Risk Informed Approach in Nuclear Power Plants: The Brazilian Experience

Anna Letícia B. de Sousa, Renato A. Fonseca, Pedro Luiz da C. Saldanha
Comissão Nacional de Energia Nuclear, CGRC/DRS, Brazil

Paulo Fernando F. Frutuoso e Melo
Programa de Engenharia Nuclear, COPPE, Universidade Federal do Rio de Janeiro, Brazil

1. INTRODUCTION

The fundamental licensing approach for nuclear power plants has been based on a deterministic viewpoint, where a set of rules and requirements has been defined with the objective of ensuring a high level of safety.

However, a probabilistic safety analysis has been carried out for most nuclear power plants in the world over the last twenty five years. General guidelines addressing these probabilistic safety assessments (PSA) have been followed both by guidance of the International Atomic Energy Agency (IAEA) and also of the United States Nuclear Regulatory Commission (NRC), so that these analyses are of sufficiently high quality.

As a consequence of this evolution a new approach emerges, applying an integrated decision-making process that combines the insights from the deterministic approach and the probabilistic analysis with further requirements, where applicable (legal, regulatory, cost-benefit, etc.) in making decisions. This approach is being increasingly adopted by regulatory bodies in making decisions about safety issues (including plant licensing) at nuclear facilities and in organizing their activities, optimizing the use of resources and reducing the unnecessary burden on the licensees without compromising safety.

The use of risk-informed by a regulatory body sets an integrated process in making decisions about safety issues at nuclear facilities.

The risk-informed decision making approach aims to integrate in a systematic manner deterministic and probabilistic safety considerations to obtain a balanced decision. In particular, there is explicit consideration of both the chances of events and their potential consequences, together with such factors as good engineering practice and sound managerial arrangements. The basic components of risk, chances of occurrence and consequence, are based on sound knowledge or data from experience, or derived from a formal, structured analysis such as a PSA.

This paper presents the risk-informed approach experience in nuclear power plants operation in Brazil and discusses the lack of specific standards to be issued by the regulatory body in accordance with international guidelines. It identifies the need for specific standards and the use of a reactor oversight program with the risk-informed process to complement specific information of each plant in order to cover aspects of applications for temporary or permanent modifications carried out by utilities.

2. RISK- INFORMED GENERAL APPROACH

The modern approach is to apply an integrated decision-making process that combines the insights from the deterministic approach and the probabilistic analysis with further requirements, where applicable (legal, regulatory, cost-benefit, etc.) in making decisions. This approach is being increasingly applied by regulatory bodies in making decisions about safety issues (including plant licensing) at nuclear facilities and in organizing their activities so that their resources are more efficiently used and there is a reduction in the unnecessary burden on the licensees without compromising safety [1].

For many years, risk considerations have been used in making safety decisions and determining regulatory requirements. The increased maturity of probabilistic safety assessments (PSA) gives a more rigorous way for providing much of the detailed risk information for use in the safety decision making and regulatory processes. The integrated decision making process provides an efficient way for ensuring that safety decisions are taken on a sound basis.

The use of risk information by a regulatory body as part of an integrated decision making process addresses the way in which risk information is being used as part of an integrated process in making decisions about safety issues at nuclear plants – commonly referred to as risk-informed decision making, and how risk information is being used by regulatory bodies as an input to the activities they carry out – sometimes referred to as risk-informed regulation.

The risk-informed approach aims to integrate in a systematic manner quantitative and qualitative, deterministic and probabilistic safety considerations to obtain a balanced decision. In particular, there is explicit consideration of both the chances of events and their potential consequences together with such factors as good engineering practice and sound managerial arrangements. The basic components of risk, chances of occurrence and consequences, are based on sound knowledge or data from experience, or derived from a formal, structured analysis such as a PSA. Figure 1 outlines the general risk-informed approach [1]. It can be seen from this figure that the traditional approach for making safety decisions concerning nuclear plants is the one shown on the left. Requirements are set on plant process variables (as temperatures, for instance). The plant design can face the so called design basis accidents (like the so called double-ended break loss of coolant accident – LOCA). In this sense, mitigating systems are designed. Details on this subject should be pursued in [2]. On the other hand, the right branch in Figure 1 outlines the probabilistic approach. Here, credible accidents are considered, where their consideration takes into account event frequencies.

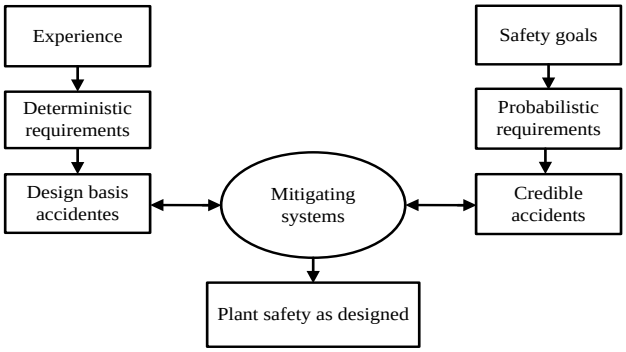

Figure 1- The risk-informed general approach [3].

PSA is a methodology that can be applied to provide a structured analysis process to evaluate the frequency and consequences of accidents scenarios in nuclear power plants. NRC first applied PSA in the Reactor Safety Study [4]. An important initiative [5] was the issuance of Generic Letter GL-88-20 [5], which originated the program known as IPE (Individual Plant Examination). This was because the Reactor Safety Study did not consider each plant individually in the risk assessment.

Since that time, NRC has been using risk assessment and directing the issuance of decisions on complex items associated with or related to safety such as: (a) total loss of power (station blackout); (b) anticipated transients without reactor shutdown (ATWS); (c) pressurized thermal shock events (PTS); and (e) Maintenance Rule.

