (2007) xxx, OECD/NEA, 2007

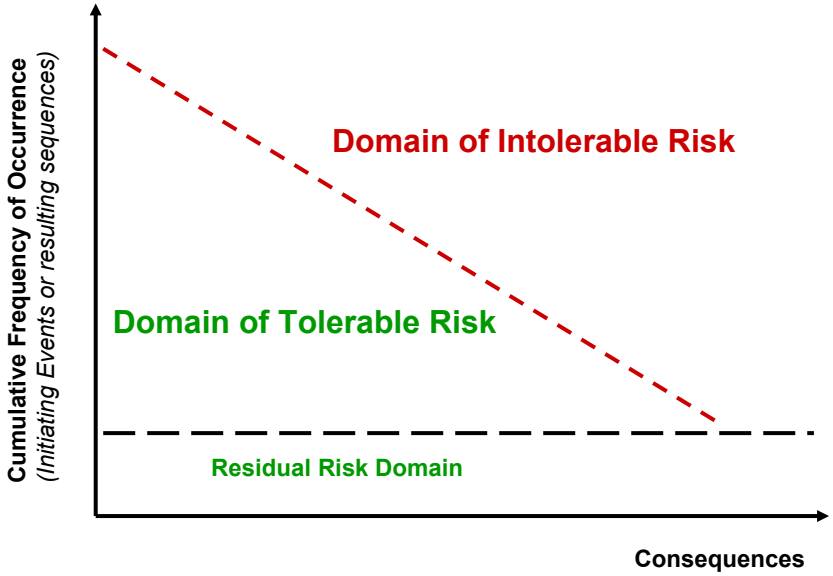
[13] IAEA. Safety Assessment for Facilities and Activities General Safety Requirements No. GSR Part 4 (Rev. 1). 2016.

[14] IAEA, A Framework for an Integrated Risk Informed Decision Making Process - INSAG-25. INSAG. 2011.

Appendix 1 - The "domain of risk" and concept of "optimal risk reduction"

The definition and implementation of the safety architecture of a nuclear installation must be fully coherent with the principles of the Defence-in-Depth (DiD) and this coherence must be assessed with a high level of confidence. Deterministic and probabilistic approaches are recognized to be complementary elements for the safety assessment of nuclear installations and the assessment of the DiD can be supported by Probabilistic Safety Assessments (PSA). The link between DiD and PSA can be achieved through a risk-informed approach by taking the reliability of the safety-related components into account and by managing the uncertainties and their propagation.

In a "risk informed" approach, the concept of risk (a combination of the frequency of occurrence and consequences of an event) can be used to make the link between deterministic and probabilistic analyses. Several elements contribute to the integration of the deterministic approach with the notion of risk. First, the frequency vs. consequence charts (also known as Farmer's curve shown in Fig. A.1.1 delineating the "tolerable risk domain") provide a tool to identify what is allowable and what is considered unacceptable. The consideration of this curve allows addressing the full set of possible plant conditions, categorized as a function of their estimated frequency of occurrence. The basic idea is to guarantee extremely low consequences for frequent events and extremely low frequencies for highly hypothetical accidents that could lead to severe plant conditions.



Schematic representation of the Risk domain
(the so called Farmer Curve)

Fig. A1.1 – The Farmer's curve: The Risk domain

Once the system architecture is defined, the designer has to prove that for all the conditions which the plant has to deal with, the system response (i.e. the response provided by the safety architecture) allows the corresponding risk to be kept within the tolerable domain. The concept of "optimal risk reduction" rests on this notion of risk looking for an improved mastering of the domain of the tolerable risk and the reduction ALARP of the consequences of all the abnormal conditions.

Appendix 2 - An improved implementation of Defence-in-Depth principle

The final acceptability of a concept should remain based on the degree of meeting the Defence-in-Depth (DiD) principles. The strategy of DiD (i.e. the adoption of adequate safety architectures) ensures that the fundamental safety functions are reliably achieved and with sufficient margins to compensate for equipment failure, human errors and hazards, including the uncertainty associated with estimating such events. This can be done through comprehensive coverage of the risk domain from frequent abnormal events to very low frequency accidents.

