Lessons learned form IRSN review of Flamanville 3 Level 1 PSA

G. Georgescu and F. Corenwinder,

Institute for Radiological Protection and Nuclear Safety, BP 17, 92262 Fontenay-aux-Roses, France, gabriel.georgescu@irsn.fr

Abstract

In the frame of the construction and licensing of Flamanville 3 NPP the PSA plays an important role for the EPR Project assessment. The PSA was used for early design verification of EPR Reactor, several design improvement being defined based on these PSA insights and following the discussions with the French and German safety authorities. IRSN, as the French Safety Authority (ASN) technical support organization, performs the review of the PSA developed by the plant operator (EDF). The paper presents the main issues regarding the using of "design PSA", identified by IRSN following the review of the internal events Level 1 PSA transmitted by EDF in the frame of the anticipated instruction of the application for operating license of the Flamanville 3 reactor.

Keywords: New reactors, EPR, PSA, licensing

1. Introduction

In the frame of the construction and licensing of Flamanville 3 NPP (FLA3) the PSA plays an important role for the EPR Project assessment. In fact, the PSA was developed and used for early design verification from the beginning of the design by the EPR reactor designer (AREVA). Several design improvement being defined based on these PSA insights and following the discussions with the French and German safety authorities.

Today, there are many uses of PSA in the frame of FLA3 new reactor project. PSA has a role for the verification of the plant safety level as a complement of the deterministic safety demonstration. It has to be noted that the "Technical Guidelines" for EPR [2] requires the using of the probabilistic approach in order to show the achievement of a significant reduction of the global core melt frequency comparing with the existing NPPs. Many other PSA applications, related to the development of a new reactor, are equally performed. For example, the PSA is used to support the demonstration of "practical elimination" of the large early releases, equally requested by the "Technical Guidelines". The PSA is also involved in the verification of the completeness of the deterministic multiple failures situation (Risk Reduction Categories) features.

2. IRSN assessment of FA3 PSA

In the frame of the FLA3 application for operation license, EDF will provide a rather complete set of Level 1 PSAs:

- Level 1, internal events PSAs related to the reactor core and spent fuel pool,
- internal hazards Level 1 PSAs (fire, explosions, flooding),
- assessment of some external hazards (earthquake, high wind),
- heavy load drop assessment.

Up to now, IRSN fully analyzed the Level 1, internal events PSAs for reactor and for spent fuel pool. The objective of this analysis is to support the ASN position regarding the acceptability of FLA3 PSA

methods at this stage of the project, having in mind that a complementary IRSN analysis will be also necessary in the frame of the technical instruction of the operating license application. It is mainly requested to state on the fulfillment of the French standard requirements (PSA fundamental safety rule [1]) and on the compatibility of the EDF PSA methods with the PSA state-of-the-art methods. ASN also requested to IRSN to analyze the PSA preliminary results (core damage frequency and contributions, systems reliability, etc.).

Following this ASN request, IRSN performed a detailed analysis of the EDF PSA documents. The analysis was also supported by the using of the PSA developed independently by IRSN for EPR reactor. The IRSN report was provided to ASN which released its position statement at the beginning of 2011.

It has to be noted that the decision making process involving the new reactors design PSA is a complex task. The lack of plant-specific operating experience data and operations procedures at the design stage may lead to PSA results that do not reflect the future as-built, as-operated plant. The detailed plant procedures needed to assess human performance may not be available. IRSN attempted to identify the most critical aspects as well as the ways to improve the representativeness of the design PSA in order to allow the decision making-process especially in the frame of licensing activities.

The most important issues, especially when they are specific for a design PSA, are presented in the following paragraphs.

3. Plant available information

3.1 Design information

The design PSA is inevitably based on partial design information, the PSA model including assumptions regarding the future plant design. As a consequence the final design of the plant systems may be different from the design which was considered in the PSA modeling. This is the case mainly for I&C systems, electrical distribution systems (as for example the power supply sources for individual components), equipments type and manufacturer (mainly needed to estimate the possibility for CCF - Common Cause Failures) etc.

