

KEPCO International Nuclear Graduate School

**Estimation of Human Error Probability during  
SGTR Accident in Angra-2 NPP using SPAR-H and  
IDHEAS-ECA**



AN INDIVIDUAL PROJECT REPORT SUBMITTED TO THE FACULTY OF  
GRADUATE SCHOOL  
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF  
MASTER OF ENGINEERING  
NUCLEAR POWER PLANT ENGINEERING

by

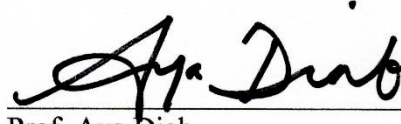
*Diogo Tertuliano Fernandes Pires*

December 2023

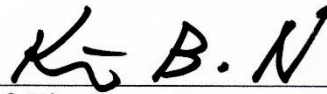
[This page is blank]

The individual project report of Diogo Tertuliano Fernandes Pires is approved.

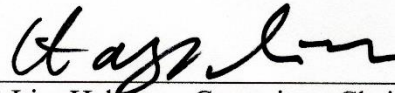
Examination Committee Members:



Prof. Aya Diab



Prof. Kim Bum-nyun



Prof. Lim Hak-kyu, Committee Chair

KEPCO International Nuclear Graduate School

December 2023

## [TABLE OF CONTENTS]

<b>[TABLE OF CONTENTS]</b> .....	<b>iii</b>
<b>[LIST OF FIGURES]</b> .....	<b>v</b>
<b>[LIST OF TABLES]</b> .....	<b>vi</b>
<b>[ACKNOWLEDGEMENTS]</b> .....	<b>viii</b>
<b>[VITA]</b> .....	<b>xi</b>
<b>[REFERENCE LIST]</b> .....	<b>xi</b>
<b>[ABSTRACT OF THE INDIVIDUAL PROJECT REPORT]</b> .....	<b>xiv</b>
<b>1 INTRODUCTION</b> .....	<b>1</b>
<b>1.1 PURPOSE OF THIS STUDY</b> .....	<b>3</b>
<b>2 PLANT FAMILIARIZATION</b> .....	<b>5</b>
<b>2.1 COMPARISON BETWEEN ANGRA-2 AND APR-1400</b> .....	<b>7</b>
<b>3 METHODOLOGY</b> .....	<b>18</b>
<b>3.1 ANGRA-2 HRA METHODOLOGIES</b> .....	<b>20</b>
<b>3.2 SPAR-H</b> .....	<b>22</b>
<b>3.3 IDHEAS-ECA</b> .....	<b>23</b>
<b>4 SGTR ACCIDENT ASSESSMENT</b> .....	<b>29</b>
<b>4.1 DESCRIPTION OF SGTR PHENOMENA IN ANGRA-2</b> .....	<b>29</b>
<b>4.2 SGTR EVENT TREE DEVELOPMENT FOR ANGRA-2</b> .....	<b>36</b>
<b>4.3 HFE IDENTIFICATION FOR SGTR IN ANGRA-2</b> .....	<b>53</b>
<b>4.4 TASK ANALYSIS OF THE HFE IDENTIFIED FOR ANGRA-2 DURING SGTR</b> <b>55</b>	
4.4.1 Identification Of Error Modes .....	57
4.4.2 HFE Definition .....	65
4.4.3 Timeline Analysis.....	71
<b>5 CURRENT ANGRA-2 HRA ASSESSMENT AND HEP RESULTS</b> .....	<b>77</b>
<b>5.1 BRIEFLY DESCRIPTION OF ANGRA-2 HRA</b> .....	<b>77</b>
<b>5.2 HEP RESULTS FROM ANGRA-2 HRA FOR THE HFE CONSIDERED ...</b> <b>78</b>	
5.2.1 HFE1: Identification and Isolation of affected SG .....	78
5.2.2 Cooldown RCS at 50K/h by TBV/ADV/MSSV.....	78
5.2.3 Drain the feedwater tank (LAA) in case of SG feedwater pump failure .....	78
5.2.4 Replenish emergency feedwater tanks (LAR) for RCS long term cooling.....	79
<b>6 HRA ASSESSMENT BY SPAR-H</b> .....	<b>80</b>
<b>6.1 HEP QUANTIFICATION FOR HFE1</b> .....	<b>80</b>
<b>6.2 HEP QUANTIFICATION FOR HFE2</b> .....	<b>85</b>
<b>6.3 HEP QUANTIFICATION FOR HFE3</b> .....	<b>88</b>

<b>6.4</b>	<b>HEP QUANTIFICATION FOR HFE4 .....</b>	<b>93</b>
<b>6.5</b>	<b>DEPENDENCY ANALYSIS OF HFE1 AND HFE2.....</b>	<b>99</b>
<b>7</b>	<b>HRA ASSESSMENT BY IDHEAS-ECA.....</b>	<b>103</b>
<b>7.1</b>	<b>HFE1: IDENTIFICATION AND ISOLATION OF AFFECTED SG (I&amp;I-SG) 104</b>	
7.1.1	Step 1: Scenario Analysis .....	104
7.1.2	Step 2: Analyzing Human Failure Events (HFE) .....	110
7.1.3	Step 3: Modeling Failure of critical tasks .....	112
7.1.4	Step 4: Assessing Performance Influencing Factor Attributes Applicable to CFM .....	115
7.1.5	Step 5: Estimation of $P_C$ – The sum of HEP of CFM .....	119
7.1.6	Step 6: Estimation of $P_T$ – the convolution of the distribution of $T_{avail}$ and $T_{req}$ .....	119
7.1.7	Step 7: Calculate the overall HEP .....	120
7.1.8	Step 8 – Dependency Analysis .....	121
<b>7.2</b>	<b>HFE2: COOLDOWN RCS AT 50K/H BY TBV/ADV/MSSV.....</b>	<b>121</b>
7.2.1	Step 1: Scenario Analysis .....	121
7.2.2	Step 2: Analyzing Human Failure Events (hfe).....	122
7.2.3	Step 3: Modeling Failure of critical tasks .....	124
7.2.4	Step 4: Assessing Performance Influencing Factor Attributes Applicable to CFM .....	126
7.2.5	Step 5: Estimation of $P_C$ – The sum of HEP of CFM .....	127
7.2.6	Step 6: Estimation of $P_T$ – the convolution of the distribution of $T_{avail}$ and $T_{req}$ .....	128
7.2.7	Step 7: Calculate the overall HEP .....	128
7.2.8	Step 8 – Dependency Analysis .....	129
<b>7.3</b>	<b>HFE3: DRAIN THE FEEDWATER TANK (LAA) IN CASE OF SG FEEDWATER PUMP FAILURE .....</b>	<b>144</b>
7.3.1	Step 1: Scenario Analysis .....	144
7.3.2	Step 2: Analyzing Human Failure Events (hfe).....	146
7.3.3	Step 3: Modeling Failure of critical tasks .....	149
7.3.4	Step 4: Assessing Performance Influencing Factor Attributes Applicable to CFM .....	151
7.3.5	Step 5: Estimation of $P_C$ – The sum of HEP of CFM .....	154
7.3.6	Step 6: Estimation of $P_T$ – the convolution of the distribution of $T_{avail}$ and $T_{req}$ .....	155
7.3.7	Step 7: Calculate the overall HEP .....	155
7.3.8	Step 8 – Dependency Analysis .....	156
<b>7.4</b>	<b>HFE4: REPLENISH EMERGENCY FEEDWATER TANKS FOR RCS LONG TERM COOLING .....</b>	<b>157</b>
7.4.1	Step 1: Scenario Analysis .....	157
7.4.2	Step 2: Analyzing Human Failure Events (hfe).....	159
7.4.3	Step 3: Modeling Failure of critical tasks .....	161
7.4.4	Step 4: Assessing Performance Influencing Factor Attributes Applicable to CFM .....	164
7.4.5	Step 5: Estimation of $P_C$ – The sum of HEP of CFM .....	168
7.4.6	Step 6: Estimation of $P_T$ – the convolution of the distribution of $T_{avail}$ and $T_{req}$ .....	168
7.4.7	Step 7: Calculate the overall HEP .....	169
7.4.8	step 8 – dependency analysis .....	170
<b>8</b>	<b>RESULTS AND DISCUSSION .....</b>	<b>171</b>
<b>9</b>	<b>CONCLUSION .....</b>	<b>178</b>

## [LIST OF FIGURES]

Figure 1 - Aerial photo from Angra-1 and Angra-2 NPP site.....	5
Figure 2 – Angra-2 OP flowchart .....	13
Figure 3 – APR-1400 OP flowchart.....	16
Figure 4 – SPAR-H framework .....	23
Figure 5 – Illustration of the IDHEAS-ECA process .....	25
Figure 6 – IDHEAS-ECA framework.....	26
Figure 7 – Angra-2 SGTR Event tree .....	48
Figure 8 – HTA for HFE: Identification and Isolation of affected SG.....	56
Figure 9 - HTA for the HFE: Cooldown RCS at 50K/h by TBV/ADV/MSSV .....	57
Figure 10 - Timeline diagram for HFE1 .....	73
Figure 11 - Timeline diagram for HFE2 .....	74
Figure 12 - Timeline diagram for HFE3 .....	75
Figure 13 - Timeline diagram for HFE4.....	76
Figure 14 – $P_c$ estimation for HFE1 .....	119
Figure 15 - $P_t$ estimation for HFE1 .....	120
Figure 16 - $P_c$ estimation for HFE2 .....	128
Figure 17 - $P_t$ estimation for HFE2 .....	128
Figure 18 – IDHEAS-DEP dependency analysis process.....	130
Figure 19 - $P_c$ estimation for HFE3 .....	155
Figure 20 – $P_t$ estimation for HFE3 .....	155
Figure 21 - $P_c$ estimation for HFE4 .....	168
Figure 22 - $P_t$ estimation for HFE4.....	168

## [LIST OF TABLES]

Table 1 – Typical information for HRA .....	18
Table 2 – PIFs in IDHEAS-ECA .....	27
Table 3 – Procedure analysis based on CSF affected by human/system action .....	36
Table 4 – Top event description of SGTR event tree .....	48
Table 5 – Accident sequence description base on affected CSF .....	52
Table 6 – SHERPA error taxonomy .....	58
Table 7 – Additional cognitive items to augment the SHERPA taxonomy.....	58
Table 8 – Error modes applied for HFE: Identification and Isolation of affected SG.	59
Table 9 – Angra-2 HRA HEP result for HFE1 .....	78
Table 10 - Angra-2 HRA HEP result for HFE2.....	78
Table 11 - Angra-2 HRA HEP result for HFE3.....	78
Table 12 - Angra-2 HRA HEP result for HFE4.....	79
Table 13 – SPAR-H dependency table .....	100
Table 14 - Baseline scenario .....	106
Table 15 – Summary of HEP Quantification for HFE1.....	120
Table 16 - Summary of HEP Quantification for HFE2 .....	129
Table 17 – Predetermination analysis for HFE1 and HFE2 .....	132
Table 18 – R1: Functions or systems cognitive dependency.....	133
Table 19 - R1: Functions or systems Consequential dependency.....	134
Table 20 - R1: Functions or systems resource-sharing dependency.....	136
Table 21 – R2: Time proximity consequential dependency .....	137
Table 22 – R3: Personnel cognitive dependency.....	138
Table 23 - R3: Personnel consequential dependency .....	139
Table 24 - R3: Personnel resource-sharing dependency.....	140

Table 25 – R4: Location consequential dependency .....	141
Table 26 – R5: Procedure cognitive dependency .....	143
Table 27 - Summary of HEP Quantification for HFE3 .....	156
Table 28 - Summary of HEP Quantification for HFE4 .....	169
Table 29 – Total HEP result for each HFE .....	172
Table 30 – Dependency HEP results .....	175



## [ACKNOWLEDGEMENTS]

I am immensely grateful to God, whose grace and guidance have been my constant source of strength and inspiration throughout my academic journey. His blessings have illuminated my path, and i am profoundly thankful for his unwavering support.

To my parents, pillars of my existence, i express my deepest gratitude. Your sacrifices, love, and encouragement have been the driving force behind my quest for knowledge. Thank you for the education you gave me and through it comes my strength and courage to face and complete this master's degree.

To my wife, my rock and confidant, thank you for your boundless love, understanding, and patience. Your unwavering support has been my motivation to persevere through challenges. You took care of me and your son like a warrior and without measuring efforts. I will be forever grateful for the sacrifices you made to see me succeed and all this success I dedicate to you. My love, my passion, and my safe harbor.

To my son, you are my joy and inspiration. Your innocent laugh and boundless energy have been a source of motivation even on the hardest of days. I am grateful for your presence in my life and even though you are a little guy, you taught me to be strong and face life's challenges like no one else. You were a brave warrior who faced all the challenges imposed on you with manhood and was successful in all of them. You will always be an example to be followed. Bravo Zulu.

My deep gratitude to my new family in South Korea. Aunt Eun Bee-choi and Uncle Juliano welcomed my family and gave us all the care we needed to have the best

possible experience here in South Korea. I thank God for our new Korean family. My sincere thanks for all the support and companionship.

I express my sincere appreciation to Professor Lym for their guidance, mentorship, and invaluable insights. Your expertise and dedication have shaped my academic journey and expanded my horizons. I am grateful for the knowledge and wisdom you have shared with me.

I would like to express my deep gratitude to Professor Aya Diab who inspired me with all the knowledge that was transferred to me in her classes, and which was certainly part of the development of my work.

To Professor Kim Bum-nyun, thank you for opening my mind beyond the scope of Probabilistic Risk Analysis and for all the knowledge and guidance to be a leader in the nuclear power plant industry.

Special thanks to my lab teammate, Muttalab. Your collaboration and camaraderie have enriched my academic experience. Together, we overcome challenges and celebrate successes, and I am grateful for the teamwork we cultivate. You will always be a source of inspiration to me. A brother that KINGS gave me. I wish all the success in the world for you and your family.

Lastly, I extend my gratitude to the Brazilian Navy and Brazilian Defense, Naval, Army and Airforce Attaché Office in the Republic of Korea for their support and the opportunities provided during my academic pursuits. The skills and values instilled during my service have been instrumental in shaping my character and approach to challenges.

This master's degree is not just an individual achievement, but a collective triumph, made possible by the support, love and guidance of these remarkable

individuals and entities. I am truly blessed by God to have all this support and I hope to continue my journey with the knowledge and skills gained during this quest.

## [VITA]

June 23, 1980	Born, Recife, Pernambuco, Brazil.
December 20, 2006	B.S., Electronic Engineering Universidade Federal de Pernambuco (Federal University of Pernambuco) - UFPE Recife, Pernambuco, Brazil.
[Graduation year]	M.S., [Graduate major, if any] [Graduate school] [Graduate school location (city, province)]
March 16, 2009, to present	Lieutenant Commander Aramar Nuclear Instruction and Training Center Brazilian Navy

## [REFERENCE LIST]

- [1] J. Xing, Y. J. Chang, J. DeJesus Segarra, “The General Methodology of An Integrated Human Event Analysis System (IDHEAS-G),” NUREG-2198, May 2021.
- [2] J. Forest, A. Kolaczowski, E. Lois, Kelly, “Evaluation of Human Reliability Analysis Methods Against Good Practices”, NUREG-1842, September 2006.
- [3] ANGRA-2 PSA Report.
- [4] Eletrobras Eletronuclear, “Final Safety Analysis Report (FSAR) - Central Almirante Álvaro Alberto - Unit 2,” 2007 - Rev.10.
- [5] KHNP, “Final Safety Analysis Report - APR-1400”, 2018 - Rev.3.
- [6] KTA-Geschaefsstelle, “Nuclear Safety Standards Commission (KTA) – Requirements for the Operating Manual,” KTA-1201, 2015-11.
- [7] KKS – Codification system, “System, Equipment, and Components Identification for Nuclear Power Plants”, Angra-2, 2004.

- [8] Park, Jinkyun, and Wondea Jung. "OPERA—a human performance database under simulated emergencies of nuclear power plants." *Reliability Engineering & System Safety* 92.4 (2007): 503-519.
- [9] Gertman, D., Blackman, H., Marble, J., Byers, J., & Smith, C. (2005). "The SPAR-H Human Reliability Analysis Method", NUREG/CR-6883, US Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Washington, DC.
- [10] Xing, J., Chang, Y. J., & DeJesus Segarra, J. 2021a. "The General Methodology of An Integrated Human Event Analysis System (IDHEAS-G)", NUREG-2198, U.S. Nuclear Regulatory Commission.
- [11] EPRI TR-100259, "An Approach to the Analysis of Operator Actions in Probabilistic Risk Assessment," 1992.
- [12] Boring, Ronald L. "Current human reliability analysis methods applied to computerized procedures," No. INL/CON-12-25624. Idaho National Lab. (INL), Idaho Falls, ID (United States), 2012.
- [13] Swain, Alan D., and Henry E. Guttmann. "Handbook of human-reliability analysis with emphasis on nuclear power plant applications," Final report. No. NUREG/CR-1278; SAND-80-0200. Sandia National Lab. (SNL-NM), Albuquerque, NM (United States), 1983.
- [14] Boring, Ronald L. "Fifty years of THERP and human reliability analysis," No. INL/CON-12-25623. Idaho National Lab. (INL), Idaho Falls, ID (United States), 2012.
- [15] Diogo, P., Mutallab, A., Obuya, O., Lim, H., "Study of Variability Effect of Performance Influencing Factors in Human Error Probability Quantification," Kepco International Nuclear Graduating School, KINGS/PR-SC106-2023-02.
- [16] Cho, J., Hong, Y., Ko, S., Park, S., Choi, S., Lim, H., "Development of SGTR ET Based on Operating Procedures," Kepco International Nuclear Graduating School, KINGS/PR-SC106-2022-01.
- [17] Angra-2 Operational Procedures.
- [18] Boring, R. L. (2015). Defining human failure events for petroleum applications of human reliability analysis. *Procedia Manufacturing*, 3, 1335-1342.
- [19] Buddaraju, Dileep. Performance of control room operators in alarm management. Louisiana State University and Agricultural & Mechanical College, 2011.
- [20] Diogo, P., Mutallab, A., Obuya, O., Lim, H., "Comparative Study of Performance Influencing Factor in IDHEAS-G and SPAR-H," Kepco International Nuclear Graduating School, KINGS/PR-SC106-2023-01.

- [21] Xing, J., J. Chang, and J. DeJesus. "Integrated Human Event Analysis System for Event and Condition Assessment (IDHEAS-ECA)." (2020).
- [22] Park, Jooyoung, Awwal Mohammed Arigi, and Jonghyun Kim. "A comparison of the quantification aspects of human reliability analysis methods in nuclear power plants." *Annals of Nuclear Energy* 133 (2019): 297-312.
- [23] Kichline, M., Xing, J., & Chang, Y.J. (2021). Integrated human event analysis system dependency analysis guidance (IDHEAS-DEP). RIL 2021-14, Washington, DC:US Nuclear Regulatory Commission.

**[ABSTRACT OF THE INDIVIDUAL PROJECT REPORT]**

**Estimation of Human Error Probability during SGTR Accident in Angra-2 NPP  
using SPAR-H and IDHEAS-ECA**

**by**

**Diogo Tertuliano Fernandes Pires**

**Master of Engineering in Nuclear Power Plant Engineering**

**KEPCO International Nuclear Graduate School, 2023**

**Professor Hak-kyu Lim, Chair**

With the advancement of technology in nuclear industry, nuclear power reaches the state-of-the-art levels and drastically reduce risk contributions by system and equipment. However, despite significant improvements in operator conduct inside and outside the control room, the probability of human error has become relatively greater contributor to the risk of nuclear power plants. Therefore, human error analysis has become one of the biggest challenges in PRA of a nuclear power plant. Currently several human reliability analysis methodologies have been developed for specific applications which are very well established for actions taken in the main control room, however, these methods have lack of structure to assess digital control rooms or external event. In this way, NRC and EPRI developed the IDHEAS-ECA methodology as a new HRA method to replace existing and standard HRA methods. In this study, SPAR-H and IDHEAS-ECA was used to recalculate the human error probability for

identified human failure events in SGTR initiate event in Angra-2. Therefore, the results showed that IDHEAS-ECA can produce standard HEP results in comparison with consolidate HRA methods for actions taken in the main control room, however, the need for more specific guidelines is identified to reduce the variability in quantifying the probability of human errors due to the complex structure proposed by IDHEAS-ECA.



# 1 INTRODUCTION

After Three Mile Island (TMI) accident, probabilistic risk analysis (PRA) became crucial in the risk management of nuclear power plants, which can identify and recognize the key vulnerabilities of nuclear power plants thereby strengthen nuclear safety and operational efficiency.

With the advancement of technology in nuclear industry, mechanical, electrical, electronic and instrumentation components in nuclear power plants have been evolved significantly, reaching state-of-the-art levels and drastically reducing risk contributions. However, despite significant improvements in operator conduct inside and outside the control room so as to reduce human error probability (HEP) by introducing training, procedures and man-machine interface improvements, the HEP has become relatively greater contributor to the risk of nuclear power plants. This has resulted in an effort by nuclear industry to qualify and quantify human error. Therefore, human error analysis has become one of the biggest challenges in PRA of a nuclear power plant.

Currently several human reliability analysis methodologies have been developed for specific applications with weaknesses and limitations. In order to create a methodology that covers the applicability of the HRA methodologies widely used in nuclear industry with the scientific basis, the variability of results, and data analysis, the NRC created "The General Methodology of An Integrated Human Event Analysis System" (IDHEAS-ECA) [1]. In 2021, IDHEAS-ECA was released and elaborated

based on the strength of each methodology designed before to provide an enhanced tool which has a broad scope of application. It is based on scientific modeling of human cognitive – it is structured in a way to decrease variability of results from analyst to analyst and has an improved database for quantification from several domains. However, HRA for not being an exact science, regulatory bodies and HRA experts requires the adoption of standard and consolidate HRA methods established as a reference in this field. In HRA there is not right or wrong, the main goal is to maintain the consistency and reliability of HEP results. Currently, first-generation methods are highly consolidated and accepted by major regulatory entities in the United States and Brazil. Therefore, IDHEAS-ECA, as it is a relatively recent methodology, still needs to go through a consolidation process, demonstrating its ability to produce consistent and reliable results.

In this way, Angra-2 did not consider the use of IDHEAS-ECA but rather utilized a combination of other HRA methodologies. Based on NUREG-1842 [2], each methodology has its own unique application and structure to estimate the HEP and it is not possible to manage as many HRA-related situation as possible to quantify the HEP, using only one methodology. In order to compute the HEP for Angra-2, and to follow the standard methods, Electronuclear employed the concept of the Electric Power Research Institute (EPRI) approach by combining HCR/ORE+CBDTM and THERP methodologies. As such, the cognitive error was deduced from HCR/ORE+CBDTM while the THERP methodology was used to compute the execution error [3].

Electronuclear followed the EPRI approach to combine three methodologies available to contemplate all important context aspects from cognitive and execution part which affects human performance to calculate the HEP for Angra-2, but now,

IDHEAS-ECA, as a second generation methods, promises to be friendly user, can be applied for several domains, can address the cognitive and action part, and can fulfill the gaps addressed on the result obtained due to its improvement as well as its ability to limit weakness associated with other methods. Therefore, this study aims to compare the results obtained by IDHEAS-ECA, SPAR-H and those from the methods used by Angra-2 HRA to identify the qualitative and quantitative improvements which could be obtained during HEP quantification. Furthermore, the results of this study will be used to draw conclusions on how to improve the structure of the current Angra-2 procedure, which is taken as a reference for the operational procedure of Brazilian microreactors under development, enhancing the procedures that will be designed. This includes philosophically analyzing the impact on HEP considering the structure of Angra-02 operational procedures (OP) compared to that of APR.

## **1.1 PURPOSE OF THIS STUDY**

This work aims to validate the Integrated Human Event Analysis System (IDHEAS-G) method for Human Reliability Analysis (HRA) so as to ascertain its HEP accuracy, credibility, consistency, improvement, and regulatory compliance. Accuracy is important to ensure that the estimated human error probability (HEP) values are accurate and reliable. HEP values can lead to incorrect risk assessments and potentially compromise safety. Credibility of the method and the results it produces is a critical component of risk assessment in nuclear power plants, and decision-makers need to have confidence in the methods used to produce risk estimates. Consistency is important to ensure that the method produces consistent results across different applications and scenarios, and consistency HEP is necessary for making meaningful

comparisons between different risk assessments and for identifying trends and patterns in HEP values. Improvements in the method and the underlying models is important, because methods need to be continuously improved to keep pace with advances in technology and changes in the industry. Finally, validating the IDHEAS-ECA method is important for regulatory compliance. The Nuclear Regulatory Commission (NRC) has developed the IDHEAS-ECA HRA method with a plan to replace the SPAR-H HRA method, and validating the IDHEAS-ECA method is necessary to ensure compliance with NRC regulations [16]. Additionally, this work aims to build my own perspective of SGTR HRA analysis and how IDHEAS-ECA may enhance qualitatively and quantitatively the HEP result for the HFEs.

Recently, my organization embarked on the development of OP for a microreactor. In this project, Angra-2 OP is used as a base for the development of the OP. Thus, this study leverages the comparison in between APR-1400 and Angra-2 in terms of OP to make an appropriate recommendation for the enhancement of the OP under design for the microreactor project.

## 2 PLANT FAMILIARIZATION

Angra-2 NPP is located on Itaoma Beach, in Rio de Janeiro, at the extreme Southeast of Atlantic coast in the state of Rio de Janeiro, at a partially sheltered bay, surrounded by mountains whose elevations vary from 200m to 700m. It is situated between Serra do Mar and the Big Island Bay, in the region of Angra dos Reis.

The site has 500m of front and 400m of depth, with an elevation of 5m above the sea level. The nearest road is the highway Rio-Santos (BR-101). Figure 1 shown the NPP location of Angra-1 and Angra-2 NPP.



**Figure 1 - Aerial photo from Angra-1 and Angra-2 NPP site.**

Angra-2 is a PWR-style reactor with an electrical output of 1350MWe. Its model was from the old SIMENS/KWU and currently belongs to AREVA NP. This plant uses light water as a coolant and moderator, diluted boron for long-term power control and subcritical margin, and control rods for short-term power control. This design uses a proven German four-loop technology located in the reactor containment

building, which has a spherical shape made of an external concrete structure and an internal steel structure. The nuclear plant layout has the containment building at the center of the plant, surrounded by main buildings in a way that ensures the system and components are interconnected to reduce costs, optimize the length of pipes and cables, improve physical separation, enhance building shielding, facilitate maintenance and access to the nuclear area.

The safety philosophy of the Angra-2 plant is based on risks from nuclear radiation, generation and accumulation of fission products, and activation products. To manage this risk, safety resources are designed to ensure that no radioactive material will be released to environment in amounts unacceptable by regulatory agencies, during normal operation or during and after postulated accidents. In this way, three fundamental safety objectives must be met:

- Safe reactor shutdown and long-term subcriticality.
- Long-term residual heat removal.
- Confinement of radioactivity.

To meet Angra-2's fundamental safety objectives and ensure safe plant operation, several safety measures are applied, including multiple protection barriers (fuel pellet, fuel rod, primary cooling system, and containment), defense in depth, safety margin, negative coefficients (moderator temperature, fuel temperature, and void), material/equipment quality, redundancy and diversity of safety systems, maintenance, operator training, operation manuals, etc. Among the safety measures adopted in the Angra-2 project, only aspects related to the study of the human error probability (HEP) during steam generator tube rupture (SGTR) will be briefly detailed in this section.

## 2.1 COMPARISON BETWEEN ANGRA-2 AND APR-1400

To be able to extract good insights from this analysis and to build good points to enhance procedure design and HRA analysis, it is important to describe the major differences between Angra-2 and APR-1400 design technology. Therefore, the major points considered for comparison are the critical safety functions which must be monitored by the operator in any plant condition, whether it in accident condition, abnormal or normal operation; the safety systems involved in mitigating the event; structure of the operational procedure and organizational flowchart, and training process.

### **Critical Safety Functions:**

According to chapter 18.3 from Angra-2 FSAR [4], the critical safety functions that must be monitored by the operator and the reactor protection system (RPS) to ensure the primary safety objectives at any circumstance are:

- a) **Subcriticality:** Insert sufficient negative reactivity by control rod and/or boron to set the subcriticality condition for the reactor to break the reaction chain and diminish energy production from the fuel to avoid unacceptable reactivity transients.
- b) **Primary side coolant inventory:** Ensure enough coolant to remove the heat from the core in adequate way, recharging the primary system before the PZR loses their level or to avoid the rise of PZR level preventing the primary system to be solid. Level control among the adequate levels is essential to avoid a scram and to promote an efficient control of primary system pressure by the heaters and spray system.

- c) **Primary side heat transport:** Heat transport from the heat source (reactor) to the heat sink (steam generator) by natural circulation or active circulation. In the case of secondary side heat sink function failure, FRG feed and bleed should be deployed.
- d) **Secondary side heat sink:** Remove adequately the heat produced in the reactor core and transfer it to the secondary side of the steam generator (SG), protecting the primary side against overpressure.
- e) **Steam generator feedwater supply:** Ensure an adequate supply of feed water on the secondary side of the SG to ensure removal of heat from the reactor core.
- f) **Primary circuit integrity:** Limit the pressure on the primary side under the maximum pressure permitted for the reactor coolant boundary to avoid any possibility of integrity failure.
- g) **Containment integrity:** Avoiding lose the integrity of the containment will prevent losing inventory to cooldown the reactor by steam escape to the annulus or prevent the steam damage safeguard systems located inside the annulus which is responsible to maintain vital systems working correctly.

During HRA analysis, understanding the safety functions are essential to describe the event, the actions that the operator and safety system need to perform to mitigate the accident, and most important is to define if a human action is important or not to be considered as a critical human action, which could be or not subject of HEP quantification.

In the other hand, according to chapter 7.5 from APR-1400 FSAR [5], the critical safety function considered are:

- a) Reactivity control;



- b) Maintenance of vital auxiliaries;
- c) RCS inventory control;
- d) RCS pressure control;
- e) Core heat removal;
- f) RCS heat removal;
- g) Containment isolation;
- h) Containment temperature and pressure control; and
- i) Containment combustible gas control.

After a simple analysis of the procedures, three main points were identified that differ between these two designs, which are: 1) Angra-2 does not consider the maintenance of vital auxiliaries as a critical safety function, however, the power systems available for the plant are verified by the operator during the execution of the SPTA through the OP-3-1.1 procedure; it was identified that verification by the operator of the critical containment integrity safety function during the SPTA is not foreseen through the OP-3-1.2 procedure; and finally, the APR-1400 has more critical safety functions associated with containment.

**Safety Systems:**

The main difference observed between the two designs is in the safety injection system at the following points: APR-1400 injects coolant directly into the reactor vessel through a technology called Direct Vessel Injection (DVI), while in Angra-2, injection is performed in the hot or cold leg, depending on prior alignment. Another point is that the coolant flow in the safety injection system is not closed in Angra-2 unlike the system designed for the APR-1400 plant, for example, in the case of feed and bleed. In Angra-2 project, the water from the borated water storage tanks (JNK) is injected into the core

through high-pressure pumps and during depressurization, by the pressurizer relief valves (POSRV), the released steam goes to the pressurizer relief tank (JEG). The JEG has limited capacity, and if the tank reaches its maximum coolant limit, a safety valve broken, releasing excess coolant into the containment reservoir. On the other hand, APR-1400 design, the borated water used by the safety injection system to inject into the RCS comes from the In-Containment Refueling Water Storage Tank (IRWST). In case of overpressure, the pressurizer relief valves will discharge steam into the IRWST tank. Thus, this design has a closed circuit for primary cooling through the Feed and Bleed process.

### **Operational Procedure (OP):**

The operational procedure (OP) in the MCR in Angra-2 are physically distributed in the MCR inside drawers in cabinets, following a framework designed to facilitate the access and search. Angra-2 OP follows a guide report by the Nuclear Safety Standards Commission (KTA) – document Requirements for the Operating Manual - KTA-1201, from Germany regulatory body [6]. This document has the guidance to model the OP structure and the content necessary to manage and operate the NPP with safety in normal or accident condition. The EOP has the followings chapter distribution and structure:

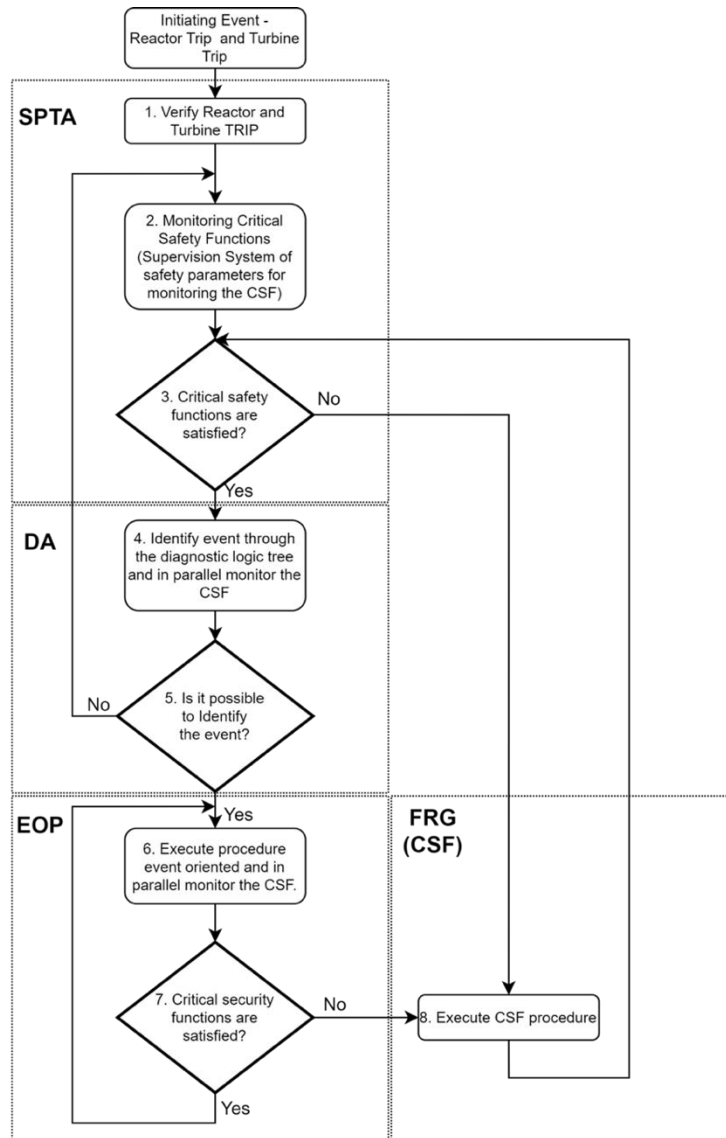
- Chapter 0 – Table of Contents and Introduction
- Chapter 1 – Plant Regulations
  - Personnel Organization
  - Control Room and Shift Regulation
  - Maintenance Regulation
  - Radiation Protection Regulation

- Guard and Access Regulation
- Alarm Regulation
- Fire Protection Regulation
- First Aid Regulation
- Chapter 2 – Plant Operation
  - Pre-requisites and Conditions for Operation
    - General Pre-requisites and Conditions for Operation of the Plant
    - Pre-requisites and Conditions for Power Operation
    - Pre-requisites and Conditions for the Phases of No-power Operation
  - Safety-related Limit Values
  - Testing Schedule
  - Criteria for Notifiable Events
  - Normal Operation
  - Abnormal Operation
- Chapter 3 – Design Basic Accident (Incidents)
  - Condition Oriented (Protective-goal Oriented) Handling of Design basis accidents (incidents)
  - Event Oriented Handling of Design Basis Accidents (Incidents)
- Chapter 4 – System Operation
  - Nuclear Power Production including Containment
  - Nuclear Auxiliary Systems
  - Water-Steam Circuit
  - Steam Turbine System

- Coolant Water System
- Auxiliary and Ancillary Systems, Water Supply and Disposal
- Electrical Systems and the Instrumentation and Control Systems
- Handling of Fuel Assemblies and of Heavy Loads inside the Containment Vessel
- Chapter 5 - Malfunction and Hazard Alarms

In summary, Angra-2 OP guides the operator at all phases of the plant at normal condition, from cold shut down to 100% power until exchange spent fuel condition with heat removal by recirculation mode (Chapter 1, chapter 2 and chapter 4), and during DBA and severe accident by through condition oriented or event oriented OP (chapter 1, chapter 3, chapter 4, and chapter 5).