This coverage is attained by using the best data from experience feedback (when available) for improving the quality of data and analyses, and developing a systematic methodology to identify and manage the risks. Moreover, this methodology has so to merge Defence-in-Depth and probabilistic insights generating a Risk-informed approach. The objective of such an approach is to generate safety requirements usable by the designer integrating deterministic success criteria and probabilistic success criteria (cf. Fig. A2.1).

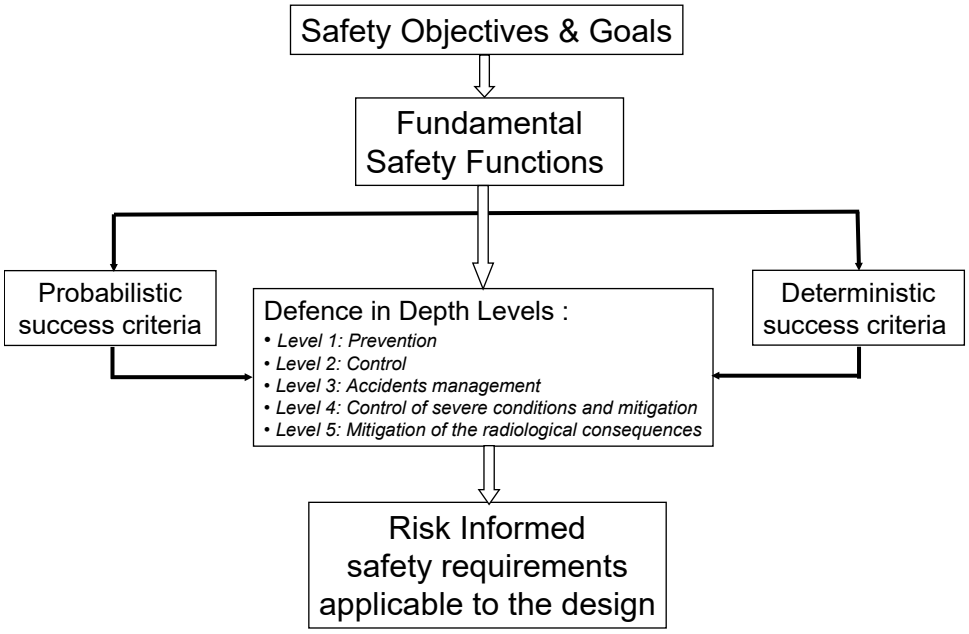


Fig. A2.1 – Defence in depth and Risk-Informed Safety Philosophy
Master Logic Diagram

The strategy of defence in depth in nuclear safety is discussed in Ref [3] in terms of five levels, together with the objective of each level, the essential means of meeting this objective, and the deterministic considerations involved in the implementation of defence in depth.

The setting of a quantitative safety goal stated in probabilistic terms, i.e., frequency limits for various consequence levels, enables probabilistic considerations, including success criteria, to be factored into the implementation of defence in depth, as shown in Figure A2.1. The deterministic and probabilistic considerations are therefore integrated into the comprehensive implementation of defence in depth. Such success criteria are essential to correctly design the provisions that implement the levels of the DiD; the performances of these provisions have to

be defined in terms of physical performances and required reliability; finally, the provisions have to be – if needed/justified – safety classified. The final goal of this process is the optimization of the whole safety related architecture in terms of performances, reliability and costs.

The definition of these criteria needs the implementation of the DiD principles in a way compatible with the notions brought by the “Risk Domain”. Discussions are still underway to define an agreed approach to do that. This philosophy is applicable to improve safety during operation and maintenance, including shutdown states.