This aspect can have an important impact on the PSA results. On the one hand, IRSN believes that the design PSA tractability has to be enhanced. Also, for any new design evolution or clarification, the impact on PSA has to be assessed, and the PSA should then be updated earlier or later depending on this estimated impact.

On the other hand, IRSN estimates that the role of PSA in the designing of new reactors should be better identified and documented.

3.2 Operating profile

In the frame of a design PSA, the operating profile (POS - Plant Operating States and durations) is always provisional, since the operating experience is not available. Then, in the PSA the POS are considered based on assumptions regarding the refuelling, plant availability, etc.

IRSN believes that this aspect is not a major issue for a design PSA and the approach proposed by the utility complied with the PSA safety rule. However, as soon as the operating experience becomes available the PSA should be updated accordingly.

3.3 Accidental procedures

Generally the detailed accident procedures are not available while developing the design PSA. As a consequence the human reliability analysis is performed based on assumptions and simplifications regarding the future accident procedures.

The impact of this aspect on the PSA results can be important. Nevertheless, IRSN believes that using a conservative/screening approach (like, for example, Swain screening model) is an acceptable approach for a design PSA. However, this approach has to be completed by a qualitative verification of the existence of the given operator strategies in the preliminary version of accident procedures or accident guidelines.

3.4 Preventive maintenance

The modelling of the preventive maintenance is an important aspect, mainly if it is foreseen to perform such activities during the power operation. IRSN considers that the modelling of only components unavailabilities based on provisional maintenance durations, is not enough to conclude on the safety impact of the future preventive maintenance strategies and also on the safety importance of the specific design features which are provided for maintenance (like for example the possibility to interconnect redundant electrical trains).

IRSN believes that the design PSA should analyze, beside components unavailabilities, the maintenance specific configurations. Moreover, the possibility for new initiating events occurring during maintenance activities (for example, loss of two electrical divisions) or induced by maintenance activities (mainly by human errors) has to be deeply investigated.

3.5 Technical Specifications

The design PSA considers generic and simplified Technical Specifications (TechSpecs). For IRSN this aspect should not have a strong impact on the PSA results. Moreover, the PSA may be generally used later to define the future TechSpecs. IRSN believes that the PSA can be updated when the detailed TechSpecs will be available and after an initial operating experience, without a strong impact on the licensing processes.

4. Data

4.1 Reliability data

The reliability data employed in a design PSA are taken generally from the existing plants operating experience and from other available sources (NUREG, international data bases). The method to choose the most appropriate data consists on the evaluation of similarity of the new reactor components with the existing available data. For IRSN this approach is acceptable in principle. However, the similarity analysis between new reactor components and the operating experience which was used to quantify the existing reliability data is not an easy work. This analysis has to consider, beside the component type and safety classification, also the operating conditions, the surveillance requirements (test intervals), the component population used to quantify the data, the recent operating experience trends, etc. The justification of choosing a given data has to be fully traceable and documented. Moreover a comparison between several sources may be desirable, especially if the difference between the data is important.

For new or revolutionary components, reliability studies are preformed or expert opinion is used. IRSN believes that sensitivity studies may be useful in order to reduce the uncertainties related to this aspect.

4.2 Common Cause Failure (CCF)

For a design PSA, the CCF parameters are generally based on existing operating experience completed by international available sources (NUREG). Generic values may be also used if it is considered that the available information is not pertinent for the selected CCF group. Since, there are in general no big discrepancies between CCF parameter values from different sources, IRSN considers that this approach is acceptable. However, it has to be documented and traceable.

Regarding the definition of CCF families, the design PSA uses assumptions in order to identify the groups of redundant components for which CCF contributions should be taken into account. IRSN considers that the approach is, in principle, acceptable. However, for IRSN the assumption of fully diversification of some redundant components (when it is assumed that the CCF is not possible) has to be justified by a through analysis. This analysis has to cover all the CCF causes and mechanisms (type, manufacturer, environment, maintenance, etc.) as well as the perpetual character of these conditions over the plant lifetime. This aspect refers mainly to components of a similar type, but produced by different manufacturers (like Diesels, batteries, etc.), and for which some parts may be provided by the same supplier or for which the same maintenance, maintenance materiel or spare parts may apply. Sensitivity studies may be useful in order to identify the potential CCF families for which detailed studies may be necessary.