In addition to the description of the content of operational procedures and the conditions under which they are utilized, in a human reliability analysis, it is of paramount importance to understand how the procedures are hierarchically organized and how they interrelate. Therefore, in the event of an accident, the procedures for Angra-2 must be handled by the control room operators in accordance with the procedure "Operator Task Concept - Emergency Operation Guide" (OP-3-1.1), which organizes the procedures according to figure 2, as shown below.



**Figure 2 – Angra-2 OP flowchart**

As depicted in the flowchart, the “Emergency Operation Guide Procedure (OP-3.1.1) organizes the deployment of the procedures by the operator into 4 phases, namely: standard post TRIP actions (SPTA); diagnose analysis (DA); emergency operational procedure (EOP); and safety critical functions recovery guidance (FRG). In summary, following the TRIP, the operator should execute steps 1, 2, and 3 of the SPTA phase. In step 1, the operator should verify the reactor TRIP, reactor protection warnings, plant

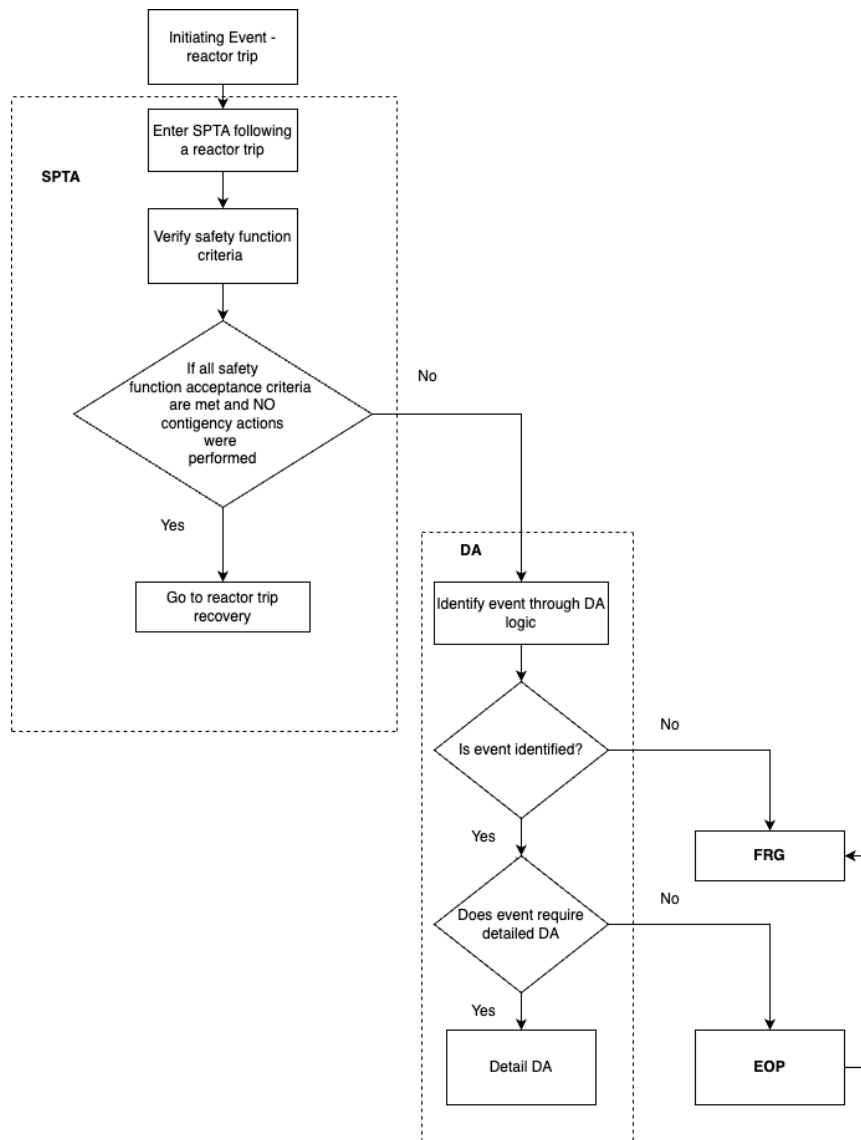
status, and the insertion of all control banks through OP-3-1.1. In step 2, the operator should monitor all safety critical functions (SCF) through procedure "Monitoring of Safety Critical Functions" (OP-3-1.2). If any SCF is not met, the operator should execute the corresponding FCS restoration procedure (OP-3-2.1/3-2.2.1/3-2.2.2/3-2.2.3/3-2.2.4/3-2.2.5), bringing the plant to a safe and normalized condition. If they are all OK, step 3 is assured, and the operator can proceed to the diagnostic analysis (DA) phase. In this phase, the operator should execute the procedure "Logical Diagnostic Tree (LDT)" (OP-3.1.3) to identify the occurring event. If the event is identified, the operator proceeds to the emergency operational procedure (EOP) for the specific event while concurrently monitoring the SCF. If identification is not possible, the operator returns to step 2 of SPTA. Finally, during the execution of the respective EOP, if any SCF is violated, the operator must exit the EOP and proceed to the FRG, bringing the plant to a safe and normalized condition.

Additionally, the OP from Angra-2 follows a Germany methodology to codify all the systems, equipment and components, and they are identified by a system code called "Basic Structure of the Identification System – KKS" and was created to facilitate the exchange of information in all phases of the NPP [7]. In summary, each system will be identified by a trigram, each equipment by a diagram, and each component by a single letter. Therefore, the KKS identification is extensively used in the procedure and facilitates the handling of procedures, the communication inside and outside of MCR, and the identification of any system, equipment, or component by operators. During any accident event, the identification of system, equipment and components are well defined, and this framework certainly decreases the possibility of

any misunderstanding during exchange of information and either receiving or sending information.

Given the description of Angra-2 procedures, the most significant differences observed were in the operational procedure structure, which the operator should follow during an emergency response, and the fact that procedures in Angra-2 are used in a physical version, whereas in APR-1400, a digital version is employed.

Regarding to the first point, through a comparative analysis between the flowchart in Figure 2 (Angra-2) and the flowchart in Figure 3 (APR-1400), a notable difference identified is that the OP structure of Angra-2 allows the operator to decide to return to the beginning of SPTA in case of uncertainty about the diagnosis of the event or if the operator completes the execution of an FRG. On the other hand, the OP structure of APR-1400 guides the operator to navigate through the procedures in a one-way direction, irrespective of whether the event can be diagnosed or not.



**Figure 3 – APR-1400 OP flowchart**

**Training Process:**

In Angra-2, each operator goes through a training process that is divided into 5 modules lasting 3 days per year. Each day has 4 hours of theoretical classes and 4 hours of simulator classes. Events from the DBA list and some events outside the project base are trained. Within this scope, the operator trains the SGTR twice a year. However, the training process in APR-1400 was not assessed as such no further comparison was made.





### 3 METHODOLOGY

Currently, there are various Human Reliability Analysis (HRA) techniques available to address human errors in Probabilistic Safety/Risk Assessments (PSA/PRA). These techniques encompass traditional concerns like human-machine interactions and the practicality of actions in PRA scenarios. Moreover, many of these methods have been developed to specifically target errors in decision-making and errors of commission/omission. Due to the variations in the methods and their underlying models, there is considerable interest in evaluating HRA techniques and ultimately validating the approaches and models on which they are based. This validation is necessary to determine the reliability of HRA outcomes when decision makers rely on them for making informed decisions about risks.

At the most fundamental level, all HRA methods share a common objective, which is determined by the HRA's role within the PRA. This objective can be broken down into three main components: (1) determining which Human Failure Events (HFEs) should be incorporated into the accident sequence model of the PRA, (2) conducting a qualitative analysis of these HFEs, and (3) quantifying the probability associated with these HFEs [14]. To extract useful information for HRA, Table 1 shown a typical information for HRA as well as how it can be extracted [8]. The information will be used for HEP quantification using SPAR-H and IDHEAS-ECA.

**Table 1 – Typical information for HRA**

<b>Information</b>	<b>Extraction technique and/or method</b>
Available procedure	Task analysis of emergency operations
Description of required task	

The person and/or team that have to perform the required task, and the level of experience	Interview with operators
The time need to correctly perform the required tasks	Time-line analysis
Demand of perception, cognition and action to perform the required task.	Task analysis of procedural steps and protocol analysis
Error types applicable for required task.	Hierarchical task analysis through Sharp analysis.

In accordance with Table 1, human reliability analysis will be conducted as follows:

- Description of the steam generator tube rupture event in Angra-2;
- Development of the SGTR event tree in Angra-2;
- Identification of Human Failure Events (HFE) in Angra-2; and
- Hierarchical task analysis (HTA) of the HFE defined for SGTR in Angra-2, followed by:
  - Applicable error modes (SHERPA);
  - HFE definition; and
  - Base timeline analysis.
- HEP quantification; and
- Dependency HEP analysis.

Additionally, in this section, the HRA methodologies used in Angra-2 PSA, Standardized Plant Analysis Risk-Human Reliability Analysis method (SPAR-H) [9] and the General Methodology of An Integrated Human Event Analysis System (IDHEAS-ECA) [10] are briefly explained.

### 3.1 ANGRA-2 HRA METHODOLOGIES

As it was previously highlighted, the assessment of the cognitive component of Human Error Probabilities (Pc) in the HRA of Angra-2 follows the methodology proposed by EPRI, which utilizes the HCR/ORE and CBDTM methods and selects the highest calculated value.

The HCR/ORE methodology originated following the TMI accident in 1979. EPRI initiated the Operator Reliability Experiments (ORE) project between 1986 and 1990 to collect and analyze data on the cognitive aspects of operator response in full-scope control rooms of nuclear power plants. These data were utilized to scrutinize the hypotheses underpinning human cognitive reliability (HCR), which was conceptualized in 1984 as a means to quantify and estimate the operational reliability in the control room. It is an empirical method that cognitively models operator actions that are time-sensitive [11]. Due to the specificities of HCR/ORE, EPRI developed the Cause-Based Decision Tree Method (CBDTM) in 1992 as a more straightforward framework for calculating the cognitive or human error component of risk in nuclear power plants. The technique was created as a supplement to HCR/ORE, primarily to deal with circumstances where time is not a constraint. It is a method of analysis focused on the recognition of failure mechanisms and mitigating factors. Suitable for rule-based behavior, such as when procedures are followed. The CBDTM Method takes timing into consideration when applying recovery factors, and it implicitly considers stress when making decisions in the decision trees [12].

The combination of these methods recommended by EPRI is noteworthy due to the complementary nature of HCR/ORE and CBDTM. HCR/ORE is reliant on and significantly influenced by time-related information, potentially yielding irrelevant

results if the time available for the cognitive phase is excessively long. It is specifically designed for analyzing time-dependent human interactions. In contrast, CBDTM focuses on analyzing human/machine and human/procedure interfaces, with the time factor being less critical compared to HCR/ORE. Its primary impact lies in determining the degree of dependency for recovery factors. Consequently, for tasks where time is not a critical factor, HCR/ORE may yield values of limited significance, at times being unrealistic. In such scenarios, CBDTM emerges as the more suitable method. Conversely, in situations where the cognitive analysis is time-sensitive, CBDTM might produce inappropriate values, making HCR/ORE the more realistic approach.

In the other hand, the estimation of the execution component ( $P_e$ ) of HEP is determined using an evaluation based on the THERP method. Several tables from chapter 20 of THERP are used, as appropriate, to estimate the value of  $P_e$  [13]. The application of THERP for the estimation of  $P_e$  follows a logic of reviewing each procedure to identify the critical steps (i.e., the essential steps to complete the task) and whether there are any recovery mechanisms present (e.g., flow verification, valve position, etc.). The issue of recovery is also evaluated in the context of the time available for completing the necessary actions. This method is widely used and provides a comprehensive task analysis that can support HEP estimation. THERP considers both latent and active HFE and focuses fundamentally on ruled-based behavior when operators are following procedures [14].

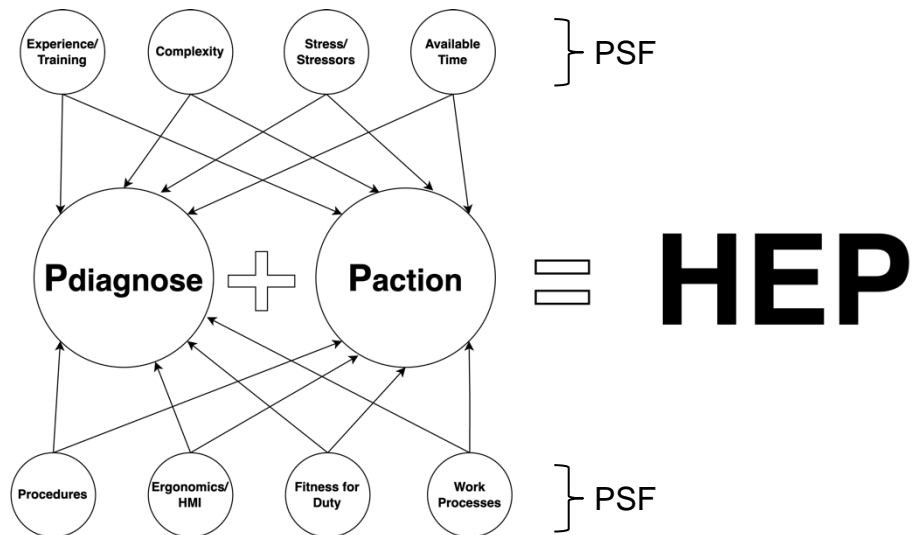
The final HEP value is the sum of  $P_c$  and  $P_e$ , where:  $HEP = P_c + P_e$ , and  $P_c$  is the probability of failure in the cognitive stage, and  $P_e$  is the probability of failure in the execution phase.

### 3.2 SPAR-H

The Standardized Plant Analysis Risk-Human Reliability Analysis (SPAR-H) method was created in the 1990s by the Electric Power Research Institute (EPRI) and the Idaho National Laboratory (INL) to quantify the cognitive or human error component of risk in nuclear power plants. The method was developed based on experience gained in field-testing the Analysis Risk Model (ASP/SPAR) human reliability analysis (HRA) method, which was used in the development of nuclear power plant (NPP) models. The method was updated in 1999 and renamed SPAR-H, and in 2003, it was updated again to enhance its general utility and make it more widely available. SPAR-H is a well established and widely used HRA methodology in the nuclear industry. The fundamental structure of SPAR-H breaks human actions into two parts, diagnosis and action, and utilizes the concept of nominal HEP for diagnosis and action, which are average expected values in the absence of PIF effects. The nominal HEPs are:

- $P_{\text{Diagnosis}} = 1.00\text{E-}02$ ; and
- $P_{\text{Action}} = 1.00\text{E-}03$ .

SPAR-H takes into account the context in which the operator is inserted to apply the PSFs and the dependence balancing the nominal HEP, as shown in Figure 4.



**Figure 4 – SPAR-H framework**

An influential element of this method is the simplicity and clarity in estimating the HEP. Unlike first-generation methods, SPAR-H is built on a precise approach to human performance derived from scientific studies of human behavior that have been translated from activities conducted in nuclear power plants. An analysis of operational experiences revealed that eight PSFs, as illustrated in Figure 4, are related to human performance in the operation of nuclear power plants.

### **3.3 IDHEAS-ECA**

The Integrated Human Event Analysis System (IDHEAS-ECA) was created by the US Nuclear Regulatory Commission (NRC) and the Electric Power Research Institute (EPRI) in 2015 as a new approach to Human Reliability Analysis (HRA) for internal, at-power nuclear power plant (NPP) events. IDHEAS-ECA final report was released in 2021 [10]. The IDHEAS-ECA method integrates the strengths of existing HRA methods and enhances HRA in the following ways:

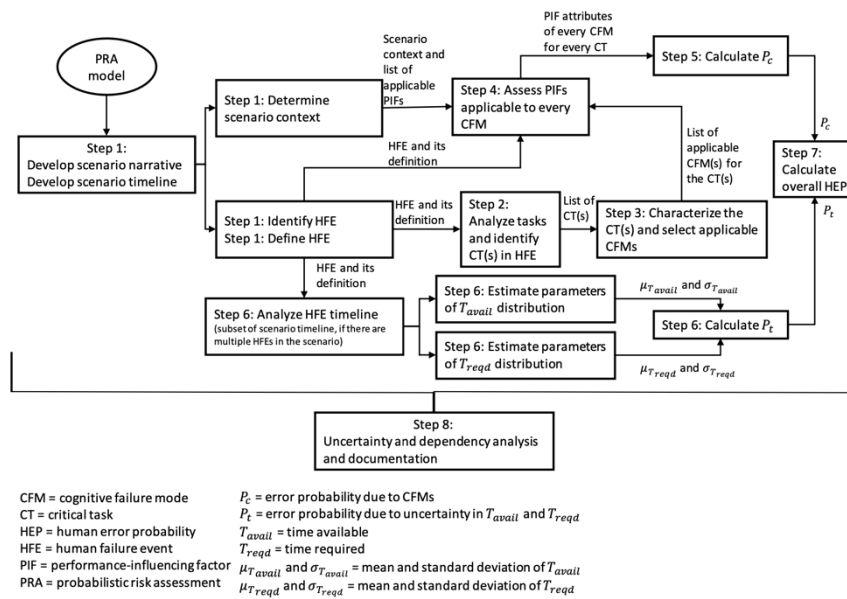
- Application scope

- Scientific basis
- HRA variability
- Data for HRA

The IDHEAS-ECA method provides a structured approach to task analysis through crew response diagrams and a model addressing time. The method was motivated by the need to improve upon existing HRA methods and provide a more comprehensive and reliable approach to HRA for internal, at-power NPP events. IDHEAS-ECA demonstrates the ability to enhance the results obtained from HRA both qualitatively and quantitatively. In this way, IDHEAS-ECA will resolve the issues related to the analysis of human actions concerning time. Unlike the first-generation methodologies that are either highly sensitive or insensitive to the time factor, IDHEAS-ECA includes the calculation of failure probability over time in its structure, relating the available time to perform the action and the required time through a convolution integral of the density and distribution functions of time, as we can see in Figure 6 [10]. As a result, the total HEP generated by IDHEAS-ECA does not have an extreme or negligible dependence, avoiding significant variations that render the HEP impractical to use.

Additionally, IDHEAS-ECA provides guidance for the analyst to conduct both cognitive failure probability analysis and time analysis, ensuring consistent results when used by different analysts. Moreover, this method allows for a detailed review of all analysis steps, contributing to the achievement of more consistent and constant results. Figure 5 shows all step-by-step guidance from IDHEAS-ECA.

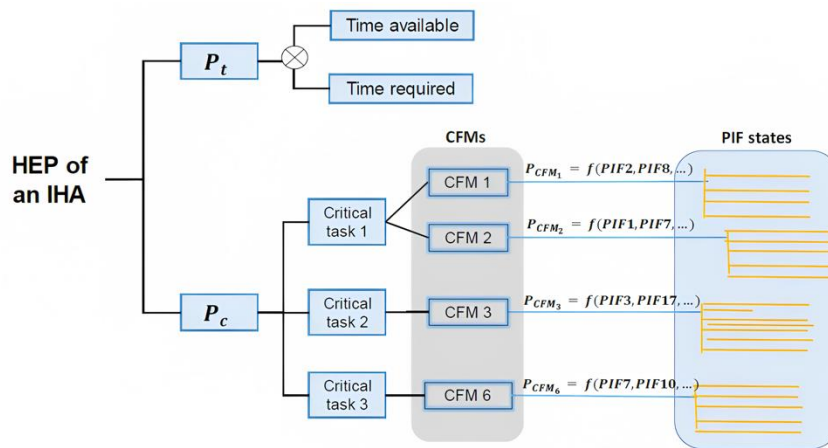




**Figure 5 – Illustration of the IDHEAS-ECA process**

Furthermore, IDHEAS-ECA has an extensive database, enabling its application in the analysis of plants with specific characteristics, as well as the analysis of situations that deviate from the patterns adopted by first-generation methodologies. It is capable of analyzing contexts beyond the control room and encompassing new technologies [15].

The methodological structure of IDHEAS-ECA is based on two parts: failure probability over time and failure probability of cognitive modes, as shown in Figure 6.



**Figure 6 – IDHEAS-ECA framework**

In the cognitive mode structure, IDHEAS-ECA models critical tasks using five macrocognitive functions: detection, understanding, decisionmaking, action execution, and interteam coordination. Failure of any of these functions is called a Cognitive Failure Mode (CFM). IDHEAS-ECA employs the use of base HEP for the given Cognitive Failure Mode (CFM) using the following three PIFs to build the HEP base for each CFM:

- Information availability and reliability (INF)
- Scenario familiarity (SF)
- Task complexity (TC)

Furthermore, IDHEAS-ECA provides a wide range of performance influencing factors (PIFs) and PIF attributes, which, based on context and boundary conditions, are connected to cognitive failure modes, degrading them. All PIFs are categorized into four different categories: Environment and situation, systems, personnel, and task. These categories entail a total number of twenty (20) PIFs. Table 2 below shows the PIFs used in IDHEAS-ECA [10].

**Table 2 – PIFs in IDHEAS-ECA**

<b>Environment and Situation</b>	<b>System</b>	<b>Personnel</b>	<b>Task</b>
<ul style="list-style-type: none"> <li>• Work location accessibility and habitability</li> <li>• Workplace visibility</li> <li>• Noise in workplace and communication pathways</li> <li>• Cold/heat/humidity</li> <li>• Resistance to physical movement</li> </ul>	<ul style="list-style-type: none"> <li>• System and I&amp;C transparency to personnel</li> <li>• Human-system interfaces</li> <li>• Equipment and tools</li> </ul>	<ul style="list-style-type: none"> <li>• Staffing</li> <li>• Procedures, guidelines, and instructions</li> <li>• Training</li> <li>• Teamwork and organizational factors</li> <li>• Work processes</li> </ul>	<ul style="list-style-type: none"> <li>• Information availability and reliability</li> <li>• Scenario familiarity</li> <li>• Multi-tasking, interruption, and distraction</li> <li>• Task complexity</li> <li>• Mental fatigue</li> <li>• Time pressure and stress</li> <li>• Physical demands</li> </ul>

This structure allows the analyst to conduct a more detailed qualitative analysis, which can provide better insights for risk management through informed risk decision-making. It also allows for a more diverse and varied application, covering all types of human failure events, resulting in reduced result variability [15].

In summary, IDHEAS-ECA will not yield significantly different results compared to the human reliability analysis conducted by Angra-2. This is due to the combination of methods used, which expands the application spectrum of the analysis, and the fact that they are well-established methods for analyzing accidents in the control room. However, IDHEAS-ECA will provide greater consistency in the results due to the use of a single methodology and a detailed guide for calculating the human error probability (HEP) for all important human actions considered. Additionally, IDHEAS-ECA encompasses a vast number of performance-influencing factors (PIFs) and PIF attributes, covering a wide range of contextual specificities. This allows the analyst to

connect these factors to cognitive failure modes, resulting in a qualitatively richer analysis that clarifies the key areas for improvement and risk management.

## 4 SGTR ACCIDENT ASSESSMENT

Among all the Initiating events (IE) identified for a PWR-type plant, SGTR is one of the most likely to occur [16]. This IE is a unique type of LOCA, in that reactor coolant leakage bypasses the containment boundaries through the u-tubes. SGTR requires numerous manual actions from the operator to mitigate the accident and prevent the release of radioactivity into the environment and may involve the failure of one or more tubes, causing the total coolant leakage rate to exceed the capacity of the primary volumetric control systems (KBA). Given these considerations, the event chosen as the subject of this study is the complete rupture of multiple 2A tubes, resulting in a rupture-induced leakage initially at a rate of approximately 40 kg/s, which is subsequently reduced to 20 kg/s through automatic actions.

### 4.1 DESCRIPTION OF SGTR PHENOMENA IN ANGRA-2

The technical background to describe the SGTR phenomena in Angra-2 is based on the operational procedure (OP-3-3.5) and thermal hydraulic behavior described in Final Safety Analysis Report (FSAR) chapter 15 [17][4]. Therefore, the phenomena and automatic actions that characterize the loss of primary coolant to the secondary system in U.N. Angra 2 are as follows:

The leakage of primary coolant into the secondary system results in a drop in primary system pressure, a reduction in the pressurizer level, and an increase in activity in the main steam line, particularly in the affected steam generator.

In this context, the volumetric control system (KBA) through the control of coolant extraction and injection into the RCS (Reactor Coolant System) is unable to

maintain the PZR (Pressurizer) level above 2.28 meters. This triggers the JT limitation signal, which activates the safety injection system (JND), shuts down the Reactor Coolant Pumps (JEB), and isolates the primary and containment systems.

In the main steam lines of each steam generator, there are two types of detectors, namely, Geiger-Müller counters for detecting N-16 activity and NaI (TI) scintillator detectors for detecting noble gases. When the activity limit is exceeded in the main steam line, the reactor limitation system generates the JR52 signal, which initiates the shutdown of the plant through the limitation system (JT), triggering the S-class alarm "Main Steam Tube Rupture" (JR06). Reactor and turbine TRIP occurs either when  $P_{RCS} < 131\text{bar}$  or 300 seconds after the JR52 limitation signal is generated, whichever comes first. At this point the RCS inventory is controlled by the SIS and the SG feedwater flow is controlled automatically by the main feedwater pump (LAC) and start stop pump (LAJ) from the main feedwater tank (LAB). From this point on, several manual actions must be performed by the operator to recover the plant and these actions include:

- a) Identify and isolate the steam generator.
- b) Initiate cooling at a rate of 50 K/h.
- c) Depressurize the RCS.

To provide a clearer illustration of Angra 2 power plant's behavior after identify the SGTR accident and all necessary manual actions, in accordance with reference [17], operational procedure (OP) "3.3.5 - Steam Generator Tube Rupture with Violation of Main Steam Activity Limits" outlines the automatic and manual actions required to mitigate the accident as follows:

Automatic actions:

- a) S-class alarm: Steam Generator Tube Rupture I

- i) Signals: [Main Steam Activity > Max] + [Containment/Atmosphere  $\Delta P < 20\text{mbar}$ ] activate the S-class alarm.
  - ii) If the PZR level drops below 2.28m during the event, the S-class alarm: Steam Generator Tube Rupture II is activated when PZR level < 2.28m and SRR pressure < 109bar.
- b) After identifying the U-tube rupture in the steam generator, the protection system activates the JR52-Cooling Signal via limitation.
- i) Reactor and generator power are reduced at a rate of 20%/min to a power level < 30%.
  - ii) To assist in this reduction, the protection systems inject boron at 7000 ppm, start the second AP pump of the volumetric control system, and reduce coolant extraction through the high-pressure reducer to 6kg/s for 360s.
- c) After the increase in main steam pressure due to load rejection resulting from power reduction, the steam generator pressure control system opens the turbine bypass valves to maintain pressure at 79 bar. The power reduction that caused the increase in main steam pressure decreases the  $\Delta P$  between primary and secondary, reducing the leakage through the rupture. During the automatic actions, the reference value is reduced to 76bar.
- d) Maintenance of primary inventory by the volumetric control system.
- i) The limitation system starts the second high-pressure pump of the volumetric control system.
- e) The reactor protection system will perform the following automatic actions when the PZR level < 2.28m, as a result of the deficiency in leakage makeup used by the limitation system:

- i) Isolation of the SRR.
  - ii) Start of the additional boron injection system.
  - iii) Shutdown of the RCPs.
  - iv) Isolation of the containment.
- f) When the SRR pressure is below 30% or 210s have passed since the main steam activity limits were violated (S-class alarm: Steam Generator Tube Rupture I), the protection system initiates the main spray from RCP  $\Delta P$ , boron injection system spray, and auxiliary spray to bring the plant pressure  $< 89\text{bar}$ .
- g) The reactor protection system trips the reactor and turbine if:
- i) RCS pressure  $< 131\text{bar}$  and reactor power  $> 12\%$ ; or
  - ii) 300s have passed after the S-class alarm: Steam Generator Tube Rupture I.
- h) Pressure reduction is stopped when RCS pressure  $< 89\text{bar}$ , and the pressure reduction via coolant injection through the pressurizer spray is transferred to injection into the loops. In case of SRR isolation, the pressure reduction is stopped at a higher level than  $89\text{bar}$  determined by the natural circulation saturation  $\Delta T$  (RCS shutdown).
- i) The level of all steam generators is reduced from  $12.2\text{m}$  to  $11.1\text{m}$ , gaining margin to mitigate coolant leakage through the affected steam generator rupture, avoiding overfilling of the affected steam generator before the start of manual actions.
- j) The reactor protection system isolates the feedwater line of the affected steam generator when the level reaches  $13.5\text{m}$ .

Understanding the Angra-2 response after identification of SGTR is important to define the sequence of events during Event Tree modeling and to build the base



timeline for the HFE identified for this event. In summary, the most crucial automatic actions for accident mitigation include the reactor trip (TRIP), ensuring the subcriticality of the plant, and the activation of the safety injection system (JND), ensuring control of the primary inventory. In addition to these primary actions, the reactor limitation and protection system anticipates operator actions to reduce the pressure gap between the primary and secondary systems, thereby decreasing leakage through the breach by reducing primary pressure and increasing secondary pressure. Furthermore, it lowers the setpoint of steam generator (SG) level by 1 meter to allow additional time for the manual actions that the operator must subsequently perform. The subsequent section elucidates the manual actions conducted by the operator during the accident mitigation, outlining the associated consequences and involved safety functions.

Manual actions:

- a) Identification and isolation of the affected steam generator (SG). The operator can identify it through the N16 detectors, mismatch of SG level and feedwater flow. After isolating the affected SG, there may be an increase in pressure and the operator should limit the pressure using the heating line avoiding radiation release to the environment.
- b) The operator should initiate RCS cooling through the unaffected GVs at 50K/h. The initial cooldown by the unaffected SG allows heat transfer from primary side to secondary side maintaining RCS at a subcooled state allowing the operator to depressurize the RCS. It is preferable to cooldown the RCS using the TBV which will preserve the inventory for SG through the closed cycle, and in case of isolation failure and will maintain the radiation contained in the

secondary system. In the case of TBV failure, ADVs have the same effect to cooldown the RCS. Cooling down the RCS through ADVs, Operator should replenish the SG water supply due to secondary open cycle cooling.

- c) Increase the pressurizer level to 4-6m using the auxiliary boron injection system spray (JDH) to maintain inventory during coolant contraction.
- d) Shutdown the safety injection pumps, ensuring that the available coolant inventory is sufficient to continue the maneuver and allow the operator to decrease RCS pressure.
- e) Reduce the RCS pressure to approximately 80bar, minimizing the leakage rate through the rupture. During the phase when RCPs are shut down, the operator should maintain an overpressure of 2 to 3bar between the RCS and the isolated SG to prevent steam formation in the U-tubes of the affected SG, aiming to maintain natural circulation in this SG. Reducing the RCS pressure under the affected SG overpressure will avoid affected SG to overfilling/over-pressurizing, preventing connecting the RCS with the atmospheric pressure, and avoid the affected SG to overpressure opening the MSSV releasing radioactivity steam.
- f) Initiate the volumetric control system to control RCS inventory during cooldown.
- g) Control the pressure in the isolated SG to prevent steam formation in the tube bundles, leading to loss of natural circulation. The operator should maintain the primary pressure 2 to 3bar above the main steam pressure using heaters, if available, or by relieving pressure from the affected GV through the heating line. Preferably, use the PZR heaters for radiological reasons.

- h) During cooling at a rate of 50K/h, the operator should ensure demineralized water inventory in the emergency feedwater system pools (LAR) in the case of SG feedwater loss from the feedwater tank (LAA) through the closed cycle. In the case of RCS cooling down at 50K/h by the secondary system, the operator should follow the FRG and establish the feed and bleed process to cooldown the RCS until the RHR system entry point. To support this condition, the operator should replenish the RHR system inventory.
- i) If RCPs are not available, the operator should cool the plant at a rate of 5K/h to maintain natural circulation and gain time to restore power to the RCPs. This condition occurs due to a loss of offsite power, which will not be considered in this analysis. Therefore, the RCPs will be available.
- j) Restore auxiliary power supply when the main grid or standby grid is available. For this analysis, loss of offsite power will not be considered, ensuring the power supply to the RCPs.
- k) Start two RCPs if they are in failed mode in the unaffected loops diametrically opposite to each other.
- l) Ensure that the RCP in the affected loop remains out of operation and secure it against restart.

After the RCPs are online, reduce the RCS pressure during cooling at a rate of 50K/h, maintaining the pressure within the saturation pressure margin of 15bar. If the RCPs are inoperable, maintain a subcooling margin of 15K.

## 4.2 SGTR EVENT TREE DEVELOPMENT FOR ANGRA-2

Maintaining the critical safety functions is crucial to prevent core damage in nuclear power plants. Therefore, it is crucial to define and summarize all the critical safety functions involved during SGTR to define the key safety system and operator actions which should be done to mitigate the event. In this way, a detailed analysis of each step of the procedure will be performed, describing the system/human action, and the safety function supported by that system/human action. Table 3 below shows the detailed analysis of the steps in OP-3-3.5. NOTE: Each step represented by letters represents automatic actions, while steps represented by numbers represent manual actions.

**Table 3 – Procedure analysis based on CSF affected by human/system action**

<b>Step#</b>	<b>Step Name</b>	<b>Description</b>	<b>Safety Function</b>	<b>System/Human Action</b>
<b>Identif.</b>	SGTR I.E. Identification	Operator should identify the event to ensure he is dealing with the event through the correct OP.	N/A	The operator should deploy SPTA and DA OPs to identify the event and deploy the OP-3-3.5. This step is to re-check event identification.
<b>A</b>	High activity in the main steam line actuation.	Limitation system identify the high activity beyond the limit in the main steam line actuating the limitation signal JR52.	N/A	The operator should check the activity measured by the instrument in the main steam line and check the reduction of power.
<b>B</b>	Alarm class S: “SG rupture I”	Protection system will alarm in the hardware alarm system (HAS) for operator detection.	N/A	Operator detection on HAS panel.
<b>C</b>	Compensate PZR level drop	Limitation system will diminish the flow in the extraction line or close, it depends on the level drop of	Primary side coolant Inventory	Limitation system. Operator should check the

		the PZR in comparison with the reference level and will turn on the second injection pump.		automatic actuation.
<b>D</b>	Power reduction for < 30%	Limitation signal JR52 will reduce the power at a rate of 20%/min until <30%. Turn on Acid boric and demineralized injection system (KBC). Turn on additional acid boric system. Turn on second pump of injection system. Turn of PZR heaters. Reduction of Reference Level of SG from 12.2m to 11.2m.	Primary side coolant Inventory	The actions are made by the limitation system to gain time for the manual action of the operator reducing the SG level and decreasing the rate of leakage. The operator should check all automatic actions.
<b>E</b>	Open main steam turbine bypass	Automatic actuation will control the main steam pressure at 79bar through the turbine bypass.	Primary side coolant Inventory	Operator should check if the turbine bypass is working properly through their control valves. The system automatically increases secondary pressure to reduce the leakage from the RCS to affected SG.
<b>F</b>	RCS reduction pressure	Limitation system will start to reduce the pressure in the RCS through spray of RCS, boron injection system (JDH), auxiliary spray and turn of heaters. When: <ul style="list-style-type: none"> <li>- Activity in the main steam line &gt; max value of reference;</li> <li>and</li> <li>- Reactor power &lt; 30%; or</li> <li>- After 210s of the JR52 alarm signal.</li> </ul>	Primary side coolant Inventory; and Primary circuit integrity.	The operator should check the automatic actuation of the system.
<b>G</b>	Start reactor/turbine TRIP	Reactor protection system trip the reactor, through the control assembly insertion, and turbine when:	Subcriticality	Operator should check all control rod bank insertion.

