Risk-Informed design process of the IRIS reactor

Andrea Maioli

Department of Nuclear Engineering, Politecnico di Milano technical University: via Ponzio, 34/3, 20133 Milano, Italy, andrea.maioli@polimi.it

David J. Finnicum

Westinghouse Electric Co.: 20 International Dr., Windsor, CT 06095 USA, david.j.finnicum@us.westinghouse.com

Luca Oriani

Westinghouse Electric Co., Science and technology Department: 1344 Beulah Rd., Pittsburgh, PA 15235 USA, OrianiL@.westinghouse.com

Chiara Leva

Department of Management, Economics and Industrial Engineering, Politecnico di Milano technical University: via Colombo, 40, 20133 Milano, Italy, chiara.leva@polimi.it

Davide Lamperti

Department of Nuclear Engineering, Politecnico di Milano technical University: via Ponzio, 34/3, 20133 Milano, Italy

Marco Ricotti

Department of Nuclear Engineering, Politecnico di Milano technical University: via Ponzio, 34/3, 20133 Milano, Italy, marco.ricotti@polimi.it

Abstract – *Westinghouse is currently conducting the pre-application licensing of the International Reactor Innovative and Secure (IRIS). The design philosophy of the IRIS has been based on the concept of Safety-by-Design^{TM} and within this framework the PSA is being used as an integral part of the design process. The basis for the PSA contribution to the design phase of the reactor is the close iteration between the PSA team and the design and safety analysis team. In this process the design team is not only involved in the initial phase of providing system information to the PSA team, allowing in this way the identification of the high risk scenarios, but it is also receiving feedback from the PSA team that suggests design modification aimed at reaching risk-related goals.*

During the first iteration of this process, the design modifications proposed by the PSA team allowed reducing the initial estimate of Core Damage Frequency (CDF) due to internal events from 2E-6/ry to 2E-8/ry. Since the IRIS design is still in a development phase, a number of assumptions have to be confirmed when the design is finalized.

Among key assumptions are the success criteria for both the accident sequences analyzed and the systems involved in the mitigation strategies. The PSA team developed the initial accident sequence event trees according to the information from the preliminary analysis and feasibility studies. A recent coupling between the RELAP and GOTHIC codes made possible the actual simulation of all LOCA sequences identified in the first draft of the Event Trees. Working in close coordination, the PSA and the safety analysis teams developed a matrix case of sequences not only with the purpose of testing the assumed success criteria, but also with the perspective of identifying alternative sequences developed mainly by relaxing the extremely conservative assumptions previously made.

The results of these simulations, bounded themselves with conservative assumptions on the Core Damage definition, suggested two new versions of the LOCA Event Tree with two possible configurations of the Automatic Depressurization System. The new CDF has been evaluated for both configurations and the design team has been provided with an additional and risk-related perspective that will help choosing the design alternative to be implemented.

I. INTRODUCTION

IRIS (International Reactor Innovative and Secure) is a modular 1000 MWt (~ 335 MWe) light water reactor with an integral configuration, which has been under development since October 1999 by an international team led by Westinghouse Electric Co. and currently comprising 21 organizations from ten countries. The IRIS design characteristics, as well as its safety features have been reported in several prior publications (see e.g. Refs. 1-2) and are therefore not repeated here.

IRIS is presently undergoing pre-application licensing [3] with the USNRC with the goal of attaining final design approval by 2010 on the road to deployment of the first IRIS module by 2015 or even slightly earlier.

IRIS has been primarily focused on achieving a design with innovative safety characteristics. The first line of defense in IRIS (a Level 0 of the defense-in-depth philosophy) is to eliminate event initiators that could potentially lead to core damage. In IRIS, this concept is implemented through the "Safety-by-Design"^{TM} approach, which has been already presented in several papers (see for example refs 1,2 and 4). To fully achieve the potential of improved safety performance inherent in the IRIS Safety-by-Design^{TM}, a Risk-informed approach to the design phase has been adopted as one of the key features to increase the overall safety of the IRIS reactor.

In the IRIS approach, the usage of Probabilistic Safety Assessment (PSA) is required from the very beginning of the design phase and also implies a very close interaction between the PSA team and the design and safety analysis teams.

In this paper, the application to the design of probabilistic analysis results related to internal events will be presented.

II. RISK-INFORMED APPROACH

The Risk-Informed approach to the design phase of the reactor can be depicted as an evolution of the PSA procedure that is currently adopted in the nuclear industry. In order to better understand how this approach impacted the initial design phase of the reactor and what makes it different from a classical PSA approach, we can refer to Fig.1. On the upper part we can see how a classical PSA procedure can be schematized, with the design and safety analysis teams providing information to the PSA team necessary to analyze and identify the most relevant risk scenarios. Since for licensing purpose a PSA procedure is usually initiated during the late design phase, the initial set of information provided by the design team can be updated and revised according to the development of the project. The flow of information, however, remains substantially one-way, with the PSA results used only to provide insights on the safety of the project, usually mostly for verification and with limited impact on the plant design.