4.3 Loss of ultimate heat sink

The loss of main ultimate heat sink is generally a dominant contribution initiating event. Consequently the approach used to quantify the frequency and the scope of this initiating event is very important for a design PSA.

The frequency of loss of main ultimate heat sink may be quantified by using the experience (nuclear and non-nuclear). IRSN believes that it is necessary to verify the applicability of available experience to the given site and given design and to assess the related uncertainties.

Another approach is to develop reliability studies based on the intake structure and of the pumping station design. This approach is considered acceptable by IRSN. However the approach has to cover not only the design basis situations (daily or yearly pumping station detritus arrival and cleaning) but also the beyond design basis situations having a longer return period but with potentially much higher intensity.

In the case that a second, diversified ultimate heat sink is foreseen for the new reactor design, the independency between the main heat sink and the secondary heat sink has to be toughly justified. The justification applies to all aspects which may threaten the independency or the diversity of the two heat sinks: sea/river related hazards and other external hazards, design of intake structures, design of pumping station systems, maintenance, internal hazards (flooding, fire and explosion).

5. Support systems modelling

5.1 I&C

I&C is modeled in a design PSA by using fault trees. These fault trees are generally developed at the level of macro-components, since the I&C systems are too complex to be possible to develop fault trees up to individual components. The macro-components can be defined based on a logical

decomposition (as for example the COMPACT model employed by EDF) or based on systems decomposition (more classical model used, for example, by IRSN).

IRSN considers that both approaches are acceptable and can be used in a design PSA. However, justifications have to be provided regarding the validity of the model. These justifications may include:

- the performance of a Failure Mode and Effects Analysis (FMEA) for the different sub-systems of I&C systems (platforms, networks, computers, human machine interfaces, etc.),
- the performance of a dependency analysis between the I&C sub-systems and components (dependency matrix),
- the analysis of the impact of the failure of ventilation and cooling systems on the I&C.

Even the I&C model in the PSA may be simplified at the design stage, IRSN believes that some important aspects have to be carefully modeled: the I&C support systems, the miscalibration human errors and the CCF between redundant I&C systems. Moreover, the potential "loss of I&C systems" as well as "spurious I&C" initiating events have to be deeply analyzed in all reactor states and considered in the PSA model if necessary.

5.2 Ventilation systems

The utility proposed by simplification, the ventilation systems are not modeled in the design PSA. The IRSN position is that this simplification is not acceptable, mainly because it may lead to neglect important interdependencies between safety systems and support systems.

IRSN considers that the design PSA should model the ventilation systems, even in a simplified and conservative way. The initiating events induced by the loss of ventilation should be also investigated and modeled in the PSA if necessary. Moreover, for IRSN, the design PSA should be capable to be used to assess the potential cliff-edge effects related to the variation of the outside temperature (to demonstrate that the risk increase is not important when the outside temperature is higher or lower than threshold values).

6. Human factor assessment

6.1 Pre-accident human factor

In the design PSA the preaccidental human errors are quantified based on incomplete or generic information regarding the components position indicators or alarms, surveillance requirements, maintenance, administrative measures, etc. On the one hand, IRSN considers that the impact of this aspect is not very high on the PSA results. However a mostly conservative model (considering for example the recovery possibilities only when the design can be confirmed) may be preferable.

On the other hand, IRSN considers that the most important issue regarding the pre-accidental human factor is the correct identification of the possible dependencies between different human actions performed on redundant trains, including the calibration of sensors. IRSN believes that the pre-accidental human factor dependencies have to be carefully analyzed and documented.

6.2 Post-accident human factor

As already mentioned, IRSN believes that using a conservative/screening approach (like, for example, Swain screening model) is an acceptable approach for a design PSA. However, IRSN considers that one of the most important issues regarding the post-accidental human factor is the correct identification and modeling of the possible dependencies between redundant human actions.

IRSN believes that the dependencies between the post-accidental human errors have to be carefully analyzed and treated in the design PSA preferably by using conservative rules. The modeling can be further upgraded when the detailed design and accident procedures will be available.