NRC issued the Probabilistic Safety Assessment Policy Statement [6], which incorporated risk assessment as a tool into the regulatory process. It consists of elements that have originated the Risk-informed Decision Making (RIDM) and the Performance Based Regulation (PD).

On January 2001, Paragraph 69 of the 10 CFR 50 (the U.S. Code of Federal Regulations, reachable at nrc.gov), which regulates RIDM, was issued.

We present in the next two subsections discussions concerning the regulatory documentation on RIDM, mainly the one issued by the U. S. Nuclear Regulatory Commission and also some documents from the International Atomic Energy Agency (the referenced documents can be easily found in their respective Internet sites, nrc.gov and iaea.org) and in the second one a discussion on published papers on the subject. This literature review is by no means exhaustive: it is just an outline of recent work on the subject. The approach of the RIDM model developed by the NRC is shown in Figure 2

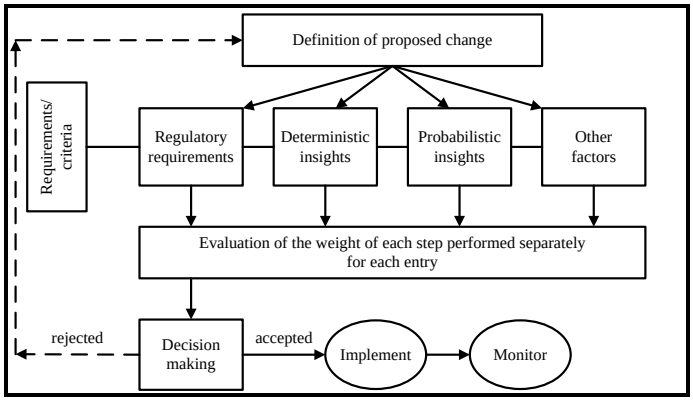

Figure 2- RIDM model developed by the NRC

2.1 Regulatory documentation concerning RIDM

The following PSA-based RIDM regulatory guides have been issued: (*a*) changes in the bases of the specific plant licensing, RG-1.174 [7] ; (*b*) assessment of changes and implementation of technical specifications, RG-1.177 [8]; (*c*) in-service inspections in pipes, RG-1.175 [9] and RG-1.178 [10]; (*d*) an approach to determine the technical quality of APS results for RIDM, RG 1.200 [11] (*e*) fire protection, RG 1.205 [12]. Many of the current regulations, based on deterministic requirements, cannot be quickly replaced.

Regulatory Guide 1.174 [7] describes the approach accepted by NRC to assess the nature and impact of licensing basis conditions (LBC) by considering engineering aspects and application of risk insights.

Regulatory Guide 1.200 [11] describes the approach accepted by NRC to determine that PSA quality, in part or in whole, is sufficient to assure its results so that they can be used in regulatory decision making.

The International Atomic Energy Agency (IAEA) has, over the years, sponsored and promoted activities and issued technical documents related to RIDM. Among the latest highlights are Refs. [13] and [14]

Ref. [13] was prepared with the participation and contributions of experts from Belgium, the Czech Republic, Finland, the Netherlands, Sweden, Switzerland and the United States. In-service inspection is an integral part of defense in depth programs for nuclear power plants, to ensure safe and reliable operation. Traditional in-service inspection programs have been developed using deterministic approaches. However, as probabilistic approaches are being developed, risk insights are being used to optimize in-service inspection programs by focusing in-service inspection resources on the most risk significant locations.

Ref. [14] is intended to promote a common understanding among the international nuclear community (designers, suppliers, constructors, licensees, support organizations and regulators) of how the

concept of risk can be used in making safety decisions relating to nuclear installations. The integration of operating experience, deterministic considerations, probabilistic considerations, consideration of uncertainties and other factors serves to help ensure coherent and balanced decisions.

According to NASA [15], risk management (RM) is an integral aspect of virtually every challenging human endeavor, but well-defined RM processes have only recently begun to be developed and implemented as an integral part of systems engineering at NASA, given the complex concepts that RM encapsulates and the many forms it can take. However, few will disagree that effective risk management is critical to program and project success. Recent NASA RM processes have been based on Continuous Risk Management (CRM), which stresses the management of risk during implementation. In December 2008, NASA introduced Risk-Informed Decision Making (RIDM) as a complementary process to CRM that is concerned with analysis of important and/or direction-setting decisions. Earlier, RM was considered equivalent to CRM; now, RM is defined as comprising both CRM and RIDM.

2.2 General concepts

'Risk insights' is used to refer to the results and decisions that are made after probabilistic safety assessments are performed. It is necessary to distinguish three approaches or treatments in the decision making process: (*a*) Risk Based (RB); (*b*) Risk Informed (RI); and (*c*) Performance Based (PB), NRC [16, 10], EC [17].

The risk-based approach to decision making is the one where only the numerical results of a probabilistic safety assessment are taken into consideration. This causes a strong dependence on the results of risk assessment, due to uncertainties associated with PSA (such as completeness and use of data). NRC does not endorse the risk-based approach, however does not invalidate the use of probabilistic calculations to demonstrate compliance with some criteria.

The risk-informed approach to the process of regulatory decision making represents a philosophy according to which the outcomes and decisions arising from a risk assessment are considered along with other factors to establish requirements that will best target on issues related to the design and operation that impact safety and health of the public. The RI approach extends and improves the deterministic treatment because it: *a*) allows explicit consideration of a wide range of changes for safety; *b*) provides rationale for prioritizing these changes based on risk, operational experience and/or engineering judgment; *c*) facilitates the consideration of a broad range of resources to support these changes; *d*) identifies and describes uncertainty sources in the analysis; and *e*) leads to proper decision making, providing a mechanism to test the results sensitivity to a set of assumptions.

