Safety of Gen-IV Reactors
Dr. Luca Ammirabile, Euratom, EU

Berta Oates: Patricia is the Technical Group Manager of the Radiological Group at the Pacific Northwest National Lab, and she is also the Chair of the Gen IV International Forum Education and Training Task Force.

Patricia Paviet: Thank you very much, dear Berta. Good morning, everyone. I'm very happy to have Dr. Luca Ammirabile from the European Commission Joint Research Center in Petten, the Netherlands, with us today. He is a Group Leader of the NUclear Reactor Accident Modelling team of the Nuclear Reactor Safety and Emergency Preparedness Unit. His current research activities are core thermal-hydraulic analyses, deterministic code application and development, and safety assessment of advanced reactors.

Since 2014, he has been Co-chair of the working group on Risk and Safety of the Gen IV International Forum. He is also European Commission Representative of the OECD/NEA Working Group on the Analysis and Management of Accidents and also the Working Group on the Safety of Advanced Reactors.

Prior to 2007, when he joined the European Commission, Dr. Ammirabile worked at Tractebel Engineering in Belgium in the Thermal-hydraulics and Severe Accident Section in support of the safety assessment of the Belgian Nuclear Power Plants.

In 2003, he earned his PhD from the Imperial College of London and in '99 he earned his master’s degree in nuclear engineering from the University of Pisa, Italy.

So without any further delay, I give you the floor, Luca, and I thank you on behalf of the GIF Education and Training Task Force for volunteering to give this webinar. Thank you so much, Luca, and you have the floor.

Luca Ammirabile: Thank you, Patricia, and welcome, everyone, to this webinar on the safety of Generation IV systems.

As you see from the summary of this webinar, I am going to talk about the establishment of the safety approach of Generation IV systems based on the work done by the Risk and Safety Working Group, which is one of the cross-cutting methodology working groups that has been established within GIF.

I hope you see the view here. We will start our virtual journey with a recall of the GIF safety goals. I will then shortly speak about the scope and the objectives of the Risk and Safety Working Group before going more into details of the basis safety approach for Generation IV reactors. I will also briefly descript the ISAM, the Integrated Safety Assessment Methodology that was developed by the group to assess the safety of Gen IV systems with a very short pilot application of the methodology itself. I will then close this webinar with an overview of the ongoing Risk and Safety Working Group activities.

So let's start with a recall of the Generation IV safety goals. So as you well know, at the beginning of GIF, the Technology Roadmap was drafted, where a set of goals were put in place for four main domains: sustainability, economics, proliferation assistance and physical protection, and indeed, safety and reliability.

These goals were put into place literally to stimulate the research for innovative systems and also to somehow motivate and guide the research and development on Generation IV systems.

As for concerned safety and reliability, we have then three goals. The first calls for Gen IV system operation that will excel in safety and reliability, a system that will have a very low likelihood and degree of reactor core damage, and finally, a Gen IV system that will eliminate the need for offsite emergency response

We will shortly see the interpretation of these goals into the safety approach for Generation IV systems, but the first point that I want to raise is the fact that these goals, as embedded into the Generation IV International Forum, should be applicable to all six Generation IV systems, despite their very deep different characteristics.

In fact, you can see on this table all the differences that the six systems have in terms of particularly neutron spectrum, type of coolant, and operational pressure, and temperature, as well as differences in reactor size.

It's clear then that there was somehow a need to have a kind of harmonized approach on safety for Generation IV systems, and these eventually led in 2004 to this establishment of the Risk and Safety Working Group, which is one of the three methodologic working groups, cross-cutting working groups, of GIF.

The RSWG had in particular the objective to promote a consistent approach on safety for Generational IV systems, define what are the safety principles and objectives based on Generation IV safety goals with a clearer view to guide somehow safety-related R&D activities, and finally, the development of a technology that could be technology neutral, sorry, a methodology that could be technology neutral and that could lead to the assessment, safety assessment, of Generation IV systems.

Let's now go a bit more into what are the main aspects of the Generation IV safety philosophy as developed within the Risk and Safety Working Group.