6.3 Crisis team modeling

In the design PSA, the crisis team may be considered in a simplified way. For example all the decision human errors are considered as being negligible if the crisis team is in place. IRSN considers that this modeling of the crisis team, even if it is not in principle wrong, can lead to introduction of some optimism in the PSA model: undeveloped accident sequences, omission of some execution errors and omission of some equipment failures.

IRSN believes that the crisis team modeling should be enhanced by taking into account the crisis team decision error probability (mainly based on available information for the crisis team during the accident), the execution error probability (mainly for the irreversible errors) as well as the reliability of the mitigations.

7. Initiating events

7.1 Initiating events common to reactor and spent fuel pool

In general the reactor and the spent fuel pool are considered in the design PSAs as being independent. As a consequence in the PSA developed for the reactor, respectively for the spent fuel pool, it is considered that all mitigations means and human resources are fully available.

IRSN considers that this assumption may be optimistic, since the mitigation and support systems may be shared between the reactor and the spent fuel pool and that the operating crew has to handle simultaneously both installations in accidental situation.

IRSN believes that these aspects should be carefully treated, especially for the initiators with a long reparation time (like the loss of last heat sink or loss of outside power supply) as well as for the hazards (like for example the internal fire, especially if the spent fuel make-up system is also the firefighting system).

7.2 Reactor PSA initiating events

The initiating events list is generally developed in a design PSA by compiling existing plants PSA initiating events lists and international practices. This list is then completed by using deductive methods, in order to identify specific initiators for the given new reactor type.

For IRSN this approach is acceptable. Nevertheless the approach itself does not guarantee the completeness of the list, especially if the initial boundary conditions definition is not complete or not appropriated for the objectives of the design PSA (as for example the loss of ventilation initiators or loss of I&C initiators may be excluded). IRSN considers that these aspects should be carefully treated.

7.3 Spent fuel pool PSA Initiators quantification

The method used to quantify the initiating events may differ between the reactor PSA and spent fuel pool PSA. In fact for some initiators, the available time to recover the situation before the total loss of cooling of the spent fuel pool can be long. This kind of initiating event can be then interpreted as a pre-initiating event for the loss of cooling initiating event. The quantification of the frequency of the

total loss of cooling initiating event considers then the recovery probability. This quantification can be performed separately from the PSA model by using other methods (Markov chains for example).

For IRSN this approach is acceptable. Nevertheless some precautions should be taken in order to ensure the coherence with the PSA developed for the reactor (as some of the initiating events affect both installations simultaneously) and to ensure the correct modeling of the dependencies (mainly when the pre-initiating event is a loss of support system: electrical busbar or cooling system).

8. Accident sequences

8.1 Functional analysis

In order to develop the accident sequences in the design PSA, functional analyses are generally developed. These analyses are supported by appropriate thermohydraulic studies.

IRSN considers that this approach is the best approach to follow for the development of the event trees, because it allows to define precisely the accident sequences and in the same time to reduce the modeling uncertainties. Nevertheless, the transposition of the functional analysis in the PSA model should be carefully performed, mainly to ensure that all the dependencies identified by these analyses are taken into account in the PSA model.

On the other hand, IRSN mentions that the PSA model cannot be limited to the development level of the functional analyses, since the PSA generates, in fact, many other failures combinations and dependencies which cannot be all explicitly treated in the functional analysis. This aspect should be taken into account while developing the accident sequences and while defining the systems success criteria.

8.2 Recovery factors modeling

The design PSA may consider recovery actions and corrective factors (to take into account for example the fact that some initiators recovery time is much shorter that the modeled systems mission time: ex: short loss of outside power over diesels mission time). The recovery factors consider the repair time and different time for the loss of system using a specific formula. This approach is acceptable in principle, but the effective modeling of the corrective factors may be difficult, especially when a “point” value is used instead of a fault tree. In fact, the using of a point value may lead to fail to identify important dependencies and finally to a non-conservative PSA model.

8.3 Sumps clogging

In the design of new reactors, special devices or systems may be provided to avoid the sumps clogging and to ensure the long term operation of the safety injection system and of the containment cooling system.

IRSN believes that the role of these devices or systems should be modeled in the PSA. This aspect is important for the using of the PSA for design verification, but also for the application of the PSA for TechSpecs definition and surveillance requirements definition.

