Martorell-Aygues, P.; Marton Lluch, I.; Sánchez Galdón, AI.; Martorell Alsina, SS.; Sanchez Saez, F.; Saiz-Córdoba, M. (2018). Evaluation of risk impact of Completion Time changes combining PSA and DSA model insight and human reliability analysis. Reliability Engineering & System Safety. 178:97-107. https://doi.org/10.1016/j.ress.2018.05.008

Evaluation of risk impact of Completion Time changes combining PSA and DSA model insight and human reliability analysis

P. Martorell , I. Martón , A.I. Sánchez , S. Martorell ,
F. Sánchez-Sáez , M. Saiz

PII: S0951-8320(18)30164-9
DOI: 10.1016/j.ress.2018.05.008
Reference: RESS 6159

To appear in: *Reliability Engineering and System Safety*

Received date: 9 February 2018
Revised date: 11 May 2018
Accepted date: 18 May 2018

Please cite this article as: P. Martorell , I. Martón , A.I. Sánchez , S. Martorell , F. Sánchez-Sáez , M. Saiz , Evaluation of risk impact of Completion Time changes combining PSA and DSA model insight and human reliability analysis, *Reliability Engineering and System Safety* (2018), doi: 10.1016/j.ress.2018.05.008

Highlights

- Evaluation risk impact of completion time changes
- Combination of deterministic and probabilistic model
- Identification of unknown accident sequences using thermo-hydraulic simulations
- Increasing human error probability accuracy through best estimate codes
- More realistic PSA model

Evaluation of risk impact of Completion Time changes combining PSA and DSA model insight and human reliability analysis

P. Martorell[1,3], I.Martón[1,3], A.I. Sánchez[2,3], S. Martorell[1,3*], F. Sánchez-Sáez [1,3], M. Saiz [1],

[1]*Department of Chemical and Nuclear Engineeing. Universitat Politècnica de València, Valencia, Spain*

[2]*Department of Statistics and Operational Research. Universitat Politècnica de València, Valencia, Spain*

[3]*MEDASEGI group (http://medasegi.webs.upv.es/home/)*

[*] *Corresponding author: smartore@iqn.upv.es*

ABSTRACT:

Although in risk screening of equipment structures, systems and components, changes can be accomplished directly using RG 1.174, a plant change may also include changes to human actions. Human reliability analysis is an integral part of probabilistic safety assessment modeling. Using best estimate codes can identify unknown accident sequences as well as quantify more realistic probabilities of human error. This paper proposes a three-step approach to evaluate the risk impact of changes to completion time within nuclear power plant technical specifications, using a probabilistic safety assessment model refined by a best-estimate safety analysis and human reliability analysis. A case study is presented focusing on a completion time change of the residual heat removal system of a nuclear power plant using a level 1 low power and shutdown probabilistic safety assessment. Thus, the application case shows that the change could be accepted from a risk viewpoint, in particular, because of the risk increase imposed by extending the completion time is partially compensated by the risk decrease due to the human error probability reduction since the stress level is reduced.

LIST OF ACRONYMS

AFWS	Auxiliary Feed Water System
BE	Basic Event
CT	Completion Time
DSA	Deterministic Safety Analysis
ET	Event Tree
FT	Fault Tree
FB	Feed and Bleed
HA	Human Action
HEP	Human Error Probability
HFE	Human Failure Event
HRA	Human Reliability Analysis
IAEA	International Atomic Energy Agency
LCO	Limiting Condition for Operation
NRC	Nuclear Regulatory Commission
NPP	Nuclear Power Plant
IE	Initiating Event
PSA	Probabilistic Safety Assessment

PSF	Performance Shaping Factor
PWR	Pressurized Water Reactor
RCS	Reactor Coolant System
RG	Regulatory Guide
RIDM	Risk-Informed Decision Making
RHRS	Residual Heat Removal System
RWST	Refueling Water Storage Tank
SF	Surveillance Frequency
SG	Steam Generator
SR	Surveillance Requirements
SSC	Structures, Systems and Components
TH	Thermal Hydraulic
THERP	Technique for Human Error Rate Prediction
TRC	Time Reliability Correlation
TS	Technical Specifications
TW	Time Window

NOTATION

P_d	Diagnosis error probability
P_e	Response execution error probability
ΔCDF	Change in Core Damage Frequency
CDF_a	Core Damage Frequency before the change
CDF_b	Core Damage Frequency after the change
CDF_0	CDF when the equipment is known not to be down for maintenance
CDF_1	CDF when the equipment is known to be down for maintenance
$ICCDP$	Incremental Conditional Core Damage Probability
d_M	Yearly equipment downtime
$d_{M,\,a}$	Yearly equipment downtime after the change
$d_{M,\,b}$	Yearly equipment downtime before the change
f_M	Yearly average frequency equipment to be down
u_M	Yearly equipment unavailability

1 INTRODUCTION

The safe operation of Nuclear Power Plants (NPPs) is based on Technical Specifications (TS) that establish operational limitations and test requirements with the aim of keeping the plant's risk within the regulated limits. The TS were originally based on Deterministic Safety Analysis (DSA) and engineering judgment as part of the licensing conditions. Probabilistic Safety Assessment (PSA) has been shown to be a useful tool for reviewing TS consistency from a risk point of view. Particular attention has been paid to the role of the Surveillance Frequency (SF) as part of the Surveillance Requirements (SR) and to Completion Time (CT) as part of the Limiting Conditions for Operation (LCO).

In 1995, the US Nuclear Regulatory Commission (NRC) adopted a policy statement [1] which laid down that PSA methods and data should be used in all regulatory matters in a manner that complements the deterministic approach and supports the defense-in-depth philosophy. Since then several Regulatory Guides (RGs) and NUREG reports have been issued by the NRC on an integrated approach to risk-informed regulation [2–6]. The most important regulatory guides on risk informed TS condition evaluation are RG 1.174 [2] and RG 1.177 [3]. The former lays the foundation for using PSA in Risk-Informed Decision Making (RIDM) on specific changes to the licensing basis, while the latter proposes a more specific approach that focuses on plant specific changes to the TS.

The original US NRC policy statement in 1995 and the first drafts of RG 1.174 and RG 1.177 in 1998 established that all sources of uncertainty must be identified and analyzed so that their impacts can be understood. General guidance on addressing uncertainties from modeled and non-modeled risk contributors in this context, i.e. identification of sources key to decision, treatment and analysis of uncertainties, are specifically addressed in NUREG-1855[5] and EPRI-1026511[7].

In this way, in the last years some works [8, 9] was published showing the need for the appropriate consideration of the uncertainties in the PSA in order to adequately support the risk-informed decision making.

Changes to the risk screening of equipment Structures, Systems and Components (SSCs) can be accomplished directly using RG 1.174. Although previous work has focused on the evaluating the risk impact on plant-specific changes to TS [10,11], changes to human actions may also be included. NUREG-1764 [12] provides guidance in addressing human performance aspects of changes to operator actions that are credited

for safety, especially those involved in changing the licensing basis of the plant, within the scope of RG 1.174.

It is widely accepted that the human factor is an important part of the design and risk assessment of large complex systems. As an integral part of a PSA modeling, Human Reliability Analysis (HRA) is a systematic framework to identify, model and quantify Human Failure Events (HFEs) in the operation of an NPP. Several studies have focused on the benefits of using DSA and PSA together to improve the accuracy time windows of operator actions, i.e. the time interval in which operators have to perform an action to make the plant safe. Calculating Human Error Probability (HEP) can be done by HRA techniques [13–16], while Thermal Hydraulic (TH) simulations using best estimate codes could evaluate the appropriateness of the accident scenarios pre-established by PSA models, identifying and characterizing unknown accident sequences and success criteria [17]. Starting from the International Atomic Energy Agency's (IAEA) structured framework [18] , the combined results of both approaches provide an input on integrated risk-informed decision making to ensure nuclear reactor safety [19–21].

This paper proposes a three-step approach to evaluating the risk impact of CT changes, based on a refined PSA model through improved DSA and HRA, which addresses model and parameters uncertainties in an integrated manner following the integrated approach to risk-informed decision-making defined above.

The paper is organized as follows: Section 2 describes the methodology used to evaluate the risk impact of TS changes as a result of more realistic HEP quantification, combining DSA and PSA insights under the US NRC regulatory framework. Section 3 gives the results of a case study evaluating the risk impact of a change to the CT of the Residual Heat Removal System (RHRS) of a Pressurized Water Reactor (PWR) using the available low power and shutdown PSA and Section 4 contains the concluding remarks.

2 METHODOLOGY

2.1 Outline of evaluation of risk impact on TS changes addressing HRA

Fig. 1 outlines the main steps of an approach for evaluating the risk impact of changes to CT within NPP TS, using a PSA model refined through HRA and best estimate TH codes. The approach proposed here is consistent with the principles and framework of RIDM on plant-specific changes to the licensing basis.

