OUTAGE KEY SAFETY FUNCTIONS CONFIGURATION RISK ASSESSMENT FOR A 3 LOOPS WESTINGHOUSE PWR

M.M. CID, J.DIES, C.TAPIA, P. DIAZ[1]

Nuclear Engineering Research Group (NERG), Department of Physics and Nuclear
Engineering (DFEN), Technical University of Catalonia (UPC)
Av. Diagonal 647. 08028 Barcelona – Spain, +34 934010767
manuel.martinez.cid@upc.edu; javier.dies@upc.edu; carlos.tapia@upc.edu,
pedro.diaz.bayona@upc.edu

ABSTRACT

The methodology developed provides guidance on the use of Probabilistic Safety Assessment (PSA) for the risk-informed evaluation of Guides which ensure the compliment of Outage Key Safety Functions (OKSFs) in Nuclear Power Plants. The methodology has been applied to the 3rd and 13th Plant Operational States (POSs) as a Pilot experience. These POSs are within the operating mode 4 (Hot Shutdown) of a 3 loops Westinghouse Pressurized Water Reactor. The addressed Guide requires the operability of just one charge pump as boric acid supply source. PSA gives a Core Damage Frequency increase (ΔCDF) of $1.19 \bullet 10^{-6}$ year^{-1} for the unavailability of the charge pump in standby, consequently, the maximum exposure time (time for the increase of Core Damage Probability of the configuration to reach 1.0E-06) for this situation is T= 53.6 hours. Given an average time for the POSs of 40 hours, it is concluded that the charge pumps requirement is correct. However, it could be improved with the inclusion of an additional inventory replacement function. This would limit the effect on Risk of the charge pump unavailability. Furthermore, the need for the external electrical sources to be available during mode 4 is ratified. The procedure requires the operability of both supply sources during the POSs. The unavailability of one of supply sources them involves a ΔCDF equal to $1.64 \bullet 10^{-5}$ year^{-1} and a maximum exposure time of T= 3.89 hours. This requirement is considered appropriate from the risk-informed regulation point of view.

Key Words: Plant Operational State, Outage Key Safety Functions, Core Damage Frequency, Probabilistic Safety Assessment, Performance Technical Specifications.

Nomenclature

ΔCDF: Increase of the Core Damage Frequency due to the variation of a system parameter.

ΔCDP: Core Damage Probability increase. Analogous to ICDP (Increase of Core Damage Probability)

CDFM0: Core Damage Frequency associated to the Mth mode of Operation.

T. exp (h): Maximum exposure time.

[1] Corresponding Author

1. Introduction

The objective of the methodology developed is to assess the risk associated to the configurations of systems that the Safety Functions allow during non-full power Operating Modes (2-6). A low power and shutdown modes PSA is used to determine the risk of the configurations to be assessed. The assessment of configurations is based on the analysis of the Performance Technical Specifications (PTS) and the Guide which states the maintenance of systems affecting the Outage Key Safety Functions (OKSF) in any Plant Operational State (POS). The methodology is divided in the following tasks:

Obtaining a PSA model. It is necessary to create a new database from the PSA database and from the PSA data of the plant. This database should be restricted to the Operating Mode the systems' configurations to be assessed are related to. The Operating Mode analyzed is referred to herein as Mode M. The creation of the database restricted to Mode M consists in: the elimination of the maintenances, calibration and testing events, the filtering of accident sequences, and the prorating of the frequencies of the initiating events (IE). Non-Mode M accident sequences are screened out from the database.

Safety functions analysis. It is mandatory to identify the OKSF considered in the PTS, the Guide, and the PSA for M Mode. Key Safety Functions (KSFs) from the three sources are compared and then separated into two groups depending on whether they are common to the three documents or not. Each group of functions is called Zone. PSA functions are obtained from the headers of the Event Trees of M mode accident sequences.

Configuration analysis. The Configurations to be analyzed are identified in this step. The term Configuration refers to either a system or a group of systems and describes the situation of those systems in terms of operational state. Systems are either unavailable, in stand-by, or operating. The Configurations must be in compliance with the accomplishment of the OKSFs. These Configurations contain Systems or components whose unavailability is permitted by the OKSFs. Forbidden Configurations in which OKSFs are not accomplished are also postulated for the purpose of assessing the conservatism of OKSFs. .

