Research Article

Risk-Based Allowed Outage Time and Surveillance Test Interval Extensions for Angra 1

Sonia M. Orlando Gibelli,¹ P. F. Frutuoso e Melo,² and Sérgio Q. Bogado Leite¹

¹ *Comissão Nacional de Energia Nuclear, DRS/CGRC, 22294-900 Rio de Janeiro, RJ, Brazil*

² *Programa de Engenharia Nuclear, COPPE/UFRJ, 21941-972 Rio de Janeiro, RJ, Brazil*

Correspondence should be addressed to Sonia M. Orlando Gibelli, sonia@cnen.gov.br

Received 27 February 2012; Accepted 7 May 2012

Academic Editor: Mohammad Modarres

Copyright © 2012 Sonia M. Orlando Gibelli et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In this work, Probabilistic Safety Assessment (PSA) is used to evaluate Allowed Outage Times (AOT) and Surveillance Test Intervals (STI) extensions for three Angra 1 nuclear power plant safety systems. The interest in such an analysis lies on the fact that PSA comprises a risk-based tool for safety evaluation and has been increasingly applied to support both the regulatory and the operational decision-making processes. Regarding Angra 1, among other applications, PSA is meant to be an additional method that can be used by the utility to justify Technical Specification relaxation to the Brazilian regulatory body. The risk measure used in this work is the Core Damage Frequency, obtained from the Angra 1 Level 1 PSA study. AOT and STI extensions are evaluated for the Safety Injection, Service Water and Auxiliary Feedwater Systems using the SAPHIRE code. In order to compensate for the risk increase caused by the extensions, compensatory measures as (1) test of redundant train prior to entering maintenance and (2) staggered test strategy are proposed. Results have shown that the proposed AOT extensions are acceptable for two of the systems with the implementation of compensatory measures whereas STI extensions are acceptable for all three systems.

1. Introduction

Traditionally, Technical Specifications (TS) such as limiting conditions of operation, which include system/component AOT and STI, have been established based only on deterministic analysis [1, 2] and engineering judgment [2]. However, the experience with plant operation indicates that some elements of the requirements may be unnecessarily restrictive, and a few may not be conducive to safety [2], stressing the need to review them based on probabilistic models capable of assessing the incremental risks associated with their modifications.

In the last decades, PSAs have been elaborated and used not only to support risk-informed regulation but also to evaluate new plant designs, among other applications. Due to its broad modeling capability, which includes system functions and common-cause failure events (CCF), PSA is especially suitable for the analysis of TS modifications. Risk-based methods to improve TS requirements are meant to (1) evaluate the risk impact of TS modifications in such a

way as to objectively justify them and (2) provide risk-based information for the regulatory decision-making process [1].

This work presents an evaluation of AOT and STI extensions for three Angra 1 safety systems [3] through the use of its PSA Level 1 study, namely (1) Safety Injection System (SIS), (2) Service Water System (SWS), and (3) Auxiliary Feedwater System (AFWS). The SIS is a two-train standby system; the SWS is a two-train system but with three pumps (one of which is a swing) where one pump is in service during normal operation and the other two are in standby mode, and the AFWS is a standby system with two motor-operated pumps plus a turbine-driven pump as diversity. They were chosen to cover the types of typical safety systems of a Westinghouse two-loop PWR design. The calculations are carried out by means of the SAPHIRE code [4] with Angra 1 PSA data as the baseline input. The development of Angra 1 PSA resulted in an average estimation for the Core Damage Frequency (CDF) value of $4.015E - 05$ per reactor-year, originated from internal events and including the external event flood, although typically Level 1 PSAs evaluate the core

TABLE 1: AOT and STI proposed extensions.

System	AOT	STI
Safety injection system (SIS)	24 hours → 168 hours	1 month → 3 months
Service water system (SWS)	48 hours → 168 hours	1 month → 3 months
Auxiliary feedwater system (AFWS)	48 hours → 168 hours	1 month → 3 months

damage frequency by considering only internal accident scenarios [5]. The proposed extensions are shown in Table 1.

At first, the analyses of the AOT and STI extensions are carried out separately. However, at the end of the study, simultaneous analyses of TS modifications for two systems are also evaluated. Nevertheless, contributions to risk originated by interactions between AOT and STI are out of the scope of this work.

The risk measure adopted in this work is the CDF that can be obtained from a PSA Level 1, as part of its results. TS modifications resulting in small risk increments, that is, increments smaller than $1.0E - 06$ /reactor-year, are considered acceptable whenever the related CDF is less than $1.0E - 04$ /reactor-year. However, for CDF increments greater than $1.0E - 06$ /reactor-year, the acceptability of TS modifications depends on an evaluation process that should be performed in accordance with the applicable safety criteria. In this work, the U.S. Nuclear Regulatory Commission (NRC) safety criteria for TS risk-based evaluation are adopted [6]. As part of this study, two types of compensatory measures are proposed to compensate for risk increments associated with TS modifications: (1) test of the system redundant component, right before entering the AOT and (2) modification of the current test strategy from sequential to staggered, when applicable.

We present in the following a discussion of the state of the art of the subject, concerning the use of probabilistic approaches for the discussion of allowable outage time and surveillance test interval extensions.

Reference [7] presents results of studies of interactions between AOT and STI. The quantification of the interactions is developed in terms of risk, through the use of PSA methods. For such, an approach for modifications of AOT and STI and their effects in risk is used, taking into account the interactions between the two parameters. The work is divided into several steps and aims to present approaches that can encompass risk measures from the component level to the CDF risk level. However, the study presented in this paper concentrates the analysis only in the component level. According to its conclusions, it would be necessary to include a system-level approach or above CDF in order to make it possible to include test strategies and common-cause failures. For such, the authors developed an algorithm to deal with interactions between AOT and STI.

The methodological approach presented in [8] includes the calculation of the risk impact of a TS modification proposal, through the use of PSA. The calculations had been developed for the Seabrook and south Texas plants. The risk measures used for carrying out the study are the system's unavailabilities and the CDF. The acceptance criteria adopted in the study approve changes whose modifications in the risk do not exceed 10%. The difference between this approach

and our work lies mainly in the adoption, in the latter, of compensatory measures to neutralize the risk impact increase associated to the TS modification.

Reference [9] deals with the comparison between the risk increase associated with AOT extension and the risk associated with plant shutdown. Examples are shown for the Residual Heat Removal and Service Water systems of a BWR. The study suggests the use of the compensatory measure and test of the redundant train, for the decision-making process between continued operation with AOT extension and plant shutdown.

Reference [10] discusses the interactions between AOT and ST interval requirements by using probabilistic methods. The proposed methodology encompasses (a) the definition of AOT and STI interactions; (b) their quantification in terms of risk using PSA methods; (c) an approach for evaluating simultaneous AOT and STI modifications; (d) an assessment of strategies for giving flexibility to plant operation through simultaneous changes on AOT and STI using tradeoff-based risk criteria.

Reference [11] deals with STI optimization based on PSA methods. The approach is divided into three levels: component, system, and plant. The study concentrates on the system level application that, according to the authors, has presented results that differ from the existing technical specification STI requirements. Sequential and staggered testing strategies are used. Test strategies are introduced through the development of fault trees that include several time-dependent variables related not only to the test interval, but also to the repair time and duration of the test. The cited work uses PSA methods and Markov processes [12] to model dependences in the component and system levels.

Reference [13] presents an analysis of time-dependent unavailabilities of periodically tested components under various test and repair policies in which component renewals may eventually take place. Cost functions are developed under three different preventive maintenance policies, including test, maintenance, repair, and accident costs. The roles of different costs and aging parameters are explicitly obtained for several models, mainly in the case of an extended Weibull failure rate.

