TECHNICAL SPECIFICATIONS REVIEW OF NUCLEAR POWER PLANTS: A RISK-INFORMED EVALUATION

Pedro Luiz da Cruz Saldanha, saldanha@cnen.gov.br and plsaldanha@gmail.com
Comissão Nacional de Energia Nuclear- CGRC/CNEN, Rua General Severiano 90, Sala 426, 22294-900, Rio de janeiro, RJ, Brasil.
Anna Letícia Sousa, alsousa@cnen.gov.br
Comissão Nacional de Energia Nuclear- CODIN/CNEN, Rua da Passagem 123, 9º andar, 22290-030, Rio de Janeiro, RJ, Brasil.
Paulo Fernando Ferreira Frutuoso e Melo, frutuoso@nuclear.ufrj.br
Programa de Engenharia Nuclear, COPPE, Universidade Federal do Rio de Janeiro, Caixa Postal 68509, 21945-970, Rio de Janeiro, RJ, Brasil.
Juliana Pacheco Duarte, jduarte@nuclear.ufrj.br
Departamento de Engenharia Nuclear, Escola Politécnica, Universidade Federal do Rio de Janeiro, Caixa Postal 68509, 21945-970, Rio de Janeiro, RJ, Brasil

Abstract. *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. The risk-informed approach aims to integrate in a systematic manner quantitative and qualitative, deterministic and probabilistic safety considerations to obtain a balanced decision. Probabilistic Safety Assessment (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. Technical Specifications (TS) are specifications regarding the characteristics of nuclear power plants (variables, systems or components) of overriding importance to nuclear safety and radiation protection, which is an integral part of plant operation authorization. Limiting Conditions of Operation (LCO) are the minimum levels of performance or capacity or operating system components required for the safe operation of nuclear plants, as defined in technical specifications. The Maintenance Rule (MR) is a requirement established by the U. S. Nuclear Regulatory Commission (NRC) to check the effectiveness of maintenance carried out in nuclear plants, and plant configuration control. The control of plant configuration is necessary to verify the impact of the maintenance of a safety device out of service on plant safety. The Electric Power Research Institute (EPRI) has assessed the role of probabilistic safety analysis in the regulation of nuclear power plants with the following objectives: a) to provide utilities with an approach for developing and implementing nuclear power station risk-managed technical specification programs; and b) to complement and supplement existing successful configuration risk management applications such as MR. This paper focuses on the evaluation of EPRI's methodology on risk-informed decision making of changes to allowed outage times as a result of planned maintenance observing MR requirements. The case study is related to planning maintenance whose completion time exceeds the established TS allowable outage time.*

Keywords*: Risk-Informed Regulation, Technical Specification, Maintenance Rule, Risk-Managed Technical Specifications.*

1. INTRODUCTION

Over the last fifteen years a Probabilistic Safety Analysis (PSA) has been issued for most nuclear power plants in the world. General guidelines for issuing these PSAs have been followed both by guidance of the International Atomic Energy Agency (IAEA) and also of the U. S. Nuclear Regulatory Commission (NRC), so that these analyses are of sufficiently high quality to be used.

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 licensees without compromising safety.

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 into the activities that 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 consequence, are based on sound knowledge or data from experience, or derived from a formal, structured analysis such as a PSA.

This paper focuses on the evaluation of Risk-Managed Technical Specifications by EPRI (2006) methodology with risk informed decision making of changes to allowed outage times as a result of planned maintenance observing the MR requirements. The case study is related to plan emergency diesel generator maintenance.

2. REGULATORY DOCUMENTATION CONCERNING RIDM

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 (NRC, 1975). An important initiative (NRC, 1988) was the issuance of Generic Letter GL-88-20, which originated the program known as IPE (Individual Plant Examination). This is 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 (NRC, 1995), which incorporated risk assessment as a tool in the regulatory process. It consists of elements that have originated the Risk-informed Decision Making (RIDM) and the Performance Based Regulation (PD).

