DISS. ETH NO. 19321

# DISCRETE DYNAMIC EVENT TREE MODELING AND ANALYSIS OF NUCLEAR POWER PLANT CREWS FOR SAFETY ASSESSMENT

A dissertation submitted to

ETH ZURICH

for the degree of

Doctor of Sciences

presented by

DAVIDE MERCURIO

Laurea di Dottore in Ingegneria Nucleare, Polytechnic of Milan

Date of birth, $18^{th}$ February 1980

citizen of Italy

accepted on the recommendation of

Prof. Dr. Wolfgang Kröger, examiner

Prof. Dr. Michael Horst-Prasser, co-examiner

Dr. Vinh N. Dang, co-examiner

2011

*"C'est le temps que tu as perdu pour ta rose qui fait ta rose si importante"*

Le Petit Prince, Antoine de Saint-Exupéry

*To Stefania and to my parents*

# Abstract

Current Probabilistic Risk Assessment (PRA) and Human Reliability Analysis (HRA) methodologies model the evolution of accident sequences in Nuclear Power Plants (NPPs) mainly based on Logic Trees. The evolution of these sequences is a result of the interactions between the crew and plant; in current PRA methodologies, simplified models of these complex interactions are used.

In this study, the Accident Dynamic Simulator (ADS), a modeling framework based on the Discrete Dynamic Event Tree (DDET), has been used for the simulation of crew-plant interactions during potential accident scenarios in NPPs. In addition, an operator/crew model has been developed to treat the response of the crew to the plant. The "crew model" is made up of three operators whose behavior is guided by a set of rules-of-behavior (which represents the knowledge and training of the operators) coupled with written and mental procedures. In addition, an approach for addressing the crew timing variability in DDETs has been developed and implemented based on a set of HRA data from a simulator study. Finally, grouping techniques were developed and applied to the analysis of the scenarios generated by the crew-plant simulation. These techniques support the post-simulation analysis by grouping similar accident sequences, identifying the key contributing events, and quantifying the conditional probability of the groups. These techniques are used to characterize the context of the crew actions in order to obtain insights for HRA.

The model has been applied for the analysis of a Small Loss Of Coolant Accident (SLOCA) event for a Pressurized Water Reactor (PWR). The simulation results support

an improved characterization of the performance conditions or context of operator actions, which can be used in an HRA, in the analysis of the reliability of the actions. By providing information on the evolution of system indications, dynamic of cues, crew timing in performing procedure steps, situation assessment, and crew challenge, these results are useful and relevant for the analysis of the crew's diagnosis/decision-making and, more generally, of operator cognitive tasks. A comparison of the operator-plant simulation results based on the DDETs with classical PRA/HRA analyses of selected actions found significant differences in the available time for operator actions, dynamic response of the system, and necessary cooldown time. In addition, using grouping techniques, failure and close to failure scenarios have been identified, analyzed, and an assessment of the PSFs has done to support the calculation of the Human Error Probabilities (HEPs).

# Abstract in Italian

I modelli di valutazione probabilstica del rischio (Probabilistic Risk Assessment, PRA) e di analisi di affidabilità umana (Human Reliability Analysis, HRA) in impianti nucelari, modellano l'evoluzione degli scenari incidentali trimite alberi di guasto (Fault Trees) e alberi di eventi (Event Trees). Sebbene la struttura dei PRA è sufficientemente adeguata per modellare questi scenari incidentali, non sempre le interazioni tra operatori e impianto e soprattutto l'effetto dell'impianto sulle ripsoste degli operatori sono inclusi (per esempio risposta ad allarmi, stati fisici critci per l'impianto oppure andamento inaspettato dei parametri di processo).

In questo studio, il software ADS (Accident Dynamic Simulator) che è basato su alberi di eventi discreti e dinamici (Discrete Dynamic Event Tree, DDET) è stato utilizzato per la simulazione delle mutue interazioni operatore-impianto nucleare durante scenari incidentali. In particolare, è stato sviluppato un modello di team di operatori d'impianto all'interno del software ADS. Il modello è composto da tre operatori la cui risposta è guidata da un accoppiamento tra una serie di regole di comportamento (che modellano la conoscenza e l'addestramento degli operatori) con le procedure dell'impianto (sia formali che mentali). Inoltre, è stato sviluppato un approccio per la gestione della variabilità delle risposte degli operatori basato sul concetto di "tendenza" il quale è stato ulteriormente confrontato con dati disponibili da studi in simulatori d'impianti nucleari. Infine, la grande quantità di dati prodotti dovuti al numero di scenari e in particolare al numero di eventi durante la loro evoluzione sono stati analizzati sviluppando tecniche di raggruppamento che consentono di ridurre la loro complessità. Cio' è stato fatto identificando la serie

di eventi che portano ad un gruppo comune e caratterizzano la probabilità del singolo gruppo. Questi dati sono stai poi utilizzati per caratterizzare la risposta degli operatori o per ottenere informazioni utili da un punto di vista dell'affidabilità umana attraverso un caso studio. Infine, i rusultati sono stati confrontati con un approccio di analisi di affidabilità unama classico sottolineando le differenze tra i due approcci e il valore aggiunto di un approccio dinamico.

Il modello è stato applicato per l'analisi di uno uno scenario incidentale dovuto ad una piccola perdita di liquido di raffreddamento (Small Loss Of Coolant Accident, SLOCA) in un reattore ad acqua pressurizzata (Pressurized Water Reactor, PWR). I risultati della simulazione hanno fornito una migliore caratterizzazione delle delle situazioni che influenzano le prestazioni sia dell'impianto che degli operatori nella sala di controllo. Questi risultati hanno fornito informazioni sull'evoluzione del sistema di indicazioni, la dinamica dei segnali, i tempi degli operatori nelle esecuzione delle procedure, la valutazione della situazione attuale, e il carico di lavoro degli operatori che sono importanti per il trattamento degli errori che possoni avvenire in impianti nucleari. Alcuni risultati sono stati confrontati con i risultati ottenuti da un classico modello PRA dell'impianto. I risultati ottenuti identificano una serie di differenze nella modellazione delle azioni dell'operatore ed in particolare il tempo disponibile per effettuare le azioni. Inoltre, utilizzando tecniche di raggruppamento sono stati individuati scenari di fallimento del sistema e scenari vicino al fallimento. Essi sono stati analizzati e caratterizzati in termini di probabilità di accadimento. I risultati, sono stati poi utilizzati per il calcolo dei fattori che influenzano le prestazioni degli operatori nella sala di controllo (Performance Shaping Factors, PSFs).

# Acknowledgments

I am so grateful to those people who have made this research possible.

This work would have been impossible without the love and patience of Stefania and my family.

Stefania, to whom this dissertation is dedicated to, has been a constant source of love, concern, support, care, and strength all these years. **Grazie Ste!**

I would like also to express my heartfelt gratitude to my parents Luciana and Gregorio, to whom this dissertation is dedicated to as well, for their understanding and their help even if physically far away.

In addition, a big and sincere thank you to my sisters Sabina and Amela, my brother-in-law Enea, and my fantastic nephew Samuele for their support during the whole PhD period.

I also owe an enormous debt of gratitude to Luca for his encouragement, support, and friendship demonstrated throughout these years and for the long runs we have done together.

This research project has been possible thanks to the support of several people. I would like to acknowledge the aid, technical guidance, feedbacks, and encouragement from the following people:

- **Professor Wolfgang Kröger**. Head of the Laboratory for Safety Analysis (LSA) at the Swiss Federal Institute of Technology Zurich (ETHZ)
- **Dr. Vinh N. Dang**, **Dr. Luca Podofillini**, and **Dr. Stefan Hirschberg**. Energy Systems Analysis (LEA) at the Paul Scherrer Institut (PSI)
- **Professor Enrico Zio**. Polytechnic of Milan
- **Professor Ali Mosleh**. University of Maryland
- **Dr. James Chang** and **Dr. Kevin A. Coyne**. U.S. Nuclear Regulatory Commission
- **Dr. Olivier Zuchuat**. BKW FMB Energie AG

Finally, I want to thank the Eidgenössisches Nuklearsicherheitsinspektorat **ENSI** (Swiss Federal Nuclear Safety Inspectorate) that sponsored this research.

# Contents

# List of Figures

# List of Tables

# Nomenclature

| | |
|---|---|
| ADAPT | Analysis of Accident Progression Tree |
| ADS | Accident Dynamic Simulator |
| CD | Core Damage |
| CDF | Cumulative Distribution Function |
| CVCS | Chemical and Volume Control System |
| DDET | Discrete Dynamic Event Tree |
| DENDROS | Dynamic Event Network Distributed Risk Oriented Scheduler |
| DETAM | Dynamic Event Tree Analysis Method |
| DPD | Discrete Probability Distribution |
| DYLAM | Dynamic Logical Analytical Methodology |
| ECCS | Emergency Core Cooling System |
| EFW | Emergency FeedWater |
| EOP | Emergency Operating Procedure |
| FCM | Fuzzy C-Means |
| HEP | Human Error Probability |
| HFE | Human Failure Event |
| HPI | High Pressure Injection |
| HRA | Human Reliability Analysis |
| IDAC | Information, Decision, and Action in a Crew context |
| IE | Initiating Event |

| | |
|---|---|
| ISA | Integrated Safety Assessment |
| LPI | Low Pressure Injection |
| MC | Monte Carlo |
| MCDET | Monte Carlo Dynamic Event Tree |
| MFW | Main FeedWater |
| MSIV | Main Steam Isolation Valve |
| NPP | Nuclear Power Plant |
| PDF | Probability Density Function |
| PORV | Power Operated Relief Valve |
| PRA | Probabilistic Risk Assessment |
| PSA | Probabilistic Safety Assessment |
| PSF | Performance Shaping Factor |
| PWR | Pressurized Water Reactor |
| RCS | Reactor Coolant System |
| RHR | Residual Heat Removal |
| SAMG | Severe Accident Management Guidance |
| SCM | SubCooling Margin |
| SG | Steam Generator |
| SGTR | Steam Generator Tube Rupture |
| SLOCA | Small Loss Of Coolant Accident |
| SVG | Scalable Vector Graphic |
| TETRA | Transient Response and Test Analyzer |
| USNRC | United States Nuclear Regulatory Commission |
| XML | eXtensible Markup Language |

## Chapter 1

# Introduction

## Contents

## 1.1 Motivation

The safety of complex systems involves close integration between the human operators and the hardware of the system. During accident scenarios in nuclear power plants, control room operators are required to perform a range of tasks to maintain the system in a safe state while bringing it to a stable shutdown condition. Frequently, operators have to manage complicated situations in a brief time frame. The result is that they can take inadequate actions leading the system in undesired conditions.

Current models and techniques to predict human errors rely on quasi-static analyses of the interactions of crew and plant. In such analyses, it is difficult to account for important aspects of the dynamic context such as the timing of the plant indications, the workload associated with the procedures, and the on-going tasks and focus of attention of the operators. Therefore, simulation-based approaches that combine human and system behaviors may support a better understanding of the operator response.

The objective of this study is to model and analyze the crew-plant interactions during accident scenarios in a nuclear power plant for obtaining HRA insights. A basic assumption for the crew model is that the crew response during an accident is a combination of procedure-following and actions supported by the knowledge and training of the operators. Mental procedures and a set of rules-of-behavior represent this knowledge and training. The crew model is implemented in the Accident Dynamic Simulator, i.e., a Discrete Dynamic Event Tree tool used for dynamic Probabilistic Risk Assessment. In this work, a tool and a methodology for the modeling and analysis of the dynamic interactions between control room operators and plant were developed. The dynamic approach can inform the Human Reliability Analysis by simulating jointly the Nuclear Power Plant and the control room crew response.

## 1.2 Background

Classical approaches for accident scenario analyses applied into a Probabilistic Risk Assessment (PRA) or Probabilistic Safety Assessment (PSA) are structured frameworks that analyze the system with respect to the failure and success of components or human actions. With common frameworks such as event tree and fault tree analyses the evaluation of the crew-plant interactions during an accident scenario require simplified models. Nevertheless, these frameworks have proven to be useful and have resulted in the identification of unforeseen plant weaknesses/vulnerabilities and in consequent modifications of the plant, its operations and operating procedures, and the training of the personnel. In spite of this success, the existing, quasi-static[1] PRA frameworks have significant limitations.

First, the variability in the timing of automatic and personnel actions, which may influence the evolution of scenarios and therefore the estimated risk, can only be considered in a restricted manner. Typically, for hardware failure events as well as operator actions, a few values of the time of occurrence of the events in the scenario judged to be conservative are selected and analyzed. However, defining which values are conservative can be problematic due to the dynamic interactions. For example, an early and complete failure of emergency coolant injection could be conservative in thermal-hydraulic terms (yielding a maximum fuel temperature) but easier for the operators to diagnose and therefore to manage than a partially successful injection phase, which would produce initial indications of success that may mask the degraded cooling of the core.

Second, the current PRA framework does not consider comprehensively the context where the operator actions are taken. Human factors and the experience from accident precursors and accidents suggest that decision-making is a dominant contributor to the operator errors. Consequently, the analysis and quantification of operator errors need to consider the operators' situation assessment and its evolution during the accident scenario. This situation assessment introduces so-called cognitive dependencies among operator ac-

[1] In this context quasi-static means that the dynamics are treated as series of snapshots.

tions; in other words, the likelihood of a correct situation assessment and of performing correct actions is influenced by the situation assessment earlier in scenarios. This information on the situation assessment associated with preceding actions is considered but not explicitly included in the accident scenario models of existing PRAs.

In addition, in classical frameworks, a significant preprocessing effort carried out by the analysis of success criteria conditions is required for the analyst to acquire a detailed knowledge of the system and its dynamics. During the scenario progression, three major contributors could in principle affect its evolution and outcome:

- the sequential order of the success and failure events;
- the timing of occurrence of events; and
- the type and timing of the of control room operator response.

To overcome the previous issues, a study of accidents in Nuclear Power Plants (NPPs) needs to consider the interaction between control room operators, physical processes, and interventions of automatic systems. Prior to the Three Mile Island accident in 1979, the role of the control room operators received little attention in nuclear safety [Mosey, 1990]. After that, all nuclear accidents have been reviewed, from Windscale to Chernobyl, and the root cause analysis has shown that the "human error" is an important component in all nuclear accidents. As a result, human error and human behavior have come to be treated in the same way as technical (hardware) systems. This is a limitation, and for a complete analysis of nuclear accidents, it is necessary to consider the role of operators in the process of human-system interactions because besides the role of controlling the system during working operations, operators have to actively interact with it during emergency or accident situations. Therefore, in order to handle these human-machine interactions models of operators must be employed [Hollnagel, 1996] in a simulation-based environment.

When an abnormal situation occurs, the preferred mode of response by control room

operators[2] is to follow the guidance of procedures. In evaluating when the operators will reach a specific assessment of the plant state and perform the required actions on the plant, the steps of the procedures and the associated workload must be taken into account. The crew's execution of the procedure steps and the timing of these tasks are influenced by the crew as well as by the plant response. In addition a response based on the operators' knowledge and training has been observed in some events and in simulated situations in which the operators have perceived the procedures as incomplete [Woods, 1984], [Roth et al., 1994], and [Carvalho, 2006a]. In such situations, the control room operators' assessment of the state of the plant and of the required actions differs from those obtained by following the procedures. A combination of alarms or particular plant parameter behaviors may, for instance, cause the operators to consider performing actions supplementary to those directed by the procedures, anticipating actions that may be required by the procedures, or transferring to other procedures. Opportunities for these alternatives arise because the procedures in practice cannot provide fixed, parameter-based criteria for all decisions and therefore include some steps that involve operator judgment. Therefore, the interpretation of the procedures, the performance of the procedure steps, and the assessment of the actual plant state interact and lead the operator and crew response.

In this context, dynamic methodologies attempt to couple dynamic and stochastic processes to represent the response of the physical processes, the intervention of automatic control and safety systems, and actions of the personnel during an accident scenario [Siu, 1994]. This is achieved by embedding models of the physical process and human operator dynamics within stochastic simulation engines reproducing the occurrence of components success and failure transitions along the scenarios. In the past years a number of dynamic methodologies have been investigated. Some of these methodologies are based on Monte Carlo (MC) discrete event simulation [Labeau et al., 2000] and [Marseguerra and Zio, 1996], dynamic flowgraph methodology [Garrett and Apostolakis, 2002], [Yau et al., 1995], and [Matsuoka, 2006], Petri nets [Volovoi, 2004], and Discrete Dynamic Event Trees

[2] "Control room operators" and "control room crew" are considered synonymous. Often the terms control room is omitted for convenience.

(DDET) [USNRC, 1975], [Cojazzi, 1996] and [Hofer et al., 2002]. These methodologies mainly focus on the analysis of the interactions between the plant physical response and equipment response (success or failure); together these responses comprise the "machine" response. A few applications have addressed the interactions between the crew response and the "machine" response.

The dynamic analysis described in this study refers to the modeling of crew behaviors in the DDET framework [Sheng and Mosleh, 1996], [Gertman et al., 1996], [Hofer et al., 2002], [Kloos and Peschke, 2006], [Dang, 2000], and [Metzroth et al., 2008]. This work uses the DDET framework as implemented in the Accident Dynamic Simulator (ADS) software tool [Sheng and Mosleh, 1996]. ADS, even if still under development, has been identified as suitable tool for the description of the human-machine system evolution during an accident scenario after an initiating event, i.e., an internal or external event to the plant that perturbs its normal operation. In ADS, an operator model has been used and further developed, adding new features and new capability to better represent the crew response during accident scenarios. The operator actions are guided by coupling a set of rules-of-behavior with a procedure-following operator response based on formal and mental procedures.

## 1.3 Objective and scope of the PhD project

The overall aim of this dissertation work can be summarized as:

- develop the crew model, i.e., extend its scope by adding capabilities or models of specific behaviors;
- develop a model for the crew time variability based on existing HRA data;
- develop and apply post-simulation strategies for the analysis of the DDET-generated scenarios;

- develop a methodology for using DDET-based human-machine system approaches for informing HRA; and

- use the dynamic approach to get insights for safety analysis.

A number of models of operator have been developed [Chang and Mosleh, 1999], [Cacciabue, 1996]. In terms of the cognitive tasks of situation assessment (diagnosis) and response selection, these focus mainly on the operators' knowledge-based behavior and response. Only a few models address the procedure-guided response, the main response mode of operators, in which the procedures direct the focus of the operators and specify the actions to be taken, depending on the plant information [Dang, 1996]. The novel aspect of this work and one area in which this work makes a contribution is the modeling of the crew behaviors associated with the operators' procedure-guided response mode. This response mode combines strict procedure-following with the use of knowledge and training in the form of mental procedures and rules-of-behavior; simulation modeling appears to be essential to the analysis of the interplay between procedures and rule-based cognitive behavior [Rasmussen, 1981], [Rasmussen, 1983]. The work on the human performance model complements the modeling of the operating crew in a DDET framework [Chang and Mosleh, 2006a,b,c,d,e].

Applications of this work are in PRA and HRA. The integrated modeling of the plant-operator response achieved in this work provides improved capabilities to obtain insights to be used in the accident sequence analysis component of PRA, e.g., by identifying interactions between the operators' response and system response as well as between procedure instructions and trained knowledge and rules. The more thorough understanding of these interactions will additionally provide an improved basis for HRA, by supporting the analysis of tasks and performance contexts and the quantification of Human Error Probabilities (HEPs).

During accident scenarios (i.e., after initiating events), the control room crew is continuously monitoring the plant and it performs actions according to the plant procedures

foreseen for these situations and the associated training. The path through the procedures and the appropriate crew response is continuously determined by the state (parameter values) of the system variables. In parallel, the automatic systems are responding analogously according to their designed rules. Consequently, the operator actions and automatic system responses both change the evolution of the system variables, thereby producing dynamic interactions during the evolution of the scenario. The outcome of the scenarios strongly depends on the intervention of the automatic systems, on the actions selected by the crew, and on the timing of these actions.

For safety assessment, predicting and assessing crew performance involves understanding the indications available to the operators, and the procedures and training that support decision-making and performance in a given situation. Dynamic aspects are important to both. When do cues appear? When do operators perceive these cues and take actions on the plant? Simulator facilities such as NPP training simulators offer the possibility to observe the (dynamic) response of a few crews in a selection of scenarios, yielding highly realistic and detailed information on the interactions of system (physical process and automatic systems) and the crew. However, to obtain a comprehensive understanding of the impact of the variability in the crew response and of the timing of the operator actions in a range of scenarios, this information may ideally be extended with simulation models in which the operator response and the plant and its systems are jointly simulated.

In this work the modeling of crew variability in time performance is performed within the DDET framework. The fundamental and well-known approach is to obtain distributions of the performance times or durations of each task of interest. In a Monte Carlo task simulation, e.g., [Siegel and Wolf, 1969], the time to perform a series of tasks is obtained by sampling from each of the distributions. In the DDET, the analogous approach is to discretize the distributions for the performance times of the individual tasks, using a Discrete Probability Distribution (DPD), e.g., [Coyne and Mosleh, 2008].

The applicability of this work is in the modeling and analysis of a set of accident scenarios following an Initiating Event. The main goal is the development of a methodology

for the identification and quantification of potential vulnerabilities in the joint human-machine system response that could lead the NPP to unsafe conditions. The methodology is applied to a case study for a NPP.

In the proposed work, the DDET analysis will be performed for selected accident scenarios following a specific initiating event of a NPP. The analysis will focus on the operators' use of the procedures in conjunction with their knowledge and training. A second area of contribution for this work is in the development and evaluation of strategies and tools for constructing DDET models and analyzing DDET results. One issue relates to the perception that DDET modeling requires an impractically extensive set of inputs. In addition, the treatment of diverse scenario variants and dynamic interactions generate large, detailed trees of scenario histories. These require further analysis in order to draw conclusions and obtain the desired insights. Contributions to the resolution of these issues are essential steps to realizing the potential of dynamic tools for PRA and dynamic risk assessment.

## 1.4 Classical and dynamic PRA

Classical PRAs are comprehensive, structured, and logical analysis methods aimed at identifying and assessing risks in complex technological systems for the purpose of cost-effectively improving their safety and performance [Stamatelatos et al., 2002]. In a PRA of NPPs, accident scenarios, which are dynamic by nature, are analyzed with event trees.

An event tree graphically represents the various accident scenarios that can occur after an initiating event (Figure 1.2). An event tree starts with an initiating event and develops scenarios, based on whether a plant system succeeds or fails in performing its function. The event tree then considers all of the related systems that could respond to an initiating event, i.e., the so-called functional events or top events, until the sequence ends in either a safe recovery or reactor core damage.

For each top event in the event tree, success criteria are identified based on thermal-

hydraulic calculations. A success criterion is a condition that must be verify in order to have the success of the top event in the event tree. Success criteria can be identified for systems and for operator actions. Table 1.1 gives some examples of success criteria. The identification of the success criteria using a set of thermal-hydraulic calculations for a PRA analysis is fundamental for the calculation of the failure probabilities of the events in the event tree.

**Table 1.1:** Example of success criteria for an initiating event of a generic NPP.

| **Functional event** | **Success criteria** |
|---|---|
| Reactor vessel makeup | 1-out-of-3 trains of the Feedwater System<br>or<br>2-out-of-3 trains of the High Pressure Injection |
| Decay heat removal | 1-out-of-2 trains of Residual Heat Removal System<br>or<br>2-out-of-3 trains of Spray System |
| Manual depressurization | Operators depressurize the system in 'x' hours |

Figure 1.1 shows how the thermal-hydraulic calculations for the identification of success criteria enters in the PRA framework. For instance, thermal-hydraulic calculations support the identification of the N-out-of-M trains of a system necessary for the success of the functional event (e.g., 1-out-of-3 trains of the Feedwater System for reactor vessel makeup).

In the HRA, success criteria are important for the quantification of HEPs of given actions. In particular, the cognitive available time for an action $T_{cog}$ is defined as the difference between the maximum time window of the action ($T_{max}$, determined by thermal-hydraulic calculations) and the actual time needed for performing the action ($T_p$), which is assessed based on experience or simulated scenarios (Eq. 1.1).

$$T_{cog} = T_{max} - T_p \tag{1.1}$$

The time window of the human action actually represents the success criterion for the action. It represents the time interval in which operators have to take decisions and

perform the action in order to lead the plant in a safer state. This time will be used for the estimation of the HEP to be included in the event tree and fault tree logic.

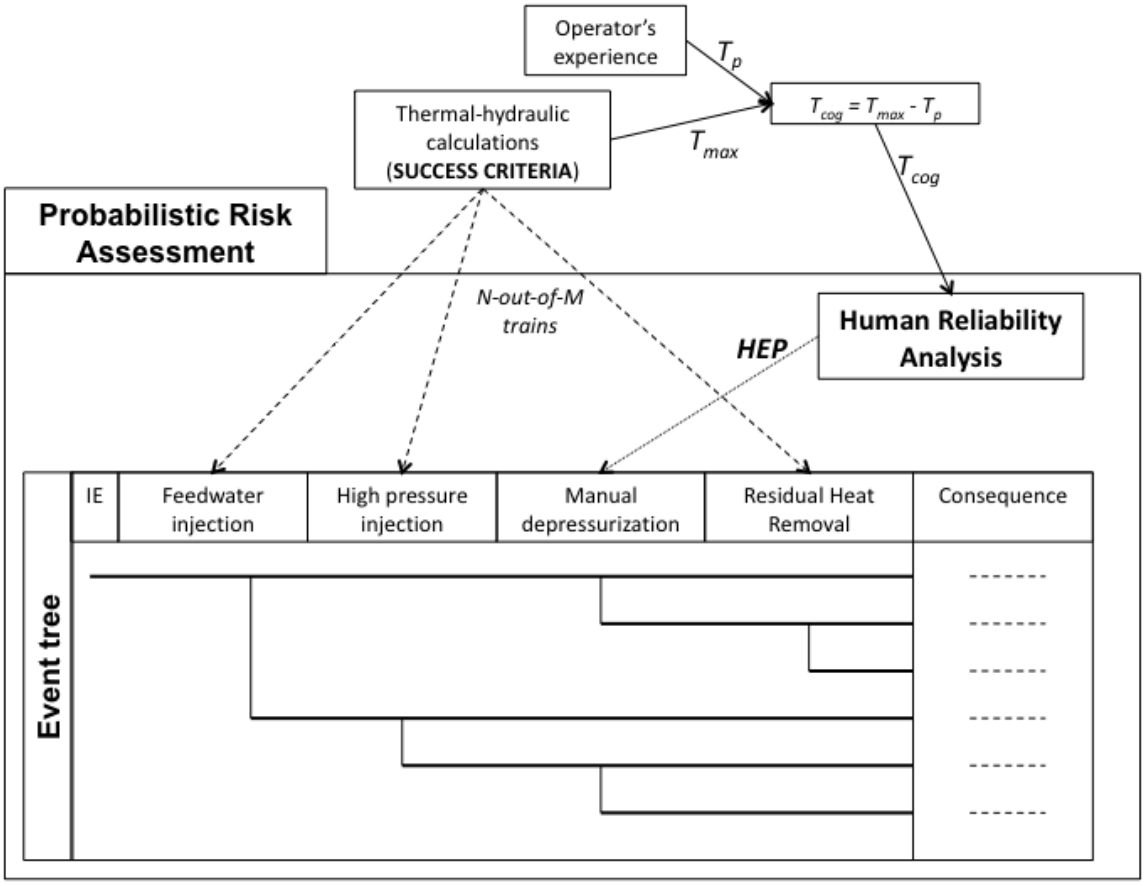



**Fig. 1.1:** Thermal-hydraulic calculations are used to obtain system success criteria and the operator cognitive time to be used in the HRA (upper right part). These are inputs to the PRA framework (bottom part), i.e., the event tree.

Figure 1.2 is a typical example of an event tree. In event trees, dynamics are difficult to address because of their quasi-static approach nature based on series of snapshots. In fact, if one wants to consider the state of the system when the event C fails, one snapshot is the IE, the success of A, and failure of B. Whereas one success of C is given by the IE, the failure of A, and the success of B. The PRA is done considering the state of the previous system until the point of interest (i.e., failure of C or success of C). The success criteria defined for the events do consider the timing of the equipment or

operator response; some examples are the time by which diesel generators must provide backup electrical power following a loss of AC power, the time window for the operators to execute an action, or the time duration for which equipment must function. However, the sequence models consider the timing of the events in a restricted manner. To remain manageable, the sequence model can only treat a representative time for each failure or success event; a given event tree sequence therefore represents many possible realizations of a sequence evolution by a bounding sequence with conservative or representative event timing assumptions. The actual timing of these events may impact the next phase of the scenario and in particular the response of the operator.

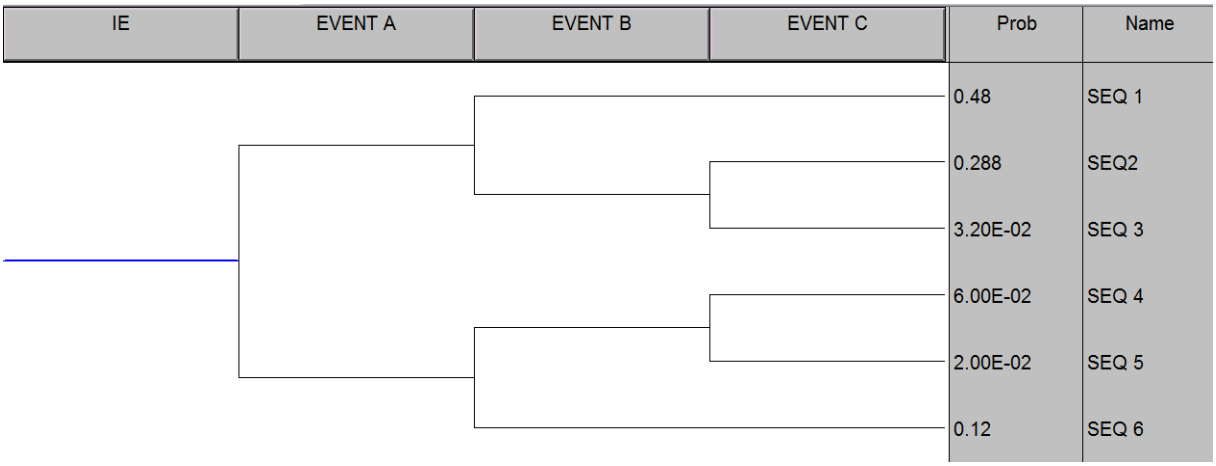



**Fig. 1.2:** Example of a classical event tree. After the IE, success (upper branches) and failure (lower branches) paths in the event tree are developed to obtain the sequence probabilities. The success and failure probabilities of the events, i.e., A, B, and C, are calculated using fault trees which calculate the event probabilities decomposing the logic of the systems associated to the events.

This classical approach has some limitations. First, in a snapshot approach (or classical approach), the analysts' selection of the representative timing of automatic and operator actions, i.e., "when snapshots are taken", defines the sequences. This means that the quality of the analysis of the sequences will depend on the analysts' assumptions concerning representative timing. In making these assumptions, the analysts are limited in terms of the sources of variability that they can practically keep track of. In addition, they are

limited in terms of their ability to consider the combined effect of these variabilities with respect to a conservative modeling of the sequence.

Second, with system snapshots one can see the effects of events on the plant but the "state" of the operator may be ambiguous. In other words, the event sequence indicates whether or not a required operator action took place (in the allowable time window); however, the human failure event may have occurred because the operators' situation assessment was erroneous or because they failed to carry out the action appropriately. In the former case, the erroneous situation assessment may affect the likelihood of subsequent human failure events: an inappropriate diagnosis may affect how new plant information is interpreted and contribute to subsequent erroneous assessment and human failure events. In the latter case, the operators' assessment is sound, which subsequently supports their assessment of the developing scenario.

Finally, in the classical approach the pace of the operator in performing actions according to plant specific procedures (the typical control room operator response) is not fully addressed. In fact, the timing of any operator action depends on what the operators have done before, their previous and current decisions, and their speed in executing procedure steps. All these factors lead to complex dynamic interactions between operators and plant which are difficult to assess.

In classical PRAs, the characterization of the context where the operators have to act, is based on accident sequence diagrams, the success criteria, and the limited number of thermal-hydraulic simulations. These runs cover the bounding sequences and do not show comprehensively the relevant interactions between physical processes, the interventions of automatic control and safety systems, and the actions of the personnel. Indeed, the performance conditions make up the context for the actions of personnel and at the same time, this context is changed by the actions.

Consequently, characterizing these conditions requires analyzing the plant behavior, the automatic control and safety systems, and the operators' response that affects both, which is the idea behind the dynamic PRA. The inclusion of an operator model in the joint

plant-operator simulation analysis explicitly accounts for the evolution of the crew understanding and decision making, yielding a broader characterization of the performance conditions. Such information is useful in predicting the probability that the operators fail in the situation assessment. The identification of the alternative response strategies "triggered" by the current crew situation assessment and the plant conditions provides insight not only on whether but also on how the operators may fail. This approach can be used to analyze undesirable actions that can be performed and to identify the potential decision-making errors. Finally, the joint simulation can treat the consequences of such errors and their impact on the scenario and on further demands on the hardware and operators.

### 1.4.1 Discrete Dynamic Event Tree framework

There are different interpretations of the word "dynamic" when used in PRA. One use of the term dynamic PRA or "living PRA" is in the conventional PRA techniques to describe periodic updates to reflect any changes in the plant configuration [Sancaktar and Sharp, 1985]. A second interpretation is when the PRA model is updated to account for equipment aging [Vesely, 1991]. The third use is to describe an approach that includes modeling of dynamic processes that take place during the plant system evolution. In other words, all plant physical characteristics are represented as time-dependent parameters, and the event tree is developed on a time scale. This dissertation is related to the latter definition of dynamic PRA.

Discrete dynamic event trees (DDETs) are produced by software coupling stochastic failure/success events (e.g., hardware failures and operators crew actions) with the continuous-time behavior of the plant process variables, usually captured by a simulation that solves the differential equations governing the plant physical evolution. Example of these software are: DYLAM [Cojazzi, 1996], MCDET [Hofer et al., 2002], [Kloos and Peschke, 2006], ADAPT [Metzroth et al., 2008], ADS [Sheng and Mosleh, 1996], and [Mercurio et al., 2008]. The latter has been used in this work.

A DDET is a tree in which branches may occur at different points in time. A DDET has three essential characteristics:

- all possible combinations of system states must be considered at each branching point;
- branchings are performed at arbitrary discrete points in time; and
- the number of sequences can quickly grow if approximations are not applied.

Therefore, the model can be applied in a simulation-oriented framework. The strength of the model is that the user does not have to specify all possible event sequences at the beginning of the analysis. Instead, the user must specify a small set of rules and the simulation generates the event sequences.