Where appropriate, a regulatory approach with information on risk can be used to reduce unnecessary conservatism in deterministic treatment, or can be used to identify areas with insufficient conservatism in deterministic analysis and provide the foundation and additional requirements or regulatory actions.

The RI approach lies between the risk-based approach and the purely deterministic treatment. The details of the regulatory approach to be used will determine where the RI-based decision will fall in this spectrum. The concept of defense in depth remains the principle of regulatory practice. The findings and decisions arising from risk assessment can make the elements of defense in depth clearer due to the PSA quantitative approach.

Rules can be either prescriptive or performance based (PB). Prescriptive requirements specify particular aspects, activities or program elements to be included in the project or process, as a means of achieving the desired goal. A performance-based requirement depends on results (measured or calculated, i.e., performance data) to be found. It provides the licensee greater flexibility to achieve these results.

RIDM philosophy is the reconciliation of the results of PSA insights with the traditional deterministic analysis. Often, PSA results conflict with deterministic insights (defense in depth and safety margin, for example). It is noteworthy that the use of RIDM by the licensee is voluntary.

As a result of policy implementation methodologies for the use of risk information, NRC expected the regulatory process would improve in three aspects: *a*) by PSA incorporation into regulatory decisions; *b*) preserving agency's resources; and *c*) reducing unnecessary effort on licensing.

RIDM follows principles for implementation and evaluation of changes proposed by the licensee, and to evaluate these changes a series of assumptions is adopted by the regulator. It is expected that the proposed changes meet the set of principles described below. PSA techniques can be used to ensure and show compliance with these principles, which are displayed in Table 1.

Table 1- Principles to be followed by RIDM

Principle	Description
1	Change meets the existing law and is explicitly related to the requested exception or rule change.
2	The proposed change is consistent with the philosophy of defense in depth.
3	The proposed change has sufficient margins.
4	When the proposed change results in an increased frequency of core damage and/or risk, this increase should be small and consistent with the regulations laid down in Ref. [7].
5	The impact of the proposed change should be monitored using performance measures.

The evaluation of proposals and licensing acceptance guides adopt these same five principles, according to the eight assumptions detailed next.

- Assumption # 1: All safety impact of the proposed change has been assessed in an integrated manner as part of the general approach of risk management, in which the licensee uses risk analysis to improve operational and engineering decisions in the identification of actions to reduce risks, and not to justify the elimination of licensing requirements perceived as undesirable. For those cases where risk increases are proposed, the benefits should be consistent with the increased risk proposal. The approach used to identify changes in requirements must also be used to identify areas where the requirements should be increased or reduced.
- Assumption # 2: The content (scope and quality) of engineering analysis (deterministic and probabilistic) performed to conduct and justify the proposed changes have been appropriate to the change nature and scope and should be based on the plant as built and operated, reflecting its operational experience.
- Assumption # 3: The plant-specific PSA that supports all licensee proposals has been subject to quality control and an independent evaluation or certification.
- Assumption # 4: Consideration of appropriate uncertainties has been provided and decision interpretations supplied, using a monitoring, feedback and corrective actions program to consider significant uncertainties.
- Assumption # 5: The use of core damage frequency (CDF) and large early release frequency (LERF) as a basis for PSA acceptance is an acceptable approach to Principle 4.
- Assumption # 6: Variations in estimates of CDF and LERF arising from proposed changes to licensing bases will be limited to small increments. Cumulative effects of these changes will be monitored and considered in decision making.
- Assumption # 7**:** Proposal acceptance will be evaluated by licensee in order to ensure that all principles are met.
- Assumption # 8: Data, methods and evaluation criteria used to support regulatory decisions should be documented and available for public scrutiny.

Regulatory Guide 1.174 [7] describes the approach accepted by NRC to assess the nature and impact of licensing basis conditions (LBC) by considering engineering aspects and application of risk insights. Regulatory Guide 1.200 [11] describes the approach accepted by NRC to determine that PSA

quality, in part or in whole is sufficient to assure its results so that they can be used in regulatory decision making. Figure 3 illustrate the role of the above discussed regulatory guides.

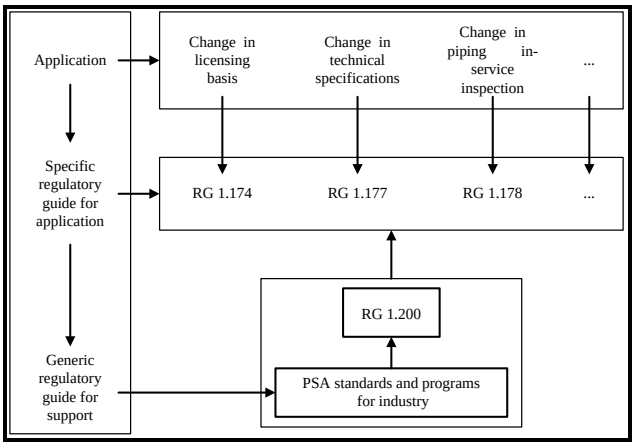

Figure 3 – Role of NRC regulatory guides in RIDM

2.3 PSA currents applications

As aforementioned about NRC, the worldwide nuclear power industry has been using risk assessment and directing the issuance of decisions on complex items associated with or related to safety. Some regulatory bodies as NRC (USA) [18] and STUK (Finland) [19] have explicit requirements where the licensee shall use the PSA to enhance nuclear power plant safety, to identify and prioritize plant modification needs and to compare the safety significance of alternative solutions.

