GIF/RSWG/2007/002

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

Revision 1

November 24, 2008

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

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 3

Chapter I: Introduction 7
I.1 Background 7
I.2 Objectives of the report 8
I.3 Scope and Structure of the Report 9

Chapter II: Risk and Safety Working Group Charter and Objectives 11
II.1 The GIF Risk and Safety Working Group 11
II.2 RSWG Terms of Reference 11
II.3 RSWG meetings 12

Chapter III: Generation IV Safety Philosophy 14
III.1 Goals for Generation IV 14
III.2 A Cohesive Safety Philosophy 16
III.3 Potential for Safety Improvements 17
III.4 Re-examination of the Approach to Safety 19
III.5 Main Safety Principles for Generation IV Systems 21
III.5.1 Defence in Depth (DiD) 21
III.5.2 Risk-Informed Design 24
III.5.3 Simulation, Prototyping, and Demonstration 25

Chapter IV: Design and assessment of innovative systems 26
IV.1. Current plant experience 26
IV.2. Gen IV Systems: a need for re-examining the safety approach 27
IV.3. Design of innovative systems 28
IV.3.1 Objectives and ways for the design improvement 28
IV.3.2. The steps for the design 29
IV.3.3. Design Basis Conditions 32
IV.3.4. Design Extension Conditions 33
IV.3.5. Residual Risk 34
IV.4. Assessment of innovative systems 35

Chapter V. Generation IV Safety Methods and Tools 40
V.1 Objective Provision Tree 40
V.1.1 Elemental structure of OPT 41
V.1.2 Hierarchy structure of OPT 42
V.1.3 Safety functions/principles and relevant DiD level to be assessed by OPT 42
V.1.4 Documentation for OPT review 43
V.1.5 Utilization of OPT in the stage of preliminary conceptual design 43

V.2 Use of PSA in the preliminary conceptual design phase 44
V.3 Relation with the PR&PP evaluation method 45
V.3.1 Commonalities in the analysis method between safety and PR&PP 45
V.3.2 Commonalities in countermeasures of safety and PR&PP 46
V.4 Objective Provision Tree Demonstration/Case Study 46
V.4.1 Experience of Bohunice NPP 47
V.4.2 Experience from the pilot use of the OPT methodology for JSFR 47
V.4.3 Conclusions 48

Chapter VI Future activities of the RSWG 50
VI.1 Develop and finalize the definition of the safety principles and the safety objectives 50
VI.2 Identify the crosscut R&D 51
VI.3 Identification and implementation of specific R&D efforts 51
VI.4 Miscellaneous 52

REFERENCES 54

Appendix 1 - The “domain of risk” and concept of “optimal risk reduction” 55

Appendix 2 - An improved implementation of Defence-in-Depth principle 56

Appendix 3 - The Objective Provision Tree and the Line of Protection concepts 58

Appendix 4 - Principle of “practical elimination” 65

Appendix 5 - Generation IV Nuclear Systems 66

Appendix 6 - Safety margins and Uncertainties 76

Appendix 7 - Safety functions/principles and relevant DiD level to be assessed by OPT 79

Appendix 8 – Example on application of the PSA method to a conceptual design of a SFR system 84

Appendix 9 - R&D for the homogenization of the safety architecture’s design and assessment 85

Abreviations 91

Executive Summary

This document, the first major work product of the Generation IV International Forum (GIF) Risk and Safety Working Group (RSWG), presents the findings and recommendations of the group based on its work to date. Much additional work remains to be done by the RSWG. However, the objectives, principles, attributes, and tools presented in this document are intended to immediately provide designers of Generation IV systems with concepts and methods that can help guide their R & D activities in a way that promotes the safety basis and efficient licensing of advanced nuclear technologies.

The RSWG was formed to promote a homogeneous 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, potentially present a diverse set of design and safety issues. A number of these issues 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 more transparent than this current generation of plants.

The Generation IV research and development program is guided by a GIF IV Technology Roadmap document (Ref. [1]) which identified three specific safety goals for Generation IV systems "*to be used to stimulate the search for innovative nuclear energy systems and to motivate and guide the R&D on 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*.

In its first two years of existence, 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 and demonstrate achievement of these goals. This has been done coherently 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 (Gen II) in most countries of the world is already very good. In parallel, versus the Gen II systems, the quantitative safety objectives applicable to the reactors of the third generation (e.g. AP1000 and EPR) are very ambitious and guarantee an improved level of protection reducing the level of risk in a demonstrable way. The RSWG believes that this achieved level is excellent and can be kept as a reference for future reactors. Meanwhile, although not formally required, further safety improvement 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.

- 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 Gen IV systems and the need for an homogeneous strategy 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: be in agreement with current and foreseen future regulations; be able to demonstrate the full implementation of defence in depth; allow for a plants' design and assessment which will exhibit both deterministic practices and probabilistic objectives over an enlarged spectrum of design conditions, including severe plant conditions; handle internal and external hazards so as to achieve as much as possible the coherency with the approach adopted for internal events; allow 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 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 which 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, as a complement of the deterministic approach, the use of PSA techniques and complementary tools as design drivers throughout the design process.

- For Gen 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 Gen IV energy systems should cover the full range of safety significant conditions. The historical notion of a single bounding design basis accident must be replaced by a "spectrum" of possible accidents that, while low probability, represents with high confidence the range of physical events that could conceivably challenge the plant. Specific efforts should be made for demonstrating the "practical elimination" of initiators, sequences or phenomena associated with the extremely low residual risk. Among other considerations, these efforts should be based on the experience in the implementation of this concept for latest designs, specific R&D and engineering judgement.

  - Updated safety analysis methods should be applied to examine the full range of safety-significant issues. As part of an adequate treatment of the full spectrum of design conditions including the domain of severe plant conditions, these updated methods must, for example, consider internal events and hazards in a homogeneous way, the treatment of physical protection issues as well as of new sources of uncertainty.

  - Objectives and practices for the design improvement are identified within the report. 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 experience; 2) rationalization of the design approach by the deliberate adoption of the ALARP principle on a cost benefit basis 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 emphasise the treatment of the severe plant conditions through provisions of measures that help managing such conditions.

  - For these new concepts, the achievement of the safety demonstration's robustness rests on the capacity of the designer and the developer to be exhaustive in the recognition of risks stemming from phenomena considered for the design. Whenever possible, plant design features based on natural phenomena and physical properties of materials should be used to demonstrate, in an "intuitive" manner, the ability of the plant to arrest 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 s on workers and citizens.

  - Practical instruments are suggested to be used by the designers to support the design activity as well as the assessment activities. Among others, the Objective Provision Tree and the notion of Line of Protection which will allow schematizing the whole safety architecture. The availability of this systematic representation of the safety architecture may certainly help the plant design and assessment.

- **Future activities of the RSWG**

  - Finally it is worth noting that a specific section is devoted to the future activities of the RSWG. These will focus on further developing the objectives, the principles and the tools presented in this document, proposing a technology neutral general framework of technical safety criteria and assessment methodologies, testing and demonstrating the applicability of the given framework and assessment methodologies and finally proposing necessary crosscutting safety related R&D. Concerning the relationships with the developers and the designers, it is expected that

the definition of a common agreed safety approach will provide essential insights for the correct definition of the Gen IV systems' safety related R&D. Strong interactions have to be implemented 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 11 countries, Argentina, Brazil, Canada, Euratom, France, Japan, Republic of Korea, Republic of South Africa, Switzerland, the United Kingdom, and the United States have agreed to set up the Generation IV International Forum (GIF) with the aim to organize and co-ordinate international collaboration on research and development (R&D) for the fourth generation of nuclear energy systems (Generation IV). The Generation IV will represent new and better solutions to the world's future energy and environment challenges while allowing continued economic development and growth throughout the world.

The first units of the Generation IV nuclear energy systems (demonstrators or prototypes) are envisaged to be put in operation in the period 2020 - 2030. In order to get a favorable public perception they will have to be able 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 will likely introduce substantial innovative technological changes compared to current plants and these changes will have to be accommodated within a licensing and regulatory framework expected at the time of the deployment of these new systems.

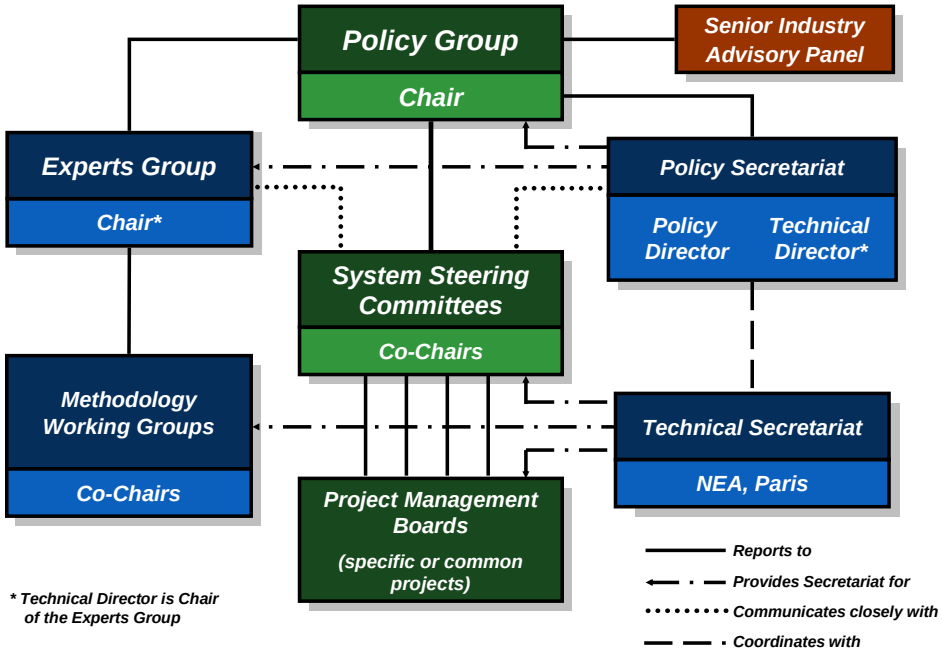
As described in its Charter and subsequent GIF Policy Statements, the GIF is led by the Policy Group (PG). The Policy Group is responsible for the overall framework and policy formation and for interactions with third parties. An Experts Group (EC) is advising the Policy Group on R&D strategy, priorities 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 System Steering Committee will plan and integrate 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 below.

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, physical protection and proliferation resistance in the context of R&D planning, in particular[1]:

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

[1] A Economic Methodology Working Group (EMWG) provides methods for the economic assessment

GIF Governance Structure



The primary objective of the RSWG is the implementation of a harmonized approach on long-term safety, and to address risk and regulatory issues in development of the next generation systems. To this end, the RSWG will focus particularly on proposing safety goals and evaluation methodology and advising and assisting the Experts Group and Policy Group on interactions with the nuclear safety regulatory community, and other relevant interlocutors including IAEA. Concerning the relationships with the developers and the designers, strong interactions have to be implemented 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.

On its side, 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 has to interact with the PR&PP Working Group to assure a mutual understanding of safety 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. The report should provide insights and assist the Experts Group and the Policy Group for the definition of the most adequate safety related Gen IV R&D.

In order to achieve the general objective, three more detailed objectives were defined that

have guided the development of the work:

- Motivate the need for an innovative approach;
- Provide the foundations for this approach;
- Help identifying the needed instruments & tools.

As a complementary objective it is worth noting that the document is also an essential contributor to help identifying the needed supportive crosscut R&D effort. The identification by the SSCs of system specific and dedicated R&D efforts will also take profit of the report content.
Although this report presents a number of thoughts and recommendations, it really represents only the start of the efforts for the RSWG.

I.3 Scope and Structure of the Report

This report is the first deliverable of the RSWG. It contains initial integrated considerations of the Group helpful to achieve and demonstrate an improved safety of future reactor systems. It emphasizes the need for a technology neutral approach capable of addressing the issues of all the Gen IV systems, i.e. for their design and their assessment.

After a short recall about the GIF background, the objective of the report its structure and scope (Introduction), 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 organizations. The key part of this Chapter is devoted to the scope of work that has been undertaken by the RSWG.

Chapter III proposes a Generation IV safety philosophy. It recalls and develops 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 Gen 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 Gen 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 a pilot application of the Objective Provision Tree (OPT) methodology, for assessment of the implementation of defence in depth concept in the design and operation of NPP, is described along with a simplified visualization of the OPT methodology. Insights from practical applications of this methodology are also summarized. Besides the first application to conventional High Temperature Reactors technology (Ref. IAEA TECDOC 1366), complementary example refers to the study performed by the Bohunice NPP (Slovak

republic) for the two units equipped with WWER 440/V213 reactors. The second example is related to the study performed within the context of the RSWG's work. In this study the OPT methodology was applied to assess the current design of the Japan Atomic Energy Agency Sodium Cooled Fast Reactor (JSFR). Possible commonalities in the analysis method between safety and PR&PP are succinctly addressed by the chapter.

In Chapter VI future activities of the RSWG are presented such as further development of the objectives, the principles and the tools presented in this document to achieve a technology neutral general framework for the Gen 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 attributes and characteristics of 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 from interested GIF Members. In addition, each SSC and the PR&PP Working Group may be represented by one representative. These representatives are responsible for informing the RSWG on risk and safety issues related to the relevant technological system or PR&PP issues/progress of work and for transfer of the findings and advice of the RSWG to the SSCs or to the PR&PPWG. The RSWG may involve other experts from external organizations as resource for advice and resolution of specific tasks. The Policy Director can act as a liaison to the RSWG for the Policy Group, and may attend RSWG meetings as an observer.

The RSWG has two co-chairs nominated by the representatives and approved by the PG. Currently representatives of the United States and of France are co-chairing the RSWG. 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, in practice it has been so far two times per year. The interface to the SSCs is assured through SSCs representatives. One of the co-chairs participates in meetings of the EG to inform the EG 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 are asked to maintain an active interface with the IAEA, which participates as an observer in the RSWG, and other international organizations that address safety and regulatory issues.

II.2 RSWG Terms of Reference

The revised RSWG Terms of Reference (November 2007) specify the following RSWG scope of work:

- *Identify and promote a common and consistent risk informed approach to safety in the design of Generation IV systems by:*
    - *Proposing safety principles, objectives and attributes based on the Gen IV safety goals 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 Expert Group and the Policy Group on the application of the safety approach for Gen IV systems.*
- *Promote development of a Generation IV safety database.*
- *Interact with the PRPP 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 Generation IV development*
- *Report annually to the Experts Group 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 for the correct definition of the Gen 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 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. Finally it has to be noted that the Multinational Design Evaluation Program (MDEP) initiative plans to address the Gen IV licensing and adequate interaction should be foreseen.

II.3 RSWG meetings

The scope of the RSWG work is demanding and may need to be further refined. The RSWG, in its first meetings, devoted considerable time to the discussion of the question of "how safe is safe enough". While recognizing that the answer to this question is of the responsibility of the countries' Safety Authorities the discussions led to identify and largely resolve a number of issues, e.g.:

- the content of a cohesive safety philosophy applicable to all the Gen IV systems
- the objectives and the ways to be pursued to meet the potential safety improvement
- the basic principles for an approach applicable to the design and the assessment of innovative systems including the ways to assess the adequacy of the defence in depth principle application and especially to address the treatment of severe plant conditions
- the role of passive features
- the possible role of available instruments (e.g. the PSA techniques) 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
- an agreed way for the integration of the physical protection issues
- an agreed approach to address internal and external hazards in a more coherent 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 (e.g. the severe plant conditions)
- the preparation of a comprehensive manual for the Objective provision tree implementation
- the identification of a clear path forward on how to define QA standards.

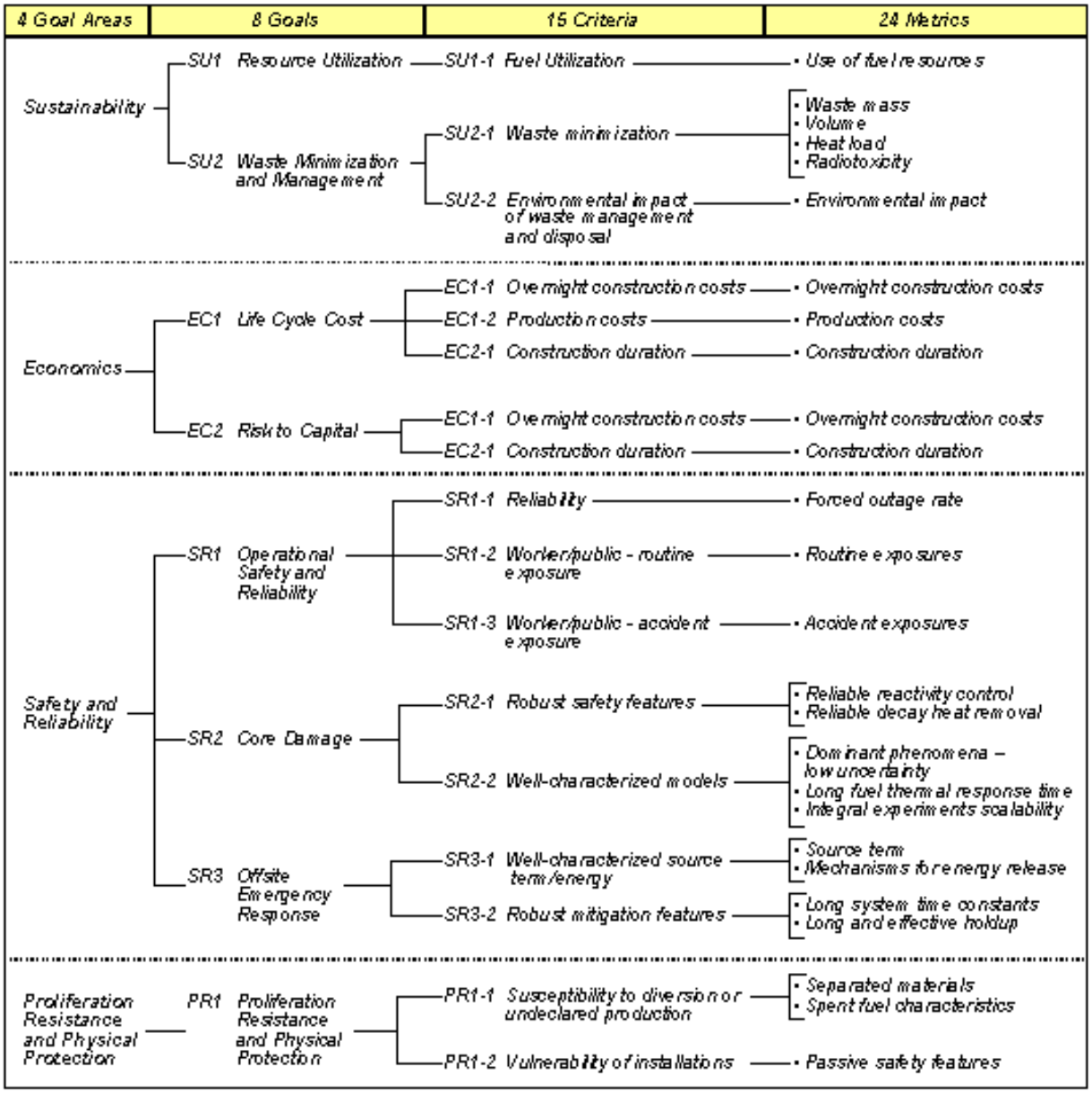
It was observed that development of advanced safety assessment methodologies (e.g. risk-informed approach), will be an evolving process, and the group agreed to build on the work performed elsewhere, in particular within IAEA and EURATOM projects.