Appendix 3 - The Objective Provision Tree and the Line of Protection concepts

The principles of the suggested Risk-informed approach are schematized on figure IV.2. The objective is the definition of the safety requirements needed for the design and for the assessment of the safety architecture of a nuclear installation. Based on such requirements, the designer can define the safety architecture of the installation and can design the "provisions" which compose this architecture. Practically this can be made by means of the Objective Provisions Tree (OPT) the logic of which is detailed hereafter. The objective of the OPT (Fig.A.3.1) is the identification, for each level of Defence-in-Depth, with regard to each of the safety functions, of the provisions requested to realize the required missions.

For a given level of Defence-in-Depth, and according to the progress of the approach (Safety functions ⇨ Challenges ⇨ Mechanisms ⇨ Provisions), for a given mechanism, the full set of provisions represents the Line of protection (LOP) which realizes the wanted mission. The LOP integrates all sort of provisions and characterizes them, in a homogeneous way, through their performances, their reliability and the conditions of their mutual independence.
The originality of the OPT, with regard to the conventional methods of representation of the safety architecture, lies on the fact that all the provisions, are considered independently of their nature; this can represent an interesting precursor for the PSA/PRA. Specific activities have to be launched to develop the methodology and to fully exploit its potential.

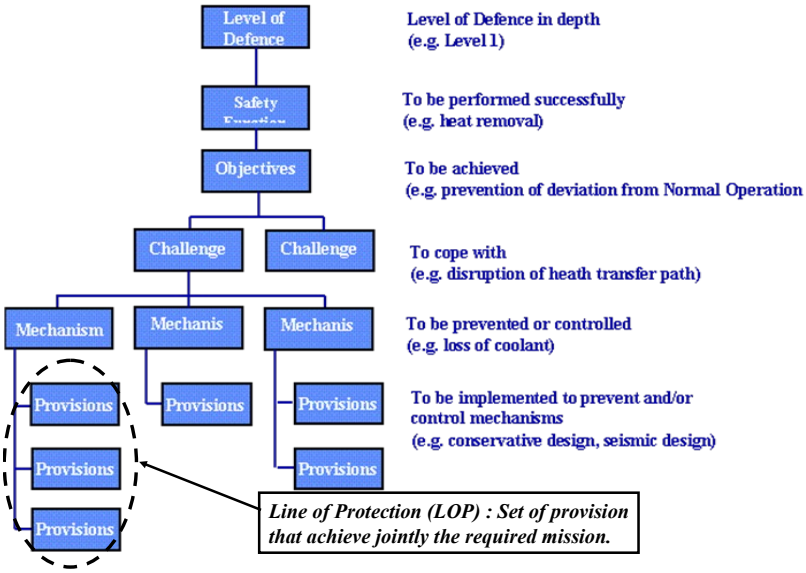


Fig. A3.1 – Simplified representation of Objective Provisions Tree

A.3.1 Methodology consideration

Following the publication of IAEA TECDOC 1366, Considerations in the Development of Safety Requirements for Innovative Reactors: Application to Modular High Temperature Gas Cooled Reactors (Ref. [4]) in which the notion of OPT is mentioned for the first time, the IAEA published in 2005 a Safety Serious Report No 46: Assessment of Defence in Depth for NPPs (Ref. [5]) which main objective was to present a practical tool for inventorying the defence in depth capabilities of a NPP, including both the design features and the operational measures. To achieve this goal, the definition of defence in depth and the guidance on its implementation agreed upon by international consensus (Ref. [3] & [4]), have been combined into a logical framework that can be used for assessing the comprehensiveness and quality of defence in

depth at a plant.

The assessment method presented in Ref. [5] was supposed to be directly applicable to existing light water and heavy water reactors, and to spent fuel transported or stored in the pools outside the nuclear reactor coolant system on the site of these reactors. With some minor modifications, the method could also be used for other types of reactors such as reactors cooled with gas or with liquid metal. The publication suggested that in the future the method could be modified to be applicable also for new or innovative reactor designs.

All five levels of defence in depth (table I, Ref. [4]) are covered in the IAEA report. For given objectives at each level of defence, a set of challenges [10] is identified, and several root mechanisms [11] leading to the challenges are specified. Finally, to the extent possible the comprehensive list of safety provisions, which contribute to prevent that the mechanism takes place, is provided. The broad spectrum of provisions, that encompass the inherent safety features, equipment, procedures, staff availability, staff training and safety culture aspects, are considered.