Based on Ref. [20] the most common applications in the USA are listed here and will be presented below. This applications are related to eight initiatives for fundamental improvements to the Standard Technical Specifications that are under development by the U.S. industry and discussed with the NRC staff [21]: Maintenance Rule and configuration risk management; Regulatory Oversight Process; Individual risk-informed allowed outage time (AOT) changes; Emergency technical specification (TS) changes; Risk-informed mode change assessments; Risk-informed treatment of missed surveillances; In-service inspection; and Containment testing.

2.3.1 Maintenance Rule and configuration risk management (paragraph (a)(4))[20]

The Maintenance Rule (10 CFR 50.65) is considered an enabler of risk-informed regulation. The Maintenance Rule brought risk-informed thinking into the plant by requiring that maintenance impacts of "risk-significant" components be considered over the long term by controlling effects on reliability and availability and in the short term by influencing day-to-day maintenance activities.

The basis of the Maintenance Rule involves the identification and monitoring of risk-significant structures, systems and components (SSCs). This process involves plant-specific identification of the most safety-significant SSCs based on the plant PSA, and implementation of a monitoring program with defined performance goals. Operationally, the focus on safety-significant SSCs has led to a decreased focus on unimportant SSCs, which improved operational efficiency and effectiveness.

Another key part of the Maintenance Rule is contained in paragraph (a)(4), which addresses configuration risk management (CRM). Licensees are required to assess and manage the risk associated with every maintenance activity on a risk-significant SSC. Plant operators, work control personnel, and work planners can focus on the risk implications of maintenance activities in the plant, while gaining

flexibility in scheduling maintenance activities. CRM has improved plant safety by focusing on shorter periods of SSC unavailability, especially in higher risk configurations. Outages have become safer, reducing their complexity.

Operationally, the (a)(4) initiative [21] has significantly increased the degree of flexibility in scheduling maintenance activities and has supported higher quality maintenance practices. Moving maintenance activities from outages to periods of power operation enables shorter, less complex outages, which improves operational flexibility.

2.3.2 Regulatory Oversight Process (ROP) [20]

A more recent regulatory development is the Regulatory Oversight Process (ROP), which adopts a risk-informed approach to the oversight and assessment of licensee performance. NRC (USA) [18] and STUK (Finland) [19] have explicit requirements for ROP. Here again, the understanding of risk has focused attention on the most safety-significant events and performance deficiencies rather than on obscure design basis conditions that have little real impact on safety.

2.3.3 Technical Specifications (TS) Enhancements [20]

The nuclear power industry and the NRC have worked together to address a large number of TS enhancements that benefit from risk-informed approaches. Some of these risk-informed technical specification (RITS) changes were developed through specific industry initiatives, while others were developed on an ad hoc basis. The TS changes fall into the following broad categories: Individual TS Changes; Emergency TS Changes; Risk-Informed Mode Changes; Risk-Informed; and Treatment of Missed Surveillances

2.3.4 Individual TS Changes [20]

The approach to making individual risk-informed changes to TSs is described in Regulatory Guide 1.177 [8]. Nearly 100 risk-informed changes to individual TSs have been submitted and approved in the past ten years. Many of these changes have improved maintenance management on key equipment such as diesel generators, service water systems, and other risk-significant SSCs.

While equipment outage time has increased in many cases, this increase has been offset by other controls designed to more effectively manage plant risk. CRM requirements dictate proper controls on plant configuration during key maintenance activities to monitor, control, and minimize the safety impact of the out-of-service equipment. These controls do not exist in traditional deterministic TSs. Operationally, risk-informed TSs provide greater flexibility in maintenance scheduling, ensure higher quality maintenance, and enable shorter, less complex outages.

For example, many nuclear power plants have justified extensions to the allowed outage time (AOT)/completion time (CT) for emergency diesel generators (EDGs) using risk-informed approaches. These extensions reference the risk reduction improvements resulting from the Station Blackout Rule (10 CFR 50.63) and other enhancements made as a result of plant-specific PSAs. As part of that justification, the licensee must demonstrate that the incremental risk during the outage is very small, and must take appropriate risk management actions to further control plant configuration and risks, including: limits on additional out-of-service equipment; consideration of expected weather and grid conditions; and operating staff briefings on loss of offsite power response

Many plants were able to justify extensions from 3 days to 14 days, enabling maintenance activities previously performed during outages to be performed at power. Such a change impacts outage critical path and directly reduces the length of planned outages by several days. In addition, the complexity and

work scope of the outage plan is reduced by not having to work around the divisional power unavailability caused by the EDG maintenance.

Risk-informed TS changes can also be used to justify one-time or temporary changes. For example, a twin unit pressurized water reactor (PWR) obtained a temporary TS change to allow an extended completion time for a condition with two of the four available service water pumps out of service. The site justified an extension from the typical 72 hours for this configuration to up to 144 hours in order to allow needed repairs to be performed and avoid a dual unit shutdown. Like the permanent change for EDGs described above, the justification demonstrated that the incremental risk during the outage would be very small.

2.3.5 Emergency TS Changes

Emergency TS changes are typically required when a planned AOT/CT will be exceeded, forcing a plant shutdown. A risk-informed emergency change has many benefits, including the avoided plant shutdown, increased controls on plant configuration during the unavailability, and confirmation of minimal safety impact. Operationally, the emergency change enables plant personnel to focus on restoring affected equipment, rather than dealing with a forced outage. This supports improved planning and performance of repair activities.

Although relatively infrequent, emergency AOT extensions can have substantial benefit. For example, the South Texas Project (STP) received an emergency 99-day AOT extension following a catastrophic failure of one of the Unit 2 EDGs because many replacement parts were either unavailable or obsolete, and thus had to be fabricated. The CRM Program identifies roles and responsibilities for key risk management compensatory actions (both quantitative and qualitative measures) used to manage plant risk levels for the duration of the condition, Ref.[20].