		<ul style="list-style-type: none"> <li>- <math>P_{RCS} &lt; 131\text{bar}</math>; and</li> <li>- Reactor power <math>&gt; 12\%</math>; or</li> <li>- After 300s of the JR52 alarm signal.</li> </ul>		
<b>H</b>	Verify if the plant is under emergency power supply	It will not be considered loss of normal power.	N/A	N/A
<b>I</b>	Interrupt the reduction of pressure in the RCS	Limitation system stop the reduction of pressure when RCS pressure $< 89\text{bar}$ . Turn off spray on the PZR and change injection of JDH and KBA from top of PZR to loop leg. Also, reduce the main steam line pressure from 79bar to 76bar.	N/A	Operator should check if the limitation system stopped all spray in the top of PZR and if the pressure stopped dropping.
<b>K</b>	Verify if the PZR level $< 2.28\text{m}$	Operator should verify if the PZR level $< 2.28\text{m}$	N/A	Detect the PZR level.
<b>Q</b>	Isolation of RCS	When PZR level $< 2.28\text{m}$ the protection system will turn on the extra boration system (JR41), isolate the RCS (JR43), turn of RCPs (JR44) to maintain natural circulation and ensure heat removal through the secondary side.	Primary side coolant Inventory; and Primary side heat removal.	Operators should check if the action is done.
<b>R</b>	Initiate emergency core cooling criteria (ECCS)	Reactor Protection system identify: <ul style="list-style-type: none"> <li>- <math>P_{RCS} &lt; 109\text{ bar}</math>; and</li> <li>- <math>L_{PZR} &lt; 2.28\text{m}</math>.</li> </ul> Then, initiate the ECCS through the following actions: <ul style="list-style-type: none"> <li>- Containment isolation</li> <li>- High pressure safety injection</li> <li>- Turn off RCP</li> <li>- Isolate principal feedwater to the SGs.</li> </ul>	Primary side coolant Inventory	Operator should check if the actions are done.
<b>S</b>	Class S Alarm: "SG rupture II"	Reactor protection system just identify the second phase for SGTR event when initiated HSIP signal (JR 34), limitation cooling signal (JR52), and containment pressure is not $> 30\text{mbar}$ .	Primary side coolant Inventory	Operator should check the indication of alarm.

1	Verify NPP condition	<p>The operator checks all plant safety functions.</p> <ol style="list-style-type: none"> <li>1) Whether in power or subcritical</li> <li>2) Primary side refrigerant inventory</li> <li>3) Primary side heat transport</li> <li>4) Secondary side cold source</li> <li>5) supply of steam generators</li> <li>6) Primary circuit integrity</li> </ol>	N/A	<p>The Operator should verify if the plant has not violated any of the 6 safety functions. If any safety function is violated, the operator must follow deploy the related FRG to reestablish the safety function.</p>
2	Identify the affected SG	<p>The operator must, through the available variables, identify the affected GV. The variables are:</p> <ol style="list-style-type: none"> <li>1) Activity on the main steam lines</li> <li>2) Activity in GVs by sampling</li> <li>3) Positions of the supply water control valves</li> <li>4) Supply water flow to the GV</li> <li>5) GVs Water Level</li> </ol>	Primary side coolant inventory.	<p>Detect the Ruptured SG. If not done properly, the operator still can cooldown the RCS using the affected SG too, however, the operator must be prepared to replenish the coolant inventory in the safety injection system tank (JNK).</p>
3	Isolate and limit the pressure at 80 bar in the SG affected	<p>The operator should isolate and align the heating line system of the affected SG to prevent loss of inventory and radiation release.</p>	Primary side coolant inventory.	<p>Isolate the real affect SG and control their pressure, through the heating line, avoiding radiation release. If not done properly the operator must be prepared to replenish the coolant inventory in the safety injection system tank (JNK).</p>
4	Initiate RCS cooling at a rate of 50K/h until 60 bar in the	<p>If the turbine bypass valve (MAN) is available, the operator should cooldown the reactor at a rate of 50K/h in closed cycle through the MAN valves (1 of 6 is</p>	Primary side coolant inventory; Secondary side heat sink; and	<p>Operator initiate RCS through the TBV (MAN) valves. This action will allow the operator</p>

	main steam line	enough). If MAN is not available and the cooldown signal is actuated (JR86), the operator should cooldown the reactor in open cycle through the main steam relief valves (MSRVs / ADVs), and if ADVs fail, it could be maintained by the MSSVs.	Steam generator feedwater supply.	to decrease pressure in the RCS below the ruptured SG pressure and decrease differential pressure among the secondary side decreasing coolant leakage through the rupture. During cooling through the closed cycle, the operator must be aware of any alarm that may cause this condition to be lost. If lost, the operator should replenish the emergency feedwater pools tanks (LAR).
<b>5</b>	Verify if the pressure in the affected SG > 82bar	The operator should be alert, during RCS cooldown, to the rise of pressure in the affected SG above 82bar. If it happens, the operator should execute the step 6.	N/A	Detection of SG pressure rise above 82 bar. If the operator detects it, he should execute step 6.
<b>6</b>	Limitation of main steam pressure in the affected SG	The operator should use the MSR (ADV) of the affected SG, for the shortest possible period, to decrease pressure.	N/A	The operator should open ADV when MS > 82 and should close it when pressure < 80bar.
<b>7</b>	Verify if ECCS criteria is achieved	Operator should check if SIS is actuated.	Primary side coolant inventory.	Verify SIS condition.
<b>25</b>	Rise PZR level	The operator should rise the PZR level for 4-6m through the supplemental boron injection system (JDH) using the spray in the top of the PZR to inject borated water with 2300ppm concentration. The coolant is replenished by the high pressure safety	Primary side coolant inventory.	The operator should rearm the memory group V and align the supplemental boron injection system (JDH), and monitor the rise of level, decrease



		injection (HPSI) pumps and the supplemental boron injection system (JDH) will decrease pressure to allow the HPSI system inject water until the PZR achieve 4-6m. This maneuver is to facilitate the injection of coolant through the HPSI pumps. The operator should be pay attention to pressure margin among RCS and affected SG.		of pressure to maintain pressure margin between RCS and affected SG. When the level is achieved, the operator should change the injection for the loop legs.
<b>26</b>	Turn off all HPSI pumps	The operator should turn off all HPSI to allow the operator decrease pressure. The HPSI pumps head is around 109 bar.	Primary side coolant inventory.	The operator should turn off all HPSI pumps to allow decrease RCS pressure.
<b>27</b>	Verify if affected GV level > 13m	If the affected SG level > 13m, the operator should reduce this level. This verification is to monitor the high level in the affected SG to prevent solidification which can cause a LOCA through the MSSV without control.	N/A	The operator should detect the high level of affected SG and should execute the step 28 to diminish this level.
<b>28</b>	Reduce level of affected SG	The operator should use the purge line system to reduce the affected SG level under the steam dryers.	N/A	The operator should choose one purge system, align it, and diminish the level until uncovers the steam dryers.
<b>29</b>	Verify the PZR level.	The operator should verify the PZR level, and if the level is $\leq 4m$ , he should execute the step 30.	Primary side coolant inventory.	The operator should monitor and detect the drop in the PZR level and should execute the step 30.
<b>30</b>	Rise the PZR level	The operator should rise the PZR level using 1 safety injection pump.	Primary side coolant inventory.	The operator must turn on an HPSI pump, monitor the level rise up to ~6m and then turn it off.
<b>31</b>	Reduce RCS pressure	The operator should reduce the RCS pressure to 80 bar using the supplemental boron injection system (JDH)	Primary side coolant inventory.	The operator will redirect one supplemental boron injection

		paying attention to maintain the RCS pressure 2~3bar to avoid saturation and loss of natural circulation in the affected SG loop.		system (JDH) line to inject water through the spray in the top of the PZR (JEF) until the pressure achieve ≈80bar. Then, the operator should redirect the injection to the leg.
<b>32</b>	Verify pressure in the intact SGs and coolant outlet Temperature in the RCS.	The operator should identify the followings values: - Pressure in intact SGs ≈60bar; and - Outlet coolant temperature < 295Cel. If this condition is achieved, go to step 33, if not, go back to step 27.	N/A	Detect if the intact SG pressure and RCS outlet temperature achieve the determined SP, if not, the operator should monitoring all steps from 27 to 32 until he can move forward.
<b>33</b>	Stop cooling at a rate of 50K/h	The operator should stop Cooling the RCS at a rate of 50K/h to execute some actions to prepare the reactor for cooling it until the RHR condition entry.	N/A	The operator will stop cooling the RCS through the turbine bypass valve control actuation to reestablish some system for long term cooling.
<b>34</b>	Starting volumetric control system (KBA)	The operator should start the volumetric control system to control the inventory in the RCS.	Primary side coolant inventory.	The operator should remove the isolation signal from the reactor protection system and follow the manual of the system to align it.
<b>35</b>	Verify energy supply	If power supply is available, go to step 36, if not, go to step 45 (Path D).	N/A	Detecting the power supply availability and choose the right path to follow.
<b>36</b>	Remove containment isolation	The operator will remove the isolation of the containment to allow him to connect the KBA system to help him control the RCS inventory through the PZR level.	N/A	The operator should reset the containment isolation signal and normalize the

				ventilation system in controlled areas.
<b>37</b>	Borate RCS to 2300ppm	The operator should borate the RCS to 2300ppm concentration using the Boric acid and demineralized water injection system.	Subcriticality	The operator should verify the boron concentration using specific OP, choose one line of Boric acid and demineralized water injection system and align it to inject boric acid water into the RCS system by the legs.
<b>38</b>	Ensure that RCP of the affected SG loop does not start.	Ensure that RCP of the affected SG loop does not start, avoiding pressure build-up and bubble drag to the core due to reduced pressure and energy buildup in the affected loop.	Primary side heat transport.	The operator should check if the RCP in the affected loop is off, cover the buttons to prevent against reclosing, and finally electric isolate the RCP.
<b>39</b>	Align condenser exhaust through activated carbon filters.	The operator should align the exhaust through the filters to prevent Radiation release.	N/A	Alignment of condenser exhaust gases through filters using specific OP.
<b>40</b>	Turn on 2 of 4 RCPs	The operator should start 2 of 4 RCPs diametrically opposite to allow the operator cooldown the RCS to RHR entry conditions.	Primary side heat transport.	The operator should choose the RCPs from the intact SGs loops, check if the PZR level is around 6~8m, rise the RCS pressure margin of 5 to 10 bar, turn on the RCPs, and monitor the real pressure in the RCS.
<b>41</b>	Restart RCS cooling down at 50K/h rate and pressure drop.	The operator should restart cooling the RCS and pressure drop to achieve the RHR entry conditions.	Reactor coolant inventory control; and supplying the	The operator should use at least one turbine bypass valve to cooldown RCS until the

			steam generator.	average temperature $\approx 120\text{Cel}$ , and he should pay attention to the level of PZR. If the level drops under 4m, he should stop the cooldown and refill it using the HPSI pump (one is enough). At the same time, the operator should use the auxiliar spray through the KBA system adjusting the valve to decrease pressure until $\approx 31\text{bar}$ . During pressure drop, the operator should maintain pressure margin of 15 bar due to the RCP operation.
<b>42</b>	Verify if RHR condition is achieved	The operator should confirm: - Reactor outlet coolant temperature $\leq 120\text{ Cel}$ ; and - RCS pressure $\leq 31\text{ bar}$ . If the variables are achieved, the operator should go to step 43, if not, the operator should go back to step 41.	N/A	Detect RHR entry condition through the reactor outlet temperature and RCS pressure.
<b>43</b>	Transfer cold source to the residual heat removal (RHR) System.	Transfer reactor cooling through the secondary side for RHR system (JNA).	N/A	Operator shall check the temperature and pressure for RHR entry condition, and then, he should align at least 2 of 4 lines of RHR system and start the correlated line pumps.
<b>44</b>	RCS cooling to cold subcritical condition.	Cooldown RCS to cold subcritical condition through RHR.	N/A	Operator must start the cooldown through specific OP and monitor

				RHR operation during RCs cooldown.
--	--	--	--	------------------------------------

Through the analysis carried out from Table 3 and chapter 15 of FSAR, it is identified that the safety functions which could be affected through the event are:

- **Subcriticality:** The subcriticality of the reactor must be ensured to prevent the reactor power from exceeding the plant's heat removal capacity. Failure to maintain subcriticality may compromise the integrity of the reactor core if other functions are not executed effectively.
- **Primary side coolant inventory:** Make sure there is adequate coolant inventory to effectively remove the heat from the core and facilitates RCS pressure control.
- **Primary side heat transport:** If secondary side heat sink function failure, FRG feed and bleed should be deployed.
- **Secondary side heat sink:** By releasing steam and pumping feedwater into the steam generator (SG), the heat generated in the reactor core is effectively removed and transferred to the secondary side, safeguarding the primary side from overpressure and core integrity. RCS heat removal through feed and bleed can be employed to support this safety function if secondary heat removal fails.
- **Steam generator feedwater supply:** To guarantee heat removal from the reactor core, it is crucial to ensure that there is an enough supply of feed water for the SG. In the case of secondary closed cycle failure, the operator should replenish coolant to the emergency feedwater pools tanks (LAR).

- **Primary circuit integrity:** This function is necessary to prevent RCS boundary to exceed the designed pressure, and also to limit the leakage from the RCS to the secondary side through the ruptured SG.

For the elaboration of the event tree, the following assumptions are considered:

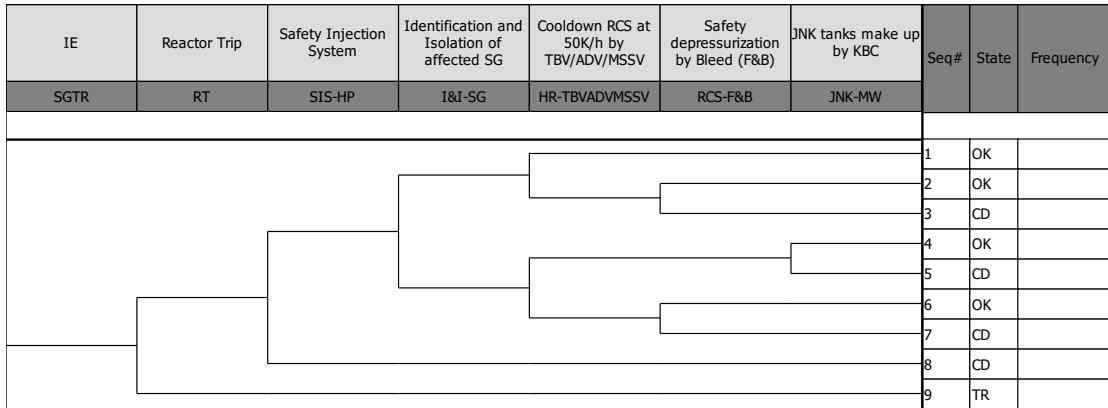
- The rupture occurs in SG10.
- It is not assumed any condition which the operator could not recognize the event or identify if any CSF is not satisfied.
- It is not considered any time spent by the operator reading the thermohydraulic explanation at the beginning of each procedure. It is only assumed that the operator directly executes the procedure steps for composing  $T_{cog}$  and  $T_{exe}$  in the base timeline.
- The sequences are developed until the situation is reached where long-term residual heat removal is maintained through the SGs by dumping steam through turbine bypass or relief valves and feedwater through the emergency feedwater (LAR) system.
- Mission time is 24 hrs.
- Trip failure during SGTR event is assumed transfer to another initiate event and no further sequence of events was model in this event tree.
- In the case of SIS failure (High pressure head), it is assumed core damage due to the absence of operator guidance for rapid cooldown to achieve the low pressure head entry condition for RHR system.
- Considering that the maximum leakage rate due to rupture is 40kg/s and that, in order to uncover the core, the RCS needs to lose 180,000kg, if we conservatively assume that this rate will occur throughout the entire event,

it will result in an available time of 4,500s. On the other hand, cooldown the RCS through 50K/h rate from 300Cel to 120Cel, give us a a delta T of 180Cel, will take 12,960s. Therefore, it is essential to maintain the primary side coolant inventory by the SIS until the operator can cool down the plant and reduce the leakage rate caused by the rupture. Additionally, if it is considered the average rate of 25kg/s instead of the 40kg/s, based on the thermal hydraulics behavior, the available time will be 7200s, even so, the SIS is essential to maintain the primary side coolant inventory. However, if the operator by his action decreases the differential pressure between the RCS and the affected SG, the leakage is almost diminished to zero and the primary side coolant inventory is maintained without the necessity of HPSI actuation.

- It is not considered loss of offsite power.
- The ECCS signal will not close the main steam line isolation valve, allowing the operator to still using the secondary side to cooldown the RCS in a closed cycle through the turbine bypass valve, however, the operator should pain attention to the feedwater tank level alarm, which if the max level is achieve, the protection system will stop the condenser pump, resulting in the loss of the secondary side.
- Situations where the leak cannot be isolated are considered to lead to core damage if there is no means to stop the leak; therefore, if a possible situation leads to flooding of the affected SG, this situation is considered to lead to uncontrolled depressurization of the affected SG and consequently an uncontrolled primary leakage through the u-tube rupture. Therefore, it is

crucial for operator to start cooldown and depressurized the RCS as soon as possible to control the leakage and prevent radiation release.

The event tree developed for Steam Generator Tube Rupture (SGTR) IE in Angra-2 is depicted in Figure 7.



**Figure 7 – Angra-2 SGTR Event tree**

Table 4 provides descriptions of each top event from SGTR event tree. Briefly description of the event, operator and systems actions, and success criteria are provided. The KKS code of each system is wrote between brackets.

**Table 4 – Top event description of SGTR event tree**

SGTR Top Event Descriptions	
Event	Description
SGTR	<p><b>Steam Generator Tube Rupture:</b>            Steam generator tube ruptures include one or more u-tube failure, so that the volumetric and control system (KBA) is not able to maintain the RCS coolant inventory.            The event chosen for this thesis will be the complete rupture 2A of multiple tubes generating a leak for the rupture of the order of 40kg/s and after automatic performances is reduced to approximately 25 kg/s.            The plant behavior is PZR pressure and level decrease; high level of activity in the main steam line; and rise of level in the affected SG. Once the alarm of high level appears in alarm screen the operator will deploy respectively alarm procedure to find out what is happening. The system will automatically identify the SGTR when the activity</p>



	<p>in the main steam line is higher than max level and start executing automatic actions as previously described until reactor TRIP.</p>
RT	<p><b>Reactor TRIP:</b>  The Signal RESA (JR11) is generated by <math>P_{RCS} &lt; 131\text{bar}</math> or 300 sec after detected activity on the affected SG main steam line (JR52). The reactor shutdown system makes the rapid insertion of the control bars. Its objective is to protect the reactor power reduction and the maintenance of subcriticality.  After reactor TRIP, operator should deploy the SPTA procedure (OP-3-1.1/3-1.2) to check plant condition and if all the 6 critical safety functions are satisfied. If anyone is not satisfied, operator should deploy the specific FRG, if all is ok, operator should follow to DA procedure (OP-3-1.3) to identify the event and related procedure to deal with SGTR (OP-3-3.5).  Successful criteria are met when all fuel elements, disregarding the most reactive, are inserted into the core.</p>
SIS	<p><b>Safety Injection System (SIS):</b>  The Safety injection pump (JND) injects borated water into the Reactor Coolant System (RCS) from the Borated Water Storage Tanks (JNK) through either the hot or cold legs. The purpose of the safety injection system is to maintain the RCS coolant inventory by injecting borated water during a loss of coolant accident, ensuring coolant inventory in the primary system and consequently removing residual heat. The safety injection system is activated by the Reactor Protection System (RPS) when the pressure and level in the pressurizer (PZR) are lower than the safety injection system setpoint for activation. In the event of a safety injection failure by the reactor protection system, the operator must intervene manually through FRG.  The success criteria is that 1 out of 4 safety injection pumps provide borated water from the Borated Water Storage Tanks (JNK).</p>
I&I-SG	<p><b>Identification and Isolation of Affected SG:</b>  The affected steam generator (SG) is identified through activity records in the steam and purge lines of the SG, valve positions of main feedwater system (LAB), feedwater flow rates to the SGs, or levels within the SGs [17]. Any potential increase in main steam pressure above 81 bar is constrained using the heating line of the affected SG and by RCS cooling down and depressurization.  The available time frame for carrying out manual actions is approximately 2900 seconds following the occurrence of the S-class alarm "Main Steam Tube Rupture I" (JR06).  Once the tube rupture is identified, the ruptured SG is isolated as follow:</p> <ol style="list-style-type: none"> <li>1. Close SG full load shutoff valve</li> <li>2. Close the SG low load blocking valve.</li> <li>3. Close main steam block valve SG.</li> </ol>

	<ol style="list-style-type: none"> <li>4. Close the SG bloc valve of the main steam relief pressure control valve.</li> <li>5. Close SG main steam relief pressure control valve.</li> <li>6. Close the SG1 purge flow control valve, collector inlet 60.</li> <li>7. Close the SG1 purge flow control valve, collector inlet 50.</li> <li>8. Close the isolation valve of the internal sampling containment "LCQ11".</li> <li>9. Close the external containment isolation valve of the affected SG train.</li> <li>10. Close the SG level control valve.</li> </ol> <p>The success criterion is that the affected SG10 is isolated by closing the MSIV, MISBV, ADVs, AFW, FW, and SG sampling valves.</p>
<p>HR-TBV ADV MSSV</p>	<p><b>Cooldown RCS at 50K/h by TBV/ADV/MSSV:</b>  Feedwater injection into the SG after reactor shutdown is accomplished using one main feedwater pump (LAC) that remains operational, along with two start and stop pumps (LAJ) that start automatically when <math>L_{SG}</math> reaches 10.2 meters or feedwater flow drops below 135 kg/s after reactor Trip. Steam removal is carried out through the turbine bypass valve (TBV - MAN) or main steam relief valve (ADV - LBA) or main steam safety valve (MSSV - LBA), giving priority to the use of the turbine bypass valve, so that the radiation released from the primary to the secondary by the rupture will be confined in the secondary circuit. At this point, the system will maintain secondary pressure around 76 bar through the MAN valves.</p> <p>To achieve cooling at a rate of 50 K/h down to 62 bar at closed cycle, either a main feedwater pump (LAC) or a start and stop pump (LAJ) is required to feed the intact GVs. Steam extraction is performed using one MAN valve. If only the start and stop system (LAH) feeds the SGs, the isolation of purge line is necessary. The loss of both the feedwater and start and stop system (LAB/LAH) to any intact GV will activate the associated emergency feedwater pumps (LAS), introducing external coolant into the closed cycle, potentially causing the loss of the closed cycle if the water level in the feedwater tank (LAA) becomes too high.</p> <p>Success criteria: 1 TBV or 1 ADV or 1 MSSV valve in operation and one feedwater pump or 2 start stop pump with the purge line closed.</p> <p><b>In case of closed cycle failure, operator should replenish emergency feedwater make up tanks by GHC or PE or SGA for long term heat removal:</b></p> <p>If secondary heat removal by closed-cycle is not feasible to cooldown the reactor, the operator's alternative is to maintain primary cooling through the secondary system in an open-cycle arrangement. In this scenario, steam generators are supplied either by the start and stop system (LAH), if there is a water supply from the demineralized water supply system (GHC) to the feedwater tank (LAA), or by</p>

	<p>emergency feedwater pumps (LAR) with steam discharged into the atmosphere through the main steam relief valves (LBA).</p> <p>Residual heat removal is accomplished with one intact steam generator fed by a start and stop pump (LAJ) or an emergency feedwater pump (LAS), and steam extraction via the relief control valve (LBA). In the case of feedwater supplied by a LAS pump, it is necessary to replenish the corresponding pool of the emergency feedwater system (LAR), or two intact steam generators are fed by two LAS pumps with steam extraction through relief control valves, with consideration for replenishing the LAR pools as described below. To sustain long-term feedwater supply with LAH, replenishment of water to the LAA tank is required via the demineralized water supply system (GHC). Water supply from GHC to LAA occurs automatically when LLAA = 1.3 meters [6].</p> <p>On the other hand, to maintain feedwater to the steam generators with emergency feedwater pumps (LAS), water must be replenished to the emergency feed water system (LAR) pools through the Demineralized Water Supply System (GHC), Safety Service Cooling System (PE), or Firefighting Water System (SGA). The available time to begin water replenishment is approximately 3 hours [6]. If feedwater to the SGs via LAR is provided by 2 or more LAS pumps, the available time for replenishing water to the LAR pools is considered sufficiently ample [6]. Conservatively, a time window of 3 hours, equivalent to 10,800 seconds, will be assumed.</p> <p>The operator must identify the low level alarm of the emergency power system pools on the alarm screen, proceed to the 5-LAR-PDO alarm procedure, identify the solution to reestablish the tank level (LAR) and consequently carry out the procedure 3-2.2.4 “Replenish demineralized water”, item 2.3 of section 4.2.2.</p> <p>Success criteria: At least 1 out of 2 pumps (GHC) should be in operation and the pool tanks should be connected by one interconnection valve for each pool (20/30/40) and at least one of the other interconnection valves from (20/30/40).</p>
RCS-F&B	<p><b>Safety depressurization by Bleed (F&amp;B):</b></p> <p>If secondary heat removal (closed and open cycle) is not available and the operator fails to remove the decay heat, he can still remove the decay heat through the feed and bleed operation deploying the specific FRG. It consists of safety injection by the high pressure safety injection pump (JND) and primary relief by the pressurized operated relief valves (POSRVs). This process provides a heat removal path from the core.</p> <p>The success criteria for this event are that 1 of 4 POSRVs must open and 1 JND must inject coolant to RCS.</p>
JNK-MW	<p><b>JNK tanks make up:</b></p> <p>This event evaluates the water supply capacity of JNK tanks. In the event of ruptured steam generator isolation failure and the impossibility to reduce the PZR pressure, eliminating the coolant</p>

	<p>leakage through the rupture, the operator must refill the JNK borated water tanks before exhaustion to prevent the low pressure refrigerant injection pump from cavitating and stopping working. This event follows the failure of the top events: IIC-SG (isolation of damaged SG) or cooldown RCS at 50K/h by TBV/ADV/MSSV (SC-HR). If the level of the JNK tanks is lower than the minimum operating level, they must be filled through the boric acid and demineralized water (KBC) injection system, following the alarm procedure (5-JNK.PDO). The operator operates a boric acid make-up pump to supply water to the JNK (4-2.4.PDO, section 9).</p> <p>The success criterion is that 1 of 2 borated water makeup pumps supply water to the JNK tanks from the boric acid and demineralized water system (KBC).</p>
--	---

On sequence, Table 5 describe each event sequence by stating if each critical safety functions considered are satisfied or not and the specific reason which the sequence leads to core damage.

**Table 5 – Accident sequence description base on affected CSF**

Seq. #	Critical Safety Functions (CSF) condition (OK / NOK)						State
	Sub-criticality	Primary side heat transport	Primary side coolant inventory	Secondary side heat sink	Steam generator feedwater supply	Primary circuit integrity	
1	OK	OK	OK	OK	OK	OK	OK
2	OK	OK	OK	NOK: HR-ADV/TBV/MSSV failure	NOK: HR-ADV/TB/MSSV failure	OK	OK
3	OK	NOK: RCS-F&B Failure	OK	NOK: HR-ADV/TBV/MSSV failure	NOK: HR-ADV/TB/MSSV failure	OK	CD
4	OK	OK	OK	OK	OK	OK	OK
5	OK	OK	NOK: JNK-MW failure	OK	OK	OK	OK

6	OK	OK	OK	NOK: HR-ADV/TBV/MSSV failure	NOK: HR-ADV/TB/MSSV failure	OK	OK
7	OK	NOK: RCS-F&B Failure	OK	NOK: HR-ADV/TBV/MSSV failure	NOK: HR-ADV/TB/MSSV failure	OK	CD
8	OK	NOK: SIS fails	---	---	---	OK	CD
9	NOK: RT	---	---	---	---	OK	TR

#### 4.3 HFE IDENTIFICATION FOR SGTR IN ANGRA-2

Through the detailed analysis of the impact on critical safety functions by the systems/human actions described in the procedure (OP-3-3.5) and the elaboration of the event tree for the SGTR accident, the HFE considered important in the accident mitigation process are:

- Identify and isolate the affected SG – This action is important to control radiation release and to control the leakage by the administration of differential pressure between the RCS and the affected SG. In the case of this HFE failure, the operator should be concerned to replenish the borated water storage system (JNK), because affected SG is considered to be used for RCS cooldown, increasing differential pressure between RCS and affected SG which will rising the leakage rate. Those tanks are the supply tanks used by the SIS to recover RCS inventory and operator should use the boric acid and demineralized water injection system (KBC) to make up the JNK tanks. Additionally, this condition would result in radiation release to

the environment through the MSRVs or MSSVs in the case of cooling at 50K/h in the open cycle, releasing radiation, which is one of the safety goals, however, it is still possible to cooldown the reactor core in the case of SG identification and isolation failure. The consequences are primary inventory lost to outside of the containment and the necessity to replenish for long term heat removal.

- Cooldown RCS at 50K/h by TBV/ADV/MSSV – This human failure event comprehends the followings tasks: cooldown RCS as soon as possible using priority the turbine bypass valve, considering control of radiation release and to conserve SG feedwater supply, or relief valve or main steam safety valves. Additionally, operator should monitor and maintain the level on the feedwater storage tank (LAA) to avoid loss of the closed cycle; If closed cycle is lost, operator should replenish the pools tanks (LAR) and connect then after low level is achieved to maintain the SG feedwater supply function. These actions are done to maintain the followings safety functions: secondary side heat sink; and SG feedwater source.
- RCS depressurization: Operator should depressurize RCS to maintain coolant boundary integrity, prevent radiation release by avoiding rise of affected SG pressure resulting in radiation release by MSSV pressure relief, and to diminish the leakage from RCS to the affected SG bypassing the containment. In the case of affected SG identification and isolation failure, the operator still can reduce pressure, however, the leakage through the rupture is not minimized like the first condition and the operator should be

concerned to replenish the borated water storage system (JNK). The HEP for this HFE was not considered for this analysis.

- Feed and bleed: In the case of RCS cooldown at 50K/h failure, the operator should deploy the FRG (OP-3-2.2.2) to cooldown reactor by feed and bleed. The HEP for this HFE was not considered for this analysis.
- JNK tanks make up: In the case of failure to identify and isolate the affected SG, it is considered that during the cooldown coolant from the RCS will remain leakage to the affected SG and will be part of RCS cooling process affecting the CSF Primary side coolant inventory. Therefore, the operator should replenish the demineralized water from the JNK tanks by the KBC system to maintain the CSF Primary side coolant inventory.

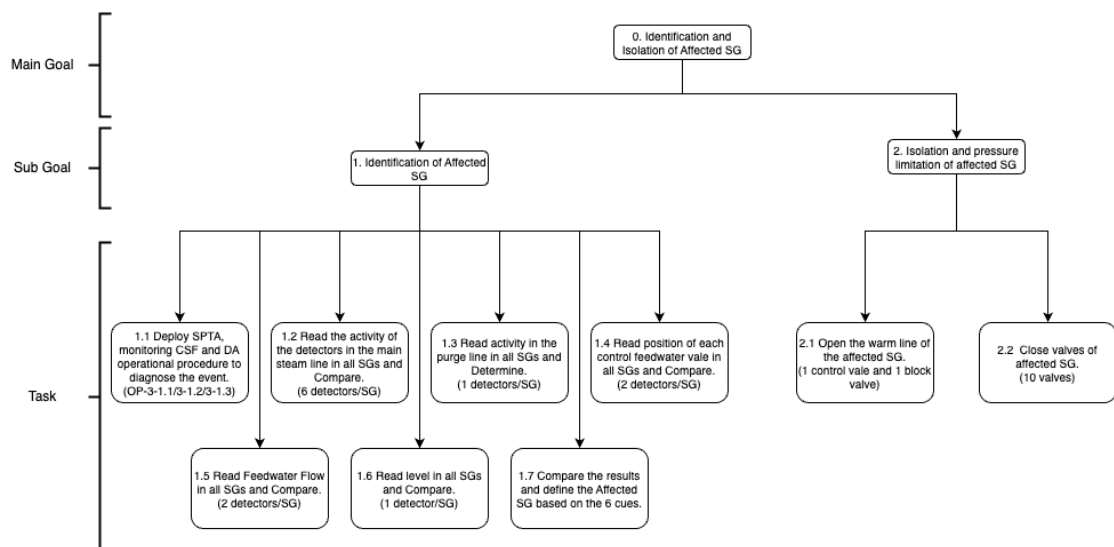
NOTE: Only the two first HFE are considered subject for HEP quantification for this report.

#### **4.4 TASK ANALYSIS OF THE HFE IDENTIFIED FOR ANGRA-2 DURING SGTR**

In this section a simple task analysis is performed to outline the actions performed as part of a main activity to provide a systematic means to organize the information collected relating to the task. The Hierarchical Task Analysis (HTA) method was employed for this investigation. HTA is a simple and flexible methodology that decomposes the task into subtasks using a hierarchical structure with higher-level goals and lower-level tasks to achieve those goals [18]. For each HFE was build a flowchart to define the main goal, sub-goals and tasks to accomplish sub-goals and finally the main task. If the action does not represent any issues for the equipment or

system response and will not impact the safety function related to the main goal, this action will be disregarded in the construction of the flowchart.

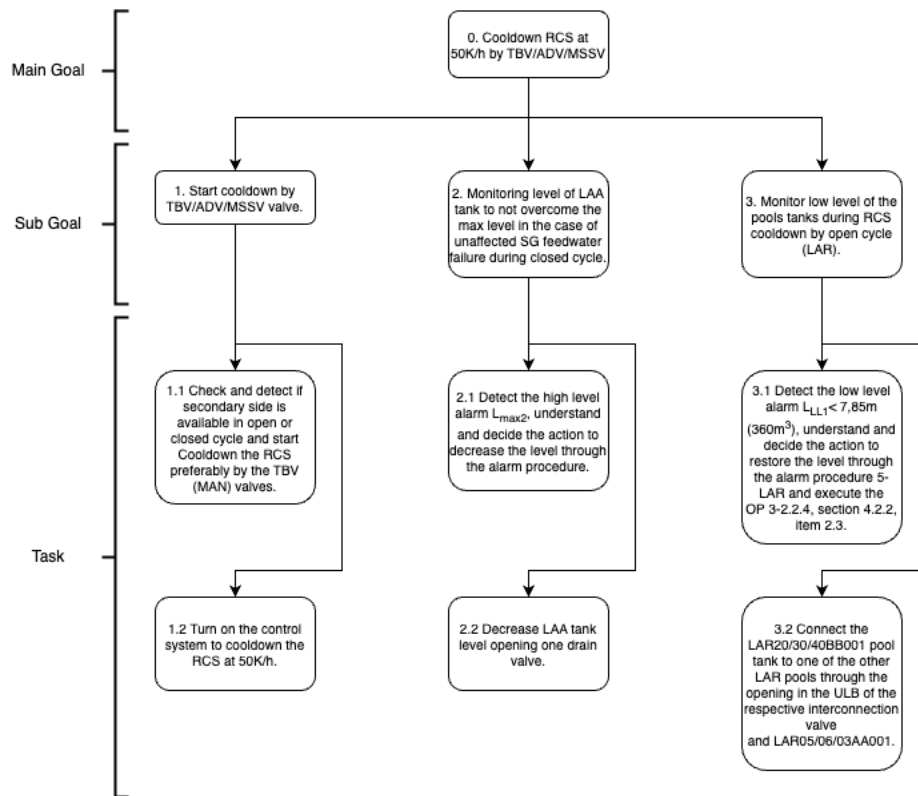
Figure 8 shown the HTA for the HFE – Identification and Isolation of affected SG. The task decomposition was made based on the actions done by the operator guided by the SPTA (OP-3-1.1/3-1.2), DA (OP-3-1.3) and SGTR emergency procedure (OP-3-3.5) until the step to isolate the affected SG.



**Figure 8 – HTA for HFE: Identification and Isolation of affected SG**

The figure 9 shown the HTA for the HFE – Cooldown RCS at 50K/h by TBV/ADV/MSSV. The task decomposition was made based on the actions done by the operator guided by the SGTR emergency procedure (OP-3-3.5) and previous HRA considerations from Angra-2 PSA.





**Figure 9 - HTA for the HFE: Cooldown RCS at 50K/h by TBV/ADV/MSSV**

#### 4.4.1 IDENTIFICATION OF ERROR MODES

After the definition of the basic task for each subgoals to accomplish the goal, it was applied the error mode for each task done by the operator using the Systematic Human Error Reduction and Prediction Approach (SHERPA) taxonomy. The SHERPA taxonomy makes use of hierarchical task analysis (HTA) that hierarchically organizes the steps of a task to apply the types of possible errors, in other words, the taxonomy is used to identify credible errors associated with a sequence of human activity. SHERPA provides a taxonomy of errors including action, retrieval, check, selection, and information communication errors, as shown in Table 6. SHERPA considers mainly actions, perceptual, and communication errors and it is recommended by the literature

to add cognitive items to augment SHERPA taxonomy [18]. In this way, Table 7 shown the additional cognitive items used in this analysis.