The idea of a DDET simulation is to identify branching points or nodes in the system evolution (i.e., time-points along the simulation at which stochastic events occur), save the state of the system at each branching point and successively pursue the simulation of all branches. Branching points can be generated whenever a system, a component, or an operator action is needed. Each branch represents a possible outcome of the stochastic event. Simulating the scenario evolution from all branching points allows exploring all possible behaviors of the system parameters and process variables.

The evolution of a dynamic event tree is shown in the left hand side of Figure 1.3 and the corresponding evolution of a generic plant parameter is shown in the right hand side of Figure 1.3. Each path represents a different branch of the scenario. The top of the left hand side shows the tree after the simulation of sequence 1, whose end state (e.g., stable shutdown or plant damage) is determined by the calculated plant process variables and systems states. In this run, three branching events (represented by undeveloped nodes) arise and the complete human-machine system state (state of plant parameters, equipment states, and operator state) is stored for each node. The outcome of a node can also be multiple like for example when considering timing variability of crew response.

Once having simulated the first sequence in Figure 1.3, the DDET software returns to the last node in the sequence (marked 'a'), reloads the overall state and simulates the sequence 2 to the end state of the undeveloped path. Once again, the end state is determined by the calculated plant conditions. In this example, no additional events arise. At this stage, the software returns to the next undeveloped nodes (marked 'b', 'c', 'd', and 'e' in Figure 1.3), reloads the overall state stored in the nodes and simulates the resulting sequences up to the end state. The simulation continues until all nodes have been developed. As one can see in the right hand side, the evolution of the parameters (in Figure 1.3 only one parameter is shown) is affected by the events occurred during the simulation. As soon as an event occurs along the scenario, the different outcome can lead to different parameter behaviors (sequences 1, 2, 3, and 4 in Figure 1.3) or to the same parameter behavior (sequences 5 and 6). In the latter case, the event marked as 'e' does not affect that parameter behavior. But on the other hand, other parameters might be affected by the same event 'e'.

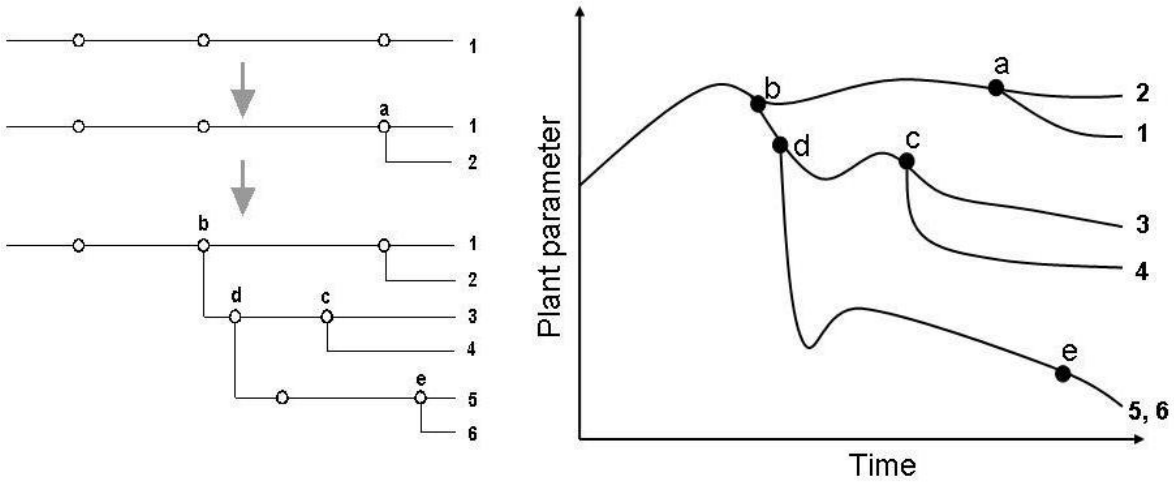



**Fig. 1.3:** Example of Discrete Dynamic Event Tree construction (left hand side) with the corresponding effect on a plant parameter evolution (right hand side).

A motivation for adopting the DDET approach for the analysis of accident sequences is that the method can explicitly model and treat the process variables, the time depen-

dence, and hardware systems. In addition, in the DDET framework an operator or crew model can be incorporated including variables describing the operator or crew response. Therefore, in a DDET framework dynamic interactions between plant and operator or crew can be directly treated.

## 1.5 Organization of this PhD work

This PhD work has been performed in three main parts: *a*) development of the DDET tool, crew model, and post-simulation strategies for the analysis of DDET-generated results; *b*) preparation of the input of the system and of the crew model based on the plant-specific PRA, and generation of scenarios; and *c*) analysis of the DDET-generated results for informing HRA and comparison with classical approaches. All these elements of the work have been performed in an iterative way in order to calibrate and improve both the system and crew model.

In particular, during the first phase, the model of the plant has been built up with the aim of modeling the selected case study for the demonstration of the capability of the dynamic approach; this included the development of the thermal-hydraulic model with controls, components, systems, and alarms. Then, a crew model based on a procedure-guided operator response has been developed and implemented in the ADS simulation environment which has been also improved for the integration of the crew model. Finally, post-simulation strategies have been developed to handle the great amount of data generated by the simulation.

In the second phase, the input for both the system (control panel) and the crew (procedures and rules-of-behavior) has been created. Based on this input, the simulation tool has been run to generate the DDET scenarios necessary for the analysis.

In the last phase, the DDET-generated scenarios have been used to demonstrate the capability of the dynamic approach, to obtain insights for HRA through the Performance Shaping Factors (PSFs), and to compare results from classical and dynamic approaches.

This dissertation report is organized as follow. In Chapter 2 a literature review of typical control room operator response and existing HRA and operator models is presented. In particular the focus will be on models related to the one presented in this PhD work and on some limitation of the current operator models. In Chapter 3 an overview of the simulation framework (ADS) and in particular the developed operator model is described. Chapter 4 describes the methodology developed for the analysis of the DDET scenarios, i.e., the use of a classifier for classification of scenarios based on similarities and a DDET parser. Chapter 5 illustrates the case study implemented in this PhD work, the scenario modeled, and the operator actions implemented in the operator model. In Chapter 6, an high level overview of the plant parameter evolutions is shown and results are presented and discussed focusing on their use to inform HRA and comparison with classical HRA approaches. Finally in Chapter 7 some conclusions are drawn.

## Chapter 2

# Literature Survey

## Contents

This chapter provides a selected bibliography of the more recent studies on crew performance in NPP training simulators, and classical and advanced dynamic HRA methods. This review is not intended to be exhaustive but only a selection of the studies closely related to this dissertation work has been chosen.

In particular, a literature review on how control room crews usually behave in NPPs during accidents is presented in Section 2.1; this includes a description of the typical procedure-guided crew response and studies in simulators to understand how crews handle accidents. Then, an overview of the classical methods for HRA is presented in Section 2.2 underlying the strengths and weaknesses of these methods. Next, in Section 2.3, a selection of some of the most recent advanced methods for HRA is presented. Finally Section 2.4 presents the limitation of the current models and the main features of the model proposed in this work.

## 2.1 Typical control room crew response

As soon as an abnormal or emergency condition arises in a NPP, the control room crew is instructed to respond and interact with the system trying to mitigate the potential undesired consequences. Three types of operator response are considered:

- *knowledge-driven*: the response of the operator is based only on the operator's knowledge and training (i.e., rules-of-behavior);

- *procedure-following*: the response of the operator depends only on written procedures, i.e., the operator strictly follows them; and

- *procedure-guided*: the response depends on both procedures and knowledge and training of the operator who does not strictly follow the procedure, but in addition cognitive processes guide the response.

During an accident scenario (as well as during normal conditions) the typical control room operator response is guided mainly by procedures, i.e., a set of instructions that the operators must follow during accident situations. In order to examine the operator performance in control rooms, empirical studies are usually conducted in NPP training simulators. Data are collected by observing the behavior of control room operators during emergency scenarios. An interesting point is to examine how control room operators interpret and use procedures in response to events. Three important works have been done in this direction, i.e., [Woods, 1984], [Roth et al., 1994], and [Carvalho et al., 2005], [Carvalho, 2006a], [Carvalho et al., 2006b].

In [Woods, 1984] the author synthesizes some results from several studies of operator performance during simulated NPP emergencies. Understanding how operators perform during emergency events is critical to the design and evaluation of human-machine system interaction. In the work one of the main analyzed issues is how the operators utilize Emergency Operating Procedures (EOPs) during emergencies. The analysis is based on a database which collects data about operator performance. In general, EOPs are a static and sequential list of activities that the operator must perform during the accident. The analyzed data show that the actual operations are dynamic, i.e., events occur at indeterminate times, operators can perform parallel actions, and several parameters need a continuous or semi-continuous monitoring. Therefore, in order to achieve goals within procedures, a goal controlled approach is usually adopted by control room operators trying to match the static nature of the procedures with the dynamic nature of the accident evolution. Controlled approach means that control room operators do not strictly follow actions contained in procedures but they constantly correct possible errors and control the step results, through a feedback mechanism. As underlined by Woods, operators have to understand how the various steps of procedures work together to produce intended effects.

In [Roth et al., 1994] data from training simulators of two plants running an Intermediate System Loss Of Coolant Accident scenario are collected. They analyzed results to

identify situations where higher-level cognitive activities take place to deal with situations not fully addressed by the procedure. The results of the study supported that crew situation assessment and response planning continue to play an important role, even when EOPs are employed. They argue that there are mainly two approaches in the study of procedure response by control room operators during emergency scenarios. The first one is that operators strictly follow EOPs, i.e., they just have to be able to read and follow each step in the EOPs. The second one is that a higher-level cognitive activity plays an important role in following EOPs. The role of the situation assessment and response planning is quite important even if EOPs are employed because they enable the crew to identify and deal with situations not fully addressed by the procedures. The main result of the study conducted by [Roth et al., 1994] demonstrates that the operator performance during emergency scenarios is guided by a higher-level cognitive activity, such as situation assessment and response planning in performing EOPs. During the scenario evolution, several crews recognized that some of the steps in the procedure were inappropriate to the situation and should not be followed and they performed the response based on knowledge and training.

Finally, experiments conducted in a real control room during micro incidents [Carvalho et al., 2005], [Carvalho, 2006a], and [Carvalho et al., 2006b] demonstrate that there are limitations in strictly following procedures by control room operators. In fact, they argue that procedures do not consider the variability of individuals, the application conditions are not always well defined, the procedure will not be always used in the right moment, the design of the procedures cannot consider aspects like habits, culture, sociology aspects, of the crew, and finally procedures refer to ideal situations modeled by the designers. The procedure approach is static and ignores the dynamic characteristic of the work activities. There are situations where the operators decide to accomplish their scheduled tasks rather than following test procedures; therefore, operators use analogies, cooperation, hypothesis test, tacit knowledge to solve their problems in unfamiliar situations, rather than standard operational procedures. In other words they use training and

experience. Indeed work is often accomplished through a dynamic redistribution of tasks or roles, involving interactions between individuals, in a cooperative, opportunistic, and situated way.

As the three studies show, the key point is the interpretation of the procedure steps based on the cognitive assessment on the plant situation. The dynamics of the plant are important to be taken into consideration when following procedures. Therefore, real control room operators do not strictly follow procedure but in addition to the procedure-following response they use their knowledge and training to perform each procedure step.

In the context, advanced methods for HRA that try to capture the pattern of a typical control room operator response during accidents have been developed in the last decades. Those methods, presented in Section 2.3, are based on the so-called first generation HRA methods introduced in Section 2.2.

## 2.2 Classical treatment of human performance

In current PRAs, the propagation of an accident scenario from an IE is analyzed in two major steps [USNRC, 1975]. First, event trees are used to model the scenarios based on success and failure of safety systems and operator actions, then the likelihood of the scenario and the probability of the occurrence of the top events is quantified using fault trees.

The purpose of HRAs is to estimate the likelihood of particular human actions not being taken when needed, or other human actions that may cause hazardous events (by themselves or in combination with other conditions) occurring. Failures to take actions to prevent and cause hazardous events, are commonly called "human errors" in HRA. HRA methods are some structured approaches that aim at estimating the probability of failure for a given action. However, this estimation needs to take into account the work environment and task conditions under which the work is done, since these can provide an important influence on the likelihood of errors.

Human reliability analysis employs a set of tools to estimate the likelihood of required human actions being performed when needed. These likelihoods can then be incorporated into the overall risk assessment, so they can be combined with other probabilities in the fault/event tree framework, such as those of equipment faults and other hazardous states, to estimate the overall likelihood of hazardous events.

An exhaustive description of the currently used HRA methods can be found in [Forester et al., 2006]. Those methods are:

- Technique for Human Error Rate Prediction (THERP) [Swain and Guttmann, 1983];
- Accident Sequence Evaluation Program (ASEP) HRA Procedure [Swain, 1996];
- Human Cognitive Reliability (HCR)/Operator Reliability Experiments (ORE) Method [Hannaman et al., 1986];
- Cause-Based Decision Tree (CBDT) Method [et al., 1992];
- Electric Power Research Institute (EPRI) HRA Calculator [Julius et al., 2005];
- Standard Plant Analysis Risk HRA (SPAR-H) Method [Gertman et al., 2005];
- A Technique for Human Event Analysis (ATHEANA) [ATH, 2000];
- Success Likelihood Index Methodology (SLIM) Multi-Attribute Utility Decomposition (MAUD) [Embrey et al., 1984];
- Failure Likelihood Index Methodology (FLIM) [Chien et al., 1988]; and
- A Revised Systematic Human Action Reliability Procedure (SHARP1) [Wakefield et al., 1992].

Many of these HRA models are based on either time-reliability curves or simple information processing models, such as a signal-organism-response model. The level of task

decomposition is more closely associated with the type of action than the underlying processes driving the operator behavior. Therefore, these methods are limited in their ability to fully account for contextual factors and additionally have some limitations summarized as: they do not provide strong basis for the calculation of error probabilities, they are analyst-dependent, they do not explicitly consider the context where the operator actions are taken, and the mutual interaction between operators and plant and vice versa is not addressed.

Advanced methods should include various needs and requisites like: *a*) better explanatory (causal) models, *b*) more explicit role for context both in error identification and probability estimation, *c*) more scientific basis for selecting and measuring PSFs, *d*) more formal use of knowledge accumulated in the behavioral sciences, *e*) reduced reliance on expert judgment, *f*) more realistic representation of the dynamic of human-system interactions, *g*) traceability, consistency and repeatability. Therefore, advanced methods must be able to mainly identify the human response in the PRA context, estimate the failure probability of the response, and identify the causes of errors to support the development of preventive measures.

## 2.3 Operator models

In this paragraph a set of operator models is described. The models here described do not completely cover the entire spectrum of the existing models and they cover only several of the ones in the nuclear field. The models cited in this chapter are briefly described in Appendix A.

So far, a number of operator models have been developed in HRA. One of the first models for human-machine system analysis was the task simulation developed by Siegel and Wolf [Siegel and Wolf, 1969]. The model focuses on tasks that have to be performed by operators in a given available time. A typical characteristic of task simulations is that they do not model the plant behavior in the human-machine system and the tasks

generally depend on the system design. This means that tasks and available time to perform certain tasks depend on the pre-analysis of the system. Task simulation is the base for a number of models developed for aircraft crew and NPP crew simulation. A model developed in the nuclear field is MICROCREWS that simulates the flow of actions following tasks across time in a NPP.

Extensions of task simulation are models still based on task simulation in which the plant behavior in the human-machine system model is explicitly treated. This family includes models such as PROCRU and INTEROPS. In both, the operator model considers the knowledge-bases capabilities for fault diagnosis, situation assessment, decision-making process, and procedure generation. In addition, two other important models have been developed in the last years and they have been implemented in MCDET and ADAPT framework. In both of them, the model implemented is based on a procedure-based operator response and the knowledge-driven operator response is not included.

The bulk of operator models are based on cognitive models. These models introduce features to represent the cognitive mental state of control room operators. Examples of these are CES, COSIMO, NPPCREW, JAERI, IDAC , DETAM, OPSIM, and SYBORG. In several of them, such as OPSIM, NPPCREW, DETAM, and IDAC, the procedure-following responses are also partially handled.

The development and the use of a particular human-machine system model depend on the context where it has to work and on the scope that it has to address. In situations where only set of tasks have to be performed models like task simulation are accurate; on the other hand, situations in which a direct human-machine system interaction is required, more sophisticated models are needed.

The application of a particular operator model depends also on the scope to be handled. For example if the scope of the operator model is to simulate the communication between members of a crew PROCRU model is appropriate or if the scope is to simulate the interaction between operators and environment, models like MIDAS, or IDAC are adequate. Table 2.1 summarizes the scope of different operator models with a relative

**Table 2.1:** Summary of the scope of different operator models.

| Scope | Description | Operator model |
|---|---|---|
| Communication | Communication process among the members of a crew | PROCRU |
| Interaction | Interaction between operators and environment | MIDAS, SYBORG, IDAC, TBNM |
| Operator's behavior | Behavior of a single operator during abnormal conditions | CES, COSIMO, OPSIM |
| Procedure-following response | Written or mental procedures guide the response of the operator | Task simulation, MICROCREWS, MCDET, ADAPT |
| Cognitive behavior | Cognitive behavior based on both rule-based and knowledge-based response | PROCRU, NPPCREW, JACOS, IDAC |
| Rule-based behavior | Cognitive behavior based on rule-based response | PROCRU, DETAM |
| Knowledge-based behavior | Cognitive behavior based on knowledge-based response | CES |
| Timing of nominal action | Execution of an action at normal time and different than normal | Task simulation |
| Procedure-guided | Human behavior based on the combination between procedure-following response and knowledge and training of the operator | IDAC (partially) |

short description. Notice that the same model can address different scopes.

In the next Section a small set of operator models strictly related to the one developed in this PhD work are presented, i.e., DETAM, MCDET, ISA, and ADAPT.

### 2.3.1 Dynamic Event Tree Analysis Method (DETAM)

The Dynamic Event Tree Analysis Method (DETAM) for accident sequence analysis allows a general treatment of the integrated response of a NPP and its operations to an Initiating Event (IE) [Acosta, 1991] and [Acosta and Siu, 1993]. DETAM is a generalization of the Dynamic Logical Analytical Methodology (DYLAM) [Cojazzi, 1996].

The DYLAM methodology is a tool for integrating deterministic and probabilistic failure events; the first version has been implemented in 1981 [Amendola and Reina, 1981]. The basic idea of DYLAM is to provide a tool for coupling the probabilistic and physical behavior of a system for reliability analysis. The physical part of the system is contained in a numerical simulation whereas the components of the system are modeled in terms of working state (success, failure, stuck open, stuck close, etc.). The simulation is driven by the history of the states of the components which have random transition during the evolution of the scenario. The top conditions of the system can be analyzed in terms of values of process variables. The main characteristic of DYLAM is to follow different paths resulting from the initial states of the components and from transitions of the component states and to drive the simulation.

The generalization of DYLAM consisting in the implementation of an operator model in the DYLAM framework is DETAM. In fact, if the plant state is described in terms of the hardware states and process variables only, DETAM is similar to DYLAM. The difference between DETAM and DYLAM becomes evident if the operator crew is considered.

In the DETAM approach, the plant process variables and the operators' understanding affect each other during the evolution of the scenario events. In fact, *a*) the plant process variables linked to the operators' actions determine the timing of events; *b*) the plant process variables lead to different required actions; and *c*) the operators' actions lead to changes in the process variables. In addition, the operators' understanding of the current accident evolution may affect the likelihood of future actions. In DETAM, the operators' understanding is called crew's "diagnosis state". Supported by experimental studies described in [Itoh et al., 1990] the operator's mental model during simulation exercises might be mapped in a two-dimensional matrix; the first dimension corresponds to the diagnosis state whereas the second dimension corresponds to the actions that the operator (or the crew) is planning to take. In addition in order to characterize the crew a third state, i.e., the crew's quality state, characterizes the ability to perform tasks. The crew's quality state models the influence of Performance Shaping Factors (PSFs) like

stress. This third state model has not been implemented but only theoretically considered.

The crew diagnosis state considers the operators' understanding of the past and current conditions. DETAM defines the diagnosis state in terms of operators' understanding and state of five safety functions. The operators basically monitor the five safety functions and based on their evolution and value they draw conclusion about the current scenario (steady state, SLOCA, SGTR, etc.). A high level diagram of the diagnosis state is shown in Figure 2.1. Note that simple rules can be assigned to model the likelihood of incorrect diagnosis.

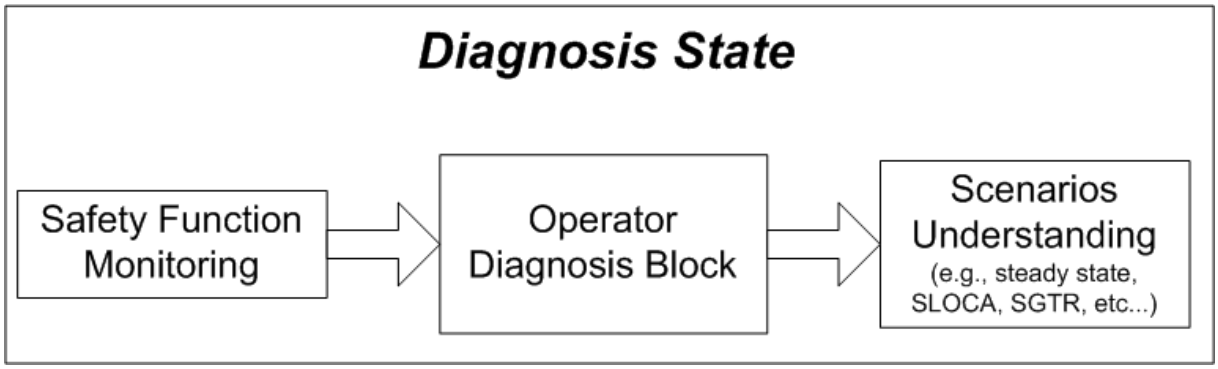



**Fig. 2.1:** Diagnosis state mental model in DATAM.

The crew planning state refers to a set of actions that the operators are planning to take. In DETAM, the set of actions are closely relates to actions within procedures. Other actions are treated in a very limited way. There are two levels of states, i.e., the procedure sub state and the procedure step sub state. The first specifies which emergency procedure must be followed and the second one indicates the step in the followed procedure. The transition between the procedures depends on the indication within the procedure step whereas transition between procedure steps are guided by the procedure. In DETAM the probability to skip procedure steps is also implemented. Figure 2.2 shows the crew planning state mental model at a very high level.

For a DDET point of view, DETAM and in particular DYLAM is a very powerful model and it has drawn the basis for the further DDET models. As pointed out by the authors, one of the bottlenecks of the model is the quantity of generated scenarios. This

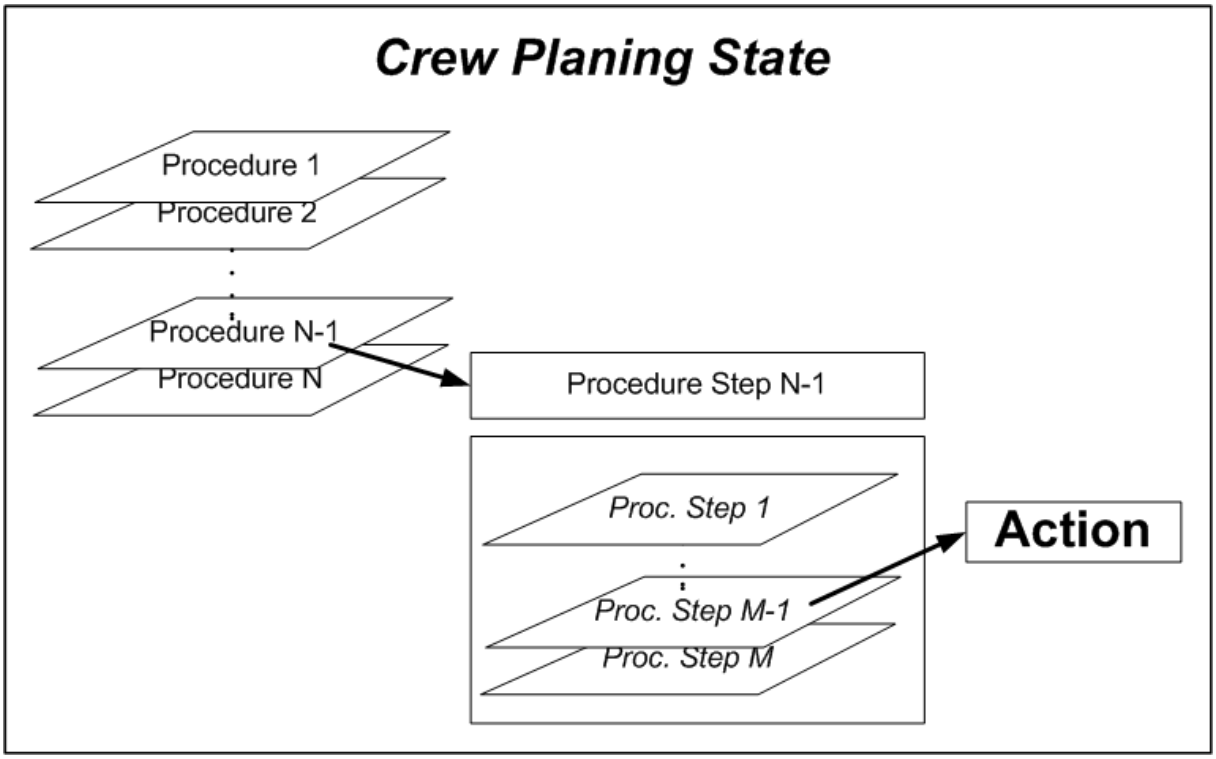



**Fig. 2.2:** Crew planning state mental model in DATAM.

issue has been considered and solved in this dissertation project and it will be further explained in Section 3.1.4.

### 2.3.2 Monte Carlo Dynamic Event Tree method (MCDET)

The MCDET method is a combination of Monte Carlo (MC) and Discrete Dynamic Event Tree [Kloos and Peschke, 2006]. MCDET is linked to a deterministic code (MELCOR) that solves thermal-hydraulic equations. In MCDET both the aleatory (stochastic) and epistemic (state of knowledge) uncertainties are treated. In MCDET usually the discrete variables are treated by the DDET whereas the continuous variables are treated by MC. The number of sets is $n$. For each set of values provided by the MC, a DDET is generated in MCDET. The diagram of the MCDET simulation is shown in Figure 2.3.

The authors of MCDET underline that the tool is capable of accounting any deterministic or random transition in time and space. If random transitions have only discrete

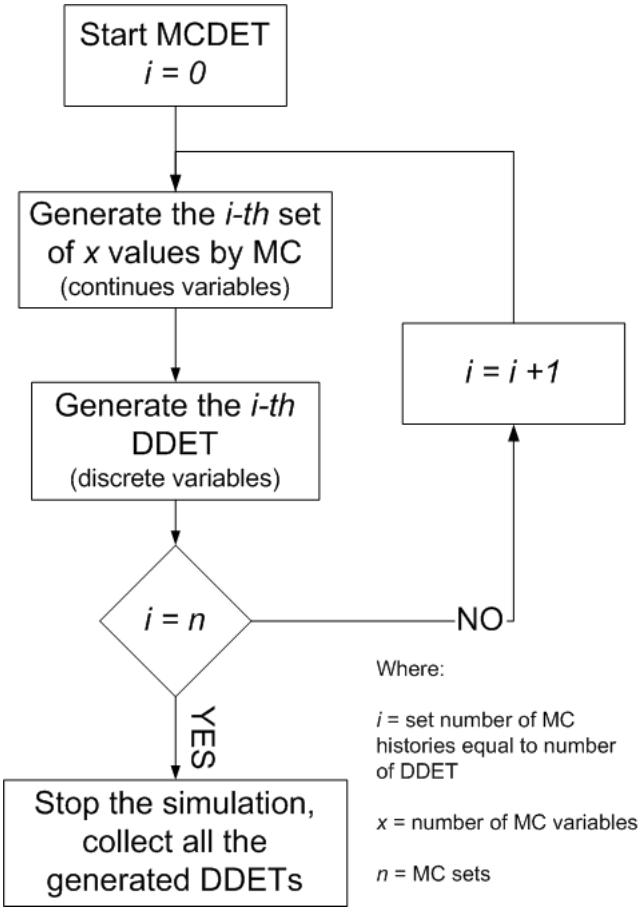



**Fig. 2.3:** MCDET simulation diagram.

alternatives, MCDET keeps track of all the alternatives and generates a DDET. If also transitions are associated with continues variables, MCDET uses MC to generate alternatives and produces a random sample of DDETs. In order to keep the computational effort practicable, a probabilistic cut off criterion is introduced, i.e., the conditional probability of the sequence is less than a certain threshold then the sequence is cut off.

Recently within the MCDET framework, a crew module has been added as described in [Peschke and Kloos, 2008a], [Peschke and Kloos, 2008b]. The combination of the crew module and a deterministic dynamics code is capable of handling the interactions within operators, hardware, and the physical process. Coupling the stochastic module MCDET to this combination provides a simulation tool that is able to account for stochastic influences on the dynamics of the complex system, and, vice versa, for the influence of the

dynamics on the stochastic.

In the MCDET framework, a scheduler organizes the interaction between crew, hardware, and plant. In order to build up the DDET, the scheduler first calls the routine which sets the initial and boundary conditions (initialization of the scheduler items). Then, depending on the condition, the deterministic dynamics code or the crew module routine is activated calculating the first DDET sequence. If there is a branch to be generated due to either human actions or hardware components, MCDET selects the branch to be calculated next whereas the information of all other branches, which still have to be calculated, is kept in memory according to a first-in-last-out structure. If there is not any branch left to be calculated, the DDET is completed. The construction of a new DDET starts with the activation of the MCDET routine which provides the initial and boundary conditions.

The human actions modeled in MCDET are mainly based on procedures. MCDET can be seen as a task simulation methodology where the human actions are modeled according to the task the operators have to accomplish. A model for the implementation of Human Error Probabilities (HEPs) is also included in the MCDET framework. As the authors argue, the crew module of MCDET focuses on the consequences (actions, communications) of a prevalent mental state and cognitive behavior and does not explicitly model mental and cognitive processes. It permits situation-dependent sequences of human actions to be run as they are expected for a dominant cognitive behavior. PSFs such as stress, knowledge, or ergonomics are considered as dynamic quantities that change in the course of time.

### 2.3.3 Integrated Safety Assessment methodology (ISA)

The Integrated Safety Assessment (ISA) methodology was first developed in 1993 [Izquierdo-Rocha and Sanchez-Perea, 1994]. Further developments of the model can be found in [Munteanu and Aldemir, 2003] and [Queral et al., 2004]. The model is based on three

main elements: a plant simulation code, a computerized procedure system, and an interface module between plant code and the procedures. The entire model is based on a dynamic generation of event trees.

The dynamic event tree generation was developed in 1999 by the Spanish researchers Munoz, Minguez, and others. The tool was called DENDROS (Dynamic Event Network Distributed Risk Oriented Scheduler), was developed mainly to model response of safety features to a transient for Level 1 PRA and is a discrete event processor, managing messages coming from different calculation modules including the physical system simulator and decision processes. It is designed for a distributed computing environment using a network of processors exchanging information through an independent channel. During a simulation, the scheduler makes a decision about the need to create new processes if a setpoint is crossed (branching point), changes the already running processes to stand-by state for later reuse, or even forces some non-active ones to terminate based on the end conditions, such as probability falling below a user-specified cut off value. Whenever a branching point is detected, a request is sent to the decision module in order to know whether a simulation of the resulting possible sequences is needed. Then, the decision module computes the probability of the sequence either from given data or fault trees in the form of binary decision diagrams, and compares it with the cut off value to complete the decision.

The plant model is based on the TRETA code (Transient Response and Test Analyzer) linked to DENDROS [Munoz et al., 1999]. TETRA is a simulation system able to simulate all the plant systems including controls, protections, and balance of the plant. Within TETRA a module which simulates the thermal-hydraulic of the plant is included. The module models the plant process behavior based on a single and two-phase regime.

The procedure following system is based on COPMA-III developed at the Halden Reactor Project. It is a support system which guides the operators during the execution of the emergency procedures. COMPMA-III basically models the set of procedures implemented by the analyst depending on the event under analysis. The procedure system is

then connected via buses to the thermal-hydraulic plant model.

As one can understand, the ISA methodology is mainly based on a procedure-following model meaning that no cognitive activities are modeled.

### 2.3.4 Analysis of Accident Progression Tree methodology (ADAPT)

The Analysis of Accident Progression Tree (ADAPT) methodology has been developed in the DDET framework [Metzroth et al., 2008], [Hakobyana et al., 2008]. ADAPT generates a DDET controlling the evolution of the scenario under consideration and creating branches specified by the user through rules. ADAPT can execute several scenarios, in particular any severe accident and any type of simulator as long as it is possible to produce a text input file and the simulation can be stopped and restarted any time during the evolution.

In the ADAPT framework, in addition to rules related to hardware components, branching rules related to human actions can be introduced. In this way, the effect of the operator actions on the scenario evolution can be seen in the generated scenario. The human actions incorporated in ADAPT are related EOP actions.

In order to get branching probabilities for the human actions, the SPAR-H model [NUREG/CR-6883, 2005] has been used. SPAR-H breaks down the HEP into two components whose probabilities are treated separately: diagnosis component and action component. Within each component PSFs are used to account for specific variabilities.

Even if in principle any thermal-hydraulic code can be used, currently for the thermal-hydraulic part, MELCOR Severe Accident Analysis Code in used. The model so far has been applied in a PWR NPP with Westinghouse EOPs.

## 2.4 Limitations of current operator models

As already underlined in Section 2.1 the dynamics of the plant are important to be taken into consideration when following procedures. Therefore, real control room operators do not strictly follow procedures (which are static by nature) but in addition to the procedure-following response they use their knowledge and training to perform each procedure step. Thus, in the context of modeling the operators' behavior during accidents in NPPs both the strict procedure-following approach and operator knowledge and training must be considered.

In classical HRA analyses and in the literature review performed in this PhD thesis, models that explicitly consider both the procedure-following operator response and the cognitive response based on knowledge and training have not been indentified. They mainly focus on models that strictly follow procedures. For example, the operator model implemented in DETAM, is a good starting point for further analysis. It must be pointed out that the tasks considered in the application of the model are not very different with regard to the ones considered in the conventional PRA. In particular the calculation of the available time windows is done by the analyst and it is used to develop the understanding of the crew behavior during the evolution of the scenarios. In addition, there is not a casual model of the operator behavior; the analyst supplies the likelihood of the operator state transitions.

In MCDET and ISA, the main focus is the procedure-following operator response. There are not features that involve operators' understanding and training. The same apply for ADAPT. In addition, ADAPT has been developed for a Level 2 PRA analysis whereas in this dissertation work the main focus is the Level 1 PRA where the operators have to interact with the plant in order to avoid the core damage.