Risk quantification. The quantification is performed when the different Zones have been split into groups, and the restricted database has been created. The Core Damage Frequency (CDF) and the Core Damage Frequency Variation (ΔCDF) for each Configuration are computed with RiskSpectrum®. The maximum exposure Time (T. exp.) is evaluated for a Core Damage Probability (CDP) equal to 10^{-6} and compared to the duration of the M Operating Mode.

The Risk quantification step is divided in two. The PSA exclusive KSFs are analyzed first to assess whether they should be taken into account in the Guide. Common Key Safety Functions between the three sources (PSA, Guide and PTS) are evaluated next. The obtained results are used to draw conclusions and propose recommendations and changes. Configurations regarding different KSFs should be assessed together providing the simultaneity is accepted in the Guide so as to address defense in depth. The methodology is summarized in Figure 1. Different steps of the methodology are explained in sections 2, 3, and 4.

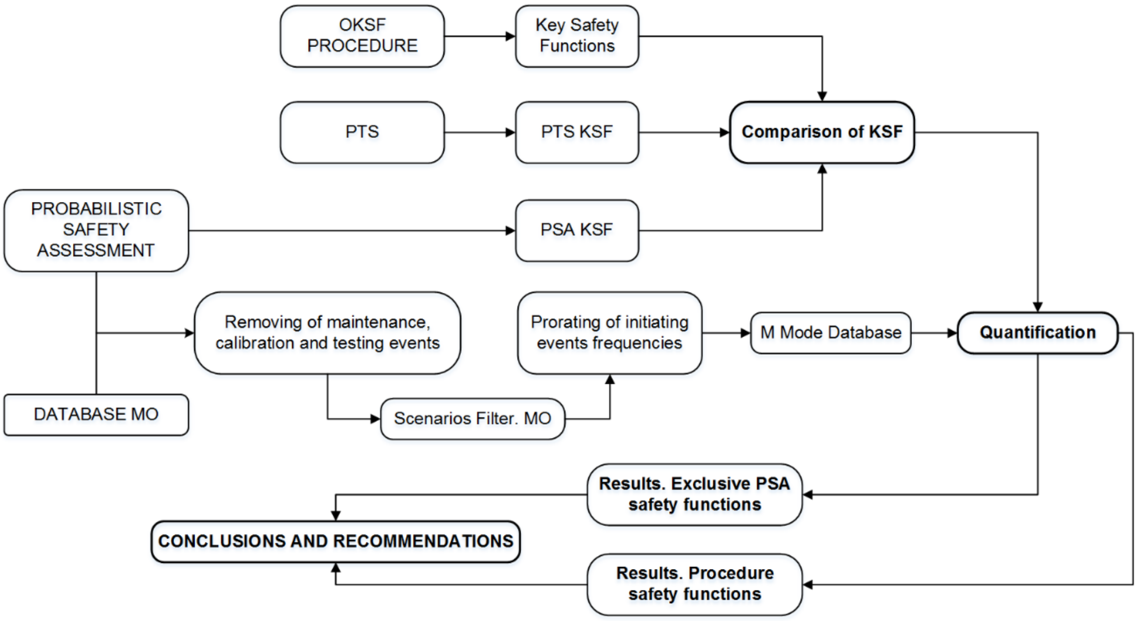
OKSF PROCEDURE
Key Safety Functions
PTS
PTS KSF
Comparison of KSF
PROBABILISTIC SAFETY ASSESSMENT
PSA KSF
Removing of maintenance, calibration and testing events
Prorating of initiating events frequencies
M Mode Database
Quantification
DATABASE MO
Scenarios Filter. MO
Results. Exclusive PSA safety functions
CONCLUSIONS AND RECOMMENDATIONS
Results. Procedure safety functions

Fig 1 Methodology followed to develop the analysis

2. Obtaining a PSA Model M mode exclusive database

The first step of the methodology is to adapt the PSA database to the specific conditions of the M Operating Mode for the quantification results to only represent the situation of the Mode. Thus, the analysis is restricted to the Mode of study. The Core Damage Frequency resulting from this database is called CDF_{M0}. The procedure to obtain the database and this value is explained in this section.