**Table 6 – SHERPA error taxonomy**

<i>Actions Errors</i>		<i>Checking Errors</i>	
A1	Action too long/short	C1	Checking omitted
A2	Action mistimed	C2	Check incomplete
A3	Action in wrong direction	C3	Right check on wrong object
A4	Action too little/too much	C4	Wrong check on right object
A5	Misaligned	C5	Check mistimed
A6	Right action on wrong object	C6	Wrong check on wrong object
A7	Wrong action on right object	<i>Retrieval Errors</i>	
A8	Action omitted	R1	Information not obtained
A9	Action incomplete	R2	Wrong information obtained
A10	Wrong action on wrong object	R3	Information retrieval incomplete
<i>Information Communication Errors</i>		<i>Selection Errors</i>	
I1	Message not transmitted	S1	Selection omitted
I2	Wrong message transmitted	S2	Wrong selection made
I3	Message transmission incomplete		

**Table 7 – Additional cognitive items to augment the SHERPA taxonomy**

<i>Decision Errors</i>	
D1	Correct decision based on wrong/missing information
D2	Incorrect decision based on right information
D3	Incorrect decision based on wrong/missing information
D4	Failure to make a decision (impasse)

#### **4.4.1.1 Error modes applicable to HFE: Identification and Isolation of affected SG**

Table 8 shows the defined error modes applied for each task based on the activity description.

**Table 8 – Error modes applied for HFE: Identification and Isolation of affected SG**

<b>Task #</b>	<b>Task activity</b>	<b>Description</b>	<b>Error Modes (SHERPA)</b>
1.1	Operator should deploy SPTA to check plant condition and if CSF is satisfied, and DA to identify the event and find out the proper OP to deal with this event.	The procedure is diagnose and symptom-oriented guiding the operator to make decisions through the flowchart. The information is well provided and the error modes applicable are related to decision error. However, inside the control room has five minds to revise any decision and the procedure has double check.	D1; D2
1.2	The operator should read the activity in the main steam line to compare the values and find out which SG has the highest activity value.	The operator will check out for one cue in several instruments (6 for each SG). Therefore, he certainly will read the activity in all of instruments, however, he could read it in a wrong instrument, or he could omit the reading of some instrument. Due to wrong/missing information the operator could select the wrong SG, so, it is considered checking errors.	C1; C2; C3
1.3	The operator should read the activity in the purge line and compare which SG has the highest value.	The operator will check one cue in one instrument in each SG. It is necessary to read all 4 instruments to be able to compare and decide the correct affected SG, so, it is considered checking errors.	C1; C2
1.4	The operator should read the opening % at control valves to compare which has the lowest value.	The operator will check one cue in two control valves (full load and low load) in each SG. It is necessary to identify opening % in all valves in each SG to be able to compare and decide the correct affected SG, so, it is considered checking errors. Additionally, the operator could read one de value in only one valve for a certain SG and decide that this value is	C1; C2; C3

		the reference, however, this valve could not be the operational valve during the value check, giving to the operator a false value for decision.	
1.5	The operator should read the flow at least in one instrument located in each SG feedwater line to be able to compare the lowest flow.	In each SG has 2 instrument to measure the feedwater flow. The operator should read at least one instrument in each SG to be able to compare the values. In this way, it is considered checking errors.	C1; C2
1.6	The operator should read the level in each SG and compare the values.	In each SG has 1 instrument to indicate the second max high level. The operator should read each instrument for all SG. It is considered checking error.	C1; C2
1.7	The operator should compare the results obtained in the task 1.1 to 1.5 and decide the SG that should be isolated.	This decision depends on the correct readings from the task 1.1 to 1.5, so, it is considered correct decision because the procedure is based on guided decisions, however, the selection will be made based on data checking error or wrong information, so, it is considered checking and decision errors.	D1; S2
2.1	The operator should open the warm line of the affected SG through 1 block valve and 1 control valve.	The action is simple and has only 2 valves to actuate in the affected SG, however, it is considered that the operator could do this action in the wrong SG, or he could omit the action in one valve. It is considered action error. The selection will be made based on data checking error or wrong information.	A6; A8
2.2	The operator should close all valves connected to the SG	Each SG has 10 valves to be closed, so, it is considered that the operator could do this action in the wrong SG, or he could omit the action in one valve, so, it is considered action errors.	A6; A8

Task 1.1 to 1.7 were applied error modes related to build up data for plant condition, identification of the event and what SG is affected. These actions are guided by SPTA, DA and related emergency procedure, and the operator are trained to recognize easily. It comprises most of reading cues and check conditions to understanding and decide that SGTR is occurring. Therefore, the task 1.1 to 1.7 are considered cognitive activities for HEP quantification. In the other hand, the error modes for the tasks 2.1 and 2.2 are pure execution of the SG isolation through valve alignment. These tasks are simple and straightforward the possible errors modes considered are operation omission, the operator could skip some action on an equipment, or commission, due to execute the operation on the wrong equipment. Therefore, the tasks 2.1 and 2.2 are considered execution activities for HEP quantification.

In conclusion, it is assumed that all tasks in Table 8 belong to the same HFE defined as HFE1 - identification and isolation of the affected SG. This consideration is in line with is stated in the step 5 of the reference [18], which indicates that any tasks associated with a particular hardware system or safety function outcome should be consolidated into a unified HFE.

#### **4.4.1.2 Error modes applicable to HFE: Cooldown RCS at 50K/h by MAN/TBV/MSSV**

Table 9 shows the defined error modes applied for each task based on the activity description.

<b>Task #</b>	<b>Task activity</b>	<b>Description</b>	<b>Error Modes (SHERPA)</b>
1.1	Check and detect if the secondary side is available to cooldown	The operator should check if at least 1 of 6 TBVs (MAN) or 1 of 4 ADVs (LBA) or 1 of 8 MSSVs valves is	A8; S2

	the RCS in closed cycle or open cycle.	available to operate and select the valve to operate giving preference to cooldown using the TBVs. Therefore, it is considered action and selection error.	
1.2	Turn on the control system of turbine bypass valve at 50K/h to cooldown the RCS. (1 control system actuation)	The operator should press one switch to turn on the control system to start the cooldown at 50K/h. It is a very simple action, and the action error mode is considered.	A8
2.1	Detect the high level alarm $L_{max2}$ , understand the condition and decide the plan action to decrease the level through the alarm procedure.	During the cooling of the RCS at a rate of 50K/h in closed cycle, the operator must be aware of the possibility of failure of the stop and start pumps and/or the main power supply of the SG, so that this condition in closed cycle is not lost. This task is a condition outside the procedure flowchart and the operator must be aware of this event as soon as it occurs. In this case, the diagnostic action is not guided by the logical flowchart, however, it is guided by the alarm procedure which is outside of the logic flowchart. In this case, the operator must detect, understand and decide what to do. Therefore, after the high level alarm in the LAA tank, the operator must identify the alarm, understand that if no action is taken, it will trigger a sequence of actions by the protection system that will make it impossible to cool the RCS through the closed cycle and he need to act as soon as possible to avoid it. The issue is that the operator should choose the correct plan in the alarm procedure and there is no place to mark each solution verified. In this way, the error mode applied for this action is that the	C1; R1; R2; D1; S2

		operator may omit to check a possible solution, correct decision based on incorrect information, or may incur a wrong selection in the alternative solution for the issue.	
2.2	Decrease LAA tank level opening 1 drain valve.	The operator should open 1 drain valve to maintain the level under the second max level alarm for the LAA tank. The action error mode is considered.	A6; A8
3.1	Detect the low level alarm $LLI < 7,85m$ ( $360m^3$ ), understand and decide the action to restore the level through the alarm procedure 5-LAR and execute the OP 3-2.2.4, section 4.2.2, item 2.3 “Replenish demineralized water”.	During the cooling of the RCS at a rate of 50K/h in open cycle, the operators need to detect low levels in the tanks and the need to replenish water in the demineralized water pools of the Emergency Feeding Water System (LAR) trains in operation. This task is a condition outside the procedure flowchart and the operator must be aware of this event as soon as it occurs. In this case, the diagnostic action is not guided by the logical flowchart, however, it is guided by the alarm procedure which is outside of the logic flowchart. In this case, the operator must detect, understand, and decide what to do. Therefore, after the low level alarm in the pools tanks (LAR), the operator must identify the alarm, understand that if no action is taken, the SGs will be empty and not capable to cooldown the RCS due to the loss of emergency SG feedwater source. The issue is that the operator should choose the correct plan in the alarm procedure and there is no place to mark each solution verified. In this way, the error mode applied for this action is that the operator may obtained incomplete information or omit to check all the possible	C1; R2; D1; S2

		solutions, correct decision based on incorrect information, or may incur a wrong selection in the alternative solution for the issue.	
3.2	Connect the LAR 20/30/ 40BB001 pool tank to one of the other LAR pools through the opening in the ULB of the respective inter-connection valve and LAR05/06/03AA 001 to replenish demineralized water.	The operator must start the demineralization system (GHB), the demineralized water supply system (GHC) to replenish pool tanks (LAR) and connect the pools tanks (LAR) of the SG emergency feedwater system (LAR). These are sequential operations of valves and pumps, where part of the valves operated are carried out by the field operator. The error mode applicable are action error and information error due to external communication.	A6; A8; I2; I3

In this analysis, the primary objective of human action is to cool the Reactor Coolant System (RCS) at a rate of 50K/h with preference in closed cycle to avoid radiation release. This top event is crucial to mitigate the SGTR (Steam Generator Tube Rupture) accident allowing RCS cooling and depressurization to avoid solidification of affected SG, to maintain the feedwater inventory of the intact steam generators ensuring backup water supply for the SGs during the cooling process. To support this top event, 3 subgoals are required and they are defined as follows:

- I. Initiate the cooling through the turbine bypass valves - this is the main action to promote RCS cooldown.
- II. Detect the high-level alarm of the LAA tank in case of failure of the SG feedwater pumps - this action aims to maintain closed-loop cooling and secure the feedwater inventory of the SGs in case of a closed-loop loss due to the failure of the main feedwater pumps or trip.



- III. In the case of closed-loop RCS cooling failure, the operator should detect the low level alarm to replenish the emergency feedwater system inventory by starting the GHC and GHB system and connecting the pools tanks (LAR) through demineralized water replenish valves and connection valves.

For HEP quantification, it is assumed that each subgoal will be considered as one HFE. Even though, the tasks are associated with a particular safety function, however, each subgoal is associated with different system failure. Therefore, subgoal 1 will be HFE2 - Cooldown RCS at 50K/h by TBV/ADV/MSSV, subgoal 2 will be HFE3 - Drain the feedwater tank (LAA) in case of SG feedwater pump failure, and subgoal 4 will be HFE4 - Replenish emergency feedwater tanks (LAR) for RCS long term cooling. To achieve the main objective successfully, it is necessary for the operator to accomplish the HFE2, and to detect and act if the HFE3 and HFE4 occurs. Each HFE, subject of the main goal, should be considered in the fault tree for the top event Cooldown RCS at 50K/h by TBV/ADV/MSSV.

#### **4.4.2 HFE DEFINITION**

This section describes the scope of the analysis and identifies the key point for each HFE.

##### ***4.4.2.1 HFE1: Identification and Isolation of affected SG***

After the RTGV occurs, the reactor's limitation and protection system will perform several automatic actions to mitigate the accident. When the operator identifies the alert of activity in the main steam line above the maximum allowed and subsequently the TRIP of the reactor, the operator must execute the SPTA procedure to

check the condition of the plant and whether any safety function is not ensured (OP -3-1.1/3-1.2). If any CSF is violated, the operator must proceed to the specific FRG to reestablish the safety function. If all are satisfied, the operator must execute the DA (OP-3-1.3) to identify the event in question. Once the event is identified, the operator will execute the procedure that deals with SGTR to identify the ruptured SG and isolate it.

It is considered that the operator stress is affected due to intermittent alarms that occur during the event and to the legal and environmental consequences that may occur based on the high probability of radiation release given that the primary coolant is bypassing the containment limits, furthermore, several variables should be monitored implying in the complexity of the human actions.

During the process of identifying the plant condition and the initiating event, the procedures that are Diagnostic/Symptom-oriented prevent possible decision errors on the part of the operators which will be guided during the event. There are 5 variables to identify the affected SG allowing self-review of the diagnose and then the operator should close all 10 valves to isolate it. The isolation could be rechecked if affected SG pressure decrease during cooldown.

The error modes applicable to HFE1 in section 4.4.1.1 are mitigated by considering that the KKS code and three-way communication prevent decision, selection, verification, omission, and commission errors.

Scenario description:

- I. Initial condition: Steady state, full power operation
- II. Initiating event: SGTR

- III. Operator action success criteria: Operator should identify the occurrence of SGTR, and then he should identify the affected SG and isolate it to reduce the leakage as soon as possible maintaining the pressure of RCS above 2 to 3 bar of the affected SG.
- IV. Consequence of failure: The affected SG will be solid if this action is not taken. With the solid SG the relief valve will oscillate between open and closed to reduce the pressure of the ruptured SG, resulting in a condition where the operator will no longer be able to control the loss of refrigerant from the primary to atmosphere. The time available for this action is 1925 seconds based on thermohydraulic simulation in Angra-2 simulator after the JR52 signal.
- V. Cue: maximum activity reached in the main steam line, reactor trip and containment pressure constant.

#### **4.4.2.2 HFE2 - Cooldown RCS at 50K/h by TBV/ADV/MSSV**

HFE2 is a straightforward execution guided by the procedure and it is considered only action part for quantification using SPAR-H. This HFE2 is comprised of the tasks 1.1 and 1.2 where the operator should check the availability of the bypass or ADVs or MSSVs valves to cooldown RCS. Preferably, the operator should select the TBV valve to start the cooldown at 50K/h.

It is considered that the operator stress is affected due to intermittent alarms that occur during the event and to the legal and environmental consequences that may occur based on the high probability of radiation release given that the primary coolant is

bypassing the containment limits, furthermore, several variables should be monitored implying in the complexity of the human actions.

KKS code and three-way communication prevent the error modes applied in section 4.4.1.2

Scenario description:

- I. Initial condition: Steady state, full power operation
- II. Initiating event: SGTR
- III. Operator action success criteria: start cooldown at 50K/h by 1 of 6 turbine bypass valve (MAN).
- IV. Consequence of failure: The affected SG will be solid if this action is not taken. With the solid SG the relief valve will oscillate between open and closed to reduce the pressure of the ruptured SG, resulting in a condition where the operator will no longer be able to control the loss of refrigerant from the primary to atmosphere. The time available for this action is 1925 seconds based on thermohydraulic simulation in Angra-2 simulator after the JR52 signal.
- V. Cue: TAVG constant and SG level and pressure rising.

#### **4.4.2.3 HFE3 - Drain the feedwater tank (LAA) in case of SG feedwater pump failure**

The HFE3 demand by the operator to detect, understand, and plan what to do based on the alarm procedure (OP-5-LAA), therefore, it is considered the diagnose and action part for HEP quantification using SPAR-H. The HFE3 comprised by the tasks 2.1 (diagnose part) and 2.2 (execution part). In the event of a failure of the feedwater pumps (LAC) and the generator steam's stop and start system (LAJ), there will be a

water inventory imbalance in the secondary feedwater tank (LAA) operating in a closed cycle, resulting in an increase in the LAA tank level. When the tank level reaches 2.7m, the high-level 1 alarm will be triggered as the operator's initial alert. The operator will then execute the corresponding alarm procedure (OP-5-LAA). Upon reaching a tank level of 2.85m and triggering the high-level 2 alarm, the operator is already aware of the LAA tank level increase. In the high-level 2 alarm, the operator will be instructed to open the drain valve (LAA10AA051).

It is considered that the operator stress is affected due to intermittent alarms that occur during the event and to the legal and environmental consequences that may occur based on the high probability of radiation release given that the primary coolant is bypassing the containment limits, furthermore, several variables should be monitored implying in the complexity of the human actions.

Potential error modes applied in the SHERPA analysis are mitigated by the three-way communication structure using KKS encoding. Additionally, operators are trained to identify and recognize alarms during accident conditions, and in this scenario, two alarms are generated for the same event. However, the alarm procedure is in narrative form and does not have a specific place to mark the actions performed and should be accounted.

Scenario description:

- I. Initial condition: RCS cooldown by turbine bypass valve in closed cycle (MAN).
- II. Initiating event: SG Feedwater pump failure and start and stop pump failure.
- III. Operator action success criteria: open one drain valve in the LAA tank.

- IV. Consequence of failure: loss of RCS cooldown by closed cycle.
- V. Cue: High level alarm max2 in the LAA tank.

#### **4.4.2.4 HFE4 - Replenish emergency feedwater tanks (LAR) for RCS long term cooling**

The HFE4 demand by the operator to detect, understand, and plan what to do based on the alarm procedure (OP-5-LAR), therefore, it is considered the diagnose and action part for HEP quantification using SPAR-H. The HFE4 comprised by the tasks 3.1 (diagnose part) and 3.2 (execution part).

In the event of the operator's failure to prevent the feedwater tank (LAA) level from rising to high level 3, the protection system will turn off the main condensate system (LCB) pumps, causing the loss of RCS cooling by the secondary in closed cycle. In this scenario, the SG relief will be through the ADVs valves, and the SG supply will be through the emergency feed water system (LAR). As soon as the emergency power supply pumps start, when the SG level reaches 5m, the level of the pool tanks (LAR) drops and when it reaches below 7.85m (low level 1) the operator must carry out the alarm procedure corresponding (OP-5-LAR) to reestablish the supply water inventory of steam generators for long-term heat removal. Among the operator's actions in the alarm procedure, he must execute the FRG relating to the critical safety function "steam generator water supply".

It is considered that the operator stress is affected due to intermittent alarms that occur during the event and to the legal and environmental consequences that may occur based on the high probability of radiation release given that the primary coolant is bypassing the containment limits, furthermore, several variables should be monitored implying in the complexity of the human actions.

Potential error modes applied in the SHERPA analysis are mitigated by the three-way communication structure using KKS encoding. Additionally, operators are trained to identify and recognize alarms during accident conditions and each tank will trigger its own alarm, so, more than one alarm from the unaffected SG LARs pool are generated for the same event. However, the alarm procedure is in narrative form and does not have a specific place to mark the actions performed and should be accounted.

Scenario description:

- I. Initial condition: RCS cooldown by the main steam relief valve in open cycle (ADV).
- II. Initiating event: Emergency feedwater pool tanks (LAR) achieve the low level  $< 7,85\text{m}$  ( $360\text{m}^3$ ) generating an alarm.
- III. Operator action success criteria: connecting the pool tanks 20/30/40 through the connection valve and replenish the water by the replenish valve. 2 valve per pool tank should be open.
- IV. Consequence of failure: The available demineralized water may not be sufficient to cover the demand required in the event of an accident, affecting safety function Cold source of secondary side and Steam generator feedwater.
- V. Cue: Low level alarm  $< 7,85\text{m}$  in the pool tank (LAR).

#### **4.4.3 TIMELINE ANALYSIS**

In this section, for each HFE, time estimates are detailed and summarized graphically.

#### **4.4.3.1 HFE1: Identification and Isolation of affected SG**

Timing analysis:

- I.  $T_0 = 0s \rightarrow$  SGTR occurrence.
- II.  $T_{sw} = 2900s \rightarrow$  This is the time considered for the affected SG to be overfilled. The time window is based on current Angra-2 PSA document [3].
- III.  $T_{delay} = 320s \rightarrow$  The time delay is based on FSAR chapter 15, and this is the time for Angra-2 NPP to achieve the point where the operator has all the cues to start the diagnose [4].
- IV.  $T_{cog} = 780s \rightarrow$  The diagnose time for SGTR identification is based on current Angra-2 PSA document [3]. This mean time consists of the operator diagnose through the Standard Post Trip Action (SPTA) to analyze plant condition and if all safety functions are meet and then to execute the diagnose Analysis (DA), identifying the event until the point where the operator identifies the affected SG in the EOP-step#2.
- V.  $T_{exe} = 300s \rightarrow$  The execution time is based on current Angra-2 PSA document [3]. This mean time consist of the isolation of the affected SG based on the guidance by the EOP-step #3.



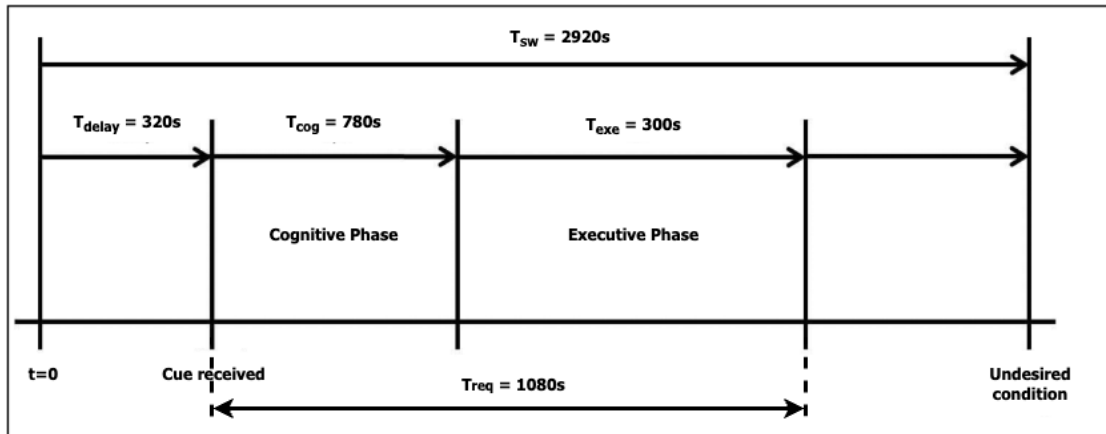


Figure 10 - Timeline diagram for HFE1

#### 4.4.3.2 HFE2 - Cooldown RCS at 50K/h by TBV/ADV/MSSV

Timing analysis:

- I.  $T_0 = 0\text{s} \rightarrow$  The operator finishes executing the step#3 of the OP [1].
- II.  $T_{\text{sw}} = 1520\text{s} \rightarrow$  The time window is based on the time to overfill the affected SG, the same used for HFE1, subtracting the time spent by the operator to diagnose and finish the step#3 of the OP [17].
- III.  $T_{\text{delay}} = \text{N/A}$ .
  - d.  $T_{\text{cog}} = \text{N/A}$ .
  - e.  $T_{\text{exe}} = 300\text{s} \rightarrow$  This action consists of the start of RCS cooling through the unaffected SG based on the guidance by the EOP-step #4. The PSA from Angra-2 state that the time required to execute this action is 300 seconds [3]. This action is based on verification of the availability of TBV and ADV valves, set the valve, and turn on the cooldown at 50K/h.

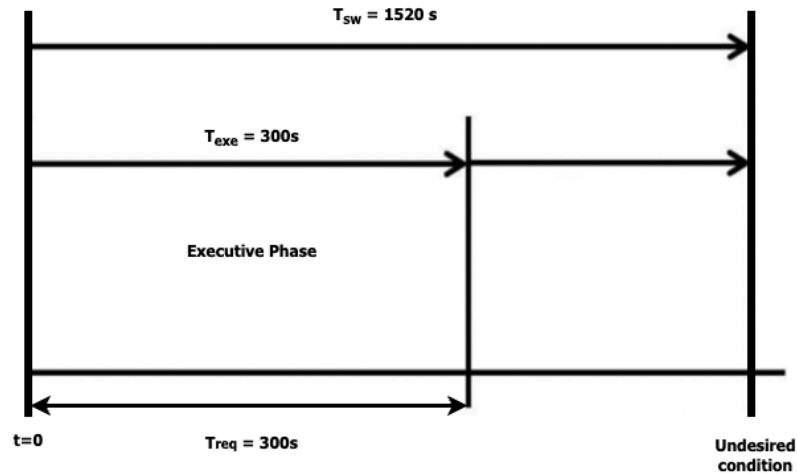


Figure 11 - Timeline diagram for HFE2

#### 4.4.3.3 HFE3 - Drain the feedwater tank (LAA) in case of SG feedwater pump failure

Timing analysis:

- I.  $T_0 = 0\text{ s} \rightarrow$  The high level max 2 in LAA tank is achieved producing an alarm.
- II.  $T_{sw} = 5400\text{ s} \rightarrow$  Based on the PSA for Angra-2, the time window for the level of the LAA tank to rise from 2.85m to 3.2m is 1:30 min (5400 seconds) [3].
- III.  $T_{delay} = 25\text{ s} \rightarrow$  Based on the literature, the operator during an accident mitigation takes around 25 seconds to acknowledge an alarm [19].
- IV.  $T_{cog} = 300\text{ s} \rightarrow$  In the absence of data from Angra-2 PSA for this HFE, it will be considered, based on FSAR and literature, 5 minutes for the cognition time and 1 min for execution time of each step in a procedure [4][8]. Considering that,  $T_{cog}$  for detect the alarm, get the alarm procedure, understand that the rise of the LAA tank could cause the loss of the condenser pump (LCA) will take 300 seconds.

- V.  $T_{exe} = 300s \rightarrow$  In the absence of data from Angra-2 PSA for this HFE, it will be considered, based on FSAR and literature, 5 minutes for the cognition time and 1 min for execution time of each step in a procedure [4][8]. Considering that, once the operator diagnoses the event, he should execute all the 5 possible solutions to this alarm which will take 300s.

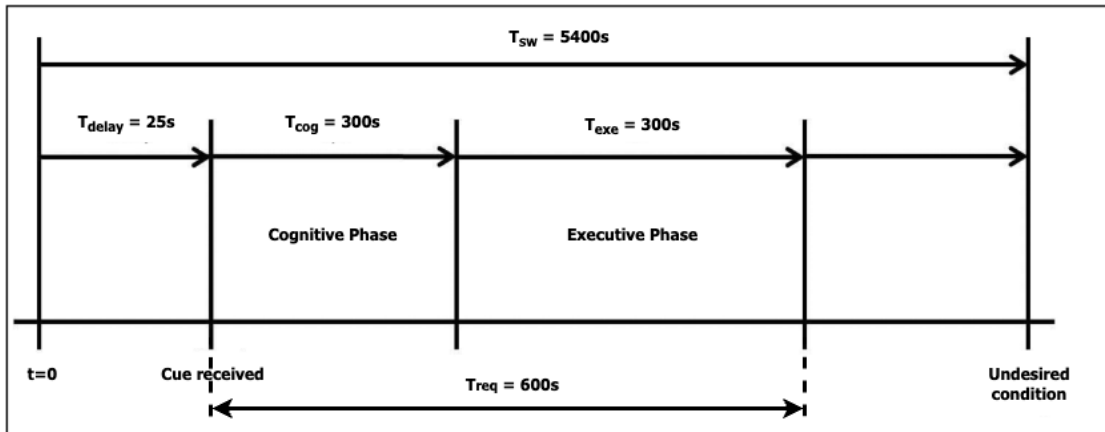


Figure 12 - Timeline diagram for HFE3

#### 4.4.3.4 HFE4 - Replenish emergency feedwater tanks (LAR) for RCS long term cooling

Timing analysis:

- I.  $T_0 = 0s \rightarrow$  The level of the LAR tank will achieve the low level  $< 7,85m$  producing an alarm which will trigger the cue for the operator to recognize it [3].
- II.  $T_{sw} = 11.972s \rightarrow$  Based on the PSA for Angra-2, the time window for the level of the LAR tank to be empty from  $L < 7,85m$  (360m<sup>3</sup>) is 199,5 minutes [3].
- III.  $T_{delay} = 25s \rightarrow$  Based on the reference, the operator during an accident mitigation takes around 25 seconds to acknowledge an alarm [19].

- IV.  $T_{\text{cog}} = 300\text{s}$  → Based on the angra-2 PSA analysis [3][4], it is considered 5 min for the operator to diagnose the situation and identify the proper solution through the alarm procedure which will guide him to execute the OP- 3-2.2.4, section 4.2.2, action #3.
- V.  $T_{\text{exe}} = 2400\text{s}$  → Once the operator identifies the alarm and diagnoses the necessity to replenish and connect the pool tanks (LAR), the operators would spend 40 minutes to carry out all the necessary maneuvers in the MCR and locally by filed operator to open all the interconnection valves of the LAR pools [3].

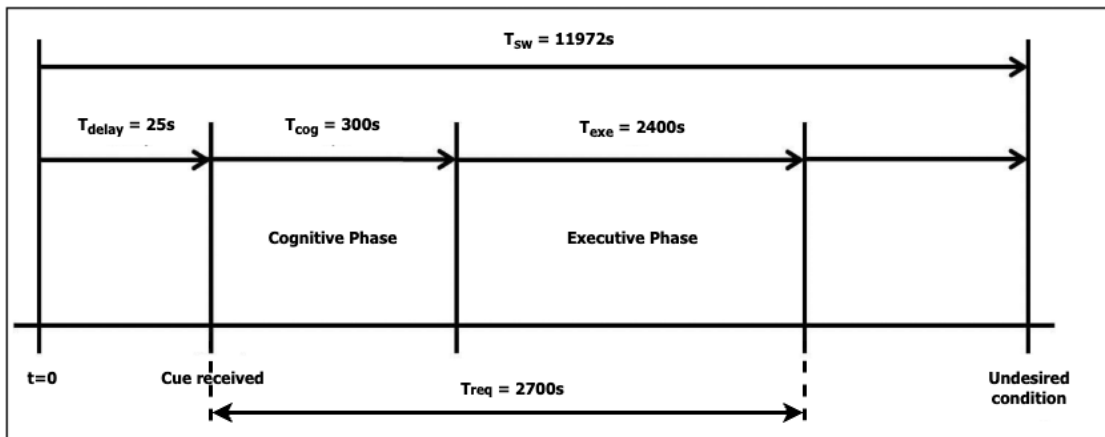


Figure 13 - Timeline diagram for HFE4

## **5 CURRENT ANGRA-2 HRA ASSESSMENT AND HEP RESULTS**

In this section, the results obtained from the human reliability analysis conducted for the steam generator rupture event in Angra-2 will be presented, considering the same human failure events (HFE) addressed in this study. This will enable a comparative analysis of the outcomes derived from the CBDTM, HCR/ORE, THERP, SPAR-H, and IDHEAS-ECA methods, aiming to assess the consistency, reliability, and qualitative enhancement that IDHEAS-ECA will provide, as proposed by the NRC.

### **5.1 BRIEFLY DESCRIPTION OF ANGRA-2 HRA**

In the human reliability analysis conducted within the probabilistic risk assessment of Angra-2 was chose to adhere to the EPRI's recommendation, wherein the probability of error in the cognitive phase ( $P_c$ ) is determined using the CBDTM and HCR/ORE methods, and the probability of error in the executive phase ( $P_e$ ) is derived through the THERP method. Additionally,  $P_c$  will be composed by the highest value calculated between the CBDTM and HCR/ORE methods, assuming a conservative approach. In summary, the final Human Error Probability (HEP) value is the sum of  $P_c$  and  $P_e$ , where  $HEP = P_c + P_e$ .

## 5.2 HEP RESULTS FROM ANGRA-2 HRA FOR THE HFE CONSIDERED

### 5.2.1 HFE1: IDENTIFICATION AND ISOLATION OF AFFECTED SG

Table 9 – Angra-2 HRA HEP result for HFE1

HFE	Method			Final HEP
	CBDTM	HCR/ORE	THERP	
	P <sub>c</sub>	P <sub>c</sub>	P <sub>e</sub>	
Identification and Isolation of affected SG	5.0E-04	N/A	5.3E-03	5.8E-03

### 5.2.2 COOLDOWN RCS AT 50K/H BY TBV/ADV/MSSV

Table 10 - Angra-2 HRA HEP result for HFE2

HFE	Method			Final HEP
	CBDTM	HCR/ORE	THERP	
	P <sub>c</sub>	P <sub>c</sub>	P <sub>e</sub>	
Cooldown RCS at 50K/h by TBV/ADV/MSSV	4.4E-04	8.3E-04	1.1E-04	9.4E-04

### 5.2.3 DRAIN THE FEEDWATER TANK (LAA) IN CASE OF SG FEEDWATER PUMP FAILURE

Table 11 - Angra-2 HRA HEP result for HFE3

HFE	Method			Final HEP
	CBDTM	HCR/ORE	THERP	
	P <sub>c</sub>	P <sub>c</sub>	P <sub>e</sub>	
Drain the feedwater tank (LAA) in case of SG feedwater pump failure	5.5E-03	N/A	2.6E-03	8.1E-03

## 5.2.4 REPLENISH EMERGENCY FEEDWATER TANKS (LAR) FOR RCS LONG TERM COOLING

Table 12 - Angra-2 HRA HEP result for HFE4

HFE	Method			Final HEP
	CBDTM	HCR/ORE	THERP	
	$P_c$	$P_c$	$P_e$	
Replenish emergency feedwater tanks (LAR) for RCS long term cooling	5.1E-03	3.6E-15	1.3E-03	6.4E-03

## 6 HRA ASSESSMENT BY SPAR-H

In this section, it is calculated the HEP for each HFE defined in section 4 for SGTR in Angra-2 following the worksheet from SPAR-H method. The reference information considered for HEP quantification are described in section 4. For each HFE event is calculated the cognitive part and the action part and if a HFE does not consider any of the  $P_{diagnose}$  or  $P_{action}$ , this part unconsidered is applied zero to compose the final HEP.

### 6.1 HEP QUANTIFICATION FOR HFE1

#### Diagnose quantification:

<b>Human Action :</b>		Operator fails to diagnose the affect SGTR correctly.			
<b>Diagnose HEP :</b>		1,00E-02			
No	PSF	PSF Level	Multiplier for Diagnosis		Specific Reason
1	Available Time	Inadequate	1,0		The time required to perform the cognitive phase is 780s. Assuming the average leakage of 23kg/s through the rupture after automatic actuation and if nothing is done, after 2920s the affected SG will be solid. Subtracting $T_{delay}$ and $T_{exec}$ from the $T_{sw}$ , the $T_{avail} = 2240s$ . In this way, the available time for the cognitive phase is considered expansive time.
		Barely adequate	10		
		Nominal time	1		
		Extra time	0,1		
		Expansive	0,01		



2	Stress	Extreme	5	During SGTR multiple instruments from radiation detection and annunciator alarm unexpectedly at the same time it is expected that this event will produce a certain level of stress in the operator impacting his ability to diagnose. Therefore, it is considered high stress for this event due to the significance loud and continuous noise from the radiation alarm.
		High	2	
		Nominal	1	
3	Complexity	Highly	5	The operator should analyze 5 types of variables to identify which SG is affected by the rupture. In this way, it is considered a very low probability that the operator during this diagnosis will read the values of these tracks incorrectly six times to the point of erroneously identifying the steam generator affected by the rupture. However, it is many variables to verify. Therefore, it is considered moderately complexity.
		Moderately	2	
		Nominal	1	
		Obvious Diagnosis	0,1	
4	Experience/Training	Low	10	It is assumed that simulator training emphasizes diagnosis of SGTR and the operator understand it. The cues to identify the event is very clear and easy to find. The operator trains SGTR twice times a year. Therefore, it is considered nominal value.
		Nominal	1	
		High	0,5	

5	Procedures	Not available	50		The Angra-2 OPs manage the accident oriented by event which protect the NPP against design basic accidents, and safety function which maintain their critical safety functions. The procedure is organized through a logic flowchart which guide the operator to identify the accident or to ensure the safety function, and to guide any operator decision and actions during the whole process. Therefore, the Angra-2 OPs are diagnostic and symptom-oriented.
		Incomplete	20		
		Available, but poor	5		
		Nominal	1		
		Diagnostic/Symptom-oriented	0,5		
6	Ergonomics	Missing/Misleading	50		This PSF level is chosen nominal considering that the design of the plant supports correct performance.
		Poor	10		
		Nominal	1		
		Good	0,5		
7	Fitness for Duty	Unfit	1		This PSF level is chosen nominal considering that the operator has a strong capability to diagnose what is happening in the MCR for a long period. He is trained and very well prepared for this kind of situation.
		Degraded Fitness	5		
		Nominal	1		
8	Work Process	Poor	2		This PSF level is chosen good considering that the work process in the main control room is based on 3 way communication. Furthermore, all the work planning and execution is conducted based in documents from KTA, structured in KKS codification, which enhance the safety culture in the ANGRA-2 NPP.
		Nominal	1		
		Good	0,8		

$$P_{diagnose1} = HEP_{base} \cdot PIF$$

$$P_{diagnose1} = 1 \times 10^{-2} \times 0.01 \times 2 \times 2 \times 1 \times 0.5 \times 1 \times 1 \times 0.8$$

$$P_{diagnose1} = 1.6 \times 10^{-4}$$

**Action Quantification:**

<b>Human Action :</b>		Operator fails to correctly isolate the SG		
<b>Action HEP :</b>		1,00E-03		
No	PSF	PSF Level	Multiplier for Diagnosis	Specific Reason
1	Available Time	Inadequate	1,0	
		Time available	10	
		Nominal time	1	
		available (>5x)	0,1	
		available (>50x)	0,01	
2	Stress	Extreme	5	
		High	2	
		Nominal	1	
3	Complexity	Highly	5	

The time required to perform the action phase is 300s, and for conservatism assumption is considered a time margin of 1 min to execute the action. Therefore, Tavail = 360s and this PSF is considered nominal.