8.4 By-pass LOCA

The primary circuit interface system breaks which can lead to containment bypass accidents are normally modeled in any design PSA. The core damage frequency related to this kind of accident should be very low (for EPR reactor, this type of situation is included in the category of accidents which have to be “practically eliminated”). One of the most important aspects related to bypass

accident analysis is the assessment of the impact of the primary inventory flow outside containment on the safety and support systems. In general, the most vulnerable systems are the electrical power supply and the I&C systems.

IRSN believes that the modeling of the bypass LOCA in the design PSA should be supported by a detailed analysis of the possible primary flow environmental effects on the electrical and I&C systems located in the buildings which are directly or indirectly impacted.

8.5 Spent fuel pool PSA repairing modeling

In the frame of a spent fuel pool PSA the recovery of cooling systems is one of the most important mitigation. The quantification of the recovery probabilities depends mainly on the systems design and systems installation, as well as on the equipment reliability data (the time to repair). At the design stage, as some of this information may be missing, the PSA considers assumptions to quantify the recovery probabilities for different accident sequences.

IRSN believes that the assumptions used to quantify the recovery actions should be thoroughly documented and traceable. Additionally, the coherence should be ensured between the reliability data used for the reactor PSA and the spent fuel pool PSA.

8.6 Spent fuel pool passive devices

In order to avoid the accidental loss of inventory of the spent fuel pool by siphoning, generally, anti-siphoning devices are considered in all designs. Even if the failure probability of these devices should be very low, IRSN believes that this contribution should be modeled explicitly in the PSA. This aspect is important for the using of the PSA for design verification, but also for the application of the PSA for TechSpecs definition and surveillance requirements definition.

8.7 Definition of the spent fuel pool accident sequence unacceptable consequences

In the frame of a spent fuel pool PSA the definition of the unacceptable consequences is different from the reactor PSA. For example the boiling of the spent fuel pool inventory can be considered as unacceptable consequence if the spent fuel pool building is not a full containment.

IRSN believes that the definition of the spent fuel pool PSA accident sequence unacceptable consequences should be coherent with the global safety objectives of the plant and with the global context of the safety assessment.

9. Conclusions

For the EPR Reactor, the PSA was developed from the beginning of the design by the reactor designer (AREVA). This PSA was used for early design verification, several design improvement being defined based on these PSA insights and following the discussions with the French and German safety authorities.

The decision making process involving the new reactors design PSA is a complex task. The lack of plant-specific operating experience data and operations procedures at the design stage may lead to PSA results that do not reflect the future as-built, as-operated plant. The detailed plant procedures needed to assess human performance may not be available.

IRSN attempted to identify the most critical aspects as well as the ways to improve the representativeness of the design PSA in order to allow the decision making-process especially in the frame of licensing activities.

10. References

6. ASN, “Règle Fondamentale de Sûreté - Développement et utilisation des études probabilistes de sûreté" (2002).
7. Letter ASN, “Options de sûreté du projet de réacteur EPR” (2004).

IRSN
INSTITUT DE RADIOPROTECTION ET DE SÛRETÉ NUCLÉAIRE
Faire avancer la sûreté nucléaire

Lessons learned form IRSN review of Flamanville 3 Level 1 PSA

G. Georgescu and F. Corenwinder
IRSN France

OECD/NEA Workshop on PSA for New and Advanced Reactors, Paris, 20 - 24 June 2011

Introduction

- For the EPR Reactor, the PSA was developed from the beginning of the design by the reactor designer (AREVA)
  - This PSA was used for early design verification, several design improvement being defined (SBO Diesels, Heat Sink diversification…)
- Today there are many uses of PSA in the frame of Flamanville 3 (FA3) new reactor project:
  - Safety level and design verification, classification, demonstration of "practical elimination" of the Large Releases, multiple failures categories (RRC) definition, TechSpec development, preventive maintenance)

Introduction

- IRSN performed the review of the EDF FA3 internal events Level 1 PSA for reactor and spent fuel pool
- Several important issues regarding the using of "design PSA" in the context of new reactors development and licensing were identified
- The ASN letter was published in January 2011