Reference [14] presents a section dedicated to technical specifications in respect of limiting conditions of operation, requirements of tests, and the use of PSA to present the concepts for the evaluation of what would be "optimum," in terms of AOT and STI associated risk. The work cites the use of PSA related to the treatment of common-cause failures. It also emphasizes the relevance to distinguish the single-event AOT from the cumulative AOT (for example, yearly AOT). The paper also evaluates the risk associated with the STI variations and the test-limit risk. The work

presents a calculation proposal of AOT extensions and their comparison with the acceptance risk criteria. The adoption of compensatory measures to compensate possible risk increases is not included in the work.

Reference [15] uses a method for evaluating the risk associated with AOT for several plant configurations, based on risk measures. The risks associated with various plant configurations considered in the study are compared with an adopted risk criterion, and the results obtained for the various proposed configurations are compared among each other. However, a methodology of compensatory measures is not introduced for configurations that include AOT extensions, when risk exceeds the acceptable ones, according to the criterion.

Reference [16] presents a proposal of simultaneous optimization of parameters related to risk-based test and maintenance and functions of cost, modeled through genetic algorithms in the system level. The work presents an example of application of the methodology for the high-pressure injection system. The results present values of costs and unavailabilities of valves and pumps, establishing a correspondence with test intervals and periods of preventive maintenance for the same valves and pumps.

Reference [17] proposes a new method for explicit modeling of single-component failure event within multiple common-cause failure groups simultaneously. This method is based on a modification of the frequently utilized beta factor parametric model. The motivation for developing this method lays in the fact that one of the most widespread softwares for fault tree and event tree modeling as part of the probabilistic safety assessment do not comprise the option for simultaneous assignment of single-failure event to multiple common-cause failure groups.

Reference [18] deals with common-cause failure probabilities in fault-tree analyses including testing and time dependencies of standby safety systems. Modeling and quantification of common-cause failures of redundant standby safety systems can be implemented by implicit or explicit fault-tree techniques. The paper derives common-cause event probabilities for both methods for systems with time-related CCFs modeled through generic multiple failure rates. The impact of test interval periods and test staggering strategy are included. An economic model provides insights into the impacts of various parameters: the optimal test interval increases with the increase in redundancy and testing cost and decreases with the increase of accident cost and initiating event rates. Staggered testing with additional tests allows the estimation of the longest optimal test intervals.

As part of a risk-informed reviewing of technical specifications, [19] considers a method for determining risk-balanced allowed outage times for a VVER440 plant. The method was tentatively applied to the emergency core cooling system including accumulators, low-pressure injection, and recirculation. Two different risk measures are interesting in studying AOTs: the AOT single event risk and the average yearly risk [2]. Both are required to stay within predetermined criteria. The longest outage time that satisfies both constraints has been established as the risk-based AOT.

Reference [20] presents the development and application of a multiple objective genetic algorithm to perform the simultaneous optimization of periodic test intervals (TI) and test strategies, both included in test planning (TP). Lessons learned from the high pressure injection system results show that the double-loop multiple-objective evolutionary algorithm is able to find the Pareto set of solutions.

Reference [21] presents a proposal of maintenance risk management through the development of a pilot study which evaluates the risk of the plant during maintenance activities, using PSA methods. The article presents a modeling for common-cause failures, without, however, presenting an application for extensions of AOT and STI. The scope of the mentioned work includes a discussion of risk monitor, PSA modeling, risk measures, and acceptance criteria as well as the role of regulatory bodies.

Reference [1] discusses a method for risk-informed optimization of allowed outage times to be used in the reviewing process of technical specifications of a Finnish VVER440 nuclear plant. The method takes into account realistic component repair times and their changes with AOTs, the possibility of common-cause failures and the risk increase in extended power operation versus forced shutdown. The method has been used to review the AOTs of the plant emergency core-cooling pumps. The results suggest that the AOTs of single failures could be shortened, while the AOTs of CCFs should be changed from immediate shutdown to three days to repair. Shutdown risks and the possibility of CCFs were found to have a major effect on optimal AOTs.

Reference [22] presents the analysis of surveillance test interval by Markov processes for shutdown systems in CANDU nuclear power plants. In order to comply with regulatory requirements, the system availability is evaluated taking into account component failure rate data and the benefits of the tests. There are many factors that should be considered in determining the surveillance test intervals for shutdown systems, and these include the desired target availability, the actual availability, the probability of spurious trips, the test duration, and the adverse effects of testing, such as wearout, introduction of human errors, and additional costs. The paper uses a Markov model to quantify the effect of surveillance test duration and interval on the system unavailability and spurious trip probability. The model can also be used to analyze the variation of CDF in respect of changes in the test interval once combined with the conditional core damage model derived from event trees and fault trees of the plant PSA.

In order to calculate the risk impact caused by testing and maintenance (AOT and STI) by means of PSA, several efforts have been carried out internationally. Component and system level evaluations were found in the literature, among which only a few have chosen CDF as a risk measure. Some of the reviewed works emphasize the evaluation of interactions between the contributions of testing and maintenance. Other studies have focused on comparing the risk of plant shutdown with the risk associated with continued operation after the expiry of the AOT and STI limits. To compensate the risk increase, these works suggest the use of compensatory measures as for example, the test of

the redundant train before starting maintenance activities. Works that use genetic algorithms for optimization of TS considering cost-related parameters have also been found in the literature.

The originality of our work lies in the proposed PSA modeling to reflect the use of compensatory measures, namely test of the redundant train and/or modification of the testing strategy from sequential to staggered to compensate the increase in risk caused by AOT and STI extensions.

For that purpose, a specific methodology was developed to fit the fault simulation (or Corrective Maintenance (CM)) of system trains, whose redundancies are affected in what concerns the calculation of common-cause failures [23]. This methodology includes not only the simulation of the test of the redundant train, but also the treatment of the related common-cause failures, which must be changed to depict the newly tested train condition. Furthermore, the STI extension is also modeled, as well as the compensation for the possible introduced increase in risk, by means of modeling effects in risk when the test strategy is switched from sequential to staggered, in case it is feasible. The calculations were performed using the SAPHIRE computer code [4], taking the Angra 1 PSA as the input data. The SAPHIRE code, used by the NRC, was adopted by both Angra 1 utility and the regulatory body as a tool for calculating Angra 1 PSA, which justifies its use in our work.

This paper is organized as follows: Section 2 addresses the risk impact by considering both the AOT and STI contributions to the total CDF. Common-cause failures are treated in this context in Section 3. Initially, a 1-out-of-3:G system is analyzed and then the same analysis is detailed for a two-component system. Next, the AOT and STI modeling are discussed in Section 4 and, finally, Section 5 details the compensatory measures that are used, which are related to the test of the redundant train, as well as to the staggered and sequential test strategies. Section 6 deals with the results obtained, by first discussing the current technical specifications for Angra 1 and then presenting the system calculation results. Overall conclusions and recommendations are presented in Section 7.

2. Risk Impact

2.1. AOT Risk Impact. It is well known that component unavailability is associated with risk increase and can occur either due to Corrective Maintenance (CM) or Preventive Maintenance (PM). This work deals only with the CM type of component unavailability. The AOT of a component under maintenance is established in such a way as to provide enough time to repair it without incurring in undue risk. In order to evaluate the risk associated with the AOT, the following aspects should be considered:

- (i) risk increase;
- (ii) duration;
- (iii) frequency of occurrence.