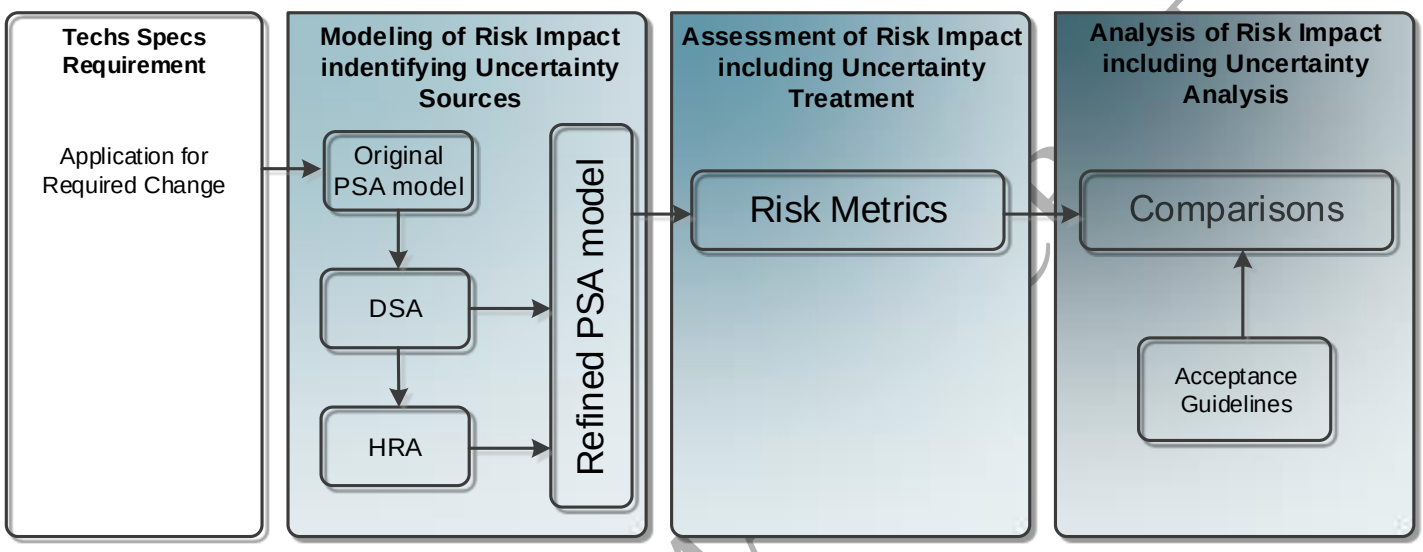

Fig. 1. Outline of RIDM on TS changes addressing HRA

2.2 Modeling of risk impact

Firstly, as concerns risk modeling in Fig.1, PSA models and data are refined with the results obtained by TH simulations, as well as a more realistic HEP quantification. The identification of not only the usually addressed sources of uncertainty linked to PSA models and data, but also the sources of model and parameter uncertainties associated with the assumptions in Completion Time therefore change the evaluation [5].

2.2.1 Deterministic Safety Analysis modeling

The first safety analyses of NPPs were performed conservatively because of knowledge limitations [24]. Deterministic Safety Analysis (DSA) was based on the use of conservative computer codes with conservative initial and boundary conditions, which could not provide precise evaluations of safety margins. As more experimental data have become available and with advances in code development the practice has now moved towards a more realistic approach together with the evaluation of uncertainties [25].

The so-called best estimate codes are able to provide more realistic information on the physical behavior and identify the most relevant safety issues. Of these, human errors in the performance of desirable diagnosis and response execution during an accident make a significant contribution to the risk. Since human errors can be a large part of the overall risk, especially in low power and shutdown modes [26], it is important that Human Error Probability (HEP) be appropriately estimated for the purpose of Probability Safety Assessment (PSA).

Human performance is highly dependent on the time available for the operator to complete his actions, and the time available is calculated by the analysis of accident scenarios. Best estimate Thermal Hydraulic (TH) codes make use of a plant specific model to determine the amount of time available to the operator for his action, i.e. Time Window (TW), ensuring that safety parameters are not exceeded [13]. A set of TH simulations are run to obtain TWs in order to estimate HEPs through the appropriate human reliability analysis techniques, as explained below.

2.2.2 Human Reliability Analysis: Human Error Probability modeling

HRA is conducted as part of the PSA for an NPP to determine how human performance affects the safety of the plant in a structured approach to identify potential Human Failure Events (HFEs) and to systematically estimate the probability of those errors using data, models, or expert judgment [27]. These probabilities are known as Human Error Probabilities (HEPs).

Post-initiator HFEs are the human errors committed during actions performed in response to an accident initiator. Each post-initiator HFE can be divided into two phases: the diagnosis and response execution phases. The former recognizes situations that require the operator's intervention, including time to think it over and take a decision, while the latter is when the action itself is performed. Accordingly, the total HEP for a post-initiator HFE can be expressed as:

$$HEP = P_d + (1 - P_d)P_e \quad (1)$$

where P_d is the diagnosis or cognitive error probability and P_e is the response execution error probability. These error probabilities are estimated separately since they are affected by a different set of factors, e.g. time, stress, etc. Nevertheless, the main steps of P_d and P_e quantification are related to the timing analysis, which is based on the results of the best estimate TH analysis. Firstly, it is necessary to identify the Time Window

(TW) to perform the action, after which it is actually too late to take any action. This TW includes the time interval to diagnose and make a decision as well as the time needed to perform the action. HEP can then be quantified applying appropriate HRA methods.

There are a number of HRA methods, which have their own advantages and disadvantages, differ in the levels of details and highlight different aspects of human actions [28,29]. Following the NRC reports related to good practice in the field of HRA [30,31], two methods were selected in this study to quantify the HEP of post-initiators HFEs: the Time Reliability Correlation, (TRC) [32] for the diagnosis phase and the Technique for Human Error Rate Prediction (THERP) [33] for the execution phase. The selection of these methods is based on the original Level 1 PSA adopted as reference, in which such human actions are quantified in this way. Both methods are briefly described below.

- The TRC method uses a lognormal distribution to calculate the probability of an operator successfully responding to a situation within a given time. This quantification system depends on primarily three factors: available time, whether it is a rule-based action (procedural actions) or a knowledge-based action (non-procedural), and whether the possibility of hesitating exists [34].
- THERP calculates the probability of the successful performance of the necessary activities for the completion of a task and involves a task analysis to provide a description of the characteristics of the human tasks being analyzed. The results are represented graphically in an HRA event tree, which is a formal representation of the required action sequence. THERP relies on a large human reliability database containing HEPs, which is based upon both plant data and expert judgments. It also takes into account the effect of other Performance Shaping Factors (PSFs), e.g. training/experience, workload, stress, procedures, etc., which can be identified by the experts.

2.2.3 Refined PSA model

The IAEA Safety Requirements entitled Safety of Nuclear Power Plants: Design IAEA Safety Standards Series No. SSR-2/1 [35] states that the safety assessment process includes the complementary techniques of deterministic safety analysis and probabilistic safety analysis. PSA Event Trees (ETs) and Fault Trees (FTs) are

defined based on expert judgment and analyzed in detail with deterministic plant simulations, e.g. thermal hydraulic and reactor physical transient accident analyses.

The capabilities of best estimate codes produce profitable results to search success criteria and to confirm the appropriateness of the accident scenarios for a postulated Initiating Event (IE) of a PSA of NPP, so that it is possible to improve the PSA models by combining probabilistic and deterministic safety analysis insights. The approach proposed in this paper seeks to obtain the following improvements:

- Identify and characterize previously unknown vulnerable scenarios as well as possible incompleteness, over or false conservatism in existing PSA and DSA models. Best estimate TH codes could be used to evaluate the appropriateness of the accident scenarios pre-established by PSA models, identifying and characterizing unknown accident sequences and success criteria. These results are reflected in the PSA model that modifies branches and quantification of ETs and FTs.
- Model and quantify with better accuracy the HEP of human actions. Best estimate TH simulations determine the amount of time available for the operator to perform an action, i.e. time window. The results of these calculations could be used to estimate the HEP more realistically through the appropriate HRA methods. The new human error quantification is included in the PSA as new probability values for the corresponding Basic Event (BE) of the FT.

Both these aims lead to a refined PSA model, representing a more realistic risk model which could be used for the risk assessment and analysis described below.

2.3 Assessment of risk impact

Next, based on Fig.1 risk assessment must be developed adopting the usual risk metrics for analyzing the completion time changes in the literature [3].

RG 1.174 establishes that the PSA should be performed in a manner that is consistent with accepted practices and also states that the quality of a PSA analysis can be measured in terms of its appropriateness with respect to scope, level of detail and technical acceptability. RG 1.177 requires that the quality of the PSA must be compatible with the safety implications of the Technical Specifications (TS) change being requested and the role the PSA plays in justifying the change.

The original PSA modeling available should thus be refined if needed on the basis of the revision of the capability of the PSA for the particular application to the analysis of changes to completion times and the way in which sources of uncertainty have to be addressed.