2.1 Treatment of maintenance events

The first step to adapt the database is to remove all the basic events related to components' unavailability associated with programmed tasks such as maintenance, tests or calibration. The performance of these maintenance tasks is already considered in the OKSFs' Guide, and is taken into account when assessing the Configurations of study. These basic events are set to FALSE in the RiskSpectrum® database for their unavailability to be null.

The value of the CDF may decrease once the modifications are implemented. This database is called Intermediate database 1 (DBI1).

2.2 Selection of accident sequences

The next step consists in the removal of all the accident sequences unrelated to the M Operating Mode. The frequency value for the accident sequences which do not belong to the M mode is set to Zero. There may be accident sequences shared between the M Mode and other Operating Modes which have to be further assessed. This database is called Intermediate database 2 (DBI2) after performing the suitable modifications.

2.3 Prorate of the frequencies of accident sequences shared between M Mode and other Operating Modes

Specific M Mode Initiators' frequencies have to be obtained and introduced into the PSA as long as the PSA considers annual frequencies for the initiators. The frequencies of accident sequences shared between M Mode and other Operating Modes have to be prorated to become the frequencies of the accident sequences for Mode M alone.

The time the Operating Mode M takes is a percentage (TM%) of all the time the Plant is in operation. This percentage is divided among the Plant Operational States the M mode takes into consideration.

It must be taken into account that only a few of accident sequences may be shared among M Mode and other Operating Modes. Consider N Mode other Operating Mode different to M Mode. The percentage of time N mode takes (TN%) is not considered when prorating. Instead, the time each Plant Operational State belonging to N Mode takes (TPOS %) is considered when prorating.

Given a shared accident sequence whose frequency for M and N modes is $\mathrm{f}_{\mathrm{M+N}}$, the new frequency restricted to M mode f_{M} can be computed using equation 1:

$$f_M = \frac{\mathrm{TM\%}}{\sum_{i=1} \mathrm{TPOS_i\%+TM\%}} \cdot f_{M+N} = X \cdot f_{M+N} \qquad (1)$$

The process of adapting the database is done when the frequency of shared accident sequences are prorated. With this database the reference CDFM0 can be calculated.

3. Safety Functions analysis

The objective of the methodology is to analyze the limitations and limits of operation of Systems affecting the Key Safety Functions accomplishment from the point of view of Risk. It is consequently necessary to identify the limits of operation and limitations to study. Limits of operation are the minimum quantity of operable Systems or components for the OKSFs to be considered accomplished. The Configurations of Systems representing the limitations are given by the OKSFs' Guide and PTSs. It is also required to assess the Safety Functions considered in the PSA. This assessment identifies the KSFs in the PSA which are not contemplated in the Guide and PTSs, and vice versa. It is also identified which Configurations can be assessed by means of the PSA model. The procedure to obtain the Key Safety Functions and the Configurations of systems from the different sources (PSA, Guide of study, PTSs) is detailed below:

3.1 Key Safety Functions in the PSA

The Safety Functions in the PSA are determined from the Headers of the Event Trees. These Headers are related solely with M Mode due to the process of adapting the database. Each Header represents a System or an actuation related to the mitigation of an Initiator. The Headers are consequently associated with the Safety Functions of the Plant. Fault Trees contain the components which make up a System and the different combinations of component failures which lead to a System unavailability. Headers' Fault Trees are assessed to deduce limits of operation for the KSFs.

3.2 PTS and Guide (OKSF) assessment

The following tasks must be carried out both for the PTSs and the Guide (OKSFs):

- Compare the POS specifications in PTSs and the Guide (i.e, what Systems and/or components have to be in operation or available to accept the state of the POS) with the previously identified PSA KSFs to identify which ones can be analyzed with the level one PSA. Limiting Conditions of Operation (LCO) will be accounted for to ensure defense in depth. The specifications directly are Configurations of systems.
- Group the specifications in Safety sub-Functions taking into consideration the functions required by the PSA (*i.e.* the Functions identified in 3.1) and the OKSFs.
- Classify all the previously obtained Functions as in figure 2.