Chapter III: Generation IV Safety Philosophy

III.1 Goals for Generation IV

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

Rollup of Metrics, Criteria, Goals and Goal Areas



Among these goals, improved safety and higher 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 safety margins are adequate, accidents are prevented, and off-normal situations do not deteriorate into severe

plant conditions. At the same time, competitiveness requires a very high level of reliability and performance.

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 with provision of design features that ensure that the plants can successfully control and mitigate any initiating events that might occur without causing core damage.

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 and that any potential releases of radiation will be small and have only insignificant public health consequences.

To this purpose it is interesting to point out that Gen IV goals are defined *"to be used 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."* Therefore these are not to be considered as mandatory.

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.

Aside from safety and reliability goals, proliferation resistance and physical protection are also essential priorities in the expanding role of nuclear energy systems; in particular the physical protection has to be explicitly considered and integrated within the design and assessment strategy as a complement of the safety concerns. Existing nuclear plants are highly secure and designed to withstand external events such as earthquakes, floods, tornadoes, plane crashes, and fires. But, given heightened concerns about such issues, further improvements have to be achieved by Generation IV designs. This goal points out the need to increase public confidence in the security of nuclear energy facilities against terrorist attacks. As indicated by the Ref. [1], physical protection against acts of terrorism has to be considered since the very first stages of the design to meet a level of protection commensurate with the protection of other critical systems and infrastructure.

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 of the world 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. The effectiveness of this organizational learning can be observed in a steady decline in the numbers of safety-related events that are occurring in operating plants in recent years. Further, one can state that 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 may represent Generation IV will require new thinking and new methods, using a proven stepwise 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.

As it has been done for 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 identification of the risks, which leans on the fundamental safety functions, must look for being 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 scenarios may be a 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 already exists that articulates much good thinking about safety philosophy. Notable examples include work performed and documented by the International Atomic Energy Agency, 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." As already mentioned, the RSWG, in its first meetings, 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 consensus 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.

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[2])
  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,

[2] 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.

when compared with Gen 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 Gen 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.

- **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 hazards in a - as much as possible - homogeneous 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, and 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, convection,

conduction, negative reactivity feedback, thermal inertia, and other "natural" physical processes. The ultimate expression of safety philosophy in Generation IV design would be 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 more simple and less critical, especially during critical phases of responding to off-normal conditions. It is expected that 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 Generation IV systems for a number of reasons that will include reduced operating costs, reduced capital costs, and overall improved plant productivity. One specific benefit of advanced instrumentation and control will be to improve the input to operators and therefore a reduced reliance on human intervention in the event of a safety challenge to the plant. Through improved plant automation, Generation IV systems could seek to minimize the need for human actions during critical phases of postulated accident conditions, but would allow for trained operators to intervene in situations in which their unique cognitive abilities and creativity may be beneficial. In short, through advanced automation, 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 demonstrating the capacity of the plant to successfully respond to a very 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 Gen 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[3].
- **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 prescriptive. It is nevertheless recognised that for innovative plants employing new technologies, it may be not be possible to apply such a performance-based approach due to the lack of practical experience, and the limitations of the relevant technology specific data.

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

- be in agreement with current and the - foreseen - future regulations
- to be able 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
- allow, for the installation's design / analysis, to manage simultaneously deterministic practices and probabilistic objectives
- 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
- allow to improve the safety demonstration for the domains where gaps still exist in the current state of art
- allow the demonstration of the achievement of a level of safety equivalent or even better with regard to the current systems.

The adoption of these criteria should on one hand guarantee that all the Gen IV designs will answer a set of coherent principles and, on the other hand, will help defining the necessary

[3] The term "Risk-informed" is linked to the USA practice and the understanding can be different in other Gen IV 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 built the safety architecture.

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 Gen IV systems which meet these technology neutral safety requirements are suitable for setting up the discussions with the regulators, for their licensing.

III.5 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 that as Generation IV conceptual designs continue to evolve, the specifics of how these principles should apply themselves in the various concepts will similarly evolve.

The important principles that the RSWG believes must be embodied in Generation IV technology include those discussed below.

III.5.1 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 extremely 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 some 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 uncertainties that, from both a design and a regulatory point of view, will require defence in depth that will be set up in ways that have not been seen before. 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 that have come to be available to focus defence in depth design provisions in such a way as to cost-effectively optimize the value of that defence in depth. 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 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 correctly designing the provisions with fulfilling the requested missions for each DiD level. The performances of these provisions have to be defined in terms of physical performances and required reliability; following these requested performances the provisions have to be – if needed/justified – adequately 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 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).

Others 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 identification of the risks, which leans on the fundamental safety functions, should look for exhaustiveness; the identification of the corresponding scenarios to be retained to design and size the safety architecture provisions must be as exhaustive as possible. It has to be noted that, coherently with the defence-in-depth principle possible lacks of exhaustiveness are compensated by consideration of enveloping situations which are taken into account independently of their expected occurrence frequency (single failure criterion; margins; postulated combinations; etc.).

- A graduated, progressive defence; without that, "short" sequences can happen for which, downstream from the initiator, the failure of a particular provision entails a major increase, in terms of consequences, without any possibility of restoring safe conditions at an intermediate stage[4].

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

- 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.

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.

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.[5]
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 GEN IV systems.

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

[5] 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.

III.5.2 Risk-Informed Design

Probabilistic safety assessment has become a highly sophisticated tool to identify potential accident scenarios, quantitatively estimate their probabilities of occurrence in a defined time period, and probabilistically estimate the consequences associated with postulated accidents in terms of a number of consequence parameters. Along with the traditional deterministic methods, the 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 evolutionary plants (Gen 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 Gen IV systems (Section III 5.1). Ideally these techniques will be applied from the earliest phases of Generation IV plant design. During the more 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 maturing 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 (Section III.5.1: exhaustiveness, progressiveness, tolerant, forgiveness, balanced, simplicity). Specific tools as for example the Objective Provision Tree (OPT) and the notion of Line of Protection (LOP) (see Chapter V and Appendix 3) have to be developed to help assessing their achievement; that will allow the designer to 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.

The logic of these tools is quite simple: for a given level of defence-in-depth, and according to the progress of the approach (*Safety functions ⇨ Challenges ⇨ Mechanisms ⇨ Provisions*), the full set of provisions needed to address a given mechanism, and so to realize the wanted mission, represents the Line of Protection. 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. The corresponding R&D work to support the development of these

tools and the methodology to implement them for the safety analysis, is an important objective within the context of the re-exam of the safety approach definition and content (see Appendix 3).

III.5.3 Simulation, Prototyping, and Demonstration

Notably, new generations of aircraft are now being created almost entirely by modelling and simulation, with wind tunnel testing and prototyping being used primarily as late-stage verification of final designs. Similarly, significant research and development that is currently being done around the world has the potential for reducing the duration of the development cycle, reducing both research and capital costs, and improving the safety of Generation IV systems.

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.

It is obvious, of course, that the use of PSA to drive Generation IV design is really just one application of this idea. However, similar benefits can 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 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 qualification 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 (Gen III) is based on past experience without putting into question the major principles established for the safety architecture. Their safety demonstration is achieved in a deterministic way, supplemented by probabilistic methods and appropriate research and development work.

Both deterministic and probabilistic methods are employed to identify the conditions that are to be addressed (i.e. challenges and mechanisms) and to design the provisions implemented to cope with them. The major sources for the identification and selection of challenges are current licensing practices and operational experience feedback.

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 to an initiating event, a sequence or a situation is assessed as unacceptable, further specific provisions are implemented:

- if possible, to consider the initiating event, the sequence or the situation, among the plant conditions addressed and managed by the design, with an acceptable cost (ALARP);
- otherwise to "practically eliminate" the initiating event, the sequence or the situation by showing, with a robust demonstration, that 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.

The latter (initiating event, sequence or situation) are considered as rejected within the Residual Risk (RR) (see Section IV.3.5 and Appendix 4).

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

- Conditions included in the Design Basis Conditions (DBC)[6]
- Conditions included in the Design Extension Conditions (DEC)[7].

The deterministic approach has been implemented for past and current plants for design and analysis purposes mainly related to the DBC; it uses 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 consider conditions generated by mechanisms which frequency of occurrence is higher than about 10^{-6} per reactor year. Several categories are conventionally defined and allowable consequences are defined for each of these categories by national regulators.

[6] 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.

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

The probabilistic approach is based upon the systematic consideration and combination of initiating events – with their own frequency of occurrence – and the frequencies of failure for 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 (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. Gen IV Systems: a need for re-examining the safety approach

The systems selected by the Gen IV initiative shows a large variety of technologies, issues and options to address these issues; this variety justifies the implementation of a re-examined agreed safety approach for their design and assessment. As far as the proposal for the definition of this approach is of the responsibility of the RSWG, it will be considered, once endorsed by GIF, as agreed at Gen IV international level.

The 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 the Gen 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 and sketched there. Ultimately such an approach allows guaranteeing that the Gen IV systems meeting these technology neutral safety requirements are suitable for deployment with regard safety.

The Appendix 5 shows the main characteristics of the Gen IV systems. The improvement of safety being a key objective, the appendix tries to identify the fields where significant technology gaps, related to safety, exist. Safety related specificities are pointed out.

Based on the Gen IV Technology Roadmap content, the table below summarizes, for each of Gen IV systems, the fields where safety related technology gaps are recognized.

	GFR	**LFR**	**MSR**	**SFR**	**SCWR**	**VHTR**
Updated Safety Approach	**X**	**X**	**X**	**X**	**X**	**X**
Fuel	**X**		**X**			**X**
Neutronics			**X**		**X**	
Thermal aerolic/hydraulic	**X**				**X**	**X**
Materials & chemistry	**X**	**X**	**X**	**X**	**X**	**X**
Fuel chemistry			**X**			
Passive Safety		**X**	**X**			**X**
Severe accident behaviour	**X**	**X**	**X**	**X**	**X** **F**or fast spectrum	**X**

	GFR	LFR	MSR	SFR	SCWR	VHTR
System Specific Features			Coupling with the fuel cycle installation			Coupling with the heat process installation
ISI&R		X	X	X		

IV.3. Design of innovative systems

IV.3.1 Objectives and ways for the design improvement

Compared to the level already achieved by the current Gen III plants the Chapter III indicates the elements on which the effort for the safety improvement has to rest: the notion of "optimal risk reduction" (ALARP); the consideration of ambitious objectives; the opportunity brought by progress in knowledge and technologies; the priority given to the prevention without forgetting the mitigation; the search for robust safety architecture; and finally the requirement for the improvement of safety demonstration's robustness.

The needed characteristics of an adequate safety approach are also resumed: risk-informed; understandable, traceable, and reproducible; defensible; flexible; performance-based (when possible). Complementary criteria are defined: 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.

Chapter III also defines important "boundary conditions" (principles, objectives and criteria) that should define an effective "safety basis" for Generation IV systems: 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 (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 Gen 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[8] is build up to insure the operability, the availability and the safety of the system (Fig. IV.1).

[8] 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*

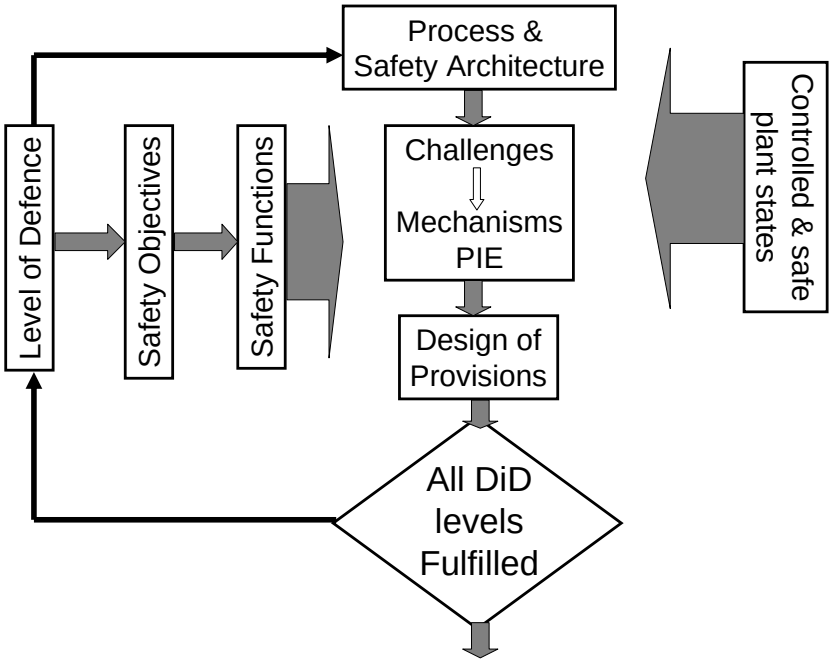


Fig. IV.1– Iterative process for the construction of the safety architecture

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, as already indicated, for future systems, an improved coherence with the treatment addressing internal and external hazards has to be looked for.

Finally, it is worth recalling that, as regards severe plant conditions, the organization of the safety design and demonstration, in particular concerning the consideration or the non consideration 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 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 consider the DBC as being addressed by the levels 1 to 3 of the DiD (cf. the INSAG 10 terminology (Ref. [3])) : *Prevention of abnormal operation and failures* > *Control of abnormal operation and detection of failures* > *Control of accidents within the design basis*), and the DEC as being connected with the levels 1 and 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 Gen IV systems.

It is important to point out that the completeness and the coherence of the R&D plans for the

different Gen 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 Gen 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; for it the RSWG will clarify later their nature and the modalities of their integration in the design of the safety architecture.
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 prerequisite for the development of a PSA model which will be used later 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;* see Section III) will also be checked.

IV.3.4. Design Extension Conditions

The suggested link of DEC with the 1st level of the DiD is justified by the need to prevent any severe plant conditions with intolerable consequences. Similarly the objective could be the practical elimination of each initiating event, sequence or situation for which it is not realistic to set up provisions for mitigation. The corresponding actions are in charge of the designer (Section IV.2).

Having said that, in addition to the design which fulfils the objectives of the Design Basis Conditions, and coherently with the 4th and 5th level of the defence in depth, a number of Design Extension Conditions (DEC) shall be considered to complete the design of the plant to assure, with a sufficient degree of confidence, that their consequences would be mastered.

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.
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 guideline value. Complementary quantitative probabilistic objectives can be defined for design purposes but they should not be mandatory:

- Guideline value for all the severe plant condition, initiated by events of internal origin, which induce severe core degradation: <10-6 per reactor year.
- Design of the installation so that the internal and external hazards are not dominant contributors for these radiological releases.

Following the logic already discussed for the OPT, as applied for the DBC, in considering design extension conditions, and in order to mitigate their consequences, the designer should identify the need to introduce additional provisions or the need to over-size some already present provisions. The consideration of these design extension conditions would allow the designer to define the right 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 equipment can be made.

Rules for the consideration of DEC

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 independency of provision needed to mitigate a severe accident versus those provided to fulfil DBC requirements (this item is directly linked to the independency 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.

All these items have to be discussed by the RSWG and an agreed position has to be found, applicable to all the Gen IV systems.

IV.3.5. Residual Risk

As indicated in section IV.1, as regards severe plant conditions single initiating events have to be "dealt with" or "excluded". Initiators, sequences or situation, 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". The detailed analysis of PWR examples confirms that two families of events have to be addressed in this respect:

- initiators/situations who can lead to the severe plant conditions or to the unacceptable degradation of the conditions of the installation[9]. This can be done by making these initiators/situations highly improbable if they cannot be eliminated by design (i.e. made physically impossible).

- specific situations during the progress of severe accident 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[10].

[9] E.g. : Fast reactivity accidents due to deborated water slugs

[10] E.g. : Direct Containment Heating (i.e. pressurized core melting); Steam explosion leading to large early releases

According to the above safety objectives, for each of these scenarios, sufficient design and operation provisions have to be taken to design them out.

In terms of application of the defence in depth (DiD), it is worth noting that the provisions which are to be implemented do not belong to the same levels of the DiD. For example. coherently with the logic of the Objective Provision Tree (OPT), provisions on design, manufacturing and operation, allowing the practical elimination of the items from the 1st family, 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, avoiding counterproductive consequences[11], will be identified during the analysis of challenges /mechanisms matching with the 3rd level of the DiD.

For the second family, above, the provisions are identified within the framework of the 4th level of the DiD. The installation is in a degraded situation (e.g. core melting), the designer has to make sure that the management of this plant condition allows, according Ref. [3], the mastery of "*severe conditions including prevention of accident progression and mitigation of the consequences of a severe accident* "[12].

For PWRs the list of initiators and situations to be practically eliminated is defined deterministically. It is the 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.

The situation is not the same for the innovative concepts which miss this feedback experience and for which the OPT can allow on one hand to dread better the search for the exhaustiveness and, on the other hand, to establish a means of communication between the designers themselves and between the designers and the safety authority.

IV.4. Assessment of innovative systems

The adequate selection of the design basis conditions, the use of enveloping and/or conservative computer codes and 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; i.e.: the latter are kept away from unacceptable damage occurrence with sufficient margins. These margins include room for insufficient knowledge or 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)

[11] I.e.: generating mechanisms which can in turn play the role of initiators; e.g. deborated water within the primary circuit caused by an SGTR.

[12] E.g. : High pressure core melt situations

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).