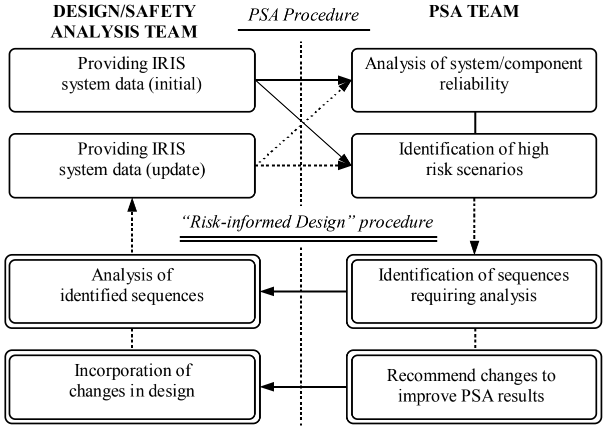
DESIGN/SAFETY ANALYSIS TEAM
PSA Procedure
PSA TEAM
Providing IRIS system data (initial)
Analysis of system/component reliability
Providing IRIS system data (update)
Identification of high risk scenarios
"Risk-informed Design" procedure
Analysis of identified sequences
Identification of sequences requiring analysis
Incorporation of changes in design
Recommend changes to improve PSA results

Fig. 1. PSA and Risk-informed design procedures

A Risk-informed design approach couples the PSA procedure described above with a structured feedback from the PSA to the design side. PSA results now have a direct influence on the plant design, rather then simply following its development.

A Risk-informed design approach is therefore not only a matter of initiating the PSA at the very beginning of the design phase; it also and overall implies an iterative, structured and close interaction between the PSA team and the design and safety analysis team. As a result of this interaction, two somehow different points of view on the design (probabilistic and deterministic) are coupled and harmonized, with a significant benefit in terms of overall plant safety.

The main "drawback" of such an approach is that probabilistic studies need to be initiated at a very early stage of the design, when several required design information may only be partially or qualitatively available. This requires a more flexible approach to probabilistic analysis than used in the past, and will be described in this paper.

II.A. Initial model development and first iteration

The IRIS Preliminary PSA has been initiated on February 2003, as a joint effort by four members of the IRIS team (Westinghouse, Polytechnic of Milan, Tokyo Institute of Technology and Mexico National Institute for Nuclear Studies).

This initial PSA model for IRIS has been developed while the design was still evolving from a conceptual to a preliminary design stage. Where the status of the design was not sufficient to provide all the PSA modeling inputs, the design team relied on engineering considerations to provide reasonable assumptions as to what the final design would be in terms of performance requirements. For example, qualitative analysis of accident events was used to complete the safety analyses for areas where quantitative analyses were not yet available. In other cases, conclusions on the IRIS design and response were based on the declared similarity with other advanced Westinghouse PWR, such as the AP600/AP1000 design (mainly for support and secondary systems).

This approach resulted in a relevant number of assumptions. A fundamental part of this initial PSA stage was therefore the documentation and monitoring of all these assumptions for further analysis and confirmation of their actual applicability. The IRIS PSA Assumptions Database is also the primary qualitative tool used to store and document all the foreseen source of uncertainties: to each assumption that is included in the database is associated a degree of uncertainty that is connected with the kind of design or analysis information that are still required. The database, as well as the uncertainty degree of each assumption, is continuously updated as the development of the design makes further IRIS-specific information available.

A detailed description of the development of the PSA model has been already presented in a previous paper [5] and it is therefore only briefly summarized here.

The starting point for the construction of a PSA model is the identification of the Initiating Events (IE): for IRIS this step was originated by a review of the classical lists of PWR initiating events in EPRI NP-2230 [6], NUREG/CR-3862 [7] and NUREG/CR-5750 [8]. These initiating events were carefully reviewed to identify those that are still applicable to the IRIS design. The Safety-by-Design^{TM} approach used by IRIS has in fact led to the elimination of several classical event initiators such as large LOCAs, RCP seals LOCAs, Control Rod Ejection, all eliminated by the integral IRIS configuration.

The SGTR are expected to be reduced in frequency as well, due to the enhanced features of the once-trough, helical coil SGs. The evaluation of the SGTR Initiating Event Frequency (IEF) is the most representative example of the approach used to quantitatively address the uncertainty due to the preliminary design. The engineering considerations originated by the review of the SG failure modes still applicable to IRIS and of the impact of the enhanced IRIS SG features on the IEF, led to the development of various possible alternatives of the model used to establish the overall failure frequency. Such alternatives were then combined by the means of a decision tree through a set of degrees of belief associated to each of the possible alternative.

For each initiator, the plant response to the challenge was evaluated with respect to the key safety functions (see [9]). The response of the plant to various combinations of successes and failures of the systems supporting each safety function was evaluated to determine whether the postulated combination of successes and failures will result in core damage or if the plant will achieve a safe, stable state. This was an interactive process between the PSA analysts, the safety analysts and the designers. Since most PSA accident sequences involve multiple failure in the safety (and in any pertinent non-safety) systems that go beyond the safety analyses (Chapter 15 analyses) that are used as the starting point for determining the general thermal hydraulic (TH) behavior for each event, the sequences for each initiator were reviewed with the safety analysts and designers to determine if the sequences were consistent with their expectations of the plant response.