SGTR is an accident which could release radioactivity material to the environment if not done correctly. There is a pressure above the operation performance if he wrongly isolates the SG. Therefore, it is considered high stress for this event due to the significant health and consequences for the public and environment.

In this action, the operator should close 10 valves related to the affected SG. The execution of steps is

		Moderately	2		relatively straightforward, but the operator could make an error of commission if he does it in the wrong SG or an error of omission if he forgets to close any of the 10 valves. Therefore, moderately complexity PSF is considered.
		Nominal	1		
4	Experience/Training	Low	3		This PSF level is chosen nominal considering that the operator has vast experience to open and close the valves which connect SG with other systems. These types of actions are done in training (twice a year) and during normal operation to warm up and cooldown the nuclear power plant.
		Nominal	1		
		High	0,5		
5	Procedures	Not available	50		This PSF level is chosen nominal considering that procedures are available and enhance performance. The KKS code and procedure structure was designed to reduce EOO and EOC to identify and communicate any system and equipment during procedure using.
		Incomplete	20		
		Available, but poor	5		
		Nominal	1		
6	Ergonomics	Missing/Misleading	50		This PSF level is chosen nominal considering that the design of the plant supports correct performance.
		Poor	10		
		Nominal	1		
		Good	0,5		
7	Fitness for Duty	Unfit	1		The operator is capable to carry out tasks in the MCR, and it is no observed any mental or physical degradation of
		Degraded Fitness	5		

		Nominal	1	the operator performance. Therefore, nominal PSF is chosen for this PSF.
8	Work Process	Poor	5	This PSF level is chosen good considering that the work process in the main control room is based on 3 way communication.
		Nominal	1	
		Good	0,5	Furthermore, all the work planning and execution is conducted based in documents from KTA, structured in KKS codification, which enhance the safety culture in the ANGRA-2 NPP.

$$P_{action1} = HEP_{base} \cdot PIFs$$

$$P_{action1} = 1 \times 10^{-3} \times 1 \times 2 \times 2 \times 1 \times 1 \times 1 \times 1 \times 0.5$$

$$P_{action1} = 2 \times 10^{-3}$$

In sequence, it is calculated the total HEP for the HFE “Identification and Isolation of Affected SG”.

$$HEP_{HFE1} = P_{diagnose1} + P_{action1}$$

$$HEP_{HFE1} = 1.6 \times 10^{-4} + 2.0 \times 10^{-3}$$

$$HEP_{HFE1} = 2.16 \times 10^{-3}$$

## 6.2 HEP QUANTIFICATION FOR HFE2

### Diagnose quantification:

It is not considered diagnose part in this HFE2 for HEP quantification.

Therefore,  $P_{diagnose2} = 0$ .

**Action quantification:**

<b>Human Action :</b>		Operator fails to start cooldown the RCS by MAN valve		
<b>Action HEP :</b>		1,00E-03		
No	PSF	PSF Level	Multiplier for Diagnosis	Specific Reason
1	Available Time	Inadequate	1,0	The time required to perform the action is 300s. Assuming that the SG will overflow if this action is not taken, the available time is 1520s. T <sub>avail</sub> is higher than the demanded time to execute the action. Therefore, extra time PSF level is chosen for diagnosis HEP calculation.
		Time available	10	
		Nominal time	1	
		available (>5x)	0,1	
		available (>50x)	0,01	
2	Stress	Extreme	5	SGTR is an accident which could release radioactivity material to the environment and damage the core if it is not managed properly and in time. Therefore, it is considered high stress for this event due to the significance health and consequences for the public and environment.
		High	2	
		Nominal	1	
3	Complexity	Highly	5	In this action, the operator should execute two simple tasks to accomplish the main goal, check the availability of the TBV or ADV valve and turn on the automatic cooldown control system. However, the operator should monitor parameters continually. Therefore, it is considered moderately complexity level for this PSF.
		Moderately	2	
		Nominal	1	

4	Experience/Training	Low	3	This PSF level is chosen high considering that the operator maneuvers this valve during training session and during normal NPP heating and cooldown process. The operator has large experience and/or training baggage to operate these valves.
		Nominal	1	
		High	0,5	
5	Procedures	Not available	50	This PSF level is chosen nominal considering that procedures are available and enhance performance. The KKS code and procedure structure was designed to reduce EOO and EOC to identify and communicate any system and equipment during procedure using.
		Incomplete	20	
		Available, but poor	5	
		Nominal	1	
6	Ergonomics	Missing/Misleading	50	This PSF level is chosen nominal considering that the design of the plant supports correct performance.
		Poor	10	
		Nominal	1	
		Good	0,5	
7	Fitness for Duty	Unfit	1	The operator is capable to carry out tasks in the MCR, and it is no observed any mental or physical degradation of the operator performance. Therefore, nominal PSF is chosen for this PSF.
		Degraded Fitness	5	
		Nominal	1	
8	Work Process	Poor	5	The organization has a well established communication framework to conduct the task and the operator is well-trained to use this communication
		Nominal	1	

		Good	0,5	pattern. The safety culture enhances the work process. Therefore, it is chosen good level for this PSF.
--	--	------	-----	---

$$P_{action2} = HEP_{base} \cdot PIFs$$

$$P_{action2} = 1 \times 10^{-3} \times 0.1 \times 2 \times 2 \times 0.5 \times 1 \times 1 \times 1 \times 0.5$$

$$P_{action2} = 1 \times 10^{-4}$$

$$HEP_{HFE2} = P_{diagnose2} + P_{action2} = 1 \times 10^{-4} \therefore P_{diagnose2} = 0$$

### 6.3 HEP QUANTIFICATION FOR HFE3

#### Diagnose quantification:

<b>Human Action :</b>		Operator fails to diagnose the high level alarm in the LAA tank		
<b>Diagnose HEP :</b>		1,00E-02		
No	PSF	PSF Level	Multiplier for Diagnosis	Specific Reason
1	Available Time	Inadequate	1,0	The time required to perform the diagnose part is 300s. Assuming that the T <sub>sw</sub> is 5400s, from the cue max level 2 and the high level when the LCA pumps will be turned of, the operator will have 5075s before the protect system turn of the condenser pump developing a sequence of events which will lose the closed cycle. T <sub>avail</sub> is much higher than demanded time. Therefore, expansive time PSF level is chosen for diagnosis HEP calculation.
		Barely adequate	10	
		Nominal time	1	
		Extra time	0,1	
		Expansive	0,01	



2	Stress	Extreme	5		SGTR is an accident which could release radioactivity material to the environment and damage the core if it is not managed properly. Additionally, the continuous noise and alarm showing up impact in the operator diagnosis. Therefore, it is considered high stress for this event.
		High	2		
		Nominal	1		
3	Complexity	Highly	5		The operator should identify the high level max2 alarm in the alarm screen table. He should understand what is happening, the probable causes and decide the plan to solve the issue. They should use the alarm manual to find out the cause and the specific solution for the case. The operator needs to identify only one cue (LAA tank high level) and he will make use of only one alarm procedure to solve the issue. However, a lot of other things are happening concurrently taking the attention of the operator. Therefore, the moderately level is considered for complexity PSF.
		Moderately	2		
		Nominal	1		
		Obvious Diagnosis	0,1		
4	Experience/Training	Low	10		It is assumed that simulator training emphasizes diagnosis of SGTR and alarm attention, and the operator understand it. The cues to identify the event is very clear and
		Nominal	1		

		High	0,5		well familiarized. The operator trains SGTR twice times a year. Therefore, it is considered nominal value.
5	Procedures	Not available	50		The Angra-2 OPs manage accidents oriented by event and symptom which protect the NPP against design basic accidents, and safety function to maintain their critical safety functions. However, the alarm procedure is structured in a narrative form without any field to check the verification of each proposed solution in response to the alarm. Therefore, the Angra-2 alarm OPs are considered as nominal.
		Incomplete	20		
		Available, but poor	5		
		Nominal	1		
		Diagnostic/Symptom-oriented	0,5		
6	Ergonomics	Missing/Misleading	50		This PSF level is chosen nominal considering that the design of the plant supports correct performance.
		Poor	10		
		Nominal	1		
		Good	0,5		
7	Fitness for Duty	Unfit	1		The operator is capable to carry out tasks in the MCR, and it is no observed any mental or physical degradation of the operator performance. Therefore, nominal PSF is chosen for this PSF.
		Degraded Fitness	5		
		Nominal	1		
8	Work Process	Poor	2		This PSF level is chosen good considering that the communication in the main control room is based on 3 way communication. Furthermore, all the work
		Nominal	1		

		Good	0,8	planning is conducted based in documents from KTA which enhance the safety culture in the ANGRA-2 NPP.
--	--	------	-----	--

$$P_{diagnose3} = HEP_{base} \cdot PIFs$$

$$P_{diagnose3} = 1 \times 10^{-2} \times 0.01 \times 2 \times 2 \times 1 \times 1 \times 1 \times 1 \times 0.8$$

$$P_{diagnose3} = 3.2 \times 10^{-4}$$

**Action quantification:**

<b>Human Action :</b>		Operator fails to drain water from the LAA tank		
<b>Action HEP :</b>		1,00E-03		
No	PSF	PSF Level	Multiplier for Diagnosis	Specific Reason
1	Available Time	Inadequate	1,0	The time required to perform the action phase is 300s, and for conservatism assumption is considered a time margin of 1 min to execute the action. Therefore, Tavail = 360s and this PSF is considered nominal.
		Time available	10	
		Nominal time	1	
		available (>5x)	0,1	
		available (>50x)	0,01	
2	Stress	Extreme	5	If the operator fails to open the drain valve, he will lose the closed cycle and will be obligate to made use of open cycle to cooldown the RCS as the last option to do it by the secondary side. Therefore, it is considered high stress for this event due to the implication of loss of options to cooldown RCS.
		High	2	
		Nominal	1	

3	Complexity	Highly	5	In this action, the operator should open 1 drain valve in the LAA tank. The execution of steps is relatively straightforward with little potential for confusion. However, the operator should pay attention on multiples variables which could demand other actions. Therefore, moderately complexity PSF is considered.
		Moderately	2	
		Nominal	1	
4	Experience/Training	Low	3	This PSF level is chosen nominal considering that the operator has more than 6 months experience and/or training and have been exposed to abnormal conditions.
		Nominal	1	
		High	0,5	
5	Procedures	Not available	50	The alarm procedure is structured in a narrative away without place to check the action, however, the operator has plenty of time to recover any EOO. Additionally, the KKS code was designed to reduce operator error when identifying system and equipment during accident mitigation. Therefore, nominal procedure PSF is considered.
		Incomplete	20	
		Available, but poor	5	
		Nominal	1	
6	Ergonomics	Missing/Misleading	50	This PSF level is chosen nominal considering that the design of the plant supports correct performance.
		Poor	10	
		Nominal	1	
		Good	0,5	
7	Fitness for Duty	Unfit	1	The operator is capable to carry out tasks in the

		Degraded Fitness	5		MCR, and it is no observed any mental or physical degradation of the operator performance. Therefore, nominal PSF is chosen for this PSF.
		Nominal	1		
8	Work Process	Poor	5		The organization has a well established communication framework to conduct the task and the operator is well-trained to use this communication pattern. Therefore, this PSF is chosen good.
		Nominal	1		
		Good	0,5		

$$P_{action3} = HEP_{base} \cdot PIFs$$

$$P_{action3} = 1 \times 10^{-3} \times 1 \times 2 \times 2 \times 1 \times 1 \times 1 \times 1 \times 0.5$$

$$P_{action3} = 2 \times 10^{-3}$$

In sequence, it is calculated the total HEP for the HFE3:

$$HEP_{HFE3} = P_{diagnose3} + P_{action3}$$

$$HEP_{HFE3} = 3.2 \times 10^{-4} + 2.0 \times 10^{-3}$$

$$HEP_{HFE3} = 2.32 \times 10^{-3}$$

#### 6.4 HEP QUANTIFICATION FOR HFE4

##### Diagnose quantification:

<b>Human Action :</b>		Operator fails to diagnose the low level alarm in the LAR tank			
<b>Diagnose HEP :</b>		1,00E-02			
No	PSF	PSF Level	Multiplier for Diagnosis		Specific Reason
1	Available Time	Inadequate	1,0		The time required to perform the diagnose part is 300s. Assuming that

		Barely adequate	10		the $T_{sw}$ is 11792s, from the beginning of LAR tanks low level to the tank depletion, the operator will have 9367s before losing the feedwater source for the SGs. $T_{avail}$ is two times higher than cognitive time and is also higher the 30 minutes. Therefore, expansive time PSF level is chosen for diagnosis HEP calculation.
		Nominal time	1		
		Extra time	0,1		
		Expansive	0,01		
2	Stress	Extreme	5		SGTR is an accident which could release radioactivity material to the environment and damage the core if it is not manage properly. Additionally, the continuous noise and alarm showing up impact in the operator diagnose. Therefore, it is considered high stress for this event.
		High	2		
		Nominal	1		
3	Complexity	Highly	5		The operator should identify at least one low level alarm from any LAR pool tanks in the alarm screen table. Then he should deploy the alarm procedure to understand what is happening, the probable causes and the actions to solve it. However, a lot of other things are happening concurrently taking the attention of the operator. Therefore, the moderately level is considered for complexity PSF.
		Moderately	2		
		Nominal	1		
		Obvious Diagnosis	0,1		

4	Experience/Training	Low	10		It is assumed that simulator training emphasizes diagnosis of SGTR and alarm attention, and the operator understand it. The cues to identify the event is very clear and easy to find. The operator trains SGTR twice times a year. Therefore, it is considered nominal value.
		Nominal	1		
		High	0,5		
5	Procedures	Not available	50		The Angra-2 OPs manage accidents oriented by event and symptom which protect the NPP against design basic accidents, and safety function to maintain their critical safety functions. However, the alarm procedure is structured in a narrative form without any field to check the verification of each proposed solution in response to the alarm. Therefore, the Angra-2 alarm OPs are considered as nominal.
		Incomplete	20		
		Available, but poor	5		
		Nominal	1		
		Diagnostic/Symptom-oriented	0,5		
6	Ergonomics	Missing/Misleading	50		This PSF level is chosen nominal considering that the design of the plant supports correct performance.
		Poor	10		
		Nominal	1		
		Good	0,5		
7	Fitness for Duty	Unfit	1		The operator is capable to carry out tasks in the MCR, and it is no observed any mental or physical degradation of the operator performance. Therefore, nominal PSF is chosen for this PSF.
		Degraded Fitness	5		
		Nominal	1		

8	Work Process	Poor	2	This PSF level is chosen good considering that the communication in the main control room is based on 3 way communication. Furthermore, all the work planning is conducted based in documents from KTA which enhance the safety culture in the ANGRA-2 NPP.
		Nominal	1	
		Good	0,8	

$$P_{diagnose4} = HEP_{base} \cdot PIFs$$

$$P_{diagnose4} = 1 \times 10^{-2} \times 0.01 \times 2 \times 2 \times 1 \times 1 \times 1 \times 1 \times 0.8$$

$$P_{diagnose4} = 3.2 \times 10^{-4}$$

**Action quantification:**

<b>Human Action :</b>		Operator fails to replenish and connect the pool tanks (LAR)		
<b>Action HEP :</b>		1,00E-03		
No	PSF	PSF Level	Multiplier for Diagnosis	Specific Reason
1	Available Time	Inadequate	1,0	The time required to perform the action phase is 2400s, and for conservatism assumption is considered a time margin of 1 min to execute the action. Therefore, Tavail = 2460s and this PSF is considered nominal.
		Time available	10	
		Nominal time	1	
		available (>5x)	0,1	
		available (>50x)	0,01	
2	Stress	Extreme	5	SGTR is an accident which produce a lot of noise in the MCR and the operator will degrade a lot the



		High	2		condition if he fails to identify it, because he will lose the secondary source of water and consequently the secondary heat sink. Therefore, it is considered high stress for this event due to the significance noise in the MCR and implications from the situation.
		Nominal	1		
3	Complexity	Highly	5		During action implementation, the operator should implement multiple procedure (e.g. alarm procedure, function recovery procedure and system procedure) to reestablish the pool tanks level for LT cooling. The execution of steps is relatively straightforward with little potential for confusion. However, the operator should make use of several procedures during this critical task. Therefore, highly complexity PSF is considered.
		Moderately	2		
		Nominal	1		
4	Experience/Training	Low	3		This PSF level is chosen nominal considering that the operator has more than 6 months experience and/or training and have been exposed to abnormal conditions.
		Nominal	1		
		High	0,5		
5	Procedures	Not available	50		The alarm procedure is structured in a narrative away without place to

		Incomplete	20		check the action, however, the operator has plenty of time to recover any EOO. Additionally, the KKS code was designed to reduce operator error when identifying system and equipment during accident mitigation. Therefore, nominal procedure PSF is considered.
		Available, but poor	5		
		Nominal	1		
6	Ergonomics	Missing/Misleading	50		This PSF level is chosen nominal considering that the design of the plant supports correct performance.
		Poor	10		
		Nominal	1		
		Good	0,5		
7	Fitness for Duty	Unfit	1		The operator is capable to carry out tasks in the MCR, and it is no observed any mental or physical degradation of the operator performance. Therefore, nominal PSF is chosen for this PSF.
		Degraded Fitness	5		
		Nominal	1		
8	Work Process	Poor	5		The organization has a well established communication framework to conduct the task and the operator is well-trained to use this communication pattern. Therefore, this PSF is chosen good.
		Nominal	1		
		Good	0,5		

$$P_{action4} = HEP_{base} \cdot PIFs$$

$$P_{action4} = 1 \times 10^{-3} \times 1 \times 2 \times 5 \times 1 \times 1 \times 1 \times 1 \times 0.5$$

$$P_{action4} = 5 \times 10^{-3}$$

In sequence, it is calculated the total HEP for the HFE3:

$$HEP_{HFE4} = P_{diagnose4} + P_{action4}$$

$$HEP_{HFE4} = 3.2 \times 10^{-4} + 5.0 \times 10^{-3}$$

$$HEP_{HFE4} = 5.32 \times 10^{-3}$$

## 6.5 DEPENDENCY ANALYSIS OF HFE1 AND HFE2

The dependency analysis will be conducted using the SPAR-H method. This method applies a dependency rating between two human actions based on the dependency tables from the THERP methodology [9]. In an HRA, the dependency analysis can be done for all task, except for the first one, and this work aims to calculate the dependency of two HFE during SGTR. SPAR-H made use of 4 factors which can be combined into 16 dependency rules, ranging from the lowest degree of dependency to a complete dependency between the HFEs, with the zero-dependency rating as the 17th option [9]. The dependency rating system in SPAR-H is based on the following factors:

- Crew: Whether the same or different crew members are involved in the execution of both HFE actions.
- Time: Whether the HFE actions occur within a short, long, or extended time interval.
- Location: Whether the HFE actions are performed in the same location, on the same panel, on the same screen, within the same system, etc.
- Additional Cues: Whether the cues among the HFEs are the same or different.

With these defined pieces of information, it is possible to fill in the Table 13 to determine the degree of dependency between the HFE actions. Follows it is explained the reasons for choosing each condition for dependency analysis.

**Crew:** The same crew performs all actions during the SGTR event, which is composed of the shift supervisor, shift foreman, reactor operator, secondary operator, and auxiliary operator. If the event occurs close to a shift change, Angra-2's operating procedures require that the same shift completes all actions until the event is under control and reaches the cooling stage of the RCS (Reactor Coolant System) through the residual heat removal system.

**Time:** Both HFE actions are sequenced during the mitigation of the SGTR event and are close in time.

**Location:** The HFE - Identification and Isolation of Affected SG and HFE - Cooldown RCS at 50K/h in a closed cycle (MAN) are executed on different panels within the control room by different operators, but under the same conditions since all actions are taken in the control room.

**Additional cues:** The HFE - Cooldown RCS at 50K/h by MAN/ADV/MSSV involves additional cues which is the constant  $T_{avg}$  after the end of the automatic actuation and beginning of manual actions by the operator, which is not relevant for identifying the SGTR event in the first HFE.

**Table 13 – SPAR-H dependency table**

Condition number	Crew (Same or different)	Time (Close in time or not close in time)	Location (Same or different)	Cues (additional or no additional)	Dependency
1	s	c	s	na	complete
2				a	complete
3			d	na	high
4				a	high
5		nc	s	na	high
6				a	moderate
7			d	na	moderate

8				a	low	
9	d	c	s	na	moderate	
10				a	moderate	
11			d	na	moderate	
12				a	moderate	
13		nc	s	na	low	
14				a	low	
15			d	na	low	
16				a	low	
17						zero

The SPAR-H methodology has 5 levels in its dependency rating – zero, low, moderate, high, and complete dependency. For each dependency level, there is an equation to correlate the task failure probability without formal dependence ( $P_{w/od}$ ), and the task failure probability with formal dependence ( $P_{w/d}$ ). These equations are described in SPAR-H as follow:

- For Complete dependence:  $P_{w/d} = 1$
- For high dependence:  $P_{w/d} = (1+P_{w/od})/2$
- For moderate dependence:  $P_{w/d} = (1+6 \times P_{w/od})/7$
- For low dependence:  $P_{w/d} = (1+19 \times P_{w/od})/20$
- For zero dependence:  $P_{w/d} = P_{w/od}$

After defining the conditions for each item in the Table 13, it was identified a high dependency between:

- HFE - Cooldown RCS at 50K/h by MAN/ADV/MSSV; and
- HFE: Identification and Isolation of Affected SG.

Using the high dependency equation to estimate the new HEP with dependency, the  $P_{w/d}$  for the HFE - Cooldown RCS at 50K/h in a closed cycle (MAN) is:

$$P_{w/d} = \frac{(1 + P_{w/od})}{2} \therefore P_{w/od} = 1.0 \times 10^{-4}$$

$$P_{w/d} = \frac{(1 + 1.0 \times 10^{-4})}{2} = 5.0005 \times 10^{-1}$$

## 7 HRA ASSESSMENT BY IDHEAS-ECA

This section shows the analysis done for SGTR event in Angra-2 following the guidance provided by IDHEAS-ECA. This work contemplates the HFE considered in the HRA analysis performed using SPAR-H and the HFE defined in Angra-2 PSA to be quantified by IDHEAS-ECA methodology, with the purpose to see how IDHEAS-ECA can improve qualitatively and quantitatively the HEP quantification for the HFE in question, as well as, to testify that IDHEAS-ECA can be considered as method which can build reliable and constant HEP results in comparison with the results obtained by Angra-2 and SPAR-H methods which are considered standard HRA methods for HEP quantification.

Based on the task analysis carried out in section 4.4, the human failure events (HFE) defined for Angra-2 which is subject of this analysis using IDHEAS-ECA are:

- HFE1: Identification and Isolation of affected SG.
- HFE2: Cooldown RCS at 50K/h by TBV/ADV/MSSV.
- HFE3: Drain the feedwater tank (LAA) in case of SG feedwater pump failure.
- HFE4: Replenish emergency feedwater tanks (LAR) for RCS long term cooling.

## **7.1 HFE1: IDENTIFICATION AND ISOLATION OF AFFECTED SG (I&I-SG)**

### **7.1.1 STEP 1: SCENARIO ANALYSIS**

#### ***7.1.1.1 Step 1.1: Develop scenario narrative***

The reactor is operating at 100% power, and all operators are available in the control room (SS-Shift Supervisor; SF-Shift Foreman; PO-Primary Operator; SO-Secondary Operator; and AO-Auxiliary Panel Operator). The alignment of the systems is normal, and no additional activities are being conducted during the event. No damage associated with the initiating event is considered. Following the rupture of the tubes in the steam generator (complete tube rupture – 2A), the pressure and the level in the pressurizer begin to decrease. The level in the affected steam generator starts to rise, and the radiation activity instruments in the main steam line, installed at the outlet of each steam generator, began to indicate an increase in radiation due to the coolant leak from the rupture, with a 20-second delay. Upon identifying activity above the maximum allowed in the main steam line, several alarms begin to indicate an abnormal condition in the plant. After identifying that radiation in the main steam exceeds the maximum allowed activity, the reactor's limitation system initiates a series of automatic actions, which are summarized as follows: reduce reactor power below 30% at a rate of 20% per minute; reduce primary pressure to 89 bar; increase the pressure control set point for the steam generators to 79 bar (the reduction in power gradually increases the steam generator pressure); TRIP the reactor when pressure is below 131 bar and power is below 12%, or 300 seconds have passed since the radiation signal in the main steam line; initiate safety injection when pressurizer level is below 2.28 meters and pressure is below 111 bar; shut down the Reactor Coolant Pumps (RCPs); inject boron with 7000



ppm; and isolating the containment and the primary system. With the initiation of the safety injection, the level is reestablished, and the pressure stabilizes at 109 bar, and the safety injection flow matches the rupture flow. After the reactor trip (TRIP), the operator begins executing the operating procedures using the "Operator Task Concept" procedure (OP-3.1.1), as knowing Standard Post-TRIP Actions (SPTA). In this operation guide, the operator is directed to verify the plant's status and confirm that all safety functions are maintained by OP-3.1.2, which is part of SPTA. If any safety function is violated, the operator is directed to the violated safety function recovery procedure (OP-3.2.1/3.2.2.1/3.2.2.2/3.2.2.3/3.2.2.4/3.2.2.5 are part of FRG). However, if the safety functions are maintained, the operator must proceed to the accident identification procedure "Logical Diagnostic Tree (LDT)" (OP-3.1.3, which is part of the diagnostic action (DA). During DA, the operator will follow a flowchart with several steps where the operator should answer to identify the event. After identifying SGTR occurrence due to the increase in radiation in the main steam line and the exceeded radiation limit, the operator is directed to the Emergency Operating Procedure (EOP) "Steam Generator Tube Rupture with Exceeded Main Steam Activity Limits" (OP-3.3.5). Following the procedure, the operator must re-verify all automatic actions performed by the reactor's limitation and protection system and assess the plant's status to confirm the ongoing accident. After this initial verification, the operator must identify the affected steam generator using five variables (main steam activity, sampling system activity, position of the steam generator water makeup control valves, flow rate of steam generator makeup water, and the level of the steam generators). The operator should isolate the affected steam generator using ten valves, limit SG pressure, initiate cooling at a rate of 50 Kelvin per hour with the intact steam generators, reduce

the Reactor Coolant System (RCS) pressure, and control the inventory of primary and secondary water.

For further understanding of the SGTR in Angra-2, Table 14 demonstrate the SGTR scenario timeline of the automatic and manual actuation in chronological order considered for this analysis and is based on the chapter 15 from Angra-2 FSAR [4]:

**Table 14 - Baseline scenario**

<b>Baseline scenario: SGTR</b>	
<b>Time (s)</b>	<b>(S):</b> System Responses
	<b>H(abc):</b> Human responses; <b>abc:</b> individual position
	<b>(N):</b> Notes
	<b>(I):</b> System generated information
<b>0,00s</b>	<b>(S):</b> N/A.
	<b>H(abc):</b> N/A
	<b>(N):</b> 2A (complete tube failure) SGTR occurs starting coolant leakage from the primary side to secondary side at a initial flow rate about 40kg/s.
	<b>(I):</b> $L_{PZR} \downarrow$ ; and $P_{PZR} \downarrow$ .
<b>20,0s</b>	<b>(S):</b> System start reduction of power at 20%/min; start second changing pump from the chemical and volumetric control system (KBA); start borated water injection system pumps (JDH); turn off PZR heaters; and reduction of SG water level by 1 m.
	<b>H(abc):</b> N/A
	<b>(N):</b> Limitation system identify high activity in the main steam line.
	<b>(I):</b> Main steam activity > max limit; $L_{PZR} \downarrow$ ; $P_{PZR} \downarrow$ ; and extraction line flow $\downarrow$ .
<b>230,0s</b>	<b>(S):</b> Start reactor coolant system (RCS) pressure reduction by PRZ spray through the main spray, boration system spray and extra spray. Additionally, the limitation system stops the power reduction.
	<b>H(abc):</b> N/A
	<b>(N):</b> 210s after the limitation system identify the main steam activity > max activity permitted, the limitation system start the phase 2 of automatic actuations.
	<b>(I):</b> Main steam activity > max limit 2 <sup>nd</sup> phase started; $L_{PZR} \downarrow$ decelerated; and $P_{PZR} \downarrow$ accelerated.
<b>320,0s</b>	<b>(S):</b> Reactor TRIP – power $\downarrow$ ; coolant temperature $\downarrow$ ; $L_{PZR} \downarrow$ ; $P_{PZR} \downarrow$ ; Leakage flow rate $\downarrow$ .
	<b>H(abc):</b> The operator start the human actions to mitigate the accident. The first step is to deploy the standard post TRIP actions (SPTA) procedure (OP-3.1.1).

	<p><b>(N):</b> The reactor TRIP occur based on what happens first: after detection of <math>P_{RCS} &lt; \min 2</math> (132bar) or 300s after detection of SG tube rupture. Conservatively for HRA analysis, it was choosed the longest time for the occurrence of reactor TRIP.</p> <p><b>(I):</b> <math>P_{RCS} &lt; 132\text{bar}</math> or passed 300s after SG tube rupture detection.</p>
359,0s	<p><b>(S):</b> <math>L_{PZR} \downarrow</math>; <math>P_{PZR} \downarrow</math>.</p> <p><b>H(abc):</b> N/A</p> <p><b>(N):</b> Reactor protection system (RPS) identify the first setpoint for SIS.</p> <p><b>(I):</b> <math>P_{RCS} &lt; 111\text{bar}</math>.</p>
	<p><b>(S):</b> RPS isolate the RCS, turn of reactor coolant pumps (RCP), end of PZR spray, and RCS pressure determined by the HHSI at 109bar, main steam pressure adjusted for 77bar, leakage rate is constant at 23kg/s, <math>L_{PZR}</math> constant at 2,6m, and <math>L_{SGTR} \uparrow</math> at a constant rate.</p> <p><b>H(abc):</b> N/A</p> <p><b>(N):</b> Reactor protection system (RPS) identify the second setpoint for SIS and start signal for HHSI (JND).</p> <p><b>(I):</b> <math>P_{RCS} &lt; 111\text{bar}</math> and <math>L_{PZR} &lt; 2,8\text{m}</math>, <math>L_{SG}</math> around 12m <math>\uparrow</math>.</p>
	<p><b>(S):</b> N/A.</p> <p><b>H(abc):</b> At this point, the operator already execute the SPTA (OP-3.1.1), verified that all safety functions criteria were satisfied (OP-3.1.2), identified the event by the DA procedure (OP-3.1.3), and recognize the failed SG (OP-3.3.5, step #1/2). After identifying the affected SG, the operator will start to execute the affected SG isolation by closing all the 10 valves involved in the process (OP-3.3.5, step #3).</p> <p><b>(N):</b> N/A.</p> <p><b>(I):</b> <math>P_{RCS} = 102\text{bar}</math>; <math>T_{AVG} = 299^{\circ}\text{C}</math>; <math>L_{PZR} = 2,6\text{m}</math>; <math>L_{SGTR} \uparrow</math>; and <math>P_{MS} = 77\text{bar}</math>.</p>
1224,6s	<p><b>(S):</b> N/A.</p> <p><b>H(abc):</b> The operator finish the isolation of affected SG (STEP #3), and start the execution of the RCS cooldown by 50K/h (OP-3.3.5, step #4).</p> <p><b>(N):</b> N/A.</p> <p><b>(I):</b> <math>P_{RCS} &lt; 111\text{bar}</math> and <math>L_{PZR} &lt; 2,8\text{m}</math>, <math>L_{SGTR} \uparrow</math>.</p>
	<p><b>(S):</b> Cooldown RCS by the TBV at 50K/h.</p> <p><b>H(abc):</b> The operator finish to start cooldown the RCS by 50K/h preferable by the TBV (MAN) (OP-3.3.5, step #4).</p> <p><b>(N):</b> N/A.</p> <p><b>(I):</b> <math>T_{AVG} \downarrow</math>; <math>P_{RCS} \downarrow</math>; <math>L_{PZR} \uparrow</math>, <math>L_{SGTR} \uparrow</math>.</p>
	<p><b>(S):</b> Cooldown RCS by the TBV at 50K/h.</p> <p><b>H(abc):</b> The operator finish to start cooldown the RCS by 50K/h preferable by the TBV (MAN) (OP-3.3.5, step #4).</p> <p><b>(N):</b> N/A.</p> <p><b>(I):</b> <math>T_{AVG} \downarrow</math>; <math>P_{RCS} \downarrow</math>; <math>L_{PZR} \uparrow</math>, <math>L_{SGTR} \uparrow</math>.</p>

### 7.1.1.2 Step 1.2: Identify Human Failure Event (HFE)

HFE1: Identification and Isolation of Affected SG. This HFE comprise all the actions taken by the operators in the MCR to identify the event, find out the affected

SG, and isolate it to avoid radiation release and decrease as much as possible the leakage from the RCS to secondary side.

### **7.1.1.3 Step 1.3: Identify the scenario/Event Context**

- **Environment and situation:** The action is performed in the MCR. During SGTR, the accessibility and habitability of the MCR is protected by the HAVC and filters, which provide barrier to prevent any MCR radiation contamination; the accessibility and visibility for any panel is assured; there is intermittent noise from the alarm system due to the accident event; Communication pathways is clear; Temperature and humidity is perfect for human comfort and not affect the human action; there is no resistance to personnel movement in MCR; so, the MCR has a protected and comfort condition for the operators during accident mitigation, only the intermittent noise due to the alarm could affect operator performance.
- **System:** All system is working as designed, therefore, the PIFs system and I&C transparency to personnel, HIS, and equipment and tools will not affect the operator performance during SGTR mitigation.
- **Personnel:** The team in the MCR is composed by 5 operator which are the Shift supervisor (SS); Shift Foreman (SF); Primary operator (PO); Secondary operator (SO); and Auxiliary panel operator (AO). Each operator goes through a training process that is divided into 5 modules lasting 3 days per year. Each day has 4 hours of theoretical classes and 4 hours of simulator classes. Events from the DBA list and some events outside the project base are trained. Within this scope, the operator trains

the SGTR twice a year. The SGTR is such that the personal stress is moderated, and mental fatigue is not affected. The safety culture, 3 way communication, well-defined function and professionalism of each operator, and team coordination support the teamwork and work process in the MCR. The OP is diagnose and symptom-oriented which support operators decision-making and the code (KKS) used for system, equipment and component identification support the operation to prevent error of commission and omission during action the event, however, the alarm procedure is structured in a narrative way without any box to check the verified probable solution which could allow the operator to skip a step.

- **Task:** The MCR operators are following the OP-3.1.1 (SPTA), OP-3.1.3 (DA), and OP-3.3.5 (SGTR EOP step#1,2 and 3). The information provided in the MCR is complete, reliable and it is presented in friendly way. SGTR is a very familiar scenario to the operator, and they understand the behavior of the NPP during the event and they can predict the event progression. No simultaneous event occurs; thus, the team in the MCR do not need to be guided by multiple procedures related for multiple tasks and distraction or interruptions of the team are expected to not affect their performance. STGR is considered moderately complex for the operator due to the number and variety of variables to be processed during the event. Therefore, during the diagnosis phase, the huge number of variables – pressure and level of the PZR; radiation in the main steam line; radiation in the SG sampling system line; SG levels; % opening of the SG feedwater valves; and SG feedwater flow – will facilitate the operator to identify the event and the

affected steam generator, however, during the executive phase, the operator must perform several actions and at the same time need to monitor the variables involved in the process. The operators are not affected by mental fatigue due to their process of training and conditioning to handle these situations. SGTR requires operators to be urgent in carrying out their actions due to the possibility of solidifying the affected steam generator, causing an uncontrollable leak of the primary refrigerant, as well as the occurrence of a significant release of radioactive material into the environment. The action in the MCR will not demand any extraordinary physical effort.