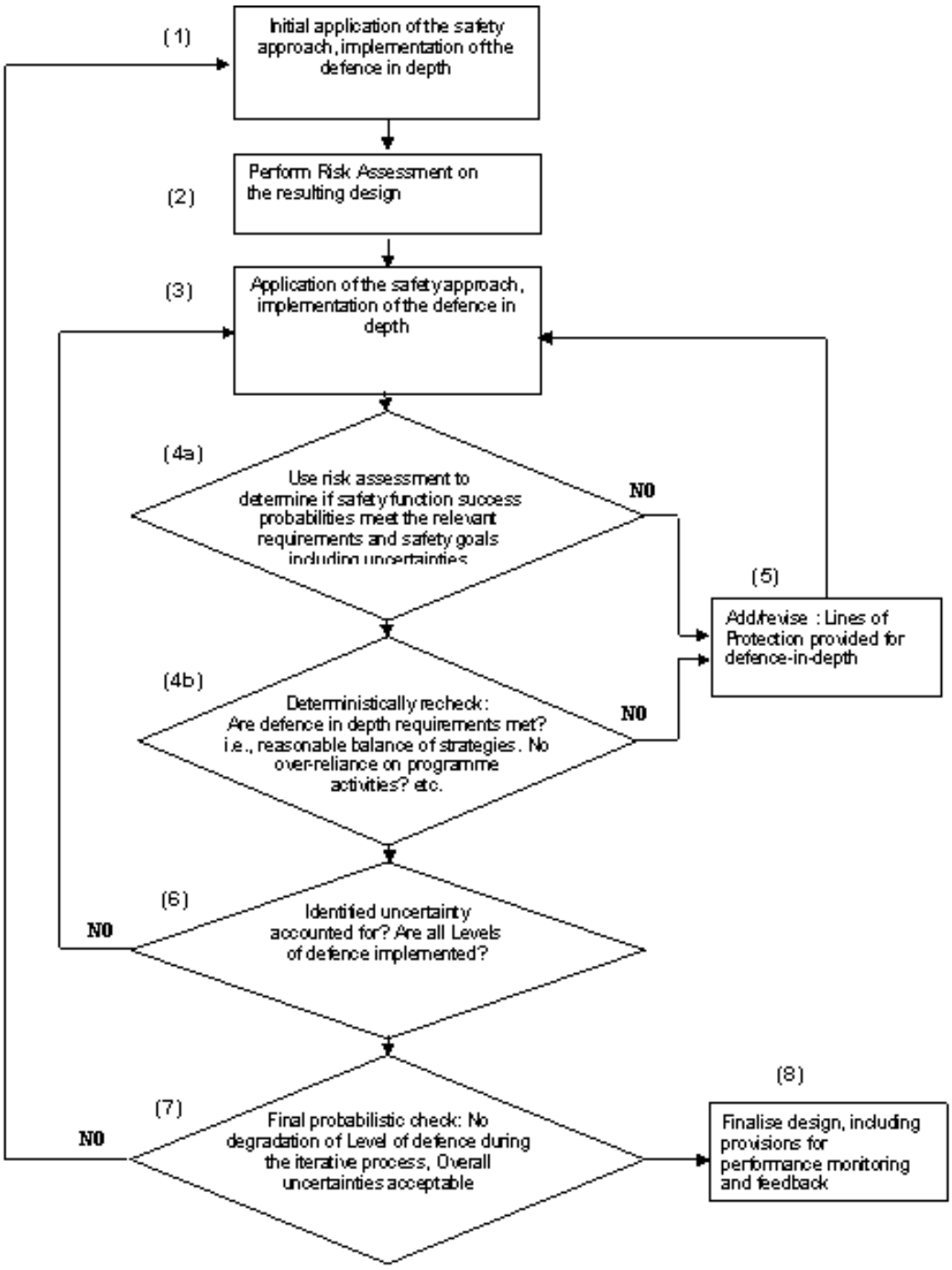


Fig. IV.2 – Design assessment: Process used to ensure that adequate defence in depth is achieved.

Stage(1) - Review of Levels of Defence

Once an initial design has been developed (see Fig.IV.1; i.e. the 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 PIE identification, 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 safety assessment. The safety assessment 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 Required 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*; cf. section III). 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 has been 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 phenomenology and this may require 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. Generation IV Safety Methods and Tools

In the previous Chapter IV, the implementation of a re-examined safety approach for GEN IV Reactor Systems was justified because of the variety and innovative type of those systems. This approach is aiming at achievement of coherent safety design and assessment of defence-in-depth (DiD).

The updated approach introduced for this sake is a "risk-informed" approach, utilizing a deterministic approach complemented with a probabilistic one. The implementation of DiD safety philosophy shall be addressed by the former one, while the achievement of implementation shall be qualitatively and quantitatively assessed by the latter one.

In the previous chapter, an Objective Provision Tree (OPT) method was suggested as a deterministic method, and the probabilistic safety assessment (PSA) as a probabilistic method. Consequently, in this chapter, the method of OPT will be explained and the way of its utilization for GEN IV Reactor Systems will be described.

The second part of this chapter describes the utilization of the PSA method in the stage of a preliminary conceptual design for the Generation IV advanced reactor systems.

Thirdly, similarities of the methods utilized both in the area of Safety and Proliferation Resistance & Physical Protection (PR&PP) will be touched, though further investigation by the RSWG on this matter is to be expected in the future.

Finally for illustration, two pilot applications of the OPT method are presented, which were performed by the Bohunice NPP for WWER 440/V213 reactor units and by the Japan Atomic Energy Agency for the current design of the JSFR sodium reactor.

V.1 Objective Provision Tree

The Objective Provision Tree (OPT) method has been proposed in Ref. [4] for the purpose of assessing the implementation of the DiD philosophy in the safety architecture of Nuclear Power Plants (NPPs) through visual presentation.

The OPT method is a top-down method with a tree structure which:

- for each level of DiD (normally level 1 to 4, sometimes to 5),
- and for each safety objective/function (in general, control of reactivity, removal of heat from the fuel, and confinement of radioactive materials) and for each safety principle,
- picks up challenges and mechanisms to the safety objectives/functions/principles,
- and provided provision(s) to prevent or control the challenges/mechanisms,
- by expressing this hierarchy structure relation in a tree form.

In the present state, a comprehensive manual (or guide) of the application of the OPT method has not been prepared yet. Nevertheless, Ref. [4] contains a comprehensive example of its application to modular high temperature gas cooled reactor for the purpose of assessing the implementation of DiD philosophy in the safety design. This type of application might be useful to overview the safety features in the plant design.

On the other hand, detailed utilization method of OPT for assessing the implementation of DiD philosophy in all the phases of the plant is shown in Ref. [5] together with an application example to an existing LWR. This type of application would be utilized to confirm fulfilment of each safety principle one by one (the example of the detail application of OPT methodology to WWER type of reactors is further discussed in this Chapter).

The OPT method is an approach expressed with plural figures of trees, and, in general, there are three levels of structures which form the logic framework of this method. Although it is a top-down method, the following explanation will be given in a bottom-up way for easier understanding:

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

In this section, these three structures are succinctly described. Details, with documentation for OPT review, and usage of the OPT method are available within the Appendix 3.

V.1.1 Elemental structure of OPT

The elemental part of the OPT structure exists at the lowest part of the tree (see Fig. V.1). This structure consists of a specified mechanism that could deteriorate safety function, and a set of provisions that is designed to work jointly to prevent or control the mechanism. The provision will be single or plural, and include hardware, engineered systems, passive or inherent features, operator's actions, administrative procedures, and so on. If plural provisions are implemented and all of them are expected to work simultaneously or sequentially (in other word, "AND logic") to achieve the mission, those provisions are placed in a vertical manner and connected with a vertical line. For a given level of the DiD, such a set of provisions is called as a Line of Protection (LOP).

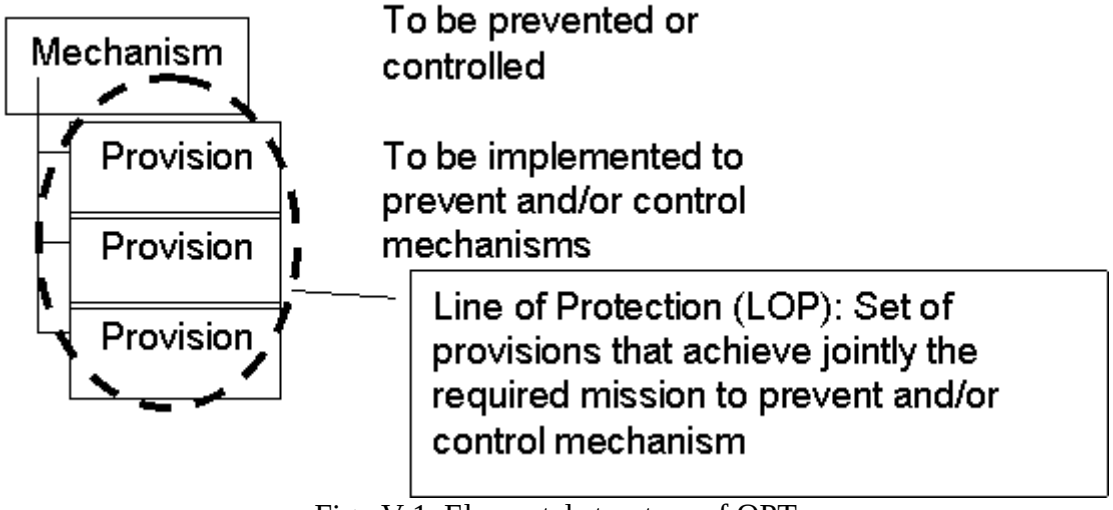


Fig. V.1 Elemental structure of OPT

While the aim of OPT methodology is to express all sets of provisions against all challenge/mechanism, this lowest part of a given tree shall be called as elemental structure in this report. The part of the tree for deductively deriving challenges/mechanisms from the safety function is the hierarchy structure of a OPT, which is described below and detailed within the Appendix 3 and 6.

V.1.2 Hierarchy structure of OPT

The hierarchy structure of OPT expresses the process of deducing safety-deteriorating mechanisms and provisions to cope with these mechanisms, starting from the DiD level and safety objective at the upper part of the tree. Normally, the hierarchy structure of an OPT consists of the following levels from the top to the bottom (see Fig. V.2):

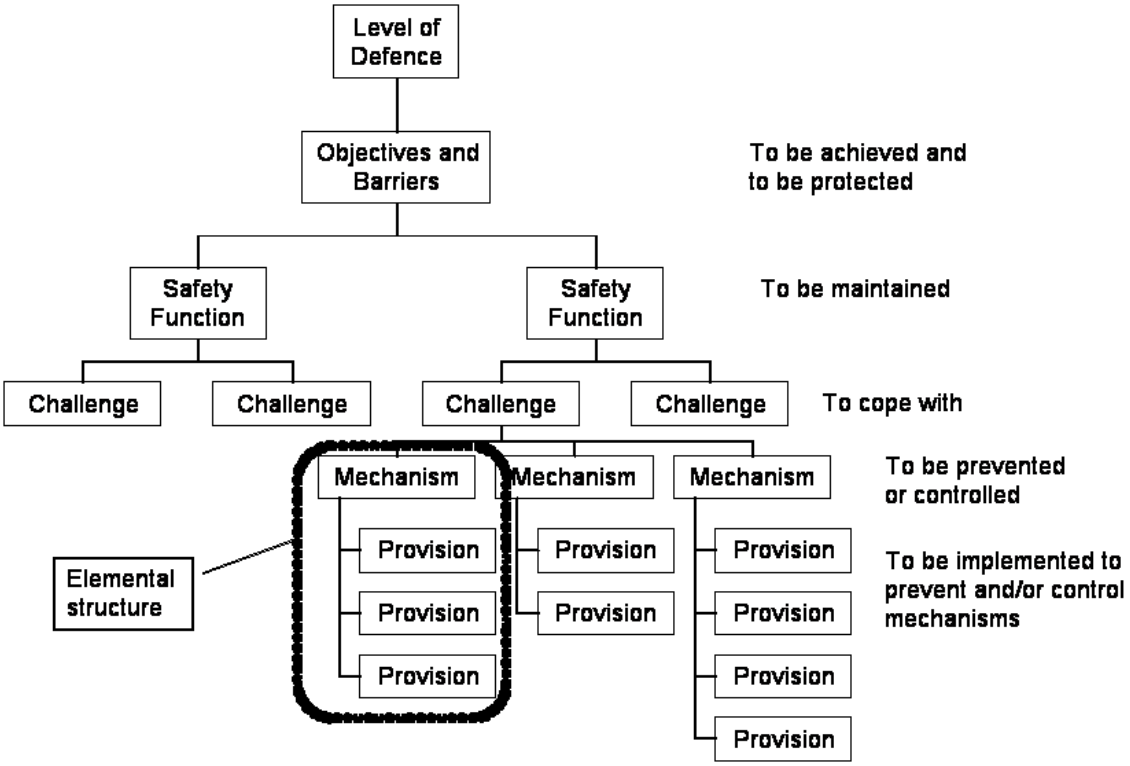


Fig. V. 2 Hierarchy Structure of OPT

- Level of DiD level 1 to 4 or 5
- Objectives and Barriers to be achieved and to be protected
- Safety Function to be maintained (to be performed successfully)
- Challenge to cope with (e.g. disruption of heat transfer path)
- Mechanism to be prevented or controlled (e.g. loss of coolant)
- Provision to be implemented to prevent and/or control mechanisms.

Normally, level of DiD and Objectives/barriers are uniquely appeared once in an OPT as shown in Fig. V.2.

V.1.3 Safety functions/principles and relevant DiD level to be assessed by OPT

As it was mentioned in the beginning of Section V.1, there are two types of OPT method

utilization. The Appendix 7 describes in detail the relation amongst Levels of DiD, safety principles (SPs) and safety functions for each method.

What is essential to capture is that this relation and the lists generated address the use of OPT method for all the phases of the plant life; the lists were made for existing LWRs and the example OPTs found in Ref. [5] were formed on the same conditions. The set of Safety Principles (SPs) themselves in Ref. [6] also has the same background. Nevertheless, these lists and examples OPTs would be also applicable to liquid metal cooled reactors, super-critical water-cooled reactors, and gas-cooled reactors with slight modifications. On the other hand, molten-salt reactor might be paid a special attention because some SPs could be different from those for LWRs.

V.1.4 Documentation for OPT review

The application of OPT methodology will result in development of a number of trees usually self-explanatory. It is however, necessary to prepare a complementary documentation along with the graphical structures to explain the appropriateness of the OPTs and in particular to give:

- arguments of appropriateness to derive "mechanism" from "safety function" and "challenge" and
- arguments to show that a set of provisions can prevent or control the safety-deteriorating mechanism.

In some cases, analytical results or experimental results would be needed to justify the appropriateness of the provision(s) against the mechanism. This might be one of the biggest challenges for GEN IV Reactor Systems in case innovative provisions are foreseen.

V.1.5 Utilization of OPT in the stage of preliminary conceptual design

The basic iterative approach to address the preliminary design of an innovative system is shown in Fig. IV.1 (§IV.3.2).

This section is devoted to describe the utilization method of the OPT in the preliminary conceptual design stage, or the viability phase, of the Generation IV nuclear power plant.

Method 1: Ref. [4]

- OPT shall be produced for each level of DiD from 1 to 4, and
- For each fundamental safety functions (control of reactivity, removal of heat from the core, and confinement of radioactive materials).
- Totally (4 x 3 =) 12 OPTs shall be produced.

Method 2: Ref. [5]

- OPT shall be produced for each Safety Principle (SP) mentioned in Ref. [6] (totally 53 safety principles), and
- For each level of DiD on which the relevant SP should be considered.

Advantages and weak points for each method are detailed in Appendix 7. They can be summarized as follows.

Namely, by Method 1, an OPT helps a user to overview the integrated safety features in the plant for the fundamental safety functions in each DiD level, and thus one can use this method to assess and confirm the balance of safety measures among the DiD levels, and to share a common understanding about the safety measures between the designers and regulators.

On the other hand, by Method 2, a user could focus on a specific Safety Principle, and confirm or analyze the sufficiency of the safety provisions against each SP in detail. However, Safety Principle does not always correspond to one of the three fundamental safety functions, but they include compound requirements for safety design, or more generic safety requirements.

Considering these complementary characteristics of integration and analysis, RSWG would propose a combined approach of the OPT utilization in the preliminary conceptual design phase as described below. The integrated plant safety design or its balance of arrangement shall be assessed by Method 1 at a level of each of the fundamental safety function and each DiD level. The compliance of the safety design (measures or policies) with each of the derived Safety Principles shall be analyzed and confirmed by Method 2. A preliminary RSWG proposal is discussed in Appendix 7.

It could be noticed that GIF Roadmap requires "preliminary safeguard and physical protection strategy" as one of the endpoints of the viability phase. In this connection, production of an OPT for "SP 242 Physical Protection of the Plant" will be a good exercise for this endpoint deliverable.

V.2 Use of PSA in the preliminary conceptual design phase

In the Section III.4 and III.5.2 among principles that characterize safety of Generation IV systems, risk informed design process and the defence in depth philosophy were pointed out. Furthermore, it should be recalled that the Roadmap of Generation IV requires a simplified PSA as one of the endpoints of the viability phase. Therefore, this section describes the utilization of PSA of advanced/innovative nuclear energy systems.

PSA itself is already a fairly matured method through its application to existing LWRs which have more than 11,000 reactor-year operation experience in the world.

On the other hand, if PSA method is applied to innovative reactors of Gen IV systems, the uncertainties of the results will normally be larger than those for existing NPPs, and thus careful attention must be paid in the usage of the absolute values of the PSA results such as a comparison with a quantitative goal or with results of other reactor designs.

However, a relative comparison between the PSA results is reasonable if those analyses are made under the same conditions and for the same type of reactor system. For example, in the safety design of a nuclear power plant, a designer can compare and select a better design option among several ones by comparison of the PSA results for each option (if they are conducted with the same analytical conditions).

A good example is shown in Ref. [7] which describes an application of the PSA method to a conceptual design of a sodium-cooled fast reactor. In the selection of the configuration of decay heat removal systems (DHRSs), a simplified level-1 PSA was conducted for 4 options

of DHRS based on the same analytical conditions. The results were compared to each other, the characteristics of each option were clarified, and the option with the lowest risk was selected and proposed by the designer. Details about this example are given in Appendix 8.

Even though various difficulties could be prospected during PSA as described above and detailed in Appendix 8, RSWG encourages the designer to utilize the PSA method in the phase of a conceptual design.