The probabilities of failure of the systems involved in the analyzed sequences were evaluated by the means of a classical fault tree analysis. Standard modeling techniques were used to develop the fault tree models for the IRIS safety systems. The models include pumps, valves, heat exchangers, motive and control power, and actuation signals. Modeled failure modes include demand failures, run failures, standby failures and common cause failures, as appropriate. The preliminary design of the main IRIS safety systems was essentially complete so development of the models was straightforward. However, there was limited design information for the support systems. For the fluid support systems such as cooling water, the PSA analysts developed simplified system design diagrams based on system descriptions in the Safety Analysis Report and the system P&IDs from the equivalent AP1000 systems. These "PSA designs" were reviewed by the system designers to ensure that they were consistent with the designers' understanding of the intended design and operation of the system. A power system model was developed based on the AP1000 power system design; the PSA analysts also assigned loads allocation, equipment control and motive power to the various buses based on elementary train separation considerations. The "PSA designs" were then used to complete the needed fault tree models.

The IRIS PSA used generic data for quantification of the models. The primary data sources used were the EPRI PSA Key Assumptions and Ground Rules (KAG) document [10], and the database used for the AP1000 PSA [11]. As needed, this information was supplemented by data from the NUCLARR database [12]. The Multiple Greek Letter (MGL) approach was used for modeling common cause failure with the appropriate factors again extracted from the AP1000 PSA or the KAG.

The primary feedback to the design team that was provided by the first analysis of the system by PSA techniques was focused on both systems performance and sequences analysis.

The first contribution of the PSA to the plant design and safety analyses was that it provided an improved understanding of the plant response to various initiators. For example, the unavailability of the Automatic

Depressurization System (ADS) following a small break LOCA in the lower part of the vessel (i.e. due to Direct Vessel Injection – DVI – line break) was identified by the PSA team as one of the dominant high risk scenario. The design and safety analysis teams responded by further investigating the potentiality of the Emergency Heat Removal System (EHRS) in order to evaluate its capability to provide adequate depressurization during the cooling phase. The preliminary safety analysis did not conceived mixed sequence (where only some train of the EHRS was working and with a partial ADS availability) since this was not required by the design basis scenarios (typically based on the single-failure assumption) usually considered during this phase of the design process. After these considerations the firstly assumed success criteria were modified.

The lack of details related to system performance induced the adoption of the concept of "bellwether sequences" for sanity checks for sequence analysis. A "bellwether sequence" is a core damage sequence that reflects a key simplifying assumption. These sequences typically involve only an initiator and one system failure and the associated core damage frequency can be estimated by a preliminary hand calculation. The hand calculation of the frequency provides a quick check on the potential impact of the simplifying assumption on overall core damage frequency. If the impact is felt to be large enough to be of concern, the assumption and associated sequence are examined in more detail to determine if additional mitigation paths could be credited, additional best estimate TH analyses would be needed to revise the assumption, or the assumption is appropriate. For the last condition, designers could then determine if a design change is warranted or the risk impact is acceptable at that point of the design phase.

One example of this procedure involves the Emergency Boration System (EBS). The initial design assumption was that actuation of the EBS was required for reactivity control following a LOCA and that failure of the system would lead to core damage due to a return to power. The approximated core damage frequency contribution for the sequences involving failure of the EBS was of the order of 4E-8/ry, which was felt to be too large to be acceptable for this particular scenario. A re-evaluation of the EBS and sequences related assumptions indicated two possible solutions. First, the design team determined that the chemical volume control system (CVCS) makeup pumps provided sufficient flow of borated water to maintain reactivity control and should be modeled as an alternate success path for boron injection. Second, the safety analysts indicated that the assumption was very conservative and that it would probably be possible to demonstrate that EBS injection was not needed based on the expected post-LOCA temperatures and as long as all of the control rods were inserted (no stuck rod). Additional best-estimate transient analyses were still needed to confirm this, but based on the safety analyst input EBS injection was not modeled as a required response for LOCA transient initiators.

The second major contribution of the initial PSA to the IRIS design was relative to the systematic addressing and solving of Common Cause Failures (CCF) groups. To make an example, CCF was affecting the availability of the EHRS that was initially designed with redundant but completely identical discharge lines. Also in this case, early safety analyses did not consider CCF in their scope, as they were traditionally based on the single-failure criterion (that can be briefly summarized as follows: safety analyses are performed assuming all non-safety grade systems to be unavailable, and all safety systems to be available, with however a single most severe failure considered). As an example, CCF event related to the failure of all the identical air operated EHRS discharge valves was identified by the PSA team as a potentially, even if unlikely, high risk event. The design and safety analysis teams responded by introducing a further diversification in the type of valves to be used in the discharge section of the EHRS (see Fig.2). Such a diversification, when coupled with the already envisioned redundancy, led to an increased reliability of the system and therefore a reduction to the plant CDF. The PSA team provided therefore a broader risk-based perspective that appears extremely useful in the initial phase of the design when the main systems design has not yet been completed with a detailed design of the undergoing support systems.