## **7.1.2 STEP 2: ANALYZING HUMAN FAILURE EVENTS (HFE)**

### **7.1.2.1 Step 2.1: Defining the Human Failure Events (HFE)**

This section defines the HFE and describe the scope of the analysis:

- Success Criteria: Identify correctly the SG ruptured through 5 variables (OP-3.3.5, step #2), and close all 10 valves specified by procedure (OP-3.3.5, step #3).
- Consequence: During RCS cooldown, it will be impossible to decrease  $\Delta P$  between RCS and affected SG resulting in lost of coolant inventory from RCS to outside of the containment during the cooling by secondary side. However, it is still possible to cooldown the reactor core safely.
- Beginning and ending points: The HFE begins when is deployed the TRIP of the reactor. After the TRIP, the operator starts to execute the SPTA, OP-3.1.1. Then he is guided to verify all 5 critical safety functions (CSF) by OP-

3.1.2. If any safety functions are not satisfied, the operator should execute the specific critical safety function recovery guidance (FRG), if all CSF is satisfied, the operator moves to the diagnose procedure (DA) OP-3.1.3 to define the accident type. When the accident is defined, the operator is guided to the OP-3.3.5 to execute the step #1 (Verify reactor status), step #2 (identify ruptured SG), and step #3 (isolate the ruptured SG).

- Relevant procedure guidance: SPTA (OP-3.1.1); CSF monitoring (OP-3.1.2); DA (OP-3.1.3); and SGTR OP-3.3.5 step #1,2,3.

NOTE: The specification for this analysis were adopted from constant values for time based on Angra-2 FSAR and current PSA under development. In future studies, the timing could be deduced based on experimental models from Angra-2 simulator.

- Cues and indications for initiating the operator action and timing:  $T_{\text{delay}}$  is based on the time between the beginning of the event and the identification of the cue, where the operator action was started through procedure guidance. The cues which the operator will start their action is the reactor TRIP. For diagnose the event, the cues are radiation on the main steam line  $> \text{max activity}$ ;  $L_{\text{SG}} \uparrow$  of the affected SG;  $P_{\text{PZR}} \downarrow$ ; and  $L_{\text{PZR}} \downarrow$ . Due to the automatic actuations done by the limitation system and reactor protection system, the reactor TRIP will occur 320 seconds after the start of the event, so the operator start to execute the procedure after this point, therefore, the  $T_{\text{delay}} = 320\text{s}$ .
- Available time to perform the operator action: The system time window ( $T_{\text{sw}}$ ) is estimated based on when the affected SG becomes solid due to the absence of actions to reduce the leakage from the RCS to the ruptured SG.

Based on result obtained from a Angra-2 simulation the  $T_{SW} = 2920s$ . In this way, the time available ( $T_{avail}$ ) is  $T_{SW} - T_{delay}$  resulting in  $T_{avail} = 2600s$ .

- Time required to perform the operation action: Based on currently PSA for Angra-2 under development [x], it is assumed that the operators take approximately 780 seconds to do the cognitive part (e.g. detection, understand, and decision-making) which comprise the SPTA (OP-3.1.1), CSF monitoring under SPTA (OP-3.1.2), DA (OP-3.1.3), and mitigation of SGTR by emergency procedure (OP-3.3.5, step #1,2), and the execution time ( $T_{exe}$ ) is assumed 300 seconds for the operator to isolate the affected SG (OP-3.3.5, step #3). The time required ( $T_{req}$ ) is the time spent by the operator to perform the cognitive and execution part following the procedure, therefore,  $T_{req} = 1080s$ . All the timing is summarized in the timeline diagram shown in Figure 10.

### **7.1.2.2 Step 2.2: Task Analysis and Identification of Critical Tasks**

To keep it simple, one crucial task is defined, which involves the recognizing the reactor trip and the radiation in the main steam line and deploy the OP procedure to isolate the affected SG. Additionally, the HFE is assumed as one critical task because the same context is applicable from the start to the end of the HFE process.

## **7.1.3 STEP 3: MODELING FAILURE OF CRITICAL TASKS**

### **7.1.3.1 Step 3.1: Characterization of Critical Tasks**

This section specifies the relevant conditions that affect the performance of the critical task.



- Critical task goal: identify the SGTR event and which steam generator suffered the rupture to isolate the affected SG as soon as possible.
- Specific requirements: Close all 10 valves specified by the procedure (OP-3.3.5, step #3) to isolate the affected SG.
- Cues and supporting information: Reactor TRIP; P<sub>PZR</sub> ↓; L<sub>PZR</sub> ↓; radiation in the main steam line; radiation in the SG sampling system line; SG levels; % opening of the SG feedwater valves; and SG feedwater flow.
- Procedure: Initially SPTA (OP-3.1.1), transition to CSF monitoring (OP-3.1.2), transition to Diagnostic Action (OP-3.1.3) and then emergency procedure (OP-3.3.5, step #1,2).
- Personnel: The team in the MCR are composed by 5 operator which are the Shift supervisor (SS); Shift Foreman (SF); Primary operator (PO); Secondary operator (SO); and Auxiliary panel operator (AO). The operators in the main control room are well-trained and perform SGTR training in the simulator twice a year.
- Task Support: Procedures specified above and MCR indications.
- Location: Main control room (MCR).
- Cognitive activities: Detection, understanding, decisionmaking and action.
- Concurrent tasks: assuming that there are no other tasks.
- Interteam coordination considerations: multiple teams are not involved with this critical task. SGTR mitigation is handle by the MCR operational team.

### **7.1.3.2 Step 3.2: Identification of Applicable Cognitive Failure Modes (CFM)**

The applicable cognitive failure mode (CFM) is identified by assessing the cognitive activities of the critical task that are associated with each macrocognitive function.

- Detection: detect cues and acquire information.
  - Operators need to acquire information by checking and reading the status of the plant, and to detect the signals that allowed the operator to compare and identify the affected SG.
  - CFM1 – failure of detection applies to the critical task.
- Understanding: diagnose problems, maintain situational awareness.
  - Operators need to be aware that an SGTR is occurring, and for that, he should assess and select the main variables related to it, which are (1) activity rising in affected SG main steam line, (2) decreasing in pressurizer level and pressure, (3) comparing SGs feedwater flow, level, % valve opening, and sample line activity.
  - CFM2–failure of understanding applies to the critical task.
- Decisionmaking: make a go/no-go decision for a pre-specified action.
  - The operator decision is guided by the procedure which is diagnostic and symptom-oriented. Each decision presented by the procedure is done based on the cues detected and the information acquired by the operator.
  - CFM3: failure of decisionmaking applies to the critical task.
- Action Execution: execute cognitively simple actions.

- The operator should close 10 valves which includes the valves in the main steam line, purge line, feedwater line, sample line, and relief. The actions performed are relatively simple actions because operators are trained to, however, the number of valves to handle is high and there are other variables to monitoring during accident mitigation.
- CFM4: failure of action execution applies to the critical task.
- Interteam coordination: the critical task is implemented by the MCR operators, which is considered an individual team and SGTR does not require coordination among multiple teams.
  - CFM5: failure of interteam coordination DOES NOT apply to the critical task.

#### **7.1.4 STEP 4: ASSESSING PERFORMANCE INFLUENCING FACTOR ATTRIBUTES APPLICABLE TO CFM**

This section will assess the PIF and its attribute applicable for each CFM based on the context, boundary condition. SPAR-H and IDHEAS-ECA PIFs correlation table, from the reference [20], will also be used to support this analysis, with the aim of uphold consistency between HEP quantifications using these methods.

**CFM 1** – Failure of detection →  $P_{CFM1} = 1.70E-04$

- Scenario familiarity: No impact (SF0).
  - Justification: Operators are trained twice a year in this scenario, and they are well-trained to detect cues related to SGTR.
- Information availability and reliability: this PIF does not apply to this CFM.
  - Justification: Table B-2 in IDHEAS-ECA document [21].

- Task complexity: No impact (C0).
  - Justification: The detection of the SGTR and affected SG are not complex, and the operator is familiarized with the cues he should pay attention.
- Environmental PIF: ENV7 - Loud or burst noise → 1.7
  - Justification: During SGTR multiple instruments from radiation detection and annunciator alarm unexpectedly at the same time.

**CFM 2** – Failure of understanding →  $P_{CFM2} = 1.30E-03$

- Scenario familiarity: No impact (SF0).
  - Justification: Operators are trained twice a year in this scenario, and they are well-trained to understand that SGTR will lead to a  $P_{PZR} \downarrow$  and  $L_{PZR} \downarrow$ , activity of MS  $\uparrow$ , and incompatibility between levels, feed water flow rates, activity in the purge lines and sample of steam generators.
- Information availability and reliability: No impact (INF0).
  - Justification: The MCR indications are reliable and complete to understand that SGTR is occurring, and the operator should identify the affected SG.
- Task complexity: No impact (C0).
  - Justification: The procedures are diagnose and symptom-oriented through a logic flowchart which is clear to the operator, so they can understand the need to isolate the affect SG.
- Environmental PIF: ENV7 - Loud or burst noise → 1.15

- Justification: During SGTR multiple instruments from radiation detection and annunciator alarm unexpectedly at the same time.
- Mental fatigue, stress, and time pressure: MF8 – Emotional stress → 1.2
  - Justification: The operator understands the possibility of radiation release during SGTR. The RCS coolant are leaking to outside of the containment and there is high chance of radiation release to the environment increasing the stress.

**CFM 3** – Failure of decisionmaking →  $P_{CFM3} = 1.00E-03$

- Scenario familiarity: No impact (SF0).
  - Justification: Operators are trained twice a year in this scenario, and they are well-trained to make decisions through the procedure based on the main cues which are the  $P_{PZR} \downarrow$  and  $L_{PZR} \downarrow$ , activity of MS  $\uparrow$ , and incompatibility between levels, feed water flow rates, activity in the purge lines and sample of steam generators.
- Information availability and reliability: No impact (INF0).
  - Justification: The MCR indications are reliable and complete to make decisions during SGTR.
- Task complexity: No impact (C0).
  - Justification: The procedures are diagnose and symptom-oriented through a logic flowchart which is clear to the operator and guide him to make decision to find out what is happening and what emergency procedure is necessary to deploy for this event.

**CFM 4** – Failure of action →  $P_{CFM4} = 1.20E-03$

- Scenario familiarity: No impact (SF0).

- Justification: The operator has vast experience to open and close the valves which connect the SG with other systems. These types of actions are done in training and during normal operation to warm up and cooldown the nuclear power plant.
- Information availability and reliability: this PIF does not apply to this CFM.
  - Justification: Table B-2 in IDHEAS-ECA document [\[21\]](#).
- Task Complexity: C31 – Straightforward procedure execution with many steps → 1.00E-03
  - Justification: Once operators identify the affected SG following the procedure, the execution of the action to isolate the affected SG requires closing 10 valves as follows: full load blocking valve; low load blocking valve; main steam block valve; blocking valve of the main steam relief pressure control valve; main steam relief pressure control valve; purge flow control valve, collector inlet 60; purge flow control valve, collector inlet 50; isolation valve of the internal sampling containment "LCQ11"; external containment isolation valve of the affected SG train; and level control valve. For the operator, these actions are straightforward but are considered many steps.
- Mental fatigue, stress, and time pressure: MF8 – Emotional stress → 1.2
  - Justification: If the operators take too much time to isolate the affected SG, it could lead to a radiation release affecting the environment increasing the stress.

**CFM 5** – Failure of interteam coordination → As stated in step 3.2, this CFM is not applicable to this critical task.

### 7.1.5 STEP 5: ESTIMATION OF $P_c$ – THE SUM OF HEP OF CFM

The estimation of  $P_c$  for the HFE is obtained using the IDHEAS-ECA and it is shown in Figure 14.

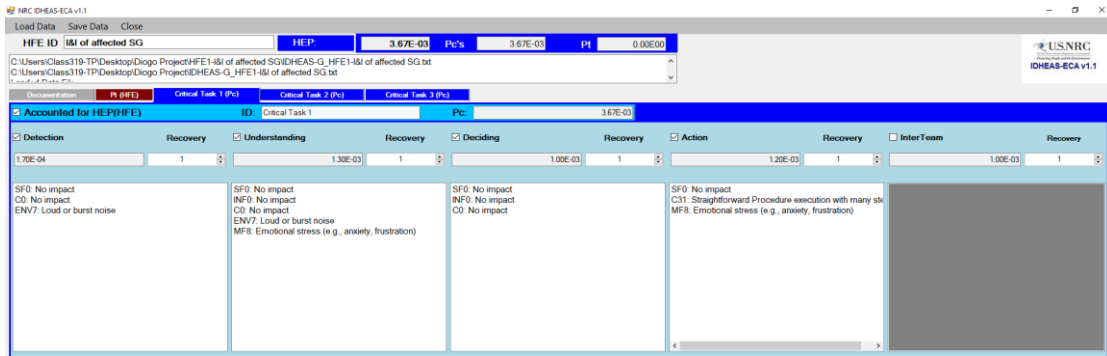


Figure 14 –  $P_c$  estimation for HFE1

### 7.1.6 STEP 6: ESTIMATION OF $P_t$ – THE CONVOLUTION OF THE DISTRIBUTION OF $T_{AVAIL}$ AND $T_{REQ}$

The estimation of  $P_t$  for the HFE1 – Identification and Isolation of affected SG is obtained using the IDHEAS-ECA and it is shown in Figure 15.

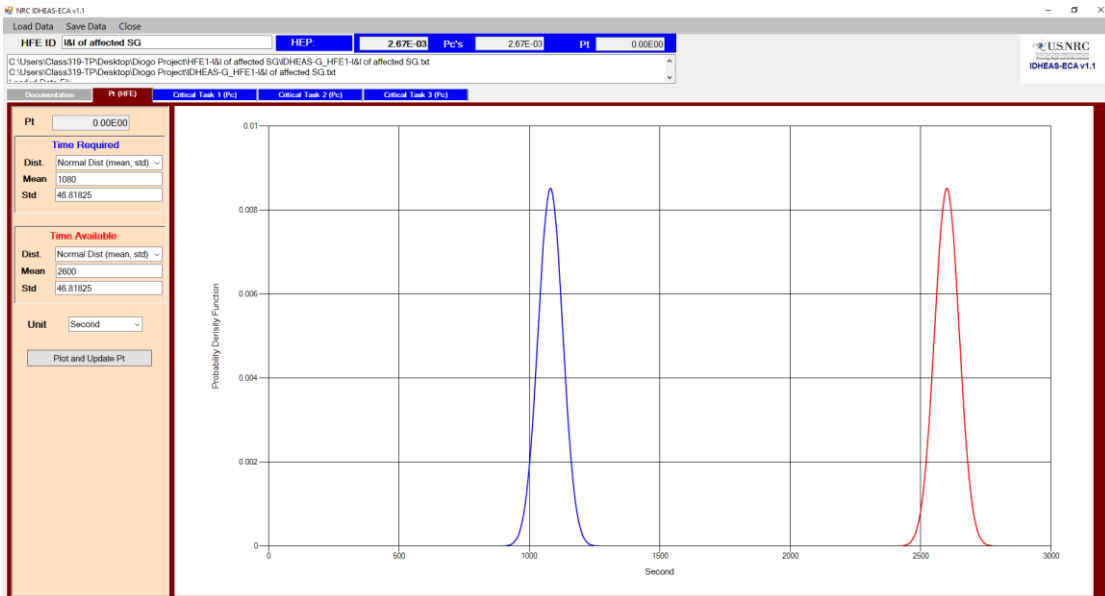


Figure 15 -  $P_t$  estimation for HFE1

### 7.1.7 STEP 7: CALCULATE THE OVERALL HEP

The summary of the HEP calculation is illustrated in Table 15.

Table 15 – Summary of HEP Quantification for HFE1

CFM	$PIF_{Attribute}$	$P_{CFM_{Base}}$	$w_i$	$P_{CFM}$
Detection	SF0: no impact C0: no impact ENV7: Loud or burst noise	$1 \times 10^{-4}$	1.7	$1.7 \times 10^{-4}$
Understanding	SF0: no impact INF0: no impact C0: no impact ENV7: Loud or burst noise MF8: Emotional stress	$1 \times 10^{-3}$	1.7 1.2	$1.30 \times 10^{-3}$
Decisionmaking	SF0: no impact INF0: no impact C0: no impact	$1 \times 10^{-3}$	N/A	$1 \times 10^{-3}$



<b>Action</b>	SF0: no impact C31: Straightforward procedure execution with many steps MF8: Emotional stress	$1 \times 10^{-4}$	$1.0 \times 10^{-3}$ 1.2	$1.20 \times 10^{-3}$
<b>TOTAL P<sub>CTI</sub></b>				$3.67 \times 10^{-3}$
<b>P<sub>t</sub></b>				0.00
<b>HEP<sub>IDHEAS-ECA</sub></b>				$3.67 \times 10^{-3}$

### 7.1.8 STEP 8 – DEPENDENCY ANALYSIS

N/A.

## 7.2 HFE2: COOLDOWN RCS AT 50K/H BY TBV/ADV/MSSV

### 7.2.1 STEP 1: SCENARIO ANALYSIS

#### 7.2.1.1 Step 1.1: Develop scenario narrative

It is assumed for HFE2, the same scenario narrative as describe in section 7.1.1.1 for HFE1.

#### 7.2.1.2 Step 1.2: Identify Human Failure Event (HFE)

HFE2: Cooldown RCS at 50K/h by TBV/ADV/MSSV (HR-TBVADVMSSV).  
The operator should execute the step 4 in the OP-3.3.5 to start cooldown the RCS and consequently cooldown the affected SG, avoiding increase of pressure in the affected SG which could lead to radiation release through the MSSV.

### **7.2.1.3 Step 1.3: Identify the scenario/Event Context**

- **Environment and situation:** It is assumed the same context stated in section 7.1.1.3.
- **System:** It is assumed the same context stated in section 7.1.1.3.
- **Personnel:** It is assumed the same context stated in section 7.1.1.3.
- **Task:** It is assumed the same context stated in section 7.1.1.3, however, an extra description for scenario/event context is required as follows. As soon as the operator finish to isolate the affected SG (OP-3.3.5, step #3), he should start cooldown the RCS at 50K/h following the step sequence of procedure guidance (OP-3.3.5, step #4).

## **7.2.2 STEP 2: ANALYZING HUMAN FAILURE EVENTS (HFE)**

### **7.2.2.1 Step 2.1: Defining the Human Failure Events (HFE)**

This section defines the HFE and describe the scope of the analysis:

- **Success Criteria:** Verify the availability of TBV/ADV/MSSV, preferable by TBV, open at least 1 TBV or 1 ADV or 1 MSSV, and turn on the RCS cooldown by 50K/h.
- **Consequence:** It will occur a rise of pressure in the affected SG leading to a release of steam by the MSSV to avoid overpressure in the secondary system, resulting in a RCS coolant loss to outside of the containment.
- **Beginning and ending points:** The HFE begins when the operator finishes to isolate the ruptured SG (OP-3.3.5, step #3), and start the cooldown of RCS at 50K/h (OP-3.3.5, step #3).
- **Relevant procedure guidance:** SGTR OP-3.3.5 step #4.

NOTE: The specification for this analysis were adopted from constant values for time based on Angra-2 FSAR and current PSA under development. In future studies, the timing could be deduced based on experimental models from Angra-2 simulator.

- Cues and indications for initiating the operator action and timing: The cues which the operator will start their action is  $T_{AVG}$  constant and SG level and pressure rising. However, operators understand the situation and they are following the procedure to mitigate the accident step by step, therefore, it is considered that this action start immediately after the operation finish to isolate the affected SG (OP-3.3.5, step #3), and  $T_{delay}$  is not applicable for this HFE.
- Available time to perform the operator action: The system time window ( $T_{SW}$ ) for this task is the time taken by the affected SG to become solid minus the time spent by the operator to execute the SPTA, DA, and OP-3.3.5 until step #3. Therefore, the  $T_{SW} = 1520s$ . In this way, the time available ( $T_{avail}$ ) is  $T_{SW} - T_{delay}$  resulting in  $T_{avail} = 1520s$ .
- Time required to perform the operation action: Based on currently PSA for Angra-2 under development [3], it is assumed that the operators take approximately 300 seconds for execution time ( $T_{exe}$ ) to verify the availability of TBV/ADV/MSSV and start cooldown the RCS by the unaffected SGs (OP-3.3.5, step #4). The time required ( $T_{req}$ ) is the time spent by the operator to perform execution part following the procedure, therefore,  $T_{req} = 300s$ . All the timing is summarized in the timeline diagram shown in Figure 11.

### **7.2.2.2 Step 2.2: Task Analysis and Identification of Critical Tasks**

To keep it simple, one crucial task is defined, which involves verify the availability of TBV/ADV/MSSV (preferable by TBV) and start up the RCS cooldown by 50K/h. Additionally, the HFE is assumed as one critical task because the same context is applicable from the start to the end of the HFE process.

## **7.2.3 STEP 3: MODELING FAILURE OF CRITICAL TASKS**

### **7.2.3.1 Step 3.1: Characterization of Critical Tasks**

This section specifies the relevant conditions that affect the performance of the critical task.

- Critical task goal: verify the availability of the TBV/ADV/MSSV in the unaffected SGs and start cooldown the RCS as soon as possible.
- Specific requirements: Verify the availability of 1 TBV or 1 ADV specified by the procedure (OP-3.3.5, step #4) and turn on the cooldown at 50K/h.
- Cues and supporting information:  $T_{AVG}$  constant; affected SG level and pressure rising; and operator finish the execution of step #3 in the procedure.
- Procedure: Emergency procedure (OP-3.3.5, step #4).
- Personnel: The team in the MCR are composed by 5 operator which are the Shift supervisor (SS); Shift Foreman (SF); Primary operator (PO); Secondary operator (SO); and Auxiliary panel operator (AO). The operators in the main control room are well-trained and perform SGTR training in the simulator twice a year.
- Task Support: Procedures specified above and MCR indications.
- Location: Main control room (MCR).

- Cognitive activities: Action.
- Concurrent tasks: assuming that there are no other tasks.
- Interteam coordination considerations: multiple teams are not involved with this critical task. SGTR mitigation is handle by the MCR operational team.

### **7.2.3.2 Step 3.2: Identification of Applicable Cognitive Failure Modes (CFM)**

The applicable cognitive failure mode (CFM) is identified by assessing the cognitive activities of the critical task that are associated with each macrocognitive function.

- Detection: At this point the operator possesses all the cues to deploy the RCS cooldown, and it just procedure implementation.
  - CFM1 – failure of detection DOES NOT apply to the critical task.
- Understanding: The operator understands the situation and know that he just need to deploy the RCS cooldown (OP-3.3.5, step #4).
  - CFM2–failure of understanding DOES NOT apply to the critical task.
- Decisionmaking: The operator decision is guided by the procedure which is diagnostic and symptom-oriented. Each decision presented by the procedure is done based on the cues detected and the information acquired by the operator.
  - CFM3: failure of decisionmaking DOES NOT apply to the critical task.
- Action Execution: execute cognitively simple actions.

- The operator should verify the availability of TBV and ADV (preferably by the TBV) and turn on RCS cooldown by 50K/h.
- CFM4: failure of action execution applies to the critical task.
- Interteam coordination: the critical task is implemented by the MCR operators, which is considered an individual team and SGTR does not require coordination among multiple teams.
  - CFM5: failure of interteam coordination DOES NOT apply to the critical task.

#### **7.2.4 STEP 4: ASSESSING PERFORMANCE INFLUENCING FACTOR ATTRIBUTES APPLICABLE TO CFM**

This section will assess the PIF and its attribute applicable for each CFM based on the context, boundary condition. SPAR-H and IDHEAS-ECA PIFs correlation table, from the reference [20], will also be used to support this analysis, with the aim of uphold consistency between HEP quantifications using these methods.

**CFM 1** – Failure of detection → As stated in step 3.2, this CFM is not applicable to this critical task.

**CFM 2** – Failure of understanding → As stated in step 3.2, this CFM is not applicable to this critical task.

**CFM 3** – Failure of decisionmaking → As stated in step 3.2, this CFM is not applicable to this critical task.

**CFM 4** – Failure of action →  $P_{CFM4} = 4.08E-04$

- Scenario familiarity: No impact (SF0).
  - Justification: The operator has vast experience to maneuver the TBV and ADV valves. These valves are used by the operator

during training session and during normal operation to warm up and cooldown the nuclear power plant.

- Information availability and reliability: this PIF does not apply to this CFM.
  - Justification: Table B-2 in IDHEAS-ECA document [21].
- Task Complexity: C33 – Simple continuous control that requires monitoring parameters → 3.4E-04
  - Justification: Once operators identify the availability of TBV or ADV, he turns on the RCS Cooldown. This action consists of checking the valve availability and turn on the 50K/h cooldown. After cooldown start, the operator should monitor some parameters to ensure action success.
- Mental fatigue, stress, and time pressure: MF8 – Emotional stress → 1.2
  - Justification: The failure of RCS cooldown could lead to a pressure increase of affected SG resulting in radiation release affecting the environment increasing operator stress.

**CFM 5** – Failure of interteam coordination → As stated in step 3.2, this CFM is not applicable to this critical task.

#### **7.2.5 STEP 5: ESTIMATION OF PC – THE SUM OF HEP OF CFM**

The estimation of Pc for the HFE2 is obtained using the IDHEAS-ECA and it is shown in Figure 16.

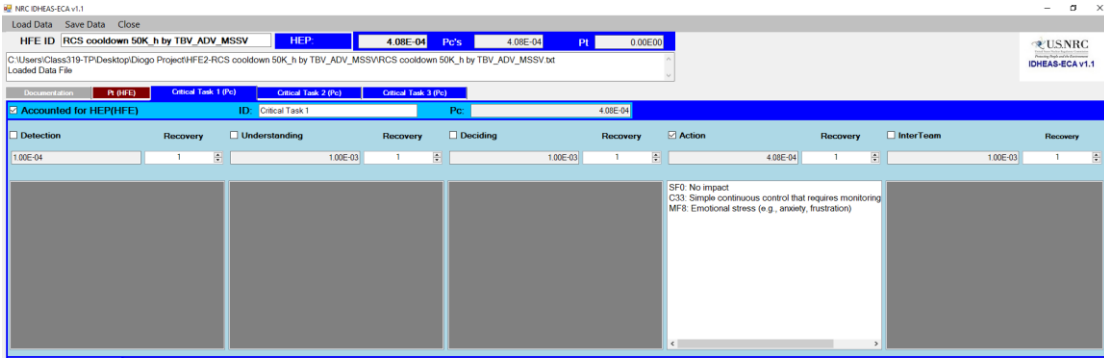


Figure 16 -  $P_c$  estimation for HFE2

### 7.2.6 STEP 6: ESTIMATION OF $P_t$ – THE CONVOLUTION OF THE DISTRIBUTION OF TAVAIL AND TREQ

The estimation of  $P_t$  for the HFE2 – Cooldown RCS at 50K/h by TBV/ADV/MSSV is obtained using the IDHEAS-ECA and it is shown in Figure 17.

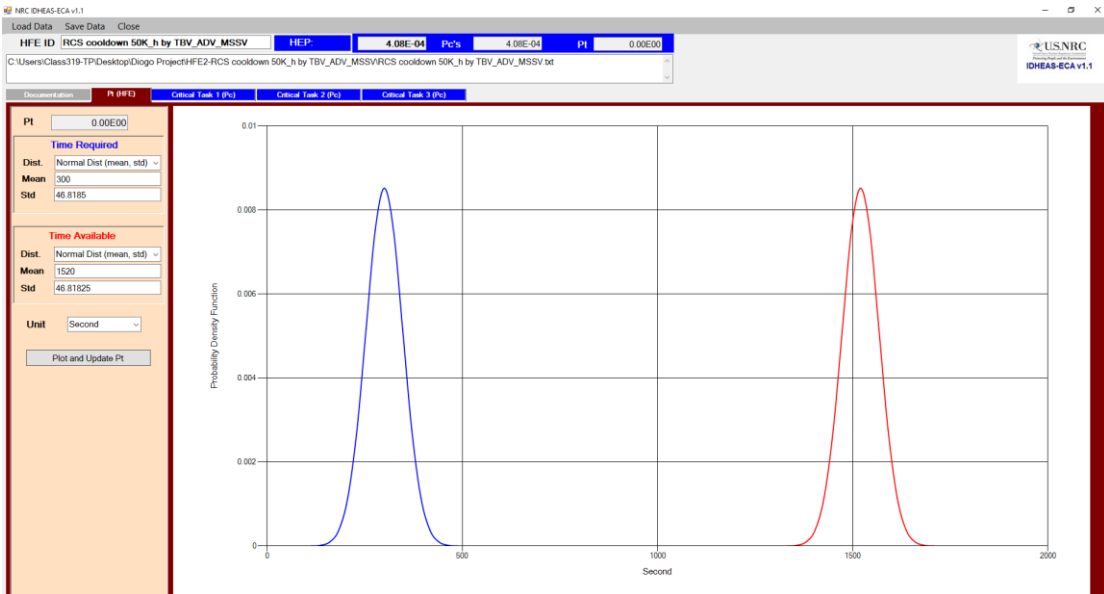


Figure 17 -  $P_t$  estimation for HFE2

### 7.2.7 STEP 7: CALCULATE THE OVERALL HEP

The summary of the HEP calculation is illustrated in Table 16.

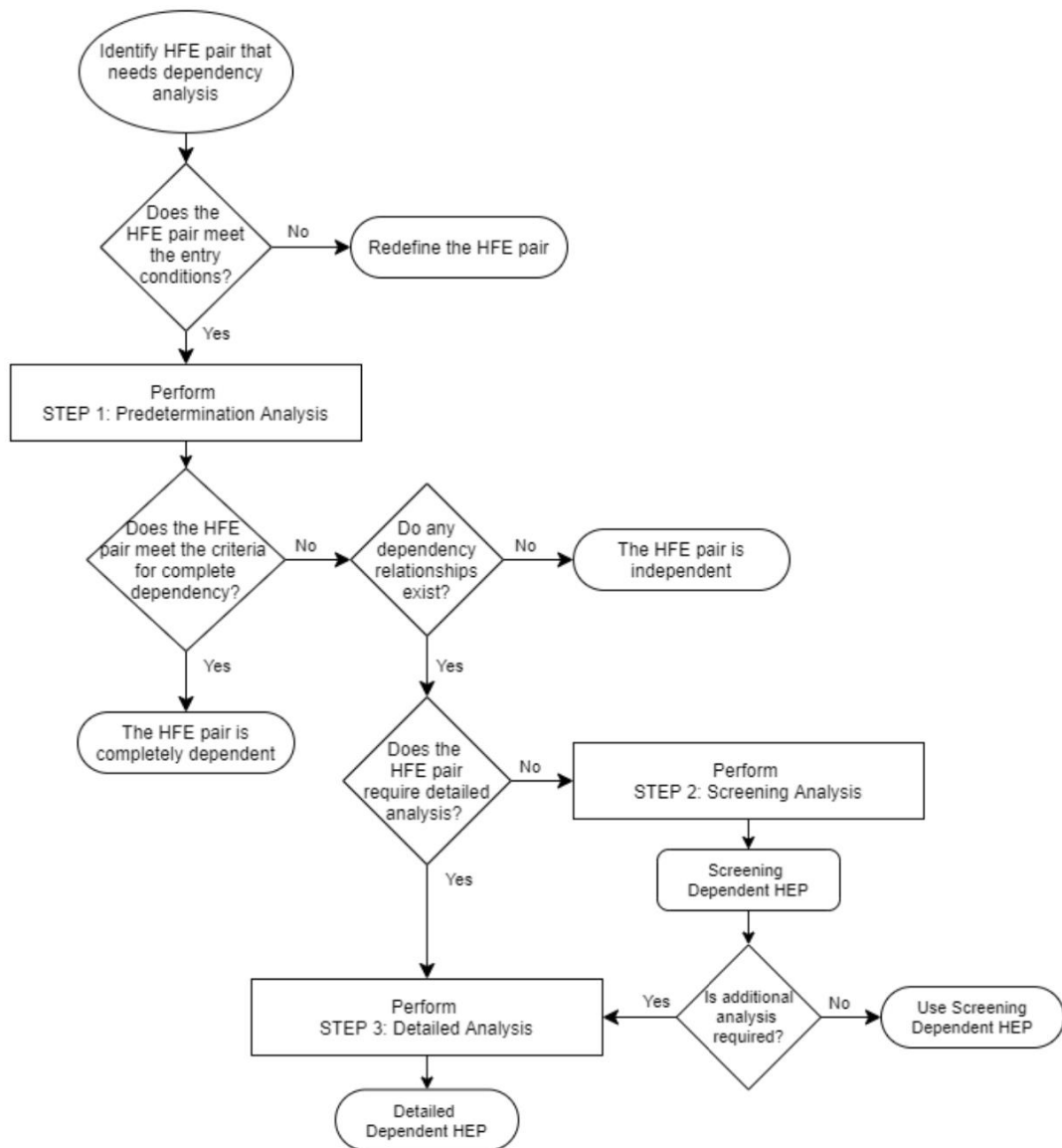


**Table 16 - Summary of HEP Quantification for HFE2**

<b>CFM</b>	<b>PIF<sub>Attribute</sub></b>	<b><math>P_{CFM_{Base}}</math></b>	<b><math>w_i</math></b>	<b><math>P_{CFM}</math></b>
<b>Action</b>	SF0: no impact TC-C33: Simple continuous control that requires monitoring parameters. MF8 – Emotional stress	$1 \times 10^{-4}$	$1 \times 10^{-4}$ 1.2	$4.08 \times 10^{-4}$
<b>TOTAL P<sub>CT1</sub></b>				$4.08 \times 10^{-4}$
<b>P<sub>t</sub></b>				0.00
<b>HEP<sub>IDHEAS-ECA</sub></b>				$4.08 \times 10^{-4}$

### 7.2.8 STEP 8 – DEPENDENCY ANALYSIS

The dependence analysis using the IDHEAS-DEP method comprises three primary components. The initial segment aims to ascertain whether HFE1 influences the HFE2 context. Subsequently, the second part entails determining the manner in which HFE1 impacts the HFE2 context. Lastly, the dependent HEP for HFE2 is computed based on contextual changes resulting from the failure of HFE1. In essence, the dependency analysis conducted by the IDHEAS-DEP method is founded upon alterations in specific contexts induced by the malfunction of the preceding HFE1 [23]. Figure 18 provides an overview of the dependence analysis process through IDHEAS-DEP.



**Figure 18 – IDHEAS-DEP dependency analysis process**

The initial phase of the dependence analysis process commences with the confirmation of whether the HFE pair satisfies the input conditions. Once these input conditions are met, the analyst proceeds with a predetermined analysis to determine the degree of dependence. If the HFE pair is found to be entirely dependent, the HEP of HFE2 transitions to 1, necessitating the incorporation of HFE2 into HFE1. If it is established that the HFE pair exhibits no dependency, complete independence is

defined between the pairs, and the previously determined HEP values remain unchanged. However, if a certain degree of dependence is identified, the analyst must ascertain which of the five dependence relationships among HFEs applies to the case, namely: function or system; temporal proximity; personnel; location; and procedural dependencies.

In the second phase, the analyst must decide whether the analysis requires a screening or detailed analysis to determine how the failure of HFE1 affects the context of HFE2. Finally, in the third phase, the dependent HEP is calculated.

Subsequently, the analysis is conducted by IDHEAS-DEP method and the dependent HEP for HFE2 in the event of HFE1 failure will be demonstrated.

#### **7.2.8.1 ENTRY CONDITION:**

The entry conditions for applying dependency analysis using this process are as follows:

1. (a) HFE1 and HFE2 are in the same PRA event sequence or minimal cutset,  
AND  
(b) there are no relevant human action success events between HFE1 and HFE2 in the sequence, OR
2. (2) The initiating event is caused by human actions and is analyzed as the first HFE, such that the subsequent HFEs need to be assessed for dependency. These are also called at-initiators and are common at shutdown [23].

The pair of HFE object of this analysis meet the conditions 1 above and the analyze should proceed to the predetermination analysis step shown in Table 17.