Several needs are important when developing an HRA model which are lacks in classical HRA models and advanced dynamic models. In particular, the following considerations are regarded as quite important:

- explicit role of the context in error identification and probability estimation;
- inclusion of recovering actions in the model;
- formal procedures as a base for the modeling of the operator response;
- formal use of the knowledge and training of the operators from simulator studies;
- realistic representation of the dynamic nature of the human-system interaction;
- estimation of the response probability; and
- identification of causes of errors to support the development of preventive or mitigating measures.

Most of the conventional and recently developed HRA methods are at the behavioral (procedural) and contextual (static or quasi-static) level whereas the conceptual (cognitive) level has been in part neglected. A model-based approach which goes in the direction of covering the three previous levels is challenging and still needed.

In this direction, the existing ADS-IDAC model is trying to encapsulate in the model the three levels just described. The main issues that the operator model developed in this dissertation work is the ability to model in addition to the strict procedure-following response the capability to implement rules which take into account the operators' understanding and knowledge and training. This model uses the previous developed ADS-IDAC model [Chang and Mosleh, 2006a,b,c,d,e], [Coyne, 2009] as s basis for the development of the operator model in this study which it is further described in Chapter 3.

The results, further presented in Chapter 6, show the ability of the tools and of the methodologies developed in this PhD work to model the crew-system response in an accurate way, i.e., close to the typical crew-system response in a typical control room, and to obtain insights for HRA. Therefore, the developed operator model embedded in the ADS software tool is able to model the operator response combining the use of plant procedures, mental procedures, and "rules" based on training.

## Chapter 3

# Model of crew response

## Contents

This Chapter introduces the model of the crew response and the implementation of it in the DDET framework. In particular, in Section 3.1 the main features of the conceptual crew model are presented. Then, in Section 3.2 the implementation of the crew model in the ADS framework is shown. Afterward, in Section 3.3 the application of the timing methodology for the current operator model is described. Finally, in Section 3.4 a summary of the arguments presented is drawn.

The main objective of this Chapter is to present the crew model focusing on the main characteristics important to support HRA. Additionally, another goal is to show how the crew model is embedded in ADS, what are the main features, and its application on a test case.

## 3.1 Main features of the conceptual crew model

A general approach of a control room operator response is based on a cyclical model as described in [Hollnagel, 2003]. The model shows how the performed actions depend on the current situation understanding which depend on the occurred events which in their turn depend on the feedback on the performed action.

The conceptual operator model is composed by four main blocks: perception, situation assessment, response planning, and execution (Figure 3.1). The perception block manages the process of acquisition of information from the plant through the control panel. The information can be alarms, particular components state, or plant behavior. The second block is the situation assessment. In this block, goals and strategies are identified based on the perceived information. In this block, the perceived information are registered and stored in the memory. Based on the perceived information, the operator can take decisions which are based on stored rules coming from previous successful experiences. The third one is the response planning block. In this block, the strategies and the identified goals are set. The strategies could be for instance following emergency procedures, perform mental procedures, or response based on training. Then, in the execution block the identified

goals and strategies are performed through actions. The execution of actions, will affect the subsequent perception, situation assessment, and response planning along with new perceived information coming from the plant.

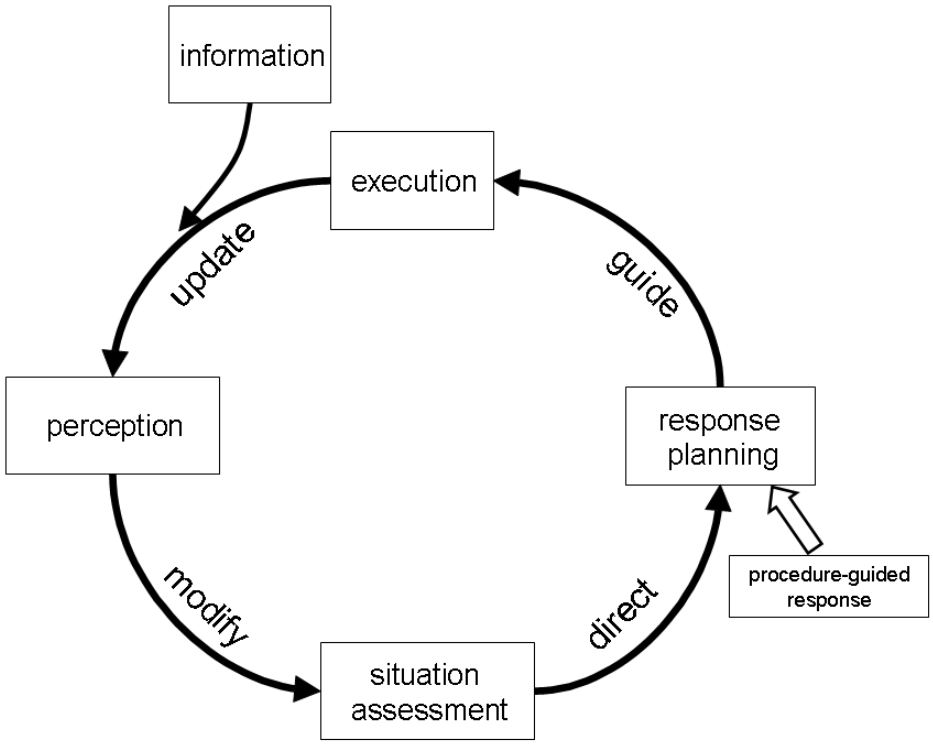



**Fig. 3.1:** Cyclical model of operator response.

In the context of the strictly procedure-following response, the operator model has just to follow steps in the procedure and the situation assessment and the understanding on the system are not considered. Once the action in the procedure is taken, the next procedure step or set of procedures have to be performed until the end of the procedures is reached.

The operator model in this work follows the directions argued by the studies based on typical training of control room operators. According to those studies (Section 2.1), the operators' performance during emergency scenario is guided by a higher-level cognitive activity based on a knowledge-driven response. The operator's response is driven therefore

by procedures and by the operator' situation assessment on the system directs the action to be taken, i.e., the so called procedure-guided response.

Therefore, the operator model developed in this work is based on both procedure-following response and knowledge and training response and it is modeled in thy cyclical model.

### 3.1.1 Procedure-following operator response

Procedures are composed by different tasks where the operators are instructed to achieve some goals. For instance, a goal could be the depressurization of the system to a certain pressure level, or the cooldown of the system, or some checks to transfer to a particular procedure if one or several criteria are verified. A task is then constituted of different procedure steps designed for accomplish the goal within the task.

Typically, accidents in NPPs, are classified in two groups: design-basis accidents and beyond-design-basis accidents. In case of design-basis accidents, the management of the accident within the plant is carried out with the aid of operating manuals or procedures. When the cause of the accident can be identified, accident management is undertaken with the guidance of event-oriented procedures. At the same time, critical safety function criteria are monitored to ensure the safety of the system. These criteria represent safety relevant conditions that must be maintained in order to preserve the plant in safe conditions within the design-basis. If one or more critical safety functions are challenged or violated it is restored by initiating the symptom-oriented accident management. The symptom-oriented procedures always have priority over the event-oriented procedures during the execution of accident management measures.

The interaction between event-oriented accident management and the continual critical safety function monitoring is specified in the operator response guide. The operator response guide also serves to direct the operator to the beyond-design-basis operating manual if the design-basis event symptom-oriented measures are insufficient to guarantee

that the critical safety functions are fulfilled.

The beyond-design-basis operating manual is structured in the same way as the symptom-oriented section of the design-basis operating manual. In the beyond-design-basis area it is legitimate to operate plant systems or system components beyond their original design specifications or they may be used for purposes other than originally planned. The majority of the beyond-design-basis procedures concentrate on preventive measures. Most of the procedures have been written in order to prevent core melt and to ensure that the core remains within the reactor pressure vessel.

This study will focus on both design-basis accidents and beyond design-basis accidents for a typical PWR power station, depending on the scenario evolution based on the failure of one or more components.

A typical procedure step is represented in Figure 3.2. In that example, operators are instructed to check the reactor level and if it is larger than a certain value $X$, have to actuate system 1. Then, after that, they have to check again the reactor level and if it is larger than $Z$ they go to the next procedure step, otherwise they loop back, they check the system 2, and they re-check the reactor level. However, if the level was not larger than $X$ at the first check, they have to see whether the level is larger than $Y$, then they have to close valve 1 and check the system 2. Afterward, they have to loop back and check again the reactor level and see whether it is larger than $X$. And so forth.

Two main issues are important to mention at this stage. The first one is the interaction between the operators and the plant (close valves, actuate systems, etc.) and the second is the dynamic of this process. In fact, the time necessary for the operator to check the reactor level, actuate the system 1 a re-check the level influences the successive scenarios evolution. If they are too fast, the reactor level has not yet reached the level Y and therefore the operators have to loop back and redo the procedure steps whereas if they are slower, the second criterion of the reactor level larger that Y is met and they transfer to the second procedure step. Therefore, the dynamics of the human-machine system interactions are important to be assessed and depending on when they occur the next

phase of the scenario might change. Evaluation of these interactions is important for HRA and they must be taken into consideration for dynamic PRA evaluations.

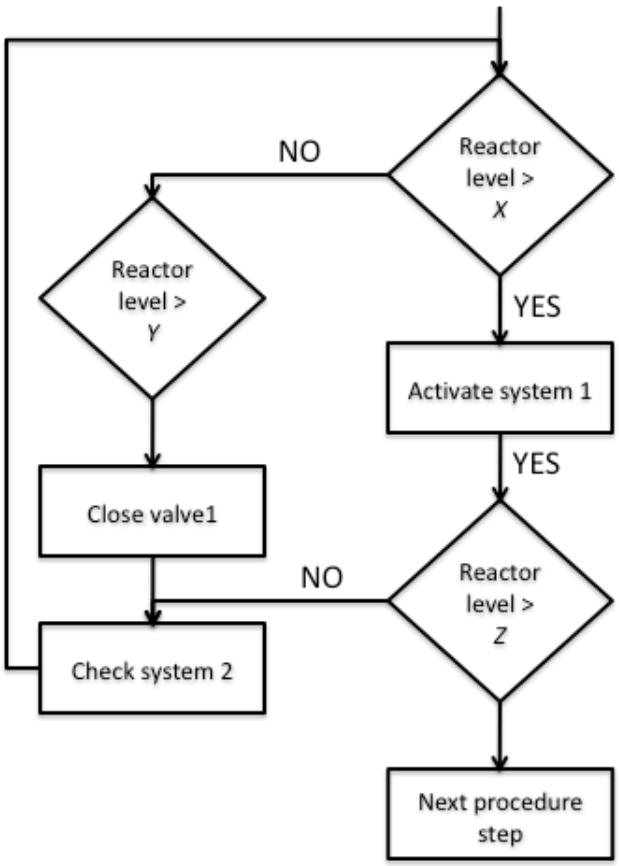



**Fig. 3.2:** Block diagram representation of a typical procedure step of nuclear power plants.

### 3.1.2 Operator knowledge and training

A typical approach for the development of a conceptual operator model based on operator's knowledge and training is to follow the Rasmussen's SRK three-level action model, which divides all the human actions in a system into three categories of skill-base (S), rule-base (R) and knowledge-base (K) [Rasmussen, 1983].

Skill-based behavior is to indicate a close relationship between information input and the response of time. A skill-based response is usually performed shortly in time and it does not depend on the complexity of the given task.

Rule-based behavior is to identify actions controlled by a group of rules. It differs from the skill-based behavior mainly because of different levels of understanding of the practices.

Knowledge-based behavior is activated when new unknown situations occur and the operators have to handle them based on their knowledge and experience. Because of the limitation of their experience and knowledge on these situations, errors are more likely to occur than in the other types of categories.

In the operator model developed during this work the second type of behavior is considered. In fact, a rule-based response is typically executed by NPP operators for mainly two reasons: unknown situations are very unlikely to happen because of the high level of operator expertise due to exercises in simulators; on the other hand operators do not immediately respond to cues coming from the plant but they use a controlled mechanism before taking actions.

The modeling of a rule-based response is done by using a direct matching mechanism where a certain operator response (execution) is activated based on rules (Figure 3.3). The input from the plant activates a certain rule (Rule 2 in Figure 3.3). Based on the instructions in the selected rule, a certain execution is done. For instance, if the operators perceive that the subcooling margin in the plant is reaching zero, the execution could be to activate or increase the injection of water. The input-execution process is coded in the rule.

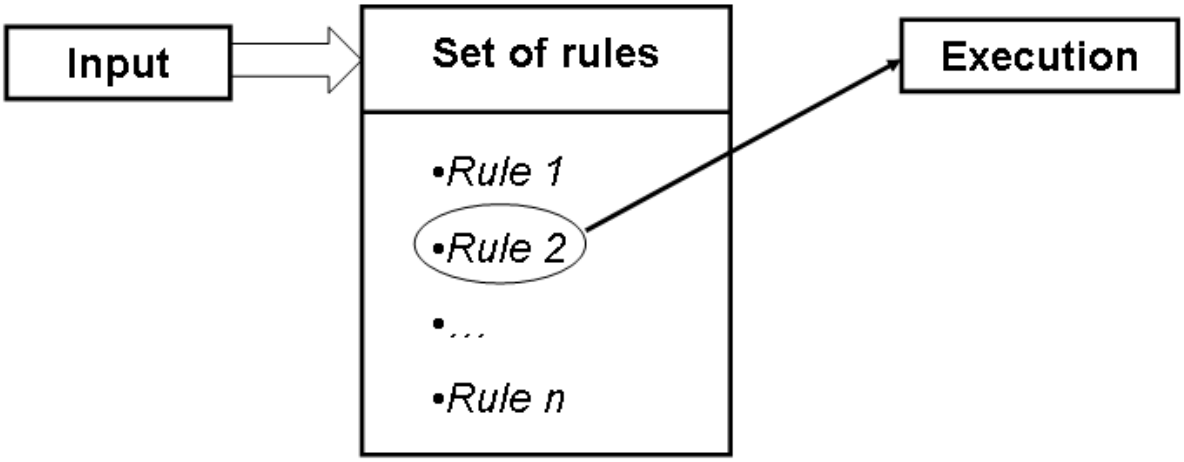



**Fig. 3.3:** Representation of the activation mechanism of rules. The perceived input activates a certain rule (Rule 2) and the execution is performed.

In general, rules are based on experience or can be based on mental procedures. Mental procedures are procedures which are memorized by operator due to their training. This means that operators know what they have to do following the procedure but not physically opening it but relying on their memory.

### 3.1.3 Crew model response

In this work, the crew model is composed by three operators:

- the decision maker (representing the shift supervisor). The decision maker is the operator who reads the procedure, manages the incoming information from the plant, and handles the response;

- the action taker (representing both the reactor operator and the auxiliary reactor operator). The action taker is the person who executes actions based on the input from the decision maker. The action taker is also able to process particular information in the same way as the decision maker (i.e., mainly checking the system information by himself/herself); and

- the safety engineer. The safety engineer is in charge of controlling the safety functions.

The flow of communication between decision maker, action taker, and plant is a loop as follow: decision maker –> action taker –> plant –> action taker –> decision maker (there is not the decision maker in case is the action taker who check the system information).

The inclusion of the safety engineer in the crew model allows the control of the safety functions which are important for the transfer to the Severe Accident Management Guidelines (SAMG). In fact, during the scenario evolution after IEs, the safety engineer has to continuously monitor the safety functions which have high priority. This means that as soon as they are violated according to plant-specific criteria, the operators have to stop the EOPs and they have to transfer to the SAMG. Even if the scope of this PhD work was the Level 1 PRA, this feature would allow the modeling of the operator response for Level 2 PRA extending the capability of the model.

The features introduced or further developed in the current crew model focus on the procedure-guided operator response model. The focus for the model development is the capability of using the ADS tool and the embedded crew model as a mean for obtaining HRA insights, i.e., how to use dynamic HRA models to improve the HRA as opposed to classical models, through a specific case study.

In order to explore different types of operator behaviors, a mechanism for crew variability has been developed. In particular, variability can be considered on the type of the operator response (start either one or two trains of a system), on the procedure steps to be followed, or on the response time. The crew model has a decision mechanism according to which strategies are decided based on the perceived information. This modeling of different decisions can be directly implemented in a DDET framework where different outcomes of an event can be followed.

### 3.1.4 Crew timing variability

In this PhD work an approach to deal with timing variability has been developed. In particular the approach is based on the concept of crew "tendency" which will be described in the next sections and it has been verified against a set of data from a NPP simulator study [Lois et al., 2008].

#### Performance time in DDETs

In a Monte Carlo framework, the time to perform a series of tasks is obtained by sampling from each of the distributions. The implementation of this approach in the DDET needs to address two related issues. The first is the appropriate discretization of the task distributions. Increasing the number of bins for each task distribution increases the number of branches, and by this the computation time. The second issue is whether there is an adequate representation of the "tails" of the distribution for a series of tasks or the overall task. Typically, there is interest in the probability of slow performances (long overall task durations) that may be "too late". However, fast performances may also be of interest because these crews may face (and/or contribute to) different scenario conditions; the corresponding scenarios may diverge from the typical scenario conditions and need to be analyzed.

Ensuring coverage of the tails requires that the Discrete Probability Distributions (DPDs) for task durations include bins towards the outliers (slow or fast values). Moreover, the scenarios involving slow (or fast) performance on several tasks may be truncated due to their low probability. Indeed, very slow and very fast overall performances are expected to be outliers. The challenge is to adequately represent these performances that are significantly faster or slower than the average, due to their relevance for safety.

### Performance time data

To determine the appropriate number of DPD bins for the performance time distributions of individual tasks and to evaluate the coverage of the time performances for the overall task, data from a NPP simulator study were used. The performance time values for two tasks were extracted and (continuous) probability distributions were fitted to this data.

**Individual task distributions** Similar to [Coyne and Mosleh, 2008] a Weibull distribution with scale parameter $\alpha$ and shape parameter $\beta$ is used to represent the time performance for each task. The Weibull distribution has been chosen because it is defined only for positive values and changing $\alpha$ and $\beta$ produces many shapes of distributions which can be used to fit the available data. For tasks defined at a level of detail appropriate for the analysis of NPP scenarios, a minimum value of the response time is suggested by the data and is consistent with realistic performance conditions and crew task loads. This minimum, which will depend on the task and context, can be modeled as an offset value. Table 3.1 summarizes the $\alpha$, $\beta$ and the offset values calculated from the available data.

The Cumulative Distribution Function (CDF) for the Weibull fit for Task 1 of the two tasks is shown in Figure 3.4, with and without the offset representing the minimum value. It can be seen that, without the offset, the distribution is shifted as a whole to the left and tends (in this case) to underestimate the probability of the longer performance times.

**Table 3.1:** $\alpha$ and $\beta$ parameters from the two task distributions.

| | $\alpha$ | $\beta$ | **Offset** |
|---|---|---|---|
| **Task 1** | 351s | 1.4 | 200s |
| **Task 2** | 301s | 1.7 | 200s |

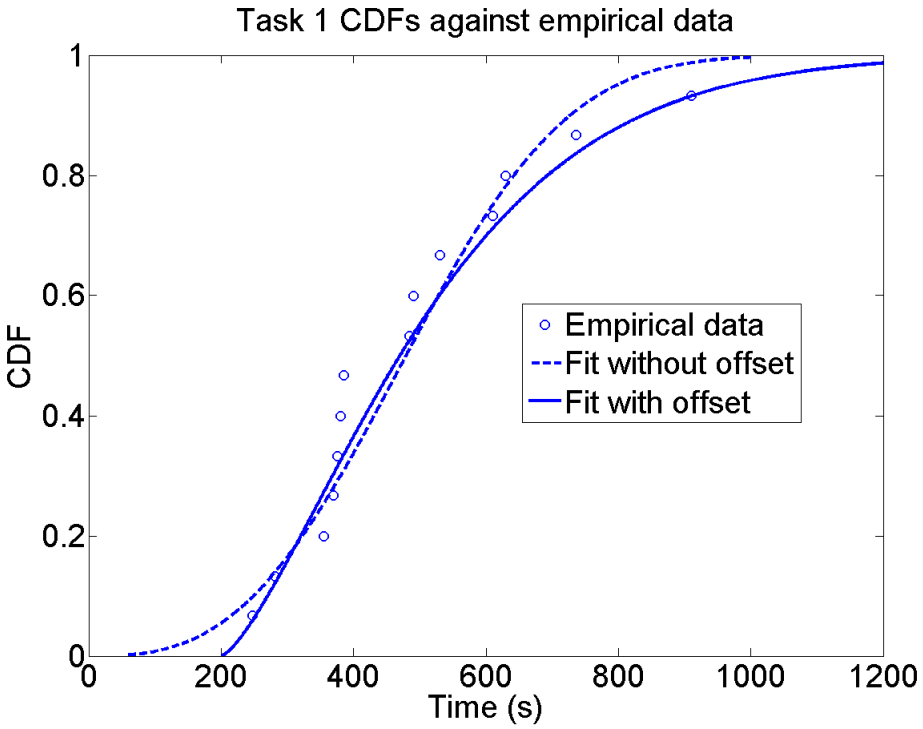



**Fig. 3.4:** Weibull fit of Task 1 performance time data. Empirical data from [Lois et al., 2008].

**Distribution for the overall or joint task** The DDET modeling of performance time variability includes the selection of the number of bins and the probability of the bins (equal probability bins or other alternatives). To verify that the DDET modeling is appropriate, a distribution for the performance time of the joint task is needed. The DDET treatment of time variability should reproduce this joint task distribution.

A distribution for the performance time of the joint task can be obtained empirically by adding the performance times of each crew for Task 1 and Task 2. An alternative is to generate the joint task distribution using the distributions of the individual tasks, since the number of performances (crews) is quite small. The MC approach was used to generate a joint task distribution. In this MC-based task simulation, only the distribution function of the crew response without considering the response of the plant is considered. The results plotted in Figure 3.5 show that the joint distribution obtained in this way significantly underestimates the probability of large performance times compared to the

empirical data.

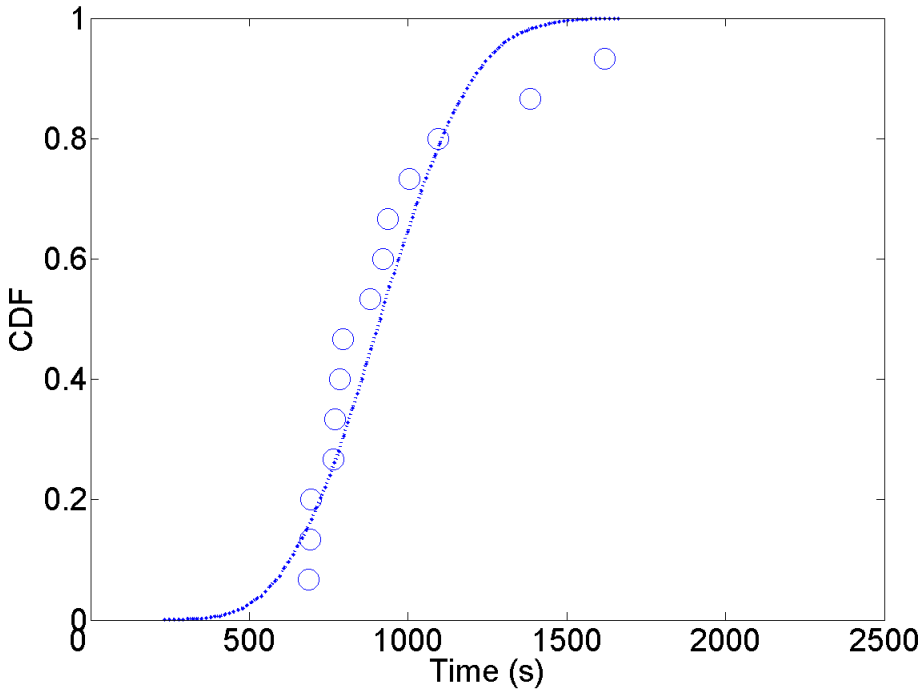



**Fig. 3.5:** CDF for the performance time of the joint task obtained using MC (dotted line) and empirical data (o) [Lois et al., 2008].

To determine whether the two outlier performances in the empirical data, shown in Figure 3.5, could be due to a correlation between the performance time of the first task and the second task, the empirical data were analyzed in terms of correlation. The data were first normalized using the Formula (3.1):

$$x_n = \frac{x - \mu_X}{\sigma_X} \tag{3.1}$$

where, $x_n$ = normalized data, $\mu_X$ = mean of the data set ($X$), and $\sigma_X$ = standard deviation of the data set. The correlation coefficient $\rho_{X,Y}$ of 0.61 supports that there is some correlation. In Figure 3.6, where the correlation between Task 1 and Task 2 is shown, it can be seen that this was particularly strong for the slow performances. In other words, the same crews produced the slowest performances.

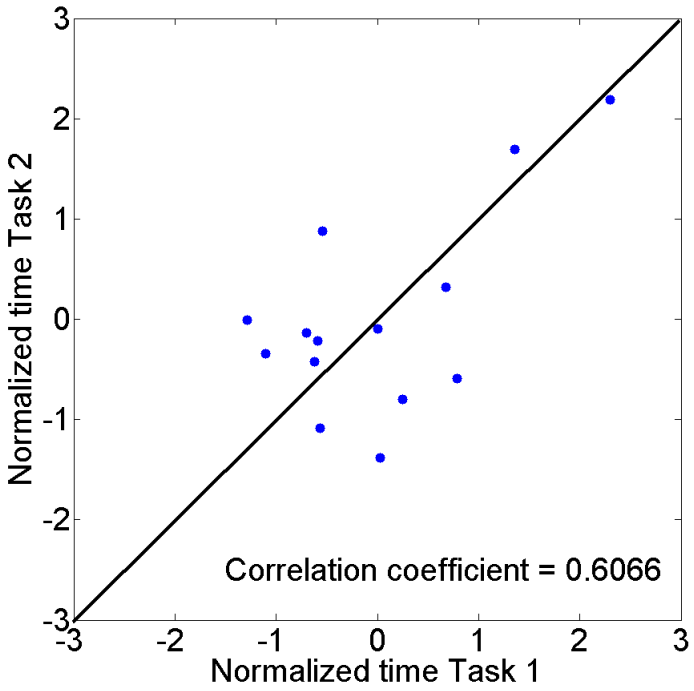



**Fig. 3.6:** Correlation plot between crew timing performance data of Task 1 and Task 2.

This cannot be generalized to conclude that those crews that are slow on the first task will always produce the slower performances on subsequent tasks (and conversely for the faster crews). On the other hand, sampling the performance times of the individual tasks independently ignores the correlation in the data. Independent sampling would tend to regress to the mean and underestimate the values towards the ends of the joint task distribution. Obtaining a correct distribution of the performance time for the joint task (or a series of tasks) requires that the correlation among the task performances is considered.

### Modeling the correlation in terms of crew tendencies

To represent the correlation, the time performance distribution for a single task was postulated to be a combination of sub-distributions, representing groups of crews.

To determine the parameters of the sub-distributions, the performance data were

analyzed further. First, the performance of each crew has been expressed as a percentile of the CDF for each task. This gives an idea about how each crew performs with respect to the other crews in the single task. These percentiles of the CDF for the two tasks were plotted, with the crews ordered based on the average of their percentiles on the two tasks, as shown in Figure 3.7. As was already seen in Figure 3.6, the two slowest crews produced the slowest performances for all tasks. However, this cannot be generalized, especially when the fast crew performances are considered. Many crews (4th, 5th and 6th) that are among the fastest on one task have a value significantly above the median on the other task.

Due to the correlation, the sub-distributions cannot be obtained by partitioning the data for individual tasks in terms of subgroups. Instead, the performances of the crews across the tasks have to be considered. The crews have to be grouped in terms of their overall performance (on all tasks) and task distributions are obtained for these groups.

Although the correlation among the fast performers is not as marked as it is among the slow performers, a group of fast crews was defined with the aim to have a general approach to treating the tendencies. In other cases, for instance, the fast crew performances may be correlated more strongly than the slow crew performances. In this case, the first three crews have been defined to define the fast tendency or group of crews and the last three as the slow group. The remainders have been considered as intermediate.

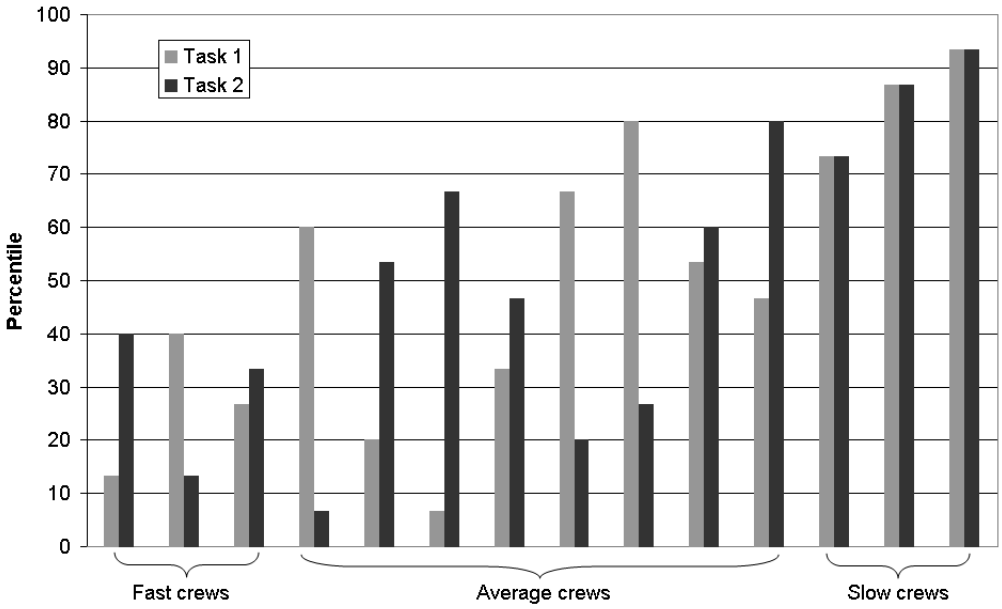



**Fig. 3.7:** Crew time performance on the two tasks, as percentiles of the CDFs for the individual tasks.

**Task time performance tendencies and sub-distributions** The sub-distributions for the three groups of crews or crew tendencies are obtained by fitting Weibull distributions to their task data. To obtain the sub-distributions, the performance data is partitioned according to the crew groups and fit separately. For instance, to get the $\alpha$ and $\beta$ for the fast distributions, data from the three fast crews have been used for each task. The same applies for the intermediate and slow distributions.

Figure 3.8 shows the resulting distributions for the tendencies compared with the overall distribution in terms of probability densities for Task 1. It can be observed that all three sub-distributions have substantial mass on the lower values, although the fast and intermediate groups of course have more mass there. Also, the slow group has a significant mass in the low end of the range whereas the fast and intermediate groups have no mass at the high end of the range.

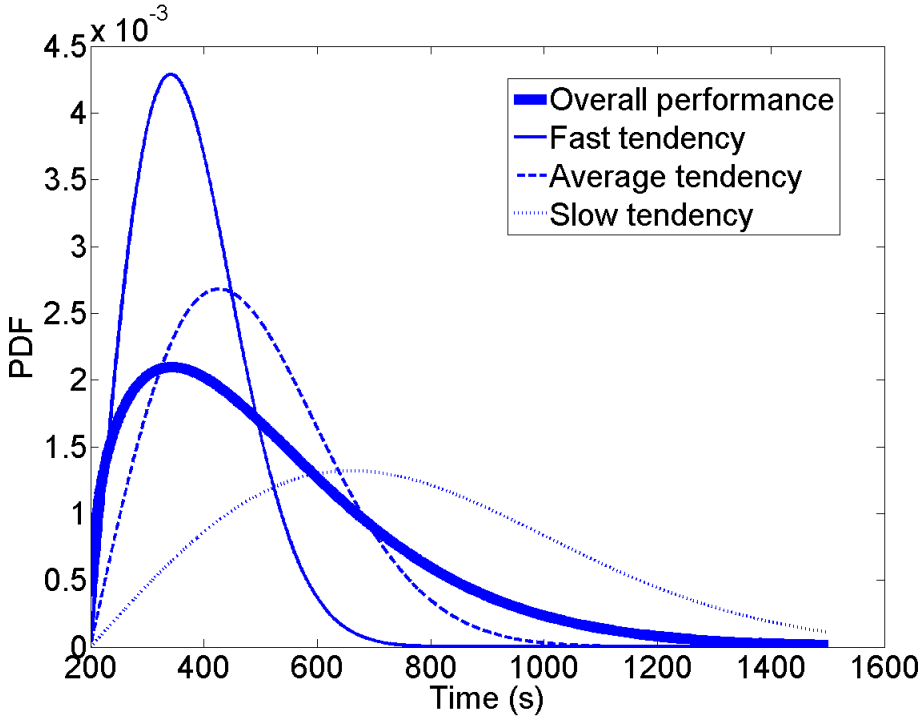



**Fig. 3.8:** Probability density functions (Weibull) for Task 1: overall distribution (thin full line) and decomposed into three sub-distributions representing the group tendencies.

The calculated $\alpha$ and $\beta$ parameters are shown in Table 3.2.

To verify that defining group tendencies and obtaining sub-distributions for the group, the performance of the overall task was simulated using the Monte Carlo task simulation approach at first.

To consider the tendencies in the MC task simulation, the performance of each group of crews on each task is separately sampled, analogous to a stratified sampling approach. In other words, the time performance distribution of the overall task is obtained for each group of crews (each tendency) separately, and the samples or results are weighted according to the distribution of the tendencies. The distribution of the tendencies (their weights) are the fraction of the crews assigned to the fast (0.214), intermediate (0.571), and slow (0.214) groups, respectively.

**Table 3.2:** Weibull parameters of the group sub-distributions for task 1 and task 2.

| **Task 1** | $\alpha$ | $\beta$ | **Offset** |
|---|---|---|---|
| Fast group | 200 | 2.0 | 200s |
| Intermediate group | 320 | 2.0 | 200s |
| Slow group | 650 | 2.0 | 200s |
| **Task 2** | | | |
| Fast group | 250 | 2.5 | 200s |
| Intermediate group | 220 | 2.0 | 200s |
| Slow group | 600 | 3.0 | 200s |

The sampling scheme based on crew tendencies and using the sub-distributions and group weights treats the correlation between the first and second tasks. Figure 3.9 shows the CDF for performance of both tasks obtained in this way and denoted "MC correlated". It can be seen that this treatment of the correlation between the tasks reproduces the data much better, throughout the range but especially in the upper tail. For comparison, the "MC uncorrelated" result, using a single distribution for each of the two tasks, is also shown (this is the result shown earlier in Figure 3.5).