So first of all, considering that the Safety Objectives of the so-called Generation III evolutionary-like water reactors are already very ambitious, there are still margins for further improvement and then for a higher safety level for Generation IV systems, considering essentially the combination of inherent advanced features due to the innovative technology and, very important, an early application of the safety approach or safety philosophy so that we can achieve a robust design in a way that safety is already from the preconceptual stage built in the design itself rather than added on.

In the second instance, the Risk and Safety Working Group recognizes the utility to base the safety assessment on both the deterministic and probabilistic approaches clearly to the extent and limits of the available experience in the potential very innovative technology.

Another point is clearly that the design should address all plant conditions, including severe plant conditions.

The design should also take due account of internal and external hazards. And should make use as much as feasible of modeling and simulation activities in the design itself.

In summary, all these attributes essentially call for a full implementation of the defense in depth already from the early design stages of Generation IV systems. And this is how, somehow, in line with the same safety and reliability goals, as well can be somehow summarized looking for an announcement of the difference in the design.

In fact, when we talk about excellence in operational safety and reliability, essentially we are addressing the safety during normal operations and anticipated operational events, focusing really on the reinforcement of Level 1 and Level 2 of defense in depth.

Then when we talk about very low likelihood and degree of reactor core damage, we want to minimize the frequency of the initiating events, introduce specific design features for the control and mitigation of accidents in order to avoid core damage. So we want to reinforce Level 2 and Level 3, and in general the design for severe accident prevention.

Finally, when we talk about eliminating the need for offsite emergency response, we look at a comprehensive safety architecture that is able to manage and mitigate severe plant conditions and also reduce the likelihood of early or large releases. In this respect, we want once again to strengthen the 4 Level defense in depth with this dedicated to the design for several accident mitigation.

So the defense in depth is already a fundamental principle of nuclear safety, and it must be preserved and even reinforced in the design of Generation IV systems. Indeed, this is the key to achieve the safety robustness that will then lead to enhancement of the safety of Generation IV designs.

In addition, to meet these objectives, the defense in depth should be implemented in a way that is first instance exhaustive so that all the risks that could affect the fundamental safety function should be identified in a comprehensive way. The defense in depth should also be progressive in the sense that accident scenarios should eventually cause a progressive failure, of sequential failure, of each level of defense in depth, and therefore reducing the likelihood of this happening without having short sequences or kind of bypass leading directly from Level 1 to Level 4.

Additionally, the defense in depth should be tolerant in the sense that any small deviation of the physical parameters outside the expected range should not lead to severe consequences. Essentially, we should not have any kind of cliff edge effect.

Another important aspect is forgiveness, to assure that a sufficient grace period is allowed for manual intervention and repair during accidental situations.

And finally, the design and the defense in depth should be balanced in the sense that a specific action sequence should not contribute in an excessive or unbalanced manner to the global frequency of the damaged plant state.

These five attributes really reinforce implementation of the defense in depth.

And additionally, I will say, we also, the design of the Gen IV system should also lead us, as far as feasible, by simple design, taking into account that generally simple design assures a high level of robustness and safety, and this amount differentiates Gen IV systems from high complexity, this experience in particular for Gen III systems.

I also want to (allay) the fact that these attributes actually defined in early 2000 or 2008, somehow already answers the challenges that came after the Fukushima accident. In fact, when we talk about progressiveness of the defense in depth, essentially, we want to avoid any short sequence as what happened for example in Fukushima, as well as any potential for cliff edge effects when we talk about tolerant implementation of defense in depth.

And also in terms of forgiveness, to have enough time to be able to have manual intervention in case of potential accident.

Let's go now more on the basis for the design and assessment. Clearly, the design of Generation IV systems should cover the full range of plant state, including severe conditions. And special attention should be given to severe plant conditions, wide implementation of specific provisions that could be put in place against such conditions.

Additionally, all internal events and internal and external results have to be considered, together with eventual uncertainties that are related to the innovative features of a new technology, and this should be put in place in particular through a combination of both experimental and modelling activity.