**7.2.8.2 PREDETERMINATION ANALYSIS:**

**Table 17 – Predetermination analysis for HFE1 and HFE2**

<b>Relationship</b>	<b>Assessment Guideline</b>	
Complete Dependency	<input checked="" type="checkbox"/> HFE1 and HFE2 use the same procedure, <b>AND</b>  <input type="checkbox"/> HFE1 is likely to occur because of issues associated with the common procedure (such as having an ambiguous or incorrect procedure HFE1 and HFE2), <b>AND</b>  <input type="checkbox"/> There is no opportunity to recover from the issue with the procedure between HFE3 and HFE4	<input type="checkbox"/> YES  <input type="checkbox"/> NO
R1- Functions or Systems	<input type="checkbox"/> HFE1 and HFE2 have the same function, <b>OR</b>  <input checked="" type="checkbox"/> HFE1 and HFE2 have coupled systems or processes that are connected due to automatic responses or resources needed	<input checked="" type="checkbox"/> YES  <input type="checkbox"/> NO
R2 – Time Proximity	<input checked="" type="checkbox"/> HFE1 and HFE2 are close in time, <b>OR</b>  <input type="checkbox"/> The cues for HFE1 and HFE2 are presented close in time	<input checked="" type="checkbox"/> YES  <input type="checkbox"/> NO
R3 - Personnel	<input checked="" type="checkbox"/> HFE1 and HFE2 are performed by the same personnel	<input checked="" type="checkbox"/> YES  <input type="checkbox"/> NO
R4 - Location	<input checked="" type="checkbox"/> HFE1 and HFE2 are performed at the same location, <b>OR</b>  <input type="checkbox"/> The workplaces for HFE1 and HFE2 are affected by the same condition (such as low visibility, high temperature, low temperature, or high radiation)	<input checked="" type="checkbox"/> YES  <input type="checkbox"/> NO
R5 - Procedure	<input type="checkbox"/> HFE1 and HFE2 use the same procedure	<input checked="" type="checkbox"/> YES  <input type="checkbox"/> NO
<input type="checkbox"/>	HFE2 is completely dependent on HFE1; thus, the adjusted probability of HFE2 is 1.0	

<input type="checkbox"/>	HFE2 is independent of HFE1; thus, the adjusted HEP of HFE2 is equal to the individual HEP of HFE2
<input checked="" type="checkbox"/>	One or more dependency relationships exist; thus, the analyst proceeds to either step 2, screening analysis, or step 3, detailed analysis to obtain the dependent HEP for HFE2

The outcome of the predetermined analysis assumed that the five dependence relationships considered by IDHEAS-DEP should be analyzed in the screening analysis. As the scope of this project is not specifically to assess different dependence analysis methods but rather to evaluate the consistency of results obtained by IDHEAS-ECA and in accordance with the guidance of IDHEAS-DEP where screening analysis should be applied when "only a quick, rough screening dependent HEP value is needed for the purpose of the HRA application" or "the individual HEPs were calculated using another HRA method and cannot be recalculated with IDHEAS-ECA" [23]. Therefore, a screening analysis of the selected dependence relationships will be executed.

### 7.2.8.3 SCREENING ANALYSIS:

Tables 18, 19, 20, 21, 22, 23, 24, 25 and 26 describe the screening analysis for each dependency relationship selected in the predetermination analysis respectively.

### 7.2.8.4 R1 – FUNCTIONS OR SYSTEMS

**Table 18 – R1: Functions or systems cognitive dependency**

<b>Potential Dependency Factors</b>	<b>Basis for Discounting the Potential Dependency Factor</b>	<b>Dependency Impact</b>
<b>R1.1</b> Use of the same functions or systems leads to cognitive dependency	<input type="checkbox"/> A- HFE2 was trained on in the scenarios in which HFE1 occurs (e.g., Feed & Bleed is the last	This cognitive dependency potentially affects the PIF for scenario familiarity, which addresses the

<p>A. Occurrence of HFE1 leads to the scenario or parts of the scenario being different from what was typically trained on; thus, the scenario associated with HFE2 becomes less familiar. (Note: Occurrence of HFE1 alters the scenario for HFE2; thus, HFE1 causes some level of unfamiliarity with HFE2.)</p> <p>B. Occurrence of HFE1 leads to an incorrect or biased mental model of the situation associated with HFE2.</p>	<p>action after others fail), so there is no unfamiliarity due to HFE1.</p> <p><input type="checkbox"/> B- HFE2 is well-trained on in various scenarios such that personnel are unlikely to develop a wrong mental model due to occurrence of HFE1.</p>	<p>mental model. Scenario familiarity is applicable when something is wrong with the mental model and no diverse methods are available to correct the wrong mental model. <b>(Discounted)</b></p>
	<p><input checked="" type="checkbox"/> A/B- There is no cognitive link (similar thought process) between the two HFEs; thus, occurrence of HFE1 has no impact on scenario familiarity or the mental model associated with HFE2.</p>	<p>Low: Pd = 5E-2</p> <p><input type="checkbox"/> Parts of the scenario become unfamiliar (e.g., different from what was trained on), <b>OR</b></p> <p><input type="checkbox"/> HFE1 creates a biased mental model or preference for wrong strategies.</p>
	<p><input type="checkbox"/> B- There are opportunities between the HFEs to break the incorrect mental model, such as multiple crews or diverse cues.</p>	<p>Medium: Pd = 1E-1</p> <p><input type="checkbox"/> Parts of the scenario become unfamiliar (e.g., different from what was trained on), <b>AND</b></p> <p><input type="checkbox"/> HFE1 creates a biased mental model or preference for wrong strategies.</p>
		<p><input type="checkbox"/> HFE1 creates a mismatched or wrong mental model for HFE2 due to close cognitive links between HFE1 and HFE2 (i.e., thought process).</p>

**Table 19 - R1: Functions or systems Consequential dependency**

Potential Dependency Factors	Basis for Discounting the Potential Dependency Factor	Dependency Impact
------------------------------	---	-------------------

<p><b>R1.2</b> Use of same functions or system leads to consequential dependency</p> <p>A. Occurrence of HFE1 makes HFE2 more complex because the systems, indications, or controls for HFE2 may be incorrect, misunderstood, or in a different status due to the occurrence of HFE1.</p> <p>B. Occurrence of HFE1 makes the information for diagnosis or decisionmaking for HFE2 less timely or less trusted (e.g., personnel discount indications or cues for HFE2 due to inadequate training on the unusual or unexpected scenario created by HFE1 or early termination of information collection).</p>	<input type="checkbox"/> A – No common equipment (e.g., different trains), different interfaces and different indications and controls	<p>This consequential dependency potentially impacts the PIFs for task complexity and information availability and reliability. <b>(Discounted)</b></p> <p>Low: Pd = 1E-2 Task is relatively simple, and one or two of the following apply:  <input type="checkbox"/> Cues for detection are less obvious  <input type="checkbox"/> Execution criteria become complicated or ambiguous.  <input type="checkbox"/> Potential outcome of the situation assessment becomes more complicated (e.g., multiple states and contexts, not a simple yes or no).  <input type="checkbox"/> Decisionmaking criteria become intermingled, ambiguous, or more difficult to assess.</p> <p>Medium: Pd = 5E-2  <input type="checkbox"/> More than two items in “Low” are applicable.</p> <p>High: Pd = 2E-1  <input type="checkbox"/> Cues are masked or must be inferred.  <input type="checkbox"/> Detection of critical information is entirely based on personnel’s experience and knowledge.  <input type="checkbox"/> Execution of the critical task requires breaking away from trained scripts.  <input type="checkbox"/> HFE1 creates ambiguity associated with assessing the situation for performing HFE2.</p>
	<input checked="" type="checkbox"/> A/B – Occurrence of HFE1 does not impact the information or cues used for HFE2, so there is no impact on information needed for HFE2.	
	<input type="checkbox"/> B – Personnel have firm information or multiple sources of information that are consistent.	
	<input type="checkbox"/> A/B – Occurrence of HFE1 is obvious, and personnel are trained to diagnose HFE2 given occurrence of HFE1.	

		<input type="checkbox"/> HFE1 creates competing or conflicting goals for decisionmaking of HFE2.
--	--	--

**Table 20 - R1: Functions or systems resource-sharing dependency**

<b>Potential Dependency Factors</b>	<b>Basis for Discounting the Potential Dependency Factor</b>	<b>Dependency Impact</b>
<p><b>R1.3</b> Use of the same functions or systems leads to resource-sharing dependency</p> <p>A. Shared tools or equipment leads to shortage of tools or equipment needed for HFE2.</p> <p>B. Shared resources (e.g., water, power, or offsite resources such as fire trucks) lead to inadequate resources or increased complexity for HFE2.</p>	<p><input checked="" type="checkbox"/> A – No shared or no shortage of tools or equipment.</p> <p><input checked="" type="checkbox"/> B – No shared or no shortage of resources.</p> <p><input type="checkbox"/> A/B – There is adequate time to perform the actions sequentially using the shared tools, equipment, or resources.</p>	<p>This resource-sharing dependency potentially impacts the PIF for task complexity because the portion of resources HFE2 shares with HFE1, such as power in FLEX events, may be reduced due to HFE1.</p> <p><b>(Discounted)</b></p>
		<p>Low: Pd = 1E-2</p> <p><input type="checkbox"/> Tool or resource shortage increases task difficulty, such as the following:</p> <ul style="list-style-type: none"> <li>– high spatial or temporal precision</li> <li>– precise coordination of multiple persons</li> <li>– unusual, unevenly balanced loads, reaching high parts</li> <li>– continuous control that requires dynamic manipulation</li> </ul>
		<p>Medium: Pd = 2E-3</p> <p><input type="checkbox"/> Complicated or ambiguous execution</p>



	<p>criteria are present, such as the following:</p> <ul style="list-style-type: none"> <li>– multiple, coupled criteria</li> <li>– open to misinterpretation</li> </ul>
	<p>High: Pd = 1E-2</p> <p><input type="checkbox"/> Action execution requires close coordination of personnel at different locations.</p>

### 7.2.8.5 R2 – Time Proximity

Table 21 – R2: Time proximity consequential dependency

Potential Dependency Factors	Basis for Discounting the Potential Dependency Factor	Dependency Impact	
<p><b>R2.1</b> Close time proximity in performing HFE1 and HFE2 leads to consequential dependency</p> <p>A. Occurrence of HFE1 reduces the time available or increases the time required for HFE2</p>	<p><input checked="" type="checkbox"/> A- The ratio of time available to time required, <math>T_a/T_r</math>, for HFE2 is greater than 4 (<math>T_a</math> is 5,06 greater than <math>T_r</math>); thus, plenty of time is available HFE2, and the dependency due to time proximity is negligible.</p> <p><input type="checkbox"/> A – There is no change in the time available and time required for HFE2 due to HFE1</p>	Use the ratio of $T_a$ to $T_r$ for HFE2 and the chart below to estimate the dependency impact. $T_a$ and $T_r$ are point estimates.	
		$T_a/T_r$	Dependency impact
		< 1	1
		$\geq 1$ and <2	1E-1
		$\geq 2$ and <3	1E-2
		$\geq 3$ and <4	1E-3
		>4	<b>Negligible</b>
<p><b>R2.2</b> Close time proximity in receiving the clues for HFE1 and HFE2 leads to consequential dependency</p> <p>A. Cues for HFE1 and HFE2 occur close in time such that the cues for HFE2 is likely to be masked or forgotten by the</p>	<p><input type="checkbox"/> A- The cues for HFE1 and HFE2 do not occur close in time.</p> <p><input type="checkbox"/> A – Personnel are trained to identify the need for HFE2 given occurrence of HFE1.</p>	This consequential dependency potentially affects the PF for task complexity by increasing the difficulty of detecting cues for HFE2.	
		<b>Low: Pa = 5E-3</b>	<input checked="" type="checkbox"/> Detecting of the cue demands switching between tasks or needs

time HFE2 needs to be performed.	<input type="checkbox"/> A – The cues remain available and salient, and there is adequate time to perform the action such that personnel could identify the cues and perform the task later without impact.	sustained attention over time.
		Medium: $P_d = 5E-2$ <input type="checkbox"/> Detection of the cue is not directed by alarms or procedures, and personnel need to continuously monitor or actively search for the cue.
		High: $P_d = 1E-2$ <input type="checkbox"/> The cue is masked such that initiating HFE2 is based on the personnel's experience and knowledge.

### 7.2.8.6 R3 – Personnel

Table 22 – R3: Personnel cognitive dependency

Potential Dependency Factors	Basis for Discounting the Potential Dependency Factor	Dependency Impact
<b>R3.1</b> Same personnel leads to cognitive dependency  A. Same person performs the two HFEs; thus, the person may incorrectly interpret the situation for HFE2 due to occurrence of HFE1.  B. Same personnel or crew makes diagnosis or decisionmaking in the two HFEs; thus, personnel may experience groupthink, which causes	<input checked="" type="checkbox"/> A- Training and experience rule out the possibility of misinterpreting the situation.  <input type="checkbox"/> A – The HFEs are not performed by the same person.  <input checked="" type="checkbox"/> A/B – Additional people are available to break group think or question the interpretation of the situation	This cognitive dependency potentially affects the PIFs for scenario familiarity, which address the mental model. Scenario familiarity is applicable when something is wrong with the mental model and no diverse methods are available to correct the wrong mental model. <b>(Discounted)</b>
		Low: $P_d = 5E-3$ <input type="checkbox"/> Parts of the scenario become unfamiliar (e.g., different from what was trained on), <b>OR</b>

a biased or incorrect mental model for HFE2.	<input type="checkbox"/> A/B – Different procedures are used for HFE3 and HFE4.	<input type="checkbox"/> HFE1 creates a biased mental model or preference for wrong strategies.
	<input type="checkbox"/> B – Same personnel or crew does not perform diagnosis or decision-making for the HFEs.	Medium: $P_d = 1E-1$ <input type="checkbox"/> Parts of the scenario become unfamiliar (e.g. different from what was trained on), <b>AND</b> <input type="checkbox"/> HFE1 creates a biased mental model or preference for wrong strategies.
	<input type="checkbox"/> B – Work process independence factors are used that could break groupthink or the wrong mental model.  <input checked="" type="checkbox"/> B – New cues before HFE2 (from procedures, indications, or success of other human actions) can break down the occurrence of HFE1 <b>AND</b> additional people are available to detect the cues <b>AND</b> adequate time is available to detect the new cues.	High: $P_d = 3E-1$ <input type="checkbox"/> HFE1 creates a mismatched or wrong mental model for HFE1 due to close cognitive links (i.e., thought process).

**Table 23 - R3: Personnel consequential dependency**

Potential Dependency Factors	Basis for Discounting the Potential Dependency Factor	Dependency Impact
<b>R3.2</b> Same personnel leads to consequential dependency  A. Mental fatigue, time pressure, or stress level increase due to the same personnel performing HFE1 and HFE2.	<input type="checkbox"/> A- Workload is similar to training situations and occurs with a single shift, so no increase in stress, time pressure, or mental fatigue.  <input type="checkbox"/> B – HFE1 and HFE2 are not performed at the same time.	This consequential dependency potentially affects the PIFs for mental fatigue, stress, time pressure, and staffing. Mental fatigue may occur due to working on cognitively demanding tasks in HFE1 and HFE2. Staffing may be impacted

<p>B. Personnel need to perform HFE1 and HFE2 at the same time.</p>	<p><input type="checkbox"/> B – Additional personnel are available to perform HFE2.</p>	<p>due to lack of personnel to perform both actions or when both actions are performed in parallel.</p>
		<p><b>Low: P<sub>d</sub> = 2E-3</b></p> <p><input type="checkbox"/> Mental fatigue increases due to sustained highly demanding cognitive activities, <b>OR</b></p> <p><input checked="" type="checkbox"/> Time pressure increases due to perceived time urgency and task load.</p>
		<p>Medium: P<sub>d</sub> = 1E-2</p> <p><input type="checkbox"/> Same personnel perform HFE1 and HFE2 in parallel, <b>AND</b></p> <p><input type="checkbox"/> HFE2 does not require complicated diagnosis.</p>
		<p>High: P<sub>d</sub> = 3E-2</p> <p><input type="checkbox"/> Same personnel perform HFE1 and HFE2 in parallel, <b>AND</b></p> <p><input type="checkbox"/> HFE2 requires complicated diagnosis.</p>

**Table 24 - R3: Personnel resource-sharing dependency**

Potential Dependency Factors	Basis for Discounting the Potential Dependency Factor	Dependency Impact
<p><b>R3.3</b> Same personnel leads to resource-sharing dependency</p> <p>A. Reduced staffing or missing key members results in higher workload than in training or lack of key knowledge needed. This would generally only</p>	<p><input checked="" type="checkbox"/> A/B – Staffing is adequate, and good work practices are enforced.</p> <p><input type="checkbox"/> A/B – Staffing, workload, and work practices are similar to training situations. (EOPs are trained upon using</p>	<p>This resource-sharing dependency potentially affects the PIFs for staffing, teamwork and organizational factors, and work practices. Work practices, such as peer checking, may change due to lack of adequate staffing (<b>Discounted</b>)</p>

<p>apply to SDPs (actually fitness for duty event) or fire events.</p> <p>B. Shared staff requires changes to the work practices for HFE2 (e.g., shortcuts, no peer chacking or supervision) to accommodate shortage of staffing due to occurrence of HFE1.</p>	<p>minimum staffing, but use of the severe accident management guidelines (SAMGs) or fire procedures may require additional personnel, shortcuts, or use of personnel outside what is normally trained upon.)</p> <p><input type="checkbox"/>B – Minimum staffing is adequate to complete both tasks without changes to the work practices.</p>	<p>Low: <math>P_d = 2E-3</math></p> <p><input type="checkbox"/> Key staff needed for HFE2 are reduced or untimely due to HFE1, <b>OR</b></p> <p><input type="checkbox"/> Teamwork factors are inadequate, such as knowledge gaps, distributed teams (personnel in multiple locations), dynamic teams (changing team members), or poor team cohesion.</p>
		<p>Medium: <math>P_d = 1E-2</math></p> <p><input type="checkbox"/> Self-checking or human performance tools (e.g., three-way communication) are not used as trained, <b>OR</b></p> <p><input type="checkbox"/> Peer checking or supervision is ineffective.</p>
		<p>High: <math>P_d = 5E-2</math></p> <p><input type="checkbox"/> Work scheduling or prioritization is poor.</p>

### 7.2.8.7 R4 – LOCATION

Table 25 – R4: Location consequential dependency

Potential Dependency Factors	Basis for Discounting the Potential Dependency Factor	Dependency Impact
<p><b>R4.1</b> Same location leads to consequential dependency</p> <p>A. HFE1 degrades the work environment for</p>	<p><input checked="" type="checkbox"/>A – HFE1 has no impact on the workplace .</p>	<p>This consequential dependency potentially affects the PIF for environmental factors. <b>(Discounted)</b></p>

<p>HFE2 (e.g., reduced workplace accessibility or habitability, abnormal heat or cold, reduced visibility, noise).</p>		<p>Low: <math>P_d = 2E-3</math>  <input type="checkbox"/> HFE3 causes any one of the following to exist for HFE4: reduced workplace accessibility or habitability, abnormal heat or cold, reduced visibility, or noise.</p>
		<p>Medium: <math>P_d = 5E-3</math>  <input type="checkbox"/> HFE3 causes two or more of the following to exist for HFE4: reduced workplace accessibility or habitability, abnormal heat or cold, reduced visibility, or noise.</p>
		<p>High: <math>P_d = 2E-2</math>  <input type="checkbox"/> HFE3 significantly impairs the work environment for HFE4, such as by causing excessive heat and humidity, poor visibility, or unstable surface for executing the action.</p>
<p><b>R4.2</b> Same location and time leads to consequential dependency</p> <p>A. HFE1 and HFE2 use the same workplace at the same time such that HFE1 may interfere with or cause distractions in the performance of HFE2.</p>	<p><input type="checkbox"/> A – HFE1 and HFE2 are not performed at the same time.</p> <p><input type="checkbox"/> A – Actions can be performed without interference.</p> <p><input type="checkbox"/> A – HFE1 is straightforward and does not require sustained attention (thus, it is resistant to interference).</p>	<p>This consequential dependency potentially affects the PIF for multitasking, interruptions, and distractions due to sharing the same location at the same time.</p> <p><b>Low: <math>P_d = 2E-3</math></b>  <input checked="" type="checkbox"/> Personnel are distracted by the outcome of HFE1.</p> <p>Medium: <math>P_d = 5E-3</math>  <input type="checkbox"/> Performance of HFE2 is frequently interrupted by the outcome of HFE1.</p>

		High: $P_d = 7E-3$ <input type="checkbox"/> Performance of HFE2 is frequently or continuously interrupted by the outcome of HFE1.
--	--	--

### 7.2.8.8 R5 – PROCEDURE

Table 26 – R5: Procedure cognitive dependency

Potential Dependency Factors	Basis for Discounting the Potential Dependency Factor	Dependency Impact
<p><b>R5.1</b> Same procedure leads to cognitive dependency</p> <p>A. Occurrence of HFE1 makes the procedure less applicable for use with HFE2 (i.e., the procedure becomes more confusing or does not match the situation well). For example, EOPs are generally well written because they are used often in training, but use of at-power EOPs at shutdown may be confusing because equipment is not in its normal configuration. Use of procedures during a fire or MCR abandonment situation may not apply as well as when at power.</p> <p>B. Occurrence of HFE1 makes personnel more likely to incorrectly interpret the procedure for use with HFE2 because</p>	<p><input checked="" type="checkbox"/> A/B – Procedure is clear, not confusing, applicable to the situations, and well-trained upon.</p> <p><input type="checkbox"/> A/B – Personnel are trained to use the procedure for the specific situations.</p>	<p>This cognitive dependency potentially affects the PIFs for procedures and guidance and for scenario familiarity due to the effect on personnel’s mental model.  <b>(Discounted)</b></p>
		<p>Low: <math>P_d = 5E-3</math></p> <p><input type="checkbox"/> HFE1 makes the procedure more confusing for personnel to follow.</p>
		<p>Medium: <math>P_d = 5E-2</math></p> <p><input type="checkbox"/> HFE1 creates a misunderstanding of the situation such that personnel are likely to misinterpret the procedure, <b>OR</b></p> <p><input type="checkbox"/> HFE1 causes unfamiliar elements in the scenario for performing HFE2.</p>
		<p>High: <math>P_d = 3.5E-1</math></p> <p><input type="checkbox"/> HFE3 creates a mismatch or wrong model for HFE4, <b>OR</b></p>

they are using the same procedure.		<input type="checkbox"/> HFE3 creates a bias or preference for wrong strategies, <b>OR</b> <input type="checkbox"/> HFE3 makes the situation for performing HFE4 extremely rare, such that personnel have no existing mental model for the situation.
------------------------------------	--	--

After running the screening analysis, the HFE2-dependent HEP is calculated by probabilistically summing the individual HFE2 HEP and each of the undiscounted dependency impact (Pd) values according to the equation provided by the IDHEAS-DEP guidance. The calculation of the new HFE2 HEP considering the screening analysis is shown below:

$$\begin{aligned}
 \text{Dependence HEP for HFE2} &= 1 - (1 - 4.08 \times 10^{-4}) \times \\
 &\quad (1 - 5 \times 10^{-3}) \times (1 - 2 \times 10^{-3}) \times (1 - 2 \times 10^{-3}) \\
 \text{Dependence HEP for HFE2} &= 9.38 \times 10^{-3}
 \end{aligned}$$

### 7.3 HFE3: DRAIN THE FEEDWATER TANK (LAA) IN CASE OF SG FEEDWATER PUMP FAILURE

#### 7.3.1 Step 1: Scenario Analysis

##### 7.3.1.1 Step 1.1: Develop scenario narrative

For HFE3, it assumed the same scenario narrative as described in section 7.1.1.1 for HFE1, however, it is made necessary to add an extra detailed and specific description as follows.

During the top-of-cooldown event of the Reactor Coolant System (RCS) at a rate of 50 Kelvin per hour, preferably, the secondary system will operate through the



turbine bypass valves (TBV), condensers, condensate pumps, the feedwater storage tank (LAA), and through the pumps of the main feedwater system (LAB) and the startup and shutdown system (LAH), in a configuration considered to be in a closed loop. In the event of SGs feedwater failure by LAB and LAH, the SGs levels would decrease, and when they reach 5 meters, the protection system initiates the signal to start the emergency feedwater pumps (LAS) for the respective trains. Upon the start of LAS operation in the closed-loop configuration, the level in LAA begins to rise, and when it reaches a value of 2.7 meters, the control room alarm LAA10EZ002XK94 (High Level 1) is generated, prompting the operators to go to feedwater storage tank alarm procedure (OP-5-LAA). After the level 1 alarm, the operator is instructed to close the LAA water makeup valve through the demineralized water supply system (GHC), which is not the solution in this scenario. Consequently, the level will continue to rise and reaches 2.85 meters, at which point the protection system will trigger the high level 2 alarm (LAA10CL002XH03). Following the level 2 alarm, the operator must acknowledge the alarm, understand the problem and its consequences by the alarm procedure, and ultimately verify and execute all possible available solutions to rectify the condition that caused the alarm. At this point, the control room operators must open valve LAA10AA051 to prevent the LAA level from reaching 3.2 meters, which would lead to the shutdown of the Feedwater Pumps (LCA) and the loss of the closed loop.

### **7.3.1.2 Step 1.2: Identify Human Failure Event (HFE)**

HFE3: Drain the Feedwater Tank (LAA) in Case of SG Feedwater Pump Failure. This HFE comprise all the actions taken by the operators in the MCR to detect the alarm,

deploy alarm procedure (OP-5-LAA), understanding what is happening and the possible solutions, and finally execute the action to open the drain valve.

### **7.3.1.3 Step 1.3: Identify the scenario/Event Context**

- **Environment and situation:** It is assumed the same context stated in section 7.1.1.3.
- **System:** It is assumed the same context stated in section 7.1.1.3.
- **Personnel:** It is assumed the same context stated in section 7.1.1.3.
- **Task:** It is assumed the same context stated in section 7.1.1.3, however, an extra description for scenario/event context is required as follows. During RCS cooldown at 50K/h at closed cycle, it is assumed the possibility of the SG feedwater failure and the operator should identify it through the alarm. The cue is the LAA tank level rising, and the consequence is the loss of the closed cycle. At this point, it is assumed that the operator is focused on the alarms that may arise during accident mitigation. When the LAA high level alarm is activated ( $L_{LAA} > 2,85\text{m}$ ), the operator should deploy the alarm procedure (OP-5-LAA), understand the situation and consequences alarm which is explained in the procedure and the consequences, then the operator should execute the 5 possible solutions provided by the procedure to avoid the LAA tank level achieve 3.2m.

## **7.3.2 STEP 2: ANALYZING HUMAN FAILURE EVENTS (HFE)**

### **7.3.2.1 Step 2.1: Defining the Human Failure Events (HFE)**

This section defines the HFE and describe the scope of the analysis:

- Success Criteria: Detect the need to drain the LAA and open the LAA drain valve (LAA10AA051).
- Consequence: If operators fail to drain the LAA, it is considered the loss of cooling by the SGs using the TBV in the closed cycle and the demand for the open cycle are considered.
- Beginning and ending points: The HFE begins when the level of LAA achieve 2,85m and the alarm (LAA10CL002XH03) is alerted on the alarm screen. The operator will identify the alarm which directs him to execute the related alarm procedure (OP-5-LAA). The operator will understand that the LAA tank achieved the high level max 2 and if nothing is done the condensate pump will be turned off. Then the operator should open the drain valve to stop the rise of LAA level.
- Relevant procedure guidance: OP-5-LAA

NOTE: The specification for this analysis were adopted from constant values for time based on Angra-2 FSAR and current PSA under development. In future studies, the timing could be deduced based on experimental models from Angra-2 simulator.

- Cues and indications for initiating the operator action and timing:  $T_{\text{delay}}$  is based on the time between the beginning of the event and the identification of the cue, where the operator action was started through procedure guidance. The cues which the operator will start their action is the high level alarm 2 (LAA10CL002XH03). For diagnose the event, the cues are high level 2 in the LAA tank  $> 2.85\text{m}$  and rising. Based on the literature, it is assumed that an operator during accident mitigation takes around 25s to

acknowledge an alarm [19], therefore, the cognition phase will start with a delay time of  $T_{\text{delay}} = 25\text{s}$ .

- Available time to perform the operator action: The system time window ( $T_{\text{SW}}$ ) is estimated based on time take by the LAA tank level to rise from 2.85m to 3.2m. Based on Angra-2 PSA, the  $T_{\text{SW}} = 5400\text{s}$ . In this way, the time available ( $T_{\text{avail}}$ ) is  $T_{\text{SW}} - T_{\text{delay}}$  resulting in  $T_{\text{avail}} = 5375\text{s}$ .
- Time required to perform the operation action: In the absence of data from Angra-2 PSA for this HFE, it will be considered 5 minutes for cognition time ( $T_{\text{cog}}$ ) and 1 minute to execute each step, based on FSAR and literature [4][8]. In this way, the execution time ( $T_{\text{exe}}$ ) to execute 5 steps stated in the alarm procedure will take 300 seconds. The time required ( $T_{\text{req}}$ ) is the time spent by the operator to perform the cognitive and execution part following the procedure, therefore,  $T_{\text{req}} = 600\text{s}$ . All the timing is summarized in the timeline diagram shown in Figure 12.

### **7.3.2.2 Step 2.2: Task Analysis and Identification of Critical Tasks**

To keep it simple, one crucial task is defined, which involves the recognizing of high level max 2 in LAA tank and deploy the alarm procedure (OP-5-LAA) to stop the LAA rise of level. Additionally, the HFE is assumed as one critical task because the same context is applicable from the start to the end of the HFE process.

### 7.3.3 STEP 3: MODELING FAILURE OF CRITICAL TASKS

#### 7.3.3.1 Step 3.1: Characterization of Critical Tasks

This section specifies the relevant conditions that affect the performance of the critical task.

- Critical task goal: identify the high level max 2 in the LAA tank and open the drain valve to avoid the loss of the condenser pump and consequently the loss of RCS cooling by SG in closed cycle.
- Specific requirements: verify the correct solution to stop the rise of LAA tank level in the respective alarm procedure and open the LAA tank drain valve (LAA10AA051).
- Cues and supporting information: LAA tank high level 2 alarm (LAA10CL002XH03),  $L_{LAA} > 2.85\text{m}$ .
- Procedure: Alarm Procedure (OP-5-LAA).
- Personnel: The team in the MCR are composed by 5 operator which are the Shift supervisor (SS); Shift Foreman (SF); Primary operator (PO); Secondary operator (SO); and Auxiliary panel operator (AO). The operators in the main control room are well-trained and perform SGTR training in the simulator twice a year considering this failure.
- Task Support: Procedures specified above and MCR indications.
- Location: Main control room (MCR).
- Cognitive activities: Detection, understanding and action.
- Concurrent tasks: assuming that there are no other tasks.

- Interteam coordination considerations: multiple teams are not involved with this critical task. SGTR mitigation is handle by the MCR operational team.

### **7.3.3.2 Step 3.2: Identification of Applicable Cognitive Failure Modes (CFM)**

The applicable CFM is identified by assessing the cognitive activities of the critical task that are associated with each macrocognitive function.

- Detection: detect cues and acquire information.
  - Operators need to detect the alarm through the alarm screen.
  - CFM1 – failure of detection applies to the critical task.
- Understanding: diagnose problems, maintain situational awareness.
  - Operators need to be aware that the alarm is related to the rise of LAA tank level, and he should deploy the alarm procedure to deal with it.
  - CFM2–failure of understanding applies to the critical task.
- Decisionmaking: make a go/no-go decision for a pre-specified action.
  - The operator should understand the consequences of the alarm and he needs to decide to execute the proper action in the alarm procedure to avoid the consequences applicable to the alarm.
  - CFM3: failure of decisionmaking applies to the critical task.
- Action Execution: execute cognitively simple actions.
  - The operator should execute 5 actions to accomplish the task goal. The actions performed are relatively simple actions because operators are trained to, however, there are other variables to monitoring during accident mitigation.

- CFM4: failure of action execution applies to the critical task.
- Interteam coordination: the critical task is implemented by the MCR operators, which is considered an individual team and SGTR does not require coordination among multiple teams.
  - CFM5: failure of interteam coordination DOES NOT apply to the critical task.

#### **7.3.4 STEP 4: ASSESSING PERFORMANCE INFLUENCING FACTOR ATTRIBUTES APPLICABLE TO CFM**

This section will assess the PIF and its attribute applicable for each CFM based on the context and boundary condition. SPAR-H and IDHEAS-ECA PIFs correlation table, from the reference [20], will also be used to support this analysis, with the aim of uphold consistency between HEP quantifications using these methods.

**CFM1** – Failure of detection →  $P_{CFM1} = 1.12E-03$

- Scenario familiarity: SF1 – Unpredictable dynamics in known scenarios, shifting task objectives →  $6.6E-04$ 
  - Justification: Operators are trained twice a year in this scenario, and they are well-trained to detect cues related to SGTR, however, this event is outside of the main course of SGTR and operator should have pay attention on this unpredictable dynamic. The occurrence of failure of the SGs' feedwater pumps resulting in the LAA level rising is unpredictable during the scenario.
- Information availability and reliability: this PIF does not apply to this CFM.
  - Justification: Table B-2 in IDHEAS-ECA document [\[21\]](#).
- Task complexity: No impact (C0).

- Justification: The detection of the LAA tank high level alarm is not complex, and the operator is familiarized with the alarm screen.
- Environmental PIF: ENV7 - Loud or burst noise → 1.7
  - Justification: During SGTR multiple instruments from radiation detection and annunciator alarm unexpectedly at the same time.

**CFM 2** – Failure of understanding →  $P_{CFM2} = 1.30E-03$

- Scenario familiarity: No impact (SF0).
  - Justification: Once the LAA tank high level alarm pop up in the alarm screen, the operator is well-trained to understand that he should recognize it and find the possible solution through the alarm procedure (OP-5-LAA).
- Information availability and reliability: No impact (INF0).
  - Justification: The MCR indications are reliable and complete to understand the alarm and what the operator should do in front of this situation.
- Task complexity: No impact (C0).
  - Justification: The alarm procedure is organized in a narrative form which contain the consequence if nothing is done, and the possible solutions, so they can understand the need to open the LAA tank drain valve.
- Environmental PIF: ENV7 - Loud or burst noise → 1.15
  - Justification: During SGTR multiple instruments from radiation detection and annunciator alarm unexpectedly at the same time.
- Mental fatigue, stress, and time pressure: MF8 – Emotional stress → 1.2



- Justification: The operator understands the possibility of radiation release during SGTR. The RCS coolant is leaking to outside of the containment and there is high chance of radiation release to the environment increasing the stress.

**CFM 3** – Failure of decisionmaking →  $P_{CFM3} = 1.00E-03$

- Scenario familiarity: No impact (SF0).
  - Justification: Operators are trained to deploy alarm procedure for an alarm response.
- Information availability and reliability: No impact (INF0).
  - Justification: The MCR indications are reliable and complete to make decisions during SGTR.
- Task complexity: No impact (C0).
  - Justification: The alarm procedures explain to the operator the consequences and all possible solutions to stop the level rising.

**CFM 4** – Failure of action →  $P_{CFM4} = 1.40E-04$

- Scenario familiarity: No impact (SF0).
  - Justification: The operator has vast experience to open and close the valves which connect the LAA tank. These types of actions are done in training and during normal operation to warm up and cooldown the nuclear power plant.
- Information availability and reliability: this PIF does not apply to this CFM.
  - Justification: Table B-2 in IDHEAS-ECA document [\[21\]](#).
- Task Complexity: no impact (C30)

- Justification: Simple execution to check some valves to finally open the drain valve of LAA tank.
- Procedures, guidance, and instructions: PG1 – Procedure guidance is less than adequate → 1.2
  - Justification: The alarm procedure is structured in a narrative form and does not have placeholders to check the execution of each solution for the alarm.
- Mental fatigue, stress, and time pressure: MF8 – Emotional stress → 1.2
  - Justification: If operators do not take appropriate measures, this could lead to the loss of cooling of the RCS by the secondary in a closed cycle, resulting in the loss of one option to cooldown the RCS and the operator is obligate to cooldown by open cycle which implicate in the critical safety function SG feedwater source.

**CFM 5** – Failure of interteam coordination → As stated in step 3.2, this CFM is not applicable to this critical task.

### **7.3.5 STEP 5: ESTIMATION OF $P_c$ – THE SUM OF HEP OF CFM**

The estimation of  $P_c$  for the HFE3 is obtained using the IDHEAS-ECA and it is shown in Figure 18.