II.B. PSA model and design parallel evolution

Following the completion of the first PSA iteration, that resulted in the overall plant internal event CDF lowered from the initial value of 2E-6/ry (which is already well below the current regulation and close to the value projected for advanced LWR designs) to 2E-8/ry, the

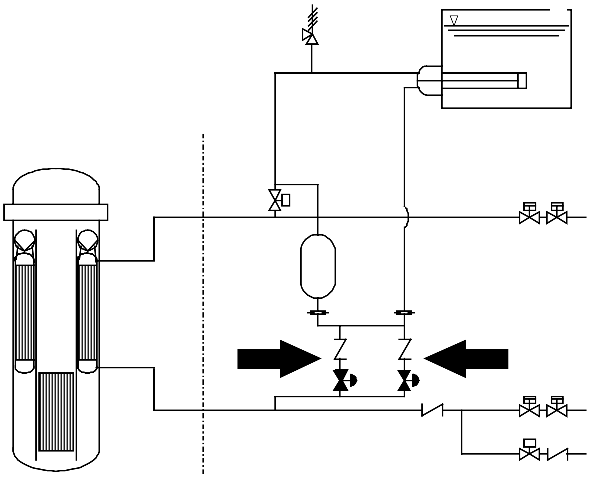

Fig. 2. Layout of a single train of the EHRS. The redundant but identical discharge lines are highlighted

TABLE I. Current results

Initiator	*IEF*	*CDF*	*%*
Reactor vessel rupture	1.00E-08	1.00E-08	51.03
Loss of Offsite Power	1.18E-01	3.48E-09	17.78
Loss of Support Systems	1.95E-02	2.43E-09	12.42
ATWS	[1]	1.83E-09	9.34
Transients with main feedwater	8.54E-01	8.37E-10	4.27
Loss of Condenser	8.50E-02	4.78E-10	2.44
Isolable Secondary Line Break (SLB)	5.96E-04	1.80E-10	0.92
Not isolable SLB	3.72E-04	1.10E-10	0.56
SGTR	1.88E-04	5.48E-11	0.28
Interfacing System LOCA	5.00E-11	5.00E-11	0.26
DVI Line break	1.32E-04	4.78E-11	0.24
Loss of main feedwater	6.05E-02	4.76E-11	0.24
Upper LOCA	8.85E-04	4.12E-11	0.21
Power excursion	4.50E-03	2.10E-12	0.01
RCS leakage	6.65E-03	3.99E-13	<0.01
ADS line break	6.49E-06	2.55E-14	<0.01
Total		1.96E-08	

Notes:

1. Due to the conservative assumptions adopted during the modeling of the ATWS scenarios, Initiating Event Frequency for ATWS events has been evaluated by adding the IEF of all the initiators leading to an high pressure accident scenario.

II.B. PSA model and design parallel evolution

focus of the PSA team moved to the continuous refinement of the large assumptions database that was generated during the performance of the initial PSA effort.

While this has been a continuous process that is still ongoing, it can be divided in phases, each phase focused on one of the major assumptions categories. Table I summarizes the results in terms of CDF for the at-power internal IEs at the end of the first PSA application. The internal events CDF history is summarized in Fig.3. The iterative relationship between the PSA and the design team is clearly indicated in the spikes in the CDF that can be seen after the dramatic reduction of the initial values due to the already described first iteration. CDF spikes are usually due to the PSA model being updated and refined; such refinements can bring light to some new issues to be discussed and addressed with the design team. The most visible spike in Fig.3 is for example due to the Human Reliability Analysis (HRA) that, along with the implementation of several design modifications identified during the first PSA iteration, has been one of the main areas of work during the second phase of the PSA development.

IRIS has been designed in order to be the least dependent possible from human intervention, due to the Safety-by-Design^{TM} and the highly automated and passive safety systems. As a result, the main contribution to CDF due to human errors is concentrated in those sequences involving the complete failure of the EHRS and the initiation of the Once Through Core Cooling (OTCC) strategy. The human errors considered in the preliminary stage are mainly post initiator human errors regarding the emergency response phase. The task analysis for the operator actions needed in emergency response was developed in close cooperation with the design team since many of the elements regarding the information available for the control room and the related commands are not yet part of the available schemes. Therefore the assumptions have been stored in the database mentioned above and connected to the human actions assessed for the PSA. All these assumptions will constitute a precious source of information during the Control Room Design phase, as well as for the development of the Emergency Response Guidelines. A critical information for the assessment of Human Errors Probability was the time window available for each critical action. An example is the action: “manual activation of the Start-up Feed Water (SFW) system” in transient scenario. Analyzing this task the TH simulations enabled to clarify that in those scenario the actual sequence foresees the automatic actuation of the EHRS before any operator action can actually take place; the automatic sequence in fact occurs in such a brief time interval that no human action can actually be performed before it. Therefore the operator intervention was considered only as a recovery in case of failure of the automatic activation sequence for the EHRS: “the manual activation of the SFW pumps will follow the failure of the EHRS automatic activation and its first manual backup”. These findings are actually in line with the “hand off” design philosophy as well. The results of the preliminary HRA analysis highlighted that the contribution of human error to the CDF is quite limited.. As mentioned above, one of the most critical operator actions is the one related to the manual activation of the ADS during the OTCC procedure. This enabled the PSA team to focus its attention, together with the design team, on a more thorough analysis of the actual sequence and the definition of a procedure improved with the consideration of human reliability principles. As a result the importance of the human error contribution diminished since the first OTCC strategy changed