Finally, a special effort should be made particularly for the demonstration of the practical elimination of all those accident sequences that can be associated with the potential for early or large releases.

So looking in particular at the plant states that Generation IV systems should cover, essentially these go from the normal operation all the way to line extension conditions, which (outer) design are essentially all the severe risk and the practically eliminated accidents.

I would like to spend some words on the notion of severe accidents. In fact, some concepts, some Gen IV concepts, can clearly associate the notion of severe accidents with that of a light water reactor associated with a core, the melting of a core. However, designs like the BSTR and molten salt reactor cannot express potential severe accident conditions through the melting of the core, even they are design characteristics. However, this doesn't mean that a severe accident, which is ???, as an accident it goes beyond the design basis, cannot be postulated.

So in any case, potential sequences that go beyond the design basis need to be assessed, but it's important to notice that according to the characteristics of some design tracks, the potential severe accident scenario can be put in Level 4, so within the design extension, but also can be put in Level 5, so out of the design itself. What is an essential aspect in the assessment is that the possible severe accident scenario is indeed considered and evaluated in a global design assessment.

So we have seen essentially what are the main principles of the safety approach for a Gen IV system. We've seen how, somehow we can assess within our design those principles, and this is essentially linked to the development of the ISAM, the Integrated Safety Assessment Methodology, that had the objective to ensure a consistent approach to the safety applied to all six systems.

The methodology consists of five tools. They are not, let's say, new in their formulation, maybe with the exception of the QSR, so the Qualitative Safety Requirements Review and the Objective Provision Tree, or OPT. But actually, it's really the systematic use of these tools that should somehow ensure the consistency of the design with the safety approach for Generation IV systems.

The set of tools can be used separately, and essentially the methodology covers the full entire cycle, from the preconceptual design all the way to the final design, licensing, and operation.

I will just shortly introduce each of these tools.

Starting with the Qualitative Safety-characteristics of Safety Requirements Review, or QSR, this tool is essentially a kind of checklist where in the form of a table, you can see here, essentially all the safety requirements, safety principles, even guidelines, are expressly mentioned in terms of classes of requirements, from the technology neutral all the way to the design specific, and for the three fundamental safety functions and defense in depth levels. Based on these tables, any specific design features or design characteristics, design system and so on, can be assessed against the current requirements, the current regulatory framework, to see indeed to which extent this is in line, the system is in line with the current requirements.

The second tool is quite well-known. It's the Phenomena Identification and Ranking Table, that is a tool quite powerful to identify really the gaps in terms of importance of phenomena, as well as the level of knowledge of those phenomena. Indeed, this tool is quite interesting, quite powerful, really to identify any potential R&D needs dedicated to the level of knowledge of important phenomena.

Then the third is the Objective Provision Tree. This is a rather qualitative tool that allows to give a graphical representation of the safety architecture, so the set of provisions that are put in place to prevent, to control, and mitigate potential accidents. In addition, it identifies essentially the risks or the initiating events. You also put in place all the potential lines of protection against specific mechanisms.

So graphically, we have for each level of defense that is specified in terms of specific objectives to be achieved and barriers that need to be protected, and then for the different safety functions, in the OPT, we identify the challenges to cope with and the mechanism that essentially are the initiating events, they need to prevented or eventually controlled through a set of provisions, it can be material, in the sense of system features or components, or immaterial in the sense of procedures put in place in order to avoid, prevent or control the mechanism itself. This is a very powerful tool because it allows to have really an overview of the safety architecture, as well as identify really the independence of the different levels of defense in depth, and potentially identify eventually ??? failure that needs to be addressed and can be addressed in advance.

And finally, we have the two remaining tools, that are the deterministic phenomenological analysis, which is the traditional safety analysis that is used to assess the response of the system to the different challenges, and the probabilistic safety analysis that allows us to define the risk spectrum on our design, and particularly to answer the three basic questions in terms of what can go wrong, how likely is this to happen, and what are the potential consequences?

So you can see here that the methodology is really a combination of a deterministic and probabilistic. It has this flexibility to announce one of the other aspects, based also at the level of maturity of the methodology itself.