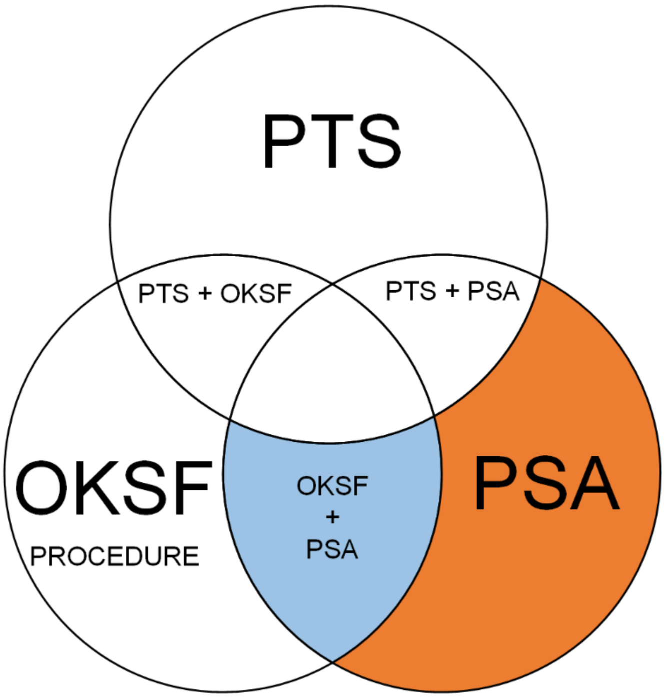

Fig 2 Space of Key Safety Functions. Venn diagram

The orange zone contains the Functions that are only considered in the PSA. The analysis of these KSFs provides their contribution to the CDF. It can be identified whether those KSFs should be introduced into the Guides and PTSs. Functions represented in blue zone are those contained both in the PSA and the Guide. The implication on Risk of these Functions can be quantified by means of the PSA. It is not possible to evaluate the Functions outside the PSA circle in the context of this methodology.

4. Quantification parameters

The following parameters, Core Damage Frequency and Maximum exposure Time for Core Damage Probability Variation, are used to evaluate the risk significance of the different Configurations and Safety Functions.

4.1 Core Damage Frequency (CDF)

The first risk measurement is the Core Damage Frequency of a specific situation. This parameter determines the frequency of core damage either for the reference case or when considering the unavailability of functions or components.

This value is obtained from the quantification of the PSA adapted model (described in section 2). This measure indicates the relative impact on Risk of a Configuration of Systems as long as the Basic Events which represent the unavailable components are set to TRUE prior to quantifying.

4.2 Maximum exposure time for a Core Damage Probability Increase (ΔCDP) of 10^{-6}

According to the reference [12], the risk acceptance criteria are based on the principles and expectations for risk-informed regulation. Risk criteria Regions (figure 3) are established in a plane generated by a measure of a baseline risk metric (Core Damage Frequency) along x-axis and the variation of that metric (CDF Increase) along the y-axis. Values can be classified in three different regions:

When the increase in CDF is small, which is less than 10^{-6} per reactor year, the application will be considered regardless of its CDF value (Region III).

Applications will be considered only if the CDF value is less than 10^{-4} when the increase is in the range of 10^{-6} to 10^{-5} (Region II). Finally, applications whose ΔCDF is higher than 10^{-5} (Region I) will not be considered.

These Risk criteria are not appropriate when assessing situations which are not permanent, such as the case of study. The time variable is introduced in the Risk analysis for finite situations. The "Increase of Core Damage Probability" (ΔCDP, equation 2) takes into account the time the plant is in a specific situation. An Increase of Core Damage Probability of 10^{-6} is accounted for as a very low Risk Increase when analyzing modifications, configurations, events, and others [1]. The Recommended Maximum Exposure Time (RMET) for a specific situation is the time needed to reach the ΔCDP 10^{-6} threshold. The RMET is the maximum time a specific situation can last to consider the plant is in a safe state. If the ΔCDP for a specific situation went higher than 10^{-6} the plant wouldn't be considered to be in a safe state anymore. The ΔCDP is computed with the following expression:

$$\Delta\mathrm{CDP} = \frac{\Delta\mathrm{CDF}\ (\mathrm{year}^{-1})\cdot \mathrm{T(h)}}{8760\frac{\mathrm{h}}{\mathrm{year}}\cdot \mathrm{TM\%}} \quad (2)$$