TABLE I. LEVELS OF DEFENCE IN DEPTH

Levels of defence in depth	**Objective**	*Essential means for achieving objective*
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation
Level 2	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance features
Level 3	Control of accidents within the design basis	Engineered safety features and accident procedures
Level 4	Control of severe plant conditions including prevention of accident progression and mitigation of the consequences of severe accidents	Complementary measures and accident management
Level 5	Mitigation of radiological consequences of significant releases of radioactive materials	Off-site emergency response

For easier and user-friendly applicability, the method presented in Ref. [5], including the overview of all challenges, mechanisms and provisions for all levels of defence, is illustrated in the form of "objective provisions trees"[12].

Further the report described the approach taken to develop a tool for the inventorying the defence in depth capabilities of NPP, e.g. the identification of the ways in which the

[10] 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.
[11] Mechanism: specific reasons, processes or situations whose consequences might create challenges to the performance of safety functions.
[12] Objective provisions tree: graphical presentation, for each of the specific safety principles belonging to the five levels of defence 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.

performance of the fundamental safety functions can be impacted as well as of the variety of options that exist for avoiding this impact for each level of defence. To this end, the interrelation amongst different elements of the DiD concept and OPT notion was established. The link between the three fundamental safety functions (FSF), the 19 subsidiary safety functions (SF), as described in Ref. [10], the Basic Safety Principles for NPP as defined by Ref. [6] and the Levels of defence and the respective physical barriers is described in Ref. [4].

A combination of expert judgement, the IAEA reference report INSAG-12 (Ref. [6]) and the IAEA Safety Standards publications (Ref. [10] & [11]) have been used to provide guidance on the comprehensive selection of the main challenges, mechanisms and provisions for each of the objective provision trees developed for different specific safety principles. As a result, altogether 68 different objective provision trees have been developed for 53 specific safety principles assigned to the five levels of defence:

- Eleven trees exclusively for Level 1
- Seven trees exclusively for Level 2
- Two trees common to Levels 1 and 2
- Three trees common to Levels 1, 2 and 3
- Eleven trees exclusively to Level 3
- Nineteen trees common to Levels 1, 2, 3 and 4
- One tree common to Levels 2, 3 and 4
- Five trees common to Levels 3 and 4
- Eight trees exclusively for Level 4 and
- One tree for Level 5.

The developed trees are considered to be self- explanatory and are included in the Appendix II of Ref. [5]. For verification of implementation of DiD at a plant it is suggested to check whether the plant has in place all provisions as specified by this Appendix. The comprehensive process applied for the development of the objective provision trees in SSR 46 gives adequate level of assurance that no essential provisions are omitted.

Users of the method presented in Ref. [5] are expected to review and compare provisions for defence in depth identified in the objective provision trees with the existing defence in depth capabilities of their plant. The objective provision trees provided the rationale for the bottom-up method, starting with the screening of individual provisions. Users are expected to evaluate for each provision the level of its implementation. If a satisfactory answer on implementation of provisions is given, then the relevant mechanism could be considered as having been prevented from occurring. Deviations are supposed to be justified by compensatory features specific to the plant or reconsidered for further strengthening of the defence in depth of the plant.
In fact, plant specific users of the OPT methodology are provided with pre-determined OPTs and their role in the assessment is simply to check the availability at the plant and adequacy of the listed predetermined provisions.
It is clear that for Generation IV the main challenge will be to develop the OPTs for all reactor systems. These trees will have to evolve with the progression of the designs.

