# Basis for the Safety Approach (BSA) for Design & Assessment of Generation IV Nuclear Systems

P. GAUTHÉ 1, T. SOFU2, L. AMMIRABILE3

1 CEA, DES, DER, Cadarache F-13108 Saint-Paul-Lez-Durance, France

2 Argonne National Laboratory, DOE, USA

3 JRC Petten, European Community

Email contact of corresponding author: paul.gauthe@cea.fr

**Abstract**

The six Generation IV reactor concepts that have been selected by the GIF members present a diverse set of design and safety characteristics. The Risk & Safety Working Group (RSWG) was formed within the GIF to promote a consistent and effective approach to assuring the safety of Generation IV nuclear energy systems.

Gen IV reactors are significantly different from the earlier generation of light water reactors. The overall success of the Generation IV program depends on, among other factors, the ability to develop, demonstrate, and deploy advanced system designs that exhibit excellent safety characteristics. While the RSWG recognizes the excellent safety record of nuclear power plants currently operating in most GIF member countries, it believes that progress in knowledge and technologies, and a coherent safety approach, hold the promise of making Generation IV energy systems even safer and simpler than this current generation of plants.

Three specific safety goals are identified for Generation IV systems : safety and reliability of normal operation, very low likelihood and degree of reactor core damage, elimination of the need for offsite emergency response.

This paper written by the RSWG discusses the ways to achieve these high-level safety objectives and the achievements made in the past ten years in safety methodologies : development of the Integrated Safety Assessment Methodology, lessons learnt from the Fukushima accident, progress in the harmonization of safety approaches and definition of the practically eliminated situations.

## INTRODUCTION

The Risk & Safety Working Group (RSWG) was formed to promote a consistent and effective approach to assuring the safety of Generation IV nuclear energy systems. The six Generation IV reactor concepts that have been selected by the GIF members present a diverse set of design and safety characteristics. A number of these characteristics are significantly different from those presented by the earlier generations of light water reactors. The overall success of the Generation IV program depends on, among other factors, the ability to develop, demonstrate, and deploy advanced system designs that exhibit excellent safety characteristics. While the RSWG recognizes the excellent safety record of nuclear power plants currently operating in most GIF member countries, it believes that progress in knowledge and technologies, and a coherent safety approach, hold the promise of making Generation IV energy systems even safer and simpler than this current generation of plants. Since its inception, the RSWG focused on defining the attributes that are most likely to help meet the Generation IV safety goals and identifying methodological advances that might be necessary to achieve these goals. This has been done consistently with the work of IAEA. The paper summarize the recommendations of the RSWG established in 2021.

## GOALS FOR GENERATION IV

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

• Resource utilization

• Waste minimization

• Reduced life-cycle costs

• Reduced risk to capital investments

• Improved operational safety and reliability

• Reduced likelihood and degree of core damage

• Elimination of the need for off-site emergency response

• Enhanced proliferation resistance and physical protection

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

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

1. Generation IV nuclear energy systems will **excel in operational safety and reliability**. The focus of this goal applies to safety and reliability during normal operation of all facilities employed in the nuclear fuel cycle, and thus, deals with the relatively likely kinds of operational events that set the forced outage rate, determine worker safety, and result in routine emissions that could affect workers or the public.
2. Generation IV nuclear energy systems will have **a very low likelihood and degree of reactor core damage**. This goal calls for design features that create high confidence that the possibility of core damage accidents will be very small for Generation IV reactors. The goal deals with both minimizing the frequency of initiating events, and introducing design provisions to ensure that the plants can successfully control and mitigate the consequences of accidents causing core damage. For accidents that do not lead to a severe accident, the design aims to ensure that the radiological consequences shall not lead to the need to implement measures to protect populations.
3. Generation IV nuclear energy systems will **eliminate the need for offsite emergency response**. It is desirable that Generation IV systems demonstrate, with high confidence, the capability of the safety architecture to manage and mitigate the consequences of severe plant conditions so that any potential releases of radiation will be small and have only insignificant public health consequences. Two cases have to be considered to fulfil this ambitious objective:
	1. In the case of a severe accident, the objective is to have very low releases such that no off-site measures are necessary. If measures are nevertheless necessary (e.g., restrictions on consumption on a crop), they shall be limited in time and space with sufficient time for their implementation. Even temporary evacuation of populations should not be necessary and only sheltering, limited in time and space, shall be envisaged.
	2. Accidents likely to lead to very large off-site radioactive releases, or with kinetics that would not allow for the timely implementation of necessary measures to protect populations, shall be rendered physically impossible or, failing that, extremely unlikely with a high degree of confidence (practical elimination).

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

These goals continue the past trend and seek simplified designs that are safe, and further reduce the potential for severe plant conditions and minimize their consequences. The achievement of these ambitious goals cannot rely only upon technical improvements, but will also require systematic consideration of human performance as a major contributor to the plant availability, reliability, inspectability, and maintainability. Since the proliferation resistance and physical protection are also essential priorities in the expanding role of nuclear energy systems, identifying safety and security interfaces and establishing common design principles and features that improve both the plant safety and security are also a goal of Gen IV systems.