While unique, this example demonstrates the capability and flexibility provided by risk-informed approaches. In a traditional deterministic analysis, the regulator would have had no basis on which to judge the relative safety implications. The robust plant PRA developed by STP provided the plant staff and regulator with an objective framework from which decisions could be made on the best means to manage plant safety in such a condition. Operationally, STP gained an additional 99 days of full power plant operation.

2.3.6 Risk-Informed Mode Change

As part of an industry RITS initiative, licensees can justify a change in plant mode when all mode change requirements are not met. The justification includes a risk-informed assessment of the safety implications of the mode change for the given condition. The condition must be corrected once the mode change has been completed, in accordance with TSs. The initiative allows the plant startup/shutdown process to safely proceed when the conditions involved are not safety significant. The safety benefits of this initiative accrue from the plant focus remaining on safe operation and not on insignificant constraints to mode change.

Operationally, this process allows concurrent operational activities to continue so that the mode change can be planned effectively. The process also prevents the diversion of resources to less safety-significant activities and supports a controlled change in mode.

2.3.7 Risk-Informed Treatment of Missed Surveillances(RITs)

Occasionally, a licensee identifies a failure to perform a TS-required surveillance that can only be performed with the plant shut down. Another industry RITS initiative provides a structured, objective process for evaluating the risk implications of the condition. In some cases, the process can be used to

justify continued plant operation until the next plant shutdown. Plant operations remain focused on safety-significant activities while confirming that continued operation has minimal safety impact. In addition, continued power production avoids the safety implications associated with the plant transition to shutdown.

Operationally, while an avoided plant shutdown has obvious economic benefits due to increased plant availability and capacity factor, it also avoids the "organizational transient" associated with rapidly planning a forced outage.

2.3.8 In-Service Inspection [20]

One of the most widely adopted risk-informed applications in use today is the risk-informed in-service inspection (RI-ISI) process described in Regulatory Guide 1.178 [10]. RI-ISI uses operating experience and risk insights to target the pipe segments that present the greatest risk, including both the likelihood and consequences of failure. Due to its systematic, risk-informed nature, the RI-ISI process generally identifies few risk-significant welds for inspection. This translates to fewer inspections to be performed during outages and lower personnel exposures.

The safety benefits of an RI-ISI program accrue from focusing on risk-significant inspections, rather than on a deterministically identified set of welds that may or may not have any relationship to plant safety. Operationally, the benefits include fewer inspection tasks, lower personnel exposures, and shorter, less complex outages.

To cover this range of applications it is important to invest in a range of PSA studies contemplating the various scopes and various plant operating modes (POS) as: PSA Level 1, PSA level 2, Fire PSA, Seismic PSA and Low Power & Shutdown (LP & SD) PSA.

3 CONSIDERATIONS REGARDING EMERGENCY TS CHANGES, CHANGING OF OPERATION THE MODE AND RISK-INFORMED TREATMENT OF MISSED SURVEILLANCES APPLICATIONS IN THE PSA LP&SD CONTEXT

For all the applications listed above, one can see that some are more used than others. Applications such as emergency TS changes, changing the mode and risk-informed treatment of missed surveillances are applications that often require risk assessment in operating modes other than full power, where the decision making is often fraught with much subjectivity.

Although many studies indicate that the risk during shutdown is comparable to the risk associated with operation at full power [22], it is still important to study the shutdown conditions. To demonstrate the importance of shutdown the following conditions should be studied: (*i*) the initiating events that may challenge the plan in LP & SD conditions; (*ii*) the largest contributions to the core damage frequency (CDF) LP & SD; and (*iii*) the contribution of the operating states of the plant to the LP & SD CDF.

The LP&SD risk assessment study for the Surry plant [23] (a Westinghouse 3 loop PWR with atmospheric sub dry containment), shows that the POS (Plant Operational States) with reduced water inventory are most significant for risk. These states are POS 6 (mid-loop before filling), and POS 10 (mid-loop after supply). During these states, the inventory vessel (i.e., water) is reduced to approximately the midpoint of the injection nozzle of the reactor coolant system, a reduced set of equipment is available for the operators to respond to events due to testing and activities maintenance, many of the actions of the operators are complex, and containment is usually open.

The study shows that internal fire events are the most important events due to the physical separation. The dominant contributors to CDF of initiating events involve crossing the borders of several system and human error (i.e., failure of operators to mitigate the accident). The dominant contributor to core damage is the operator failure to mitigate the accident. In addition, a fire in a critical location can

damage almost all the equipment needed to mitigate accidents. Also, some flood events may result in multiple equipment failures. As to internal events (excluding fire and flood), two initiators are the most important: loss of the residual heat removal system (RHR); and loss of external power / blackout.

In the late 1990s, contemporaneously with the study mentioned above, NRC developed several studies on risk assessment shutdown [24], which looked at the assessment of the transition risk considering the behavior of Residual Heat Removal System (RHR) and Auxiliary Power Water System (AFW). NUREG-CR 6502 [25] evaluated the risk of transition, namely, the plant shutdown contribution to repair an inoperable device against the risk of repair equipment while the plant is still in operation power.

Related to human reliability analysis (HRA) these studies concluded that the dominant contributor to the CDF is the operator failure to mitigate the accident [24]. Because of the very limited number of automatic equipment actions that are typically functional during shutdown, operator actions are more dominant during shutdown than during at-power conditions. The risk is dominated by the operator understanding of the event and the ability to respond appropriately. In the PWR example, more than 98% of the core damage frequency was dominated by operator actions. Several core damage cut-sets include three or more operator actions. Therefore, understanding and modeling dependency of operator actions is a very important aspect of the total risk. Based on this analysis of PWRs, the risk of fuel damage (per hour) during shutdown operations is comparable to at-power operations.