Although simplified PSA results are expected at the end of the viability phase, RSWG again strongly recommends the designers to use the PSA method not only as an assessment tool of the final design at the end of that phase but also as a tool to support the designing process itself. The PSA method could be used for supporting design activities such as comparison/selection of design options, classifying abnormal events/accidents and their consequences for adequate arrangement of prevention/mitigation measures, considering operating procedures in the abnormal conditions and accident management, and identifying R&D items for reduction of risks and uncertainties. Those efforts during the viability phase would lead the design to a sufficient level of details from the viewpoint of safety and reliability, and hence a simplified PSA could provide the information that is expected in the Roadmap at the end of the viability phase.

V.3 Relation with the PR&PP evaluation method

There is rather close relation between safety and proliferation resistance and physical protection (PR&PP), which is also one of the four primary goals of Generation IV. Although in-depth discussion is to be done, some remarks will be made in this section for further consideration about more collaborative and consistent assessment measures between the two areas in the future.

V.3.1 Commonalities in the analysis method between safety and PR&PP

In the safety area, the process of an accident analysis can be expressed as follows:

Accident initiators -> System response -> Consequences

In the PR&PP area, the analytical process is similar (Ref. [8]):

Challenges -> System response -> Outcomes

Therefore, these two assessments require similar information for description of the problems and the analysis of the system responses. In the previous section, it is recommended to use the PSA method iteratively in the design phase. On the other hand, assessment of the PR&PP features is also recommended during the design process. Hence, it might be recommended that both assessments would be conducted in parallel.

As for the assessment tools, the event tree/fault tree method, which is a regular method for PSA, could be used for the pathway analysis of PR&PP. Similarly, instruments which are proposed by the RSWG, and in particular the "*Objective Provision Tree – OPT*", seem adequate to fulfil the objective, especially for the physical protection.

For the practical implementation, the basic idea is the identification, as a complement of the

"safety functions" (which allow – through the OPT – identifying the needed provisions and organizing the safety architecture of the system), of "security/safeguards functions" which allow to integrate, with a similar logic, the specific concerns of physical protection and could allow to identify the needed provisions. Moreover, the availability of trees which merge provisions for safety purposes and for physical protection purposes will allow the designer to verify the absence of negative interactions.

Actually, Table A6.2 (cf. Appendix 7) quoted from Ref. [5] suggests that an implementation of the Safety Principle 242, "Physical protection of plant", would be examined by the OPT method for level 1 and 2 of DiD. An example of the OPT for SP 242 is shown in Ref. [5]. Therefore, this possibility could be investigated further in the future.

The debate remains open on the feasibility of such an extrapolation to the problems of the proliferation resistance, the latter being more far from the logic of the safety's concerns.

V.3.2 Commonalities in countermeasures of safety and PR&PP

There is also a similar but slightly different feature in countermeasures for safety and physical protection particularly. In the safety design area, operator's intervention tends to be reduced in order to minimize the risk from human errors. One of the solutions is the introduction of passive safety systems. In the PP area, in order to minimize the risk from the group with malicious intention, such a safety system that requires minimum operator's intervention is more preferable. Although a passive system could be one of the solutions, an essential feature is not the passivity itself but rather a configuration where human intervention cannot disturb or stop the safety function achievement. For example, DHRS with natural circulation is a passive system, but it doesn't work if the heat transfer path to the ultimate heat sink is blocked intentionally. On the other hand, one cannot intervene the function of a passive self-actuated shutdown system (SASS) utilizing the Curie point feature because the whole system of SASS is contained within the primary system.

These examples show that there are common aspects in the analytical methodologies and countermeasures of safety and PR&PP, while a careful discrimination of the differences should be noticed. In order to realize a well-balanced and rational design of a nuclear facility from the viewpoints of safety and PR&PP, more consistency would be pursued between the safety and PR&PP design areas, even though it might take time.

V.4 Objective Provision Tree Demonstration/Case Study

A pilot application of the Objective Provision Tree (OPT) methodology for assessment of the implementation of defence-in depth concept in the design and operation of NPP was performed by the Bohunice NPP for two units equipped with WWER 440/V213 reactors. The scope of the study was limited to a number of selected safety principles related to Level 3 and 4 of defence in depth in the areas of siting and design.

Within the work of the RSWG an effort was made to apply the OPT methodology to assess the current design of the Japan Nuclear Cycle Development Institute Sodium cooled Fast Reactor (JSFR).

Main insights from both case studies are summarized below.

V.4.1 Experience of Bohunice NPP

A test application of the OPT methodology to assess the implementation of DiD has been performed by the staff of the Bohunice plant within the framework of the safety upgrading programme for the V-2 plant. The Bohunice V-2 plant consists of two units equipped with WWER 440/V213 reactors.

The scope of the study was limited to several selected safety principles related to Levels 3 and 4 of defence in depth in the areas of siting and design, namely to the following safety principles (Ref. [6]) as follows:

- SP 142 Ultimate heat sink provisions
- SP 150 Design management
- SP 154 Proven technology
- SP 158 General basis for design
- SP 168 Automatic safety systems.

During the exercise no OPTs were developed. The plant staff concentrated on the safety evaluation of the adequacy of the available NPP Bohunice provisions to prevent mechanisms and challenges as identified in the IAEA OPTs developed for LWRs.

Although, the evaluators have found a few new provisions, not included in the original IAEA trees, these findings were not further addressed, since the study was considered more as an inventorying of "defence-in-depth" provisions, rather than OPTs development exercise.

The evaluators pointed out that although in general they found the approach to be based on a sound concept, it was difficult in some cases to find the requirements or basis for justification of the adequacy of plant provisions.

Due to the large number of provisions, mechanisms and challenges, some coding system would have been helpful for practical reasons in full scope applications. A coding system was suggested to be developed in the future version of the approach. Development of an electronic version with links to various supporting documents was recommended to provide correct and full information from original documents in support of appropriate evaluation of particular provision. It was suggested to provide the user with easy crosschecking capability of evaluated provisions, mechanisms and challenges, to assist in ensuring consistency and quality of the screening process. The system was suggested to be flexible to allow the user to establish links to the existing plant documentation, too.

In general, the experience of Bohunice NPP exercise was positive, however not very much applicable to Generation IV design issues, since the exercise did not look for identifying of provisions, but rather was assessing the availability at the plant of the provisions already specified by the IAEA. What could be important for GEN IV systems however, is the identified need for having clear quidance on how to assess the adequacy of the safety provisions.

V.4.2 Experience from the pilot use of the OPT methodology for JSFR

Contrary to the exercise of Bohunice NPP the designers of Japanese Sodium Fast Reactor

made a pilot study and used the top-down approach to identify the safety objectives, functions, challenges, mechanisms and provisions needed to ensure adequate implementation of defence-in-depth for their design (Ref. [9]). They addressed the three fundamental safety functions, namely:

1. Control of reactivity;
2. Removal of heat from the core;
3. Confinement of radioactive materials and control of operational discharges, as well as limitation of accidental releases,

and developed 12 OPTs (e.g. for each function and each first four levels of defence in depth).

The exercise was found useful and productive to confirm realization of the reactor safety design based on the DiD philosophy. Furthermore it was noted that the approach suggested could be very useful for application at different stages of the design process, e.g. starting from conceptual design and finishing with detailed plant design for construction. The application of OPT method for screening of DiD application at each design stage facilitates the selection of different options and allows effectiveness of concurrent provisions to be evaluated. The authors of the study however recommended that the proposed assessment method, being a qualitative/screen out one, should have been complemented with some quantitative assessment, e.g. PSA. PSA could help to determine quantitatively the safety significance of different design provisions, however this in its turn may be not easy and feasible at an early design stage due to the lack of reliability data needed to support such studies.

One of the areas, where the support of the RSWG would be appreciated, with respect to the application of OPT methodology for GIF reactor systems, was suggested to be the development of a guidance for designers. This guidance will provide recommendations on how to apply the methodology and develop OPTs in a consistent manner and will help to distinguish well between challenges and mechanisms, areas where difficulties were experienced during the JSFR exercise.

V.4.3 Conclusions

Both studies, the Bohunice NPP and JSFR, have demonstrated that there is a lot of potential benefits for the GIF reactor designers from the application of OPT methodology. It can help to ensure that at each stage of reactor system design adequate provisions are foreseen to ensure the application of all 5 levels of the DiD concept and identify topics where more research/evidence is needed to prove this statement.

In order to facilitate the designer's use of OPT methodology it will be important for RSWG to develop an application guide. This guide can be established in an electronic form to facilitate the building up of OPTs and provide predetermined options to be selected for safety objectives, functions, challenges, mechanisms, provisions (at least for the technology neutral ones). The reference to any available safety requirements for any of those items can also be incorporated and be available for designer consultations. The experience in building detail OPTs for LWR and HWRs (used in the Bohunice exercise) can be repeated by the RSWG for the GIF reactors context. The experience gained by the GIF PRPP working group in development of an integrated web-based platform to support designers' assessment of PRPP could be useful, too.

As any safety assessment methodology, the OPT has its limitations which are mainly related to the evaluation of the adequacy of the identified provisions and their prioritization or determination of their safety significance. It is clear that for these issues traditional deterministic (accident analyses) and probabilistic safety assessment will be needed to complement the OPT. A number of iterations of combined use of all these methods will have to be done, as described also in chapter IV.3, to ensure that a comprehensive and systematic assessment has been performed for each of the GIF reactor systems.

Chapter VI Future activities of the RSWG

The future work of the RSWG has to cover three different objectives:

- To develop and finalize the definition of the safety principles and the safety objectives introduced into the previous chapters (i.e. the resolution of issues listed in section III.3);
- To identify the crosscut R&D necessary for their adoption and application;
- To help the System Steering Committee (SSC) for the identification and the implementation of the specific R&D effort needed for the development of the different systems.

More generally, and with regard to what was the approach until now, the RSWG has to widen the scope of its reflection to the parts of the nuclear system others than the reactor (e.g. fuel cycle installations).

VI.1 Develop and finalize the definition of the safety principles and the safety objectives

The previous chapters indicate safety principles and objectives which have to be developed to provide guidance applicable to the various systems.
For example, it is necessary to give practical indications to measure the degree of fulfilment of objectives for the safety architecture such as the implemented safety is verified as exhaustive, balanced, graduated, tolerant, forgiving, robust and simple. Also the RSWG must clarify the approach and the methods applicable to the definition of the situations to be considered for the architecture's provision design, and those needed to justify the exclusion of situations that the designer will want "practically exclude". The way to address the definition and treatment of the internal and external hazards has to be discussed and defined on an agreed basis.

An important complement to this activity is about the contacts with the other GIF's groups and the integration of the needs which can be specific to these groups. The example of agreed physical protection strategies, between the RSWG and the PR&PPWG is representative. Other contacts are to be developed, in particular with the Gen IV Senior Industry Advisory Panel (SIAP).

The issues still open for discussion and resolution, can be summarized as follows:

- a common understanding of undesirable end states (for example core melt) for different reactor system
- an agreed way for the integration of the physical protection issues
- an agreed approach to address internal and external hazards in a more coherent way
- an agreed and detailed complementary use of deterministic and probabilistic assessment methods, etc.
- the identification of specific rules for the detailed design and the assessment of the design extension conditions
- the preparation of a comprehensive manual for the Objective provision tree implementation
- the identification of a clear path forward on how to define QA standards.

Outside the GIF context, and coherently with the RSWG terms of reference, there is a requirement / motivation for contacts with:

- the national and / or international stakeholders involved in the elaboration of the safety practices applicable to future nuclear systems
- the bodies representative of the safety authorities, to verify continuously, and as far as possible, the pertinence and the aptness of the proposed steps.

In terms of deliverables, the practical activities and work of the RSWG will achieve the previous task 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.

VI.2 Identify the crosscut R&D

The crosscut R&D, that is applicable to all the systems independently of their technology, has to cover two main domains:

- That necessary for the development of innovative provisions;
- That necessary to allow a homogeneous evaluation of the safety architecture of systems which can be very different.

In practice the subjects are common to both domains, as far as the design tries to answer of the assessment's requirements. Once the R&D themes are identified, it is within each of them that it will be possible to identify things specific for the design and for the assessment.

At first sight, the needed R&D for the homogenization of the safety architecture's design and assessment has to cover the following items:

- Design & assessment methodologies (content and implementation);
- Safety related architecture: safety provisions identification and classification;
- Situations to be considered for the safety design/assessment;
- Severe accident managements and emergency plans;
- Safety and reliability for systems implementing specific process (e.g. very high temperature);
- Management of effluents and waste.

Each of these domains deserves specific thoughts to correctly define the needed R&D support. These thoughts are briefly and tentatively developed in Appendix 9.

VI.3 Identification and implementation of specific R&D efforts

Each of the Gen IV systems is characterized by specificities which require the development of the generic principles and objectives to succeed in defining a set of guidelines applicable by the designer.
These guidelines (e.g. number of barriers) do not have to result from a prescriptive approach

but have to be deducted and justified with regard to fundamentals, such as the safety functions.

The domains of application have to cover the normal, incidental and accidental conditions, as well as that of the severe plant conditions[13].
In a general way, the research for these specific subjects can get organized by a deep analysis, developed jointly with the SSC, of the following items:

- The key strong points of the technology;
- The weak points of the technology;
- The analysis of the available experience feedback (if any) and safety background;
- The selection of situations to be retained for the safety provisions design and of those considered as being able to be excluded by design or practically excluded;
- The identification of needs, in terms of provisions, for each of the safety functions, to guarantee the wanted degree of prevention, as well as to support the demonstration of practical exclusion for the situations which shall beforehand have been identified.
- The identification and the consideration of specific risks.

The organization of the R&D which will result from the crosscut issue and specific analysis has to end in three main domains:

- Identification of provisions allowing the integration of the experience feedback and the safety background for the systems under examination, with definition of the specific actions for the various safety functions and consideration of the risks which are specific to the system.
- Actions aiming at the prevention of the occurrence of severe plant conditions with identification of the provisions which can make highly improbable each of the sequences which can lead to them.
- Actions aiming strengthening the demonstration of the plant's capacity to manage given severe plant conditions and to prove the robustness of the confinement vis à vis of the different family of accidents and the associated phenomena.

VI.4 Miscellaneous

Moreover, coherently with the Terms of Reference the RSWG will:

- Provide consultative support on matters related to safety to SSCs and other Gen IV entities which develop specific concepts and designs.
- Advise the Expert Group and the Policy Group on the application of the safety approach for Gen IV systems.
- Promote development of a Generation IV safety database.

[13] A striking example - not necessarily exhaustive - of what these domains can cover arises from a recent joint meeting between the RSWG and the VHTR SC during which several items were raised:

- Confinement: optimum share between different barriers (coated particle, primary system, confinement/containment)
- Severe accident approach
- Credit for passive safety features
- Stochastic behavior of Pebble Bed Reactors
- Combined safety assessment of VHTRs and co-located facilities (H2 production…)
- Materials codes and standards
- Radiological source term

- Interact with the PRPP 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 Generation IV development
- Report annually to the Experts Group on status and progress of the activities including the work plan for the following years..

REFERENCES

[1] GIF IV Technology Roadmap

[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

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

The notion of Risk does integrate simultaneously the idea of frequency of occurrence for the abnormal situations and "consequences" which results from these conditions.
The basic idea is to guarantee extremely low consequences for frequent events and extremely low frequencies for highly hypothetical plant conditions (or severe plant conditions); this is graphically represented by the Farmer's curve showing the "tolerable risk domain" (Fig. A.1.1).

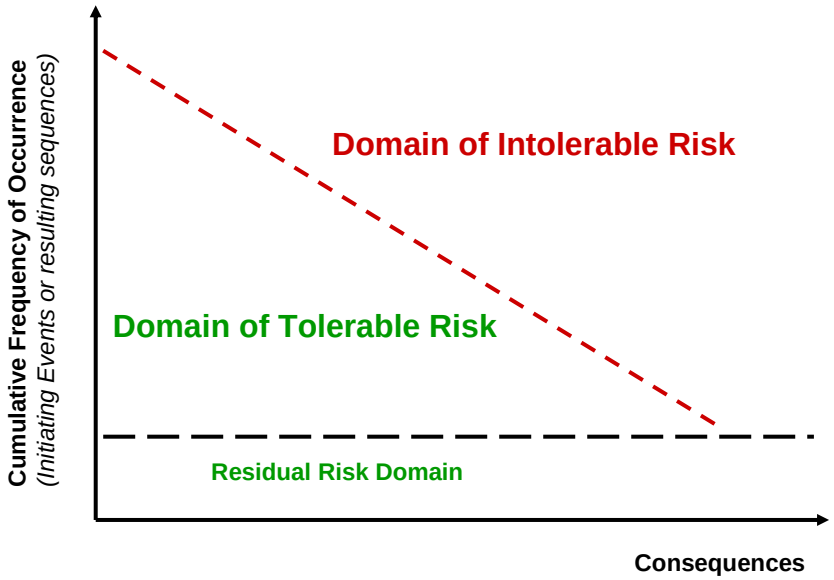


Fig. A1.1 – The Farmer's curve: the Risk domain

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 homogeneous 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).

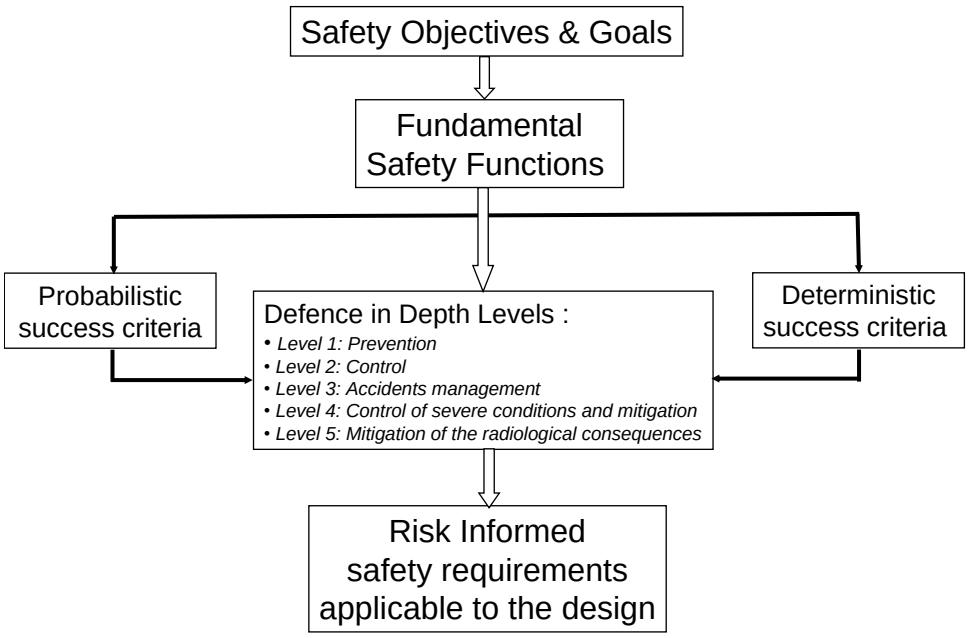


Fig. A2.1 – Defence in depth and Risk-Informed Safety Philosophy Master Logic Diagram

The strategy of defence in depth in nuclear safety is discussed in Réf [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.