Where ΔCDF is obtained as the CDF of the configuration minus the CDF reference, with no maintenance:

$$\Delta\mathrm{CDF} = \mathrm{CDF}\text{-}\mathrm{CDF}_{\mathrm{M0}} \quad (3)$$

Isolating the exposure time T and imposing ΔCDP = 10^{-6}:

$$\mathrm{T(h)} = 10^{-6} \cdot \frac{8760\frac{\mathrm{h}}{\mathrm{year}}\cdot \mathrm{TM\%}}{\Delta\mathrm{CDF}\ (\mathrm{year}^{-1})} \quad (4)$$

TM% is the annual percentage of time the M Operating Mode takes and T(h) is the maximum exposure time.

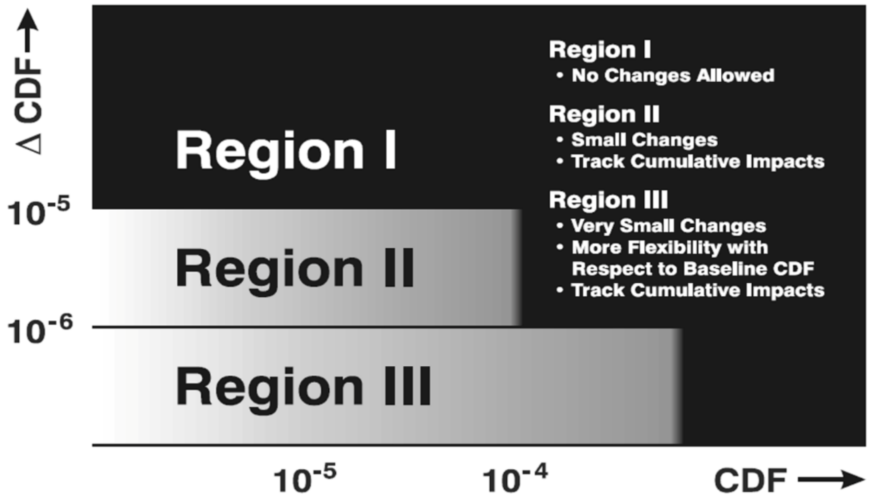

Fig 3Acceptance Crtieria for Core Damage Frequency increase [11]

5. Pilot application

The documents analyzed in the application are: level 1 PSA, OKSF procedure and Performance Technical Specifications (PTS) from a 3 loops Westinghouse Pressurized Water Reactor

(PWR). The methodology has been applied to the 3rd and 13th Plant Operational States within the Operating Mode 4.

The parameters which define the 4th Mode are in Table 1:

Table 1.

Operational Parameters in the 4th mode.

POS	Time %	Temperature (ºC)	Power condition	Multiplication Factor K_{eff}
3rd mode: Cooling with RHR	0.31 %	>93ºC	Shutdown condition	<0.99
13th mode: Heating RCS with RCP	0.42%	<175ºC	Shutdown condition	<0.99

The Safety Functions analyzed in this Mode are: reactivity control, residual heat removal, availability of electrical power, and coolant inventory control. Containment integrity is not assessed because the available PSA is Level 1.

6. Results

Safety sub-functions have been identified in the analysis of the Mode 4 Key Safety Functions. Some of these Safety sub-functions have been specifically assessed with the methodology presented. The ones analyzed belong to the Blue zone (Fig. 2). There are Configurations in the Blue zone whose unaccomplishment involves a huge increase of the CDF. The unaccomplishment of these Configurations is not accepted by the OKSF procedure. The OKSF procedure is deemed accurate for those Configurations.

Table 2 contains all the sub-functions which are accepted in different configurations in the OKSF procedure. The second column of table 2 shows the code of the gates disabled to represent the different configurations of the sub-functions or the unaccomplishment of those different Configurations. Some of these Configurations are accepted by the OKSF procedure and some are not (see column 3 from table 2). The Configurations not accepted by the OKSF procedure (i.e. unaccomplishment of a Configuration) are studied to assess the conservativeness of the procedure. The three last columns show the results obtained for each one.