4 RISK-INFORMED DECISION MAKING AND PSA APPLICATION IN BRAZIL

4.1 Decision making and the deterministic and probabilistic balance

The processes shown in Figure 2 are well controlled when the applications occur in known operating conditions and in a comfortable situation to take appropriate risk management actions to further control plant configuration and risks.

However, in some situations it is necessary extends the Defense In Depth (DID) concept beyond ensuring that sufficient equipment is functional to provide key Safety Functions (SF) by considering both [26, 27]: (*i*) the risk implications of periods with increased susceptibility to events that can lead to a reduced capability or loss of a key SF that is, higher risk evolutions (HREs); and (*ii*) development and implementation of compensatory risk management actions to maintain, protect, and restore key SFs.

As said before, for applications such as Emergency TS changes, changing the mode and risk-informed treatment of missed surveillances the decision making process often needs to take into account the decision between plant shutdown or keep it operating in an adverse condition to limit of operation or technical specifications. Often it is important to consider the risk of the plant at low power or during shutdown.

Other situations that are given special attention when it comes to applications are situations that can be associated with fire or flood initiating events.

For a decision-making process that takes into account both risk information and deterministic information it is important that both approaches go together and have properly addressed interfaces

The balance in the decision making process is not simple, besides the deterministic issues raised above it is important to look at the integrated PSA model and how plant operations uses that information and what applications one or could create to limit or regulate the use of extended AOTs [28].

It is important to always counteract the possibilities of RITS applications and ROP responses. For example, if not given proper oversight the application RITS 4b literally could let operators act as they wish as far as taking equipment out of service for considerably longer times than previously.

4.2 PSA application in Brazil

In compliance with the CNEN NE1.26 Standard [29], nuclear power plant operators must develop, apply and permanently improve a model for risk management of the plant associated with its various operating configurations. The requirement 20.3 establishes that during plant operation, the model for risk management must be applied in the quantification of the impact on plant overall risk caused by decision-making related to the following activities: (*a*) design modifications, changes or exceptions related to technical specifications; (*b*) management of system configurations; (*c*) maintenance planning and periodic testing; (*d*) analysis of operational events.

In the last decade, the CNEN staff has reviewed 24 licensee requests of exception to technical specification and most of the evaluated applications are related to maintenance planning and periodic testing including allowed outage time and surveillance test interval, relatively simple applications and well endorsed by the international community.

The fact that Brazil has little prescriptive regulation and not yet has a regulatory guide on PSA applications is not a limiting factor for applications such as those cited above (allowed outage time and surveillance test interval) for which a Level 1 PSA is sufficient. This gap in regulation is related to a decision-making process that involves risk assessment when one has more complex applications such as that involving risk mode change.

To improve Brazilian PSA regulatory guide it is relevant to take into account the state of the art, the international experiences and additionally take into consideration guidelines resulting from previous own risk-informed decision making experiences for the preparation of the PSA for use in developing a risk-informed management system able to support the regulatory staff, at least in current applications.

A non-exhaustive list of guidelines includes: (*a*) the establishment of a regulatory oversight program; (*b*) establish a scope that includes at least Level 1 PSA and Level 2 PSA and after assessing the risk of the plant in operation, low power and shutdown states, as well as the transfer between them; (*c*) improve competence in human reliability during transitions and other shutdown activities.

Additionally, for two of the three Brazilian NPPs, it has been requested the inclusion of Chapter 19 in the Final Safety Analysis Report (FSAR) [18]. Chapter 19 formally covers the regulatory oversight programs (ROP).

The numerical orientation of ROP brings a level of predictability and objectivity lacking in prior oversight methods. The ROP performance indicator elements drive improvements in risk-significant SSCs by providing a monitoring framework with regulatory responses that encourages high performance across the industry. This performance, in turn, translates to a net risk reduction and greatly reduced focus on non-safety-significant activities so that operational and regulatory resources are focused on the safety-significant activities at the plant [20].

As said in [28] a model for using risk information that sets an integrated process in making decisions is by no means simple to obtain. One needs to look at the integrated PSA model and how plant operations use that information and also how one can limit or regulate the use of the risk-informed approach. For example, as presented in [28], the application RITS 4b [21], if not properly addressed, could literally let operation allow completion times increasingly long for various reasons, including past success operational experience. However, at some point PSA analysts face new unavailability challenges with PSA acceptance criteria and the increased risk related to these systems will thereby limit the previously allowed AOT. This feedback process needs to be stated in the risk-informed integrated model for making decisions, as illustrated in Figure 4.