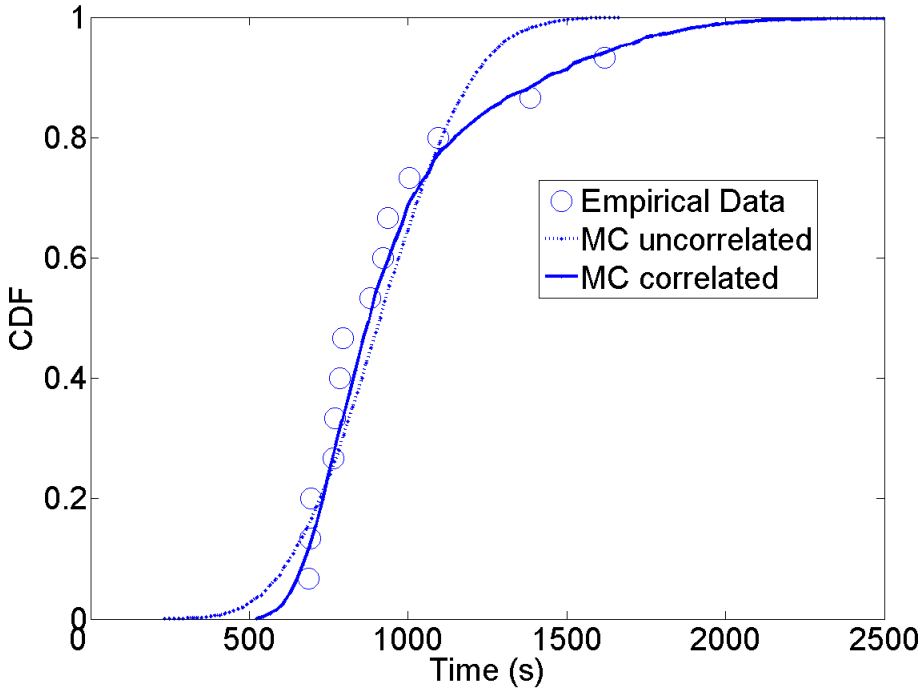



**Fig. 3.9:** Comparison between MC uncorrelated (dotted line) and MC correlated (full line) against empirical data (o).

**Treatment of the tendencies in the Dynamic Event Tree** The concept of grouping the crews in terms of tendencies can also be used in the DDET. In this case, the sub-distributions are discretized and represented as DPDs.

For each distribution, three equal-probability bins have been used. The mean performance time of the bin has been used as the characteristic value, i.e., the branching times. Table 3.3 summarizes the values for the "uncorrelated" approach that does not account for tendencies while Table 3.4 provides the characteristic values of the bins for the groups based on tendencies (the branch probabilities are always 0.33 for 3 equal-probability bins). An excerpt of the tree is represented in Figure 3.10. Only a few branches related to the fast, intermediate, and small tendency and the probability of each branch, the timing (not in scale), and the sequence probability are shown.

**Table 3.3:** Overall performance time distributions: characteristic values for the discretized probability distribution.

| | **Branching Point (BP)** | **Timing(s)** | **Branching probability** |
|---|---|---|---|
| **Task 1** | BP1 | 104 | 0.33 |
| | BP2 | 270 | 0.33 |
| | BP3 | 532 | 0.33 |
| **Task 2** | BP1 | 111 | 0.33 |
| | BP2 | 243 | 0.33 |
| | BP3 | 425 | 0.33 |

**Table 3.4:** Discretized performance time distribution characteristic values for Tasks 1 and 2.

| | **Group** | **Characteristic values** | | |
|---|---|---|---|---|
| **Task 1** | Fast | 85 | 167 | 268 |
| | Intermediate | 137 | 266 | 428 |
| | Slow | 278 | 541 | 870 |
| **Task 2** | Fast | 94 | 184 | 294 |
| | Intermediate | 127 | 216 | 316 |
| | Slow | 340 | 530 | 729 |

The results obtained considering the uncorrelated and correlated distributions are shown in Figure 3.11. The results are compared with the related results obtained by using a Monte Carlo approach. As one can see, the DDET-based task simulation results follow the same pattern as the MC-based task simulation results. The three discretized sub-distributions, (correlated distributions) approximate the MC correlated result quite well. This is also shown in Table 3.5 in terms of some of the key percentiles. In fact, comparing the percentile values between MC correlated and DDET correlated and between MC uncorrelated and DDET uncorrelated their values do not differ considerably.

In addition, when comparing the correlated results with the uncorrelated results the difference is quite important in particular at the $90^{th}$ and $95^{th}$ percentiles (slow performances). In fact, the difference between uncorrelated and correlated at the $90^{th}$ percentile is about 250 seconds and increases to about 380 seconds at the $95^{th}$ percentile. This means that in case of uncorrelated cases the underestimation of the slow crew performance is

quite important. Some difference can also be seen at the fast performances (about 50 seconds) even if not as high as in the slow performance part of the curves.

Since the distributions are discretized in three parts in case of DDET with uncorrelated distribution there are $3^2$ dots (Figure 3.11, '□') whereas in case of DDET with correlated distributions there are $3 \cdot 3^2$ dots (Figure 3.11, 'x'). It is worth noting that the 27 points in a DDET framework reproduce the overall crew performance.

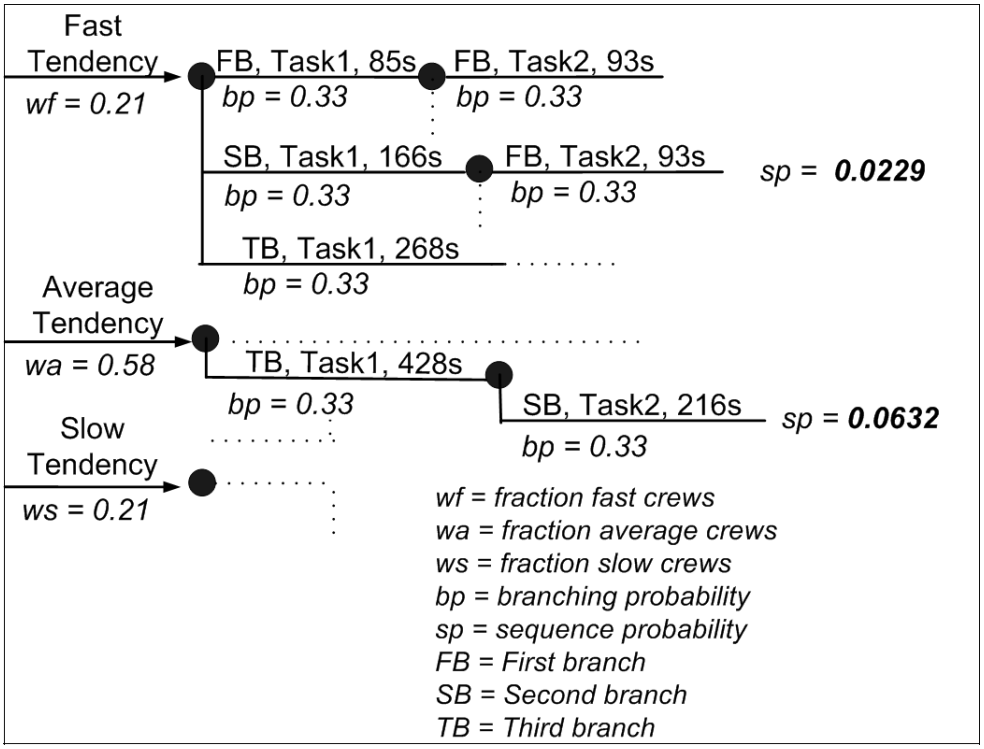



**Fig. 3.10:** Discrete Dynamic Event Tree based on fast, intermediate, and slow tendencies (excerpt).

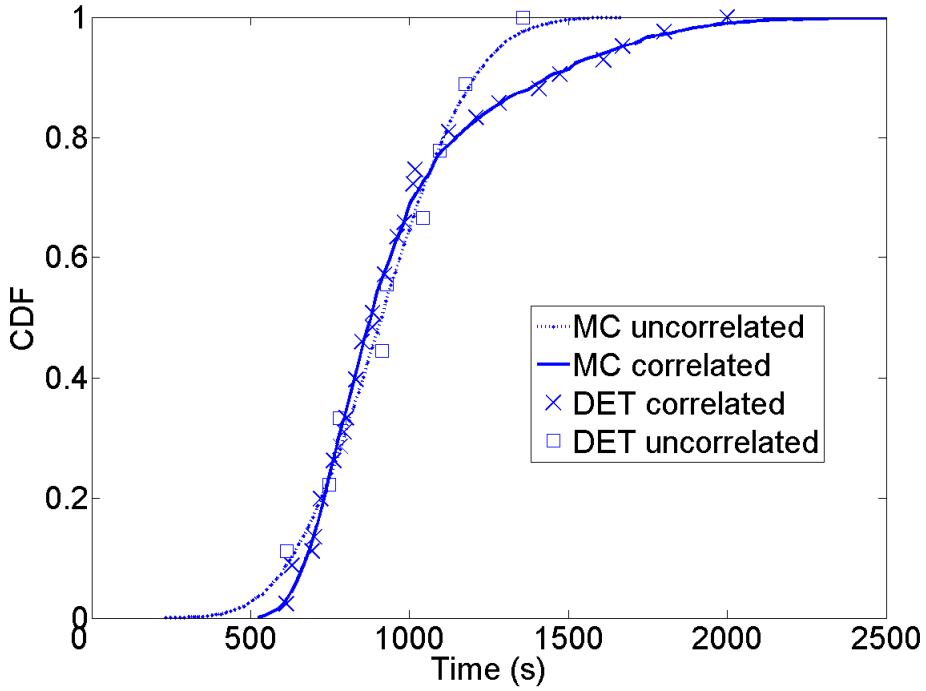



**Fig. 3.11:** MC-based uncorrelated simulation (dotted line), MC-based correlated simulation (full line), DDET-based uncorrelated simulation (□), and DDET-based correlated simulation (x).

**Table 3.5:** Set of percentiles for the uncorrelated and correlated MC and DDET approach.

| | $10^{th}$ | $50^{th}$ | $90^{th}$ | $95^{th}$ |
|---|---|---|---|---|
| **MC uncorrelated** | 628 | 912 | 1205 | 1285 |
| **DDET uncorrelated** | 604 | 920 | 1193 | 1275 |
| **MC correlated** | 676 | 879 | 1435 | 1662 |
| **DDET correlated** | 664 | 883 | 1459 | 1663 |

The results obtained so far demonstrate that the DDET-based task simulation methodology is able to represent the correlation between series of tasks and to generate the tail, i.e., extreme crew behaviors. In addition, it does so with far fewer samples than a MC approach. This methodology has been tested in the DDET framework in Section 3.3.

## 3.2 Implementation of the crew model

The crew model described in Section 3.1 has been implemented in ADS. ADS is a simulation environment whose main component is a DDET scheduler and where different operators or crew models can be embedded.

The ADS had been developed and improved since 1993. The first reference to ADS can be found in [Hsueh and Mosleh, 1993]. Then, in [Sheng and Mosleh, 1996], [Chang and Mosleh, 1999], and [Chang and Mosleh, 2006a,b,c,d,e] some developments of the conceptual model of ADS can be found. Finally, additional developments and application of the tool for safety analysis can be found in [Coyne and Mosleh, 2008].

The framework that the ADS tool implements is the DDET as described in Section 1.4.1. The ADS tool consists of six modules: Crew Module (modeling the response of the crew), System Module (modeling the plant response), Control Panel Module (modeling the control panel in the NPP control room), Hardware Reliability Module (modeling the component success/failure), Scheduler Module (monitoring the simulation evolution), User Interface Module (for the input setup and output analysis). A description of each module can be found in [Chang and Mosleh, 2006d].

Figure 3.12 shows the modules and the connection between them. The crew model can interact with the system model changing the boundary conditions through the control panel. Vice versa, the system model calculates the plant evolution which is an input to the crew model (i.e., it generates alarms, it changes control variables and parameter behaviors). The hardware reliability model generates hardware failures which can impact both the crew model and the plant model. The user model interface allows the interaction between the user and the simulation environment.

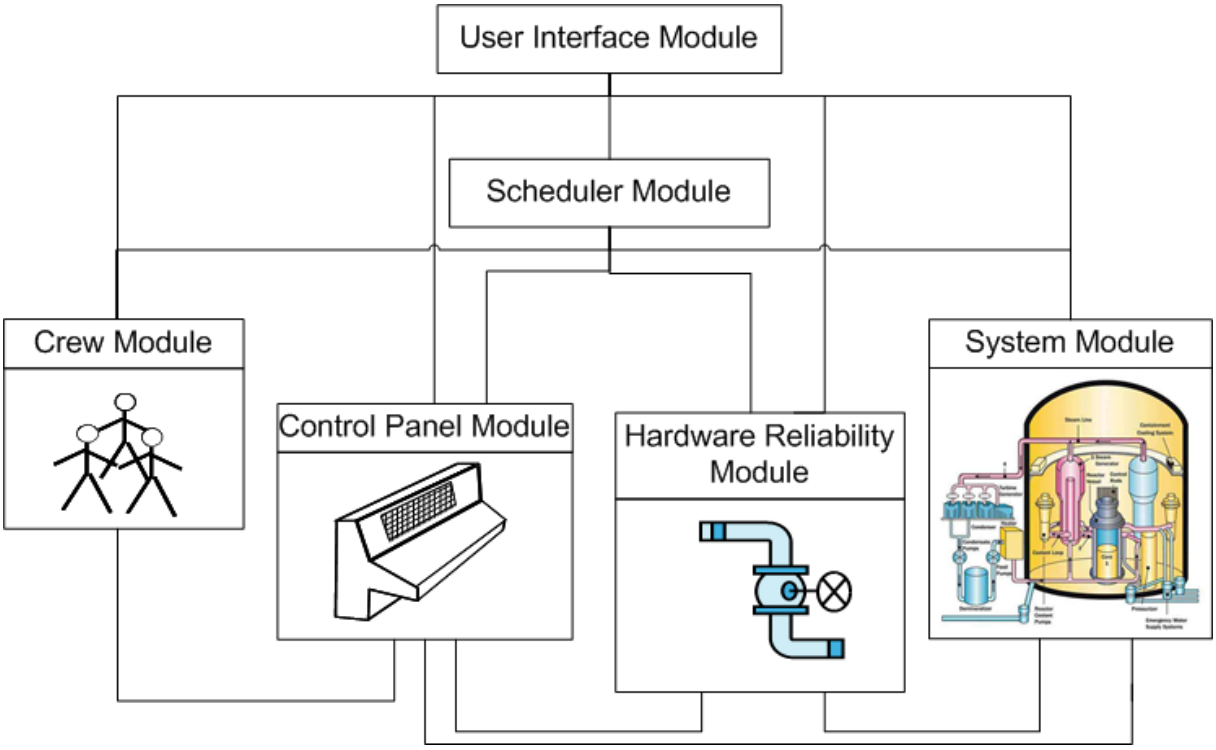



**Fig. 3.12:** High-level ADS framework.

The DDET simulation is performed and controlled by a scheduler (left hand side of Figure 3.13). The scheduler controls the module balances and the solution completeness with computational effort by focusing on certain sequences. During the simulation, component and operator state changes are permitted to occur at discrete branching points. State changes are modeled by generating one or more sequence branches at each branching point. Specific branching points and the number of branches generated at each branching point are defined by a set of analyst-supplied branching rules. Branching rules can be constructed to include sequence initiators, hardware and process variables, operatorsŠ actions, and software. A set of sequence termination rules are also identified to prevent excessive expansion of the DDET. The output of the ADS simulation is a DDET (right hand side of Figure 3.13).

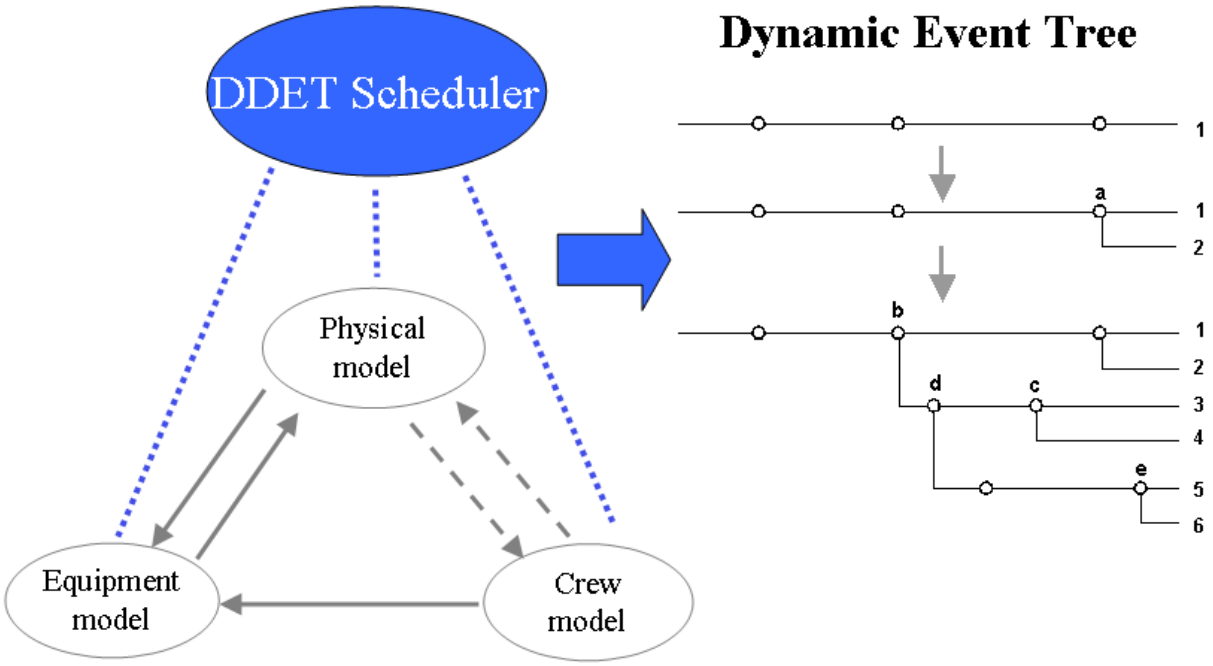



**Fig. 3.13:** DDET scheduler. The scheduler controls the simulation, i.e., interaction between physical model, crew model, and equipment model (left hand side), and produces a DDET (right hand side).

The System Module in ADS could be any thermal-hydraulic model. Currently, since the focus of the analysis is the Level 1 PRA and in particular the beginning of the scenarios, the thermal-hydraulic part is modeled by RELAP [RELAP5/MOD3.3, 2001]. The System Module of ADS can be adapted to a more versatile thermal-hydraulic engine, such as the TRACE or MELCOR code. A detailed description of the thermal-hydraulic of the case study will be described in Chapter 5.

A new structure of the input and output data was introduced to simplify the entry of input and to provide syntax-checking of the data. This has result in a big effort to make the tool easy to handle by the users and to reduce the possibility to make errors in defining the input parameters. In particular, a data structure based on the eXtensible Markup Language (XML) has been implemented. The representation of the input with the XML structure has introduced a high level of flexibility of the computerization process, a good capability of input visualization, and a capability of input control based on a validation

mechanism within the language.

The implemented crew model is based on four main parts in order to model the procedure-guided operator response behavior: procedures, rules-of-behavior, time variability, and branching point generation.

### 3.2.1 Implementation of procedures

The main structure of the use of procedures by the operators is based on the following model of procedures. The procedures can be activated by alarms, predefined rules, or from the cognitive model. Usually, the emergency procedures are the first activated and they could be for example activated by the alarm of low pressurizer level. Once the procedures are activated, the operator starts to read the first procedure, analyzes the procedure step, and checks whether is an action, an action sequence, or an if-struct. In case of action, the operator executes the action based on the available time (given as input). If there is a sequence of actions the operator executes them sequentially. In case of if-struct, first the operator checks whether the conditions (expectations) are verified and then performs the "then". Conditions are verified by checking parameters or alarms. If the conditions are verified, the "then" part which could be an action or a sequence of actions is executed. If the conditions are not verified a transfer to another procedure step is done. Usually, the last instruction of the procedure step is an action on the plant. Once the action is executed, the operator waits the response from the plant and then the next procedure step is selected.

The procedure execution continues until the time windows for the simulation is achieved or the last procedure is performed.

The previously described structure has been embedded into the ADS tool. The advantages of this procedure representation and structure can be summarized as:

- user friendly interface in adding procedures and procedure steps,;

- validation and control of the added procedures and procedure steps (due to the XML structure);
- flexibility in adding new procedures and procedure steps; and
- possibility to add different types of procedures beyond the EOPs, like normal procedures, abnormal procedures, SAMG, and safety functions (the latter have been implemented in the case study).

### 3.2.2 Implementation of the rules-of-behavior

Following the pattern developed for the procedure representation, also the rules-of-behavior structure has been modified and merged to the previous one. The rules-of-behavior are a direct matching between cues and actions. As soon as a certain number of rules (defined by the user) are activated the action is executed.

The main elements of a rule-of-behavior are: an activation time, a reset time, a branching probability, a set of rules, and a $m$-out-of-$n$ structure for the rules. The activation time tells the code the timing for the operator to check the rules. The reset time tells the tool the amount of time that the rule-of-behavior must be activated. The branching probability can be set less than one if the user wants to model the fact that the operator follows o not the rule-of-behavior (success and failure paths). The set of rules are conditions that the operator has to verify in order to see whether they are true or not. For example, if the condition is "primary temperature less than 100 °C", the operator has to check whether it is true or not. If $m$-out-of-$n$ rules are true, the rule-of-behavior is activated and the execution is performed. The latter is integrated in the $m$-out-of-$n$ structure.

### 3.2.3 Time variability

The time variability method is used for the identification and calculation of the characteristic points of the task distributions where there is timing variability in the crew response. For example, different crews execute the same task in the procedure in different times. The distribution of the crew response can be handled with the time variability method.

The identification of the characteristic values is done based on the distribution of the duration of the task to be analyzed. The calculation is done outside the DDET-framework and it will be used during the post simulation phase for the calculation of the probabilities. In ADS basically, only the duration of the times is given for the three selected characteristic points and the propagation of the probabilities in the tree is done after the simulation.

The analyst therefore, based on the task duration, identifies three characteristic times when the action can be taken based on the time variability method (Section 3.1.4). Then, the post-processing analysis recalculate the probabilities (4).

### 3.2.4 Branching generation

In the current crew model, branches can be generated due to procedure step skipping. The probability of skipping procedures and/or procedure steps was based on an input value of probability judged by the analyst. The feature was then improved by the University of Maryland adding the calculation of the probability based on a Beta distribution. A similar mechanism of branching generation has been also included in the current crew model.

With regard to the procedure-guided response, the possibility to generate branches due to procedure action time has been included. In this way, the analyst can select the number of branches (usually three) to follow based on different times to perform the procedure step within the task. This allows the variability in the crew response. In fact, for certain

important procedure steps or tasks different crews perform in different way in terms of timing. The timing and probability of the crew response is given considering available data. The user inputs the time to perform the procedure step and the probability (based on HRA data).

With respect to hardware components, an additional way to generate branches has been added. The new way allows the possibility to generate branches when considering components that can have different levels of operations. For instance, some valves can be opened at 100%, 50% or at any other level. The analyst can select the levels of operation that the component can work and the respective probability and ADS generates branches as soon as the criterion is met.

In addition branches can be generated as soon as an expectation within the procedure is met. When performing procedure steps, sometimes the operators have to meet some criteria in order to perform the action(s) according to the procedure step. In the latest version of ADS branches can be generated introducing different criteria for performing actions. For example, if the procedure step says that they have to stop the component A if the level of the water in another component is greater than X, then we can generate branches having other values in addition to X. This permits to add a model of interpretation of procedure step based on current understanding on the scenario evolution.

## 3.3 Test of the timing variability for the current crew model

The methodology so far described has been applied in the ADS in order to represent the timing variability of the crew response. The basic idea is to identify the three sub-distributions related to the fast, slow, and intermediate behavior of the crews from the available data on the crew performances to achieve different tasks.

The methodology is applied in three steps. First, before running the simulation, the

tasks considered for modeling the crew variability must be identified incorporating the importance of the tasks. For example, in tasks where checking and monitoring are the main actions, no timing variability is considered; it is assumed that all the crews perform the same due to the easiness of the task. However tasks where operators have to take actions on the plant or make procedure transfers timing variability is considered. Generally, the variability is considered only at the last procedure step in the task. Then, still before running the simulation, the estimation of the timings and probabilities based on available data and expert judgment is done. This means that the analyst identifies the distribution function, i.e., a global Weibull distribution which is able to fit the available data. Once identified the distribution, the analyst calculates the timings and the probabilities depending on the number of branches to be generated.

Second, the simulation is run considering the branching probabilities equal to 1 and the timings calculated in the first phase. In this way, the simulation is able to explore all the possible paths due to the different branching points. The correct branching probabilities will be calculated in the next phase. Probabilities equal to 1 allow avoiding truncations which can happen if the original distribution is used (since the correspondent branching point probability is less than one). On the other hand, it is necessary to recalculate the branching point probabilities after the simulation (next step) in order to consider the type of crew, i.e., fast, slow, or intermediate.

The third step is performed after the simulation. In this phase, the correct distribution function is applied to the calculated event tree. In this phase, the three sub-distributions are applied in the previous calculated branching points in order to get the results of the fast, intermediate, and slow crew behavior. The resulting probability distribution functions are then combined to obtain the global distribution function according to the developed methodology.

The last two steps will be better described in Section 4.1 where the way to handle the probabilities in the DDET of ADS will be presented.

This methodology has been applied for a simplified small LOCA scenario for a three-

loop Pressurized Water Reactor. During the scenario, the crew model has been implemented. In particular, operators are instructed to monitor and take actions according to the procedures and their experience. If all the systems and components are available, the main actions they have to perform to handle the scenario are: cooldown the plant at 100 K/h, control the steam generator levels with the emergency feedwater pumps, start the spray to increase the level of the pressurizer, stop the pressurizer sprays as soon as a certain pressurizer level is reached, and stop one by one the High Pressure Injection pumps (HPIs) if there is enough subcooling margin.

In this test of the methodology, only a few branches have been considered. In particular timing variability in transfer from the post accident procedures to small LOCA procedures (in 10s, 300s, 600s, and 1200s), variability in stopping the last high pressure injection pump (400s and 1200s), and pressurizer level value to stop the first time the sprays (3, 5, and 9 meters) have been modeled. The simulation has been stopped after the first 12000 (about 2.5 hours) seconds or when the plant reaches low pressure conditions (10 bars) and the Low Pressure Injection pumps start. Table 3.6 summarizes the numerical values which have been used in the construction of the probability functions for the two timing variability branching points. With regard to the last branching points, i.e., stop the pressurizer spray at 3, 5, and 9 meters the three probabilities used are: 0.2, 0.6, and 0.2.

**Table 3.6:** Values of Branching Point (BP) times and probabilities used in this case study for timing variability.

| | **Intermediate Crew** | | **Slow Crew** | | **Fast Crew** | |
|---|---|---|---|---|---|---|
| | Time | Probability | Time | Probability | Time | Probability |
| **BP1**[a] | 10 | 0.5 | 10 | 0.2 | 10 | 0.01 |
| | 300 | 0.39 | 300 | 0.3 | 300 | 0.1 |
| | 600 | 0.1 | 600 | 0.3 | 600 | 0.39 |
| | 1200 | 0.01 | 1200 | 0.2 | 1200 | 0.5 |
| **BP2**[b] | 100 | 0.8 | 100 | 0.5 | 100 | 0.2 |
| | 1000 | 0.2 | 1000 | 0.5 | 1000 | 0.8 |

[a]Transfer from the post accident procedures to small LOCA procedures.
[b]Stop the last high pressure injection pump.

Two examples of outputs, the cumulative probability distribution function when the flow of the HPIs is zero and when the accumulators start have been calculated. These distributions have been compared with the probability distribution functions in case of considering only the original distribution function. In latter case, the branching probabilities used for the transfer to the small LOCA procedure is 0.25 for each of the four branches, whereas the branching probability of stopping the last HPI pump is 0.5 for each of the two branches. Finally, the probability of stopping the first time the pressurizer sprays is like in the other case 0.2, 0.6, and 0.2 for each of the three branches. Figure 3.14 and Figure 3.15 shows the results of the two cumulative distribution functions in case of original distribution (□) and in case of calculated distribution function (o).

The results follow the same pattern as in the MC-based and DET-based task simulations. The calculated CDFs have a higher value at the beginning and lower value at the end in both cases. The approach of dividing the original distribution in three sub-distributions, i.e., fast, intermediate, and slow allows better represent the tails in particular to model those behaviors which are outliers in term of performance. In addition, considering this way of sampling, the correlation between series of tasks is considered; with the idea of tendency, if the crew has performed in the previous one as fast it will most likely perform as fast in the subsequent task. Without considering the correlation between tasks, the information about the type of crew is lost because each time the crew is considered performing always as intermediate crew.

One of the advantages of the developed methodology is a better representation of the typical crews' response during accidents. In fact, as the HRA data have demonstrated, there is some correlation between series of tasks which somehow must be incorporated into the DDET framework when modeling the crew-system interaction. The methodology developed in this PhD work is able to model and to better represent the crew response and in particular the variability of the responses of different crews.

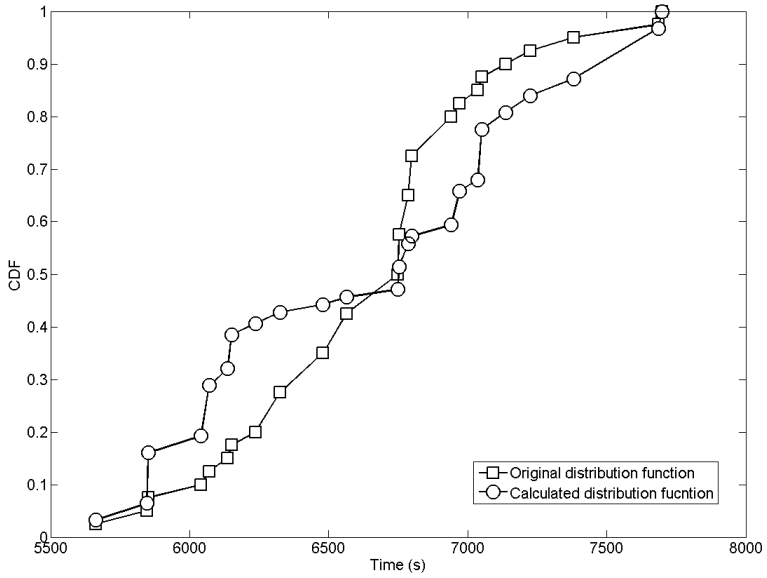



**Fig. 3.14:** Cumulative distribution functions of when operators stop last HPI pump: original distribution (□) and calculated distribution function (o).

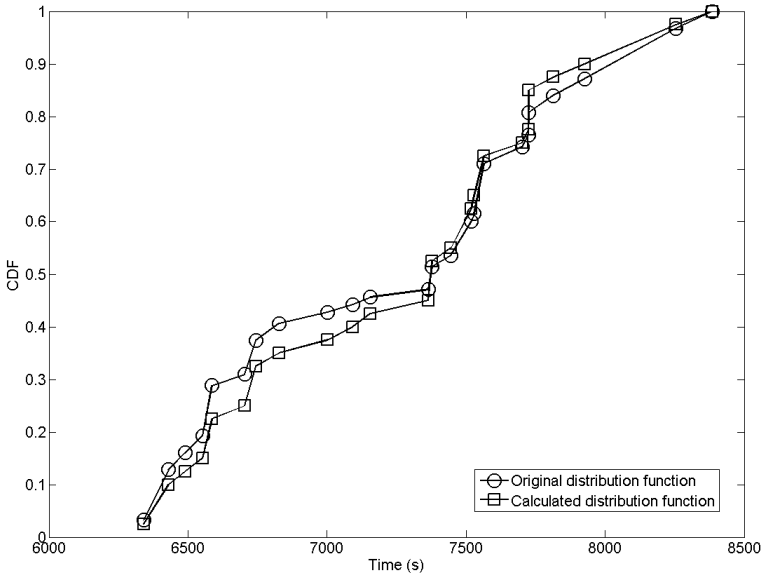



**Fig. 3.15:** Cumulative distribution functions of when operators start the accumulators: original distribution (□) and calculated distribution function (o).

## 3.4 Summary

In this Chapter, the model of crew response has been presented. Developing a crew model is an important step for a correct and realistic representation of the crew response during accidents in a NNP. Especially, the crew model will be used for the assessment of the human errors during accidents, the evaluation of the effects on plant behavior parameters, and as a tool to obtain HRA insights through the dynamic simulation and comparison with classical static risk assessment methods.

The development of the conceptual crew model has been presented focusing on the type of operator response, i.e., procedure-guided response and on the main features included (procedures and rules-of-behavior). Then, the crew has been introduced. The crew is based on a decision maker, an action taker, and a safety engineer who has high priority in the decision and execution. Next, during the development of the crew model, an approach to deal with the crew timing variability in the DDET framework has been developed. The approach, based on the concept of tendency, is based on the assessment of the probability density functions to be used for the calculation of the branching point timings and for the calculation of the DDET branching point probabilities. The validation of the tendency approach has been done through a comparison between MC and DDET results.

The conceptual model is the basis for its implementation in the ADS tool. First, a short description of the ADS tool has been introduced along with the implementation of the conceptual crew model. Then, the development of the current crew model has been presented focusing of the new features and capabilities introduced with this PhD work. In the new crew model, based on a procedure-guided operator response, a new procedure and rules-of-behavior concept and representation have been developed. In addition, new branching generation channels have been added in order to enhance the crew model capacity, i.e., a procedure step skipping mechanism, the procedure step timing variability (executing the action in the procedure at different times), different level of operations of hardware components (e.g., open a valve at 50%, 90%, or 100%), and

different expectations within procedures.

Finally, a trial SLOCA test case study has been performed to test the model and the timing approach.

## Chapter 4

# Dynamic Event Tree scenario analysis

## Contents

In this Chapter, a new way of calculating DDET probability is presented in Section 4.1. Then, in Section 4.2, an approach to identify and classify scenarios generated in a DDET analysis is described. The tools for the classification of DDET scenarios are presented in Section 4.3. Afterward, the approach for the output analysis is described in Section 4.4. Next, Section 4.5 deals with the problem of stratification of the input due to the amount of simulation data to be processed. Finally, Section 4.6 provides a summary of the arguments presented.

## 4.1 Calculation of probabilities in DDETs

In the DDET framework of ADS, the calculation of the probabilities has been shifted after the simulation of the crew-system interaction. The basic idea is to allow the tool to model any type of crew (in terms of performance) using only one DDET simulation. In this way, the approach developed during this PhD for the probability calculation in the DDET allows reducing the computational effort since only one time the simulation is run. This allows also the possibility of easily updating the probabilities as soon as new HRA data are available without re-running the DDET.