Introduction

- It has to be noted that the decision making process involving the new reactors design PSA is a complex task:
  - The lack of design information, plant-specific operating experience data and detailed plant procedures may lead to PSA results that do not reflect the future as-built, as-operated plant
- IRSN identified the most critical aspects as well as the solutions to improve the representativeness of the design PSA for the decision making-process (licensing activities)
- Here only the most important issues are presented

Design information

- The design PSA is inevitably based on partial design information
- The final design of the plant systems may be different from the considered design
  - I&C systems, electrical distribution systems, equipments type and manufacturer (CCF)...
- IRSN Conclusion:
  - The design PSA tractability should be enhanced
  - For any new design evolutions or clarifications, the impact on PSA has to be assessed
  - The role of PSA in the designing of new reactor should be better identified and documented

Accidental Procedures

- The detailed accident procedures are not available
  - The human reliability analysis is performed based on assumptions and simplifications regarding the future accident procedures.
- IRSN Conclusion:
  - Using a conservative/screening approach (like, for example, Swain screening model) is an acceptable approach
  - The qualitative verification of the existence of the given operator strategies in the preliminary version of accident procedures or accident guidelines should be performed

Initiating events

- The initiating events list is generally developed in a design PSA by compiling existing plants PSA initiating events lists and international practices
- This list is then completed by using deductive methods, in order to identify specific initiators for the given new reactor type
- IRSN Conclusion
  - The approach itself does not guarantee the completeness of the list, especially if the initial boundary conditions definition is not complete or not appropriated for the objectives of the design PSA (as for example the loss of ventilation initiators or loss of I&C initiators may be excluded)
    - These aspects should be considered when defining the initiating events list

Initiating events common to reactor and spent fuel pool

- The reactor and the spent fuel pool are considered in the design PSAs as being independent
  - all mitigations means and human resources are fully available for each one of them
- IRSN Conclusion
  - This assumption may be optimistic
    - mitigation and support systems may be shared
    - the operating crew has to handle simultaneously both installations in accidental situation
  - These aspects should be carefully treated, especially for the initiators with a long reparation time (loss of ultimate heat sink or loss of outside power supply) as well as for the hazards (internal fire, especially if the spent fuel make-up system is in the same time the firefighting system)

Preventive maintenance

- Important aspect, mainly if it is foreseen to perform such activities during the power operation
- IRSN Conclusion
  - The modeling of only components unavailabilities based on provisional maintenance durations, is not enough to conclude on the safety impact
  - The maintenance specific configurations and the possibility for new initiating events occurring during maintenance activities or induced by maintenance activities (mainly by human errors) should be analyzed
    - for example, multiple loss of electrical divisions

Reliability data

- Generally from the existing plants operating experience and from other available sources (NUREG, international data bases)
- IRSN conclusion
  - Beside the component type and safety classification, the operating conditions, the surveillance requirements (test intervals), the component population used to quantify the data, the recent operating experience trends, should be also considered
    - The justification of choosing a given data has to be fully traceable and documented
  - Comparison between several sources may be desirable, especially if the difference between the data is important
    - Sensitivity studies may be useful

CCF modeling

- The CCF parameters are generally based on existing operating experience completed by international available sources and generic values
- The definition of CCF families is generally based on assumptions regarding the design
- IRSN conclusion
  - The assumption of fully diversification of some redundant components has to be justified by a through analysis
    - All CCF causes and mechanisms (type, manufacturer, environment, maintenance, etc.)
      - Ex: components of a similar type, but produced by different manufacturers: some parts may be provided by the same supplier, same maintenance…
    - The perpetual character of these conditions over the plant lifetime

Loss of ultimate heat sink

- The loss of ultimate heat sink initiating event is in general a dominant contribution
  - The approach used to quantify the frequency as well as the scope of this initiating event is very important for a design PSA
  - The frequency of loss of ultimate heat sink may be quantified by using the experience (nuclear and non-nuclear)
- IRSN Conclusion
  - It is necessary to verify the applicability of available experience and to assess the related uncertainties
  - The beyond design basis situations (longer return period but higher intensity) should be also included here
  - The independency between the main ultimate heat sink and the secondary heat sink has to be toughly justified