Based on these aspects, three types of risk impacts associated with the AOT should be controlled: (1) CDF increment,

(2) the single AOT risk impact, and (3) the yearly AOT risk impact.

The single-event risk (r) is a function of both CDF increment and duration (d) of the component unavailability. The single event risk can be expressed by [2]

$$r = (\text{CDF}_1 - \text{CDF}_B) \cdot d, \quad (1)$$

where CDF_1 is the risk level when the component is known to be down or unavailable, and CDF_B is the baseline risk, obtained from the PSA level 1 analysis.

The yearly AOT risk (R) is defined as the single event risk multiplied by the frequency of occurrence (f)

$$R = f \cdot (\text{CDF}_1 - \text{CDF}_B) \cdot d. \quad (2)$$

The literature on risk analysis [5] presents the treatment of the calculation of single event and yearly average AOT contributions, when compared with the acceptance criteria

$$\begin{aligned} r &\leq r_c & d &\leq \frac{r_c}{\Delta R} \\ R &\leq R_c & d &\leq \frac{R_c}{\Delta R \cdot f} \end{aligned} \quad \text{Criterion } d \leq \min \left[\frac{r_c}{\Delta R}, \frac{R_c}{\Delta R \cdot f} \right], \quad (3)$$

where r_c = single event risk criterion, R_c = yearly risk criterion.

When it comes to AOT extension, both risk-type contributions must be evaluated. Whether the annual frequency of a component entering an AOT is greater than one, the yearly risk contribution will be also greater than the single-event contribution. However, this is more likely to happen when dealing with PM, which is associated with a programmed maintenance schedule. On the contrary, regarding CM assessment, the frequency of occurrence of unscheduled maintenances is expected to be close to the component failure rate, which is much lesser than one. According to the NRC risk criteria, the single-component event risk (r_c) should not be greater than $5.0E-07/\text{reactor-yr}$ and there is no established criteria for the yearly averaged risk (R_c) [24]. As this work aims to analyze component failure, which leads to a corrective maintenance, the single-event criteria is applied.

2.2. STI Risk Impact. The risk contribution associated with the component test interval is mostly related to the possibility that the component fails during the period between two consecutive tests. Since the components under consideration belong to standby safety systems, component failures are understood as standby time-related failures. An exemption lies on pump A of the SWS, which is in service during normal operation. For calculation purposes, we consider the three pumps of this system belonging to the same common-cause group.

If the test is efficient, the component failure probability (Q) drops to zero immediately after the test and starts to increase as a function of time. The average unavailability of a periodically tested component is a function of both

the failure rate (λ) and the test interval time (T) and can be expressed by [2]

$$Q \approx \frac{1}{2} \lambda T. \quad (4)$$

The increase in CDF associated with the test interval extension is

$$\Delta \text{CDF} = \text{CDF}_{\text{ESTI}} - \text{CDF}_B, \quad (5)$$

where CDF_{ESTI} is the CDF taking into account the extended test interval.

3. Treatment of Common-Cause Failures

In Angra-1 PSA, the treatment of common-cause failures is carried out by means of the Multiple Greek Letters (MGL) Model [5], which is considered the most general extension of the Beta Factor Model. In order to simulate the failure of one component in an m -component system, it is useful to utilize the Basic Parameter Model [25]. The concepts underlying this model and its relation with the MGL model are summarized below. Consider a common-cause group consisting of three identical components A , B , and C . Defining event X_I as the single independent failure of component X , C_{XY} as the common-cause failure of components X and Y (and not Z), and C_{XYZ} as the common cause failure of components X , Y , and Z , then the total failure of component X can be expressed by

$$X_T = X_I \cup C_{XY} \cup C_{XZ} \cup C_{XYZ}. \quad (6)$$

Also, if

$Q_1 = P[X_I]$ = failure probability of component X from independent causes,

$Q_2 = P[C_{XY}]$ = common-cause failure probability of components X and Y (and not Z),

$Q_3 = P[C_{XYZ}]$ = common-cause failure probability of components X , Y , and Z , and since the events are mutually exclusive, then

$$Q_T = P[X_T] = Q_1 + 2Q_2 + Q_3. \quad (7)$$

Similarly, for a two-component system the total failure of X is expressed by

$$Q_T = Q_1 + Q_2. \quad (8)$$

The MGL general equation that expresses the common-cause failure probability among k particular components belonging to a common-cause group with m components, Q_k , is [5]

$$Q_k^{(m)} = \frac{1}{\binom{m-1}{k-1}} \left(\prod_{i=1}^k \rho_i \right) (1 - \rho_{k+1}) Q_T, \quad (9)$$

where $1 \leq k \leq m$, $\rho_1 = 1$, $\rho_2 = \beta$, $\rho_3 = \gamma$, $\rho_4 = \delta, \dots, \rho_{m+1} = 0$, and Q_T is the component total failure probability. It can be seen that (7) and (8) are readily obtained from equation (9). Moreover, for the case of a two-component system, the MGL Model is reduced to the Beta Factor Model, a widely used model for common-cause analysis based on a single parameter (β), in addition to the component total failure probability. The Beta Factor Model for a two-component common-cause group is expressed by

$$Q_k^{(2)} = \begin{cases} (1 - \beta) \cdot Q_T & k = 1 \\ \beta \cdot Q_T & k = 2. \end{cases} \quad (10)$$

3.1. Failure Probability of a Three-Component System. A 1-out-of-3:G system is considered failed when all three components have failed. For that case, neglecting cut sets of type $\{C_{AB}, C_{AC}\}$ as explained in [25], the expanded fault tree can be represented by

$$\{A_I, B_I, C_I\}; \{A_I, C_{BC}\}; \{B_I, C_{AC}\}; \{C_I, C_{AB}\}; \{C_{ABC}\}. \quad (11)$$

The system (S) failure probability $S = A_T \cap B_T \cap C_T$ will be then

$$Q_S = P[S] = Q_1^3 + 3Q_1Q_2 + Q_3. \quad (12)$$

For a three-component system, the conditional failure probability, given that component A has failed, can be expressed by

$$P\left[\frac{S}{A_T}\right] = \frac{P[A_T \cap B_T \cap C_T]}{P[A_T]} = \frac{Q_S}{Q_T}. \quad (13)$$

Developing the conditional probabilities for the addition of the minimal cut sets, one can obtain the expression for the Basic Parameter Model:

$$\frac{Q_S}{Q_T} = Q_1^2 \frac{Q_1}{Q_T} + 2Q_1 \frac{Q_2}{Q_T} + Q_2 \frac{Q_1}{Q_T} + \frac{Q_3}{Q_T}. \quad (14)$$

For practical considerations, taking into account that we are considering a 1-out-of-3:G logic, and using the approximation $Q_1 \approx Q_T$, then (14) reduces to

$$\frac{Q_S}{Q_T} \approx Q_1^2 + 3Q_2 + \frac{Q_3}{Q_T}. \quad (15)$$

Next, by using $Q_2 = (1/2)\beta(1 - \gamma)Q_T$ and $Q_3 = \beta\gamma Q_T$, then (15) becomes

$$\frac{Q_S}{Q_T} \approx Q_1^2 + \frac{3}{2}\beta(1 - \gamma)Q_T + \beta\gamma. \quad (16)$$

Applying (16) for Angra 1 SWS, considering the adopted values for $\beta = 0.02$, $\gamma = 0.63$, and assuming Q_1 and $Q_T < 10^{-3}$, it is reasonable to consider the approximation

$$\frac{Q_S}{Q_T} \approx \beta\gamma, \quad (17)$$

where Q_S/Q_T represents the system failure given one component has failed and $\beta\gamma$ represents the common-cause failures. A detailed discussion on this subject can be found in Appendix E of [25].