The approach consists of setting to 1 the branching probabilities due to human events, like for example crew timing variability. In this way, ADS can follow and model all the possible paths due to human events avoiding truncation problems. Then, after the simulation, the probabilities of each sequence are recalculated depending on the type of crew the analyst wants to consider. In case of slow crews, the calculated branching probabilities will be skewed towards slow behaviors while in case of fast crews the branching probabilities will be skewed towards fast behaviors. The branching probabilities are calculated after the simulation according to the approach described in Section 3.1.4.

A tool that automatically calculates the branching probabilities has been developed and first tested on the test case study (Section 3.3) and then applied to the case study described in Chapter 5. Figure 4.1 visualizes the way in which the probabilities are

calculated in ADS. As an example, only one task and two crews (slow and fast) are considered. The timing branches for the task are three, i.e., fast response, intermediate response, and slow response. The simulation is run once using some predefined timings for each branch and probabilities equal to 1. Then, after the simulation, the probability of each sequence is recalculated considering the fact that each considered sequence comes from a fast crew (sub-DDET 1 in Figure 4.1) or a slow crew (sub-DDET 2). As one can see, for the sub-DDET 1 the probability of a fast response is higher than intermediate which is higher than slow (0.7, 0.2, and 0.1 respectively). Whereas for the DDET 2 the probability of a slow response is higher than intermediate which is higher than fast (0.6, 0.3, and 0.1 respectively). In order to calculate the total probability of each sequence, the previously calculated probabilities must be multiply by the fraction of fast and slow crews. That is, the resulting sequence of the DDET is the weighted sum of each corresponding sequence in each sub-tree. For instance, the probability of sequences 1 is equal to $w_f \cdot Pseq_1$ + $w_s \cdot Pseq_1$. The same applies for the other sequences. The resulting probabilities for each sequence (labeled SP in Figure 4.1) are then the correct probabilities that take into account the distribution of the operator response in time and the fraction of each type of crew.

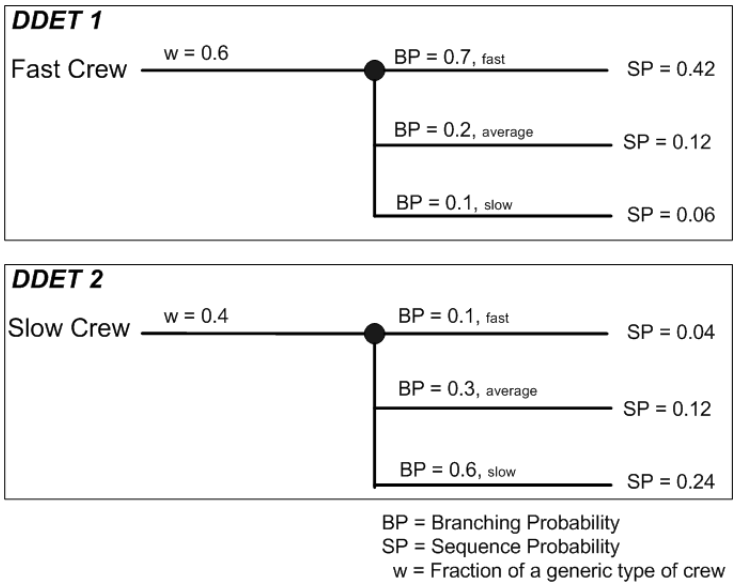



**Fig. 4.1:** Example of two DDETs based on fast (upper side) and slow crews (lower side).

## 4.2 Classification approach

A challenge arising from dynamic approaches to PSA is that the number of scenarios to be analyzed is much larger than that of the classical fault/event tree approaches, so that the a posteriori information retrieval can become quite burdensome and difficult [Labeau et al., 2000]. Additionally, since no minimal cut sets are generated, it is impractical to acquire information on dominant scenarios and important systems, components, or human actions. In order to overcome these difficulties, a method to identifying and grouping the scenarios of a dynamic safety assessment, with the aim of finding the principal patterns of system evolutions towards failure [Mercurio et al., 2008] and [Podofillini et al., 2010] is proposed. The scenarios are grouped combining information of the end state, events sequence and process variables evolutions. A classification algorithm is the basis of the grouping approach and it is mathematically described in Appendix B.

Dynamic approaches bring some clear advantages from the point of view of the completeness of the analysis and of the information content made available. First, there is potential for the identification of accident scenarios which may have been overlooked by the analyst when building the accident sequence models at the basis of the fault/event trees. Second, conservative simplifying assumptions made by the analyst, for example on the evolution of some process parameters, can be relaxed as the process evolution is simulated directly by the underlying dynamic models. Third, the identification and grouping of scenarios of failure or close to failure can give insights for HRA analyses. Finally, additional informative content becomes available as a result of the dynamic analysis, in the form of time-dependent probability density functions of components states and process parameters values. In this respect, the amount of information retrievable from dynamic methodologies, in terms of number of scenarios and probability distributions, can be overwhelming and generally calls for a significant effort in the post-processing phase [Labeau et al., 2000].

Indeed, while the typical outcome of the dynamic safety analysis is the time evolution

of the probability of the process variables exceeding pre-defined safety threshold, the focus is mainly on the system and process states at the end of the scenarios, with limited use of the information contained in the actual evolution towards these states. On the contrary, proper use of the information on the evolution of the scenarios can provide significant safety insights on the dominant scenarios with respect to the criticality and efficiency of the protections designed to counteract them. In this context, some performance risk metrics may be computed and in addition some dynamic contributions to the end state can be characterized like events and dominant contributors to the end state, causes and mechanisms which are relevant to the end state. This framework is a first step towards the quantification of important events leading to a particular end state or in other words prime implicants.

The problem of identifying critical scenarios in dynamic reliability studies has been recently studied in [Demmou et al., 2004], where the stochastic aspects of the system evolution are represented by means of Petri nets. The method proposed in [Demmou et al., 2004] is based on the identification of the transitions through which a final state of interest can be reached. It is a qualitative method: the scenario probability does not enter in the search scheme. In addition, the problem of grouping similar sequences with respect to the process variables evolution is not addressed.

Within a DDET simulation framework for dynamic safety analysis, the information on the evolution of the system is hidden in the simulated branches. Among these branches, there are sequences that reproduce qualitatively similar behaviors in terms of the evolution of the physical parameters and of the sequences of events, mainly differing for the actual timing at which these occur. Other sequences may instead differ in behavior, because characterized by different combinations of occurred events, and still reach the same final outcome state. Hence, the difficulty in identifying and grouping similar scenarios is in the fact that sequences composed of similar events can correspond to rather different process parameters evolutions and, possibly, end states, depending on the events timing or order of occurrence. Therefore, grouping the scenarios only on the basis of the occurred events

and end states may be misleading and accountancy of the physical behavior of the process variables ought to be included [Labeau et al., 2000].

## 4.3 Post-simulation data analysis tools

The ADS tool, generates as output a DDET as described in Section 1.4.1. In particular, the main component of the output is a set of accident scenarios composed by the time evolution of events that have occurred during the scenario evolution. These events can be grouped into three types as summarized in Table 4.1.

**Table 4.1:** Typical output events from dynamic analysis

| **Type of output** | **Events** |
|---|---|
| Plant behavior | - parameters<br>- rates<br>- signals<br>- control variables |
| Operator actions | - cognitive states<br>- rules-of-behavior<br>- mental belief<br>- actions in procedure steps<br>- conclusions/decisions/strategies |
| Plant events | - alarms<br>- automatic system actions<br>- component states |

All these events make up the data set that can be used for the output analysis. It is worth to mention that the amount of DDET-generated data can be very large because of the level of modeling of the human-system interactions. This has been the main motivation of the development of tools and strategies for the output analysis. The analysis is done with a classifier and parser described in the following sections.

### 4.3.1 The scenario classification approach

The classification tool is based on a clustering algorithm which takes into account not only the final system states but also the timing of the events and the process evolution. The classifier is a tool able to identify the geometric partition of the patters[1] to be classified based on some training scenarios or data given to the tool. The training of the tool is done considering a set of known scenarios from previous analysis, generally from databases, or form expert judgment. The idea is therefore to use these scenarios to build up groups in a $n$-dimensional space and to classify new scenarios in the identified groups. In addition, scenarios not belonging to the identified groups are labeled as unknown or unforeseen and they are further analyzed to identify the reasons of not belonging to any group. It is worthwhile to mention that the number of training patterns is not fixed but the analysts, based on his/her experience, can identify the minimum number of patterns necessary for the training phase. In general, at least two patterns per group are necessary to train the tool even if a number larger than two would help the identification and construction of a better partition.

The underlying idea of the approach proposed in [Mercurio et al., 2008] is to group the DET-generated scenarios in classes or groups[2] of "similarity", by combining information from both the event sequences and the patterns of evolution of the process variables.

In all generality, this leads to a task of pattern classification, i.e., the partitioning of objects into classes. Often in engineering, the complexity of the problems forces one to resort to empirical pattern classification techniques in which an algorithm is built through a process of learning based on a set of patterns labeled with the class they belong to. This kind of techniques is termed "supervised" and the available pre-classified data are termed "training" data [Zio and Baraldi, 2005a]. In the case here considered, the objects to be

[1] A pattern is any variable which could represent some characteristics of the considered component or system. In this context a pattern is a $n$-dimensional signal whose components are the parameters' evolutions at a fixed time. For example, if a scenario is based on Temperature1, Pressure1, and Pressure2 behaviors (3-D signal), the pattern is a 3-D point whose components are Temperature1, Pressure1, and Pressure2 at a given time.

[2] In the context of scenario classification, class and group have the same meaning.

classified are the DET scenarios and the basic steps for their classification are sketched in Figure 4.2.

The first step is the a priori identification of the anticipated scenario classes for the system under analysis and of the relevant classification features. The scenarios will eventually be classified as belonging to a particular class based on the affinity of their features to those characteristic of the class. Scenario classes should distinguish different reference scenarios that the system is expected to follow in its evolution. They must be defined a priori on the basis of available knowledge on the system operation. For example, in the system presented in Section 4.3.2, three classes of scenarios are expected: *1*) the nominal operative scenarios; *2*) scenarios involving the non-automatic startup of the High Pressure Injection (HPI) system; and *3*) scenarios involving both the non-automatic startup of HPI pumps and the failure of a Turbine Bypass Valve (TBV). The identification of the features relevant to the classification is necessary to condense the scenario description into an object vector $\vec{x}$, i.e., the pattern to be fed to the classification function. The features can be either binary or continuous variables. Binary variables characterize the scenarios based on the occurrence or not of certain events, for example the intervention or failure of a safety system; continuous variables characterize the scenario based on the evolution of the process variables.

The successive steps of the procedure are typical of a supervised classification scheme: training of the classifier on patterns of known classes and test of the classifier on new patterns. As for the classification technique, an evolutionary possibilistic FCM classifier paradigm is used in this work. An important asset of this technique is related to the use of the possibilistic classifier for recognizing unanticipated scenarios, referred to in the following as "unknown", i.e., patterns of evolution that were not foreseen as reference in the a priori analysis and thus do not fall in any scenario group. The evolutionary possibilistic FCM classifier filters them out avoiding that they be misclassified as known scenarios and, more importantly, revealing new dynamic failure patterns that were not identified in the a priori analysis. The identification of new, unforeseen evolutionary

patterns completes the analyst knowledge on the system with information on unexpected failure scenarios and may aid to suggest additional and more effective safety-oriented improvements of the system.

The procedure for constructing the evolutionary possibilistic clustering algorithm is composed by a possibilistic clustering algorithm that finds the geometric clustering in the feature space based on a Mahalanobis metrics. Then, if the obtained clustering partitions are not close to the physical classes, the Mahalanobis matrix is updated using an evolutionary fuzzy C-Means algorithm [Zio and Baraldi, 2005a]. The optimal metrics thereby obtained are then used for the classification problem [Yuan and Klir, 1997]. Once the scenarios are classified properly, the probability of each class can be estimated and the dominant evolutionary patterns identified, in terms of both failure events sequences and process variables evolutions. A description of the algorithm can be found in Appendix B and in [Mercurio et al., 2008].

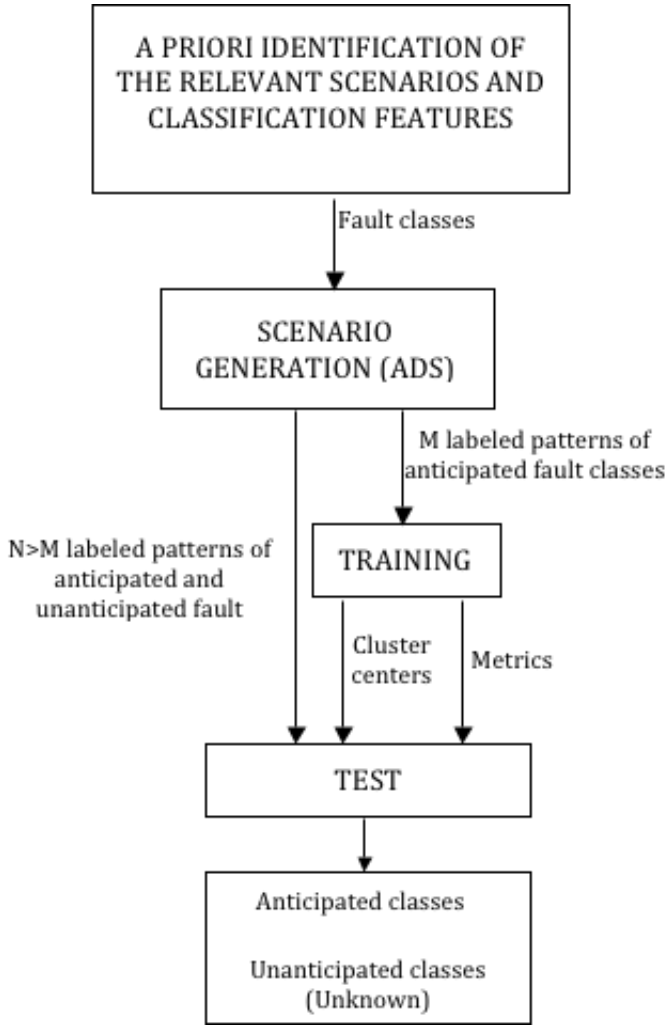



**Fig. 4.2:** The scenario classification approach.

### 4.3.2 Test case study - SGTR event

The classification approach has been tested on a test case. The scenario analyzed is a SGTR of a two-loop Pressurized Water Reactor (PWR) as described in Appendix E.

#### Branching generation

The ADS is used to generate the DET that develop from the SGTR initiating event. The frequency of the IE is 0.005/y. The simulation covers the first 2000 seconds (about 33

minutes) after the IE. The branching points and the corresponding branching probabilities are listed in Table 4.2. Branching points correspond to hardware failure events as well as to human failure events.

Concerning the hardware failure events, the failure on demand of the HPI automatic start up and the failure on demand of the TBV of loop A (TBVA) are modeled. Concerning human action events, the following types of interactions are modeled: cognitive actions (i.e., failure to perceive that the pressurizer level is below the lower threshold and failure to manually start up HPI pumps); delay in following a mental procedure (turn HPI pumps on when the pressurizer level is below the lower threshold) as well as a written procedure (SGTR procedure step 7.4); checks on the status of a system (i.e., check if the HPI pump is automatically started and in the negative case manually re-start it).

Except for the human actions listed in Table 4.2, the outcome of all the other human actions mentioned previously is assumed to guarantee success. Similarly, all other components and systems involved in the SGTR event except for the HPI pumps and the TBV are assumed to work as designed.

As already described, during the simulation of each branch, the branches probabilities are updated based on the branching point probabilities. The branches are truncated (i.e., the simulation of the branch is interrupted and the ADS moves on to simulate the next branch) when their probability is below a threshold value of $1.0 \cdot 10^{-9}$.

At the end of the simulation, ADS generated a total of 60 branches (i.e., scenarios to be classified).

**Table 4.2:** Branching points considered in the SGTR event model.

| | **Branching point** | **Probability**[1] |
|---|---|---|
| Hardware Failure Events | - Non-automatic start up of HPI | 0.01 |
| | - TBVA failure | 0.01 |
| Human Failure Events | - Failure to perceive that pressurizer level is below the lower threshold | 0.2 |
| | - Failure to manually start up HPI | 0.4 |
| | - Delay (40 s) to turn on HPI when the pressurizer level $<$ 200" | 0.3 |
| | - Delay (20 s) to carry out SGTR procedure step 7.4 (maintain pressurizer level $>$ 80") | 0.3 |
| | - Failure to check if HPI has automatically started and in the negative case manually start it | 0.2 |

**A priori identification of the anticipated scenarios and relevant classification features**

Three classes of scenarios are identified a priori:

- **class 1**: nominal scenarios, with all components and operators' actions successful;
- **class 2**: scenarios with HPI failure to start on demand and success of the TBV of loop A; and
- **class 3**: scenarios with HPI failure to start and stuck open TBV of loop A.

Figure 4.3, Figure 4.4, and Figure 4.5 show the behaviors of three relevant process variables (the reactor cooling system pressure, the steam line pressure, and the steam generator level) representative of the three scenario classes. The HPI activation signal is generated on low RCS pressure. At around 115 seconds, the reactor trips and the RCS pressure immediately decreases. In case of successful HPI start (class 1 in Figure

[1]Although the probability values have not been validated, in practice they are regarded as credible values which can be used to apply the proposed classification methodology.

4.3), the RCS pressure recovers until the operators reach the depressurization step in the corresponding EOP and perform it accordingly (around 900 seconds), using the pressurizer spray system. The level in SG A increases (Figure 4.5) due to the RCS-to-secondary side leak (note that the uncontrollable rise in the level in one SG is one of the cues for diagnosing the SGTR event).

In case the HPI fails to start (classes 2 and 3), the operators are directed by the EOPs to start it manually. In case the operators succeed to manually start the HPI, the scenario evolves as class 1; in case of failure, the RCS pressure continues to decrease (Figure 4.3, classes 2 and 3). The pressure decrement in the RCS is faster in case of the stuck open failure of the TBV (class 3), which also causes the drop in the secondary side pressure (Figure 4.4).

In case of HPI failure, the level in the ruptured SG remains lower than in case of HPI success (classes 2 and 3 compared to class 1 in Figure 4.5). It is also interesting to notice the saw-tooth behavior of the SG level in Figure 4.5, which results from the intermittent functioning of the emergency FW system for SG level control. Scenarios are classified based on the instantaneous values of the triplet of process variables:

1. RCS pressure
2. Loop A Steam Line (SL) pressure
3. Loop A SG level

As previously mentioned, the DET generated 60 scenarios. The patterns to be classified are triplets of values of the mentioned variables, taken every 5 seconds along the evolution. Therefore, every scenario is converted into 400 patterns (if the simulation is not interrupted earlier than 2000 seconds because the truncation probability threshold is reached). This entails that the classification of the scenarios, which is made on the instantaneous pattern, is time-dependent. It can be foreseen that at early stages in the transient, the classification will be poor since the scenarios belonging to the three classes

have similar characteristics (note that up to the HPI branching point all scenarios are perfectly overlapped). On the other hand, it is expected that the scenario classification will be more solid as the transient progresses and the scenarios features become distinct.

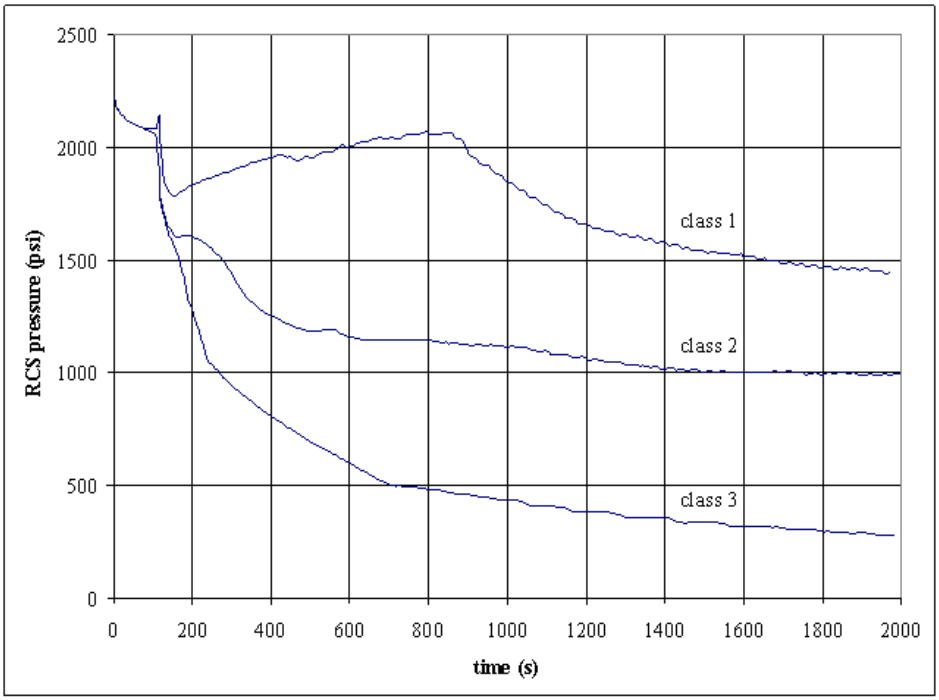



**Fig. 4.3:** Behavior of the RCS pressure for class 1, 2 and 3 scenarios.

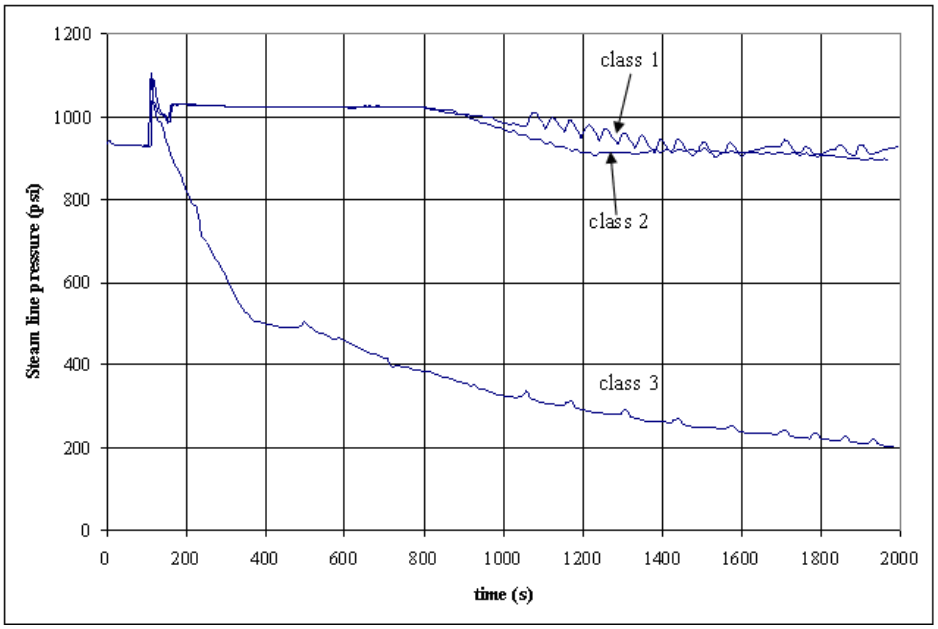



**Fig. 4.4:** Behavior of the steam line pressure for class 1, 2 and 3 scenarios.

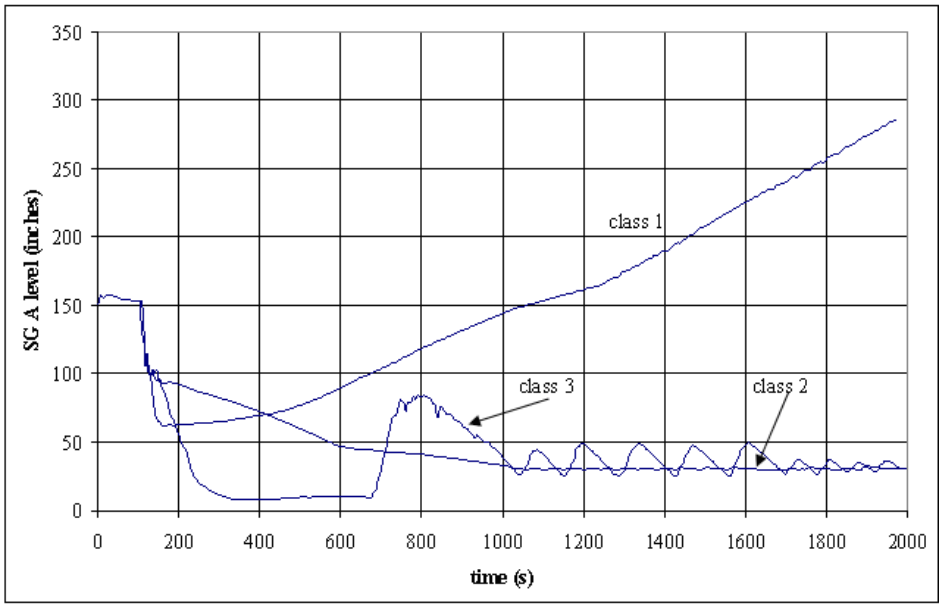



**Fig. 4.5:** Behavior of the steam generator A level for class 1, 2 and 3 scenarios.

**Scenario classification and scenario analysis**

The main outcome of this step is the grouping of the sampled scenarios in the three a priori defined classes and the identification of unanticipated scenario classes that were possibly left out in the a priori identification of relevant scenarios. These latter unanticipated scenario classes will be referred to as "unknown".

This procedure can be subdivided into two steps:

1. Training of the possibilistic evolutionary FCM classifier on the basis of a set of the nine labeled scenarios (three evolutions for each one of the three process variables) representative of the three classes. This amounts to a set of 9*400 labeled patterns, each one constituted by a triplet of values of RCS pressure, SL pressure and SG level at a given time, and the integer label of the corresponding scenario class.

2. Use of the possibilistic and fuzzy classifiers to classify the 60 DET-generated scenarios. The search of the optimal membership functions has been done setting the value of the degree of fuzziness $r_m$ to 2.0, which means a low degree of fuzziness in the resulting partition. The possibilistic evolutionary FCM procedures are fed with the above labeled patterns to identify the centers and metrics of the clusters in the three-dimensional space.

The second step of the procedure entails that the 60 DET-generated scenarios be fed into the possibilistic evolutionary FCM classifier for the scenario classification. Results are shown in Figure 4.6, Figure 4.7, and Figure 4.8. The upper part of the Figures shows the membership values assigned to the scenarios of a given class (e.g., class 1 for Figure 4.6) to that specific class (i.e., the correct class 1), as a function of time. The lower part of the Figures shows the membership values assigned to the other two classes (i.e., the incorrect classes 2 and 3). The Figures confirm the good performance of the classifier, which produces high values of membership to the correct class and low values of membership to the incorrect classes.

Figure 4.6, Figure 4.7, and Figure 4.8 show that in all the three cases the possibilistic evolutionary FCM classifier is able to recognize the correct class in the mid-late part of the scenario. In fact, at the beginning of the scenario (until about 100 seconds) the process behavior is in practice the same for the three classes (Figure 4.3, Figure 4.4, and Figure 4.5), therefore the classifier has no elements to classify the scenarios into the correct class. The early stage of any scenario is usually assigned to class 1 (upper part of Figure 4.6, and lower part of Figure 4.7, and Figure 4.8) because this class covers better the features of the early scenarios, i.e., "high" values of RCS pressure, SL pressure and SG level (Figure 4.9). After about 100 seconds the correct scenario classes start to be identified, as their characteristic features become distinguishable.

It is interesting to note that a number of class 1 scenarios have low membership value at the beginning of the scenario, around 500 seconds (Figure 4.6, upper part). These are scenarios in which the HPI failed to start up on demand and the operators were successful to start it manually, as they are instructed to do by procedures. The behavior of the RCS temperature for this type of scenarios is shown in Figure 4.10. The earlier stage of the scenario is similar to class 2 scenarios (HPI failed), thus explaining the rather high values of membership to class 2 (lower part of Figure 4.6). After the operators have recovered the HPI, the scenarios proceed as those of class 1 (Figure 4.10). Accordingly, they are recognized as such by the classifier (the membership to class 1 returns high and that to class 2 drops to zero).

Figure 4.8 shows that the membership values of class 3 scenarios drop between about 800 and 1000 seconds, then restoring back to high values. This can be understood by looking at the behavior of the SG level for class 3 scenarios in Figure 4.5. In the mentioned 800-1000 seconds time window there is a rise in the SG level before the Emergency Feed Water (EFW) control brings the level down to below 50". The level increment carries the patterns away from the cluster centers, thus making the classification more problematic. These patterns can be identified in the far right side of Figure 4.13, which shows the projections of the clusters onto the features planes.

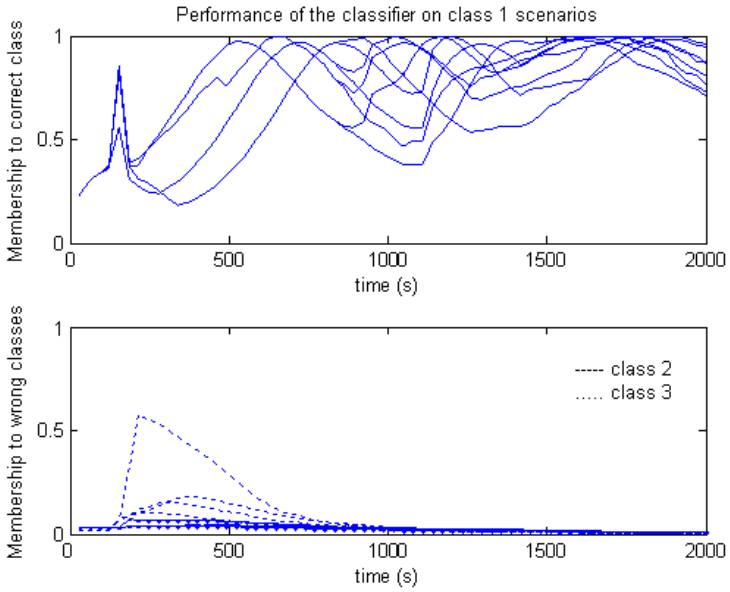



**Fig. 4.6:** Performance of the classifier on class 1 scenarios. Upper plot: membership to the correct class 1; Lower plot: membership to the wrong classes 2 and 3.

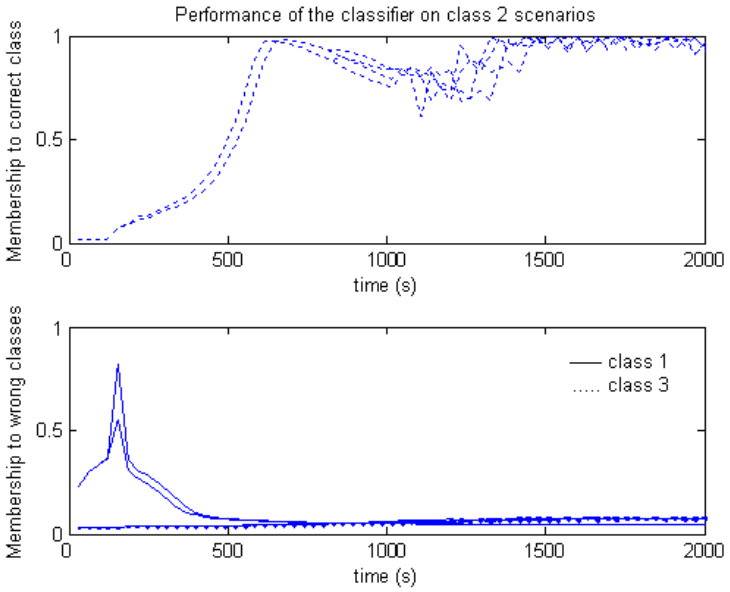



**Fig. 4.7:** Performance of the classifier on class 2 scenarios. Upper plot: membership to the correct class 2; Lower plot: membership to the wrong classes 1 and 3.

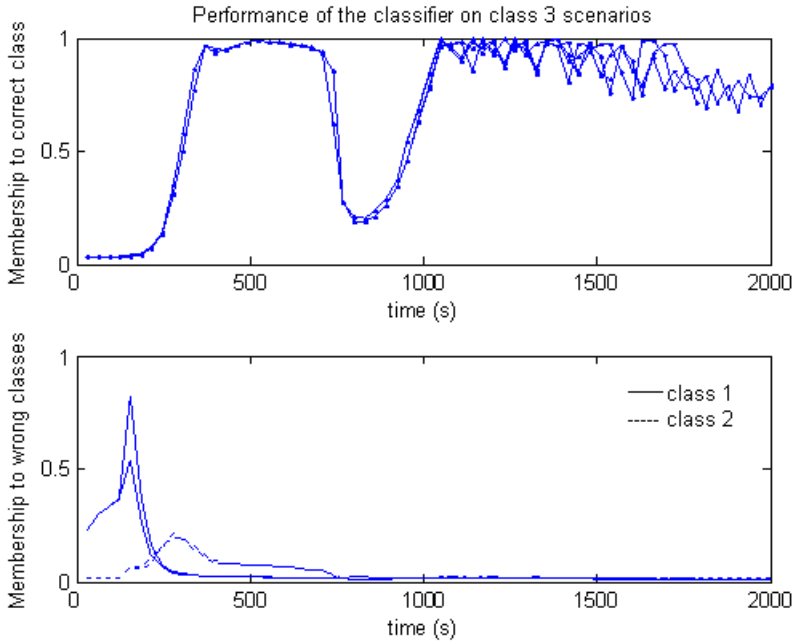



**Fig. 4.8:** Performance of the classifier on class 3 scenarios. Upper plot: membership to the correct class 3; Lower plot: membership to the wrong classes 1 and 2.

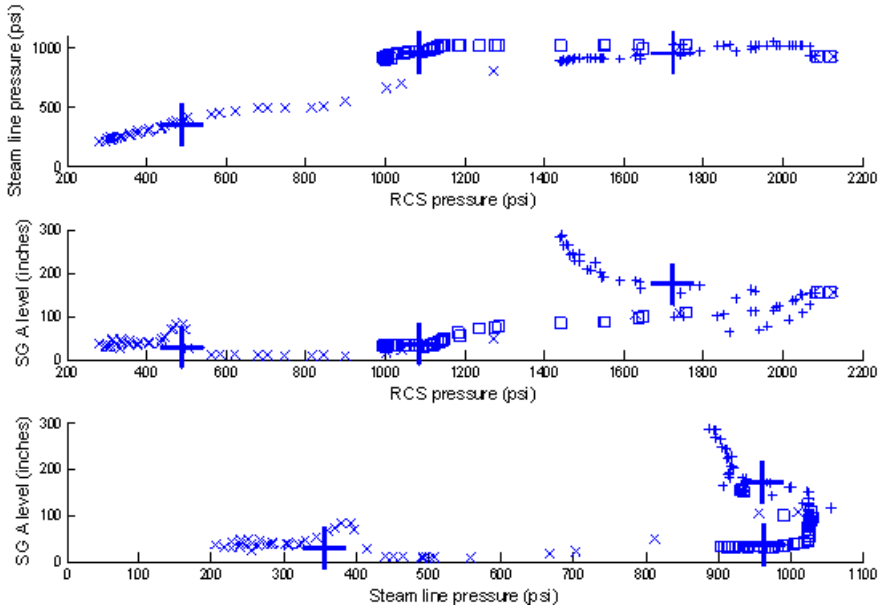



**Fig. 4.9:** Position of the patterns belonging to class 1 (+), class 2 ([]), class 3 (x) and position of the corresponding cluster centers (+).