I&C modeling

- The I&C fault trees are generally developed at the level of macro-components
  - Logical decomposition (EDF COMPACT model) or systems decomposition (IRSN)

- IRSN Conclusion
  - Justifications have to be provided regarding the validity of the model
    - Failure Mode and Effects Analysis (FMEA) for the different sub-systems of I&C systems (platforms, networks, computers, human machine interfaces…)
    - Dependency analysis between the I&C sub-systems and components
    - Impact of the failure of ventilation and cooling systems on the I&C
  - The I&C support systems, the miscalibration human errors and the CCF between redundant I&C systems should be modeled
  - The potential "loss of I&C systems" as well as "spurious I&C" initiating events have to be analyzed in all reactor states

Human factor assessment

- The pre-accidental HRA is based on incomplete or generic information

- The detailed accident procedures are not available for post-accidental HRA

- The crisis team may be considered in a simplified way

- IRSN Conclusion
  - The most important issue regarding the human factor is the correct identification and quantification of the dependencies:
    - pre-accidental HRA: actions performed on redundant trains
    - post-accidental HRA: redundant mitigations
    - conservative assumptions or qualified information should be used
  - The crisis team modeling should take into account the decision error, the execution error (mainly for the irreversible errors), as well as the reliability of the systems

Sumps clogging

- In the design of new reactors, special devices or systems may be provided to avoid the sumps clogging and to ensure the long term operation of the safety injection system and of the containment cooling system
- IRSN Conclusion
  - The role of these devices or systems should be modeled in the PSA
    - This aspect is important for the using of the PSA for design verification, but also for the application of the PSA for TechSpecs definition and surveillance requirements definition

By-pass LOCA

- The By-pass LOCA are normally modeled in any design PSA
- The core damage frequency related to this kind of accident should be very low
  - For EPR reactor, this type of situation is included in the category of accidents which have to be "practically eliminated"
- One of the most important aspects is the assessment of the impact of the primary inventory flow outside containment on the safety and support systems (electrical power, I&C, etc.)
- IRSN Conclusion
  - The modeling of the bypass LOCA in the design PSA should be supported by a detailed analysis of the possible primary flow environmental effects on the electrical and I&C systems located in the buildings which are directly or indirectly impacted

Spent fuel pool PSA initiators quantification

- The available time to recover the situation before the total loss of cooling of the spent fuel pool can be long
  - The quantification of the frequency of the total loss of cooling considers then the recovery probability. This quantification can be performed separately from the PSA model by using other methods (Markov chains for example)

- IRSN Conclusion
  - The coherence with the reactor PSA (as some of the initiating events affect both installations simultaneously) should be ensured
  - The modeling of the dependencies should be treated carefully (mainly when the initiating event is a loss of support system: electrical busbar or cooling system)

Spent fuel pool PSA repairing modeling

- The recovery of cooling systems is one of the most important mitigation

- The quantification of the recovery probabilities depends mainly on the systems design and systems installation, as well as on the equipment reliability data (the time to repair)

- At the design stage, as some of this information may be missing, the PSA considers assumptions to quantify the recovery probabilities for different accident sequences

- IRSN Conclusion:
  - The assumptions used to quantify the recovery actions should be thoroughly documented and traceable
  - The coherence should be ensured between the reliability data (time to repair) used for the reactor PSA and the spent fuel pool PSA

Spent fuel pool PSA unacceptable consequences

- The definition of the unacceptable consequences is different from the reactor PSA
  - For example the boiling of the spent fuel pool inventory can be considered as unacceptable consequence if the spent fuel pool building is not a full containment
- IRSN Conclusion:
  - The definition of the spent fuel pool PSA accident sequence unacceptable consequences should be coherent with the global safety objectives of the plant and with the global context of the safety assessment

CONCLUSIONS

- In the context of the anticipated instruction of the application for operation license of FLA3 reactor, the French Safety Authority (ASN) asked IRSN to analyze the FLA3 EPR
- The decision making process involving the design PSA is a complex task
  - The design PSA specific issues need to be identified
  - The impact of incomplete information needs to be assessed
  - Iterative approaches should be applied