Table 2.

Functions and corresponding quantification parameters.

SUBFUNCTION	*DISABLED GATE* [2]	*Accepted*	*CDF (year^{-1})*	*ΔCDF (year^{-1})*	*T(h)*
Operability of boric acid supply lines	ARB48-OM	Yes	$1.17 \cdot 10^{-6}$	$1.63 \cdot 10^{-7}$	392
	ARHPI1-OM	Yes	$1.33 \cdot 10^{-6}$	$3.21 \cdot 10^{-7}$	199
	ARHQ1-OM	Yes	$1.32 \cdot 10^{-6}$	$3.12 \cdot 10^{-7}$	205
	AR1001AR	Yes	$1.48 \cdot 10^{-5}$	$1.38 \cdot 10^{-5}$	4.64
	AR1001CR	Yes	$2.20 \cdot 10^{-6}$	$1.19 \cdot 10^{-6}$	53.60
	AR1001AR	Yes	$1.54 \cdot 10^{-5}$	$1.44 \cdot 10^{-5}$	4.44
	ARAB3010	Yes	$1.17 \cdot 10^{-6}$	$1.63 \cdot 10^{-7}$	392

[2] [12]

Operability of boric acid supply sources	AR1T001B	No	$1.91\cdot10^{-4}$	$1.90\cdot10^{-4}$	0.34
	ARAB3010 + ARAB3020	No	$4.15\cdot10^{-6}$	$3.14\cdot10^{-6}$	20.30
External electrical sources	ARCATA1F	No	$1.74\cdot10^{-5}$	$1.64\cdot10^{-5}$	3.89
	ARCATA2F	No	$7.26\cdot10^{-6}$	$6.25\cdot10^{-6}$	10.20
Operability of emergency Diesel Generators	ARTOP1-OM	No	$1.81\cdot10^{-6}$	$8.03\cdot10^{-7}$	79.64
	ARTOP2-OM	No	$1.78\cdot10^{-6}$	$7.68\cdot10^{-7}$	83.27
Operability of energy distributors systems	ARCA107AF	No	$2.43\cdot10^{-4}$	$2.42\cdot10^{-4}$	0.26
	ARCA109AF	No	$2.72\cdot10^{-4}$	$2.71\cdot10^{-4}$	0.24

The most adverse combination of configurations which is accepted by the OKSF procedure has been also assessed in a simultaneity analysis (i.e. different configurations from different safety functions addressed at the same time). The configurations analysed together are accepted by the OKSF procedure both in an isolated manner and simultaneously. This assessment is meaningful from the point of view of defense in depth. The disabled gates and basic events for this combination are not described due to confidentiality issues, although they are related to the sub-functions in Table 2. The RMET of the most adverse combination of configurations is 1.74 h.

6.1 Highlights of the study

The OKSF procedure requires the operability of both Emergency Diesel Generators (DG) during the POSs. The unavailability of the DG with the highest implication on Risk indicates a CDF increase (ΔCDF) of $8.03\cdot10^{-7}$ year^{-1}. Therefore, the Recommended Maximum Exposure Time is 79.64 hours. Given an average time for the POSs of 40 hours, this specification is too conservative according to PSA and risk-informed regulation when assessed alone. Allowing the maintenance of one DG should be further analyzed since the RMET is much higher than the time the POSs take. It should be addressed by means of a simultaneity analysis whether allowing the maintenance of one DG has any implication on defense in depth.

On the other hand, both the availability of the external electrical sources and the operability of energy distributors systems is ratified. The procedure requires the operability of both external electrical supplies during the POSs. The unavailability of one of them (transformer failure) involves a ΔCDF equal to $1.64\cdot10^{-5}$ year^{-1} and a RMET= 3.89 hours. The procedure requires the operability of both energy distributor systems. The unavailability of energy distributors systems is represented in Table 2 by means of vital bus bars local failures. The most adverse situation involves a RMET = 0.24h. Both restrictions are considered appropriate from the point of view of PSA and Risk-informed regulation.