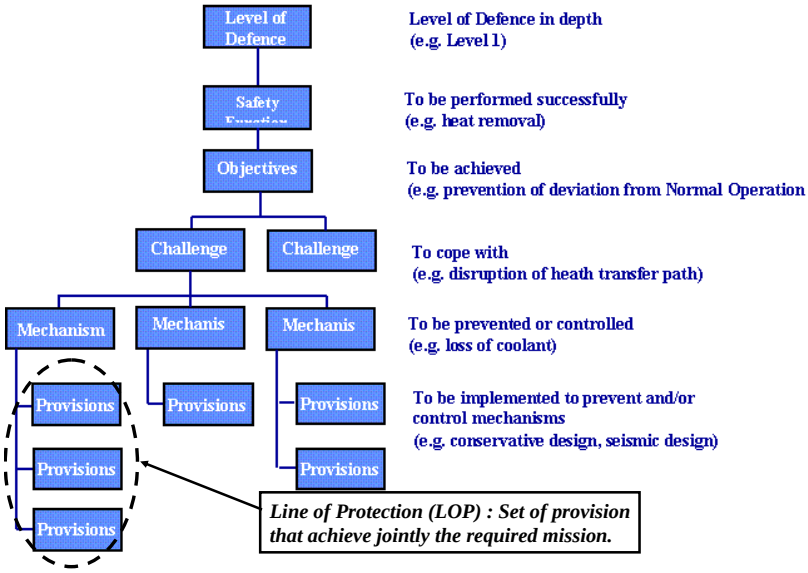


Fig. A3.1 – Simplified representation of Objective Provisions Tree

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[14] is identified, and several root mechanisms[15] 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 the 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"[16].

[14] 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.
[15] Mechanism: specific reasons, processes or situations whose consequences might create challenges to the performance of safety functions.
[16] 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.

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 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 (fig.2, Ref. [4]] is described and illustrated in the developed objective provision trees.

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 provisions trees developed for different specific safety principles.

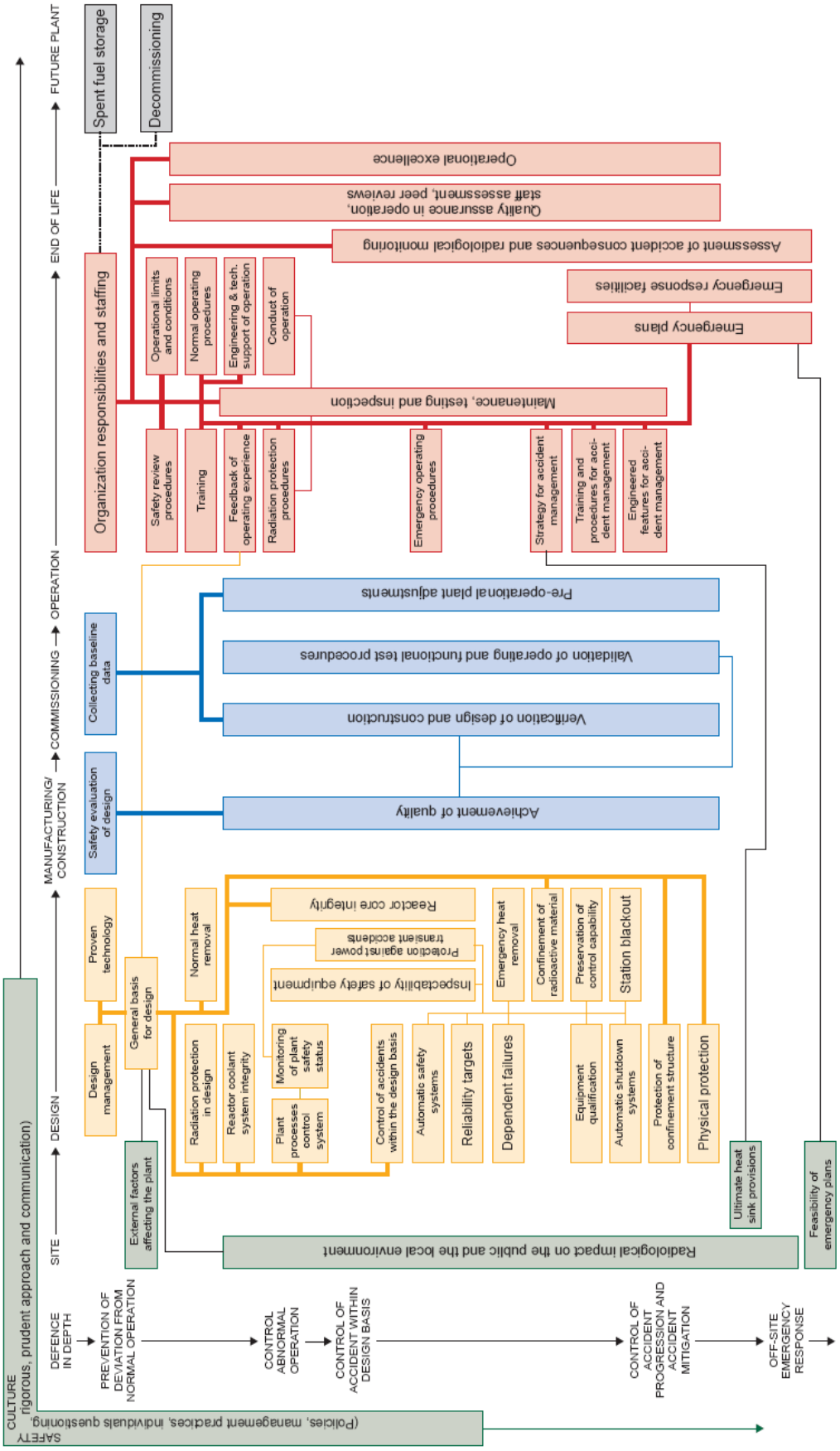


FIG.A3.2 Schematic presentation of the specific safety principles of INSAG-12 showing their coherence and their interrelations [Ref. 6]

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 RSWG believes that 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 GEN 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[17];
- 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

[17] e.g.: Structural failures.

conditions which can affect the behavior of these "defences"[18];

- 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[19].
- Has to achieve an objective for having, as far as possible, a progressive behavior[20] and the possibility for "fail safe" human intervention.

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

---

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

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

[20] 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

Appendix 4 - Principle of “practical elimination”

As regards the treatment of the plant severe conditions or the severe accidents, and coherently with the approach applied internationally, the organization of the safety design and demonstration has to aim at the following two main objectives:

- During the design phase, all the plausible single initiating events have to be addressed by the designer. Once selected, e.g. based on their envelope character, a set of postulated single initiating events have to be “dealt with” or "excluded". To “dealt with” a single initiating event means designing and sizing the provisions requested to address its prevention and nevertheless managing its consequences. On the other side, a limited number of postulated single initiating events can be "excluded" if it can be demonstrated with certainty that sufficient provisions are foreseen to make these postulated single initiating events practically impossible to happen. This holds especially for those postulated events where it is not realistic to set up provisions for the management of their consequences. The demonstration for the exclusion lies on the implementation of sufficient provisions to "practically eliminate" this type of postulated event, i.e. making it practically impossible; in this case the consequences of such rare events will not be addressed by the design.
- As a complement to the concern above, a limited number of postulated accident sequences which lead to severe plant conditions and/or specific situations which, as the latter, would lead to large early releases will become "practically eliminated" for, here also, it is not realistic to set up provisions for the management of their consequences. However, more importantly - as for the postulated single initiating events - design provisions have to be taken and implemented to eliminate these postulated sequences or situations with sufficient confidence if they cannot be considered theoretically as physically impossible. As for the excluded postulated initiating events the consequences of such postulated sequences and situations then will not be addressed by the design.

As a matter of example, for the EPR, few items (postulated initiating events, sequences or situations) are concerned by this approach for the “practical elimination”:

- Accident sequences involving containment bypassing;
- Reactivity accidents resulting from fast introduction of cold or deborated water;
- Reactor pressure vessel rupture;
- High pressure core melt situations;
- Global hydrogen detonations and in-vessel and ex-vessel steam explosions threatening the containment integrity.

As it is made for the EPR, for the future reactors, it is necessary to identify postulates of initiators, postulated sequences and situations whose consequences will not be addressed by the design but for which preventing provisions, sufficient to achieve a robust demonstration of their practical exclusion, will be set up into the architecture of the system.

Appendix 5 - Generation IV Nuclear Systems

The Generation IV roadmap process culminated in the selection of six Generation IV system concepts. The motivation for the selection of six systems is to

- Identify systems that make significant advances toward the technology goals
- Ensure that the important missions of electricity generation, hydrogen and process heat production, and actinide management may be adequately addressed by Generation IV systems
- Provide some overlapping coverage of capabilities, because not all of the systems may ultimately be viable or attain their performance objectives and attract commercial deployment
- Accommodate the range of national priorities and interests of the GIF countries.

The following six systems, listed alphabetically, were selected as Generation IV by the GIF:

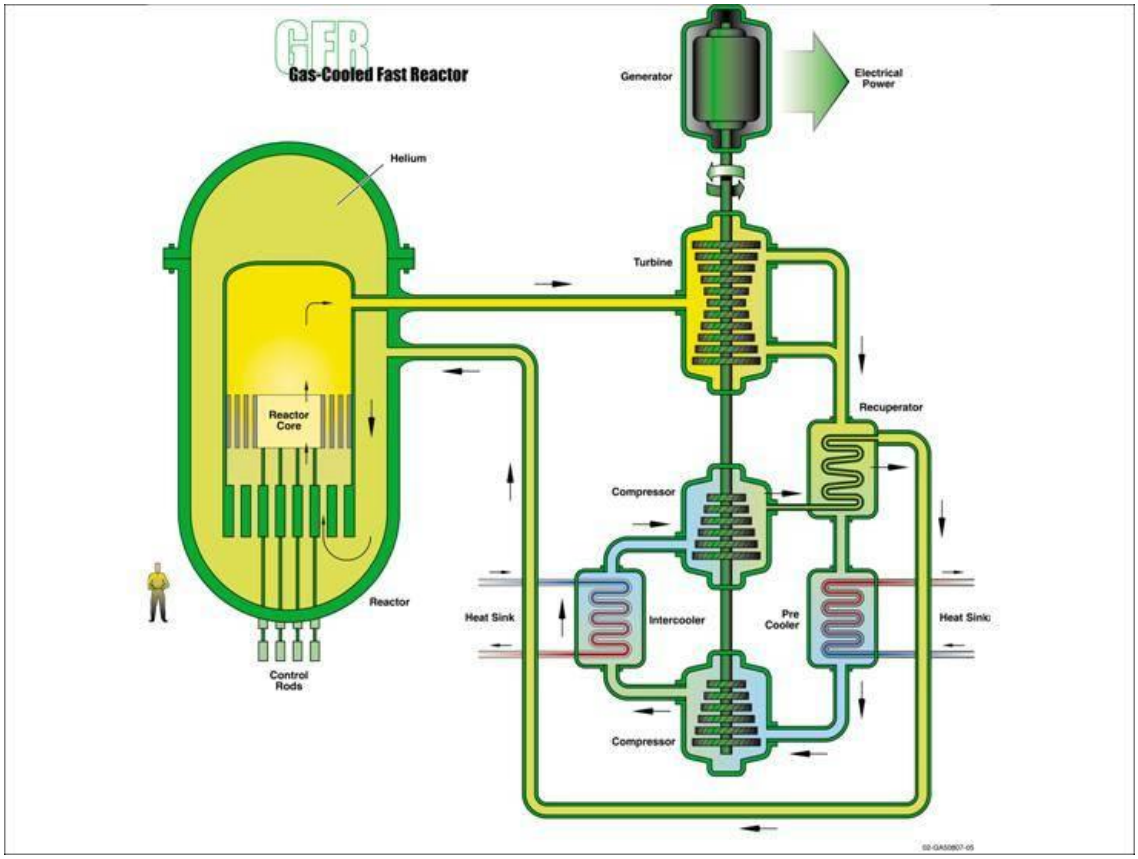
Generation IV System	Acronym
Gas-Cooled Fast Reactor System	GFR
Lead-Cooled Fast Reactor System	LFR
Molten Salt Reactor System	MSR
Sodium-Cooled Fast Reactor System	SFR
Supercritical Water-Cooled Reactor System	SCWR
Very-High-Temperature Reactor System	VHTR

A.5.1 - GFR – Gas-Cooled Fast Reactor System

The Gas-Cooled Fast Reactor (GFR) system features a fast-neutron spectrum and closed fuel cycle for efficient conversion of fertile uranium and management of actinides. A full actinide recycle fuel cycle with on-site fuel cycle facilities is envisioned. The reference design in Ref. [6] was a 600-MWth, helium-cooled system operating with an outlet temperature of 850°C using a direct Brayton cycle gas turbine for high thermal efficiency. Actually a reference version with 2400 MWth and indirect cycle is considered.

Several fuel forms are being considered for their potential to operate at very high temperatures and to ensure an excellent retention of fission products: composite ceramic fuel, advanced fuel particles, or ceramic clad elements of actinide compounds. Reference core configurations are being considered based on plate-based fuel assemblies.

The GFR system is top-ranked in sustainability because of its closed fuel cycle and excellent performance in actinide management. It is rated good in safety, economics, and in proliferation resistance and physical protection. It is primarily envisioned for missions in electricity production and actinide management.



Safety related technology gaps for the GFR

Demonstrating the viability of the GFR requires meeting a number of significant technical challenges.

The development of an innovative fuel is the foundation of the GFR safety characteristics. Among other safety challenges, those which address the decay heat removal systems have to consider the significantly higher power density (in the range of 50 - 100 MWth/m^3) and the reduction of the thermal inertia provided by graphite in the modular thermal reactor designs. Specific concerns are expected for the prevention and the management of severe plant conditions.

Performance issues related to safety & reliability include the development of materials with superior resistance to fast-neutron fluence under very-high-temperature conditions
For the design of the GFR an ad-hoc safety approach is required that relies on intrinsic core/fuel properties supplemented with additional safety provisions – active and/or passive - as needed. In particular the implementation of specific and innovative fuels and materials can allow suggesting specific and innovative approaches to address the severe plant conditions domain.

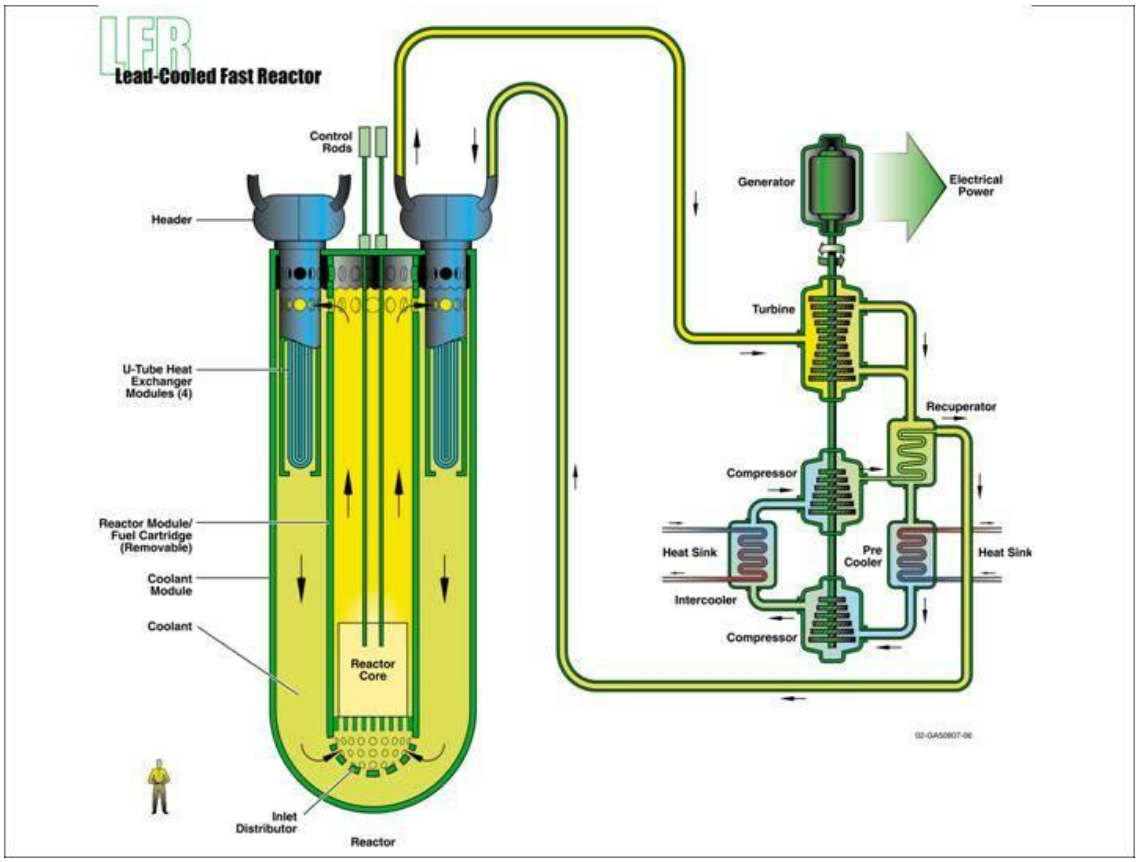
A.5.2 - LFR – Lead-Cooled Fast Reactor System

The LFR system features a fast-neutron spectrum and a closed fuel cycle for efficient conversion of fertile uranium and management of actinides. A full actinide recycle fuel cycle with central or regional fuel cycle facilities is envisioned. The LFR can also be used as a

burner of actinides from spent fuel by using inert matrix fuel. A burner/breeder could use thorium matrices. The system considered by GIF would use either lead or lead/bismuth eutectic as the liquid-metal coolant for the reactor. Note that actually lead is considered the reference option and lead-bismuth the backup coolant for the reactor.

Options include a range of plant ratings. The two options that comprise the dual-track approach of this R&D Plan are the small transportable system of 10–100MWe size that features a very long refuelling interval, and the larger, system rated at about 600MWe, intended for central station power generation.

In the GEN IV technology evaluations the reference LFR system is top-ranked in sustainability because a closed fuel cycle is used, and in proliferation resistance and physical protection because it employs a long-life core. It is rated good in safety and economics. The safety was considered enhanced by the choice of a relatively inert coolant.