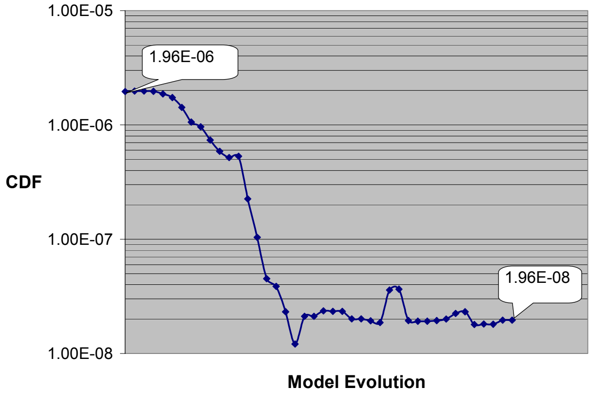

Fig. 3. Internal Event CDF history for the IRIS

following a more detailed description of the system response.

A second major improvement of the IRIS PSA model obtained during the second phase was the inclusion in the model of an accident category not fully analyzed during the first iteration: Anticipated Transients Without scram. This accident category was initially assumed to be a minor contributor to the overall IRIS CDF. The very low level of CDF obtained for IRIS made the verification of such assumption a mandatory step during the second PSA phase.

The ATWS evaluation involved again joint efforts between the PSA team and the IRIS core/plant designers and transient analysts to determine ATWS consequences as a function of physics parameters and availability of plant features (e.g., number of safety valves, alternative shutdown systems, etc.). The most severe ATWS transients are characterized by a large power mismatche between the reactor coolant system (RCS) and the main steam system (MSS). Major factors that mitigate these AWTS transients are 1) primary system coolant volume capability of absorbing the power mismatch, 2) pressurizer safety valve capacity to limit pressure increases and 3) a negative moderator reactivity coefficient to shut down core power generation as the reactor coolant temperature increases/density decreases. The IRIS design inherently includes much larger RCS and pressurizer volumes, relative to core power, compared to current PWRs. Therefore, the IRIS RCS pressure and temperature would rise more slowly during an ATWS transient, providing more time for moderator feedback to reduce core power. The IRIS PSA team then worked with the IRIS design team and transient analysts to perform sensitivity studies on the pressurizer safety valve area and reactor moderator coefficient to obtain parameter sets that resulted in acceptable ATWS consequences (i.e., peak RCS pressure <22 Mpa). From these sensitivity studies, the team members identified an improved design set of pressurizer safety valves that resulted in an ATWS contribution to CDF of 1.7E-9/ry. This is less than 10% of the current overall CDF.

This iterative process of assumption review and verification and the resulting design details that need to be more deeply investigated keep the PSA model and the actual design in close correlation.

III. LOCA ASSUMPTIONS REVIEW

What we are outlining here is clearly a recursive procedure that must be updated every time a new piece of information about the design or the analysis upon with the assumptions are based become available.

Even if the procedure of assumption reviewing has been already described with some examples in the previous section, it is worthwhile to pay particular attention to a third iteration of the methodology that we are here outlining, since the main focus of this so far last iteration was on LOCAs. Several early assumptions relative to the response to SBLOCA were made in the initial development of the IRIS PSA model; as a results of these assumptions, often based only upon preliminary safety analyses, a classical high-risk accident category was reduced to impact for just around 1% on the overall CDF.

The third iteration of this risk-informed approach has therefore been a critical one since the success criteria for LOCA have been finally tested with a more complete set of TH simulations. These simulations were made possible by a recent coupling between GOTHIC and RELAP codes.

III.A. GOTHIC and RELAP coupling

The IRIS novel LOCA safety approach poses some new issues for computational and analysis methods since the IRIS integral reactor coolant system and containment are strongly coupled, and the system response is based on this interaction. A preliminary assessment has led to the conclusion that in order to develop an appropriate evaluation model for the IRIS SBLOCA, the containment/vessel coupling had to be correctly captured [13]. For this reason a coupled RELAP/GOTHIC model was developed by the University of Zagreb. A simple direct coupling of the modified version of RELAP5 mod3.3 [14] used for IRIS analyses and GOTHIC [15] was used with connections at the points of hydraulic contact (the break, ADS, and gravity makeup flow paths). The connections are comprised of a time dependent volume component on the RELAP5 side (representing the containment backpressure) and a flow boundary condition (to provide the mass and energy release term) on GOTHIC side. The existing detailed RELAP5 model of the reactor coolant system and of the engineered safety features is used for these analyses, together with a simplified GOTHIC model of the containment. The RELAP/GOTHIC coupling developed for IRIS analyses has been described in [16].

The RELAP5 model of the Reactor Coolant System has been described in previous papers [17] and is shown in Fig. 4. The same RELAP5 plant model used for Non-LOCA analysis has been used, with the only differences related to the contact points between the reactor coolant system and the containment model, and some modeling improvements to better represents plant systems important for LOCA analyses (e.g. the ADS and DVI). The containment model used for these analyses has also been discussed in previous papers [19] and is shown in Fig. 5.