The following PSA-based RIDM regulatory guides were issued: (a) changes in the bases of the specific plant licensing, RG-1.174 (NRC, 2011a) ; (b) assessment of changes and implementation of technical specifications, RG-1.177 (NRC, 2011b); (c) in-service inspections in pipes, RG-1.175 (NRC, 1998) and RG-1.178 (NRC, 2003); (d) an approach to determine the technical quality of PSA results for RIDM, RG 1.200 (NRC, 2009a) (e) fire protection, RG 1.205 (NRC, 2009b). Many of the current regulations, based on deterministic requirements, cannot be quickly replaced.

Regulatory Guide 1.174 (NRC, 2011a) 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 (NRC, 2009a) 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 past year, sponsored and promoted activities and issued technical documents related to RIDM. Among the latest highlights are IAEA (2010) and IAEA (2011).

IAEA (2010) was prepared with the participation and contributions of experts from Belgium, the Czech Republic, Finland, the Netherlands, Sweden, Switzerland and the United States of America. 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 were 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 most risk significant locations.

IAEA (2011) 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.

3. TECHNICAL SPECIFICATIONS, MAINTENANCE RULE AND RISK-MANAGED TS

Technical Specifications are specifications regarding the characteristics of nuclear power plants (variables, systems or components) of overriding importance to nuclear safety and radiation protection, which is an integral part of plant operation authorization. The technical proposal should be accompanied by a summary of the bases, including the following topics: 1) safety limits, 2) setting limits safety system, 3) limiting conditions of operation, 4) requirements for inspections and periodic tests, 5) design features not included in previous topics, 6) administrative controls, and 7) radioactive effluents.

Limiting Conditions of Operation (LCO) are the minimum levels of performance or capacity or operating system components required for the safe operation of nuclear plants, as defined in technical specifications. The requirements for inspections and periodic (or surveillance) tests (SR) are conditions for the test, calibration or inspection, to ensure: (a) maintaining the necessary quality of systems and components of a plant, (b) facility operation within safe limits, and (c) meeting the boundary conditions of operation.

According Martorell et al (2012), safe operation of nuclear power plants depends on the technical specifications (TS), so that TS are part of the Licensee Basis (LB) to operate a NPP, which were established taking into account mainly deterministic criteria. The development of PRA (Probabilistic Risk Assessment) and its application since the early 80's to analyze TS changes has brought the opportunity to review TS consistency from a risk viewpoint, i.e., addressing the impact of the changes on plant safety on the basis of the risk information provided by the PSA, with particular attention to the role of the Allowed Outage Times (AOT) included within the Limiting Conditions of

Operation (LCO). Martorell et al (2012) focus on the use of importance analysis. A case study that focuses on an AOT change of the accumulators system of a nuclear power plant using a Level 1 PSA is provided.

The ,Maintenance Rule (MR) is a requirement established by the U. S. Nuclear Regulatory Commission (NRC) to check the effectiveness of maintenance carried out in nuclear plants and it is currently underway the discussion of the feasibility of its introduction in Europe and Brazil.

The Maintenance Rule (MR) is a requirement established by the U. S. Nuclear Regulatory Commission (NRC) to check the effectiveness of maintenance carried out in nuclear plants, and to plant configuration control. The control of plant configuration is necessary to verify the impact of the maintenance of an out of service safety device on plant safety. MR was consolidated in the U.S. in 1996. MR classifies Structures, System or Components (SSC) into two categories [1]: Category (a)(2), the SSCs that reach the intended performance demonstrate that the preventive maintenance is being appropriately performed, and category (a)(1), which stands for the SSCs that do not fulfill category (a)(2), and must have established goals, so that discrepancies can be revised and then return to Category (a)(2).

NRC requirements establish that all SSCs can be evaluated to verify the pertinence of their inclusion in a MR. If the SSC is directly related to safety, can mitigate accidents or transients, is part of Emergency Operational Procedures (EOP), can prevent other SSC of performing their safety functions, or causes a reactor shutdown or a safety system actuation, the SSC will be put within the MR scope. Otherwise, it remains under the existing maintenance program, outside the MR scope. The MR also requires that before performing maintenance activities the licensee shall assess and manage the increase in risk that may result from the proposed maintenance activities. The scope of the assessment may be limited to those structures, systems, and components that a risk-informed evaluation process has shown to be significant to public health and safety.