TABLE 2: Modifications on pump probabilities to simulate CM.

System/pump	Modification of independent failures	Modification of common-cause failures
SIS—train A pump	$Q_{FS} \rightarrow 1$ (true) ($Q_1^{(2)}$)	
	$Q_{FR} \rightarrow 1$ (true)	$Q_{CC} \rightarrow \beta$ ($Q_2^{(2)}$)
	$Q_{MA} \rightarrow 1$ (true)	
SWS—train A pump		$Q_{CCABC} \rightarrow \beta\gamma$ ($Q_3^{(3)}$)
		$Q_{CCAB} \rightarrow 0$ ($Q_2^{(3)}$)
	$Q_{FR} \rightarrow 1$ (true) ($Q_1^{(3)}$)	$Q_{CCAC} \rightarrow 0$ ($Q_2^{(3)}$)
		$Q_{CCBC} \rightarrow 0$ ($Q_2^{(3)}$)
AFWS—train A motor-operated pump	$Q_{FS} \rightarrow 1$ (true) ($Q_1^{(2)}$)	
	$Q_{FR} \rightarrow 1$ (true)	$Q_{CC} \rightarrow \beta$ ($Q_2^{(2)}$)
	$Q_{MA} \rightarrow 1$ (true)	

Q_{FS} stands for the pump A failure to start probabilities, Q_{FR} stands for the pump A failure to run probabilities, and Q_{MA} stands for the pump A unavailability due to maintenance.

3.2. Failure Probability of a Two-Component System. Similarly, considering a 1-out-of-2 : G system comprised by components A and B, the system conditional failure probability, given component A has failed, can be expressed by

$$P\left[\frac{S}{A_T}\right] = \frac{P[A_T \cap B_T]}{P[A_T]} = \frac{Q_S}{Q_T}. \quad (18)$$

Equation (18) can also be expressed as the sum of the minimum cut sets, which results in

$$\frac{Q_S}{Q_T} = \frac{Q_1^2}{Q_T} + \frac{Q_2}{Q_T}. \quad (19)$$

For practical considerations $Q_1 \approx Q_T$ and (19) is reduced to

$$\frac{Q_S}{Q_T} \approx Q_1 + \beta. \quad (20)$$

4. AOT and STI Extension Modeling

4.1. Current Technical Specifications. The technical specifications taken into account in this work are part of the Final Safety Analysis Report (FSAR) [3]. It is worth mentioning that Angra 1 is a two-loop plant, where most of the systems are typically a two-train type, that is, with two pumps, one in each train. An example of that is the SIS whose pumps are submitted to 24-hour allowed outage time in case of failure of one of them. Despite that fact, exemptions of system designs are also treated in this work as the SWS and the AFWS.

The SWS is a two-train system with a third swing pump, all belonging to the same common-cause group. However, one pump must be operating during normal plant operation. The SWS allowed outage time, given that one pump is failed, is 48 hours. In this system one pump is sufficient for the post-accident core-cooling operation.

The AFWS comprises two motor-operated pumps and one turbine-driven pump. However, only the two motor-operated pumps belong to the same common-cause group, being the turbine-driven diversity of the system. Therefore,

for common-cause evaluation only the motor-operated pumps are taken into account. The allowed outage time for loss of one motor-operated pump is 48 hours.

The SIS, SWS, and AFWS surveillance test intervals are one month. Concerning test strategy, the three SWS pumps are tested sequentially while the SIS and AFWS surveillance tests are staggered. Therefore, in order to compensate risk, the only candidate system to a test strategy modification to the staggered type is the SWS.

It should be mentioned that the SIS, SWS, and AFWS pump tests are performed on-line. This means that at any-time they might be demanded, they will be ready to operate.

4.2. AOT Extension Modeling. AOT extensions, for each one of the mentioned systems, are analyzed assuming a CM or a train failure in the corresponding system. By doing this, a component failure is simulated by setting its independent failure probability to one (or true) in the SAPHIRE code, and common-cause failures are treated according to (15) or (20). Since the pumps are the most important components concerning TS in the safety systems here analyzed, the extension proposals are only applied to them. Table 2 shows the modifications to be implemented on the pump probabilities, including the common-cause failures of the SIS, SWS, and AFWS to simulate CM, according to the methodology previously described. It can be noticed that, since during normal plant operation the SWS has one train in service, the analysis of that in-service train failure implies setting the pump failure-to-run probability equal to 1 (true). For the other systems, Q_1 from (20) is a combination of the pump independent unavailability modes (i.e., maintenance and failure-to-start and failure-to-run modes). Moreover, for common-cause analysis purposes, the AFWS is considered a two-train system, as explained before.

4.3. STI Extension Modeling. In order to reflect STI extensions, the calculation of CDF_{ESTI} should include modifications on the pump failure to start and common-cause failure to start unavailabilities. Therefore, for a two-component

TABLE 3: Modifications on pump probabilities to simulate STI extensions as proposed in Table 1.

System/pumps	Failure to start	Common-cause failure
SIS	$Q'_{FS} \rightarrow 3 \cdot Q_{FS} (Q_1^{(2)})$	$Q'_{CCFS} \rightarrow 3 \cdot Q_{CCFS} (Q_2^{(2)})$
SWS	$Q'_{FS} \rightarrow 3 \cdot Q_{FS} (Q_1^{(3)})$	$Q'_{CCFS} \rightarrow 3 \cdot Q_{CCFS} (Q_3^{(3)})$
AFWS	$Q'_{FS} \rightarrow 3 \cdot Q_{FS} (Q_1^{(2)})$	$Q'_{CCFS} \rightarrow 3 \cdot Q_{CCFS} (Q_2^{(2)})$

Q'_x stands for pump probabilities for the extended time period.

system, the pump unavailabilities can be expressed by (using (4) and (9) and the approximation $Q_1 \approx Q_T$)

$$\begin{aligned} Q_1^{(2)} &\approx \frac{1}{2} \lambda T_E, \\ Q_2^{(2)} &\approx \frac{1}{2} \beta \lambda T_E, \end{aligned} \quad (21)$$

where T_E is the extended test interval and β is the common-cause factor.

Similarly, in case of a three-component system, the equations expressing the test extension are:

$$\begin{aligned} Q_1^{(3)} &\approx \frac{1}{2} \cdot \lambda \cdot T_E, \\ Q_2^{(3)} &\approx \frac{1}{4} \lambda \cdot \beta \cdot (1 - \gamma) \cdot T_E, \\ Q_3^{(3)} &\approx \frac{1}{2} \lambda \cdot \beta \cdot \gamma \cdot T_E. \end{aligned} \quad (22)$$

Thus, test interval extensions can be simulated by multiplying both the pump failure to start and common-cause probabilities by an “x” factor that represents the ratio between the extended test interval and the current one. Table 3 shows that, in this work, this factor is 3, since we want to extend the current pumps STI from one to 3 months.

5. Compensatory Measures

When TS modification results in small increments in CDF, compensatory measures can be applied to compensate or balance the undue risk, in such a way that the value of the total risk is kept within acceptable levels. In this work, the compensatory measures applied are (1) test of the redundant train right before entering the AOT and (2) implementation of a staggered testing strategy, if applicable, for compensating both AOT and STI extensions.

5.1. Test of the Redundant Train. Both the single-event risk and the yearly risk are increased due to the unavailability of one train during a certain period of time, d . However, given a component failure, the overall risk can be reduced or compensated if the redundant component is submitted to a new additional test. The effect of this test is to lower the unavailability of the tested component, which is considered to be zero right after the test is performed. Then, the risk associated with the tested component starts again to increase until the next test is performed or the component is demanded.