The IRIS Small Break LOCA evaluation model was updated on the basis of the results of the IRIS SBLOCA Phenomena Identification and Ranking Table (PIRT) [18].

With this relatively mature evaluation model, the SBLOCA event tree was evaluated jointly by the design

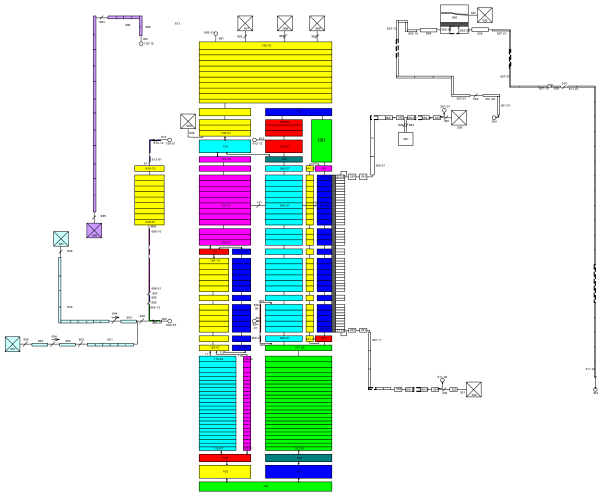

Fig. 4. Reactor Coolant System Model for RELAP5 Used in IRIS Safety Analyses

and PSA team, with special attention to the key assumptions made in evaluating the performance of the system. The key subsystems whose success or failure had a critical impact on the PSA results were identified. These systems can be grouped in different categories as follows: decay heat removal (Passive Containment Cooling System - PCCS - and EHRS) and coolant injection to the RCS (Normal Residual Heat Removal System - NRHRS - and Chemical & Volume Control System - CVCS, Emergency Boration System - EBS, Long-term Gravity Makeup System - LGMS - and indirectly the ADS, which equalizing pressure between the RCS and the containment allows for gravity injection,). In general, since both functions are required for a successful mitigation, at least one system for each category is required.

Based on these evaluations, a matrix of relevant cases to be analyzed with different combinations of assumptions relative to the 7 critical items identified above was prepared, with the added complexity that the EHRS is not an "available" or "not-available" system, but rather different numbers of available trains (1 to 4) need to be addressed. A detailed discussion of the test matrix goes beyond the purpose of this paper, and it will suffice to say that the evaluation matrix was developed considering not only deterministic, but also probabilistic (in terms of dominant sequences) considerations.

III.B. PSA Model modifications

The Standards for Probabilistic Risk Assessment provided by ASME [19] suggest the definition of Core Damage as an uncovery and heatup of the reactor core to the point at which prolonged oxidation and severe fuel damage is anticipated and involving enough of the core to cause a significant release. In the current preliminary IRIS PSA, a more conservative definition of CD has been used,

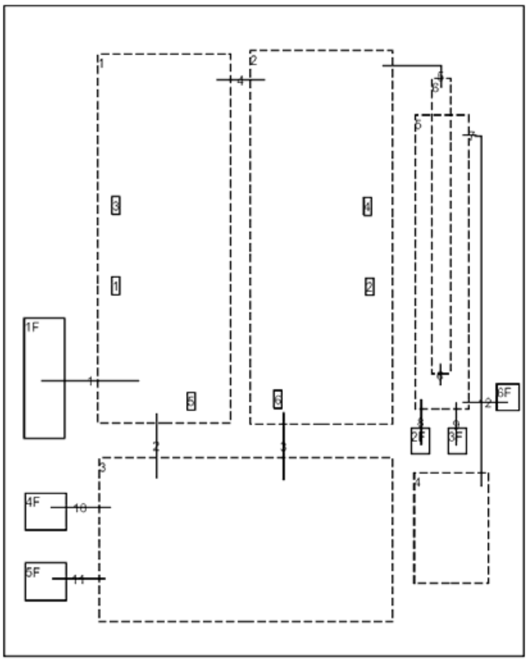

Fig. 5. Simplified Containment Model for GOTHIC 3.4 Used in IRIS Safety Analyses

i.e. a simple prolonged core uncovery has been considered as a synonym for core damage. Such a definition has been used in order to bound the uncertainties initially expected due to the preliminary design phase of the reactor and especially considering the lack of a complete set of TH analysis.

According to the definition of core damage used and relying on the capability provided by the described coupling between GOTHIC and RELAP, the results of the test matrix cases have been used not only to provide confirmation of the assumed success criteria but also to explore additional success paths initially not credited due to the high degree of uncertainties.

One of the most relevant assumptions that has been confirmed during this simulation campaign (and that was introduced in section IIA) refers to the actual demonstration that the boration function provided by the Emergency Boration System is not required in order to maintain the subcriticality of the reactor for all the LOCA cases analyzed, once the reactivity control is assured by the success of the control rods. The EBS has therefore been retained for further analysis, apart from ATWS cases, only because it can be credited for a small extra inventory that could be decisive in some near success sequences.