Basic risk measures applicable in evaluating the risk impact of CT changes are [3]: 1) Conditional risk given the limiting condition of operation, 2) Incremental conditional risk and 3) Yearly CT risk, which can be formulated adopting the *CDF* as a baseline risk measure that can be derived by using a Level 1 PSA, respectively as follows:

$$\Delta CDF_M = CDF_1 - CDF_0 \quad (2)$$

$$ICCDP_M = d_M \cdot \Delta CDF_M \quad (3)$$

$$CDF_M = f_M \cdot ICCDP_M \quad (4)$$

Eq. 2 represents the condition-specific risk, which is the increased risk when the equipment is down for maintenance, CDF_1 [year^{-1}], as compared with the reduced risk when the component is known not to be down, CDF_0 [year^{-1}], as compared both with the baseline risk, *CDF* [year^{-1}]. Eq. 3 represents the incremental conditional core damage probability ($ICCDP_M$) [dimensionless], also known as single-event CT risk for the downtime, d_M [year], associated with one occurrence of the CT. In Eq.4, CDF_M [year^{-1}]represents the yearly CT risk associated with the average yearly frequency, f_M [year^{-1}], of occurrences of the CT and the corresponding $ICCDP_M$ for each one.

In general, RG 1.174 establishes two risk metrics for evaluating the risk impact of whatever change to the licensing basis. These are the baseline risk, *CDF*, and the change in the baseline risk, *ΔCDF*, which can be formulated as follows:

$$\Delta CDF = CDF_a - CDF_b \quad (5)$$

where CDF_b and CDF_a are the baseline risk before and after the proposed change, respectively.

The following relationship applies as proposed in Ref. [10,11]:

$$CDF = CDF_0 + u_M \cdot \Delta CDF_M = CDF_0 + CDF_M \quad (6)$$

Note, the term CDF_M is given by Eq. 4. In addition, Eq. 5 can be re-written using Eq.6 as follows:

$$\Delta CDF = \left(u_{M,a} - u_{M,b}\right) \cdot \Delta CDF_M = \Delta u_M \cdot \Delta CDF_M \quad (7)$$

where $\Delta u_M = f_M(d_{M,a} - d_{M,b})$ represents the difference in the equipment unavailability contribution due to detected downtimes before and after the CT change.

Specifically concerning TS, RG 1.177 establishes one more risk metric specific to CT changes for evaluating the risk impact associated with the revised CT, which refers to the single-event CT risk after the change, i.e. $ICCDP_M$, which can be derived directly using Eq.3 with the revised downtime, d_M.

RG 1.177 also provides a comment on the acceptance guidelines on the basis of this risk metric, which affects the conditional risk, given the limiting condition of operation, i.e. ΔCDF_M, formulated by Eq.2, and therefore can be considered as the third risk metric of interest in analyzing the risk impact of CT changes.

2.4 Analysis of risk impact

Finally, risk analysis consists of the comparison of the results of the assessment of risk impact of the change against acceptance goals including treatment of uncertainties [23].

Adopting the previous risk metrics, the risk impact has to be quantified in such a way that uncertainties are treated in the most appropriate way. This should include identification of not only the usually sources of uncertainty linked to PSA models and data but also the sources of model and parameter uncertainties associated with the assumptions in CT change.

Once the risk impact of the PSA model change has been assessed it must be compared against the numeric guidelines given in RG 1.174 (see Section 2.4 in RG 1.174). In addition, for CT changes, the risk impact should also be compared with the numerical guidelines in Section 2.4 in RG 1.177.

In particular, RG 1.177 proposes adopting two acceptance guidelines for the evaluation of CT changes when using a Level 1 PSA. The first, which is the same acceptance guideline proposed by RG 1.174 for evaluating whatever change to the licensing bases, uses the baseline *CDF* and ΔCDF. Thus, the numerical acceptance guidelines are given in RG 1.174 in terms of regions defined in the space of values {*CDF*, ΔCDF} where the results of the impact on risk of a CT change are placed (see RG 1.174 for a more detailed description of such regions).

RG 1.177 establishes a second acceptance guideline specific for evaluating the risk associated with changes to CT, dealing with the single-event CT risk metric assessed after the CT change. It establishes that the licensee has to demonstrate that the CT change only has a small quantitative impact on plant conditional risk. For

example, an *ICCDP* of less than 5.0E-07 is considered small for a single CT change using a Level 1 PSA. Linked to this second guideline, RG 1.177 establishes that the *ICCDP* contribution should be distributed in time so that any increase in the associated conditional risk is small and within the normal operating background (risk fluctuations) of the plant. Clear indication is provided that *ICCDP* acceptance guideline of 5.0E-07 is based upon the hypothetical situation in which the subject equipment at a representative plant is out for five hours, causing the *CDF* of the plant, with an assumed baseline *CDF* of 1.0E-04 per reactor year, to conditionally increase to 1.0E-03 per reactor year during the five-hour period. Based on the previous paragraph, it seems that a conditional increase to 1.0E-03 per reactor year can be used as a reasonable acceptance guideline for the third risk metric. Based on this second acceptance guideline in RG 1.177, one can outline two regions in the space of values {CDF_1, *ICCDP*} where the results of the impact on risk of a CT change are placed. The region of acceptable changes is located below the boundary point {1.0E-03, 5.0E-07}.

3 CASE STUDY

This section shows the results of combining probabilistic and deterministic models in the evaluation of risk impact of a Completion Time change of the Residual Heat Removal System (RHRS) of a typical PWR accounting for the evaluation of human action changes through HRA. For sake of simplicity, a loss of the RHRS during cool down operations in hot shutdown conditions (NPP Mode 4) is the only accident scenario being presented in detail herein. The analysis of this sequence is framed within the low power and shutdown PSA of a typical PWR.

The methodology proposed in Section 2 is used to assess and analyze the risk impact of the proposed change based on a refined PSA modeling, which requires, previously, performing a deterministic analysis to develop a more accurate model of the loss of RHRS accident scenario that accounts for an improved human error probability quantification. In section 3.2, the refined model is proposed departing from the original PSA based model (section 3.2.1), which considers the results of the thermal-hydraulic analysis presented in section 3.2.2. Based on this TH analysis, the HEP is re-calculated and presented in section 3.2.3. All previous results help to build the refined model of the loss of RHRS accident scenario, which is presented is section 3.2.4. In sections 3.3 and 3.4, the results of the assessment and analysis of the risk impact of completion time change are presented using the new model.

3.1 System description and CT change proposal

The RHRS consists of two independent, redundant mechanical subsystems, each of which receives electrical power from one of two separate and redundant electrical power trains. Each subsystem consists of one motor pump, one heat exchanger, and the required piping, valves, and instrumentation. The primary function of the RHRS is to remove the decay heat from the core and reduce the temperature of the Reactor Coolant System (RCS) during plant cool down and refueling operations.

In hot shutdown conditions (NPP Mode 4), one train of the RHRS removes the residual heat from the core. When the RHRS loses the operational train, the emergency procedures require checking the availability of the redundant train, which is normally in standby. A human action (HA1) is required to start the redundant train manually. If the standby train is not recovered, an alternative way of cooling the core is to use the initial water

inventory of the Steam Generators (SGs) on the secondary, which are under wet conservation conditions. However, the Auxiliary Feed Water System (AFWS) must start to prevent the SGs from drying out. A human action (HA2) is required to start the AFWS pumps manually. If it is not possible to remove the heat by means of Steam Generators, the "Feed and Bleed" (FB) function is required. Charge pumps feeding water can recover the lost inventory and maintain the cooling down as the residual heat is evacuated through a pressurizer relief valve or a RHRS safety valve. In this case, it is necessary to restore the refueling water storage tank (RWST) to maintain the plant in stable conditions in the end.

The Technical Specifications of the original low power and shutdown PSA established that RHRS can be inoperable only for 1 hour, i.e. a Completion Time of 1 hour when it operates in cold shutdown conditions (Mode 4). The limiting conditions for operation specifically state that RHRS pumps can be de-energized for a time of one hour. The CT change proposed consists of extending the current CT from 1 to 24 h.

3.2 Modeling of risk impact

3.2.1 Original PSA model

The low power and shutdown PSA Level 1 of a typical PWR is used as a reference model. The original event tree for a loss of one RHRS train with the NPP in Mode 4 includes the next three safety functions, as shown in Fig. 2.

The first safety function, E1, states that the SG is an alternative way of evacuating residual heat. Conservatively, it refers to only two SGs, whose inventory must be recovered through AFWS motor pumps.

The second function, F4, deals with manual FB operation and consists of manual feed and bleed with a charging pump and gravity feed RWST.

The third function, TA1, refills the RWST. The water inventory must be maintained through the charging pump RWST to ensure that the residual heat is removed from the reactor core.