A.3.2 Implication of the methodology for Research and Development R&D for inherent and/or passive LOP

For some concepts, the design is based on greater use of intrinsic physical properties and/or

passives provisions to address partially or totally abnormal conditions. Such implementation:

- Led to highlight events of very low probability which involve the failure of this type of provisions[13];
- Has to consider the fact that the consequences of these events are driven by the phenomenological answer of the installation, often influenced by the environmental conditions which can affect the behavior of these "defences"[14];
- Has to address the lack of reliability data and the embryonic character of the methodologies for the evaluation of this reliability;
- Has to address the difficulty to perform tests of these provisions during the plant operation;
- Has to take into account limited possibilities of intervention of the operator for the sequences' management[15].
- Has to achieve an objective for having, as far as possible, a progressive behavior[16] and the possibility for "fail safe" human intervention.

In many cases, the understanding of how these provisions operate and of phenomena during accidental situations, require specific R&D that involves modeling and experimentation.

To complement this specific R&D, the practice of periodic plant safety re-examinations, and the link between the residual life expectancy of the nuclear installations and the results of these re-examinations, has to be taken into account. Strong requirements for the control and the maintenance of the LOP (human factor) have to be considered since the very preliminary design. Having said that, it is important to point out that "passivity" for the management of abnormal conditions should not be an objective in itself. What is aimed at is the implementation of a safety architecture that, while exploiting the favorable intrinsic characteristics, ends in the optimized implementation of active and passive provisions. The efficiency, the simplicity, the robustness and the reliability will be, with economy, the essential criteria for the evaluation of the retained options.

Research and development for complementary indicators

The correct implementation of the strategy of Defence-in-Depth (i.e. the adoption of adequate safety architecture) ensures that the fundamental safety functions are reliably achieved and with sufficient margins to compensate for equipment failure, hazards and human errors, including the uncertainty associated with estimating such events.

As indicated in Section 4.3.3, complementary and essential characteristics that ensure the effectiveness of DiD are: an exhaustive, balanced, progressive, robust and simple defence.
The PSA is a useful tool to assess two of these characteristics (balanced, progressive) but it is not sufficient to cover the full scope.

Specific indicators and tools have to be developed to help assessing the meeting of these

---

[13] e.g.: Structural failures.

[14] e.g.: Start and set up the natural convection with risks for stratification.

[15] E.g.:limited capability for manual operations on the passive systems.

[16] E.g. the behavior of a "check valve" – which can open and close - vis à vis of a "rupture disk" which can only irreversibly open

objectives, notably in the domains of, e.g.:

- the prediction of human factors' impact on safety,
- the uncertainties management (robustness) and
- the complexity of the architecture (simplicity).

Appendix 4 - Principle of “practical elimination”

Definition of practical elimination

An essential objective of the new reactor design is to limit, in the event of a severe accident, the radiological consequences on the environment and on the population. For Generation IV reactors, in the event of a severe accident, even a temporary evacuation of population should not be necessary and only a sheltering, limited in time and space, should be permissible.

The fundamental safety principle applied to reactor design is the Defence-in-Depth. The application of this principle requires extremely reliable provisions that assure prevention of severe accidents within first three levels of defence-in-depth. Despite these provisions, the fourth level also requires reliable mitigation means to manage the consequences of severe accidents assuming failure of prevention provisions.

The design aims at setting up mitigation provisions for all the possible severe accidents. Nevertheless, there may still exist some severe accident situations that cannot be reasonably covered by these mitigation provisions. If consequences of such severe accident situations without mitigation provisions might lead to either early radiological releases (not leaving sufficient time to implement emergency response) or large radiological releases (requiring the displacement of populations over a significant period of time or in an wide area), they need to be practically eliminated.

Such situations need to be identified in the design so as to make them extremely unlikely to occur with appropriate design or organization provisions. As such situations being an exception to the defence-in-depth fourth level implementation, they should be limited in number.

The practical elimination is an approach that involves, from the onset of the design process, identification of severe accident situations that would not be controllable under reasonable conditions, and therefore making them extremely unlikely to occur with a high level of confidence through appropriate design and operating provisions.

Identification of the situations to be practically eliminated

The goal is to identify, from the very beginning of the project, the situations that cannot be reasonably controlled, and to provide, as early in the design studies as possible, the provisions that will make these situations extremely unlikely with a high level of confidence.