Because of the conservative assumptions adopted for the definition of the success criteria as well as for the core damage definition itself, some assumptions, usually involving the number of EHRS trains required for the mitigation strategy, have been relaxed and the LOCA

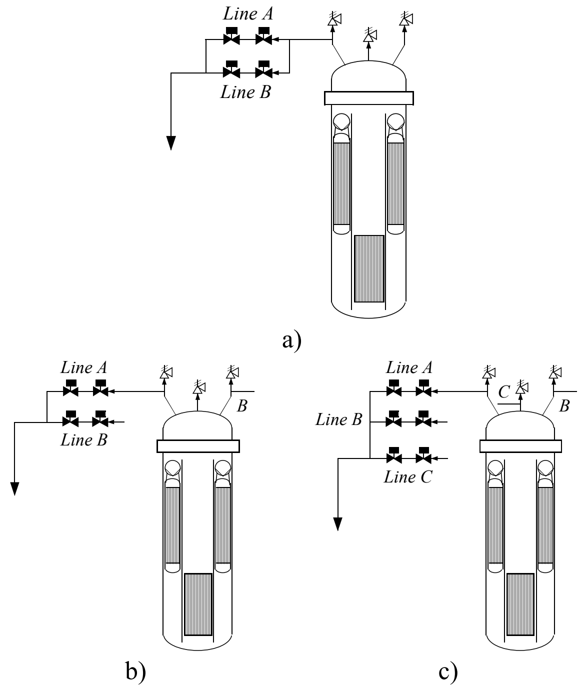

Fig. 6. a) Original ADS design. b) 2 lines ADS design. c) 3 lines ADS design

Event Trees have been consequentially simplified.

In order to provide confirmation of the success criteria, the design team realized the need for tuning some details of the design. The Automatic Depressurization System is an explicative example since, in order to grant an adequate depressurization in case of multiple failure of EHRS, slightly enhanced performances of the ADS will be required, namely an increased available flow; thus the original ADS design has been modified.

The original ADS consisted of two lines that were originally connected through a common header to the same safety relief valve line; while the enhanced ADS version implies that each ADS line is now connected to a different safety relief valve line (see Fig.6 a,b). This new configuration enables to have more than one line fully opened, which in turns grants an increased depressurization ratio that can lead some sequences to success. It must be noticed that this is not a violation of the single failure principle since the deterministic safety analyses will still be based on this principle, and it is only for beyond design basis sequences involving multiple failures in the safety systems that the improved design becomes important.

In addition to this modification, the PSA team has been requested to provide the risk impact of two alternative ADS designs (see Fig. 6 b,c): as already explained, the first option imply that the ADS is provided with two enlarged lines that are both requested for the mitigation of some advanced sequences; while in the second option the ADS is provided with a third additional line, connected with the third available safety relief valve line. At first it was thought that the second option should increase the reliability of the entire plant, however the PSA analysis shows that the addition of a third ADS line, even if results in an increase of the ADS reliability, is going to grant success only for some not primary sequences while, on the other hand, the additional ADS line slightly increases the Initiating Event Frequency (IEF) for the spurious ADS actuation event, as well as for the LOCA from the upper part of the vessel. Thus the risk informed decision process provides in this case additional and useful information for the finalization of a design that can be optimized under a broader set of perspectives.

IV. CONCLUSIONS

A risk-informed approach to the design phase of a nuclear power plant is something more than the simple initiation of the PSA at the very beginning of the design. The close interaction and the feedback that the design team can obtain from the PSA team are of paramount importance to better integrate the two sometimes not easily compatible viewpoints. Several examples have been provided in this paper to illustrate how the PSA can be applied at an early design stage and developed in parallel to a design that it contributes to define.

IRIS has taken full benefits from such an approach in achieving an internal events CDF as low as 2E-8/ry. The risk-informed approach has helped the design team to focus the attention on some risk-significant scenarios, but has also led to some significant design modifications and is also providing risk-related information to be used in the decision making process regarding the finalization of the design. IRIS is therefore using the risk-informed approach to the design phase in the most complete fashion.

Such a good result for the IRIS CDF has brought to an additional challenge to the PSA analysts since its value is now close to the order of magnitude of some kind of events that used to be considered as scarcely relevant. This is also true for some major assumptions usually considered conservatives in the framework of internal events and that in the case of IRIS resulted in generating relevant contributors to the CDF, such as the reactor vessel rupture initiating event frequency evaluation.

As described, the Level-1 IRIS PSA is being used in all possible extent in order to provide useful insights and guidance to the design of the IRIS NSSS and even to the BOP. The application of the herein described methodology is in principle applicable also to external events analysis as well as to the Level 2 of the PSA, i.e. containment performance.

It must be considered that, when dealing for example with external events, the amount of assumptions to be considered is even more extended if compared with the internal-event analyses, with the additional complication of a general lack of detailed information in the literature. Nevertheless, a first application of the herein presented methodology to the external event analysis for IRIS has been initiated by the Lithuanian Energy Institute [20].

The extension of this methodology to the Level 2 PSA has so far been anticipated with the development of a preliminary LERF model [21] that has been used in order to understand the major information that will be needed from the design team in order to apply the risk-informed approach to the design finalization of the IRIS containment.