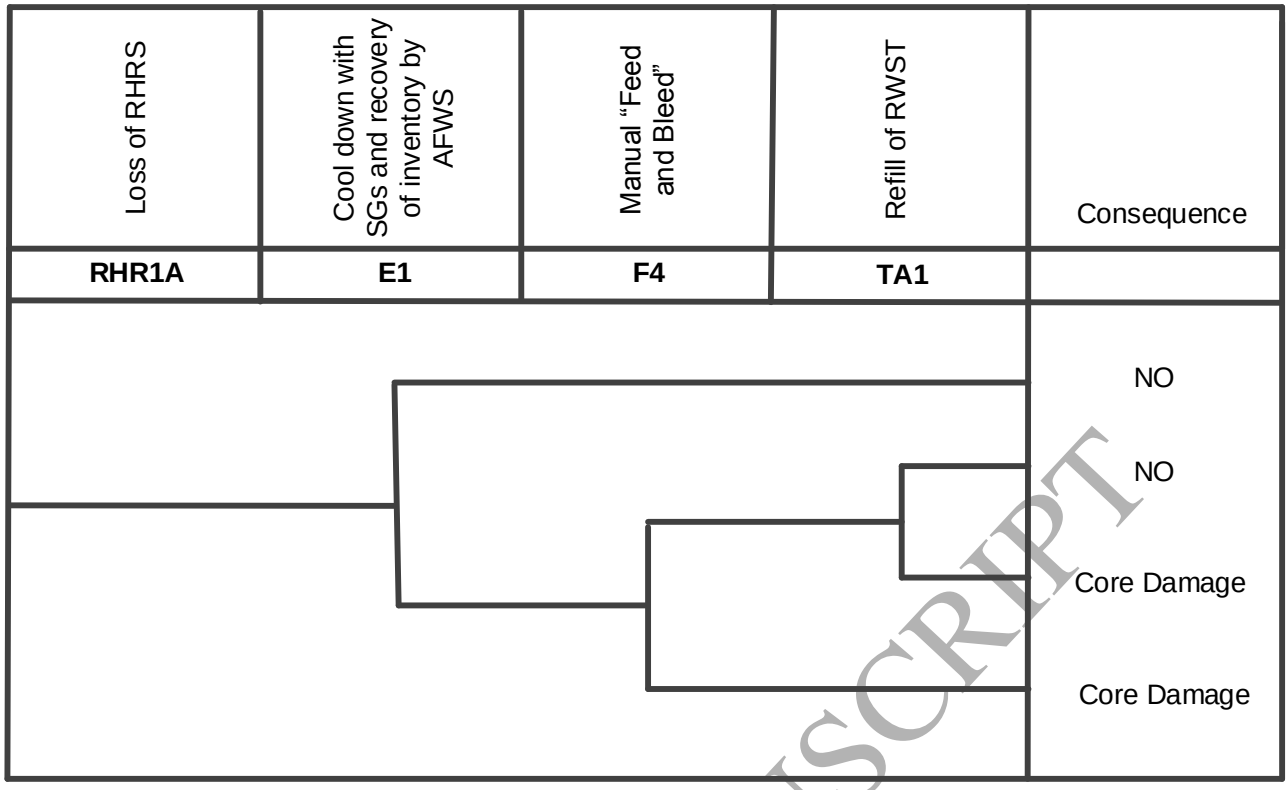

Fig. 2 Original model of the loss of the RHRS event tree

Therefore, in the original low power and shutdown PSA model, the possibility of recovering the RHRS train in service is not taken into account, i.e. HA1 is not accounted for. It is assumed that the core power at that moment of the loss of the operational RHRS train is high enough and the temperature threshold to start the standby RHRS train is soon exceeded, not leaving any time available for the operator to start the redundant RHRS train. So that, it is not given credit to HA1.

3.2.2 Deterministic model

A typical 3-loop PWR NPP has been modeled for TRACE code and run with version V5.0 Patch 4 [36], using the SNAP suite to simulate the accident sequences shown in Fig.2. The TH model of the RHRS developed is linked with the primary system, which is described in detail in Ref.[37].

This TH model is used to study the time window available for the operator to perform HA1 to start the standby RHRS train along the transient evolution, where a set of TH simulations are run considering uncertainty of TH parameters.

For example, one of the most important parameters involves the time at which the IE occurs once the plant has entered the low power operational mode. Fig. 3 considers the IE may occur randomly in the interval ranging from 100s after the beginning of hot shutdown conditions until 2000s. This period represents approximately the boundary between hot shutdown (Mode 4) and cold shutdown (Mode 5) conditions, with the plant in a normal cool down. Fig. 3 shows the evolution of RCS temperature (T_{RCS}) during the accident sequence for several simulations considering the first accidental sequence in Fig.2, where SGs act as alternative way of cooling the core. The evolution of the transient suggests the possibility of starting the standby RHRS train just after the IE occurrence, as there is enough time since the operating RHRS train is lost until the RCS temperature increases above the threshold (T_{limit}) to allow starting the standby RHRS train through HA1. It is also possible to recover the RHRS later, as soon as operating conditions permit depending on the role played by the SGs as described in the following.

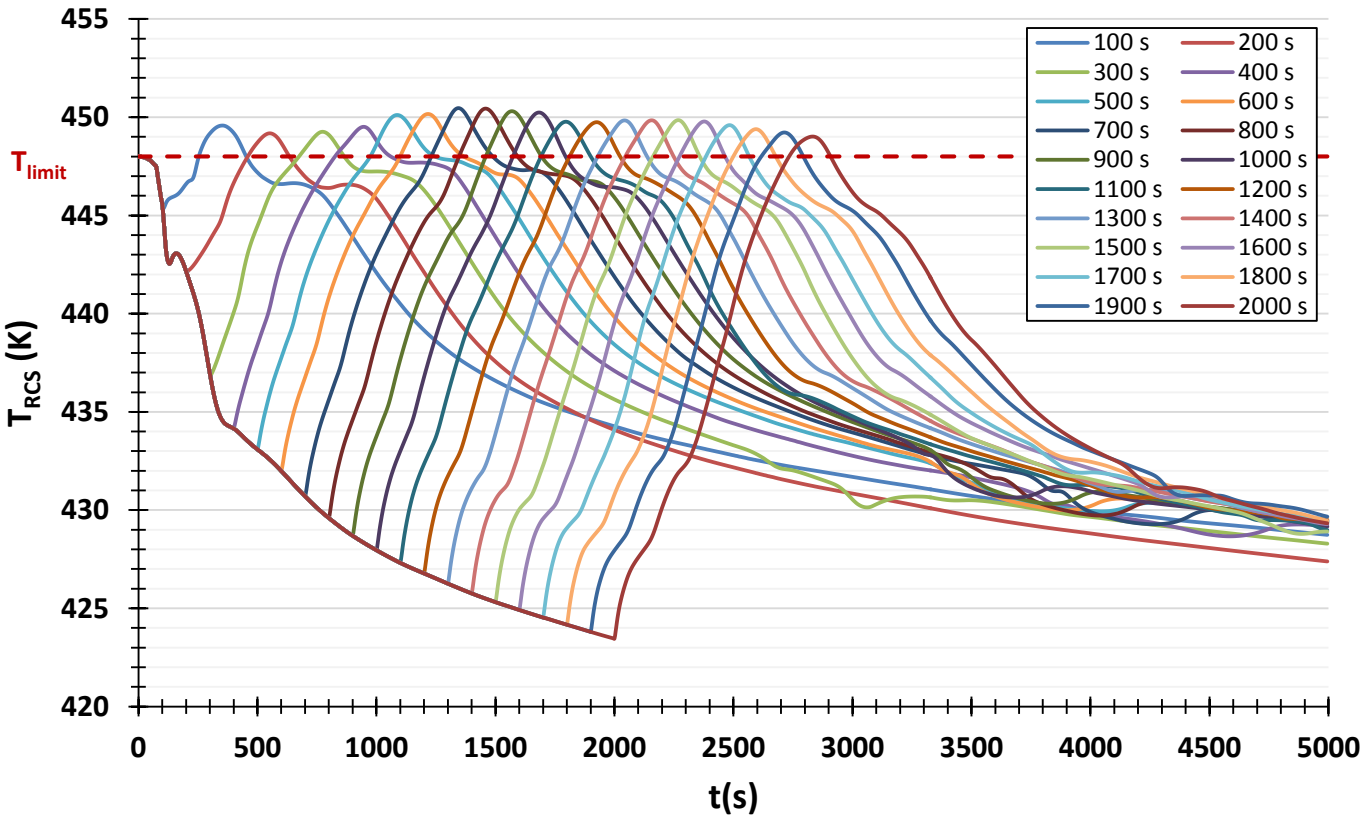

Fig. 3. TH simulations for the loss of RHRS sequence

Fig. 4 shows one simulation of the IE occurrence after 1000s and clearly shows the existence of the following time windows (TWs) along the accident sequence evolution.

First, unlike the original PSA model, it is possible to start the standby RHRS train just after the operating RHRS train is lost. The available time for performing HA1 is enough to allow removing residual heat from the RCS by means of the redundant standby RHRS train. The time available for performing HA1 is TW1.

Second, after the temperature has increased above T_{limit}, the heat is removed alternatively by means of SGs, which are kept under wet conservation conditions. However, AFWS motor pumps must be started manually by mean of HA2 to avoid SGs drying out, as established in the original PSA model. The time available for performing this HA2 is TW2.

Third, SGs allows reducing the RCS temperature below T_{limit}, which allows the standby RHRS train to be started though human action HA3. The time available for performing this HA3 is TW3.