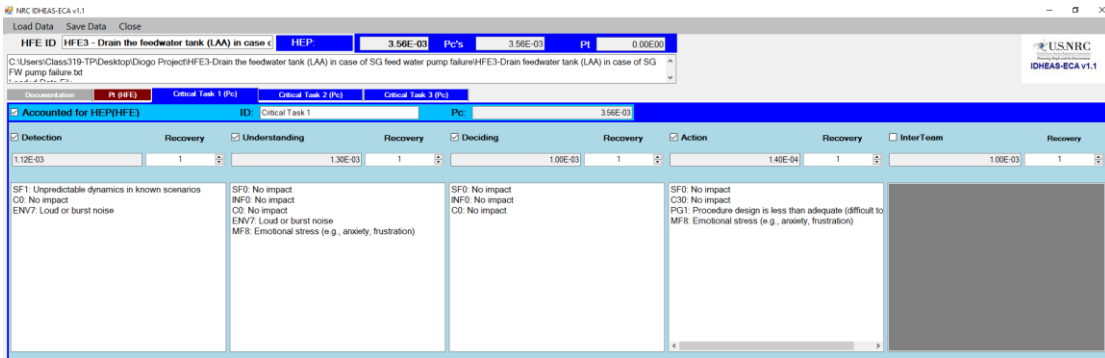


Figure 19 -  $P_c$  estimation for HFE3

### 7.3.6 STEP 6: ESTIMATION OF $P_t$ – THE CONVOLUTION OF THE DISTRIBUTION OF $T_{AVAIL}$ AND $T_{REQ}$

The estimation of  $P_t$  for the HFE3 is obtained using the IDHEAS-ECA and it is shown in Figure 19.

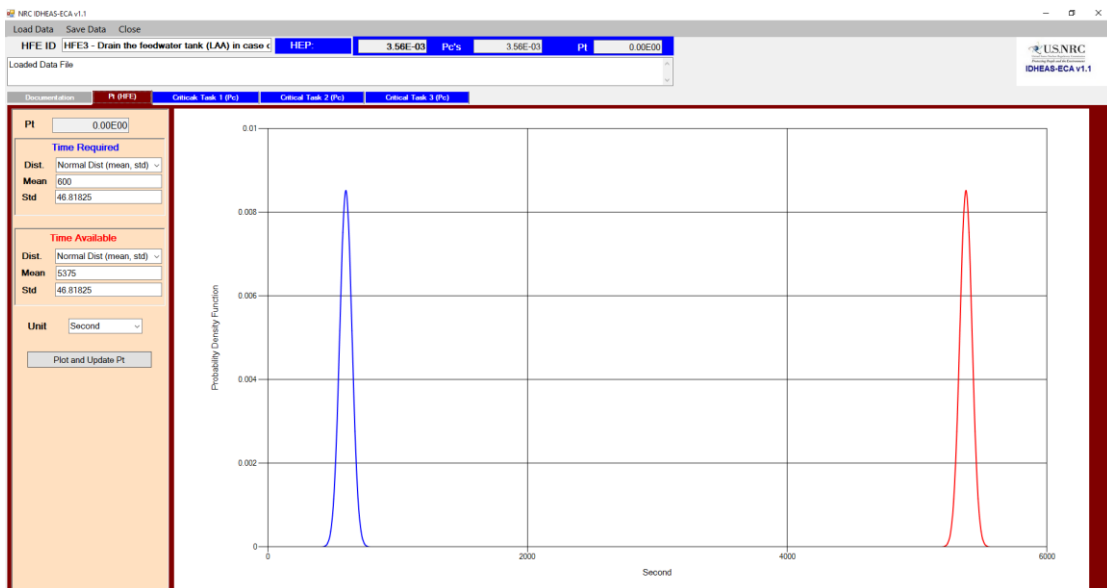


Figure 20 –  $P_t$  estimation for HFE3

### 7.3.7 STEP 7: CALCULATE THE OVERALL HEP

The summary of the HEP calculation is illustrated in Table 27.

**Table 27 - Summary of HEP Quantification for HFE3**

<b>CFM</b>	<b>PIF<sub>Attribute</sub></b>	<b><math>P_{CFM_{Base}}</math></b>	<b><math>w_i</math></b>	<b><math>P_{CFM}</math></b>
<b>Detection</b>	SF1: unpredict dynamic in known scenario C0: no impact ENV7: Loud or burst noise	$1 \times 10^{-4}$	$6.6 \times 10^{-4}$ 1.7	$1.12 \times 10^{-3}$
<b>Understanding</b>	SF0: no impact INF0: no impact C0: no impact ENV7: Loud or burst noise MF8: Emotional stress	$1 \times 10^{-3}$	1.15 1.2	$1.30 \times 10^{-3}$
<b>Decisionmaking</b>	SF0: no impact INF0: no impact C0: no impact	$1 \times 10^{-3}$	N/A	$1 \times 10^{-3}$
<b>Action</b>	SF0: no impact C30: no impact PG1: Procedure design is less than adequate MF8: Emotional stress	$1 \times 10^{-4}$	1.2 1.2	$1.40 \times 10^{-4}$
<b>TOTAL P<sub>CT1</sub></b>				$3.56 \times 10^{-3}$
<b>P<sub>t</sub></b>				0.00
<b>HEP<sub>IDHEAS-ECA</sub></b>				$3.56 \times 10^{-3}$

**7.3.8 STEP 8 – DEPENDENCY ANALYSIS**

Dependence analysis will be on applied for HFE1 and HFE2.

## **7.4 HFE4: REPLENISH EMERGENCY FEEDWATER TANKS FOR RCS LONG TERM COOLING**

### **7.4.1 STEP 1: SCENARIO ANALYSIS**

#### **7.4.1.1 Step 1.1: Develop scenario narrative**

For HFE4, it assumed the same scenario narrative as described in section 7.1.1.1 for HFE1, however, it is made necessary to add an extra detailed and specific description as follow.

After HFE3 failure leading to the loss of RCS cooling through the closed cycle, reactor cooling will be done through the unaffected SGs at open cycle via relief valves (ADVs) and the emergency feedwater system (LAR). Following the failure of startup and shutdown pumps (LAJ) and feedwater pumps (LAC), the level of GVs drops until it reaches 5 meters, at which point a startup signal is generated for the Emergency Feedwater System (LAS) pumps. Shortly after the initiation of LAS pump operation, alarms LAR10/20/30/40EG001ZV01 are triggered (content of the Demineralized Water Pool (LAR) < 360 m<sup>3</sup>, Low Level 1 < 7.85 meters). In response to these alarms, operators follow the alarm procedure (OP-5-LAR: Emergency Feedwater System "LAR"). In the sections related to alarms LAR10/20/30/40EG001ZV01, OP-5-LAR instructs operators to execute the safety function recovery guidance (FRG) OP-3-2.2.4 (Core Cooling/Steam Generator Feed), section 4.2.2, item 2.3 to "Restore demineralized water." During the execution of item 2.3 of the FRG, the operator must perform demineralized water supply system (GHC) system procedure and some valve maneuvers will be carried out in the field with the support of the field operator.

#### **7.4.1.2 Step 1.2: Identify Human Failure Event (HFE)**

HFE4: Replenish emergency feedwater tanks for RCS long term cooling. This HFE comprise all the actions taken by the operators in the MCR to detect the alarm, deploy alarm procedure (OP-5-LAR), understanding what is happening and the possible solutions, and finally execute the action to connect the LARs pools and make up demineralized from demineralized water supply system (GHC).

#### **7.4.1.3 Step 1.3: Identify the scenario/Event Context**

- **Environment and situation:** It is assumed the same context stated in section 7.1.1.3, however, additional information is made necessary as follow. It is assumed perfect condition for the field operator in the emergency feedwater building (ULB) to maneuver the valves which connects the LARs pools.
- **System:** It is assumed the same context stated in section 7.1.1.3.
- **Personnel:** It is assumed the same context stated in section 7.1.1.3, and additionally to that, the field operator are requested to connect the LARs pools in the ULB building.
- **Task:** It is assumed the same context stated in section 7.1.1.3, however, an extra description for scenario/event context is required as follows. During RCS cooldown at 50K/h at closed cycle, if operator fail to recognize the rise of LAA high level alarm, it will result in the loss of closed cycle resulting in the cooling of RCS by open cycle through ADVs and emergency feedwater system (LAR). After the initiation of SGs feed by LAS pumps, the low level alarm ( $L_{LAR} < 7,85m$ ) will pop up in the alarm screen alerting

the operator to deploy the alarm procedure (OP-5-LAR). Promptly, the operator should understand what is happening, what are the consequences, and execute the actions. In the alarm procedure, the operator will be instructed to execute the related FRG (OP-3.2.2.4) to replenish the LARs pool tanks with demineralized water for long term cooling. During the execution of this procedure, the operator must perform other support system procedures to put into operation, and field operator should open the connection valve to finish necessary actions to reestablish the minimum level required for the LAR pool tanks for long term cooling. All the tasks executed in the field are supervised in the MCR through the panels, therefore, any change in the valve position is recognized and checked in the MCR.

## **7.4.2 STEP 2: ANALYZING HUMAN FAILURE EVENTS (HFE)**

### **7.4.2.1 Step 2.1: Defining the Human Failure Events (HFE)**

This section defines the HFE and describes the scope of the analysis:

- Success Criteria: Put into operation 1 of 2 demineralized water supply systems (GHC) and open 2 of 4 LAR pool tanks connection valves.
- Consequence: If operators fail to replenish the LAR pool tanks, it is considered the failure of the LAS pumps and consequently the failure to cooldown the RCS by the unaffected SGs in open cycle.
- Beginning and ending points: The HFE begins when the level of LAR pool tanks < 7.85m and the alarm (LAR10/20/30/40EG001ZV01) is alerted on the alarm screen. The operator will identify the alarm which directs him to execute the related alarm procedure (OP-5-LAR). The operator will

understand that the LAR pool tank achieved the low level and if nothing is done the LAS pump will be turned off causing the loss of the RCS cooling by open cycle. Then the operator should put one GHC train in operation and open 2 connections valve replenish the LAR pool tanks level.

- Relevant procedure guidance: Alarm procedure (OP-5-LAR); FRG procedure (OP-3-2.2.4, section 4.2.2, item 2.3); GHC system procedure (OP-4-8.1); and emergency procedure (OP-3-3.5, section 5.2, step 2).

NOTE: The specification for this analysis were adopted from constant values for time based on Angra-2 FSAR and current PSA under development. In future studies, the timing could be deduced based on experimental models from Angra-2 simulator.

- Cues and indications for initiating the operator action and timing:  $T_{\text{delay}}$  is based on the time between the beginning of the event and the identification of the cue, where the operator action was started through procedure guidance. The cues which the operator will start their action is the low level alarm (LAR10/20/30/40EG001ZV01). For diagnose the event, the cues are low level 1 in the LAR pool tank  $< 7.85\text{m}$  and rising. Based on the literature, it is assumed that an operator during accident mitigation takes around 25s to acknowledge an alarm [19], therefore, the cognition phase will start with a delay time of  $T_{\text{delay}} = 25\text{s}$ .
- Available time to perform the operator action: The system time window ( $T_{\text{sw}}$ ) is estimated based on time take by the LAR pool tank to be empty after the start of the LAS pump. Based on Angra-2 PSA, the  $T_{\text{sw}} = 11972\text{s}$ . In this way, the time available ( $T_{\text{avail}}$ ) is  $T_{\text{sw}} - T_{\text{delay}}$  resulting in  $T_{\text{avail}} = 11947\text{s}$ .



- Time required to perform the operation action: Based on Angra-2 PSA, it is considered 5 minutes for cognition time ( $T_{\text{cog}} = 300\text{s}$ ) and 40 minutes to execute all the actions ( $T_{\text{exe}} = 2400\text{s}$ ) to connect the LAR pool tanks and to replenish them with GHC system [3]. The time required ( $T_{\text{req}}$ ) is the time spent by the operator to perform the cognitive and execution part following the procedure, therefore,  $T_{\text{req}} = 2700\text{s}$ . All the timing is summarized in the timeline diagram shown in Figure 13.

#### **7.4.2.2 Step 2.2: Task Analysis and Identification of Critical Tasks**

To keep it simple, one crucial task is defined, which involves the recognizing of low level in LAR pool tank and deploy the alarm procedure (OP-5-LAR) to recover the LAR level. Additionally, the HFE is assumed as one critical task because the same context is applicable from the start to the end of the HFE process.

### **7.4.3 STEP 3: MODELING FAILURE OF CRITICAL TASKS**

#### **7.4.3.1 Step 3.1: Characterization of Critical Tasks**

This section specifies the relevant conditions that affect the performance of the critical task.

- Critical task goal: identify the low level in any LAR tank, connect the tanks and replenish it by the GHC system to avoid the loss of the LAS pumps and consequently the loss of RCS cooling by SG in open cycle.
- Specific requirements: perceive the low level in any LAR pool tank and deploy the respective alarm procedure to recover the LAR tank through the required actions specified in the procedures.

- Cues and supporting information: LAR low level alarm (LAR10/20/30/40EG001ZV01),  $L_{LAR} < 7.85\text{m}$ .
- Procedure: Alarm Procedure (OP-5-LAA); FRG procedure (OP-3-2.2.4); Emergency procedure (OP-3-3.5); and system procedure (OP-4-8.1).
- Personnel: The team in the MCR are composed by 5 operator which are the Shift supervisor (SS); Shift Foreman (SF); Primary operator (PO); Secondary operator (SO); Auxiliary panel operator (AO); and field operator. The operators in the main control room and field operators are well-trained, and the MCR team perform SGTR training in the simulator twice a year considering this failure.
- Task Support: Procedures specified above and MCR indications.
- Location: Main control room (MCR) and ULB building.
- Cognitive activities: Detection, understanding, action and Interteam coordination.
- Concurrent tasks: assuming that there are no other tasks.
- Interteam coordination considerations: The field operator should execute some valve maneuver under the coordination of the operator in the MCR, and each change of valve position made by the field operator could be checked and verified in the MCR.

#### **7.4.3.2 Step 3.2: Identification of Applicable Cognitive Failure Modes (CFM)**

The applicable cognitive failure mode (CFM) is identified by assessing the cognitive activities of the critical task that are associated with each macrocognitive function.

- Detection: detect cues and acquire information.
  - Operators need to detect the alarm through the alarm screen.
  - CFM1 – failure of detection applies to the critical task.
- Understanding: diagnose problems, maintain situational awareness.
  - Operators need to be aware that the alarm is related to the low level of LAR pool tank, and he should deploy the alarm procedure to deal with it.
  - CFM2–failure of understanding applies to the critical task.
- Decisionmaking: make a go/no-go decision for a pre-specified action.
  - The operator should understand the consequences of the alarm and he needs to decide to execute the proper action to avoid the consequences applicable to the alarm.
  - CFM3: failure of decisionmaking applies to the critical task.
- Action Execution: execute cognitively simple actions.
  - The operator should execute alarm procedure, function procedure and system procedures in series and execute straightforward actions to accomplish the task. The actions performed are relatively simple actions because operators are trained to, however, the number of

valves and procedures to handle is high and there are other variables to monitoring during accident mitigation.

- CFM4: failure of action execution applies to the critical task.
- Interteam coordination: Communication and coordination.
  - The critical task requires coordination, by the MCR, to verify, modify and control the actions that must be performed by the field operator to connects the LAR pool tanks.
  - CFM5: failure of Interteam coordination applies to the critical task.

#### **7.4.4 STEP 4: ASSESSING PERFORMANCE INFLUENCING FACTOR ATTRIBUTES APPLICABLE TO CFM**

This section will access the PIF and its attribute applicable for each CFM based on the context and boundary condition. SPAR-H and IDHEAS-ECA PIFs correlation table, from the reference [\[20\]](#), will also be used to support this analysis, with the aim of uphold consistency between HEP quantifications using these methods.

**CFM 1** – Failure of detection →  $P_{CFM1} = 1.70E-04$

- Scenario familiarity: No impact (SF0)
  - Justification: Operators are trained twice a year in this scenario, and they are well-trained to detect the alarm from LAR pool tanks and the necessity to replenish those tanks for long term cooling.
- Information availability and reliability: this PIF does not apply to this CFM.
  - Justification: Table B-2 in IDHEAS-ECA document [\[21\]](#).
- Task complexity: No impact (C0).
  - Justification: Detecting the LAR pool tank low level alarm is not complex, because it is very straightforward and obvious. Each LAR

pool tank will emit an alarm on the alarm screen, resulting in at least 3 low level alarms, and if the operator does not perceive an alarm, he may recover through the other alarms.

- Environmental PIF: ENV7 - Loud or burst noise → 1.7
  - Justification: During SGTR multiple instruments from radiation detection and annunciator alarm unexpectedly at the same time.

**CFM2** – Failure of understanding →  $P_{CFM2} = 1.30E-03$

- Scenario familiarity: No impact (SF0).
  - Justification: Once the LAR pool tank low level alarm pop up in the alarm screen, the operator is well-trained to understand that he should recognize it and find the possible solution through the alarm procedure (OP-5-LAR).
- Information availability and reliability: No impact (INF0).
  - Justification: The MCR indications are reliable and complete to understand the alarm and what the operator should do in front of this situation.
- Task complexity: No impact (C0).
  - Justification: The alarm procedure is organized in a narrative form which contain the consequence, if nothing is done, and the possible solutions, so they can understand the necessary actions to be implemented.
- Environmental PIF: ENV7 - Loud or burst noise → 1.15
  - Justification: During SGTR multiple instruments from radiation detection and annunciator alarm unexpectedly at the same time.

- Mental fatigue, stress, and time pressure: MF8 – Emotional stress → 1.2
  - Justification: The operator understands the possibility of radiation release during SGTR. The RCS coolant are leaking to outside of the containment to the ruptured SG and there is high chance of radiation release to the environment increasing the stress.

**CFM 3** – Failure of decisionmaking →  $P_{CFM3} = 1.00E-03$

- Scenario familiarity: No impact (SF0).
  - Justification: Operators are trained to deploy alarm procedure for an alarm response.
- Information availability and reliability: No impact (INF0).
  - Justification: The MCR indications are reliable and complete to make decisions during SGTR.
- Task complexity: No impact (C0).
  - Justification: The alarm procedures explain to the operator the consequences and instruction to deploy the proper FRG and subsequent system procedure.

**CFM 4** – Failure of action →  $P_{CFM4} = 1.40E-03$

- Scenario familiarity: No impact (SF0).
  - Justification: The operator has vast experience to replenish LAR pool tanks. These actions are performed more than twice a year during training sessions because this task is done in another accidents training session.
- Information availability and reliability: this PIF does not apply to this CFM.
  - Justification: Table B-2 in IDHEAS-ECA document [\[21\]](#).

- Task Complexity: C31 – Straightforward procedure execution with many steps → 1E-03
  - Justification: Operator should execute many steps to accomplish this task guided by the FRG procedure.
- Procedures, guidance, and instructions: PG1 – Procedure guidance is less than adequate → 1.2
  - Justification: The alarm procedure is structured in a narrative form and does not have placeholders to check the execution of each solution for the alarm.
- Mental fatigue, stress, and time pressure: MF8 – Emotional stress → 1.2
  - Justification: The operator understand that he should maintain the critical safety function of SG feedwater source. If no action is taken will lead the system to core damage.

**CFM 5** – Failure of interteam coordination →  $P_{CFM5} = 1.00E-03$

- Scenario familiarity: No impact (SF0).
  - Justification: The operator in the field and MCR has vast experience to connect the LAR pool tanks. These actions are straight forward and simple to execute.
- Information availability and reliability: this PIF does not apply to this CFM.
  - Justification: Table B-2 in IDHEAS-ECA document [\[21\]](#).
- Task Complexity: No impact (C40)
  - Justification: The MCR and field operator have clear, streamlined, and crew-liked communication and coordination.

### 7.4.5 STEP 5: ESTIMATION OF $P_c$ – THE SUM OF HEP OF CFM

The estimation of  $P_c$  for the HFE4 is obtained using the IDHEAS-ECA and it is shown in Figure 20.

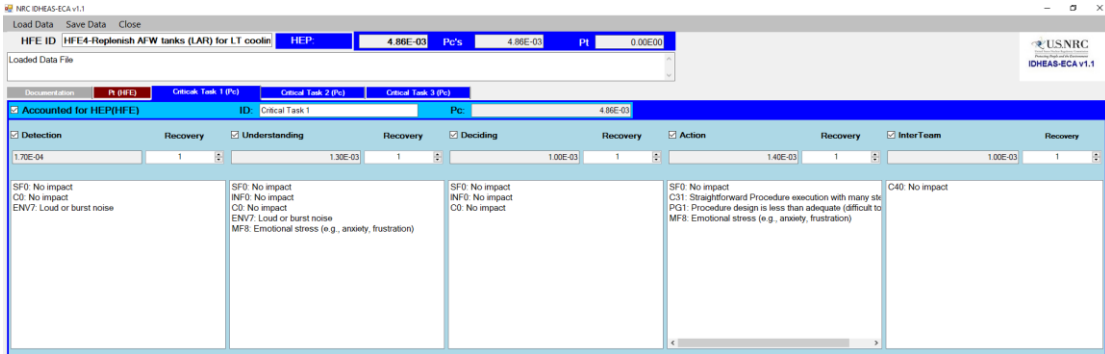


Figure 21 -  $P_c$  estimation for HFE4

### 7.4.6 STEP 6: ESTIMATION OF $P_t$ – THE CONVOLUTION OF THE DISTRIBUTION OF $T_{AVAIL}$ AND $T_{REQ}$

The estimation of  $P_t$  for the HFE4 is obtained using the IDHEAS-ECA and it is shown in Figure 21.

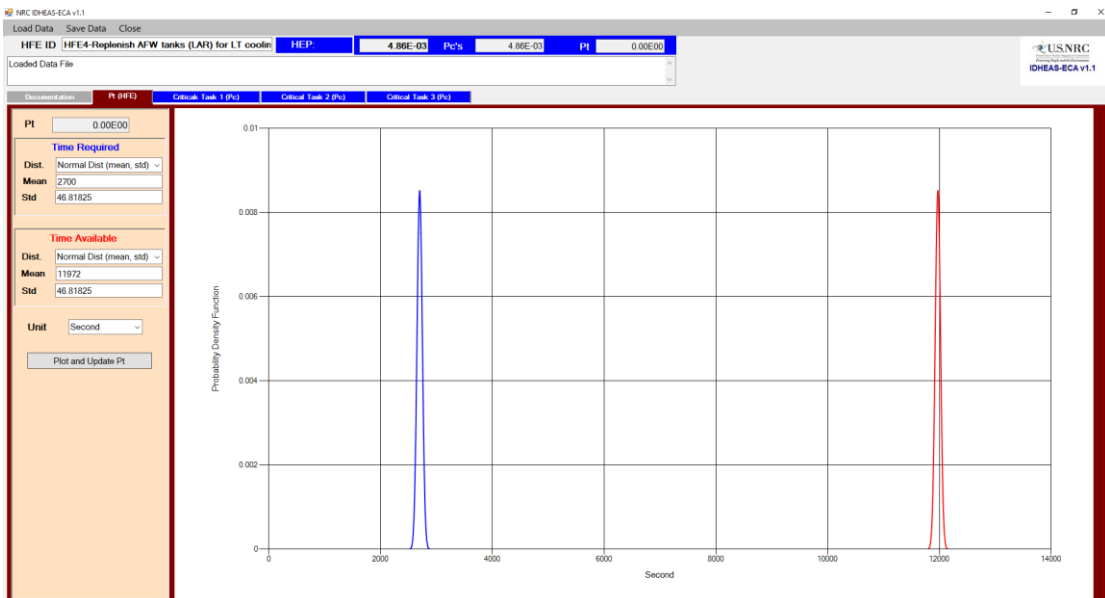


Figure 22 -  $P_t$  estimation for HFE4



#### 7.4.7 STEP 7: CALCULATE THE OVERALL HEP

The summary of the HEP calculation is illustrated in Table 28.

**Table 28 - Summary of HEP Quantification for HFE4**

<b>CFM</b>	<b>PIF<sub>Attribute</sub></b>	<b><math>P_{CFM_{Base}}</math></b>	<b><math>w_i</math></b>	<b><math>P_{CFM}</math></b>
<b>Detection</b>	SF0: no impact C0: no impact ENV7: Loud or burst noise	$1 \times 10^{-4}$	1.7	$1.7 \times 10^{-4}$
<b>Understanding</b>	SF0: no impact INF0: no impact C0: no impact ENV7: Loud or burst noise MF8: Emotional stress	$1 \times 10^{-3}$	1.15 1.2	$1.30 \times 10^{-3}$
<b>Decisionmaking</b>	SF0: no impact INF0: no impact C0: no impact	$1 \times 10^{-3}$	N/A	$1 \times 10^{-3}$
<b>Action</b>	SF0: no impact C31: Straightforward procedure execution with many steps PG1: Procedure design is less than adequate MF8: Emotional stress	$1 \times 10^{-4}$	$1.0 \times 10^{-3}$ 1.2 1.2	$1.40 \times 10^{-3}$
<b>Interteam Cordination</b>	C40: no impact	$1 \times 10^{-3}$	N/A	$1 \times 10^{-3}$
<b>TOTAL P<sub>CT1</sub></b>				$4.86 \times 10^{-3}$
<b>P<sub>t</sub></b>				0.00
<b>HEP<sub>IDHEAS-ECA</sub></b>				$4.86 \times 10^{-3}$

#### **7.4.8 STEP 8 – DEPENDENCY ANALYSIS**

Dependence analysis will be only applied for HFE1 and HFE2.

## 8 RESULTS AND DISCUSSION

The results presented in Table 29 indicate a slight variation among the methods employed to quantify HEP of the Identified HFEs in this study. This observation suggests that, despite innovations in the structure of PIF and the cognitive model of humans, IDHEAS-ECA yields consistent results when compared to SPAR-H, CBDTM, HCR/ORE and THERP. These findings affirm that IDHEAS-ECA is suitable for determining HEP for internal events, aligning with the assertions made in reference [15].

In Table 29, the HFE1 considered higher dependency recovery factor to compensate the lack of information related to the base timeline for the cognition part. In Angra-2, HFE2 considered  $P_{\text{cog}}$  and  $P_{\text{exe}}$  for HEP quantification, however, further evaluation revealed that only execution part should be considered when utilizing SPAR-H and IDHEAS-ECA. As such, the HEP result for the  $P_{\text{exe}}$  in the HFE2 is approximately the same value in all methods. A discrepancy was identified in the results for HFE3 and HFE4 through the qualitative analysis carried out by IDHEAS-ECA. Considering the contextual characteristics of HFE3 and HFE4, it can be asserted that HFE4 is more complex, demanding more from the operator and involving activities outside the reactor control room. On the other hand, HFE3 only requires the opening of a drain valve within the reactor control room. Consequently, SPAR-H and IDHEAS-ECA align with this assertion, while results obtained through CBDTM, HCR/ORE, and THERP introduce a comparative inconsistency among their outcomes.

In summary, IDHEAS-ECA produces higher values due to the excess of PIF attributes applied for each CFM considered for the HFE. The lack of knowledge of the

psychological science related to CFM and the lack of information about Angra-2 crew behavior are the possible reasons. CBDTM+HCR/ORE+THERP has the highest values probably because Angra-2 analysts considered higher dependency levels when there is not much information for the base timeline or due to the over conservatism assumed. Finally, SPAR-H shows to have the lowest values even though it is a method that generally brings higher values due to its characteristic of having more generalized weights of its PIFs. In other words, the HEP results obtained using the CBDTM, HCR/ORE, and THERP methods, when compared to SPAR-H and IDHEAS-ECA, exhibit a more conservative nature when the base timeline used bring more favorable PIF levels, in accordance with J. Park's statement [22].

**Table 29 – Total HEP result for each HFE**

<b>HFE#</b>	<b>Angra-2</b>	<b>SPAR-H</b>	<b>IDHEAS-ECA</b>
<b>HFE1</b>	5.8E-03	2.16E-03	2.67E-03
<b>HFE2</b>	9.4E-04	1.00E-04	4.08E-04
<b>HFE3</b>	8.1E-03	2.32E-03	3.56E-03
<b>HFE4</b>	6.4E-03	5.32E-03	4.86E-03

IDHEAS-ECA was developed with the intention of integrating the strengths of HRA methods considered standard, particularly to enhance the areas of expanding the method's scope of application, providing a more detailed scientific foundation for understanding human cognitive mechanisms in the face of human error, and reducing the variability of obtained results. However, due to its more elaborate and complex structure, it is evident that this method reinforces certain aspects while also demonstrating a noticeable increase in the complexity of applying it for HRA analysis.

To achieve a broader scope of application, IDHEAS-ECA was designed with an extensive list of PIFs and their attributes, ensuring a much wider applicability

compared to existing standard methods. This broad spectrum of PIFs enables analysts to apply this method to events within the reactor control room or external events, including those involving new technologies applied in more advanced reactors (digital control rooms, Small Modular Reactors, etc).

Moreover, qualitatively, IDHEAS-ECA brings a much more detailed description of each HFE. For instance, in calculating the HEP for HFE3 and HFE4, it was possible to qualitatively characterize the Angra-2 alarm procedure by assigning the attribute "PG1: Procedure design is less than adequate." This attribute considers the lack of space for marking the executed action, a nuance that could not be captured with SPAR-H due to its broad definition of PIFs. However, this broad capability of PIFs, combined with the five CFM, significantly increases the potential combinations that can be assigned between applicable CFMs and PIF attributes, resulting in an increased variability.

Furthermore, a challenge encountered in this work was identifying which PIF attribute should or should not be applied to a CFM, requiring the analyst to possess a deeper understanding of the psychological aspects of human behavior. For example, assumptions were made that attributes like "ENV7: Loud or burst noise" and "MF8: Emotional stress" would affect CFM detection, understanding, and action. These assumptions were based on personal understanding and may not necessarily align with the views of other analysts. My recommendation is to collaborate with psychologists and conduct interviews with operators to ascertain which PIF attributes truly affect CFMs, thereby minimizing the negative impact of increased result variability. A contributing factor to reducing variability is the well-defined structure of the proposed analysis. Through this structure, peer reviews of each HFE analysis become

straightforward, aiming to identify any non-conformities with the adopted standards in the analysis of each HFE.

SPAR-H and IDHEAS-DEP are two methods used for HRA that differ in their dependency analysis methods with respect to the degree of detail of how the context is modified for HFE2 if HFE1 fails. Both of them take into consideration the change of context for HFE2 in the case of HFE1 failure and it means that both methods analyze dependency in the HFE level and not at the subtask level like THERP, however, they differ in the structure to analyze the change in the context between HFEs. SPAR-H define the context through their four factors which are time, location, same person or crew, and cues. Each factor is determined based on the context description and the analyst just pinpoint if the factor affect or not the HFE2 considering the failure of the HFE1. However, IDHEAS-DEP divides the analysis into five factors which are function or system, temporal proximity, personnel, location, and procedure. Each of these factors is analyzed according to cognitive, consequential and resource sharing contextual dependence, creating an additional layer of analysis. Furthermore, each contextual dependency analyzed is divided into three levels high, medium, and low that will be considered in the calculation of the final HEP. Therefore, the dependency analysis proposed by IDHEAS-DEP has a much higher degree of detail than SPAR-H, allowing the analyst to specifically determine each weight that will be applied in the composition of the HEP dependency, while SPAR-H has a simpler analysis that basically consists of yes or no bringing in a more conservative HEP dependency results compared to IDHEAS-DEP as shown in Table 30. Additionally, It was observed that the variability of HEP dependency obtained by IDHEAS-DEP increases due to a more detailed analysis structure.

**Table 30 – Dependency HEP results**

<b>HFE#</b>	<b>SPAR-H</b>	<b>IDHEAS-DEP</b>
<b>P(HFE2 HFE1)</b>	5.0005E-01	9.38E-03

During the conduct of this HRA, several recommendations for improvements were identified for the new design of the Brazilian microreactor.

In the development of the baseline timeline for HFE1, the time required for the cognitive part ( $T_{cog}$ ) takes into account the operator's execution of the SPTA (OP-3-1.1), CSF (OP-3-1.2), DA (OP-3-1.3), and the EOP (OP-3-3.5) procedures. The operator is guided by the flowchart during the execution of these procedures, and he is allowed to return from DA to SPTA in case of being unable to identify the event. In a hypothetical situation where the operator cannot identify the event and no critical safety function is compromised, the operator could potentially find themselves in a vicious cycle without defining actions until either a critical safety function is compromised, or the event is identified. This hypothetically prolonged  $T_{cog}$  could significantly affect the operator's failure probability in terms of response time and the elevated stress of not being able to define actions based on the procedure. Therefore, it is recommended that the procedure follows a unidirectional flow, and in the event of non-identification of the event through DA, the operator should proceed to execute safety functions. If none of these functions is compromised, the operator should shut down the plant according to a specific procedure. This ensures that the flowchart is executed unidirectionally until the plant shutdown procedure is completed, whether through an emergency procedure or a critical safety function.

In addition to the baseline timeline, it was identified that in the Angra-2 procedures, the thermo-hydraulic explanations are incorporated within the same

procedure. Assuming that the operator will read the narrative explanation of the event before executing the steps would impact both the cognitive time ( $T_{\text{cog}}$ ) and the executive time ( $T_{\text{exe}}$ ) of any HFE. For the purposes of this analysis, it was not considered that the operator reads the thermo-hydraulic explanation at the beginning of each procedure. Therefore, it is recommended that each procedure be divided into two separate parts, where one should contain only the steps to be executed by the operator to mitigate the accident, and the other should include the thermo-hydraulic explanations. These explanations can be consulted at an opportune moment to aid in understanding the current condition of the plant.

The alarm procedures lack a structure for operators to mark the execution of each proposed action to resolve the alarm in question. Therefore, it is recommended that alarm procedures in narrative form be restructured to allow operators to mark the actions that have been executed, thereby reducing the probability of any omission errors.

By comparing the OP of Angra-2 and APR-1400, it was observed that the APR-1400 model incorporates a process in the procedure for checking CSF that includes five designated spaces for markings—one for each operator. Given the significance of this aspect, it is logical for the verification process to engage all five operators. This is facilitated by the digital OP in APR-1400, allowing all operators in the main control room to simultaneously monitor and confirm actions during accident mitigation. Consequently, it is recommended to implement the digital OP in the procedures of the Brazilian microreactor.

Lastly, in the event tree developed for this project, the cooling at 100K/h is not envisaged in the case of a failure of the Safety Injection System (SIS) for cooling the Reactor Coolant System (RCS) until the condition allows the connection of the residual



heat removal system. However, it is recommended to consider this action to reduce the probability of failure in this event sequence. Therefore, it is recommended to consider cooling at 100K/h in the event of SIS failure to reduce the probability of core damage in this branch of the event tree.

## 9 CONCLUSION

In conclusion, this study shows that IDHEAS-ECA are adequate in determining the HEP like standard HRA methods, however, IDHEAS-ECA have a very complex structure to connect the PIF and its attributes for each CFM making it more complex to use by analyst increasing variability. A good point to compensate this problem is the framework to develop the analysis which make it easy for peer review allowing any inconsistency that can increase the variability of results to be identified. Therefore, IDHEAS-ECA demands from the analyst a better understanding of the cognitive behavior from the Angra-2 crew and the psychological science to connect the PIF attribute with each CFM and it is made necessary more development to enhance IDHEAS-ECA guidance to connect PIFs attributes with each CFM applicable for the HFE to decrease variability of HEP results.

HEP dependency analysis via SPAR-H and IDHEAS-DEP produced completely different results. The very small result of dependency HEP from IDHEAS-DEP could lead to an undervaluation of the NPP risk. However, IDHEAS-DEP brings more traceability for the results and rely on a more detailed analysis enhancing dependency HEP reliability. This big gap in the HEP dependency values is because SPAR-H oversimplifies and deals more broadly with the details that connect the dependency between a pair of HFE, while IDHEAS-ECA breaks down each detail more specifically were the analyst can analyze and apply each specific point. This clearly results in an inconsistency of results between the two methods requiring further development for dependency analysis.

Finally, the recommendations to enhance OP are to implement digital OP to allow all operators in the main control room to confirm and validate important human actions; the OP should be structured in an unidirectional path to reduce any possibility of indecision in the actions to be taken to mitigate the accident; the alarm procedure should be treated as a step-by-step guide with space reserved to verify the action execution; and the thermo-hydraulic analysis should be separated from the operator's actions in each procedure for quick execution to reduce any impact in the timeline considered for each HFE.