Safety related technology gaps for the LFR

While the nearer-term options focus on electricity production and rely on more easily developed fuel, clad, and coolant combinations, the longer-term option seeks to further exploit the inherently safe properties of Pb.

As regard safety, LFR holds the potential for advances compared to state-of-the-art liquid metal fast reactors. Viability phase has to prove the following:

- The favorable neutronics of Pb and Pb-Bi coolants in the battery option which enable low power density, natural circulation-cooled reactors with fissile self-sufficient core designs that hold their reactivity over their very long 15- to 20-year refueling interval.

For modular and large units more conventional higher power density, forced circulation, and shorter refueling intervals are used, but these units benefit from the improved heat transport and energy conversion technology.

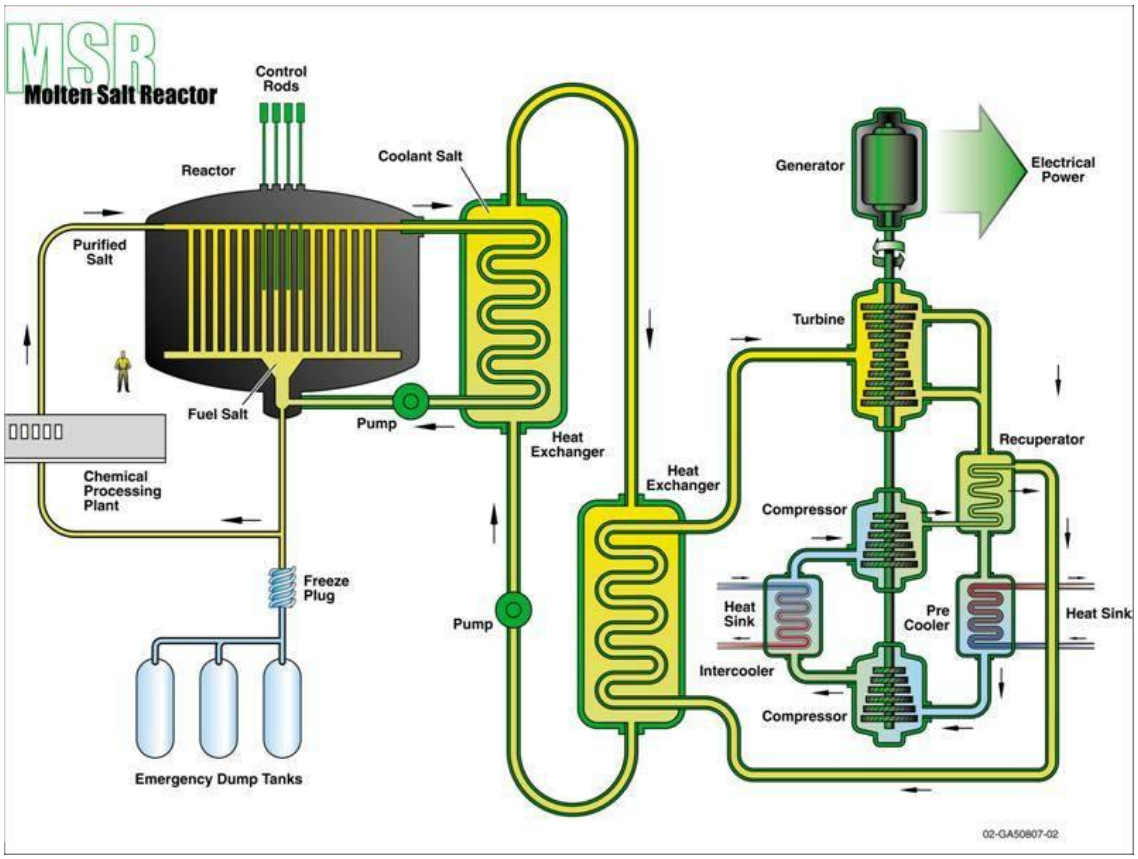
- The compatibility between structural materials and lead / lead bismuth.
- For the mid term, the increased inherent safety features and controllability advantages which lie on a heat transport circuit with large thermal inertia and a coolant that remains at ambient pressure.
- The favorable properties of Pb coolant and nitride fuel which, if combined with high temperature structural materials, can extend the reactor coolant outlet temperature into the 750–800ºC range in the long term; this high temperature option will have to face the hardened issues, e.g.: corrosion, Pb chemistry.
- The assurance of reliable and effective thermostructural reactivity feedback is key to the passive safety and to the passive load following design strategy and will require coordinated neutronics/thermal-hydraulics /structural design of the core.

Concerning the severe accident domain it is considered that the thematic will be analogous to the one selected for the Sodium fast reactor.

A.5.3 - MSR – Molten Salt Reactor System

The Molten Salt Reactor (MSR) system features an epithermal to thermal neutron spectrum and a closed fuel cycle tailored to the efficient utilization of plutonium and minor actinides. A full actinide recycle fuel cycle is envisioned. In the MSR system, the fuel is a circulating liquid mixture of sodium, zirconium, and uranium fluorides. The molten salt fuel flows through graphite core channels, producing a thermal spectrum. Actinides and most fission products form fluorides in the liquid coolant. The homogenous liquid fuel allows addition of actinide feeds with variable composition by varying the rate of feed addition. There is no need for fuel fabrication. The reference plant has a power level of 1000 MWe. The system operates at low pressure (<0.5 MPa) and has a coolant outlet temperature above 700°C, affording improved thermal efficiency.

The MSR system is top-ranked in sustainability because of its closed fuel cycle and ‘excellent performance’ in waste burndown. It is rated ‘good’ in safety, and in proliferation resistance and physical protection, and it is rated ‘neutral’ in economics because of its large number of subsystems.



Safety related technology gaps for the MSR

Prior programs have provided information to help demonstrate MSR safety. Nevertheless, a comprehensive safety analysis remains to be done.

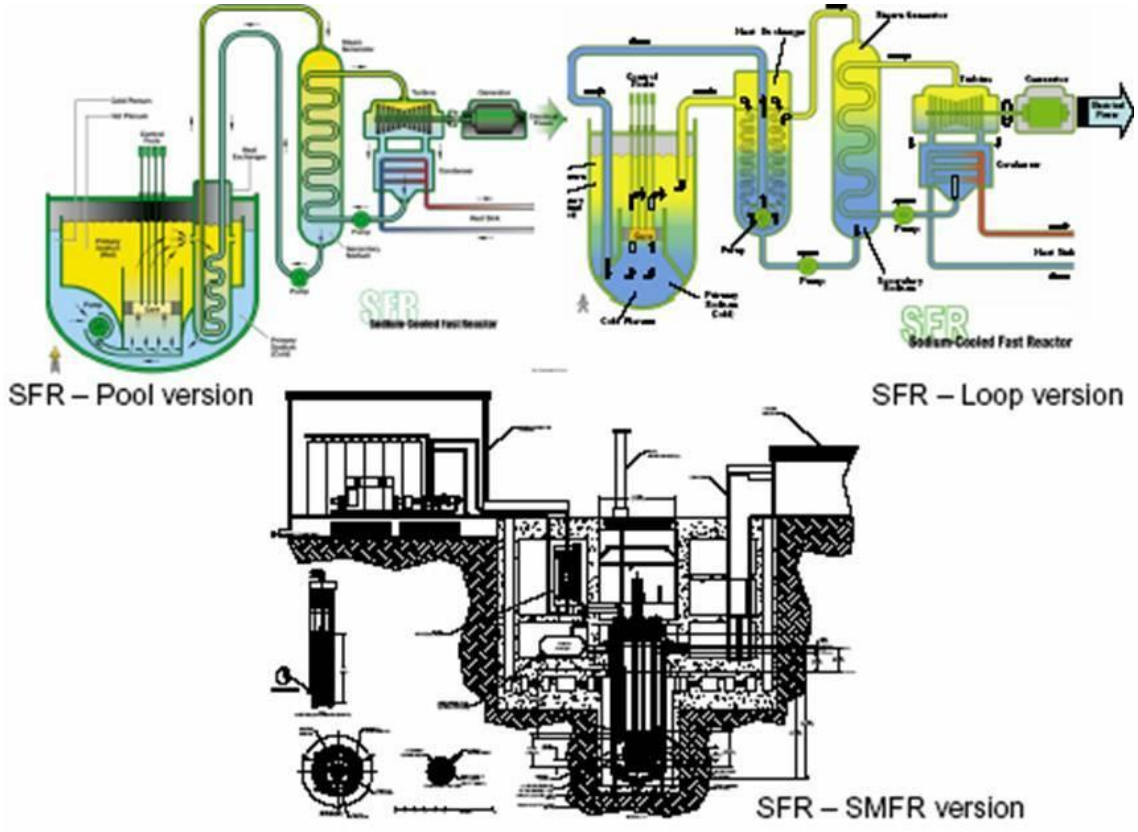
The safety characteristics of MSR systems are very distinctive due to liquid and circulating fuel, compared to more classical systems. Some MSR specific features appear favourable to safety: operation at low pressure; temperature reactivity coefficient of the salt strongly negative; large design margins and strongly negative void effect in case of boiling; possibility, in case of emergency, to drain the fuel salt into reservoirs designed to guarantee sub-criticality and to cool down the fuel salt by passive means; on-line reprocessing of the fuel salt with continuous extraction of FP (which feasibility has to be proven), leading to a low inventory of fissile materials, drastic reduction of the potential source term and lowered residual heat.

In contrast, other features are challenging to safety, for example: positive temperature reactivity coefficient of the graphite used as moderator; absence of the "classical" first barrier to FP release; spreading of radionuclides all over the primary circuit and the reprocessing unit (confinement of tritium, formed in noticeable quantity in a MSR); uncertainties on the physical and chemical behaviour of molten salt mixtures; on-site coupling of the reactor and reprocessing unit.

To cope with these unique safety features implies to consider a totally renewed approach for the safety design and assessment of the MSR. In particular the way to address the domain of severe accident has to be fully redefined to address the general Gen IV objectives and principles while integrating the specificities of this system.

A.5.4 - SFR – Sodium-Cooled Fast Reactor System

The Sodium-Cooled Fast Reactor (SFR) system features a fast-spectrum reactor and a fuel suitable for a closed cycle. The primary mission for the SFR is the effective management of high-level wastes and uranium resources.



Using liquid sodium as the reactor (primary) coolant, allows high power density with low coolant volume fraction. The primary system operates at near-atmospheric pressure with typical outlet temperatures of 500-550^{o}C; at these conditions, large margin to coolant boiling is maintained. The reactor unit can be arranged in a pool layout or a compact loop layout. Plant sizes ranging from small modular systems (50 MWe - SMFR) to large monolithic reactors (2000 MWe), either Pool (EFR & Kalimer like) or Loop type (JSFR like), are considered.

The Generation IV Technology Roadmap ranked the SFR highly for advances it offers toward sustainability goals. The SFR is also highly rated for safety performance. With innovations to reduce capital cost and improve efficiency, the SFR promises to be an attractive option for electricity production.

The SFR has the highest technical maturity level among Generation IV systems; its development approach builds on technologies already developed and demonstrated for sodium-cooled reactors and associated fuel cycles in fast reactor programs worldwide.

Safety related technology gaps for the SFR

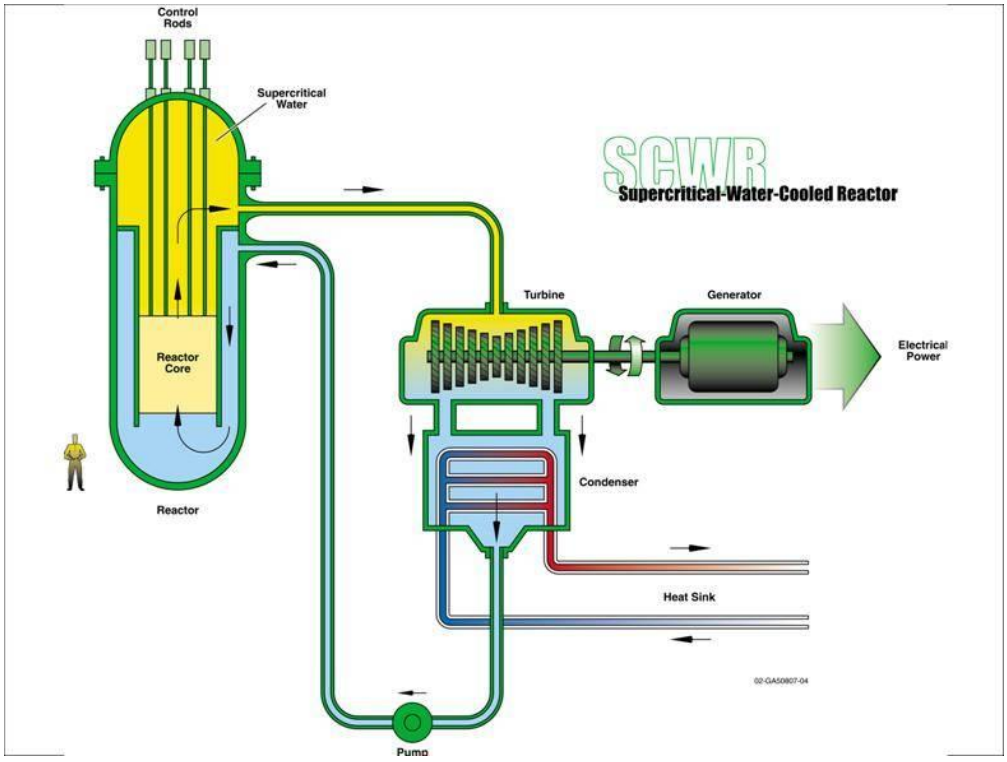
As indicated, the reactor unit can be arranged in a pool layout or a compact loop layout. For

both options, there is a relatively large thermal inertia of the primary coolant.
A large margin to coolant boiling is achieved by design, and this is an important safety feature of these systems. Another major safety feature is that the primary system operates near the atmospheric pressure, pressurized only to the extent needed to move fluid. Sodium reacts chemically with air, and with water, and thus the design must limit the potential for such reactions and their consequences. To improve safety, a secondary sodium system acts as a buffer between the radioactive sodium in the primary system and the energy conversion system.

A focused program of safety R&D is necessary to support the SFR. Worldwide experience with design and operation of such systems has shown that they can be operated reliably and safely. Aside the research for options which can improve the performances of the SFR (i.e. operation, economy), the safety related R&D challenges for these systems in the Generation IV context are (1) to verify the predictability and effectiveness of the mechanisms that contribute to respond safely reliably to design basis transients and anticipated transients without scram, preventing core degradation, and (2) to ensure that bounding events considered in licensing can be sustained without loss of fuel coolability or loss of containment function. Specific risk, linked to the coolant reactivity, have to be addressed.

As detailed later, for the SFR a proposal for the safety approach including the treatment of severe plant conditions is now available. The whole core melting will play an essential role within this approach, to be considered to prove the robustness of the confinement and within the context of the practical exclusion of some situations.

A.5.5 - SCWR – Supercritical-Water-Cooled Reactor System



Supercritical Water-Cooled Reactors (SCWRs) are a class of high temperature, high pressure water-cooled reactors that operate above the thermodynamic critical point of water (374°C,

22.1 MPa) to achieve a thermal efficiency approaching 44%. The SCWR system features two fuel cycle options: the first is an open cycle with a thermal neutron spectrum reactor; the second is a closed cycle with a fast-neutron spectrum reactor and full actinide recycle. The fast-spectrum option depends upon the materials' R&D success to support a fast-spectrum reactor.

In either option, the reference plant has a 1700-MWe power level, an operating pressure of 25 MPa, and a reactor outlet temperature of 550°C. Passive safety features similar to those of the simplified boiling water reactor are incorporated. Owing to the low density of supercritical water, additional moderator is added to thermalize the core in the thermal option. Note that the balance-of-plant is simplified because the coolant does not change phase in the reactor. Nevertheless drawbacks in terms of contamination of the primary circuit and components (as for example the turbine) has to be carefully evaluated.

The SCWR system is highly ranked in economics because of the high thermal efficiency and plant simplification. If the fast-spectrum option can be developed, the SCWR system will also be highly ranked in sustainability. The SCWR is rated good in safety, and in proliferation resistance and physical protection. The SCWR system is primarily envisioned for missions in electricity production, with an option for actinide management (fast spectrum).

Safety related technology gaps for the SCWR

Concerning safety, SCWRs have unique features that may offer advantages or disadvantages compared to state-of-the-art LWRs.

No boiling crisis (i.e., departure from nucleate boiling or dry out) exists due to the lack of a second phase in the reactor, thereby avoiding discontinuous heat transfer regimes within the core during normal operation. Simplicity drawn by the suppression of steam dryers, steam separators, recirculation pumps, and steam generators can help assessing the system response. These are favourable from safety point of view.

A lower-coolant mass flow rate per unit core thermal power and a lower-coolant mass inventory results from the once-through coolant path in the reactor vessel and the lower-coolant density opens the possibility of smaller containment buildings but is unfavourable for the management of transient of heat removal. Prevention and management of abnormal situations - flow instability; LOCA - have to be managed carefully; some of them, as for example the instabilities, could be critical for fast-spectrum option.
Concerning the severe accident domain it can be considered that, for the Thermal spectrum version, there will not be major differences compared to the current LWR. This is not the case for the Fast spectrum version for the specificities of the fast cores essentially due to the risk of recriticality.