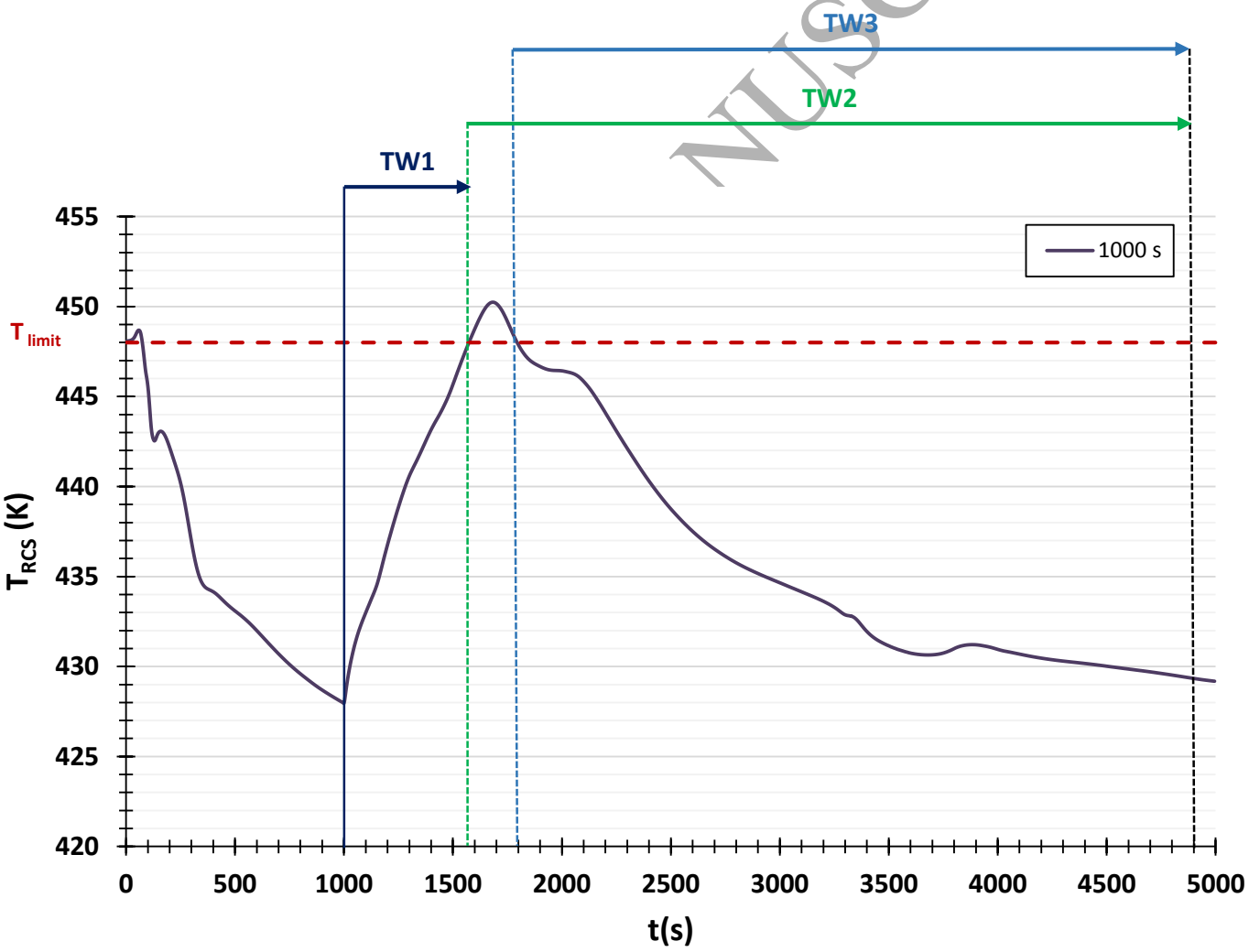

Fig. 4. Time windows available during loss of RHRS sequence

Therefore, the TH model is used to study not only the time window available for the operator to perform HA1 to start the standby RHRS train along the transient evolution, but also to study the time windows available for the operators to perform HA2 and HA3. A set of TH simulations are run considering uncertainty of TH parameters. This way, the Monte Carlo method is used adopting Latin Hypercube sampling and sample size 1000 to obtain samples of the time windows TW1, TW2 and TW3.

3.2.3 HEP quantification

Once the different time windows have been determined through TH simulations, the corresponding HEPs must be evaluated for each time window using the corresponding values of TW1, TW2 and TW3. The relationship between the human actions involved in this sequence, the TWs extracted from TH simulations and human errors are the following:

- Failure of the operator to perform HA1 to start the standby RHRS train in TW1, named FORHRS_W2
- Failure of the operator to perform HA2 to start the standby RHRS train in TW3, named FORHRS_E1
- Failure of the operator to perform HA3 to start the AFWS motor pumps in TW2, named FOAFWS_E1

Quantification of HEP depends on P_d and P_e as shown in Eq.1 in section 2.2.2. For the diagnosis phase, P_d is calculated with the TRC method for each human error FORHRS_W2, FOAFWS_E1 and FORHRS_E1 considering the corresponding time window available TW1, TW2 and TW3, respectively. The data of response time correlation versus probability of the Ref. [32] (Figure 6-1) are used considering rule-based actions and without hesitancy. This P_d probability reflects the failure probability of a wrong diagnosis in each TW. For the execution phase, the execution probability (P_e) is quantified by the THERP method. Each human action HA associated to each TW is divided and listed into human simple tasks required to perform successfully the corresponding action. Then, the failure probability of these simple tasks is estimated using Tables 20 of Ref. [33]. Operational stress is considered in this work to appear as a shaping factor in calculating Pe. High stress levels with routine or procedurally guided tasks were assumed initially, considering that the operator has a very short time to successfully perform all the tasks (see Table 17-1 of Ref.[33]). In the original situation, for human action HA1 and HA3 the operators have 1 hour at the maximum to perform these actions no matter the TW1 or TW3 available, because of the current technical specifications establish that RHRS can be inoperable just for 1 hour, i.e. a completion time of 1 hour is stablished by technical specifications.

Table 1 gives the results obtained through human reliability analysis. This table shown both two contributions, diagnosis probability (P_d) and response execution probability (P_e), as the total HEP, calculated using Eq.1, for each time window. These human error probabilities are characterized by the mean values as well as for the standard deviations of a log-normal distribution, which have been obtained by Monte Carlo simulation using Latin hypercube sampling. HEP obtained is included in the low power and shutdown PSA refined model.

Table 1. HEP obtained for each time window

		Pd		***Pe***		***HEP***	
Time window	**Basic Event**	**Mean**	**Standard deviation**	**Mean**	**Standard deviation**	**Mean**	**Standard deviation**
TW 1	FORHRS _W2	6.937E-03	2.933E-04	1.004E-02	6.145E-04	1.695E-02	1.751E-03
TW 2	FOAFWS _E1	4.914E-06	1.472E-10	1.598E-03	1.556E-05	1.603E-03	1.566E-05
TW 3	FORHRS _E1	4.159E-05	1.054E-08	1.004E-02	6.145E-04	1.008E-02	6.196E-04

3.2.4 Refined PSA model

As a result of DSA (TH simulations) and HEP quantification, it is necessary to introduce some modifications to the event tree corresponding to the loss of one train of the RHRS in the original full power and shutdown PSA available.

First, in the original low power and shutdown PSA model, the possibility of starting the standby RHRS train was not considered. It was assumed T_{limit} is soon exceeded, not leaving any time for the operator to restart the standby RHRS train. However, the TH simulations give credit to the possibility of starting the redundant train, it is to say HA1, but however with the possibility of human error FORHRS _W2 too. A new header, W2*, has been therefore added, plus a new sequence on the event tree which leads the plant to a safe state. Table 1 shows the HEP value for FORHRS _W2.

Second, TH simulations show it is possible to recover the availability of the redundant RHRS train later on in the transient evolution when the RCS temperature drops below T_{limit}. This is possible as a consequence that initial water inventory of the SGs kept under wet conditions allows it. Then, two options exist instead of just one to complete the E1 safety function, i.e. either starting AFWS motor pumps though HA2 or starting the RHRS train in standby now available through HA3. The new header is named E1*. Table 1 shows the HEP values for both human actions HA2 and HA3, i.e. FOAFWS _E1 and FORHRS _E1 respectively.

Fig. 5 shows the refined RHRS event tree considering the new header W2* and the updated header E1*. The E1* fault tree replaces the original E1 fault tree available, (see Fig. 6). These changes, together with the modified HEPs of the human actions mentioned in the previous section define the refined PSA model.