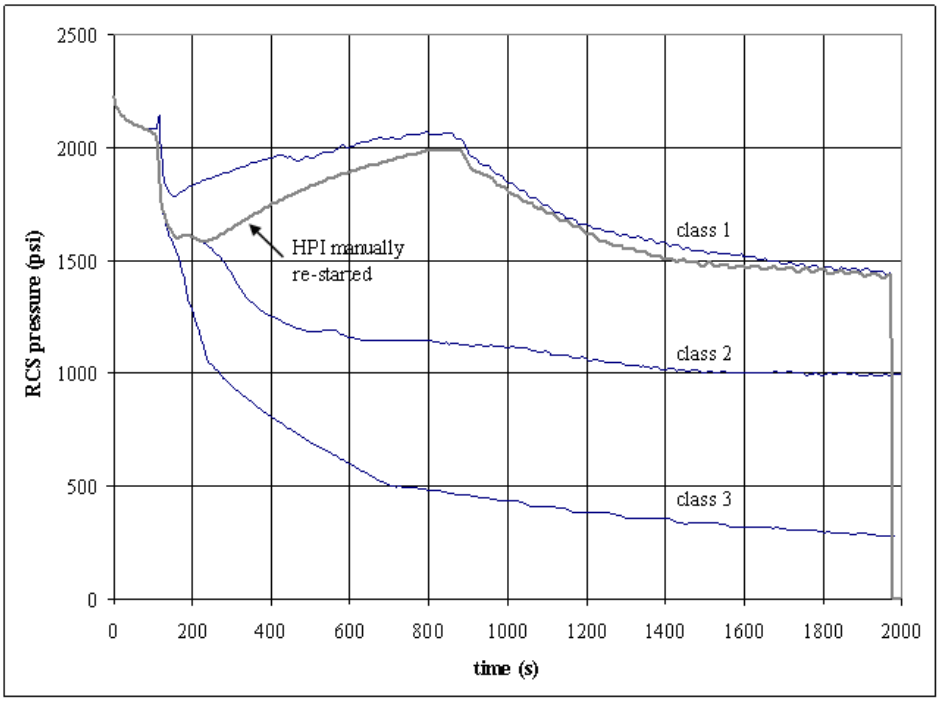



**Fig. 4.10:** Evolution of the RCS pressure: effect of manual HPI start on class 1 scenarios.

### Analysis of the "unknown" scenarios

The possibilistic evolutionary FCM classifier identified 18 scenarios as unknown. Their membership values are shown in Figure 4.11. It can be seen that these values are not large for any of the available classes: membership to class 3 has the highest values, ranging within 0.2 and 0.5, while those to the other classes are in practice zero.

The events that lead to these scenarios have been analyzed a posteriori and it was found that they are characterized by failure of the loop A TBV, with correct functioning of the HPI. Figure 4.12 shows the behavior of the RCS pressure for these scenarios. The evolution is rather similar to that of class 3 scenarios, and in practice coincident up to about 600 seconds after the IE. This explains the large values of membership to class 3 up to about 600 seconds and why these scenarios still maintain some degree of membership to class 3 at later times. Figure 4.13 shows the position of the unknown patterns as compared to class 3 patterns, further confirming that the features of class 3 and unknown

patterns are rather similar.

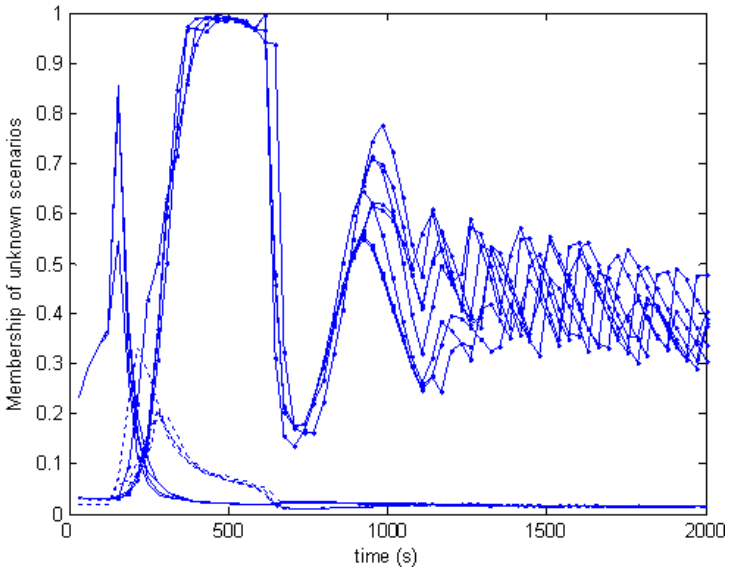



**Fig. 4.11:** Performance of the classifier on "unknown" scenarios: (-) membership to class 1, (–) membership to class 2, (.-) membership to class 3.

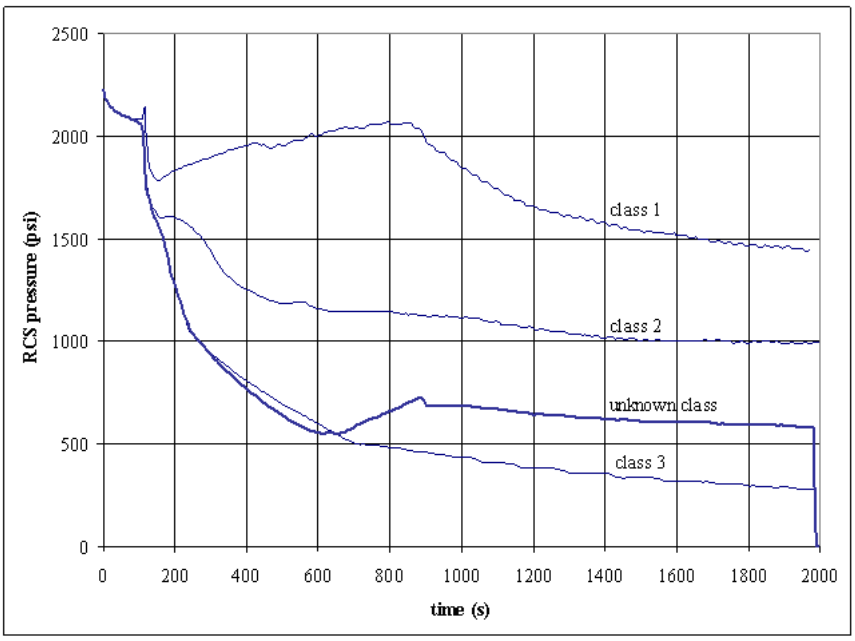



**Fig. 4.12:** Evolution of the RCS pressure for classes 1, 2, 3 and "unknown" scenarios).

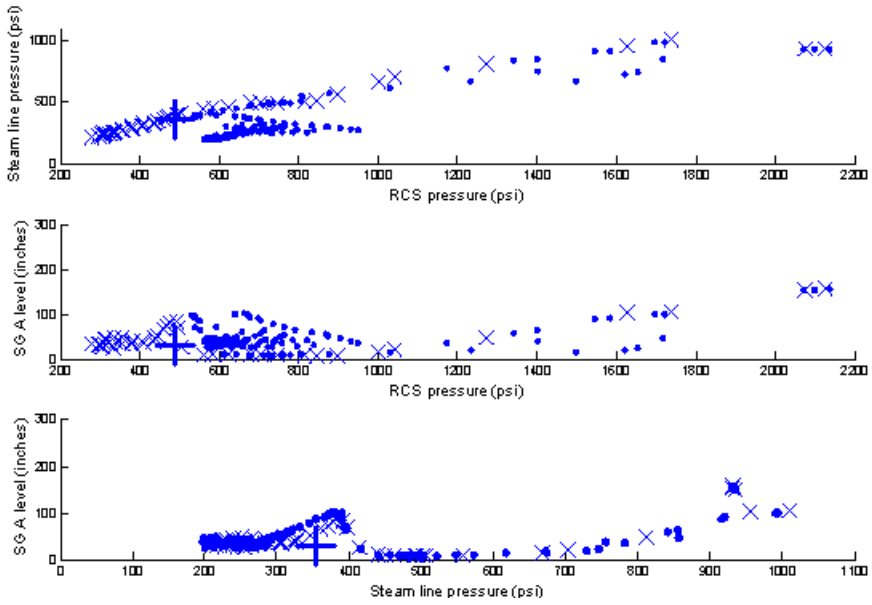



**Fig. 4.13:** Position of the patterns belonging to class 3 (x) and unknown (.) and position of the cluster centers (+).

### 4.3.3 DDET parser

Within the scope of this PhD work, a DDET parser has been developed in order to better handle the DDET-generated output scenarios. The main idea behind the DDET-parser is the reduction of the amount of information to be handled by the analysis. In fact, the output of ADS is a series of DDET sequences where all the information about the events occurred during the scenario evolution are saved as displayed in Figure 4.14. This makes the analysis and the understanding of the DDET extremely difficult and complicated. Therefore, a tool able to parse and reduce the information in the DDET has been considered important and necessary for the output analysis of the DDET-generated scenarios.

In Figure 4.14 a snapshot of a DDET sequence is depicted. In particular, for the beginning of the sequence 1 only four elements ("Hardware Reliability", "Alarm", "Goal", and "Alarm") are shown with their respective characteristics like, the identifier ID, the time when the event has happened, and some features of the event. For example, for

the "Hardware Reliability" element, the sender and the receiver of the events are shown, the component and control name, the functional state, and the probability are included. For the other elements, some other information is included. Notice that also the current probability is shown.

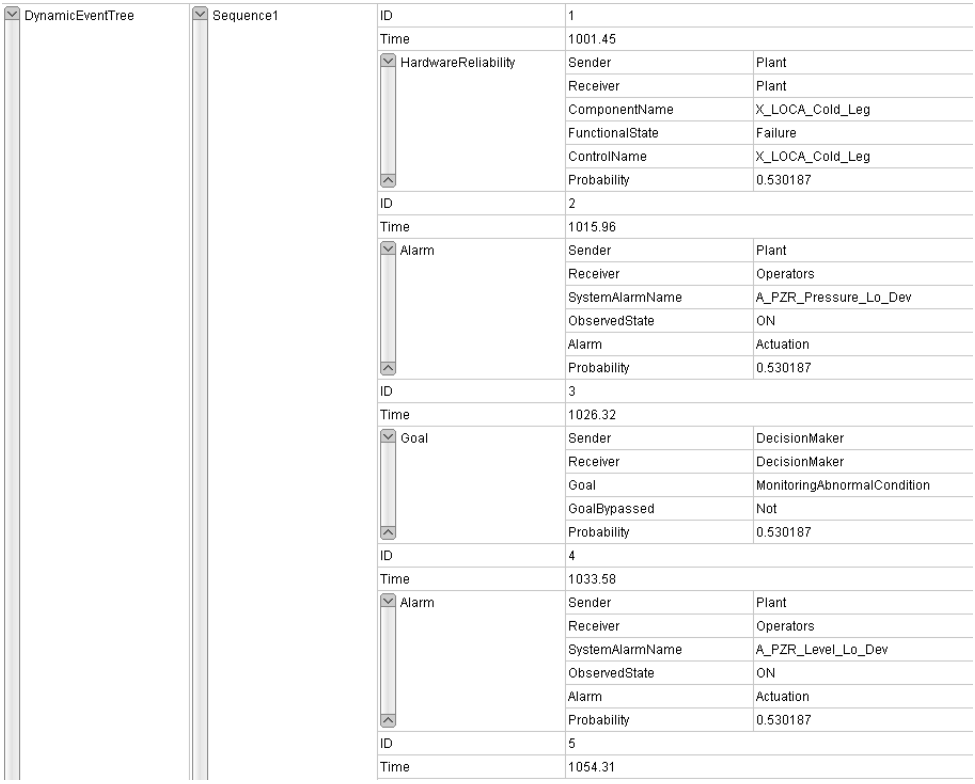



**Fig. 4.14:** Example of DDET-generated sequences.

In general in a DDET, events can be either hardware (component and system failure, generated alarms, etc.) or human events (human failure events, timing of actions, procedures, etc.). All these events can arise during the scenario's evolutions depending on the interaction between hardware or humans and system. Consequently in the generated DDET all this events result mixed together making the resulting DDET hard to understand. In particular, when many scenarios are generated by the tool, with all this amount of information it is easy to lose the progression of a particular type of event in the overall DDET, e.g., the procedure step evolution over time. Therefore, the power of the DDET-parser is to generate different views of the same DDET based on some input

parameters (types of events) allowing a simplification of the DDET that can be explored and studied by the analyst.

Basically, the DDET parser works like a filter in which the information that are not relevant for the analysis are filtered out. This allows the analyst to focus his/her analysis on a particular type of event. A generic DDET is shown in the left hand side of Figure 4.15 where three types of events has happened during the evolution of the DDET, i.e., type A, B, and C. Then, if the analyst is interested only on type A events occurred in the DDET, the visualization of the DDET generated by the parser will be only a type-A DDET as shown in the Figure 4.15 on the right hand side. In principle, more than one type of event can be shown in the tree (e.g., type A and B) and in the generated visualization of the DDET there are only events related to A and B. Note that the generated DDETs are not in scale in terms of timing of events but each event in the DDET has associated the time along with the probability when that particular event has occurred.

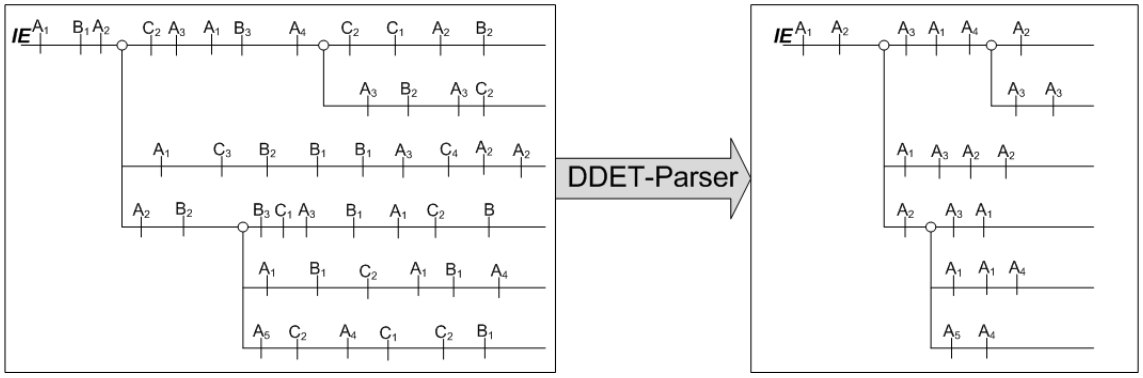



**Fig. 4.15:** Generic DDET where only types of events A, B, and C are shown (left hand side) and parsed DDET where only types of events A are visualized (right hand side).

The DDET parser is a tool able to read DDETs written in XML format in which each event has a particular tag that identifies the type of event. For instance, typical tags are "Procedure step", "Alarm", and "Hardware reliability" which corresponds to when the operators enter into a particular procedure step, when there is an alarm and which is its characteristic, and when there is an hardware event respectively. Once interesting/relevant types of events have been identified, the parser filters out "unimportant"

events and the resulting DDET is produced and could be shown using any XML editor. An example of generated visualization of DDET is shown in Figure 4.16 where only events related on when operators enter in the procedure steps are shown. In particular, in the visualized DDET, information about the timing of events, probability of events, and type of branches ("Timing variability" in Figure 4.16) are shown.

In is worthwhile to mention that actually two types of visualization of the DDET are produced by the parser. The first one, as shown in Figure 4.16 it a visualization of a typical event tree as usually done for any tree. It is based on the Scalable Vector Graphic (SVG) language[3] and the tree can be visualized by using any browser. Whereas, the second one is essentially a DDET written in XML in which instead on having the typical structure of event tree there is a structure based on series of sequences (Figure 4.17). For each event, some characteristics of the event and the time when the event has occurred is shown.

The DDET-parser is a tool which has been widely used for the analysis of the DDET-generated scenario in Chapter 6. It is one of the basic tools used in the developed approach for DDET output analysis as further described in Section 4.4. It is also worth to mention that since the DDETs generated are very large, it is difficult to have an entire plot of them on figures in this document. Therefore, only some small snapshots have been shown.

[3]SVG is a language for describing two-dimensional graphics in XML. SVG allows for three types of graphic objects: vector graphic shapes (e.g., paths consisting of straight lines and curves), images, and text. In the DDET-parser, vector graphic shapes are used.

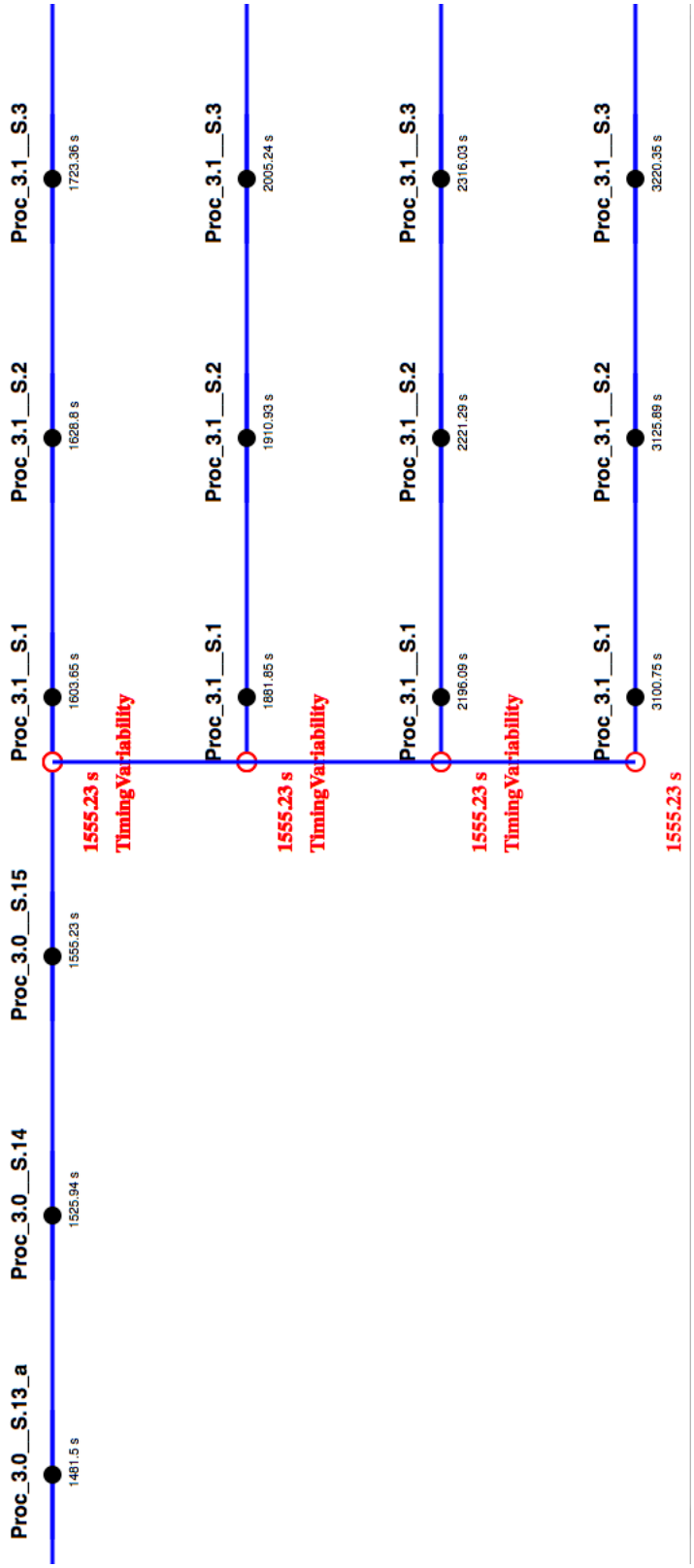



**Fig. 4.16:** Example of parsed DDET where only the timing of entering in procedure steps are visualized. Proc = procedure, S. = step.

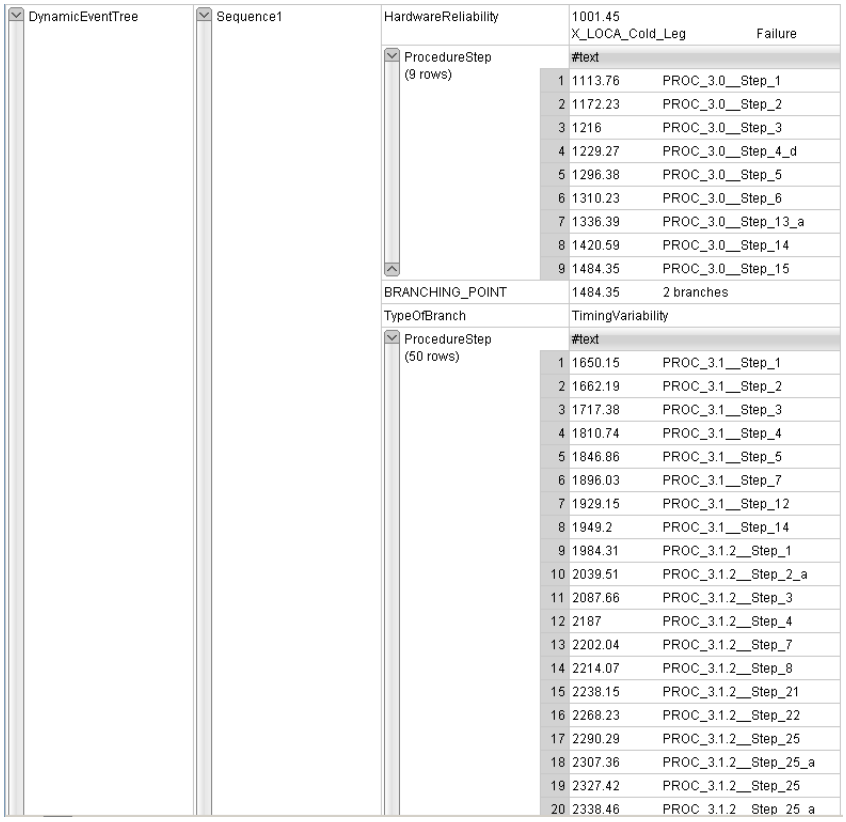



**Fig. 4.17:** Example of parsed DDET where the visualization of series of sequences is shown. In this case, events related to hardware events, procedure steps, and branches are visualized.

## 4.4 DDET output analysis approach

In Section 4.3.1 the scenario classification approach and a first application of the DDET-generated scenario classification has been presented. A step forward is the application of the classifier to DDET-generated scenarios to inform HRA. The structure of the classifier has been kept as described in Section 4.3.1 but the focus of the application is different. The idea is to develop an approach using the described classifier and parser to analyze the DDET-generated scenarios of failure or close to failure. In particular, the grouping of scenarios based on some similarity and its quantification in terms of probability is used for the identification of events leading to the particular group (in general the ones with highest probabilities or unsafe scenarios).

In this Section, a description on how to use the classifier for the DDET-generated scenario analysis is provided. The approach will extensively be further used Section 6.2.2 for the identification and analysis of failure scenarios and in Section 6.2.2 to analyze the control of the plant by different crews.

This approach is based on a structured guideline which would help the analyst to deal with the problem of the analysis of DDET-scenarios. The following steps must be followed in order to analyze the output scenarios of a DDET.

1. Define the type of analysis to do,
2. Identify groups based on some similarity,
3. Train the classifier with an appropriate number of scenarios,
4. Classify all the DDET-generated scenarios,
5. Calculate the group probability based on the scenario probabilities, and
6. Analyze the group with the highest probabilities identifying the main contributors to the cluster.

In addition to the analysis of the highest probability scenarios, a very interesting point is the identification and analysis of failure scenarios even if in principle, their associated probability might not be the highest.

Information about both the highest probability scenarios and the failure (or close to failure) scenarios, are of interest for our purposes. The first ones give an indication on how the plant likely behaves after a certain initiating event and on the most likely actions taken by the operators whereas the second is important for the calculation of the Core Damage (CD) frequency and the identification of actions and events leading to failure.

As mentioned before, in the first step the analyst has to define the type of analysis to do, i.e., an interesting "issue" must be identified. For instance, one can be interested in

analyzing and understanding why different sequences lead to different amount of water lost through the leak. This is an indication on how the crew is good or not in handling the accident and also, from an economic point of view, how expensive the consequences of the scenario evolution after the IE might be. In fact, the smaller the water lost through the leak is, the better the crew in handling the accident and less expensive the treatment of the consequences (e.g., purification of the lost water) is. In this case the feature to be analyzed is the amount of water through the leak in time. This allows to focus the analysis on a particular issue that the analyst is interested in. Other issues must be identified by the analyst and for each one the developed approach can be applied.

The second step entails the identification of similarity in the DDET-generated scenarios. The analyst, based on experience, has to identify prototypes of groups looking at the parameter(s) behaviors. There might be scenarios with the parameter behavior the analyst is interested in, has particular evolutions which differ from the others. Those particular and interesting behaviors must be identified by hand and used in the third step for the training of the classifier with an appropriate number of scenarios.

In the third step, the analyst has to train the classifier in order to find the optimal geometric partition to be used for the classification of the DDET-generated scenarios. The number of scenarios that must be included in the classifier is not really defined. There are not guidelines or criteria on the number of scenarios but roughly about 10-20 % of scenarios are used in the training phase. The training scenarios has an important meaning from an applicative point of view. In fact, they represent those scenarios that are already known and available and represent the knowledge that the analyst has about the plant behavior.

The fourth step is the classification of all DDET-generated scenarios. The classifier already described has been used to identify the scenarios belonging to the groups identified in the second step of this approach.

The fifth step deals with the calculation of the group probabilities. Each DDET-generated scenario has a conditional probability calculated using the method described in

Section 4.1. Therefore, the probability of each group is just the sum of the probability of all scenarios belonging to the group.

The sixth step is the analysis of the groups with highest probabilities. In principle there could be several groups with high and similar probability and then more than one group might be considered and evaluated. Since those groups are the highest contributors to the total probability, they are the most interesting to be analyzed. In this context, analysis means identification of the main contributors to the group in terms of events. For instance, if the highest probability is the one of the group in which the larger amount of water is lost through the leak, the related events are the ones to be identified and characterized. This gives an idea on which are the contributors to the highest probability group and therefore on events that have a larger impact on the plant behavior. In order to identify the events leading to the group under analysis, the DDET parser is a very useful tool which extrapolates only information we are interested in from the entire DDET. In addition, groups with failure or close to failure must be analyzed in this step even if their associated probability is not the highest. This is done in order to identify which are the events that lead the plant behaving towards failure. The goal is to inform the HRA analyst on hardware and in particular human events leading to failure in order to develop new HFEs that must be analyzed in further analyses.

The added value of this approach is that not all the scenarios must be analyzed but only a small and interesting set identified in a structured way will be analyzed in detail. For instance failure scenarios, scenarios closed to failure, scenarios whose behavior might lead the operators to take a wrong decision. In addition each group and set of events leading to the group is characterized with its conditional probability. Moreover, the identification of scenarios leading to failure or close to failure consequence is an important matter from an HRA prospective. This approach is a first step toward the development and quantification of importance measures for dynamic PRA.

## 4.5 Stratified sampling of the input

Stratified sampling is a statistical method of sampling from a population or better from a sub-population independently in general when the sub-populations vary considerably. The idea of using this concept for the implementation of the input in ADS has been guided by the fact that the requirement in terms of memory are extremely expensive and therefore it is not difficult to run out of memory during the simulation losing all the information and data about the current run. Therefore, splitting the input in small parts in a particular way using the concept of stratified sampling and running different simulations, would bypass the problem of memory requirement.

In this Section, some issues about the memory requirements during the run time in the ADS tool are described. Running a DDET simulation with ADS means to run and save on local memory several times the thermal-hydraulic of the system. In particular, saving at each branching point the thermal-hydraulic process variables in the restart file [RELAP5/MOD3.3, 2001] implies saving on memory information like all the continuous and discrete state variables defined in the thermal-hydraulic model, which can became easily unmanageable from any personal computer. The real bottleneck of the tool is the thermal-hydraulic part of the ADS tool.

Different solutions have been identified in the last years. For example, a multi-processor simulation approach can be adopted [Catalyurek et al., 2006] and actually has been implemented in ADS [Zhu et al., 2008]. Another approach which is currently under study is the possibility to run the tool on cluster computers. Clusters are usually deployed to improve performance and/or availability over that of a single computer, while typically being much more cost-effective than single computers of comparable speed or availability [Bader and Pennington, 1996].

During this PhD work, a different approach has been adopted, i.e., a stratified strategy. The idea is to run a simulation with part of the input which generates a small DDET and save the simulation on hard memory. Then, run another simulation with another

part of the input and again save the generated small DDET on memory. The process continues until all the input is given to the ADS tool and all the input possibilities are explored. Afterwards, all the generated DDETs are merged together in order to have the total DDET; a tool able to merge DDETs has also been developed .

## 4.6 Summary

A new method for the calculation of the probabilities in a DDET is presented. The method consists of calculating the probabilities in the post-simulation phase and setting them equal to 1 during the simulation. The advantages are that the risk of eliminating interesting sequences is avoided and updating the DDET probabilities when new data are available can be done without re-running the model.

Then, the main issue arising from a dynamic approach is that the amount of output information to be considered and evaluated could be in principle impractical to handle due to both the number of DDET-sequences and the number of events in each sequence. An approach for DDET-generated scenarios analysis based on a scenario classification tool and a DDET-parser has been developed in order to *i*) simplify and reduce the effort to analyze the DDET-generated scenarios; and *ii*) acquire an instrument for obtaining HRA insights through the DDET-scenario analysis.

The scenario classification tool is able to group scenarios based on "similarity" identified by the analyst looking at the DDET-generated scenarios. The tool has been applied in a test case study in order to demonstrate its capability and the its usability for classification issues. In addition, a DDET-parser has been presented. The parser is able to reduce the amount of information from the global DDET on a small set the user is interested at.

The two tools are the frame for the developed approach of DDET-generated scenario analysis. The approach consists of a series of guidelines to be followed for grouping similar scenarios and characterizing their probabilities. The goal is to inform the HRA analyst

on groups of events leading failure and to calculate the failure probabilities.

Finally, a methodology for input stratified sampling has been developed and introduced in ADS for dealing with large DDETs. The idea is to split the entire input in different pieces and to run different DDET simulations for each part of input. Then, after all the DDETs are simulated, the tool is able to combine all together in a unique DDET.

The output analysis for DDET-generated scenarios has been used and applied in the case study described in Chapter 5 for the demonstration of its capability.

## Chapter 5

# Case study scenario and modeling

## Contents

This chapter describes the case study selected for this work. After the main tasks for the development of the case study in Section 5.1, an overview of a generic PWR is given in Section 5.2. The focus will be on the typical structure of a PWR and the most important safety systems available in a PWR. Then, the modeling of the case study is presented in Section 5.3. Then, in Section 6.1 the general features of the case study results will be given. This gives a clear idea of the response of the plant for each sequence in terms of plant parameters' behavior. The high level overview of the results highlights the challenges to process the results. These outcomes will be used in Chapter 6 for the analysis of the results to obtain insights for HRA. Finally, in Section 5.4 a summary of the chapter is described.

## 5.1 Main analysis tasks for the development of the case study

In order to develop the case study, it is important to "tackle the problem" in a structured way following guidelines which help the user to focus and to implement all the elements needed for a complete analysis. The main analysis tasks defined for the development of the case study can be summarized as follow:

- development of a thermal-hydraulic plant model;
- selection of a scenario to be modeled;
- analysis of the operators' tasks to be performed (task analysis);
- preparation of the input; and
- definition of the branching point rules.

In fact, once selected the plant (in this case a PWR), a specific thermal-hydraulic plant model must be chosen depending on the type of analysis. In this study, a RELAP plant model has been selected as suitable for the scope of a PRA level 1. In the thermal-hydraulic plant model the geometry, the physics, and the controls of the plant are built. In this specific case study, an available basic plant model has been used and additional components and controls have been added with the aim of making it more realistic and usable in ADS. The plant model has then been linked to ADS through the interface a new control panel has been built.

As further described in Section 5.2 several criteria have been taken into consideration for the scenario selection. The most important are its contribution to the total core damage frequency, an important role of control room operators, and of course a scenario which has already been modeled in the plant PRA. The scenario here selected is a SLOCA.

The first two points are strictly related because depending on the scenario selected in the second point, other controls, components, or systems might be added to the thermal-hydraulic part of the model. In fact, they have been developed in strict iterative way: once the thermal-hydraulic of the model is selected, the scenario selection guides the systems, components, and controls that must be added which, in turn, they influence the development of the thermal-hydraulic of the plant.

Next, a task analysis has been performed with focus on human actions that must be modeled for the selected scenario. This task analysis has been done considering the plant PRA and in particular the HRA. Several actions (some of them implemented in the plant procedures) have been selected and included in the input of the plant.

The main input to ADS are the procedures, the rules-of-behavior, and the hardware reliability. A review of the plant procedures is necessary for the identification of the correct procedures to be implemented in the considered case study. In order to identify and understand the connection between procedures and procedure steps, a database has been developed as further described in Section 5.3.1. The database has been built to simplify the understanding of the procedures' configuration and connection. The identified

procedures have then been implemented in the ADS framework in the new developed procedure structure (3.2.1) for modeling the response of the operator based on procedures. In addition, a set of rules-of-behavior have been implemented. The rules are based on the identification of actions during the task analysis that are not within the procedures and are based on the operator's knowledge and training. Finally, the input for the hardware reliability has been set to model component and system success and failure in the hardware reliability module.

Branching points can be generated due to variabilities in the crew response or hardware success and failure. Several criteria has been used for the identification of branching points to be modeled in ADS and they are described in Section 5.3.2.