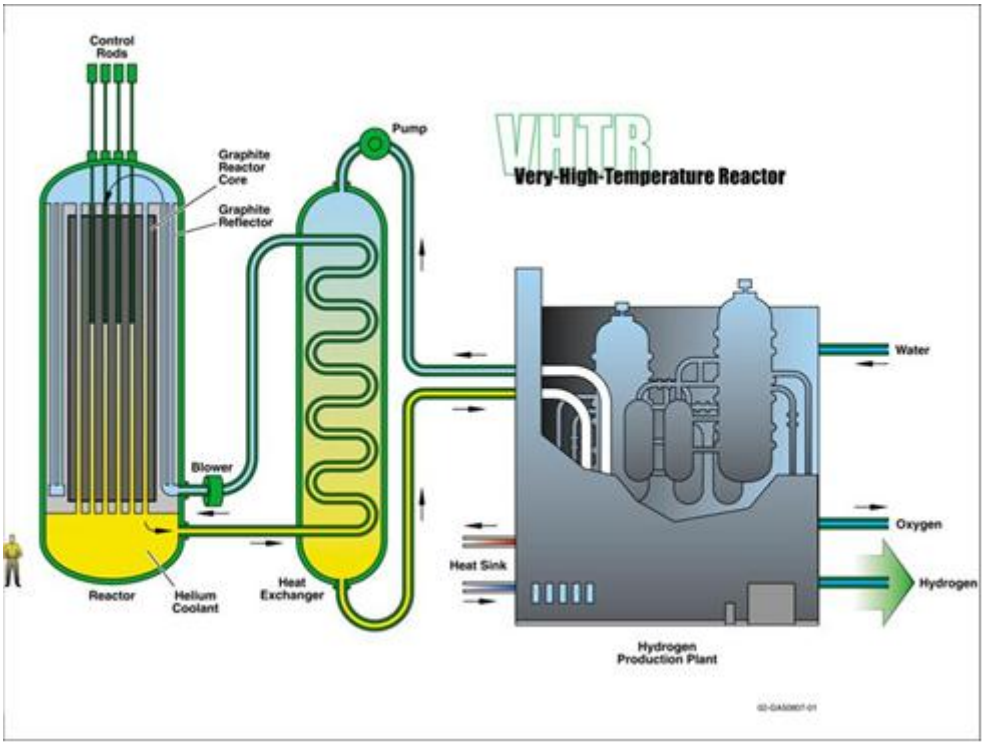
A.5.6 - VHTR – Very-High-Temperature Reactor System

The Very-High-Temperature Reactor (VHTR) technology addresses advanced concepts for helium gas-cooled, graphite moderated, thermal neutron spectrum reactor with a core outlet temperature greater than 900°C, and a goal of 1000°C, specified to support production of hydrogen by thermo chemical processes. The reference reactor thermal power is set at a level which allows completely passive decay heat removal, currently estimated to be about 600 MWth.

The VHTR assumes a once-through but the potential operation with a closed fuel cycle will be assessed.

The VHTR core concepts are envisioned to be developed according to two baselines: pebble bed type and prismatic block type core. The standard UO2 fuel TRISO coated particles concept (UO2 kernel, SiC/PyC coating) may either be enhanced, through UCO fuel kernel, or be advanced through ZrC coating. Then for each concept, alternative solutions might be developed for each sub-system or component.

The electric power conversion unit may operate in either a direct (helium gas turbine) or indirect (gas mixture turbine) Brayton-type cycle. Nuclear heat applications will require an intermediate heat exchanger connected to the reactor core.



The VHTR system is highly ranked in economics because of its high hydrogen production efficiency, and in safety and reliability because of the inherent safety features of the fuel and reactor. It is rated good in proliferation resistance and physical protection.

Safety related technology gaps for the VHTR

Passive heat removal systems should be developed to likely facilitate operation of the VHTR, with a final goal of simple operation and transparent safety concepts. Demonstration tests should be performed on the VHTR to verify the performances and the reliability of the system's passive characteristics.

Integral analysis and demonstration of the inherent safety features of the VHTR are needed, and could potentially draw on development and demonstration of earlier International Near Term Deployment (INTD) gas reactors.

Additional safety analysis is necessary with regard to nuclear process heat applications (e.g. hydrogen production) in an industrial environment. The safe isolation of the reactor system

after failures in the heat delivery system is an essential issue for demonstration of Intermediate Heat Exchangers (IHX) and hot gas valve tightness after depressurization of the secondary circuit. Full-scale tests of valves and IHX modules will be necessary.

Design basis and severe accident analyses for the VHTR will need to include phenomena such as chemical attack of graphitic core materials, typically either by air or water ingress. Adequacy of existing models need to be assessed, and new models, may need to be developed and validated. Due to the low level of selected specific power the thermal core degradation can be excluded. Nevertheless as indicated later, to fully implement the principles of the defence in depth, there is the need to consider "severe plant conditions". These conditions are not yet defined precisely.

A.5.7 - Summary: Safety related technology gaps for the Gen IV Systems

The table below summarizes, for each of Gen IV systems, the fields where significant safety related technology gaps are recognized.

	GFR	**LFR**	**MSR**	**SFR**	**SCWR**	**VHTR**
Innovative Safety Approach	**X**	**X**	**X**	**X**	**X**	**X**
Fuel	**X**		**X**			**X**
Neutronics			**X**		**X**	
Thermal aerolic/hydraulic	**X**				**X**	**X**
Materials & chemistry	**X**	**X**	**X**	**X**	**X**	**X**
Fuel chemistry			**X**			
Passive Safety		**X**	**X**			**X**
Severe accident behaviour	**X**	**X**	**X**	**X**	**X** for fast spectrum	**X**
System Specific Features			Coupling with the fuel cycle installation			Coupling with the heat process installation
ISI&R		X	X	X		

Appendix 6 - Safety margins and Uncertainties

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. These steps are summarized in the following description and illustrated in Figure A6.1 (Ref. [13][12]). In this figure, vertical displacements are indicative of safety margins applicable to different steps of the safety case analysis (Transients (or DBC) assessment: *Analytical Margins*; Provisions' design: *"Barrier" Margins*; Margins on the Confinement Performances: *Source Term Margins*; Margins on the Consequences outside the plant: *Dose Margins*).

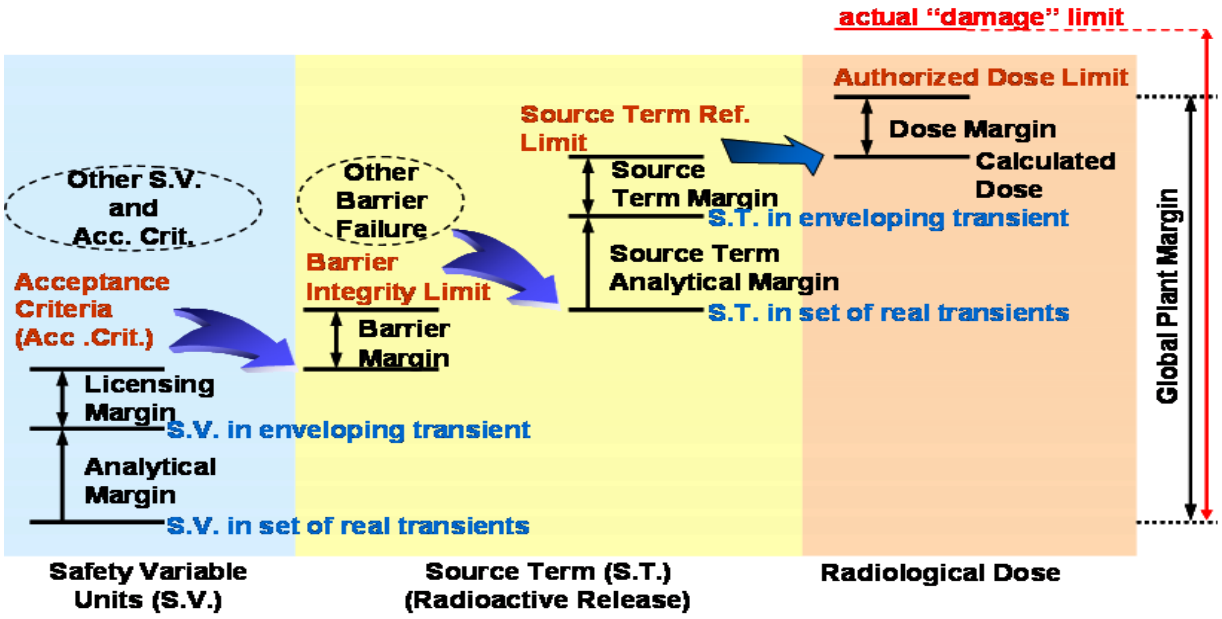


Figure A6.1 : Safety margins in typical Design Basis safety analysis

All the margins represented on Figure A6.1 can be considered as contributors to a *global plant margin* versus the safety objectives. In spite of the fact that they are all stemming from analyses realized with calculation tools, their nature is different. For that reason their contribution to the global margin is not purely additive. A conventional example of "Distribution of calculation tools predictions versus the allowable limits" is presented and discussed below.

What is worth retaining is that, as a complement to an improved quality of safety, the reduction of uncertainties paves the way for other desirable design and operational characteristics that potentially include reduced capital costs, reduced maintenance and operating costs, simplified safety management, etc. Such reduction of uncertainties of the innovative reactor systems has to be identified as a specific task for the R&D effort.

A conventional example of "Distribution of calculation tools predictions versus the allowable limits" is shown in Figure A6.2. The curve/bell on the left side refers to the values obtained, by the calculation tool, for a given safety variable, representative of the status of the plant during the transient. The distribution is the consequence of uncertainties in initial and boundary conditions, as well as in the models that are used to compute the safety variable. When applying a "conservative approach" to the safety case, the final result is represented by a unique value, labelled "conservative prediction", enveloping the whole curve.

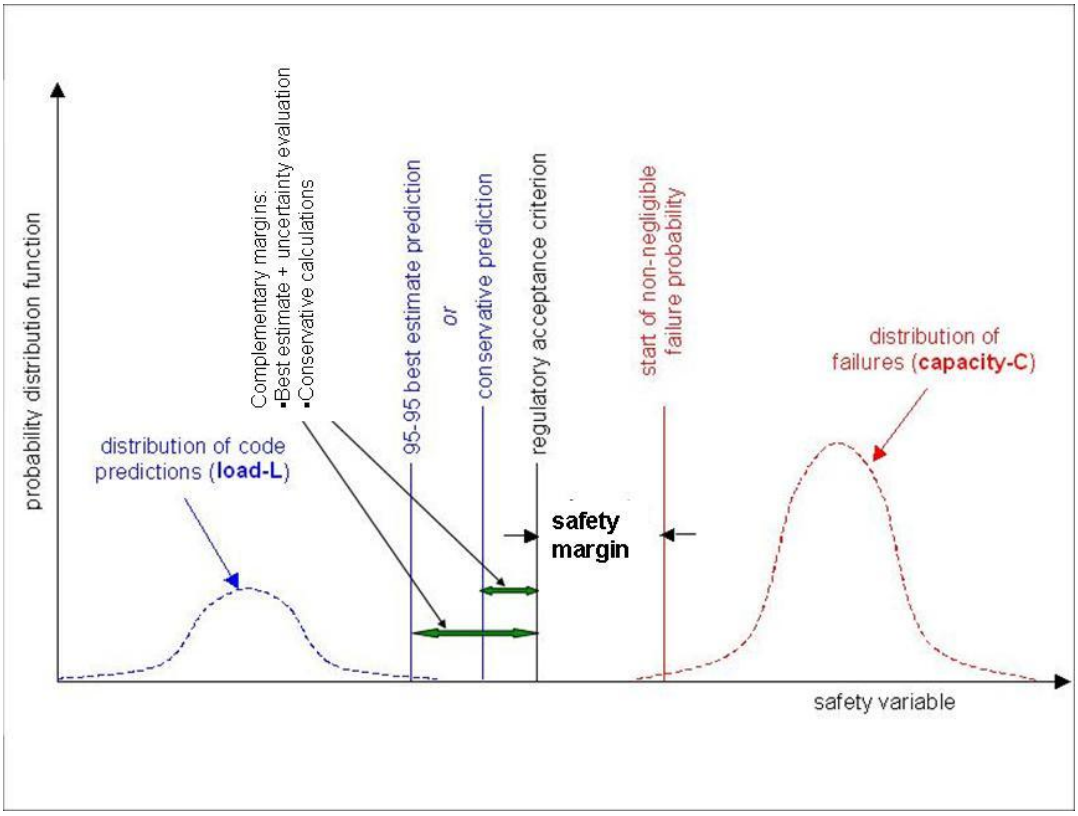


Figure A6.2: The concept of safety margins.

As an alternative to the "conservative approach", the "best estimate + uncertainty evaluation approach" allows defining a less conservative value, labelled "best estimate prediction" associated to its own uncertainty (e.g. the "95-95 best estimate prediction", representative of the 95 percentile of the plants status during the transient, with 95% of confidence level). The curve/bell on the right side refers to the allowable limit for the safety variable to avoid the failure of the correct plant behaviour, with a given probability; the distribution is the consequence of uncertainties on the limit characteristics for the plant and its provisions.

Aside the factual results described above, an "Acceptance criterion" is agreed with the regulatory body to insure the correct and conservative representation of the plant allowable limits. As indicated within the Figure A6.2, the "safety margin", for a specific criterion, is defined as the range between the Acceptance criterion and the limit associated to a non-negligible probability of failure of the plant. It is important to point out that this kind of margin is not accessible to the designer for changing the design.

Conservative predictions have to be used when the plant design and its physics are still not well defined and mastered. Best estimate approach could be adopted when there is the feeling that the uncertainties resulting from the plant's physics knowledge and modelling, from the scenarios selection, and from the lack of mastering the uncertainties evaluation, are well controlled.
The verification of the fulfilment of safety criteria resulting either from a deterministic approach or from a probabilistic approach, lead to the comparison between the "conservative prediction", or the "best estimate prediction" associated to its own uncertainty, with the "acceptance criterion". This comparison, acceptable if the latter envelopes the two former, introduces complementary margins in the design of the corresponding provisions. The

objective of a sound design is the reduction as far as possible, obviously supported by adequate demonstration, of these complementary margins and finally the achievement of an improved level of safety if the margins are accurately identified and motivated.

For this, the PSA, simplified or exhaustive, would be valuable in reducing uncertainty regarding the accidental sequence since it relies on a as exhaustive as possible identification of scenario. However, most of the existing, PSAs rely on thermal hydraulics calculations dealing with enveloping selected transients. Thus, a possible assessment of the conservatism associated to the PSA or the possibility to perform best-estimate PSAs associated to uncertainties assessment, could allow drawing a picture of margins in terms of the overall risk (including the frequency of sequences and their consequences) and not only in terms of design of provisions. In other terms, such PSAs would offer the possibility for an appreciation of the margins' extend, taking into account the likelihood of the safety case used to check the margin.

Appendix 7 - Safety functions/principles and relevant DiD level to be assessed by OPT

As it was mentioned in the beginning of Section V.1, there are two types of utilization method. This section describes the list of safety functions or safety principles for each method.

Method 1: Ref. [4]

- OPT shall be produced for each level of DiD from 1 to 4, and
- For each fundamental safety functions (control of reactivity, removal of heat from the core, and confinement of radioactive materials).
- Totally (4 x 3 =) 12 OPTs shall be produced.

Method 1, has rather simple list as shown in Table A7.1. This list shows that an OPT shall be produced for each three fundamental safety functions and each DiD level from level 1 to 4. Totally 12 OPTs will be produced to show the implementation of DiD.

Method 2: Ref. [5]

- OPT shall be produced for each Safety Principle (SP) mentioned in Ref. [6] (totally 53 safety principles), and
- For each level of DiD on which the relevant SP should be considered.

The list of Safety principles used by Method 2 are shown Table A7.2; the list goes beyond the fundamental safety functions and develops a comprehensive list of practical safety principles which are derived from the fundamental safety functions. This list can be explained as follows.

Below the three fundamental safety functions, totally 53 specific safety principles (SPs) to be observed in all the phases of the plant life are described in IAEA INSAG-12 (Ref. [6]). These 53 SPs are considered as safety related functions to be checked using OPT if all the phases of plant life is to be assessed. On the other hand, from the view point of DiD philosophy, each SP might have different requirement of safety ("safety function") according to different level of DiD, and thus different challenges, mechanisms and provisions shall be considered and provided for different DiD level. Therefore, a matrix of SPs and DiD levels shall be formulated in order to clarify the SPs and requirements to be assessed. This matrix, Table A7.2, is the list of SPs and relevant DiD level for OPT method. All the 53 SPs are shown on the left side of the table, and on the right hand side DiD levels from 1 to 5 are described. The mark "o" means a safety function that should be assessed for corresponding DiD level and the SP. As shown in Table A7.2, most of the SPs are related with several levels of DiD. In such a case, plural sub-OPTs should be made for each safety function derived from the SP, however, they could be merged if possible. There are totally 147 safety functions (147 marks of "o") identified in Table A7.2, but the number of safety functions to be assessed is effectively reduced to 68 in the report (Ref. [5]). This report explains how to allocate each SP to each DiD level, and contains a graphical representation of all the 68 sub-OPTs.

Utilization of OPT in the stage of preliminary conceptual design

The application of both methods has its advantages and week points.

Namely, by Method 1, an OPT helps a user to overview the integrated safety features in the plant for the fundamental safety functions in each DiD level, and thus one can use this method to assess and confirm the balance of safety measures among the DiD levels, and to

share a common understanding about the safety measures between the designers and regulators. It should be noticed that, since an OPT tends to become larger, one should be careful to include necessary information but with adequate level of details.

On the other hand, by Method 2, a user could focus on a specific Safety Principle, and confirm or analyze the sufficiency of the safety measures against each SP in detail. However, Safety Principle does not always correspond to only one of the three fundamental safety functions, but they include compound requirements for safety design, or more generic safety requirements. For example, "SP 233 Station Blackout" includes at least two fundamental safety functions (control of reactivity, removal of heat from the core). Again, "SP 136 External factors affecting the plant", "SP 154 Proven technology", "SP 242 Physical protection of plant" and "SP 318 Strategy for accident management" are generic safety requirements, and correspondent OPT's would consist of policies of safety design rather than specific safety systems.

Considering these complementary characteristics of integration and analysis, RSWG would propose a combined approach of the OPT utilization in the preliminary conceptual design phase as described below.

The integrated plant safety design or its balance of arrangement shall be assessed by Method 1 at a level of each of the fundamental safety function and each DiD level. The compliance of the safety design (measures or policies) with each of the derived Safety Principles shall be analyzed and confirmed by Method 2.

In the stage of the preliminary conceptual design, it may not be effective to produce so many OPT's for all the SP's because the design may not be developed in detail. Therefore, RSWG has selected the SP's to which attention should be paid in the preliminary conceptual design phase (Table A7.3). RSWG considers that the top eleven SP's in Table A7.3 are important because they are directly related to the fundamental safety functions. The bottom four SP's are rather generic but RSWG recommends that they should be confirmed in the earlier stage of the design activity.