The Nuclear Engineering Institute (NEI) issued the report NEI (1996). This document is a guideline for applying the Maintenance Rule at Nuclear Power Plants. Section 11.0 of NEI (1996) consolidates the assessment and management of the increase in risk that may result from the proposed maintenance activities.

The Electric Power Research Institute (EPRI) has assessed the role of probabilistic safety analysis in the regulation of nuclear power plant Technical Specification, EPRI (2006). This report presents a framework and associated general guidance for implementing Risk-Managed Technical Specifications as a partial replacement for existing Technical Specification, with the following objectives: a) to provide utilities with an approach for developing and implementing nuclear power station Risk-Managed Technical Specifications programs; and b) to complement and supplement existing successful configuration risk management applications such as the Maintenance Rule.

The guidance, EPRI (2006), is applicable to the determination of risk-informed completion time (RICTs), risk-management action times (RMATs) and specification of appropriate compensatory risk-management actions (RMAS) applicable to Technical Specification requirements.

Risk management thresholds for RMTS program application are established quantitatively by considering the magnitude of the instantaneous core damage frequency (CDF) and the incremental core damage frequency (ICDF) for the plant configuration of interest. The incremental frequency values are measured from their respective “no-maintenance” or “zero-maintenance” baseline frequencies as determined via PSA.

Thresholds for risk management actions may be established quantitatively by considering the magnitude of increase of the core damage frequency for the maintenance configuration. This is defined as the incremental CDF. The incremental CDF, ICDF, is the difference in the "configuration-specific" CDF_s and the baseline (or the zero maintenance) CDF_{ZM}. The configuration-specific CDF_s is the annualized risk rate considering with the out-of-service equipment unavailability:

$$ICDP = (CDFS - CDFZM)/yr \quad (1)$$

This reflects more closely the plant actual configuration during the maintenance activity. Plants should consider duration factors when setting risk management thresholds. This may be either the duration of a particular out-of-service condition, or a specific defined work interval (e.g. shift, week, etc). The product of the incremental CDF and duration is expressed as a probability (e.g., incremental core damage probability – ICDP).

Guidance for evaluating temporary risk increases by considering configuration-specific risk is provided in NEI (1996). The risk management thresholds presented in Table 1 provides the basis for RMTS program implementation, the quantitative risk management thresholds and RMTS action guidance as well as a comparison of the respective applicable Maintenance Rule thresholds.

By EPRI (2006), in a RMTS program the 10^{-6} threshold for ICDP, is referred to as Risk Management Action (RMA) threshold and the RMAT is the corresponding risk management action time. The 10^{-5} threshold for ICDP is referred to as Risk Informed Completion Time (RICT) Thresholds. These thresholds are deemed appropriate for RMTS programs because they relate to integrated plant risk impacts that are occasional and temporary in nature and are consistent with NRC (2011a) and NRC (2011b).

Table 1.RMTS Quantitative Risk Management Thresholds

Criterion	Maintenance Rule Risk Management Guidance	RMTS Risk Management Guidance
CDF		
$\geq 10^{-3}$ events/yr	Careful consideration before entering the configuration.	Voluntary entrance into configuration prohibited. If in configuration due to emergent event, implement appropriate risk management actions.
ICDP		
$\geq 10^{-5}$	Configuration should not normally be entered voluntarily.	Follow Technical Specification requirements for required action not met.
$\geq 10^{-6}$	Assess non-quantifiable factors; and establish compensatory risk management actions.	RMAT and RICT requirements apply; Assess non-quantifiable factors; and Implement compensatory risk management actions
$<10^{-6}$	Normal work controls	Normal work controls

Figure 1 provides a simple example of the RMTS process for inoperability of equipment followed by an emergent event which modifies the risk profile causing changes in the plant configuration RMAT and RICT values.