## GENERATION IV SAFETY PHILOSOPHY

Opportunities exist to further improve on nuclear power’s already excellent safety record in most countries. As a starting point, the **RSWG recognizes that the level of safety that has been attained by the vast majority of operating nuclear power plants (Generation II) in most countries of the world is already very good**. In parallel, the quantitative safety objectives applicable to the reactors of the third generation (e.g. AP1000, EPR etc…) are very ambitious and assure an improved level of protection reducing the level of risk in a demonstrable way. For Generation III reactors, the lessons learnt from the Fukushima accident has been taken into account. These lessons must also be considered at the design stage for Generation IV reactors. Considering the already ambitious Generation-III safety objectives as the reference, Generation-IV reactor systems will excel in safety, with improved safety design and more robust safety demonstration. Further safety improvements for Generation IV systems are possible through progress in knowledge and technologies and the application of a cohesive safety philosophy early in the design process. It is worthwhile and achievable to further improve what is already a very safe source of clean and reliable energy. Such improvements will, in particular, address the way to achieve the level of safety through the implementation of a safety that will be “built-in” to the fundamental design rather than “added on” to the system architecture.

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

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

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

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

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

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

## Design and assessment of innovative systems

The Design Basis for Generation IV energy systems should cover the full range of safety significant conditions. **The historical notion of a single bounding design basis accident must be replaced by a spectrum of possible accidents that represent, with a high degree of confidence, the range of physical events that could conceivably challenge the plant safety**. For accidents other than severe plant conditions, the design aims to ensure that the radiological consequences shall not lead to the need to implement measures to protect populations. In the case of severe accident, the objective is to have very low releases such that no off-site measures are necessary. If measures are nevertheless necessary, they shall be limited in time and space with sufficient grace period for their implementation. Even temporary evacuation of populations should not be necessary and only sheltering, limited in time and space, shall be envisaged. Accidents likely to lead to very large off-site radioactive releases, or with kinetics that would not allow for the timely implementation of necessary measures to protect populations, shall be rendered physically impossible or, failing that, extremely unlikely with a high degree of confidence so that they can be considered as practically eliminated. Among other considerations, these efforts should be based on the experience in the implementation of this concept for latest designs, specific R&D and engineering judgement.

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

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

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

Updated safety analysis methods should be applied to examine the full range of safety-significant issues. As part of an adequate treatment of the full spectrum of design conditions including the domain of severe plant conditions, these updated methods must, for example, consider internal events and external hazards in a consistent way, factoring in the treatment of physical protection issues along with associated uncertainties. Objectives and practices for the design improvements. To efficiently set up these practices, four complementary ways may be followed by the designer: 1) Critical and systematic examination and consideration of the feedback from the past experience; 2) rationalization of the design approach by the deliberate adoption of the ALARP principle based on a cost-benefit analysis; and 3) implementation of the concept of defence-in-depth in a manner that is demonstrably exhaustive, progressive, tolerant, forgiving and well-balanced. Finally, special attention should be given to the treatment of the severe plant conditions through provisions of measures that help managing such conditions.

Achievement of the safety demonstration’s robustness. This rests on the ability of the designer and the developer to be exhaustive in the recognition of risks stemming from phenomena considered in the design. Whenever possible, plant design features based on natural phenomena and physical properties of materials should be relied on to demonstrate, in an “intuitive” manner, the ability of the plant to prevent the accident progression with an adequate degree of confidence, an understanding of the associated uncertainties and provision of sufficient margins, and the minimization of impact on workers and public. Practical assessment tools to support the design and evaluation activities. Among the conventional tools such as PIRT, probabilistic, deterministic, and phenomenological assessments, the Objective Provision Tree and the notion of Line of Protection which allow schematizing the whole safety architecture are suggested as part of the process to help the plant design and evaluation.

## LESSONS LEARNT FROM THE FUKUSHIMA ACCIDENT

Immediately after the Fukushima Daiichi accident specific activities were launched with the objective to synthetize the lessons learned and to provide indications (requirements and recommendations) applicable for the updating of nuclear installations in operation and / or for the design and the assessment of future nuclear installations. Significant changes concern, in particular, the management of the severe accidents and the taking into account of natural hazards of external origin. The natural external hazards considered in the design have to be adequately defined. Additionally, the combination of hazards has also to be assessed (e.g., combination of earthquake and flooding). Then, the consequences of more severe natural external hazards has to be assessed in a design extension domain. The Fukushima accident has shown that, because of the occurrence of external hazard with a magnitude beyond the one considered in the design basis, multiple failures may occur inside a given plant, or simultaneously in different plants located in the nuclear site, or outside the nuclear site.