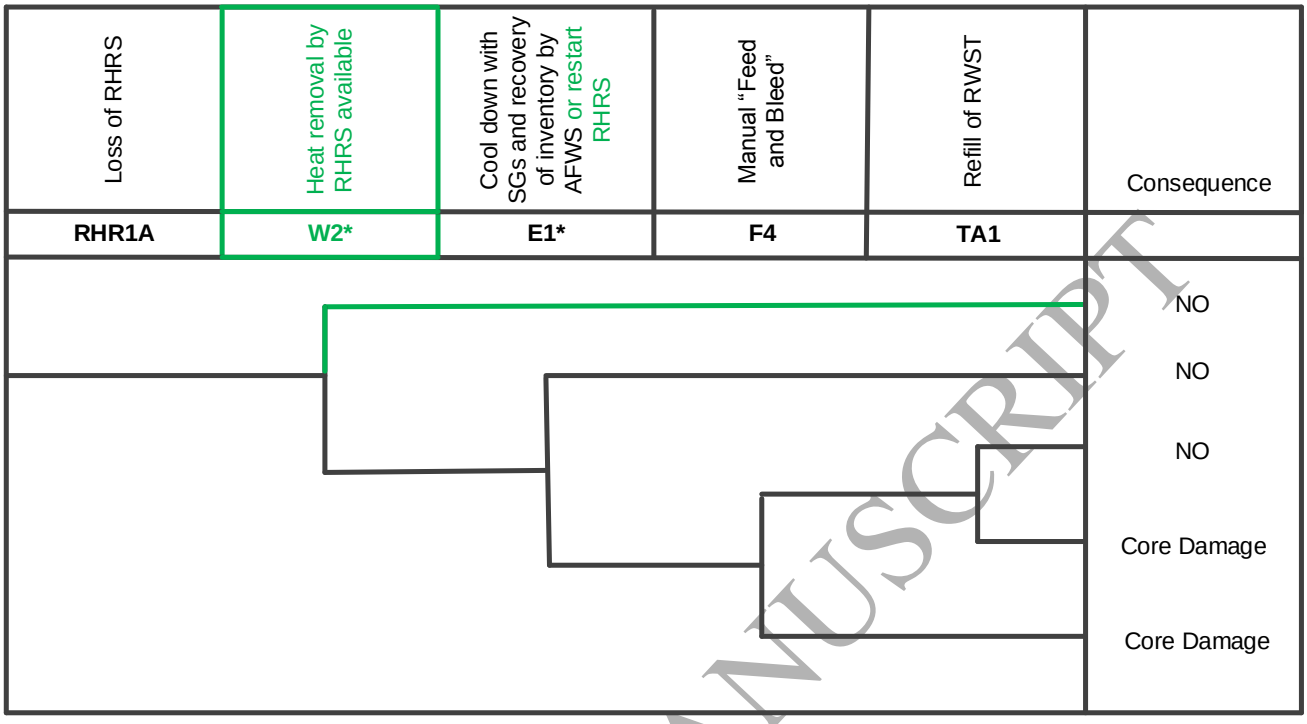

Fig. 5. Refined model of the loss of the RHRS Event Tree

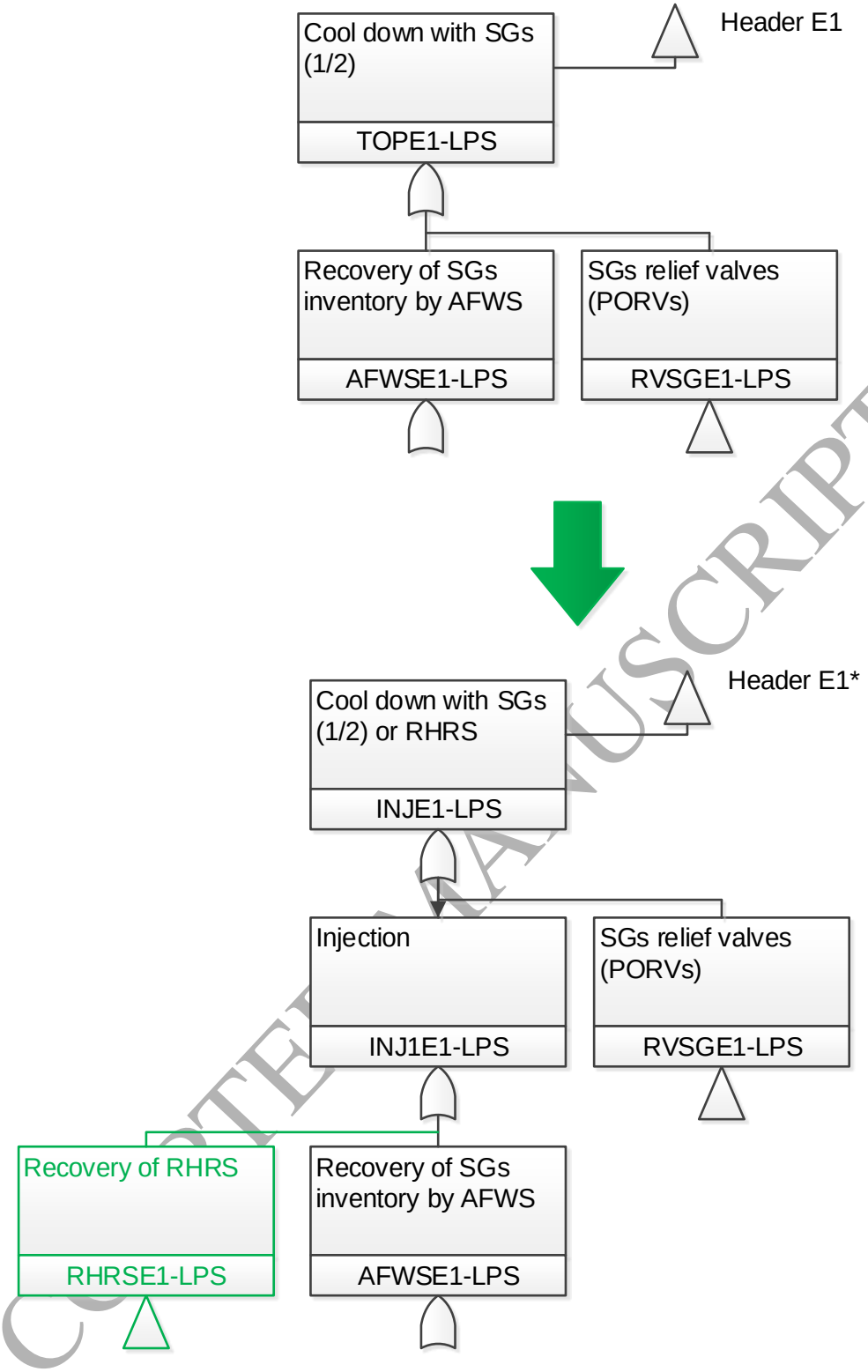

Fig. 6. E1 safety function Fault Tree modification

3.3 *Assessment of the impact on human reliability and risk of the CT change*

The CT change proposed in this work consists of extending the current completion time from 1 to 24 h for the RHRS under low power and shutdown conditions. This change implies that operators would have more time to perform the actions so that the stress level would decrease, what concerns the execution part of human action. HEP shown in Table 1 are thus reevaluated to account for the new allowed outage time. HEP and their components are calculated as explained in section 3.2.3 considering some modifications. Thus, the change only affects the response execution error probability, P_e, of human actions performed in the RHRS, i.e. HA1 and HA3. In particular, P_e is recalculated considering very low stress level (See Table 17-1 of Ref. [33]). The change does not affect the diagnostic error probability, P_d, since time windows TW1 and TW3 are lower than one hour, therefore extending from 1 to 24 hours has not impact in the human diagnosis. The results of HEP quantification after the proposed change are shown in Table 2. Note that HEPs are characterized by their mean values as well as by the standard deviation of a log-normal distribution.

Table 2. HEP obtained for each time window after CT change

		P_d		P_e		*HEP*		*ΔHEP*
Time window	**Basic Event**	**Mean**	**Standard deviation**	**Mean**	**Standard deviation**	**Mean**	**Standard deviation**	**(%)**
TW 1	FORHRS _W2	6.937E-03	2.933E-04	2.008E-03	2.458E-05	8.940E-03	4.871E-04	-89.6%
TW 2	FOAFWS _E1	4.914E-06	1.472E-10	1.598E-03	1.556E-05	1.603E-03	1.566E-05	0.0%
TW 3	FORHRS _E1	4.159E-05	1.054E-08	2.008E-03	2.458E-05	2.050E-03	2.561E-05	-391.7%

In Table 2, column 9 shows the *ΔHEP*, which measures the rise or fall in the value of HEP calculated in Table 1. The results show that the HEP of HA1 and HA3 were considerably reduced after the CT change.

Once the new HEP have been derived for each human action considered, the refined low power and shutdown PSA Level 1 is used to calculate the appropriate risk, i.e. CDF_1 and CDF_0 basic risk measures, which allow quantifying the conditional risk metric, ΔCDF_M, using Eq. 2.

CT was adopted instead of the mean downtime for maintenance d_M to quantify the second risk metric, i.e. the single-event CT risk given by Eq. 3, i.e. $ICCDP_M$.

The frequency of entering LCO was estimated using maintenance data available from a real NPP, i.e. f_M = 0.00137 years^{-1}. Note that this parameter is required to quantify the yearly CT risk, CDF, using Eq. 3, and thus also quantifying the third risk metric, i.e. ΔCDF given by Eq. 7.