The analyzed procedure only requires the operability of one charge pump as a boric acid supply source. PSA gives a CDF increase (ΔCDF) of $1.19\cdot10^{-6}$ year^{-1} for the unavailability of the pump in standby. The maximum exposure time is T= 53.60 hours. Given an average time for the POS of 40 hours, this restriction is considered appropriate from the point of view of PSA and Risk-informed regulation. However, it could be improved with the inclusion of an additional reposition of water inventory. This would limit the implication on Risk of the unavailability of the charge pump.

The RMET of the most adverse combination of configurations is much lower than the POSs duration time. Hence, procedure should be modified since this specific combination of configurations should not be allowed. All the possible combinations accepted by the procedure should be assessed in a non-pilot application so as to evaluate the defense in depth the procedure provides.

7. Conclusions

A methodology for the evaluation of systems’ configurations allowed in the OKSF procedures has been developed. The methodology is based on the use of PSA and management Risk Criteria. The methodology could be used to generally evaluate this kind of procedures.

Procedure restrictions could be ratified or relaxed, and new restrictions could be recommended, applying this methodology.

It is recommended to create first a list with all the safety functions ordered by its implication on risk. This list can be arranged by function, sub-function or Structure, System or Component (SSC). The comparison of the RMET with the Plant Operational State duration establishes criteria to evaluate those Safety Functions in the Blue zone. It is evaluated whether the RMET is longer or shorter than the POS duration. The analyzed function configuration is too conservative in case the RMET is quite longer. Otherwise, when the RMET is shorter, the function configuration should not be accepted because the plant would be at risk within the POS time. Additionally, the combined evaluation of functions is recommended for the purpose of addressing defense in depth. The combined evaluation of Safety Functions would consist on applying the criteria for configurations allowed by the Guide to more than one function together. The combined evaluation could derive to a matrix treatment of the SSC. On the other side, the same acceptance criteria can be applied to the PSA zone (Orange zone) to draw conclusions regarding the scope of the Guide and assess whether other functions should be included into the procedures.

A pilot application has been developed following this methodology. The study has been applied to a particular Operating Mode with two Plant Operational States. The results ratify the correct design of the functions in PTS and OKSF in most of the cases, although some of the configurations accepted should be rejected. The procedure is too conservative in other cases, allowing the introduction of more relaxed criteria in the procedure.

It has to be noted that it is recommended to require the model to be technically adequate by meeting the relevant PSA standards and going through a rigorous peer review. On the contrary, recommendations made with this technology would not be based on the actual best-estimate risk of the plant.

Acknowledgements

Authors are grateful to several anonymous plant engineers for their collaboration and ideas to the article.

References

1. CSN. PG.IV.07 Integrated Plant Supervision System (SISC). Spanish Nuclear Safety Council. 2007.

2. CSN. Integrated Program Implementation and Use of Probabilistic Safety Assessment (PSA) in Spain. Other Documents Collection, Vol. 7. 1998. 2nd Edition. Spanish Nuclear Safety Council. 1998.

3. USNRC. Use of Probabilistic Risk Assessment in Plant-specific Risk-Informed Decision-making: General Guidance. SR P Cap. 19. Rev. 1. November, 2002.

4. CSN. GS-1.15 Updating and maintenance of Probabilistic Safety Analysis. Spanish Nuclear Safety Council. 2004.

5. EPRI. EPRI-TR 05396. PSA Applications Guide. Final Report. 1995.

6. USNRC. Risk-Informed Regulations Implementation Plan. Secy-00-0213. October 16. 2000; Updated December 5. 2001 As Secy-01-0218.

7. USNRC. “An Approach For Plant-Specific, Risk-Informed Decision-Making” In-Service Testing, Regulatory Guide 1.175. August 1998.

8. RELCON SCANDPOWER AB. RISKSPECTRUM PSA Version 1.0.

9. NUMARC 91-06. Guidelines for Industry Actions to Assess Shutdown Management. December 1991.

10. CSN. PT.IV.301. Determination Process significance for Power Operations (SISC). Spanish Nuclear Safety Council. 2006.

11. USNRC. Regulatory Guide 1.174. An approach for using Probabilistic Risk Assessment in risk-informed decisions on plant specific changes to the licensing basis. Revision 1. November 2002.

12. NERG UPC. Annual Progress Report. Development of PSA methods in the assessment of economic and technological risks in nuclear power plants. January 2009.