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

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

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

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

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

## POTENTIAL FOR SAFETY IMPROVEMENTS

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

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

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

• The concept of “optimal risk reduction” (ALARP )

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

• The consideration of ambitious objectives

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

• 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. The latter is recognized as a fundamental principle the application of which has to be improved by, e.g.: the consideration of the internal initiators and the external hazards in a consistent way; the implementation of provisions with a logic which answers the notion of independent and successive defence-in-depth levels; the consideration of the physical protection issues; the consideration of “severe plant conditions”; the integration of the notion of "practical elimination" which will require adequate demonstration.

• Extremely Reliable Plant Systems

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

• Reduced Reliance on Human Intervention

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

## PRACTICAL ELIMINATION

An essential objective of the new reactor design is to limit, in the event of a severe accident, the radiological consequences on the environment and on the population. For Generation IV reactors, in the event of a severe accident, even a temporary evacuation of population should not be necessary and only a sheltering, limited in time and space, should be permissible. The fundamental safety principle applied to reactor design is the Defence-in-Depth. The application of this principle requires extremely reliable provisions that assure prevention of severe accidents within first three levels of defence-in-depth. Despite these provisions, the fourth level also requires reliable mitigation means to manage the consequences of severe accidents assuming failure of prevention provisions.

The design aims at setting up mitigation provisions for all the possible severe accidents. **Nevertheless, there may still exist some severe accident situations that cannot be reasonably covered by these mitigation provisions**. If consequences of such severe accident situations without mitigation provisions might lead to either early radiological releases (not leaving sufficient time to implement emergency response) or large radiological releases (requiring the displacement of populations over a significant period of time or in an wide area), they need to be practically eliminated. Such situations need to be identified in the design so as to make them extremely unlikely to occur with appropriate design or organization provisions. As such situations being an exception to the defence-in-depth fourth level implementation, they should be limited in number. The practical elimination is an approach that involves, from the onset of the design process, identification of severe accident situations that would not be controllable under reasonable conditions, and therefore making them extremely unlikely to occur with a high level of confidence through appropriate design and operating provisions.

The goal is to identify, from the very beginning of the project, the situations that cannot be reasonably controlled, and to provide, as early in the design studies as possible, the provisions that will make these situations extremely unlikely with a high level of confidence. To be able to identify these situations as the cases to be practically eliminated from the early stages of a design process, first the dominant risk factors that can lead to significant radiological releases need to be identified through a "top down" approach. A limited number of situations to be practically eliminated should result from this identification phase. It should be emphasized that the main challenge is to identify the situations for practical elimination, not the sequences that may lead to them.

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

* Type 1: The severe accidents leading to a violent energetic phenomenon likely to damage the containment in an irreversible manner (e.g. a severe accident leading to a hydrogen explosion);
* Type 2: The situations successively leading to an unacceptable deterioration of the mitigation means following a severe accident (e.g. for some reactors, the extended complete loss of residual heat removal function);
* Type 3: The severe accidents occurring when the mitigation means are not available or insufficient (e.g. accidents during fuel handling operations).

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

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

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

Practical elimination demonstrations involve only a limited number of extremely unlikely situations. Although these demonstrations would be design specific, it is possible to give some general indications. These demonstrations will be explicitly made in the safety report. The goal of this demonstration is to give evidence that the situation is extremely unlikely with a high level of confidence. The designer first examines the possibility to make this situation physically impossible under reasonable conditions. When the physical impossibility is not achieved, the demonstration relies on the following deterministic approach:

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

The provision adequacy can be evaluated as follows:

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

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

## INTEGRATED SAFETY ASSESSMENT METHODOLOGY

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

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

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

 Fig. 1. Task Flow of GIF Integrated Safety Assessment Methodology (ISAM) in Design Process



## CONCLUSION

As a starting point, the RSWG recognizes that the level of safety that has been attained by the vast majority of operating nuclear power plants in most countries is already very good. Moreover, the safety objectives applicable to the reactors of the third generation are already very ambitious and guarantee a very high level of protection reducing the level of risk in a demonstrable way. The diversity of technologies that represent Generation IV systems require new thinking and new methods, using a proven staged approach. The RSWG believes that, through advanced technology and the early application of a cohesive safety philosophy, it is worthwhile and achievable to further improve on what is already a very safe source of clean and reliable energy. Although measurable safety improvements might be achieved in a number of different ways, the RSWG believes that one of the most important fundamental means lies in the concept of safety that is “built-in, not added-on.”. 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.

ACKNOWLEDGEMENTS

The authors, as co-chairs of the RSWG, acknowledge all past and present members of the RSWG for their support and thoughts for building this cohesive safety philosophy through the years.

References

1. Technology Roadmap Update for Generation IV Nuclear Energy Systems, <https://www.gen-4.org/gif/upload/docs/application/pdf/2014-03/gif-tru2014.pdf>, January 2014.
2. An Integrated Safety Assessment Methodology (ISAM) for Generation IV Nuclear Systems <https://www.gen-4.org/gif/upload/docs/application/pdf/2013-09/gif_rsgw_2010_2_isamrev1_finalforeg17june2011.pdf>, June 2011