Equation (4) shows how the unavailability of a tested component behaves in terms of its test interval, T . It means

that, in case of a new additional test right before entering the AOT period, T can be replaced by d_{AOT} , where d_{AOT} stands for the extended duration of the failed component unavailability. Based on that, the redundant component failure to start unavailability can be expressed by

$$Q_{FS} \approx \frac{1}{2} \lambda \cdot d_{AOT}. \quad (23)$$

In addition, common-cause failures of the tested train should be replaced by

$$Q_{CCFS}^{(2)} \approx \frac{1}{2} \beta \cdot \lambda \cdot d_{AOT}, \quad (24)$$

where $Q_{CCFS}^{(2)}$ is the probability of common-cause failure to start of a two-component system, β is the beta factor for starting failures related to standby components, and we have made the approximation $Q_T \approx Q_{FS}$ in (9). It should be stressed here that $0 < d \leq d_{AOT}$, in general, where d has been used in (1) and (2) [2].

Actually, the only 3-pump system treated in this work is the SWS. This system has a particularity of being a 2-train system, but with an extra swing pump. During normal operation, one of the pumps must be running, which means that the new additional testing on standby pumps can only be applied to 2 pumps.

In addition to the Technical Specifications surveillance requirements that include test intervals, a new additional test can be performed to the redundant component, right after a component is considered failed, as a compensatory measure to the total risk. This extra test should be carried out right before entering AOT and not before AOT expires. The idea is to consider the redundant component “as good as new” right after this additional new test.

Table 4 shows the conditions used in simulating the test of the redundant pump. The unavailability of the tested component in this case is divided by four, to reflect the reduction in the pump test interval, from the original 4 weeks to the duration of the AOT (168 hours).

5.2. Staggered versus Sequential Test Strategies. Normally, TS is not prescriptive with respect to the test strategy to be adopted by the utility for the plant safety systems. However, when two redundant pumps are sequentially tested, the probability of introducing the same type of human error in both pumps increases when compared to the staggered testing strategy. The advantage in adopting staggered testing is to reduce the number of failures caused by human errors during the test performance. Consequently, the common-cause failure probabilities are reduced when the test strategy

TABLE 4: Test of the redundant train pump.

Test of the redundant train pump	Pump A: commence of AOT	Pump B: test is performed right before entering AOT	Pump C: test is performed right before entering AOT	Modifications on pump common-cause failure to start probabilities
Two- or three-component system	$Q_{FS} \rightarrow 1$ (true) $Q_{FR} \rightarrow 1$ (true) $Q_{MA} \rightarrow 1$ (true)	$Q'_{FS} = Q_{FS}/4$ $Q_{MA} \rightarrow 0$ (false)	$Q'_{FS} = Q_{FS}/4$ $Q_{MC} \rightarrow 0$ (false)	$Q'_{CCFS} = Q_{CCFS}/4$

TABLE 5: Modification of pump probabilities to simulate staggered testing strategy.

System	Modification of common-cause failure to start probability to reflect staggered testing
SIS—Pumps A and B	$Q'_{CCFS} = 1/2 \cdot Q_{CCFS}$
SWS—Pumps A and B, or B and C, or A and C	$Q'_{CCFS} = 1/2 \cdot Q_{CCFS}$
SWS—Pumps A and B and C	$Q'_{CCFS} = 1/3 \cdot Q_{CCFS}$
AFWS—A and B motor-operated pumps	$Q'_{CCFS} = 1/2 \cdot Q_{CCFS}$

applied to redundant components is switched from sequential to staggered testing.

In terms of the Alpha Factor Model, for systems submitted to sequential test strategy, the common-cause failure probability among k particular components belonging to a common-cause group with m components, $Q_k^{(m)}$, is given by [25]

$$Q_k^{(m)} = \frac{k}{\binom{m-1}{k-1}} \frac{\alpha_k^{\text{Seq}}}{\alpha_t} Q_T, \quad (25)$$

where $k = 1, 2, \dots, m$, and $\alpha_t = \sum_{k=1}^m k \alpha_k^{\text{Seq}}$.

For systems submitted to staggered test strategy, on the other side, $Q_k^{(m)}$ is given by

$$Q_k^{(m)} = \frac{1}{\binom{m-1}{k-1}} \alpha_k^{\text{Stag}} Q_T. \quad (26)$$

Q_k in the Basic Parameter model is affected by the testing strategy adopted, since for staggered testing, the number of times a group of k components is tested depends on the response to the failure observed, whereas for sequential testing all components in the group are tested at each test episode. This yields the following relation for the staggered and sequential estimators of Q_k [23]:

$$\frac{Q_k^{\text{Stag}}}{Q_k^{\text{Seq}}} = \frac{1}{k}. \quad (27)$$

Therefore, as an example, for a two-component system, when the test strategy is modified from sequential to staggered, the common-cause failure related to failure to start is reduced by a factor of two. This can be explained by the fact that staggered tests increase the number of tests “against” the common-cause failures.

According to (25) and (26), independent failures or Q_1 expressions do have different calculations depending on the

test strategy. However, in this work, these differences in test strategies concerning independent failures were taken into account in the Angra 1 PSA database.

Table 5 shows the necessary modifications of pump common-cause failure probabilities to switch the test strategy from sequential to staggered testing, when applicable.

6. Results

The calculations were carried out by the SAPHIRE code to simulate pump AOT and STI extensions for the Angra 1 SIS, SWS, and AFWS. The results indicate, most of the times, the need to introduce compensatory measures to bring the risk within the appropriate acceptance criterion.

Single-event and yearly risk results are presented for the three systems and their respective pump AOT extensions, with and without compensatory measures. It should be noticed that difficulties in obtaining Angra 1 specific data for pump unavailability due to PM and CM, led to the adoption of their failure rates as the frequencies for the calculation of the average yearly risk associated with the AOT extensions. Considering that in this work only CM contributions are taken into account and with the pump failure rates being much less than 1, one can conclude that the single event AOT is more important than the yearly risk for the AOT risk acceptance decision-making process.

Regarding the STI extensions, the risk level of the system considering the extension is compared with the CDF.

According to current TS and operational practices in Angra 1, the possibility of implementing individual AOT and STI extensions for the SIS, SWS, and AFWS taking into account the introduction of compensatory measures is presented in Table 6. We observe that, since the staggered testing strategy is already adopted for the SIS and AFWS, this compensatory measure is not applicable to these systems.

Table 7 presents the SIS results for the analysis of AOT extension, additional test of the redundant pump, and STI extension. In this table, single-event and yearly AOT risks

TABLE 6: Possibility of AOT and STI extensions for the SIS, SWS, and AFWS.

System	Test strategy is staggered	Multiple Greek letters (MGL)	Compensatory measure: test of the redundant train	Compensatory measure: staggered test strategy
SIS	Yes	β	Yes	No
SWS	No	β and γ	Yes	Yes
AFWS	Yes	β	Yes	No

TABLE 7: SIS results.

	r	R (yr ⁻¹)	Δ CDF (yr ⁻¹)	CDF ₁ (yr ⁻¹)	f (yr ⁻¹)	d (yr)
(1)	$5.0E - 07$	$1.29E - 07$	$2.6E - 05$	$6.6E - 05$	0.26	$1.92E - 02$
(2)	$2.0E - 07$	$5.2E - 08$	$1.0E - 05$	$5.05E - 05$	0.26	$1.92E - 02$
(3)			$2.0E - 08 < 1.0E - 06$	$4.017E - 05$		

(1) Analysis of the AOT extension.