To be able to identify these situations as the cases to be practically eliminated from the early stages of a design process, first the dominant risk factors that can lead to significant radiological releases need to be identified through a "top down" approach. A limited number of situations to be practically eliminated should result from this identification phase. It should be emphasized that the main challenge is to identify the situations for practical elimination, not the sequences that may lead to them.

To help identification of the situations for practical elimination, three types of serious-accident situations can be distinguished:

- Type 1: The severe accidents leading to a violent energetic phenomenon likely to damage the containment in an irreversible manner (e.g. a severe accident leading to a

hydrogen explosion);
- Type 2: The situations successively leading to an unacceptable deterioration of the mitigation means following a severe accident (e.g. for some reactors, the extended complete loss of residual heat removal function);
- Type 3: The severe accidents occurring when the mitigation means are not available or insufficient (e.g. accidents during fuel handling operations).

As a reminder, plausible severe accident situations with consequences that can be managed under reasonable technical and economic terms must be dealt with. The following situations are not part of the practical elimination and are excluded from the analysis:

- The situations corresponding to a severe accident combined with a failure of the mitigation means, independent from the accident consequences or from the events that may have caused it;
- The situations physically impossible or deemed as not plausible by expert consensus or PSA analysis.

Finally, the situations with a non-radiological environmental impact such as the releases of toxic chemical substances should be studied and addressed with specific methods; therefore, these situations are not subject to practical elimination.

Demonstration of practical elimination

Practical elimination demonstrations involve only a limited number of extremely unlikely situations. Although these demonstrations would be design specific, it is possible to give some general indications. These demonstrations will be explicitly made in the safety report.

The goal of this demonstration is to give evidence that the situation is extremely unlikely with a high level of confidence. The designer first examines the possibility to make this situation physically impossible under reasonable conditions.

When the physical impossibility is not achieved, the demonstration relies on the following deterministic approach:

- First, the identification of the plausible sequences that may lead to the dreaded situation,
- Then the definition of an adequate set of independent and sufficiently reliable provisions for the prevention of the situation to be practically eliminated, covering all the plausible sequences identified and considering the associated uncertainties.

The provision adequacy can be evaluated as follows:

- A good practice is to implement the equivalent of three independent lines of defence.
- Arguments related to the quality level of the equipment ensuring the function, to their technical specifications, to the monitoring, to the accident progressiveness, to the tolerance towards some faults, etc. can also be used.

Whenever relevant, probabilistic insights may help to strengthen the sufficiently unlikely nature of sequences leading to the dreaded situation. There is no defined cut-off frequency.

Abbreviations

DBC	Design Basis Conditions
DEC	Design Extension Conditions
DHRS	Decay Heat Removal Systems
DiD	Defence in Depth
EG	Experts Group
FMEA	Failure Modes and Effects Analysis
FP	Fission Products
FSF	Fundamental Safety Function
GFR	Gas-Cooled Fast Reactor
GIF	Generation IV International Forum
HACCL	Hazards Analysis Critical Control List
HWR	Heavy Water Reactor
IHX	Intermediate Heat Exchanger
INTD	International Near Term Deployment
ISI	In-Service Inspection
IST	In-Service Testing
JSFR	Japan Sodium-Cooled Fast Reactor
LOP	Line of Protection
LWR	Light Water Reactor
MDEP	Multinational Design Evaluation Program
MSR	Molten Salt Reactor
OPT	Objective Provision Tree
PG	Policy Group
PIE	Postulated Initiating Events
PIRT	Phenomena Identification and Ranking Table
PMB	Project Management Board
PR&PPWG	Proliferation Resistance & Physical Protection Working Group
PSA	Probabilistic Safety Assessment
QA	Quality Assurance
R&D	Research and Development
RR	Residual Risk
RSWG	Risk and Safety Working Group
SASS	Self-Actuated Shutdown System
SCWR	Supercritical Water-Cooled Reactor
SG	Steam Generator
SIAP	Senior Industry Advisory Panel
SP	Safety Principles
SSC	System Steering Committee
VHTR	Very High Temperature Reactor
V&V	Verification and Validation