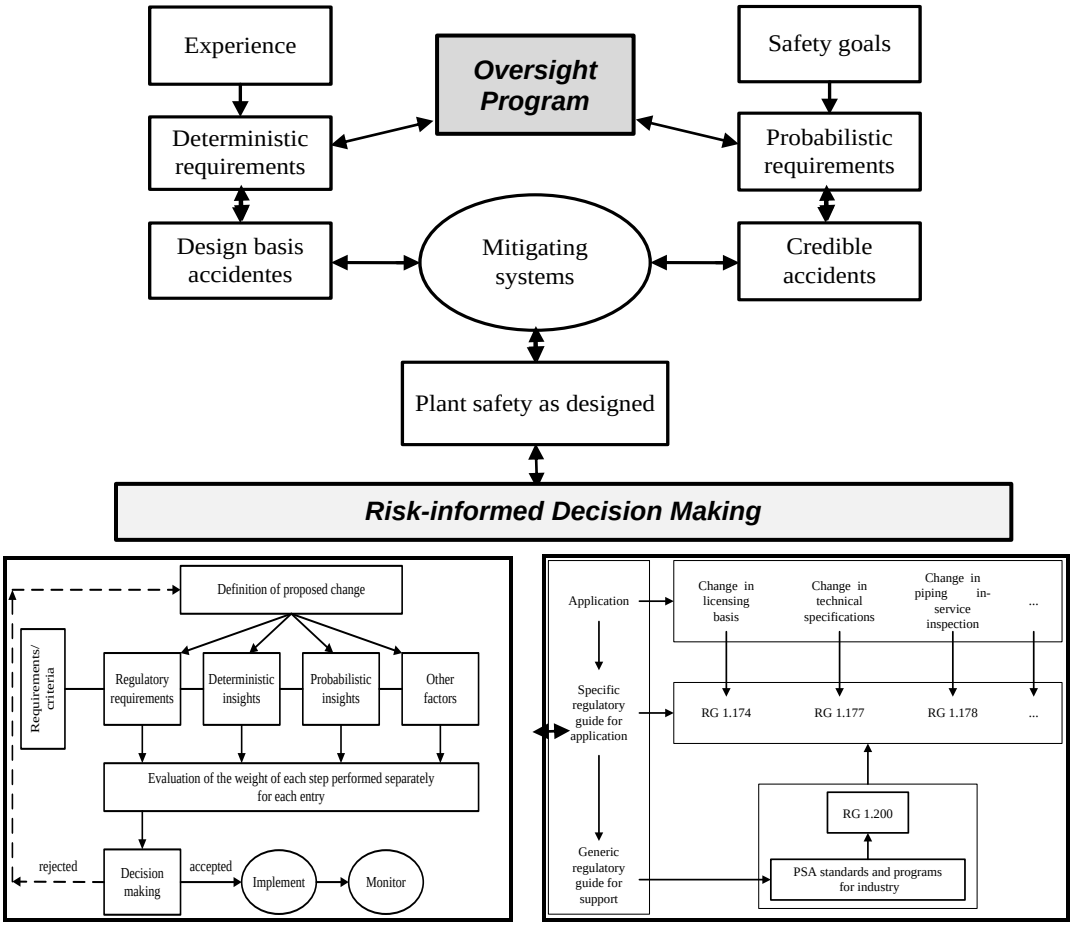

Figure 4 – Feedback process based on the Oversight Program and RIDM

5 CONCLUSIONS

Currently in nuclear plant safety, there is the premise that the deterministic and probabilistic safety approaches go together. One completes the other. The oversight program can contribute to enhance this link through the risk-informed process.

Risk-informed applications such as emergency TS changes, changing the mode and treatment of missed surveillances often require risk assessment in operating modes other than full power, where the decision making may face further subjectivity, even taking into account all principles to be followed by RIDM.

It identified the need to use the reactor oversight program at risk-informed process to complement specific information of each plant to cover aspects of applications for temporary or permanent modifications carried out by utilities.

The oversight program should be implemented due to its importance to plants and regulatory agencies, as without this the risk-informed decision making process could not fulfill its role in making a proper decision, considering the plant actual situation. In fact, making a decision without actual knowledge of the plant may be a precursor of undesirable events.

The oversight program should set up the development of Level 1^{+} PSA (base for the other PSAs), because one must examine whether all insights generated from the program are included in the event trees

and fault trees. In the opposite direction, as a feedback, after the development of the Level 1^+ PSA, it should be checked whether all the insights obtained from the PSA are fully contemplated in the oversight program.

The oversight program and the development of the Level 1^+ PSA will allow the risk-informed decision making in cases of change of technical specifications, requests for exemption, design changes results, to be an effective tool in making decisions.

In this way, it is possible to state that the oversight program, the development of PSAs, the combination of deterministic and probabilistic aspects and risk-informed decision making, are pillars that can support the safety of nuclear plants in a more conscious, efficient and effective way, because the decisions will be based on the actual plant situation.

For future work, it will be important to make the proposal discussed within the Integrated deterministic and probabilistic safety assessment (IDPSA) Ref. [32]. IDPSA was conceived as a way to analyze the evolution of accident scenarios in complex dynamic systems. In Ref. [32] is given an overview of these and discuss the related implications in terms of research perspectives. One of than, it is the compliance with the evolving regulatory requirements is anticipated to require innovative deterministic and probabilistic approaches of safety assessment for the existing nuclear power plants. In this respect, a related medium-term challenge is to combine the use of deterministic and probabilistic methodologies for safety assessment, Ref. [32].

6 REFERENCES

[1] FRUTUOSO E MELO, P. F., SALDANHA, P. L, SOUSA, A. L., "The Role of Risk-Informed Decision Making in the Licensing of Nuclear Power Plants", *Risk Assessment and Management*, Academy Publishing (Ed.), ISBN: 978-0-9835850-0-8, Available from: www.academypublish.org/book/show/title/risk-assessment-and-management (2012).

[2] FRUTUOSO E MELO, P. F., OLIVEIRA, I. M. S., and SALDANHA, P. L., "LWR Safety Analysis and Licensing and Implications for Advanced Reactors", *Nuclear Power - Operation, Safety and Environment*, Tsvetkov, P. (Ed.), ISBN: 978-953-307-507-5, InTech, Available from: www.intechopen.com/articles/show/title/lwr-safety-analysis-and-licensing-and-implications-for-advanced-reactors (2011).

[3] SNELL, V., *Nuclear Reactor Safety Design*, course notes, available from: http://epic.mcmaster.ca/~garlandw/ep714/ep714index.htm (2004).