(2) Analysis of the test of the redundant train.

(3) Analysis of the STI extension.

TABLE 8: SWS results.

	r	R (yr ⁻¹)	Δ CDF (yr ⁻¹)	CDF ₁ (yr ⁻¹)	f (yr ⁻¹)	d (yr)
(1)	$3.0E - 05$	$7.4E - 06$	$1.54E - 03$	$1.58E - 03$	0.25	$1.92E - 02$
(2)			$1.0E - 06 < 2.6E - 06 < 1.0E - 05$	$4.27E - 05$		
(3)			$2.0E - 07 < 1.0E - 06$	$4.03E - 05$		

(1) Analysis of the AOT extension.

(2) Analysis of the STI extension.

(3) Analysis of staggered testing.

are obtained using a baseline CDF_B of $4.015E - 05$ per reactor-year, as calculated by the SAPHIRE code using Angra 1 PSA Level 1 results. Also, the frequency of occurrence of AOTs appearing in this and the following tables are derived from the respective pump failure rates [26]. We observe that the incremental core damage frequency obtained for the AOT extension, $2.6E - 05$ /yr, is greater than the acceptance criterion, despite the single-event contribution obtained for the extension, $5.0E - 7$ /yr is equal to the criterion r_c . We conclude that this extension is not acceptable for the SIS without compensatory measures. Upon the simulation of the redundant train test, both the increment of the CDF and the single-event contribution diminish, as can be seen in Table 7. However, Δ CDF is now equal to $1.0E - 05$ /yr, which is exactly the boundary of the acceptance criterion. This means that despite the implementation of the compensatory measure “test of train B,” just prior to the period of the AOT, other measures could be considered in risk-based regulatory decision making, such as the availability of redundant trains of other safety systems to compensate for this increased risk. Finally, the result displayed in Table 7 for the STI extension from one month to three months shows that the value obtained for the CDF, $2.0E - 08$ /yr, is acceptable in terms of risk analysis, according to the criterion without the need of introduction of compensatory measures.

Table 8 shows the SWS results for the analysis of AOT extension, STI extension, and introduction of the staggered testing strategy. One can easily see that the value obtained for the CDF₁ upon the AOT extension, $1.58E - 03$ /yr, is

greater than the baseline, which indicates the need of a compensatory measure. Using the method presented in Table 4 for the test of the redundant train yields a result of $3.82E - 05$ /yr for CDF₁ (not shown in Table 8) that characterizes a decrease in CDF which, according to the criterion, can always be allowed. In other words, the test of the redundant pump is enough to compensate the increase in CDF caused by the AOT extension.

The value obtained for the Δ CDF upon the STI extension, $2.6E - 06$ /yr, is acceptable according to the criterion, since Angra 1 CDF_B is less than $1.0E - 04$ /yr. The introduction of staggered testing can even reduce this risk increment, as can be seen in Table 8. The value obtained for Δ CDF with the staggered testing strategy was $2.0E - 07$ /yr.

Table 9 presents the AFWS results for the analysis of AOT extension, STI extension, additional test of the redundant motor-operated pump, and additional test of the redundant motor-operated pump including the turbine-driven pump. The result of the AOT extension yields a Δ CDF of $3.0E - 04$ /yr, which is unacceptable without compensatory measures. Likewise, the simulation of the test of the redundant motor-operated pump is not enough to compensate the AOT extension, since both the increase in Δ CDF and the single-event risk do not meet the established criterion. However, the introduction of the additional test of the turbine-driven pump can also be taken as a compensatory measure. The increase in Δ CDF in this case, which is $2.42E - 04$ /yr, still remains unacceptable. Therefore, within the scope of this work an AOT extension for the AFWS should not be allowed

TABLE 9: AFWS results.

	r	$R \text{ (yr}^{-1}\text{)}$	$\Delta\text{CDF (yr}^{-1}\text{)}$	$\text{CDF}_1 \text{ (yr}^{-1}\text{)}$	$f \text{ (yr}^{-1}\text{)}$	$d \text{ (yr)}$
(1)	$5.8E - 06$	$5.1E - 06$	$3.0E - 04$	$3.4E - 04$	0.88	$1.92E - 02$
(2)	$5.0E - 06$	$4.4E - 06$	$2.63E - 04$	$3.03E - 04$	0.88	$1.92E - 02$
(3)	$4.6E - 06$	$4.1E - 06$	$2.42E - 04$	$2.82E - 04$	0.88	$1.92E - 02$
(4)			$1.0E - 06 < 1.4E - 06 < 1.0E - 05$	$4.15E - 05$		

(1) Analysis of the AOT extension.

(2) Analysis of the test of the redundant motor-operated pump.

(3) Analysis of the test of the redundant motor-operated pump and the turbine-driven pump.

(4) Analysis of the STI extension.

TABLE 10: Overview of the AOT and STI extensions.

System	AOT extension to 168 h without compensatory measures	AOT extension to 168 h with compensatory measures	STI extension to 3 months without compensatory measures	STI extension to 3 months with compensatory measures
SIS	No	Yes (restrictions applied)	Yes (no restrictions)	Not applicable
SWS	No	Yes (no restrictions)	Yes (restrictions applied)	Yes (no restrictions)
AFWS	No	No	Yes (restrictions applied)	Not applicable

TABLE 11: Results of simultaneous extensions.

	r	$R \text{ (yr}^{-1}\text{)}$	$\Delta\text{CFD (yr}^{-1}\text{)}$	$\text{CDF}_1 \text{ (yr}^{-1}\text{)}$	$f \text{ (yr}^{-1}\text{)}$	$d \text{ (yr)}$
(1)	$1.6E - 07$	$4.2E - 08$	$8.5E - 06$	$4.86E - 05$	0.26	$1.92E - 02$
(2)			$2.0E - 07$	$4.03E - 05$		
(3)	$2.0E - 07$	$5.1E - 08$	$1.0E - 05$	$5.05E - 05$	0.26	$1.92E - 02$

(1) Simultaneous AOT extensions for SIS and SWS.

(2) Simultaneous STI extensions for SIS and SWS.

(3) Simultaneous AOT and STI extensions (SIS).

under any conditions. At last, the STI extension for the AFWS can be allowed due to the fact that the ΔCDF increase is acceptable, as can be seen in Table 9.

An overview of the results of the AOT and STI extensions are presented in Table 10. The term “no restrictions” in this table means that the corresponding ΔCDF , as calculated for the extension, is smaller than $1.0E - 06$ per reactor year, while “restrictions applied” means that $1.0E - 06 < \Delta\text{CDF} < 1.0E - 05$, when CDF_B is less than $1.0E - 04$, which is the case of Angra 1.

Although plant configuration control is not in the scope of this work, we have analyzed a few combinations of simultaneous AOT and STI extensions, based on the overview of results presented in Table 10. Thus, as a very first step in developing a program for plant configuration control that allows the establishment of a risk-based planning for maintenance activities, three combinations of simultaneous AOT or STI extensions have been calculated. Table 11 presents the results obtained with the SAPHIRE code for (1) simultaneous AOT extensions for the SIS and SWS; (2) simultaneous STI extensions for the SIS and SWS; (3) simultaneous AOT and STI extensions for the SIS. Interactions between AOT and STI extensions have not been taken into account in this analysis. In what concerns item (1) of Table 11, the single-event risk r value of $1.6E - 07/\text{yr}$ is less than the criterion r_c value of $5.0E - 07/\text{yr}$ and CDF lies between $1.0E - 05/\text{yr}$ and $1.0E - 06/\text{yr}$, which makes

this configuration acceptable for the SIS and SWS AOT extensions to 168 h. For item (2), the increment value of CDF , $2.0E - 07/\text{yr}$, indicates that, based on risk analysis, the simultaneous STI extensions for the SIS and SWS are acceptable. Finally, regarding item (3), the risk of single event (r) value of $2.0E - 07/\text{yr}$ is less than the criterion, which would make this configuration acceptable by this point of view. However, the calculated ΔCDF of $1.0E - 05/\text{yr}$ is in the limit between acceptance and rejection indicating the need, in the regulatory decision-making process, to consider other aspects such as the availability of redundant trains of other safety systems, to compensate this limiting value of ΔCDF .