## 5.2 Thermal-hydraulic model of Pressurized Water Reactors

Pressurized Water Reactors (PWRs) are generation II nuclear power plants that use light water as coolant and neutron moderator [Glasstone and Sesonske, 1994]. A generic scheme of a PWR is shown in Figure 5.1. A PWR can be basically described by means of two loops (primary and secondary loop) which convert the nuclear heat produced by the core into electrical power. The primary loop includes the reactor vessel where the nuclear fuel composed by nuclear rods is located and the coolant and neutron moderator are kept under high pressure by the pressurizer to prevent the boiling of the water. The heat produced by the fission reaction in the core is removed by the coolant. In order to monitor the nuclear reaction several rods in the core are made of boron which absorbs neutrons and keeps the reaction under control. The coolant transfers the heat to the steam generators through the steam line which connect the primary system to the secondary system and then the coolant is pumped back to the core by the coolant pumps through the cold leg. The heat is transferred to the secondary side through the bundle tubes walls so that there is not mix between primary (radioactive) and secondary (non radioactive) coolant. The

main roles of the steam generators are the production of steam in the secondary side and barrier between primary and secondary side to avoid radioactive contamination of the steam. The steam produced in the steam generators goes into the turbine where it is converted into electricity. After passing in the turbine the steam flows into the condenser where it condensates to water. The resulting water is pumped out of the condenser and back to the steam generators by the main feedwater pumps. For a detailed description of a generic plant see [Todreas and Kazimi, 2001], [Todreas and Kazimi, 1990].

In addition to the previously described systems and components, other safety-related systems and components are present in any PWR. The most important system is the Emergency Core Cooling System (ECCS) [USNRC, 2003]. A typical ECCS is shown in 5.2. There are two purposes of the ECCS. The first is to provide core cooling to minimize fuel damage following a loss of coolant accident. This is accomplished by the injection of large amounts of cool, borated water into the reactor coolant system. The second is to provide extra neutron poisons to ensure the reactor remains shutdown following the cooldown associated with a main steam line rupture, which is accomplished by the use of the same borated water source. This water source is called the refueling water storage tank.

To perform this function of injection of large quantities of borated water, the ECCS consists of four separate systems: the high pressure injection (or charging) system, the intermediate pressure injection system, the cold leg accumulators, and the low pressure injection system (residual heat removal).

Another important system which has several functions is the Chemical and Volume Control System (CVCS). This system is used to *a*) maintain the amount of coolant in the primary system, *b*) control the chemical properties of the coolant, e.g., the chemical neutron absorber concentration (boron concentration), *c*) fill or empty the primary system, *d*) purify the coolant using filters and demineralisers, and *e*) maintain the level of the pressurizer at the desired set point. During the normal operation of the reactor, a small amount of water is inserted in the RCS and another similar amount of coolant is removed

from the system. These two flows are controlled by the CVCS. The so called purge water exits the RCS and after passing through heat exchangers and filters is demineralised to prevent from ionic impurities. Afterwards this water is driven to the volume control tank and can be reused as coolant.

In this study, the simulation of the plant process is performed by a RELAP thermal-hydraulic transient model [RELAP5/MOD3.3, 2001]. The thermal power production is about 3000 MWth. Figure 5.3 shows the primary side of the plant. The reactor has three coolant pumps (one for each loop), a pressurizer working at 153 bar and 344 °C connected to the first cold leg, and three steam generators. The pressurizer has two safety valves which release in the containment and a Power Operated Relief Valve (PORV) which releases in the condenser. The spray line is connected to the pressurizer from the cold leg of the first loop. There are also six accumulators, three connected to the three hot legs and three to the three cold legs. Furthermore, there are the three high and low pressure injection systems (one per loop) and a chemical volume control system connected to the cold leg of the first loop for a makeup and letdown system. As further explained, the initiating event considered in this case study is a SLOCA located in the cold leg of the second loop before the admission to the reactor.

The secondary side of the plant (Figure 5.4) has three loops which lead the steam to turbine through the steam line. The main steam at the outlet of the steam generators is at 64.5 bar and 280.3 °C. The steam dump valve releases the steam to the condenser if the steam line valve closes. Each steam generator has a Main Feedwater (MFW) system and an Emergency Feedwater (EFW) system. In order to control the secondary pressure, there are for each loop a PORV valve releasing steam to the condenser and a safety valve releasing steam to the containment. There is also one Main Steam Isolation Valve (MSIV) per loop in order to stop the steam going to the steam line if needed.

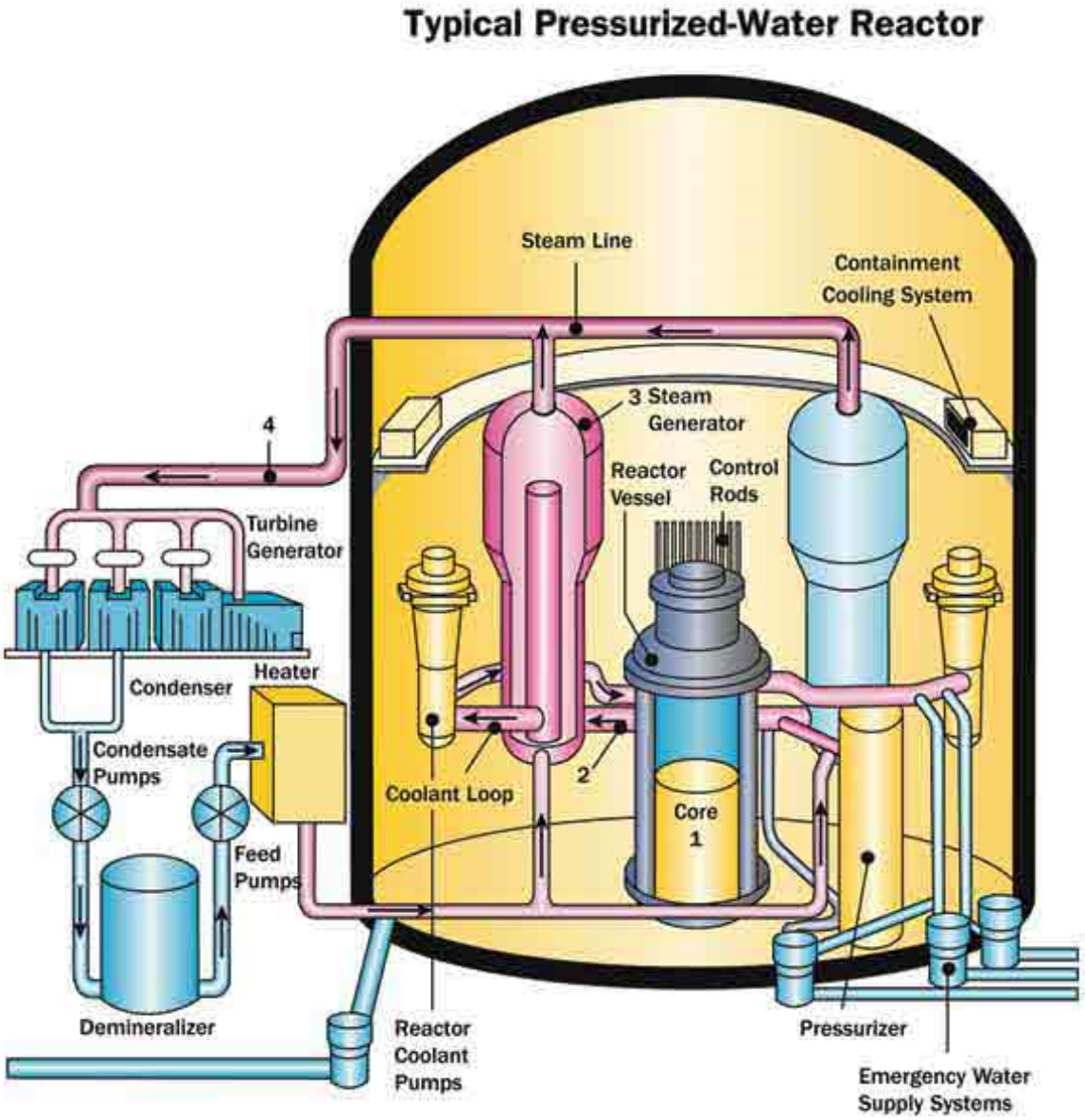



**Fig. 5.1:** Scheme of a generic PWR (source http://www.nrc.gov/reactors/pwrs.html).

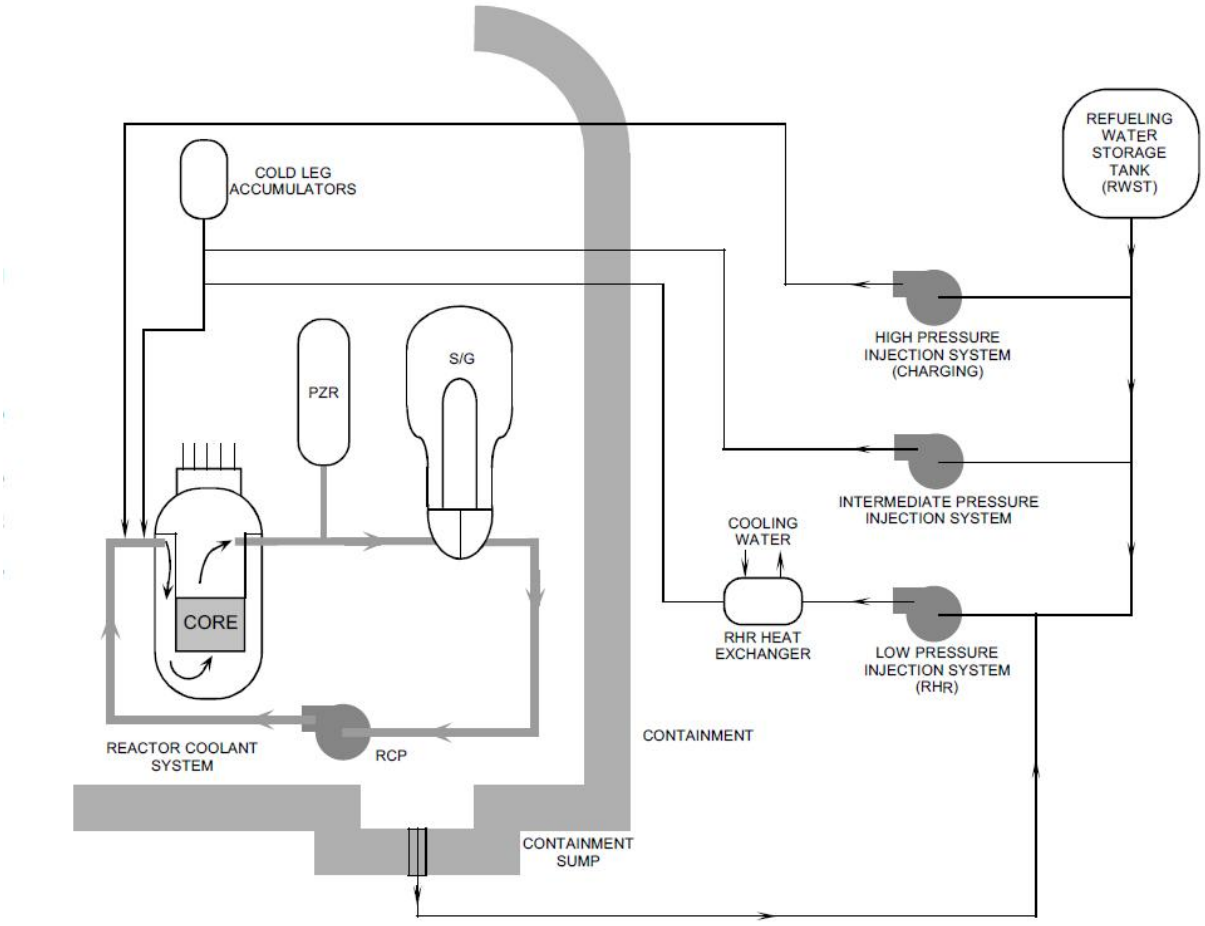



**Fig. 5.2:** Scheme of a generic ECCS for a PWR (source: USNRC).

### 5.2.1 Implementation of the control room panel

The starting point of the implementation of the systems and controls needed for coupling RELAP with ADS was an existing available input deck in which several basic components and systems were already been employed like the pressurizer safety valves (two), main coolant system, main feedwater system, steam generators (three), secondary and primary loops, and the core. In addition to the already modeled systems and components, several controls and indications and additional systems and components have been added for the purpose of the current case study. In particular: accumulator liquid levels and pressures indications, average temperature primary side indication, pressurizer level

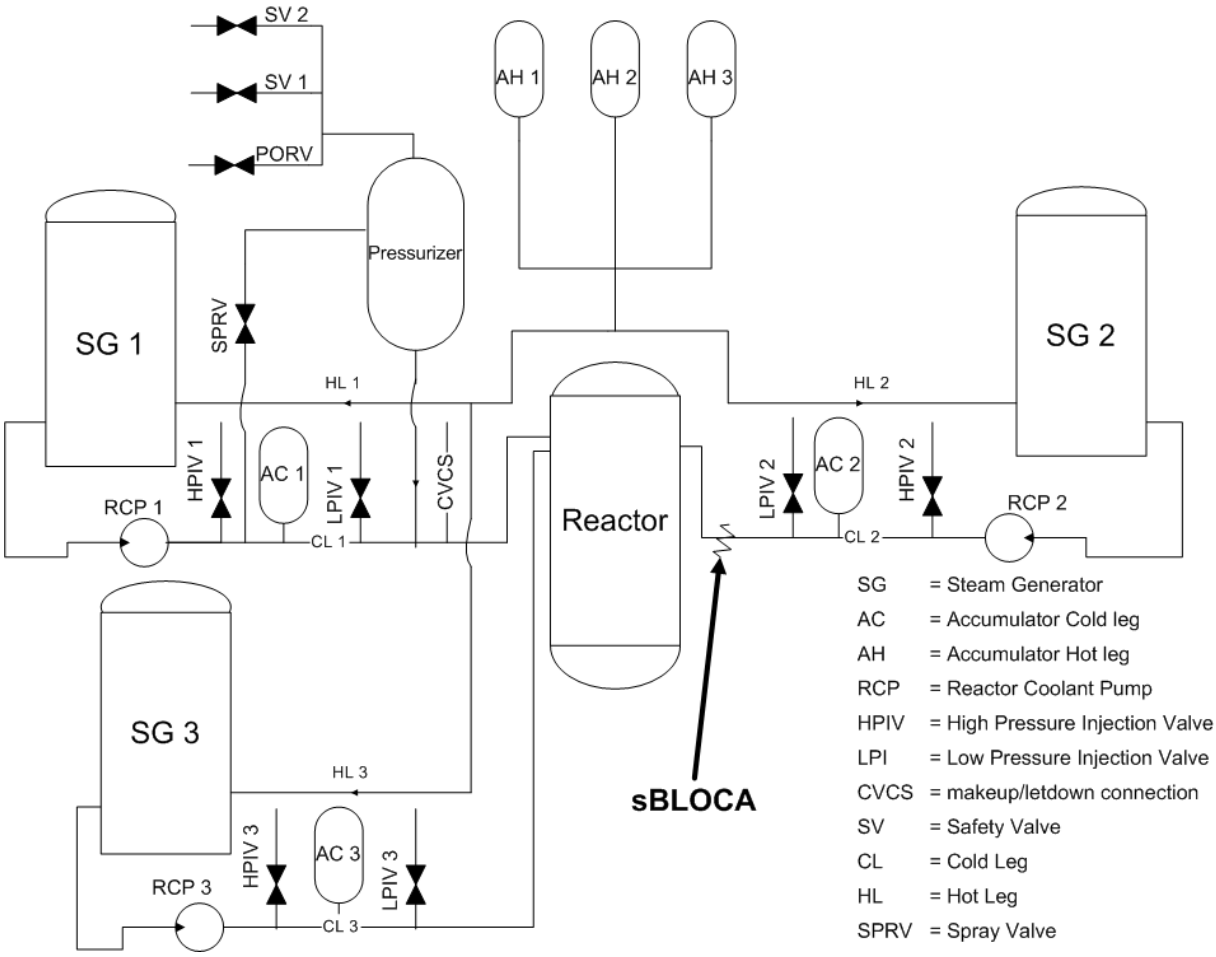



**Fig. 5.3:** Primary side schema.

control, pressurizer spray valve and PORV, ECCS system, i.e., HPI and LPI systems, charging system, main steam isolation valves, steam generator PORV valves, main feed water valves, emergency feedwater system, steam dump valve, turbine governor valve, and point kinetic model (to model the feedback of the temperature on the core power). In order to connect the plant with ADS, a new control panel has been built to model the interaction between the thermal-hydraulic part of the model and human/hardware model. In particular, about 140 displays, 60 controls, and 80 alarms have been added. The operators have a direct access to the control panel, which is the interface between the plant model and the human-machine and hardware model. Appendix D shows the control panel implemented in the case study.

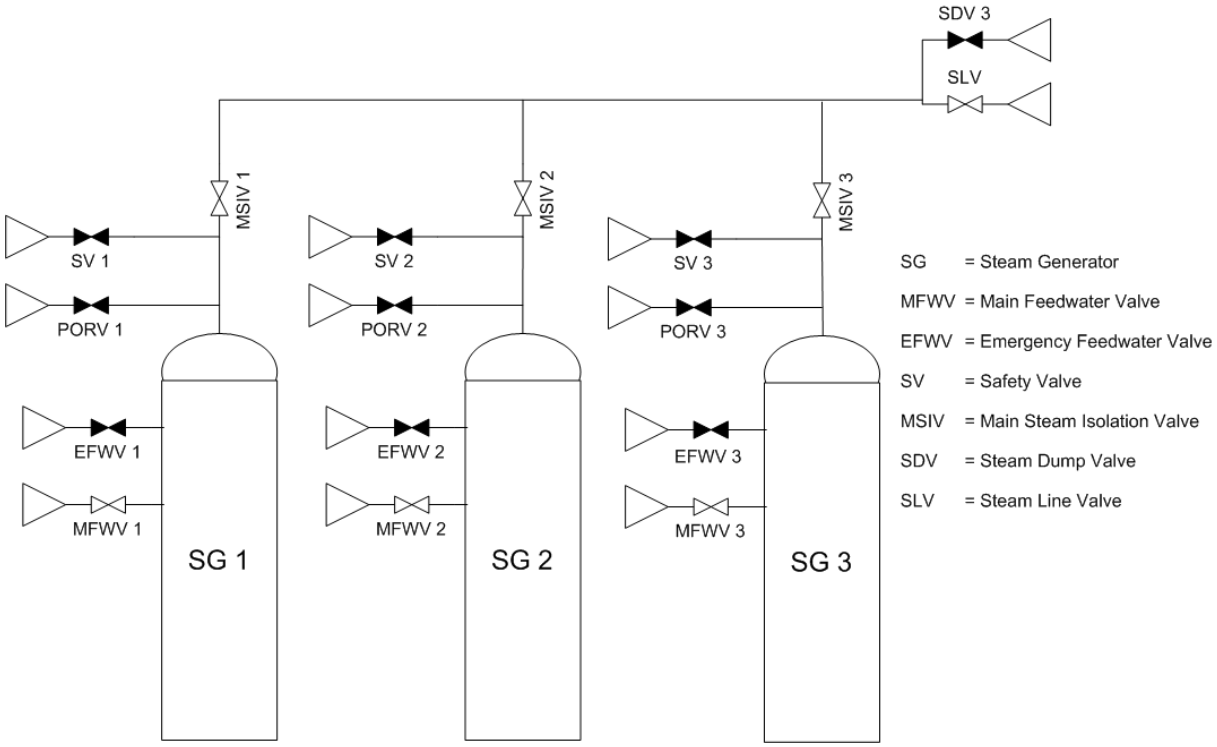



**Fig. 5.4:** Secondary side schema.

## 5.3 Modeling a small LOCA in ADS

In a typical PRA, several scenarios are considered and modeled to make safety and risk analyses of the plant. Any scenario differs to the others because of the type and position of IE, the phenomenology induced by the IE, and the accident progression. Typical scenarios considered in PRAs are anticipated transient without scram, any type of LOCA like small LOCA, medium LOCA, large LOCA, excessive LOCA, letdown LOCA, SGTRs, etc. All of them are important for the calculation of the core damage frequency.

In this work, only one scenario has been considered. Several criteria have been considered in order to choose the one to be modeled in this work. In particular they were:

- significant role of operator actions, in particular in the control room;
- scenario currently modeled in the plant PRA; and
- risk significant in typical PRA.

To test the capability of the ADS tool, in particular concerning the human model, the scenario must have a significant role of the human actions in terms of *i*) cognitive response of the operator to perceived malfunctioning of the system (alarms, incorrect behavior of key parameters, etc.); and *ii*) procedure-guided human action response during the accident behavior. In addition, the scenario has to be interesting in terms of contribution to the total core damage frequencies.

With the aim of covering the previous issues, the scenario which has been chosen was SLOCA event. The reasons which lead the selection of a SLOCA were:

- the contribution to the core damage failure is one of the highest in the current PRA;
- LOCAs are accidents generally well known, in particular the Large LOCA;
- Large LOCA has been demonstrated to be not likely from different PRAs; and
- in the SLOCA the break is not large enough to take away the heat, therefore the control room operators manually have to take actions to cooldown the system (as described in the procedures), i.e., there is significant role of the operator actions.

### 5.3.1 Operator actions during a SLOCA - task analysis

The sequences are assumed to be initiated by a two-inch break in one of the cold legs of the primary system (Figure 5.3). After the SLOCA initiating event, signals for the automatic reactor trip and high pressure injection are generated. The reactor can trip due to different criteria like low steam generator levels, high power production, low pressurizer pressure, containment isolation signal, and high pressurizer pressure. The reactor trip causes the automatic turbine trip, the start of the ECCS (high pressure injection), and the trip of the primary coolant pumps. The steam generator main feedwater pumps are isolated after the reactor trip and the emergency (auxiliary) feedwater is supplied when the steam generator low level signal is actuated. The automatic turbine trip causes the shut off the steam line valves and the steam flows directly to condenser since the steam dump valve

opens. Depending on the peak pressure reached in the secondary side after the reactor and turbine trips, the steam generator atmospheric relief valves or the steam generator safety valves open maintaining the secondary pressure approximately around 80 bars. The success criteria for a SLOCA event are that the high pressure injection maintains the reactor coolant inventory during the rector cooling down to low pressure conditions (below 10 bars) and the steam generator cooling for core decay heat removal.

According to the emergency procedures, the main goals for the operators is to cooldown at 100 K per hour through the turbine bypass valves or the steam generator atmospheric relief valves, control and maintain the steam generator levels above 8 meters using the emergency feedwater valves, start the pressurizer sprays to increase the pressurizer level to 9 meters, shut down the HPI pumps one at a time if there is enough SubCooling Margin (SCM), start the charging pumps to maintain the pressurizer level, and when the pressure is below 10 bar start the LPI for low pressure recirculation cooling. Depending on the evolution of the scenario the operators are instructed to perform other actions in addition to the previous ones. For instance, they can rapidly cooldown the system increasing the secondary cooldown if the HPIs are not available or manually open the steam generator relief valves and reduce the pressure to approximately 80-85 bars if the MSIVs close spuriously or other hardware failures prevent steam relief to the main condenser. Table 5.1 summarizes several potential human actions which could be required during a SLOCA scenario depending on the plant evolution. In the first column there are the action name whereas in the second a short description of the action. The human actions actually implemented in this work are shown in bold italics.

**Table 5.1:** List of the potential human actions during a SLOCA scenario with the corresponding description (in bold italics human modeled actions).

| Human action name | Description |
|---|---|
| ***Start the emergency feedwater pump to control the SG level above 8m*** | If in any steam generator the level drops below 8m, start the emergency feedwater pump of the affected steam generator |
| ***Cooldown the reactor coolant system below 180 °C*** | Initiate a cooldown at 100K/h or 45 K/h if the leak has been identified in the secondary side |
| Reset charging isolation | Reset the charging isolation signal before the HPI tank run out of water after the plant has been stabilized on a low pressure recirculation cooling or closed-loop RHR flow |
| Restart charging isolation | Restart at least one charging pump after the reset of the charging isolation signal |
| ***Start the auxiliary pressurizer sprays*** | Start at least one of the two auxiliary pressurizer spray lines to increase the level of the pressurizer above 5m or to reduce the coolant system pressure |
| Reset the injection signal | Reset the automatic high pressure injection signals after the flood tank level is below 0.6m and the automatic switchover to the containment sump recirculation flow has been occurred |
| | cont'd on next page |

Table 5.1 – cont'd from previous page

| Human action name | Description |
|---|---|
| ***Control the high pressure injection flow*** | Adjust the high pressure injection flow and allow the reactor coolant system pressure to fall below 10 bar before the flood tanks are drained and the automatic signals are produced for switchover to containment sump recirculation flow |
| Open the residual heat removal hot leg suction valves | Align at least one of low pressure injection pump trains for closed-loop RHR operation |
| ***Start high pressure injection*** | Start at least one HPI pump before the core starts to uncover |
| Close main steam isolation valves | Manually close the MSIVs and stop the main feedwater flow |
| Open steam generator relief valve | Manually open the steam generator relief valves and reduce the pressure if the MSIVs close spuriously or other hardware failures prevent steam relief to the main condenser |
| Start the feedwater pumps | Manually start the main feedwater pumps if they are not started automatically |
| Isolate stuck-open relief valve | Identify the stuck-open valve and close its pilot-operated isolation valve before the level of the steam generator drops below 7m and its pressure is 15 bar lower that the unaffected steam generators |
| Align sump recirculation | Align at least one low pressure injection pump train for containment sump recirculation flow before the flood tanks are drained to the automatic suction transfer level |

### Overview of the emergency procedures

The emergency procedures are structured instructions that must be followed by the control room operators in order to control and act on the plant during emergency situations. Actually, in any nuclear power plant there are other procedures like normal operating procedures (used in normal plant conditions and during the startup and shutdown of the plant), abnormal procedures (used when abnormal but not emergency situations occur), emergency procedures, and Severe Accident Management Guidance (used when severe situations occur in the plant). All these procedures are interconnected and linked together and transferring from one procedure to another depends on some criteria that must be met. In addition, within each procedure, there are procedure steps interconnected within the same procedures or connected to other procedures/procedure steps in other procedures based again on different criteria.

With the purpose of implementing these structures of procedures into ADS a database has been developed for the considered plant specific procedures. With the database the user can insert all the procedures and procedure steps of the plant with the criteria of connection to other procedures/procedure steps and the database is able to show all the connections in a table form. This approach has been considered necessary for the understanding of the framework in which the procedures of the plant work.

In this Section, an overview of the emergency procedures for the analyzed NPP will be given focusing in particular on the post trip procedure and on the LOCA procedures, which have been implemented in this study. When the reactor is no longer running in normal conditions, i.e., abnormal conditions or particular alarms have occurred the operator is required to perform recovery actions or to look at the abnormal procedures. Then, if there is a reactor trip, the operators have to start to perform the post trip procedures in which the main tasks are: immediate actions, criteria for emergency cooling, diagnosis (in order to transfer to other procedures), continue inspections, and late diagnosis. Typically in the first task the operators are required to verify the reactor and turbine trip, the availability of the electrical power supply, the secondary cooldown, and check the steam generator

levels. In the second task, the procedure steps instruct the operator to verify if they should start a cooldown. In the third task there is the transfer to other procedures. For example, there is a check of the secondary radiation to transfer to the Steam Generator Tube Rupture (SGTR) procedure or the check of the primary pressure to transfer to the LOCA procedure, and so forth. If no transfer criteria are identified in this task of the procedure, there is again the possibility to transfer in the fifth task, i.e., the late diagnosis task, after the continue inspections where the operators have to monitor the plant. Once a leak has been identified during the post trip procedures, (either within the diagnosis or the late diagnosis task), the operator is instructed to start the LOCA procedure.

In the plant considered, the LOCA procedure is divided in different procedures: *Loss of coolant from primary or secondary side*, *Normalization after the emergency cooling criteria clearing*, *Small leak inside the containment*, and *Primary depressurization with pressure difference between the inside containment and atmosphere greater than 30 mbar*. The procedures are interconnected by different criteria depending on the size of the leak, the position of the leak, the availability of plant components, and the plant evolution.

The first LOCA procedure is the *Loss of coolant from primary or secondary side*. In this procedure after a first phase of diagnosis (*ensure cooldown and diagnosis* task) where the operators are instructed to cooldown the system and to check the SG, the pressurizer, and low pressure system, the operators have to perform the *emergency pumps shut off* task where they have to check whether the pumps must be shut off if there is enough SCM and the pressurizer level is above 5 m. In the third task (*identification of cooldown instructions*) the operators have to cooldown the system through the steam valves and then transfer to the *Small leak inside containment procedure* if the low pressure is not yet reached.

Within the *Small leak inside containment procedure* the operators have to perform several tasks. One is to stop one by one the HPI pumps if there is enough SCM and the pressurizer level is above 5 meters. If there is enough level and SCM they shut off one pump, they wait until the pressurizer pressure is stable and they restart the process

for the second pump and so forth. Then, they have to start the charging system to increase and keep the pressurizer level at 9 meters and wait until the pressurizer pressure decreases below 32 bar where the accumulators start. The next procedure step instructs the operators to stop the accumulators. The primary pressure drops below 10 bar where the LPIs can start for low pressure recirculation cooling (the temperature drops below 90 °C).

During the overall process, the operators must be able to decrease the primary temperature below 180 °C using the SG PORVs (or safety valves) and at the same time to keep the SG levels around 8 meters using the EFW pumps. Figure 5.5 summarizes part of the tasks which must be performed during a small LOCA event and which have been implemented in this study.

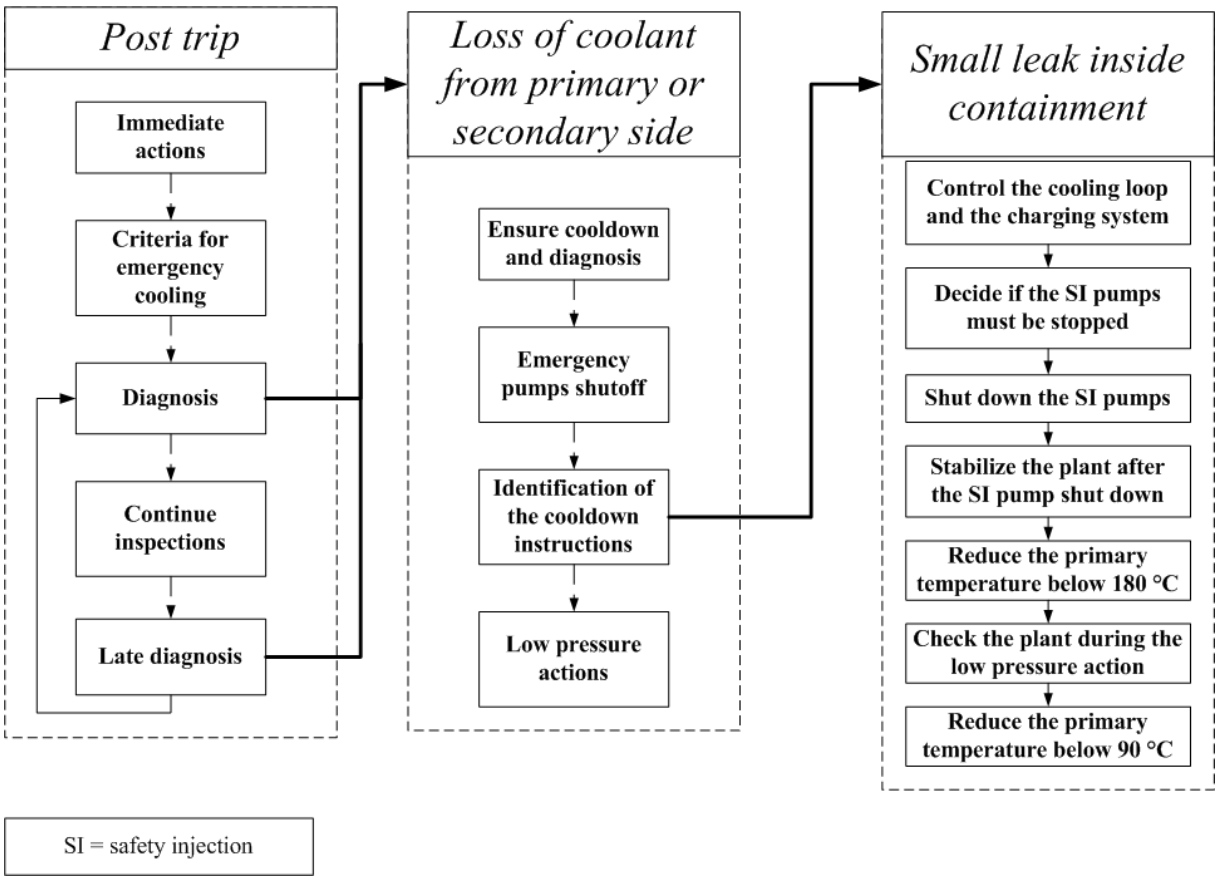



**Fig. 5.5:** Tasks within the post trip and LOCA procedures implemented in this work.

### Implementation of the procedures

The procedures implemented in this work are the post-trip procedure, and the LOCA in primary or secondary side procedure, and the SLOCA procedure. In this case study, about 80 procedure steps have been implemented considering both formal and mental procedures. A list of them is summarized in Table 5.2, Table 5.3, and Table 5.4. Within the ADS code, the user can decide whether to use a three-parameter Weibull distribution to model the time to perform a single action within a procedure step and the respective probability or to give in input the time and probability calculated before starting the simulation. In the first case, the three parameters are $t_0$ the location parameter, $\alpha$ the scale parameter, and $\beta$ the shape parameter. In general, a two-parameter Weibull distribution is enough to describe the timing to perform the procedure step. In the second case, the analyst calculates the time and the probability to perform a certain procedure step based on available data or based on experience. In this case study, the second type has been chosen. In order to simplify the problem, the variability in time has been assumed only at the identified as the most important procedure step within the task or set of tasks whereas the other steps have a single time. Notice that the effective procedure step timing depends on the availability of the operators to perform the procedure step. There are situations in which while performing the procedure step, the operator has to perform also a manual control of other parameters like for example the cooldown rate. Table 5.2, Table 5.3, and Table 5.4 show for each implemented procedure, the task, the step name, and the timing given by the analyst. In particular, in Table 5.2 the step *Check whether there is a LOCA event* (transfer) is the transfer to the *Loss of coolant from primary or secondary side procedures* and some timing variability is modeled.