[4] USNRC, *Reactor Safety Study – An Assessment of Accident Risks in US Commercial Nuclear Power Plants*, WASH-1400, NUREG-75/014, Nuclear Regulatory Commission, Washington, DC, USA, (1975).

[5] USNRC, *Individual Plant Examination for Severe Accident Vulnerabilities*, 10 CFR 50.54(f), Generic Letter GL–88–20, Nuclear Regulatory Commission, Washington, DC, USA (1988).

[6] USNRC, *Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities*, Final Policy Statement, Federal Regulation-60FR 42622, Nuclear Regulatory Commission, Washington, DC, USA (1995).

[7] USNRC, *An Approach for Using PRA in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis*, RG-1.174, Nuclear Regulatory Commission, Washington, DC, USA (2011).

[8] USNRC, *An Approach for Plant-Specific, Risk-Informed Decision Making: Technical Specifications*, RG-1.177, Nuclear Regulatory Commission, Washington, DC, USA (2011).

[9] USNRC, *An Approach for Plant-Specific, Risk-Informed Decision Making: In-service Testing Assurance*, RG-1.175, Nuclear Regulatory Commission, Washington, DC, USA (1998).

[10] USNRC, *An Approach for Plant-Specific, Risk-Informed Decision Making: In-service Testing Inspection of Piping*, RG-1.178, Nuclear Regulatory Commission, Washington, DC, USA (2003).

[11] USNRC, *An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities*, RG-1.200, Nuclear Regulatory Commission, Washington, DC, USA (2009).
[12] USNRC, *Risk-Informed, Performance-Based Fire Protection for Existing Light-Water Nuclear Power Plants*, RG-1.205, Nuclear Regulatory Commission, Washington, DC, USA (2009).
[13] IAEA, *Risk-informed in-service inspection of piping systems of nuclear power plants: process, status, issues and development*, IAEA nuclear energy series, ISSN 1995–7807, International Atomic Energy Agency, Vienna , Austria (2010).
[14] IAEA, *A framework for an integrated risk-informed decision making process: a report by the International Nuclear Safety Group*, INSAG series, ISSN 1025–2169, No 25, International Atomic Energy Agency, Vienna, Austria (2011).
[15] NASA, *NASA Risk-Informed Decision Making Handbook*, NASA/SP-2010-576, National Aeronautics and Space Administration, Washington, DC, USA (2010).
[16] USNRC, *Reactor Oversight Process*, NUREG-1649, US Nuclear Regulatory Commission, Washington, DC (2000).
[17] EC, *Final Report on the Regulatory Experience of Risk-Informed In-service Inspection of Nuclear Power Plant Components and Common Views*, Prepared by The Nuclear Regulators Working Group Task Force on Risk-Informed In-service Inspection, Brussels, Belgium (2004).
[18] USNRC, *Regulatory Guide 1.206 Combined License Applications for Nuclear Power Plants (LWR Edition)*, U.S. Nuclear Regulatory Commission, Washington, D. C., USA (2007).
[19] STUK, *Probabilistic Risk Assessment and Risk Management of a Nuclear Power Plant*, Helsinki, Finland (2013).
[20] EPRI, *Safety and Operational Benefits of Risk-Informed Initiatives*, An EPRI White Paper, Electric Power Research Institute, Palo Alto, CA, U.S. (2008).
[21] http://www.nrc.gov/reactors/operating/licensing/techspecs/risk-management-tech-specifications.html, set/09/2015.
[22] WHEELER, T.A., WHITEHEAD, D. W., and LOIS E., *Perspectives on Low Power and Shutdown Risk*, PSAM5, Osaka, Japan (2000).
[23] USNRC, *Evaluation of Potential Severe Accidents During Low Power and Shutdown Operations at Surry, Unit 1*, NUREG 6144, Rev 2, U.S. Nuclear Regulatory Commission, Washington, D. C., USA (1994).
[24] WHEELER, T.A., WHITEHEAD, D. W., and LOIS E., *Summary of Information Presented at an NRC-Sponsored Low-Power Shutdown Public Workshop*, April 27, 1999 Rockville, Maryland, SAND99-18 15, Sandia National Laboratories (1999).
[25] USNRC, *Action Requirements for AFW System Failures. An Analysis for Four Nuclear Power Plants*, NUREG/CR-6502, Rev 2, U.S. Nuclear Regulatory Commission, Washington, D. C., USA (1998).
[26] Nuclear Management and Resources Council (NUMARC), NUMARC Guidelines for Industry Actions to Assess Shutdown Management, NUMARC 91-06 (1991).
[27] EPRI, *Safety Qualitative Risk Assessment Methods for Shutdown Risk Management - 1013501*, Final Report, Electric Power Research Institute, Palo Alto, CA, US (2006).
[28] Reflection of AOT changes in PSA model, 03/17/2013, Nuclear Safety Probabilistic Risk Assessment Group (www.linkedin.com/groups/Probabilistic-Risk-Assessment-Group-2218640/about)
[29] CNEN, CNEN-NE-1.26, *Safety in the Operation of Nuclear Power Plants*, Comissão Nacional de Energia Nuclear, Rio de Janeiro, RJ, Brazil (1997).
[30] NEA/CSNI/R(2009)17, *Low Power and Shutdown Operations Risk: Development of Structure for Information Base and Assessment of Modelling Issues*, Issy-les-Moulineaux, France, (2009).
[31] NEA/CSNI/R(2005)11, *Improving Low Power and Shutdown PSA Methods and Data to Permit Better Risk Comparison and Trade-off Decision Making*, Vol. 1-3, Issy-les-Moulineaux, France, (2005).
[32] ZIO, E, "Integrated deterministic and probabilistic safety assessment: Concepts, challenges, research directions", *Nuclear Engineering and Design*, nº 280,pp-413,(2013).