7. Conclusions

The results obtained in this work show that AOT and STI extensions for the SIS, SWS, and AFWS of Angra 1 power plant are feasible without incurring in unacceptable increase in the plant total risk, mostly after the implementation of compensatory measures.

AOT and STI extensions for these systems result in different impacts on the total CDF . While AOT extensions can only be accepted for the SIS and SWS upon the implementation of compensatory measures, STI extensions are acceptable for all three systems without the need of compensatory measures. Clearly, in the decision-making process of a TS modification, other aspects such as operational experience, lessons learned

from previous TS modifications, and traditional engineering judgment are also to be considered, in addition to the risk analysis performed.

AOT extensions are meant to allow time flexibility to perform adequate component maintenance and repair, which in turn reduces both the AOT frequency and unplanned plant shutdowns. STI extensions, on the other side, can be implemented with virtually no significant contribution to CDF, thus substantially reducing an unnecessary burden of the plant team in carrying out a large number of unnecessary tests, so that their attention can be concentrated on activities more relevant to safety. Reducing the number of tests also reduces the number of occurrences of unplanned plant shutdowns caused by test-induced transients.

In what concerns TS modifications, sensitivity analyses may be necessary to address the role of key assumptions adopted during the preparation of the study, which act as a support to uncertainty analysis. Experience on sensitivity analyses developed for modifications of risk-based TS shows that the risk associated with them is relatively insensitive to uncertainties when compared, for instance, to the effect on risk from uncertainties in assumptions regarding plant design changes, or regarding significant changes to plant operating procedures [24]. Nevertheless, a sensitivity analysis of the risks associated with the components in question is recommended. Such an analysis can be done through the use of risk importance measures that may be relative or absolute and have the purpose of classifying the significance of components or systems in terms of their contributions to the overall risk. Importance measures have direct application to plant configuration control in measuring the significance of the unavailability effect of a single component that has been isolated for maintenance.

The most utilized importance measures for assessing nuclear plant components and their main applications are [5].

- (1) Birnbaum is defined as follows. the rate of change in total risk of the system with respect to changes in a risk element's basic probability (or frequency). It indicates the sensitivity of the minimal cut set upper bound with respect to a change in the basic event probability. It is sensitive to the component position in the fault-tree structure.
- (2) Fussell-Vesely is an indication of the fraction of the minimal cut set upper bound probability (or sequence frequency) that involves the cut sets containing the basic event of interest. In an aging regime, it can be interpreted as the amount of a component allowed degradation of performance as a function of risk increase. Also shows the importance of the long term averaged performance of a component (thus, it is not appropriate for measuring the importance of a set of similar components instantaneously taken out of service).
- (3) RRW (risk reduction worth) is an indication of how much the minimal cut set upper bound would decrease if the basic event never occurred. In other

words it expresses the risk change when the component is clearly available.

- (4) RAW (risk achievement worth) is an indication of how much the minimal cut set upper bound would go up if the basic event always occurred. In other words, it gives the risk increase when the component is unavailable for maintenance or due to failure.

At first, regarding the changes in TS measured in this work, the most appropriate measures of importance for the sensitivity analysis appears to be the RAW and Birnbaum, for extensions of the AOT and STI, respectively. Nevertheless, it is recommended here to also consider the Fussell-Vesely importance measure.

However, new implications on importance measuring are to be taken into account. New developments and roles of different importance measures have been pointed out [27], concerning the decision-making process on permanent and temporary configurations, technical specifications, online risk monitoring, and also ranking safety significance of systems, structures, components, and human actions. A proposal on the use of path sets, instead of cut sets has been made [28], which shows that in this manner, importance of preventing top events is addressed instead.

As earlier mentioned, this work represents an important step towards plant configuration control, which is designed to operate in an efficient and effective use of plant resources, or safety systems. Therefore, and recommended the development of a configuration control program in which the following objectives must be achieved is desirable [29]:

- (i) management of the configuration of components that are simultaneously unavailable;
- (ii) management of the standby components that are operable;
- (iii) management of the duration of the configuration (CFI);
- (iv) management of the frequency with which the configuration occurs;
- (v) management of AOT and STI interactions [7].

The calculation method presented in this work, which includes the use of compensatory measures and comparison with risk criteria, is the basic calculating tool for the management of the goals presented above. Furthermore, configuration control strategies involve the control of risk levels and risk contributions similar to those defined here and addressed during the development of this study.

Another recommendation is the inclusion of Preventive Maintenance (PM) in the AOT analysis. In this case, it is essential to develop a specific data base of plant operational experience that clearly makes the distinction between the PM and CM unavailabilities. It is worth mentioning that the collection of operational data must be targeted for PSA use [30].

The preservation of the defense in-depth principle and the observation of engineering limitations should be also emphasized. The quantitative criteria described in the regulatory guidelines [24, 31] are used to ensure that any

risk increase is within acceptable limits. However, this does not exclude traditional considerations for the decision-making process, to ensure that changes comply with the rules and regulations. Practical considerations are an integrated part of the judgment concerning the acceptability of the implementation of modifications.

It is important to address here the issue of PSA itself. PSA modeling limitations have been long discussed. One issue recently raised [32] concerns on the wide use of the so-called fault tree linking method for performing the evaluation of accident scenario frequencies [33]. This approach relies on the fact that for each initiating event, all pertinent fault trees related to the accident sequences are linked through a fault tree with an AND gate whose cut sets are generated and analyzed. Reference [33] points out that this may not be accurate. The example discussed shows that the CDF may be in error around a factor of 5. The paper proposes the use of binary decision diagrams (BDD) [34]. The BDD of a formula is a compact encoding of the truth table of this formula. It would be interesting to investigate, in this context, the role of the opposite approach to perform a PSA: the one of large event trees and small fault trees, known as event trees with boundary conditions (or explicit method) [32, 35].

Another feature to be considered is the set of PSA truncation limits [36]. According to [37], it should be adequate to retain the minimal cut sets that contribute 90–99% to the point estimate CDF. However, a tighter control could be necessary to take into account smaller probability/frequency cut sets that might have substantially larger uncertainty factors compared with those that dominate the point estimate CDF [35].

The issues raised in [32, 33] have a deep influence on the discussion of the importance measures to be used, as it is clearly mentioned in both references.

Acknowledgment

The invaluable support of Eletrobras Termonuclear S. A. on plant information is deeply acknowledged. The third author is gratefully indebted to Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) of Brazil, for financial support to this work.