TABLE A7.1 ASSIGNMENT OF SAFETY FUNCTIONS TO INDIVIDUAL LEVELS OF DEFENCE IN DEPTH (Ref.[6])

Phases of plant life	Safety function	Level of defence 1 2 3 4 5
Design	Control of reactivity	o o o o
	Removal of heat from the core	o o o o
	Confinement of radioactive materials	o o o o

TABLE A7.2 ASSIGNMENT OF SAFETY PRINCIPLES TO INDIVIDUAL LEVELS OF DEFENCE IN DEPTH (Ref. [7])

Phases of plant life	No. of SP	Safety principle (SP)	Level of defence 1 2 3 4 5
Siting	136	External factors affecting the plant	o
	138	Radiological impact on the public and the local environment	o o o o o
	140	Feasibility of emergency plans	o
	142	Ultimate heat sink provisions	o o o o
Design	150	Design management	o o o o
	154	Proven technology	o o o o
	158	General basis for design	o o o o
	164	Plant process control systems	o o
	168	Automatic safety systems	o
	174	Reliability targets	o
	177	Dependent failures	o
	182	Equipment qualification	o
	186	Inspectability of safety equipment	o o o o
	188	Radiation protection in design	o
	192	Protection against power transient accidents	o o o
	195	Reactor core integrity	o o o
	200	Automatic shutdown systems	o o
	203	Normal heat removal	o o
	205	Startup, shutdown and low power operation	o o o o
	207	Emergency heat removal	o o
	209	Reactor coolant system integrity	o o
	217	Confinement of radioactive material	o o
	221	Protection of confinement structure	o o
	227	Monitoring of plant safety status	o o o o
	230	Preservation of control capability	o o o o
	233	Station blackout	o o
	237	Control of accidents within the design basis	o
	240	New and spent fuel storage	o o
	242	Physical protection of plant	o o

TABLE A7.2 ASSIGNMENT OF SAFETY PRINCIPLES TO INDIVIDUAL LEVELS OF DEFENCE IN DEPTH (Ref. [7]) (continued)

Phases of plant life	No. of SP	Safety principle (SP)	Level of defence 1 2 3 4 5
Manufacture	246	Safety evaluation of design and construction	o o o o
	249	Achievement of quality	o o o o
Commissioning			
	255	Verification of design and construction	o o o o
	258	Validation of operating and functional test procedures	o o o o
	260	Collection of baseline data	o o o o
	262	Pre-operational adjustment of plant	o o o o
Operation	265	Organization, responsibilities and staffing	o o o o o
	269	Safety review procedures	o o o o
	272	Conduct of operations	o
	278	Training	o o o
	284	Operational limits and conditions	o o o
	288	Normal operating procedures	o
	290	Emergency operating procedures	o o o o
	292	Radiation protection procedures	o o o o
	296	Engineering and technical support of operations	o o o o o
	299	Feedback of operating experience	o o o o
	305	Maintenance, testing and inspection	o o o o
	312	Quality assurance in operation	o o o o
Accident management	318	Strategy for accident management	o
	323	Training and procedures for accident management	o
	326	Engineered features for accident management	o
Emergency preparedness	333	Emergency plans	o o
	336	Emergency response facilities	o o
	339	Assessment of accident consequences and radiological monitoring	o o o

TABLE A7.3 PROPOSAL: SAFETY PRINCIPLES TO BE ASSESSED BY OPT METHOD IN PRE-CONCEPTUAL PHASE FOR GEN IV REACTOR SYSTEMS

ID of SP	Safety Principle
142	Ultimate heat sink provisions
168	Automatic safety systems
192	Protection against power transient accidents
195	Reactor core integrity
200	Automatic shutdown systems
203	Normal heat removal
207	Emergency heat removal
209	Reactor coolant system integrity
217	Confinement of radioactive material
221	Protection of confinement structure
233	Station blackout
(from wider viewpoints)	
136	External factors affecting the plant
154	Proven technology
242	Physical protection of plant
318	Strategy for accident management

Appendix 8 – Example on application of the PSA method to a conceptual design of a SFR system

The Ref. [7] describes an application of the PSA method to a conceptual design of a sodium-cooled fast reactor. In the selection of the configuration of decay heat removal systems (DHRSs), a simplified level-1 PSA was conducted for 4 options of DHRS based on the same analytical conditions. The results were compared each other, the characteristics of each option was clarified, and the option with the lowest risk was selected and proposed for the designer.

In this paper, advantages and disadvantages among the design options are rather intuitively obvious, nevertheless, quantitative analysis using PSA method explains the differences logically. Namely, in the option 1, heat exchangers of DHRS are connected to the primary heat transfer systems (at the top of the intermediate heat exchanger), while in the option 2, they are connected to the secondary systems. One can intuitively indicate the advantage of the option 1 because the distance from the core, namely the heat source, to the heat exchanger of DHRs is shorter. In the comparison of the PSA results of both the options, it was clarified that the unreliability of the option 2 is higher than that of the option 1, and the difference was explained by the unreliability of the secondary systems. Particularly, the unreliability of the steam generator and its uncertainty are dominant among others. Based on this discussion, option 1 was selected as the design candidate.

Although it is not described, this paper implies that the PSA analysis could provide the basis of further discussion, such as, how much increase of SG reliability is necessary to improve the reliability of option 2. Then one can consider how much R&D is necessary for such improvement, and whether the investment for the R&D of SG is advantageous or not instead of investigating another design option.

Although this example introduced here is a limited application to DHRS in a conceptual design phase, an analyst of a new system might notice various issues in the process of the analysis. Namely:

- The design of DHRS and related systems is not clearly defined in detail,
- Operating procedure under accident conditions is not clearly defined,
- Hence the analyst of the PSA must assume an adequate operating procedure under accident conditions,
- A plant dynamics code is needed to establish success criteria and for various analysis,
- But the plant dynamics code is not fully validated yet,
- The reliability database of the related systems/components is not sufficient,
- Hence one must use conservative value or consider large uncertainty,
- One must investigate the influence of the large uncertainty to the results,
- One must consider how to reduce the uncertainty by R&D or alternative design, and
- One must start as soon as possible the development of the reliability database at least for the systems/components specific to the relevant plant design.

And it is often the case that a safer design is more expensive. Therefore analyst and designer will face to a trade-off (or optimization) between the risk and cost. In the case of Ref. [6], fortunately, the pipe length of DHRS is longer in the selected option and the number of containment penetration is increased, but the safety grade requirement is not applied to the secondary systems. Therefore, it was judged that the increment of the cost was not

significant and it was acceptable due to the reduction of the risk.

Appendix 9 - R&D for the homogenization of the safety architecture's design and assessment

A.9.1 The Line of Protection concept

It is agreed that the safety architecture of Gen IV systems shall fully answer the principles of defence in depth. For some of these systems the safety architecture implements and makes a greater use of intrinsic characteristics and passive engineered systems. This raises specific issues for the design and the safety analysis, especially as regards the required improvement for the demonstration[21].

To guide, evaluate or compare the implementation of defence in depth by the different systems technologies, a homogenized approach is suggested. It can be used to properly consider the specific characteristics of each of these systems the objective being the definition of the required "defences" needed to provide an adequate response to the abnormal situations.

To implement such an approach, it is useful to introduce the concept of a Line of Protection (LOP). For a given level of the defence in depth, the Line of Protection is an "*effective defence"* (cf. IAEA General Safety objective) against a given mechanism or initiating event that has the potential to impair a fundamental safety function. This term is used for any set of inherent characteristics, equipment, system (active or passive), etc., and any procedure, all being part of the plant safety architecture, the objective of which is to accomplish jointly the mission needed to achieve a given safety function[22].

For a given event, and versus a given safety function, the LOPs provide the practical means of successfully achieving the objectives of the individual Levels of Defence. 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[23]. This notion allows simplifying the approach for the design and the safety analysis: the needs are expressed in terms of LOP for a given mission. The answers from the design (the provisions) can be of different nature: intrinsic characteristics, passive systems, active systems, procedures.

---

[21] The improvement in the domains, where - already for the current concepts - gaps exist (Human factor, computational tools reliability), is discussed above.

[22] For a given plant condition, and within a level of the defence, the implemented LOP will either

- prevent the abnormal condition from deteriorating further, and/or
- return the plant from the abnormal condition to a controlled safe condition and maintain it in a safe state.

[23] Assessing the independency of the provisions is indeed a very difficult question to tackle. The Objective Provision Tree and the corollary LOP approach provides a rather scattered view of the safety architecture (e.g.: one challenge to the Safety objectives ⇨ one set of provisions ⇨ one LOP). The use of other analysis methods of the safety architecture at a more global scale might be necessary, as a complement of the LOP approach, to anticipate the effects of possible interrelations within this architecture.

A.9.2 R&D for inherent and/or passive LOP

As for safety analysis, the implementation of intrinsic characteristics and/or passive provisions :

- Led to consider events of very low probability which involve the failure of this type of provisions[24];
- 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"[25];
- Has to address the lack of reliability data and the embryonic character of the methodologies for the evaluation of this reliability;
- Has to take into account mission of longer durations due to the lesser efficiency of these LOP[26] and due to the limited possibilities of intervention of the operator for the sequences' management[27].
- Has to achieve an objective for having, as far as possible, a progressive behavior[28] and the possibility for "fail safe" human intervention.

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

A.9.3 Research and development for improving the implementation of the Defence in Depth

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 and human errors, including the uncertainty associated with estimating such failures and errors. Complementary and essential characteristics that ensure the effectiveness of DiD are:

- an exhaustive defence: the identification of initiating events used to design the safety architecture should be as exhaustive as possible;
- a balanced defence: a balanced or homogeneous defence means that no initiator family participates in an excessive and unbalanced manner to the global frequency of the plant damage states;
- a graduated defence: without a graduated, progressive defence "short" sequences can

24 E.g. : Structural failur[es.]

25 E.g. : Start and set up the natural convection with risks for stratification.

26 E.g. : Natural convection behaviour.

27 E.g. : Impossibility and ban of manual shut down of the passive systems.

28 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

appear for which, downstream from the initiator, the failure of a particular provision entails a major increase, in terms of consequences, without any possibility of restoring safe conditions at an intermediate stage;

- a simple defence: the complexity of the whole architecture as well as the complexity of operations should be minimized as far as possible particularly because this complexity is a prominent influence factor on the human reliability in operation. Furthermore, this complexity analysis is also the only way of taking the interrelations between the LOP's into account at a very early stage of the conceptual design.

The PSA is a useful tool to assess the three last characteristics but it is not necessarily sufficient. Specific indicators have to be developed to help assessing the meeting of these objectives, notably in the domain of the prediction of human factors impact on the safety (e.g. through a specific indicator for operational complexity).

A.9.4 Safety related architecture: safety provisions identification and classification

According to the «risk informed» approach, the LOP classification is defined based on their importance for the safety of the system[29].

The optimization versus risk being the objective, the frequency of occurrence for the solicitation of the LOP and the consequences induced by their failure are to be simultaneously considered. To do this, the use of the conventional risk space (e.g. Farmer's curve) can provide a useful framework.

To correctly achieve the LOP classification there is a need for an increased quality in the prediction of their performances and their reliability within the risk space; for this, the PSA can bring essential insights and contributions. Such a need so becomes the objective and the motivation of the R&D that has to be implemented on PSA methodologies and data.

A.9.5 Situations to be considered for the safety evaluation

The objectives shown for the Gen IV systems require, among others, the exclusion of significant offsite consequences and this for any accidental situation. Such a goal is extremely ambitious but it must not be considered as absolutely mandatory; as for the others goals, according to the own terms of the Generation IV Roadmap, "*it has to be used 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".*

The integration of this concern means identifying the situations to be classified in the conventional design basis conditions (DBC[30]) and those considered as design extension conditions (DEC[31]) and, within the latter, those to address the category of severe plant

---

[29] It has to be pointed out that such a classification has strong feedbacks on the economy of the system.

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

[31] Design Extension Conditions (DEC) :A specific set of accident sequences that goes beyond DBC, to be selected on deterministic and probabilistic basis and including:

- Complex Sequences: Certain unlikely sequences which go beyond those in the deterministic design basis in terms of failure of equipment or operator errors and have the potential to lead to significant releases but do not involve core

conditions.

The consensus with the Safety Authority must be found, in agreement with current practices, by integrating, in a relevant way, the following recommendations:

- For future systems, severe plant conditions have to be taken into account at a preliminary stage of the design to obtain, in the case of reactors, a significant reduction of the core damage frequency (when applicable[32]) ; accidents which have a potential of intolerable releases of radionuclides shall be eliminated by design or "practically eliminated".
- According to the previous indications one could aim to achieve, for some of the future reactors, the exclusion of whole core melting. The logic related to severe plant conditions – requested to answer the principle of the 4th level of the defence in depth - is respected through the consideration of a set of selected "severe situations" for the installation and the core – the Severe Plant Conditions / SPC – that do not correspond necessarily to the generalized melting of fuel elements. The designer can propose to take into account, among others and as a matter of example, a limited amount of core degradation.
- The scenarios to be considered for the comprehensive demonstration (situations to be dealt with or situations to be excluded) are all those considered as being plausible. The process of selection of these scenarios can be deterministic, supported, when needed or interesting, by probability considerations and experts' judgment. The selection of these scenarios has to integrate the human factor. To simplify the demonstration, the selection of envelope plant conditions (without any reference to their plausible character) has to be considered as a possible way to proceed.
- Plant conditions with potential for intolerable releases of radioactivity are considered as being "practically excluded" based on preventive and/or management provisions, implemented to address the upstream plant conditions. The efficiency of the corresponding LOP must be proved. For the moment, there are no formal rules to define the sufficient character of these measures (e.g. no probability cut-off). The demonstration will thus have to rely on criteria or reasoning for elimination based on LOP sufficient in number, in variety and in robustness, and for which the independence can be demonstrated. These criteria have to be discussed on a case by case basis according to engineer's judgment and with the support of ad-hoc analyses.
- The evaluation of Severe plant conditions for the installation which have not been excluded, is made with a "best estimate" approach (e.g. through PSA) with in parallel an estimation of the uncertainties to estimate the plausible range of the consequences and to verify the absence of any cliff edge effect. The analysis of these situations leads to set up specific constructive solutions/provisions for the management and the mitigation of the consequences (e.g. the core catcher).
- According to the principles of "risk informed" the provisions set up for severe plant conditions do not ask necessarily for the same requirements / specifications - e.g. in terms of quality for the design / manufacturing - as those required for the LOP implemented for the management of the design basis conditions. Nevertheless, as indicated above, their performances must be demonstrated, periodically, all over the

---

melt, are identified as Complex Sequences. An example is simultaneous failure of redundant functions.

- Severe plant conditions: Certain unlikely event sequences beyond Accident Conditions involving significant Core Damage which have the potential to lead to significant releases.

Appropriate design rules and criteria are set for DEC, in general different from those for DBC.

[32] For specific designs, as for example the Very High Temperature Reactor, the core of which cannot melt (due to the lower power density) or the Molten Salt Reactor the core of which is already liquid.

life of the installation and their performances and their survival proved in environmental conditions compatible with the situations during which they would be requested/operated.

- For some of the situations which have been excluded, the additional demonstration is limited to show that there are no risks of cliff edge effects. Once this demonstration realized, no additional design measures will be requested.
- Finally, the tangible efforts to decrease the radiological consequences of all the possible accidental plant conditions have to be shown.

A.9.6 Severe plant conditions management and emergency plans

The selection of the confinement/containment strategy for the 4th generation systems bears a strong stake in terms of safety and cost. The achievement of the safety objectives, defined in terms of radiological releases, is obviously common to all the Gen IV systems. To guarantee the fulfillment of these objectives, some of the Gen IV systems foresee the application of approaches for the confinement which differ from those - conventional - which envisage a permanent ultimate tight barrier (static containment).

For some systems, the logic of "dynamic confinement" [33] can allow to guarantee, with a better reliability, the fulfillment of safety objectives thanks to lower uncertainties on the load conditions for the structures. The idea is not of modifying the logic of redistribution of the roles of the various levels of the defence in depth but rather of optimizing the quality of implementation for each of these levels[34].

As an example, for the very high temperature gas cooled reactors (VHTR), the specific characteristics of containment of the radioactive products by the fuel and the low activity level of the primary helium could lead, in case of accidental primary circuit depressurization accident, not to consider the total holding of gas inventory and to plan the closure of the containment building only after depressurization of the primary circuit. This could allow minimizing both the loads on the containment structures and the risk for releases over the long-term period.

In this configuration, particular devices have to allow limitation of the internal pressure by evacuating inert uncontaminated gases outside the reactor building. The acceptability of such a concept notably rests on a greater reliability of the closure of the reactor building at the moment required, as well as on the possibilities of filtration of the installation's releases.
Generally speaking, the analysis of the safety related architecture has to allow verifying the fulfillment of all the recommendations listed above. Efforts of specific R&D are to be foreseen to support the required demonstrations.

A.9.7 Safety and reliability for systems implementing specific processes

As a matter of example, some of the Gen IV systems aim at very high temperatures,

[33] Variable degree of confinement's tightness insured over time and defined as a function of the installation's conditions and of the risk of contamination incurred outside the installation.

[34] In these conditions, it is necessary to consider the fact that an option reducing the requirements of holding an internal pressure can allows defining design criteria based on external load (natural, industrial or hostile attacks) which must be clarified.

compatible with thermo chemical processes, e.g. for H2 production, who can raise specific risks (risks of explosion within the conventional part of the installation).

Specific R&D actions are to be foreseen to exactly define the conditions and the characteristics of these risks and the modes of loading of the nuclear installation structures.
The corresponding potential hazards have to be considered, as those conventional, achieving the recommendations above. Other possible applications for the Gen IV systems could generate specific R&D needs.

A.9.8 Mastery of effluents and waste

The effluents reduction remains a priority objective. It concerns both the reactor and the fuel cycle installations. For the reactor, the problem is related to the coolant and the chemical treatments which are necessary. For the "fuel cycle", the differences between the processes under assessment (aqueous, pyrochemical or mixed) have to be quantified but one of the strongest constraints will come from the location of the installations (the seaside or the inside of lands) which will affect - for a given objective of safety - the nature of the auxiliary technologies to be implemented/operated.

The strategy recommended by the Gen IV Initiative is the closed fuel cycle to insure a significant contribution to the sustainable development. In connection with the objective of mastering the waste, this strategy will allow: reducing the volume of waste, their toxicity as well as the risks of proliferation[35]. This justified the selection of four concepts with fast spectra, over six. Moreover the Gen IV Initiative explicitly recommends the implementation of systems which include an integrated cycle (i.e. in situ reprocessing) and minimizes needs for transport. All the current or foreseen activities relative to the advanced cycles are to be organized in this context.

[35] Cf. The Gen IV Roadmap : *"Systems that employ a fully closed fuel cycle hold the promise to reduce repository space and performance requirements. ..... These strategies hold the promise to reduce the long-lived radiotoxicity of waste destined for geological repositories by at least an order of magnitude. ....The advanced separations technologies for Generation IV systems are designed to avoid the separation of plutonium and incorporate other features to enhance proliferation resistance and incorporate effective safeguards."*

Abreviations

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