This example is intended to demonstrate the application of these values in a RMTS program. At t = 0, the RMTS equipment becomes inoperable for a duration anticipated to exceed the front-stop CT. In this configuration, RMAT and RICT are calculated.

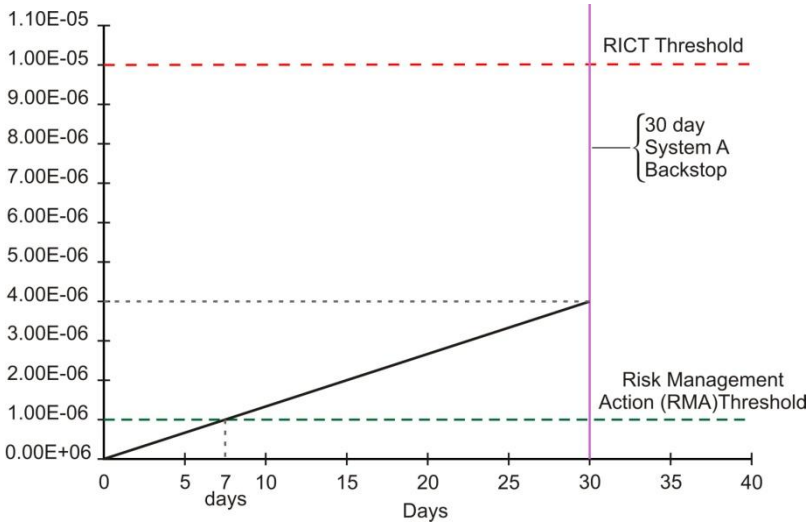

Figure 1: Configuration of Risk Management RMAT and RICT calculation

As is evident from Figure 1, the RMAT would be exceeded at time = 7 days. If the anticipated duration of the activity exceeds this time, appropriate compensatory risk management actions will be developed and implemented prior to reaching the RMAT. The RMAs shall be implemented at the earliest appropriate time. Since the 10^{-5} ICDP threshold is not reached within the 30 day back-stop CT, the applicable RICT is set at 30 days.

4. CASE STUDY

The case study is related to planning maintenance whose completion time exceeds the established Allowable Outage Time of TS and to evaluate the application of EPRI (2006). The study was based on a typical nuclear power plant of Siemens/KWU design. This design applies for safety systems of the n+2 (4 x 50%) redundancy design criteria. With the unit in power, the TS states that unavailability (out of service) of one emergency diesel generator is 14 days (AOT or CT). After this period, the unit should go to cold shutdown if the condition of the emergency diesel generator still remains unavailable.

Generic PSA data was used. It was found by using the requirements of EPRI (2006) and NEI (1996) with compensatory measures that the completion time could be extended to 30 days for the emergency diesel generator maintenance. Table 2 and Figure 2 show the results of a simulation for each emergency diesel generator. It can be seen

that risk management actions are necessary to complete the required AOT extension for DG-A, DG-B and DC D. For DG-C RMAT is 30 days.

Table 2.Results of Case Study Quantitative Risk Management Thresholds

Equipment	CDF_S 10^{-6}/yr	CDF_{ZM} 10^{-6}/yr	ICDP 10^{-6}/yr	ICDP (30 days) 10^{-6}	Normal work control (days)	Risk management actions (days)
DG-A	3.53	1.82	1.71	1.4	22	8
DG-B	3.33	1.82	1.48	1.2	27	3
DG-C	3.10	1.82	1.28	1.0	30	-
DG-D	3.62	1.82	1.80	1.5	17	13