Table 3 gives the results of CDF_1 and $ICCDP_M$ risk metrics before and after the change. Table 4 contains the results of *CDF* and ΔCDF risk metrics including not only mean values but also percentiles.

Table 3. Impact of the CT change in CDF_1 and $ICCDP_M$

Study	CDF_1 **(year^{-1})**			$ICCDP_M$ **(-)**		
	Mean	**5% percentile**	**95% percentile**	**Mean**	**5% percentile**	**95% percentile**
Refined PSA model [CT=1h]	1.18E-05	5.20E-06	2.33E-05	3.76E-10	1.67E-10	7.65E-10
Refined PSA model [CT=24h]	1.12E-05	5.07E-06	2.21E-05	8.88E-09	3.89E-09	1.84E-08

Table 4. Impact of the CT change in ΔCDF

Study	*CDF* **(year^{-1})**			ΔCDF **(-)**		
	Mean	**5% percentile**	**95% percentile**	**Mean**	**5% percentile**	**95% percentile**
Refined PSA model [CT from 1 to 24 h]	8.59E-06	3.83E-06	1.57E-05	1.17E-11	5.10E-12	2.41E-11

3.4 Acceptance of Risk Impact

This section compares the results shown in the previous section with the acceptance criteria established in RG 1.174 and RG 1.177.

First, the couple {*CDF*, ΔCDF} has to be placed in the corresponding decision region linked to the first acceptance criterion in RG 1.174. The numerical acceptance guidelines given in RG 1.174, and also in RG 1.177, in terms of regions defined in the space of values {*CDF*, ΔCDF}, are used to compare the results of the impact on risk of the Completion Time change, including the reevaluation of HEPs, (see Fig. 7). According to RG 1.174, because of the way the acceptance guidelines were developed, the appropriate numerical measures to use in comparing the PRA results with the acceptance guidelines are mean values, which refer to the means of the probability distributions that result from the propagation of the uncertainties on the input parameters and the model uncertainties explicitly represented in the model (middle point for each set in Fig. 7). The results before and after the CT change, including the reevaluation of HEPs, confirm that the guidelines are still met, even under the alternative assumptions, i.e. change remains in the appropriate region including not only mean values but also percentiles, as seen in Fig. 7.

Couples {CDF_1, $ICCDP_M$} are also compared against the second acceptance criterion established in RG 1.177 (see Fig. 8). The results of the completion time change, including the reevaluation of HEPs, remain in the appropriate region and include not only mean values but also percentiles, as seen in Fig. 8.

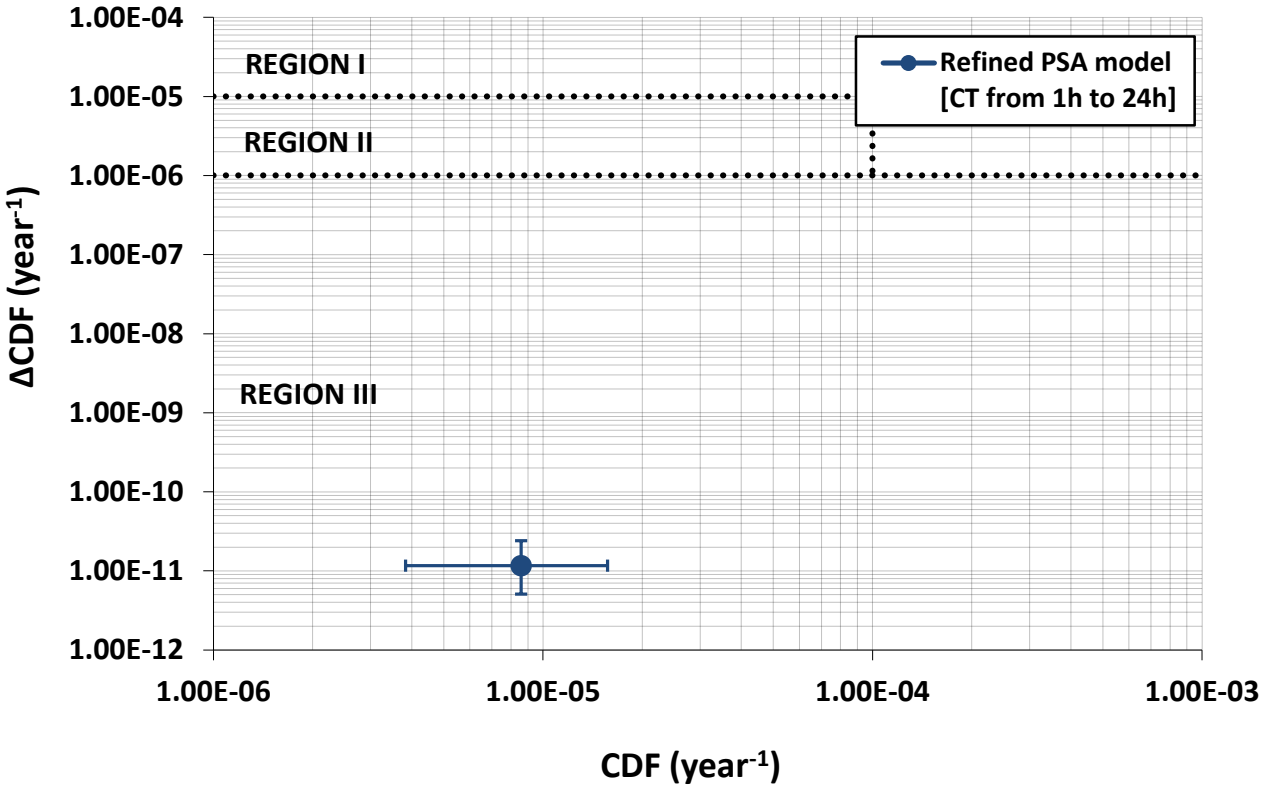

Fig. 7 Impact of the CT change on {CDF, ΔCDF}

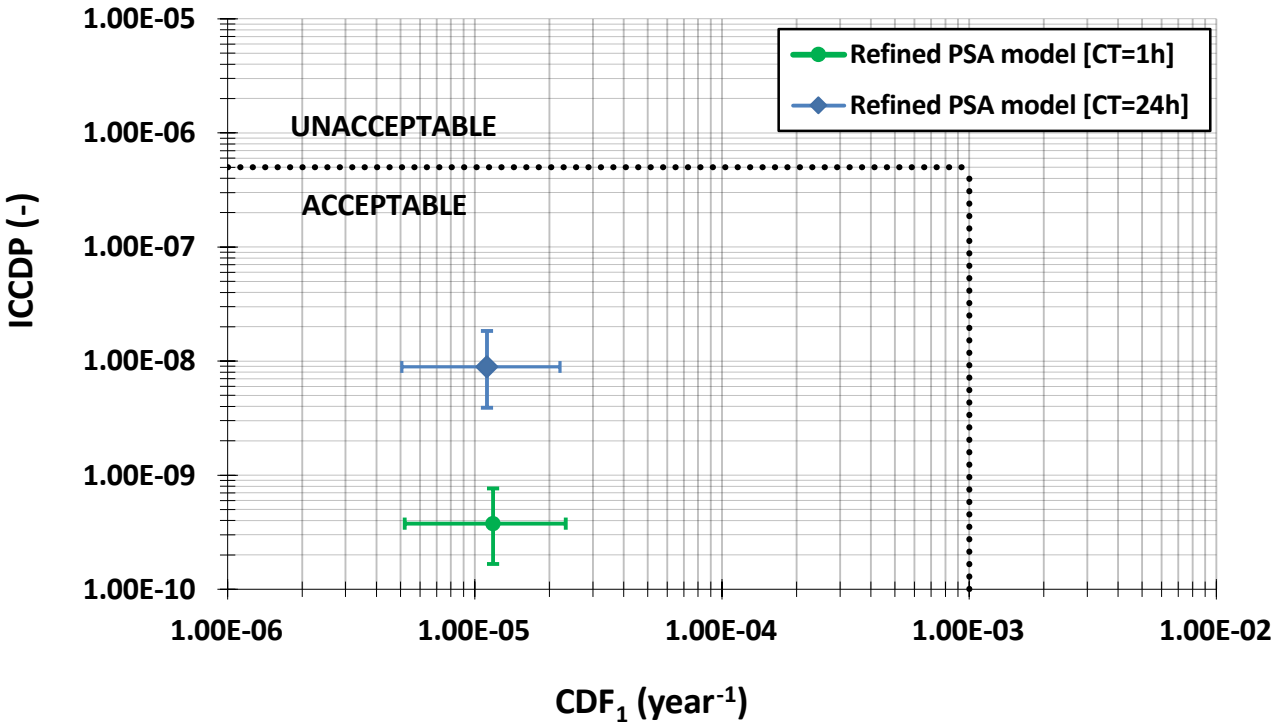

Fig. 8 Impact of the CT change on {CDF_1, $ICCDP$}

4 CONCLUDING REMARKS

This paper proposes a three-step approach for evaluation of the risk impact of changes to the licensing basis, especially on analyzing changes to completion times within NPP technical specifications, using a low power and shutdown Level 1 PSA, refined through DSA and HRA. This approach to evaluating the risk impact involves the appropriate treatment and analysis of the risk impact of model and parameter uncertainties and focuses on improvements to risk modeling, highlighting the improvements derived from combining deterministic and probabilistic approaches, together with HRA. Best estimate thermal hydraulic simulations are used not only to give credit to unknown false conservatism scenarios, but also to contribute to more accurate quantification of the HEPs, obtaining the TWs available for the operators to perform an human actions.