So these are the tools. We see now how these tools can be applied into the safety assessment itself. To do that, we need to have a kind of definition of safety assessment, and this comes from IAEA, from the agency, that identifies in terms of safety assessment essentially two steps.

The first step is the verification of the compliance or our system with what are the principles, the requirements, and the guidelines of the current regulatory framework.

The second step is actually the verification of the conformity or the safety architecture with the expected quantitative safety objectives, so to say, the design criteria that are put into place at each level of defense in depth in terms of characteristic temperatures to achieve in case of accident or in the later defense in depth level, in terms of potential release to the environment.

In this table we have the cross-cutting relationship between the different steps of the design and assessment process with the respective ISAM tools. So in the first instance, once the goals, the objectives, the principles, so the regulatory framework is put in place and a set of safety options or design options are identified, the first step, as we said before, is to verify the compliance with the current requirement, and this is mainly the work, the domain of the QSR where this compliance can be verified and eventually a process of identification, correction, can be put in place.

Once the safety option or the design option are put in place, then the design itself kicks in. So we have a first instance, the identification or what are the challenges for the safety functions, as well as identification of mechanisms or initiating events, plant conditions to be considered in the design. This is mainly the work that can be performed through a PIRT exercise together with an OPT exercise, taking into account that the OPT also identified also in a qualitative way the set of provisions that are put in place in order to cope with, to prevent, and to control the mechanism.

Once this is done, and then somehow the safety architecture is in place, then we have the design and sizing of the provisions themselves and the analysis of the response to the transients, which is the classical safety analysis. And this is done through the combination, I would say, of deterministic studies, as well as probabilistic studies, with a final assessment of the safety architecture that should be, as I said before, exhaustive, progressive, tolerant, forgiving, and balanced.

It's clear that this process is an iterative process. By itself, it can be very lengthy and generally time and resource consuming, but it's this way, in a systematic way, that should ensure really that robustness of the design itself.

I want to then conclude with a practical example of the use of ISAM. This example actually comes from our Japanese colleagues. Please don't look at the technical detail but rather on the use of the different tools.

So the reference design, the Japanese sodium fast reactor is a loop type SFR, and in terms of the decay heat removal system, it has two primary reactor auxiliary cooling systems called PRACS, which are linked with the intermediate heat exchangers, and one direct reactor auxiliary cooling system, also called DRACS, which is directly emerged into the reactor vessel.

So the first activity was really to identify the different challenges and mechanisms and through the OPT really identify the set of provisions to be put in place in order to cope with this mechanism. This is an example developed for the Level 3 for the core removal in terms of fundamental safety function.

Then the analysis was focusing on the protected loss of heat sink considering here we are in the design extension conditions, so with the failure of one of the PRACS, so the exercise wanted to assess the short-term loss, potential loss, of cooling and to assess the capability of keeping the integrity of the core using the remaining PRACS and DRACS, both of them or either one of them.

So the scenario analyzed by the deterministic study was identified by PSA through an event tree. PSA analysis gave the success or the failure within 24 hours. So the scenarios were identified and assessed through the DPA that showed that essentially only in case of operation out of both the PRACS and DRACS the core integrity could be guaranteed, while for all the other cases, this would lead to damage.

In particular, the initial design for the PSA results related to the protected loss of heat sink showed core damage frequency of 5 to 10^{-7} for the reactor here, with a heavy contribution of the short-term, so the sequences that occur within the 24 hours after reactor shutdown.

In order to improve these values, an option was to enhance the heat removal capacity of a single train within the 24 hours through the addition of a non-safety-related air-cooler blowers with associated short-term batteries. In this way, from the initial design with the application of these non-safety-related air-cooler blowers, it was possible to add an additional access path that eventually led to a reduction or the protective loss of heat sink to 9 to 10^{-9} for a reactor year, to about 50 times less than before. This is a very, very, let's say, simple example of how really the combination of OPT for the definition of the provisions and the challenges and DPA and PSA could indeed help to build in the safety.

We reach now the conclusion of this webinar.