ACKNOWLEDGMENTS

Cooperation can be considered a trade mark of the IRIS project, as it can be easily deducted by the composition of the international team developing the project. This is even truer for the IRIS PSA. The authors wish to acknowledge the hard work of the other members of the IRIS PSA team, Yuko Mizuno and Yuji Kumagai at TIT, Jorge Viais and Gonzalo Mendoza at ININ, Marco Ghisu and Maddalena Barra at POLIMI and Robertas Alzbutas at LEI, which made this paper possible. We also want to acknowledge the support and assistance of Lawrence Conway of the IRIS design team.

REFERENCES

1. M. D. Carelli, IRIS: A global approach to nuclear power renaissance, *Nuclear News*, 46, No. 10 (Sep. 2003), pp. 32-42.
2. M. D. Carelli et. al., The Design and Safety Features of the IRIS Reactor, *Nucl. Eng. Design*, 230, (2004), pp. 151-167.
3. M. D. Carelli, C. L. Kling, S. E. Ritterbush, IRIS Pre-Application Licensing, *Proc. GLOBAL 2003*, November 16-20, 2003, New Orleans, LA, USA.
4. Carelli, M.D., Petrovic, B., Ferroni, P., ”IRIS Safetyby-Design™ and Its Implication to Lessen Emergency Planning Requirements,” Proc. 13th International Conference on Nuclear Engineering (ICONE-13), Beijing, China, May 16-20, 2005,
5. D. J. Finnicum, A. Maioli, Y. Mizuno, J. Viais, G. Mendoza, G. Alonso, IRIS Preliminary PRA Analysis, *Proc. GLOBAL 2003*, November 16-20, 2003, New Orleans, LA, USA.
6. EPRI NP-2230, ATWS: A Reappraisal, Part 3: Frequency of Anticipated Transients, The Electric Power Research Institute, January 1982
7. NUREG/CR-3862, Development of Transient Initiating Event Frequencies for Use in Probabilistic Risk Assessments, Idaho National Engineering and Environment Laboratory, May, 1985
8. NUREG/CR-5750, Rates of Initiating Events at U.S. Nuclear Power Plants: 1987 – 1995, Idaho National Engineering and Environment Laboratory, February, 1999.
9. FINNICUM, D. J., et. al; “Nuclear Power Plant Safety Functions”; NUCLEAR SAFETY, Vol. 22, No. 2, March-April, 1981.
10. Advanced Light Water Reactor Requirements Document, Volume III, Appendix A to Chapter 1, PRA Key Assumptions and Ground Rules, Revision 5 and 6, December, 1993.
11. APP-GW-GL-022, Rev. 03, "AP1000 Probabilistic Risk Assessment, " Westinghouse Electric Company, LLC, May 2003.
12. NUREG/CR-4639, "Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR)," Idaho National Engineering and Environment Laboratory, October 1990.
13. Oriani, L., L. E. Conway, D. Grgi, T. Bajs, M. E. Ricotti, A. Barroso, "*Overview of Computational Challenges in the Development of Evaluation Models for IRIS*", American Nuclear Society Topical Meeting in Mathematics & Computations (M&C), April 6-10, 2003, Gatlinburg, TN, USA
14. Information Systems Laboratories; "RELAP5/MOD3.3 Code Manual, Vol. 1-8; NUREG/CR-5335, Rockville, Maryland, USA, 2001
15. Electric Power Research Institute, GOTHIC "Containment Analysis Package, Version 3.4e, Vol 1-4", EPRI TR-103053-V1, Richland, Washington, USA, 1993.
16. Grgic, D., L. Oriani, L.E. Conway, "*Development Status and Preliminary Validation of a Coupled RELAP/GOTHIC Code for IRIS Small Break LOCA Analysis,*" 5th International Conference on Nuclear Option in Countries with Small and Medium Electricity Grids, May 16-20, 2004, Dubrovnik, Croatia.
17. Grgic, D., T. Bajs, L. Oriani, "*Development of RELAP5 Nodalization for IRIS Non-LOCA Transient Analyses*", American Nuclear Society Topical Meeting in Mathematics & Computations (M&C), April 6-10, 2003, Gatlinburg, TN, USA
18. T. K. Larson, F. J. Moody, G. E. Wilson; W. L. Brown, C. Frepoli, J. Hartz, B. G. Woods; L. Oriani, "*IRIS Small Break LOCA Phenomena Identification and Ranking Table,*" International Congress on Advances in Nuclear Power Plants, ICAPP 2005, May 15-19 2005, Seoul, Korea
19. RA-S-2002, “Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications”, American Society of Mechanical Engineers, April 5, 2002
20. R. Alzbutas, J. Augutis, A. Maioli, D. J. Finnicum, M.D. Carelli, B. Petrovic, C.L. Kling, Y. Kumagai, External Events Analysis and Probabilistic Risk Assessment Application for IRIS Plant Design, *Proc. ICONE 13*, May 16-20, 2005, Beijing, China.

21. A. Maioli, D.J. Finnicum, Y. Kumagai, IRIS Simplified LERF Model, *Proc. ANES 2004 Conference*, October 3-6, 2004, Miami, FL, USA.