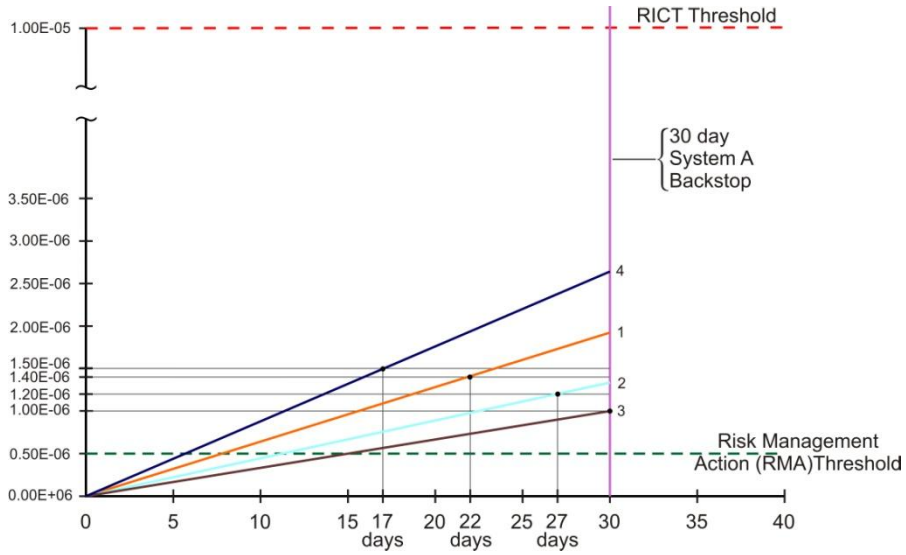

Figure 2: Case Study configuration of Risk Management RMAT and RICT calculation

5. CONCLUSIONS

Whereas PSA follows the requirements for an integrated decision-making process, the EPRI methodology is appropriate and easy to apply, allowing for consistent decision making.

The results of the case study performed show that the maintenance of emergency diesel generators for 30 days does not cause a significant increase of plant risk.

According to EPRI (2006), a particular configuration change shall be limited to a period of 30 days by technical specifications. This period was judged by EPRI as an administrative boundary prudently conservative risk management in maintenance activities.

It is noteworthy that, according to the use of risk management for the unit risk assessment, any other component / equipment that is declared inoperable simultaneously with maintaining a given DG and that affects the configuration of the unit may be returned to the original TS completion time.

6. REFERENCES

EPRI (2006). Risk-Managed Technical Specifications: Report 1011758, Electric Power research Institute, Palo Alto, CA, USA.

IAEA (2010). 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.

IAEA (2011). 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.

Martorell, S, Villamizar, Villanueva, JF, Carlos, S, and Sánchez, AI (2012). “Importance analysis in risk-informed decision-making of changes to Allowed Outage Times addressing uncertainties”, Advances in Safety, Reliability and Risk Management, Bérenguer, Grall, Guedes Soares (eds), Taylor and Francis, London, pp 2143-2151.

NEI (1996). Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants, Section 11-Assessment of Risk Resulting from Performance of Maintenance Activities, NUMARC 93-01 Revision 3, Nuclear Engineering Institute, USA.

NRC (1975). 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.

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

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

NRC (1998). An Approach for Plant-Specific, Risk-Informed Decision Making: Inservice Testing Assurance, RG-1.175, Nuclear Regulatory Commission, Washington, DC, USA.

NRC (2000). Reactor Oversight Process, NUREG-1649, US Nuclear Regulatory Commission, Washington, DC.

NRC (2001). Technical Committee Meeting on Risk Informed Decision Making (RIDM), Nuclear Regulatory Commission, Washington, DC, USA.

NRC (2003). An Approach for Plant-Specific, Risk-Informed Decision Making: Inservice Testing Inspection of Piping, RG-1.178, Nuclear Regulatory Commission, Washington, DC, USA.

NRC (2009a). 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.

NRC (2009b). Risk-Informed, Performance-Based Fire Protection for Existing Light-Water Nuclear Power Plants, RG-1.205, Nuclear Regulatory Commission, Washington, DC, USA.

NRC (2011a). 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.

NRC (2011b). An Approach for Plant-Specific, Risk-Informed Decision Making: Technical Specifications, RG-1.177, Nuclear Regulatory Commission, Washington, DC, USA.

7. RESPONSIBILITY NOTICE

The authors are the only responsible for the printed material included in this paper.