References

- [1] S. P. Sirén and K. E. Jänkö, "Risk-informed optimization of allowed outage times at Loviisa NPP," in *Proceedings of the 8th International Conference on Probabilistic Safety Assessment and Management (IAPSAM '06)*, New Orleans, Fla, USA, 2006.
- [2] P. Samanta, I. Kim, T. Mankamo et al., "Handbook of methods for risk-based analyses of technical specifications," US Nuclear Regulatory Commission NUREG/CR-6141, Washington, DC, USA, 1994.
- [3] Eletrobras Termonuclear, "Final Safety Analysis Report CNAEA," Unity 1. Rev. 33, Rio de Janeiro, Brazil, 2005.
- [4] NRC, "Systems analysis programs for hands-on integrated reliability evaluations (SAPHIRE)," US Nuclear Regulatory Commission NUREG/CR-6116, Washington, DC, USA, 1998.
- [5] M. Modarres, *Risk Analysis in Engineering: Techniques, Tools, and Trends*, Taylor & Francis, Boca Raton, Fla, USA, 2006.
- [6] NRC, "Regulatory guide 1.174: an approach for using PSA in risk-informed decisions on plant-specific changes to the licensing basis," US Nuclear Regulatory Commission, Washington, DC, USA, 2002.
- [7] S. Martorell, G. Serradell, G. Verdú, and P. Samanta, "Probabilistic analysis of the interaction between allowed outage time and surveillance test interval requirements," in *IAEA Advances in Reliability Analysis and Probabilistic Safety Assessment for Nuclear Reactors. IAEA-TECDOC-737*, pp. 204–212, Vienna, Austria, 1994.
- [8] K. N. Fleming and R. P. Murphy, "Lessons learned in applying PSA methods to technical specifications optimization," in *IAEA Advances in Reliability Analysis and Probabilistic Safety Assessment for Nuclear Reactors. IAEA-TECDOC-737*, pp. 185–191, Vienna, Austria, 1994.
- [9] T. Mankamo, I. S. Kim, and P. K. Samanta, "Risk-based evaluation of allowed outage times (AOTs): considering risk of shutdown," in *IAEA. Advances in Reliability Analysis and Probabilistic Safety Assessment for Nuclear Reactors. IAEA-TECDOC-737*, pp. 216–222, Vienna, Austria, 1994.
- [10] S. A. Martorell, V. G. Serradell, and P. K. Samanta, "Improving allowed outage time and surveillance test interval requirements: a study of their interactions using probabilistic methods," *Reliability Engineering and System Safety*, vol. 47, no. 2, pp. 119–129, 1995.
- [11] M. Čepin and B. Mavko, "Probabilistic safety assessment improves surveillance requirements in technical specifications," *Reliability Engineering and System Safety*, vol. 56, no. 1, pp. 69–77, 1997.
- [12] M. L. Shooman, *Probabilistic Reliability: An Engineering Approach*, Robert E Krieger, Malabar, Fla, USA, 1990.
- [13] J. K. Vaurio, "On time-dependent availability and maintenance optimization of standby units under various maintenance policies," *Reliability Engineering and System Safety*, vol. 56, no. 1, pp. 79–89, 1997.
- [14] I. B. Wall, J. J. Haugh, and D. H. Worlege, "Recent applications of PSA for managing nuclear power plant safety," *Progress in Nuclear Energy*, vol. 39, no. 3–4, pp. 367–425, 2001.
- [15] M. Čepin and S. Martorell, "Evaluation of allowed outage time considering a set of plant configurations," *Reliability Engineering and System Safety*, vol. 78, no. 3, pp. 259–266, 2002.
- [16] S. Martorell, A. Sánchez, S. Carlos, and V. Serradell, "Simultaneous and multi-criteria optimization of TS requirements and maintenance at NPPs," *Annals of Nuclear Energy*, vol. 29, no. 2, pp. 147–168, 2002.
- [17] D. Kancev and M. Čepin, "A new method for explicit modelling of single failure event within different common cause failure groups," *Reliability Engineering and System Safety*, vol. 103, pp. 84–93, 2012.
- [18] J. K. Vaurio, "Common cause failure probabilities in standby safety system fault tree analysis with testing—scheme and timing dependencies," *Reliability Engineering and System Safety*, vol. 79, no. 1, pp. 43–57, 2003.
- [19] T. M. J. Kivirinta and K. E. Jänkö, "Determining risk-balanced allowed outage times for Loviisa power plant," in *Proceedings of the 8th International Conference on Probabilistic Safety Assessment and Management (IAPSAM '06)*, New Orleans, Fla, USA, 2006.
- [20] S. Martorell, S. Carlos, J. F. Villanueva et al., "Use of multiple objective evolutionary algorithms in optimizing surveillance requirements," *Reliability Engineering and System Safety*, vol. 91, no. 9, pp. 1027–1038, 2006.
- [21] X. He, J. Tong, and J. Chen, "Maintenance risk management in Daya Bay nuclear power plant: PSA model, tools and

- applications,” *Progress in Nuclear Energy*, vol. 49, no. 1, pp. 103–112, 2007.
- [22] S. Cho and J. Jiang, “Analysis of surveillance test interval by Markov process for SDS1 in CANDU nuclear power plants,” *Reliability Engineering and System Safety*, vol. 93, no. 1, pp. 1–13, 2008.
 - [23] NRC, “Procedures for treating common cause failures in safety and reliability studies,” US Nuclear Regulatory Commission NUREG/CR-4780, Washington, DC, USA, 1987.
 - [24] NRC, “Regulatory guide 1.177: an approach for plant-specific risk-informed decision-making: technical specifications,” US Nuclear Regulatory Commission, Washington, DC, USA, 1998.
 - [25] NRC, “Guidelines on modeling common-cause failures in probabilistic risk assessment,” US Nuclear Regulatory Commission NUREG/CR-5485, Washington, DC, USA, 1998.
 - [26] S. M. Ross, *Introduction to Probability Models*, Academic Press, San Diego, Calif, USA, 1993.
 - [27] J. K. Vaurio, “Developments in importance measures for risk-informed ranking and other applications,” in *Proceedings of the 8th International Conference on Probabilistic Safety Assessment and Management (IAPSAM ’06)*, New Orleans, Fla, USA, 2006.
 - [28] R. W. Youngblood, “Risk significance and safety significance,” *Reliability Engineering and System Safety*, vol. 73, no. 2, pp. 121–136, 2001.
 - [29] NRC, “Study of operational risk-based configuration control,” US Nuclear Regulatory Commission NUREG/CR-5641, BNL-NUREG-52261, Washington, DC, USA, 1991.
 - [30] NRC, “Handbook of parameter estimation for probabilistic risk assessment,” US Nuclear Regulatory Commission NUREG/CR-6823, SAND2003-3348P, Washington, DC, USA, 2003.
 - [31] NRC, “Risk-informed decision-making: technical specifications. Standard review plant,” US Nuclear Regulatory Commission NUREG-0800, Washington, DC, USA, 2007.
 - [32] S. Epstein and A. Rauzy, “Can we trust PRA?” *Reliability Engineering and System Safety*, vol. 88, no. 3, pp. 195–205, 2005.
 - [33] NRC, “Probabilistic risk assessment procedures guide,” US Nuclear Regulatory Commission NUREG/CR-2300, Washington, DC, USA, 1982.
 - [34] R. E. Bryant, “Graph based algorithms for Boolean function manipulation,” *IEEE Transactions on Computers*, vol. 35, no. 8, pp. 677–691, 1986.
 - [35] L. F. S. Oliveira, P. F. Frutuoso e Melo, J. E. P. Lima, and I. L. Stal, “An application of the explicit method for analysing intersystem dependencies in the evaluation of event trees,” *Nuclear Engineering and Design*, vol. 90, no. 1, pp. 25–41, 1985.
 - [36] M. Čepin, “Analysis of truncation limit in probabilistic safety assessment,” *Reliability Engineering and System Safety*, vol. 87, no. 3, pp. 395–403, 2005.
 - [37] NRC, “Probabilistic safety analysis procedures guide,” US Nuclear Regulatory Commission NUREG/CR-2815, Washington, DC, USA, 1985.