So the summary, the Risk and Safety Working Group aims to reach a high level of safety through essentially the combination of the inherent features of the advanced technology with the early application of an improved safety approach, and this is done essentially through a systematic, a full and systematic implementation of the defense in depth in such a way that safety is built-in rather than added on.

As concerns the ISAM methodology, we don't really have new tools, but it's really the systematic approach on the ??? methodology that assures a robust demonstration, and the use of ISAM then can indeed support the safety assessment.

I want to conclude my webinar with just an overview of the ongoing activity of the Risk and Safety Working Group.

In particular, we are working now on the updates of the basis of the safety approach for Generation IV systems. This document was actually produced in 2008. The idea is really to take into account the lessons learned from Fukushima, as well as the evolution of the regulatory framework in the last ten years.

And then, other reports that are done in collaboration with the individual systems during committees. To date, we have the white paper related to the pilot application of ISAM methodology. The objective is to demonstrate the applicability of ISAM as a self-assessment for each of the Generation IV systems and provide somehow a guidance on improving the safety aspects of the Gen IV systems using ISAM.

And then the safety assessment reports for the six Generation IV systems, that is a kind of snapshot of the characteristics of these systems, of their challenges, and their remaining R&D needs.

And finally, the contribution that the group is giving to the definition of the safety design criteria for the SFR within the dedicated task force and directly in collaboration with the (SSCs) for the other designs.

Finally you see here, the link, the direct link within the GIF portal to the webpage of the Risk and Safety Working Group where you can find all the documentation developed by the Working Group in these years.

This concludes my webinar, and thank you for your attention, and I am open to your questions, to answer your questions. Thank you.

Oates: Thank you very much, Luca, for your presentation. If you have questions, please feel free to type those into the chat box. While those questions are coming in, we'll just take a quick look at the upcoming webinar presentations. In March, a presentation on the Allegro Experimental Gas Cooled Fast Reactor Project. In April, we look forward to the European Sodium Fast Reactor: An Introduction. And in May, the Formulation of alternative cement matrix for solidification/stabilization of nuclear waste.

Thank you again for participating, and if you have questions, feel free to type those in now.

We have one question. Let's see if I can get that to show for you.

Ammirabile: I don't see it.

Oates: Actually, it's a request to have the presentation provided to one of the attendees, and we will do that following today's presentation.

So again, if you have any questions at all, please feel free to type those in and we'll take as many as we have time for.

Luca, there's a question. Are you able to see the question chat box? It says, "I was wondering if you could elaborate more on the human factors."

Ammirabile: Elaborate more on the human factors?

Oates: Right

Ammirabile: So indeed, I will say this is a good thing related actually to the update that we are doing for the basic approach because this is somehow linked also to the lessons learned from Fukushima.

So in this respect, the safety approach for Generation IV systems doesn't explicitly include human factors in the attributes. The characteristics of the defense in depth when we talk about, in particular, forgiveness aim to prepare the design to be able to help somehow any potential intervention of manual intervention in the case of accident, so in order to improve somehow the capability of human action in the case of accident. This is expressed in terms of the attributes related to that.

Any specific assessment of the human factor is clearly to be done eventually in the framework of probabilistic studies that are associated with the design assessment, but we don't have any specific consideration of that within the design approach.

I think there are some questions but I cannot see them, read them.

Oates: Does anybody else have questions for the presenter today? Luca has time to take a couple more I think.

Ammirabile: Oh.

Oates: Thank you again, Luca, for taking the time to put this presentation together and share the information with us. It's greatly appreciated.

Ammirabile: Thank you.

Oates: The presentation was recorded today. If you give us just a little bit of time, a couple of days, we'll get the recorded version posted to the GIF website, where you will be able to re-review it at your leisure, along with a copy of the slide deck.

Ammirabile: Okay, thank you very much.

Paviet: Okay. Thank you. Thank you, Luca.

Ammirabile: Thank you, Patricia, also, for organizing this.

Paviet: Have a good day, everybody. Thank you, Berta, again.

Oates: Thank you. Bye-bye.

Paviet/ Ammirabile: Bye.