A case study is described focusing on a Completion Time change of the residual heat removal system of a PWR in low power and shutdown conditions. The couple {CDF, ΔCDF} is compared against the acceptance criterion established in RG 1.174 for evaluating the risk impact of whatever change to the licensing basis. The CT change can be considered acceptable from a risk point of view. In the same way couples {CDF_1, $ICCDP$}

are compared against the second acceptance criterion established in RG 1.177. The reevaluation of HEPs, taking into account operator stress as a PSF, shows a drop in CDF_1, which is consistent with lower HEP mean values. In contrast, the increased CT indicates a higher *ICCDP*, although the risk from the proposed change, i.e. CT change from 1h to 24h, remains acceptable.

It can therefore be concluded that the joint use of best estimate codes and HRA methods could be useful for evaluating the risk impact of changes to CT within NPP TS, while being consistent with the principles of the risk-informed decision making proposed by the regulatory bodies and addressing both model and parameter uncertainties.

ACKNOWLEDGMENTS

The authors are grateful to the Spanish Ministry of Science and Innovation for the financial support received (Research Projects ENE2013-45540-R and ENE2016-80401-R) and the doctoral scholarship awarded (BES-2014-067602). The study also received financial support from the Spanish Research Agency and the European Regional Development Fund.

REFERENCES

[1] USNRC. Use of probabilistic risk assessment methods in nuclear activities: final policy statement. 2015;60:42622–9.

[2] USNRC. RG 1.174. An approach for using probabilistic risk assessment in risk-informed decisions on plant-specific changes to the licensing basis, Revision 2. 2011.

[3] USNRC. RG 1.177. An approach for plant-specific, risk-informed decision making: technical specifications, Revision 1. 2011.

[4] USNRC. RG 1.200. An approach for determining the technical adequacy of probabilistic risk assessment results for risk-informed activities, Revision 2. 2009.

[5] USNRC. NUREG-1855. Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decisionmaking, Final Report (Revision 1). 2009.

[6] USNRC. NUREG/CR-6141 Handbook of methods for risk-based analyses of technical specifications. Washington DC: 1995.

[7] EPRI. Practical Guidance on the Use of PRA in Risk-Informed Applications with a Focus on the Treatment of Uncertainty. EPRI-1026511, Draft Report. 2012.

[8] Volkanovski M., Cepin M. Implication of PSA uncertainties on risk-informed decision making. Nuclear Engineering and Design 2011, 241:1108-1113. doi:10.1016/j.nucengdes.2010.02.041

[9] Zio E., The future of risk assessment . Reliability Engineering &System Safety 2018, Available online 25 April 2018. doi: 10.1016/j.ress.2018.04.020

[10] Martorell S, Martón I, Villamizar M, Sánchez AI, Carlos S. Evaluation of risk impact of changes to Completion Times addressing model and parameter uncertainties. Reliability Engineering & System Safety 2014;130:190–201. doi:10.1016/j.ress.2014.06.003.

[11] Martorell S, Villamizar M, Martón I, Villanueva JF, Carlos S, Sánchez AI. Evaluation of risk impact of changes to surveillance requirements addressing model and parameter uncertainties. Reliability Engineering & System Safety 2014;126:153–65. doi:10.1016/j.ress.2014.02.003.

[12] USNRC. NUREG-1764. Guidance for the Review of Changes to Human Actions 1994.

[13] Prošek A, Čepin M. Success criteria time windows of operator actions using RELAP5/MOD3.3 within

human reliability analysis. Journal of Loss Prevention in the Process Industries 2008;21:260–7. doi:10.1016/j.jlp.2007.06.010.

[14] Karanki DR, Rahman S, Dang VN, Zerkak O. Epistemic and aleatory uncertainties in integrated deterministic and probabilistic safety assessment: Tradeoff between accuracy and accident simulations. Reliability Engineering & System Safety 2017;162:91–102. doi:10.1016/j.ress.2017.01.015.

[15] Prasad M, Gaikwad AJ. Human error probability estimation by coupling simulator data and deterministic analysis. Progress in Nuclear Energy 2015;81:22–9. doi:10.1016/j.pnucene.2015.01.008.

[16] Voronov R, Alzbutas R. Probabilistic analysis of operators actions at the ignalina nuclear power plant taking account of the specific conditions of accident sequences. Atomic Energy 2011;110:297. doi:10.1007/s10512-011-9425-1.

[17] Lee DD, Lim H-G, Yoon HY, Jeong JJ. Improvement of the LOCA PSA model using a best-estimate thermal-hydraulic analysis. Nuclear Engineering and Technology 2014;46:541–6. doi:10.5516/NET.02.2014.003.

[18] IAEA. INSAG-25 .A Framework for Integrated Risk-Informed Decision Making Process. Vienna: 2011.

[19] Di Maio F, Rai A, Zio E. A dynamic probabilistic safety margin characterization approach in support of Integrated Deterministic and Probabilistic Safety Analysis. Reliability Engineering & System Safety 2016;145:9–18. doi:10.1016/j.ress.2015.08.016.

[20] Ibánez L, Hortal J, Queral C, Gómez-Magán J, Sánchez-Perea M, Fernández I, et al. Application of the Integrated Safety Assessment methodology to safety margins. Dynamic Event Trees, Damage Domains and Risk Assessment. Reliability Engineering & System Safety 2016;147:170–93. doi:10.1016/j.ress.2015.05.016.

[21] Borysiewicz M, Kowal K, Potempski S. An application of the value tree analysis methodology within the integrated risk informed decision making for the nuclear facilities. Reliability Engineering & System Safety 2015;139:113–9. doi:10.1016/j.ress.2015.02.013.

[22] Hess SM. Risk managed technical specifications. Progress in Nuclear Energy 2009;51:393–400. doi:10.1016/j.pnucene.2008.11.002.

[23] Caruso MA, Cheok MC, Cunningham MA, Holahan GM, King TL, Parry GW, et al. An approach for

using risk assessment in risk-informed decisions on plant-specific changes to the licensing basis. Reliability Engineering & System Safety 1999;63:231–42. doi:https://doi.org/10.1016/S0951-8320(98)00038-6.

[24] IAEA. Deterministic Safety Analysis for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-2. 2010.

[25] Wilson GE. Historical insights in the development of Best Estimate Plus Uncertainty safety analysis. Annals of Nuclear Energy 2013;52:2–9. doi:10.1016/j.anucene.2012.03.002.

[26] Vaurio JK. Human factors, human reliability and risk assessment in license renewal of a nuclear power plant. Reliability Engineering & System Safety 2009;94:1818–26. doi:https://doi.org/10.1016/j.ress.2009.05.014.

[27] ASME. Standard for Probabilistic Risk Assesment for Nuclear Power Plant Applications. 2000.

[28] Alvarenga MAB, Frutuoso e Melo PF, Fonseca RA. A critical review of methods and models for evaluating organizational factors in Human Reliability Analysis. Progress in Nuclear Energy 2014;75:25–41. doi:10.1016/J.PNUCENE.2014.04.004.

[29] Bell J, Holroyd J. Review of human reliability assessment methods. Health and Safety Laboratory, United Kingdom 2009.

[30] USNRC. NUREG-1792. Good Practices for Implementing Human Reliability Analysis (HRA) 2005.

[31] USNRC. NUREG-1842. Evaluation of Human Reliability. Analysis Methods. Against Good Practices. 2006.

[32] Hall RE, Fragola J, Wreathall J. Post-event human decision errors: operator action tree/time reliability correlation. United States: 1982. doi:10.2172/6460666.

[33] Swain AD, Guttmann HE. Handbook of human-reliability analysis with emphasis on nuclear power plant applications. Final report. NUREG/CR-1278 1983.

[34] Dougherty EM, Fragola JR. Foundations for a time reliability correlation system to quantify human reliability. Conference Record for 1988 IEEE Fourth Conference on Human Factors and Power Plants, 1988, p. 268–78. doi:10.1109/HFPP.1988.27513.

[35] IAEA. Safety of Nuclear Power Plants : Desgin, IAEA Safety Standards Series No. SSR-2/1 (Rev. 1). 2016.

[36] USNRC. TRACE V5.840 User's and Theory manuals. 2014.

[37] Martorell S, Sánchez-Sáez F, Villanueva JF, Carlos S. An extended BEPU approach integrating probabilistic assumptions on the availability of safety systems in deterministic safety analyses. Reliability Engineering & System Safety 2017;167:474–83. doi:https://doi.org/10.1016/j.ress.2017.06.020.