**Table 5.2:** Set of implemented post trip procedure steps

| Task | Step | Timing |
|---|---|---|
| Immediate actions | *Check the reactor shut down* | 30s |
| cont'd on next page | | |

Table 5.2 – cont'd from previous page

| **Task** | **Step** | **Timing** |
|---|---|---|
| | *Check the turbine shut down* | 30s |
| | *Check whether the buses are energized* | 10s |
| | *Check the three SG pressures* | 30s |
| Criteria for emergency cooling | *Cool down at 100 K/h if needed* | 30s |
| Diagnosis | *Check the main steam pressure* | 30s |
| | *Check the main steam pressure rate* | 30s |
| | *Check whether there is secondary leak* | 10s |
| | *Check whether there is a LOCA event* (transfer) | 100s<br>1500s |
| | *Check the secondary side activity* | 100s |
| | *Check whether there is a leak in any steam generator* | 100s |
| | *Stop cooldown at 100 K/h* | 50s |
| | *Check whether the main feedwater must be stopped* | 50s |
| Continue inspections | *Continue to control the plant* | 50s |
| Late diagnosis | *Check whether there is a LOCA event* | 50s |

**Table 5.3:** Set of implemented steps for the loss of coolant from primary or secondary side procedures.

| **Task** | **Step** | **Timing** |
|---|---|---|
| Ensure cooldown and diagnosis | *Check whether the leak is in the secondary side* | 10s |
| | *Cooldown at 100 K/h using the steam dump valve* | 30s |
| | *Check all SG levels* | 90s |
| | *Check the pressurizer level* | 20s |
| | *Check the low pressure signal* | 30s |
| Emergency pumps shut off | *Check the total safety injection flow* | 20s |
| | *Close steam dump valves if needed* | 60s |
| | *Check whether the safety injection can be stopped* | 10s |
| Identification of cooldown instructions | *Cooldown at 100 K/h using the steam dump valves* | 60s |
| | *Check whether the buses are energized* | 10s |
| | *Check the low pressure injection signal* (transfer) | 30s |
| Low pressure actions | *Start pressurizer sprays* | 20s |

**Table 5.4:** Set of implemented steps for the small leak inside containment procedure.

| Task | Step | Timing |
|---|---|---|
| Control the cooling loop and the charging system | *Continue to cooldown through the steam dumps* | 50s |
| | *Check the SG levels* | 30s |
| | *Check the charging system* | 10s |
| | *Check the ECCS pumps* | 10s |
| Decide if the SI pumps must be stopped | Check the emergency cooling signal | 20s |
| Shut down the SI pumps | *Check whether start up of the pressurizer sprays* | 20s |
| | *Control the spray flow* | 20s |
| | *Stop the pressurizer sprays* | 5s |
| | *Stop one by one all HPI pumps* | 20s |
| Stabilize the plant after the SI pump shut down | *Check whether to start the charging system* | 10s |
| | *Check whether start up of the pressurizer sprays* | 20s |
| | *Control the spray flow* | 20s |
| | *Stop the pressurizer sprays* | 5s |
| Reduce the primary temperature below 180 °C | *Check the primary pressure* | 20s |
| | *Check the sump* | 20s |
| | *Stop the accumulators* | 20s |

**Rules-of-behavior**

In addition to the formal procedures, a set of rules-of-behavior has been implemented in order to model the operator's knowledge and training. This set of rules have been chosen based on the task analysis performed in Section 5.3.1. In fact, not all the actions described in the PRA are covered by the procedures and it is assumed that the operators act also based on knowledge and training beyond the procedures. This knowledge and training is modeled in ADS with a set of rules-of-behavior. These rules are activated depending on the type and the number of information perceived by the operator and they remain activated until the reset time is reached. In particular, the goals implemented in this work are:

- control the steam generator levels;
- control the cooldown rate;
- control the charging flow;
- start/stop the pressurizer sprays in the late phase of the scenario;
- stop two HPIs instead of one if there is enough SCM; and
- increase cooldown rate if no HPIs are available.

In the last item there is branching generation as further explain in Section 5.3.2. Table 5.5 summarizes the rules-of-behavior implemented in the case study. There is the name of the rule, the conditions and the number of conditions to activate the rule, the action (s) to be taken, and the reset time, i.e., the amount of time in which the rule remains activated. In principle, there could also be a branching generation when a rule is activated, i.e., activation and not activation (this has not been implemented in this case study).

**Table 5.5:** List of rules-of-behavior implemented in the case study. N = 1, 2, or 3.

| **Name** | **Conditions** | **True conditions** | **Action(s)** | **Time activated** |
|---|---|---|---|---|
| SG-N high level control | -Alarm High SG-N level<br>-Reactor trip<br>-EFW pump N on | 3-out-of-3 | Reduce EFW-N flow | 60s |
| SG-N low level control | -Alarm low SG levels<br>-Reactor trip<br>-EFW pump N on | 3-out-of-3 | Increase EFW-N flow | 60s |
| Increase cooldown in loop N | -Reactor trip<br>-Rate loop N cooldown $<$ 100 K/h | 2-out-of-2 | Increase SG-N PORV flow | 60s |
| Decrease cooldown in loop N | -Reactor trip<br>-Rate loop N cooldown $>$ 100 K/h | 2-out-of-2 | Decrease SG-N PORV flow | 60 |
| Increase charging flow to control pressurizer level | -Reactor trip<br>-Make up flow available<br>-pressurizer level $<$ 9m | 3-out-of-3 | Increase the injection of the water through the charging system | 60s |

cont'd on next page

Table 5.5 – cont'd from previous page

| **Name** | **Conditions** | **True conditions** | **Action(s)** | **Time activated** |
|---|---|---|---|---|
| Decrease charging flow to control pressurizer level | -Reactor trip<br>-Make up flow available<br>-pressurizer level > 9m | 3-out-of-3 | Decrease the injection of the water through the charging system | 60s |
| Start late prays | -Reactor trip<br>-Late phase of scenario<br>-pressurizer level < 3m | 3-out-of-3 | Start the pressurizer spray | 60s |
| Stop late prays | -Reactor trip<br>-Late phase of scenario<br>-pressurizer level > 9m | 3-out-of-3 | Stop the spray | 60s |
| Stop 2 HPIs | -Reactor trip<br>-HPI Loop 1 flow = 0<br>-HPI Loop 2 flow > 0<br>-HPI Loop 2 flow > 0<br>-pressurizer level < 3m | 4-out-of-4 | Stop the HPI loop 3 | Forever |

cont'd on next page

Table 5.5 – cont'd from previous page

| **Name** | **Conditions** | **True conditions** | **Action(s)** | **Time activated** |
|---|---|---|---|---|
| Increase cooldown rate | -Reactor trip<br>-HPI loop 1 pump failed<br>-HPI loop 2 pump failed<br>-HPI loop 3 pump failed | 3-out-of-3 | Open all three SG PORVs | Forever |

### 5.3.2 Branching point events

In this case study, branching events have been generated due to human actions and hardware events. In principle, a branching point can be generated as soon as any human action or hardware component is required. Unfortunately, if an approach of modeling any actions or hardware events with branches is applied, the number of generated scenarios will be difficult to analyze due to the combinatorial explosion. Therefore, a selection of only a small set of branching points must be done in order to keep the size of the generated tree reasonably small.

The choice of the branching points to be modeled depends on the type of analysis that the analyst is expected to do. In this case study, the main interest was on the variability in time of the operator response and on the variability in the execution of actions within the procedure. In addition, also hardware success and failure has been considered important to see the operator response and behavior during component failure paths.

Based on the task analysis and the expected evolution of the plant the following branching points have been considered in this case study:

- timing variability in transfer to the *Loss of coolant from primary or secondary side* procedure;
- timing variability in stopping the last HPI;
- stop the pressurizer spray the first time (several times the pressurizer must be started up and stopped) at 5 meters (as said in the procedures), 3 meters, and 8 meters;
- stop one or two HPIs if there is enough SCM;
- success and failure of one HPI; and
- success and failure of the steam dump.

The timing variability in transferring to the *Loss of coolant from primary or secondary side* procedure and in stopping the HPI pumps has been considered because these are critical points for the subsequent evolution of the accident.

With regard to the stop the pressurizer spray the first time at 5 meters (as said in the procedures), 3 meters, and 8 meters different strategies in performing this actions, influence the workload in the future evolution of the scenario as well as the dynamics of the crew-plant interactions.

The stop one or two HPIs if there is enough SCM has been chosen because there might be situations in which during the SLOCA evolution there are not problems of SCM like in a large LOCA event for example, and the operators can have the feeling that even two HPIs can be stopped and the SCM remains enough. The effect of this type of action has been judged as interesting for the plant evolution.

The two hardware failures have been chosen because the HPI failure may influence the management of the accident by the operators since the HPIs are quite important to maintain the coolant inventory and they are used a lot in the procedures. The failure

steam dump influences the cooldown of the plant and the control of the SG PORVs used to cooldown the plant, since some additional heat is lost through the steam dump open.

The name of the branching point events, the corresponding number of branches, and the parameter values of each branch is summarized in Table 5.6.

**Table 5.6:** Event name, number of branches of the event and relative parameter values.

| **Event name** | **Number of branches** | **Parameter value** |
|---|---|---|
| Timing variability of transfer to the *Loss of coolant from primary or secondary side procedure* | 3 | **Time**: 100s and 1500s |
| Timing variability in stopping the last HPI | 3 | **Time**: 100s and 1000s |
| Stop the pressurizer spray the first time | 3 | **pressurizer level**: 5m, 3m, and 9m |
| Stop 1 or 2 HPIs | 2 | **Num. of HPIs**: 1 or 2 |
| HPI Success/failure | 2 | **HPI state**: success or failure |
| Recovery HPI | 2 | **HPI state**: recovered or not |
| Steam dump Success/failure | 2 | **Steam dump state**: success or failure |

In order to model also an operator action described in the current plant PRA, an additional failure has been implemented. The considered action is a fast cooldown during a SLOCA initiating event with no HPIs. If no HPIs are available, the operator has to cooldown at a higher than the planned 100 K/h rate to reduce the primary temperature below 225°C and pressure below 26 bar for the start of the accumulators. If the accumulators are not available the goal is to reduce the pressure below 10 bars for low pressure injection before the core damage begins. Therefore, in addition to the previous branching point rules, an additional branching point rule where no HPIs are available has been added. If no HPIs are available, a branching point is generated and a rule to increase the cooldown rate is activated. These types of scenarios will be analyzed in the last part of Chapter 6.

### 5.3.3 Implementation of the input

As already described in Section 4.5 the input of ADS must be divided (stratified) in different parts in order to be able to run the ADS code without having problems of running out of memory. In this case, a set of nine simulations has been performed and consequently the input of each simulation has been chosen in order to cover the entire input of the case study. Afterwards, once all the simulations have been run, the output of each simulation has been merged using the developed tool introduced in Section 4.5.

### 5.3.4 Example of scenario modeled in ADS

In this section, an example of the sequences of events that occur after an IE as modeled in ADS is presented. The IE is a small leak in one cold leg of a PWR (SLOCA conditions). As soon as the IE occurs, the plant starts to deviate from a nominal condition behavior. In fact, both the pressurizer level and pressure decrease, there is signal of containment isolation and main steam isolation, and the emergency feedwater pumps start running. Due to the low pressurizer level, the reactor and the turbine trip. The operators start to monitor the plant in order to understand what happened. After a while they decide to start the emergency operating procedures due to the critical behaviors of several parameters. At the beginning they check several parameters in the post trip procedure with the aim of identifying the correct initiating event and transfer to the correct procedure. In particular they transfer to the SLOCA procedure (*Loss of coolant from primary or secondary side*) because the containment pressure is larger than nominal and it is an indication of a leak in the plant (it is one of the criteria to transfer to the SLOCA procedure). At the same time the operators are able to control the SG levels using the emergency feedwater pumps. Once transferred to the SLOCA procedure the operators, besides several checks, have to cooldown the system using the PORVs, start the pressurizer sprays, stop one by one HPI pump, and start the charging system. During the scenario evolution, they have to control the cooldown rate, control the charging flow, and control the sprays.

Performing the previous actions, the operators are able to depressurize and cooldown the system to low pressure conditions.

## 5.4 Summary

In this chapter, the case study implemented and analyzed in ADS has been presented and the methodology used for the definition and development of the case study has been described. The methodology is based on the following:

- development of the thermal-hydraulic plant model;
- selection of the scenario to be modeled;
- analysis of the operators' tasks to be performed (task analysis);
- preparation of the input; and
- definition of the branching points.

At the beginning, a high level overview of a generic PWR has been given focusing mainly on the typical structure of the plant and on the most important safety systems available in PWRs plants. Then, the thermal-hydraulic plant model and the implemented control room panel has been described. The starting point of the thermal-hydraulic model was an available simple model in which the geometry and several components were already available. During this work, additional components and in particular controls have been added to make it more realistic and functional for ADS and for the modeling of the SLOCA. Furthermore, the thermal-hydraulic plant model has been connected to ADS through the interface including also a new control panel.

The selection of the scenario to be modeled in ADS has been also described pointing out mainly the criteria for the scenario selection and the motivation of the selected scenario, i.e., the SLOCA. Considering the selected scenario, a task analysis has been

performed with the intention of identifying important human actions to model in ADS. The main contribution of the task analysis was the study and analysis of the plant-specific procedures. In fact, a database able to map and show the connection between procedures and procedure steps has been developed. The database has helped the understanding of the procedures which have been further implemented in ADS. In addition, following the task analysis, human actions not modeled in the procedures but based on the knowledge and training of the operator has been identified and implemented in the so-called rules-of-behavior. Finally, the input needed for the simulation in ADS has been built and in particular the definition of the hardware reliability elements have been set to model component and system success and failure.

The last step was the definition of the branching points. Branching points can be generated due to variabilities in the crew response or due to hardware success and failure. The criteria and motivations for the selection of the branching points have been presented and described.

The stratification of the input is an important strategy used to bypass the problem of extensive memory requirement of the thermal-hydraulic calculations.

## Chapter 6

# Case study analysis and results

## Contents

In this Chapter the results obtained from the analysis of the simulation data of the case study described in Chapter 5 will be presented. At a high level, these results can be summarized as: *a*) insights about the scenarios and operator actions in the scenarios; *b*) dynamic vs. classical HRA insights; and *c*) demonstration through post-simulation data analysis techniques on how to support HRA. In Section 6.1, the general features of the case study results are presented focusing mainly on the time evolution of the plant process parameters and the calculation of the DDET probabilities. Then, in Section 6.2 the simulation data are analyzed using the developed post-simulation strategy in order to obtain insights for a dynamic approach to support an HRA through the information of Performance Shaping Factors (PSFs). In this Section, two case studies are analyzed: the first one is a SLOCA with all the HPI systems available and the second a SLOCA without any HPI system available. Then, in Section 6.3 the methodology for HRA characterization in the dynamic PRA context will be presented. The focus will be on how one can use this tool to obtain information about the scenario and potential errors that operators can have during the accident scenario evolution, and how to use dynamic approaches to help the calculation of the HEPs.

## 6.1 General features of the case study

In the first case study analyzed a total of 81 DDET sequences has been generated by the tool. In the second case study, an additional set of 22 sequences were generated. The results in this section refer only to the first set of 81 sequences. The simulation has been stopped after about 2 hours or when the plant reaches about low pressure conditions (10 bars) and the LPI pumps start. In fact, when low pressure conditions are reached, the LPI system is able to remove the residual heat from the core then the plant can be considered in safe conditions. The aim of this section is to present how the response of the plant appears for each sequence in terms of plant behavior.

In Figure 6.1 an excerpt of the generated DDET in the case study is presented. The

diagram represents only a few sequences where only the main events are shown since representing the entire DDET is not feasible. In particular, after the initiating event (SLOCA), the reactor trips (Rx trip event). After about 5 minutes, the operators have to start cooling. At this point in time there is a branching point representing timing variability to start cooling. Therefore, the different outputs of the decision to start cooling are explored making three branches in the tree (branch 1, branch 2, and branch 3). Then, in the course of the evolution of the plant, operators have to decide whether to stop the HPI pumps one-by-one or to stop the first time 2 pumps. The decision is based on the amount of SCM available. In the DDET we can explore both situations where they stop one pump (branch 4) or two pumps (branch 5). The same applies for branches 6 and 7. The final DDET generated by the software contains all the paths explored during the simulation.

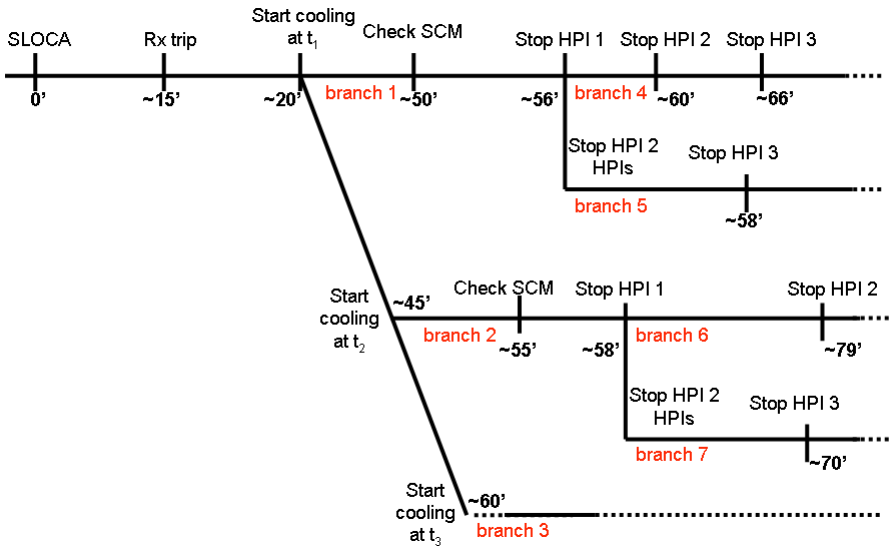



**Fig. 6.1:** Excerpt of sequences of the generated DDET where only the main events are shown.

In the output of the DDET there are also the evolutions of the parameters included in the control panel module. A description of the main parameter evolutions is now presented.

Immediately after the occurrence of the break, the primary pressure drops quickly from 152 bars to about 80 bars. Control rods fall inside the core and the power decreases.

The reactor coolant pumps are tripped due to loss of subcooling and natural circulation is maintained because of the heat still generated in the core. The decay power that still remains in the core is removed via the secondary system. There is a brief rise of secondary pressure until primary and secondary pressures reach similar values (Figure 6.2), afterwards the primary pressure is kept always above the secondary pressure. The operations performed in the secondary side are meant to slowly cooldown the secondary system and the heat in the primary system is removed through the secondary.

In all scenarios the operators have been able to cooldown the plant. In fact, the model predicts that the crews respond successfully in the case study scenario. This means that the type of crews simulated have the capability to control the system to safe conditions even if some scenarios near unsafe regions have been identified and further analyzed.

Right at the beginning of the scenario the decrease of temperature is fast but after 30 minutes the operators, responding according to the procedures, are able to control the cooldown rate. Scenarios in which the control of the cooldown is not performed are not present in this case study. It is assumed that the operators are always able to control the cooldown rate in order to meet the 100 K per hour criterion of cooling.

The effect of starting at different timings the cooldown (due to the associated branching point), is visible in Figure 6.3 where the pressurizer levels are plotted. In fact, the later the operators start the cooldown in the corresponding procedure step, the later the other procedure steps are performed and in particular the ones related to the starting of the sprays. The main visible effect of starting spraying is the increase of the pressurizer level as shown in Figure 6.3. After a few minutes from the start of the sprays (to increase the pressurizer level), the pressure decreases but it comes back to almost the same level just after they stop the sprays (see the primary side pressure behavior around 60 min in Figure 6.2). The pressure does not decrease because the HPIs keep injecting high pressure water. The pressure decreases as soon as the operators stop the HPIs (responding according to the procedures since there is enough subcooling margin). As shown in Figure 6.2, when a HPI is stopped there is a sharp drop in the pressure behavior. This is due to the fact

that fewer pumps are running and the inventory of water decreases due to the loss of water through the break. The effect of the pressurizer sprays and HPIs is also shown in Figure 6.4 where there are the behaviors of the break mass flow. When the operators spray, the pressure is reduced and there is a contraction of the volume which reduces the flow through the break. Also when one-by-one the HPIs are stopped, the amount of water outside the break decreases. Notice that as further explained, when the operators take some time to stop the last HPI, the mass through the break increases (late phase of some scenarios in Figure 6.4). This is due to the fact that the amount of water injected by the last HPI still running increases the inventory of the water in the primary loop which flows through the break.

In Figure 6.5 the subcooling margin behavior for all scenarios is shown. The minimum subcooling margin is calculated considering the difference between the current temperature and the saturation temperature of any loop and taking the minimum value. As one can see in Figure 6.5, the subcooling margin in all of these sequences is positive. This means that saturation conditions are never reached during the evolution of the considered scenarios, even if for some of them the subcooling margin becomes close to zero. This is mainly due to the fact that the injection flow provided by the three HPI pumps and the charging system is much larger than the break flow.

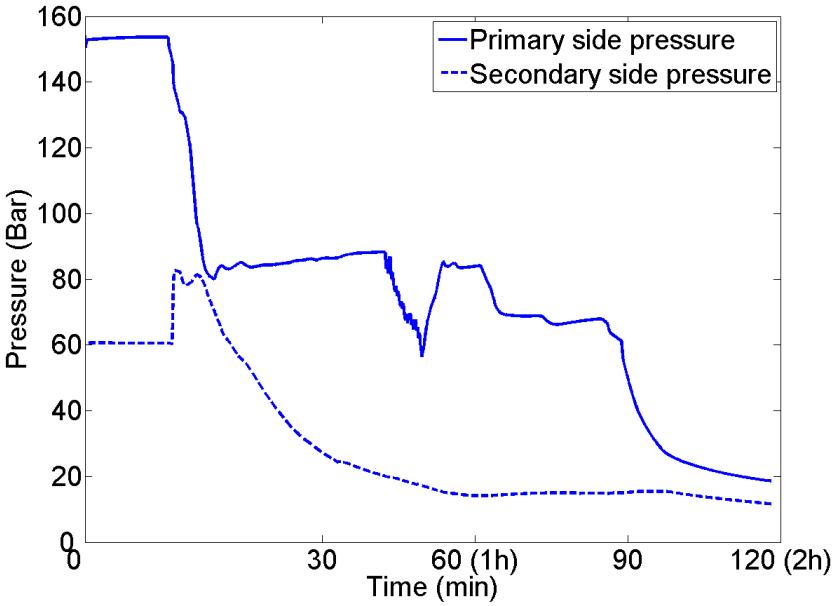



**Fig. 6.2:** Example of primary and secondary pressures for a sequence.

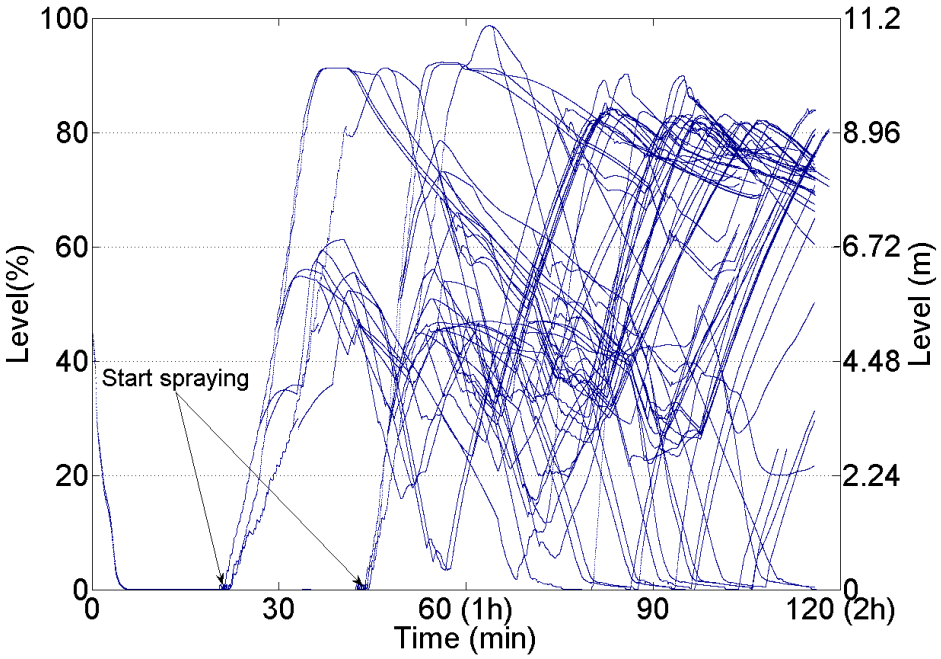



**Fig. 6.3:** Pressurizer levels (all scenarios).

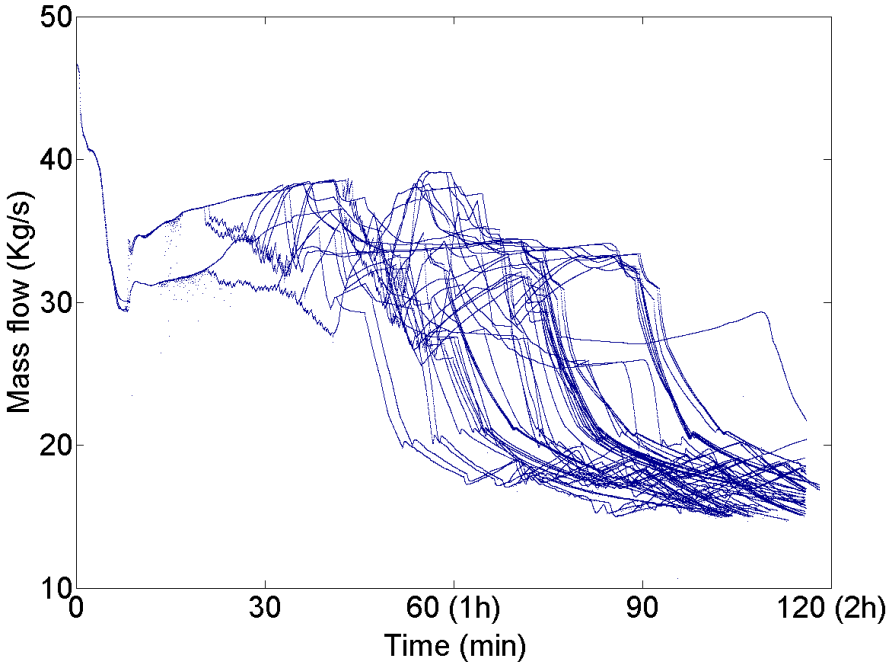



**Fig. 6.4:** Break mass flows (all scenarios).

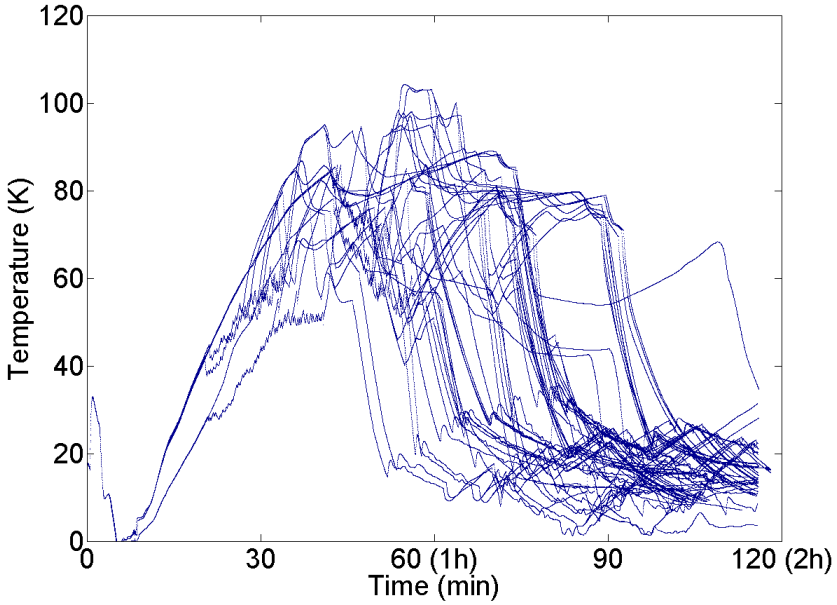



**Fig. 6.5:** Subcooling margins (all scenarios).

With regard to the secondary side, the operators are instructed to control the SG

levels using the emergency feedwater pumps. Figure 6.6 shows as an example the steam generator level behaviors in the first loop. In the other two loops the behavior is similar. As one can see, the SG levels are maintained in the 85-90% range. This is accomplished by the use of the EFW pumps as described in the procedures. In this way, the operators satisfy the goal of avoiding an overfilling of the SGs.

The turbine trip after the reactor trip, causes the closure of the main steam isolation valves and the steam can no longer flows to the turbine but it flows to the condenser. Right after the initiating event, the PORVs automatically open as shown in Figure 6.7. Then the operators manually control of the cooldown by acting on the PORVs. For scenarios where the operators start to cooldown late, there is a gap in the plot right after the starting of the manual control (after about 30 minutes). This is due to the fact that, with the automatic opening of the valves, the cooldown rate is larger than 100 K/h since is not controlled. In order to meet the criterion for the cooldown rate, the operators have to reduce the PORVs flow to establish the 100 K/h. This does not happen in case of nominal transfer since the operators are able to take manual control early in the scenario and the cooldown rate at that time is smaller.

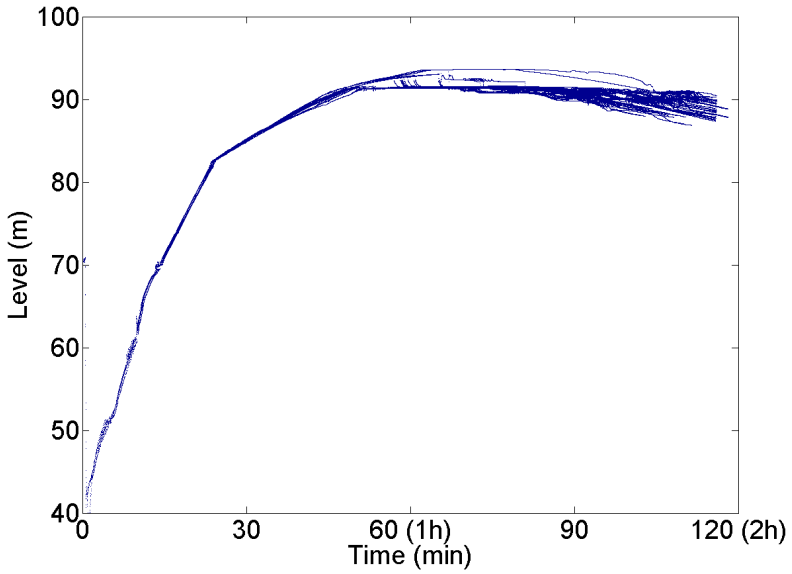



**Fig. 6.6:** Steam generator levels (all scenarios).

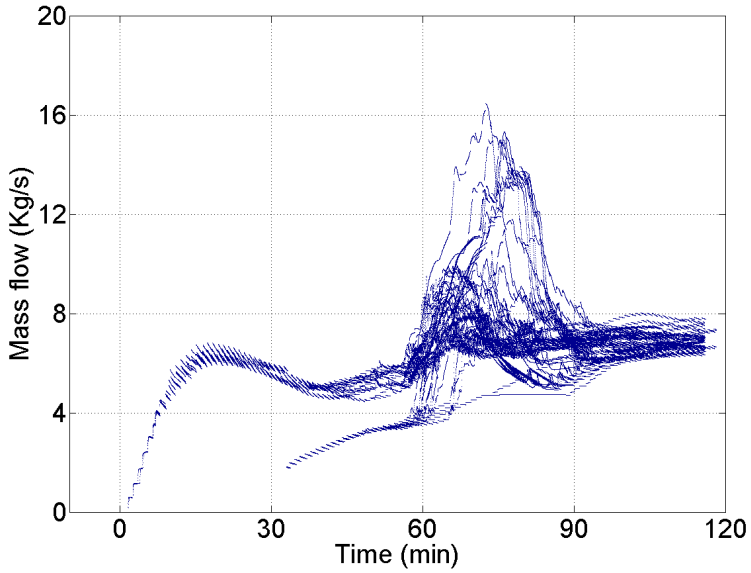



**Fig. 6.7:** PORV flows (all scenarios).

### 6.1.1 DDET-generated scenario probabilities

In this Section, the DDET-generated scenarios probabilities are calculated in order to characterize the probability of each sequence. It is important to note that the traces of the plots presented in the previous section, do not indicate the probability of occurrence of the associated scenarios (i.e., the probability of each sequence) which can vary by several orders of magnitude.

As already mentioned in Section 6.1 a set of 81 scenarios have been generated. In Table 5.6 the branching points considered in this case study have been listed and the corresponding probabilities for intermediate crews are allocated in Table 6.1. The probability of each scenario is automatically calculated based on the conditional probability of the branches.

It is worthwhile to mention that the probability of the single scenario is actually a conditional probability even if for convenience it is referred to in this work as only probability. To obtain the frequency of the sequence after the SLOCA, those probabilities

must be multiplied by the frequency of occurrence of the SLOCA.

The calculation of the DDET-generated scenario probability has been done according to the methodology described in Section 4.1; the branching probability associated to the timing of human events are set to one and the overall probabilities are recalculated in the post-simulation phase to include information about the type of crews under consideration. Then, for each considered crew, a sub-DDET is built and afterwards all of the generated sub-DDETs are merged considering the respective weight of probability of the crew type.

According to the reference PRA, the frequency of SLOCA is $1.07 \cdot 10^{-4}$/year. Some representative values have been estimated for the branching point probabilities (see Table 6.1 for the numerical values). Note that for the timing variability branches, the probability values are not real probabilities but are those used during the simulation. The real probabilities of each scenario are calculated in the post-simulation phase.

**Table 6.1:** Event name and corresponding probabilities for intermediate crews.

| **Event name** | **Number of branches** | **Branching point probabilities** | **Description** |
|---|---|---|---|
| Timing variability of transfer to the *Loss of coolant from primary or secondary side procedure* | 3 | (1.0, 1.0, 1.0) | Procedure step timing variability |
| Timing variability in stopping the last HPI | 3 | (1.0, 1.0, 1.0) | Procedure step timing variability |
| Stop the pressurizer spray the first time | 3 | (0.2, 0.6, 0.2) | Stop spraying at 3, 5, or 8 m |
| Stop 1 or 2 HPIs | 2 | (0.8, 0.2) | Operator decides to stop 2 HPIs if enough SCM |
| HPI success/failure | 2 | ($9 \cdot 10^{-4}$, $1 \cdot 10^{-3}$) | Hardware failure |
| Recovery HPI | 2 | (0.7, 0.3) | Operator recovery action |
| Steam dump success/failure | 2 | ($9 \cdot 10^{-4}$, $1 \cdot 10^{-3}$) | Hardware failure |

The Probability Distribution Functions (PDFs) of the timing variability of the crew response are calculated based on the concept of "crew tendency". If the crews are "fast" the corresponding PDFs are skewed towards fast performances, if they are "slow" they

are skewed towards slow performances, and if they are "intermediate" the corresponding PDFs are almost symmetric.

In this case study all three types of crews have been considered. For each associated timing action, three branches are generated, therefore only three representative points for distribution are considered. Table 6.2 summarizes the branching probabilities used for each type of crew and the fraction of the corresponding type of crew.

**Table 6.2:** Type of crew, fraction of type of crews, and branching point probabilities BP (BP1: transfer to the *Loss of coolant from primary or secondary side* procedure. BP2: variability in stopping the last HPI.

| **Type of crew** | **Fraction of types of crew** | **BP1** | **BP2** |
|---|---|---|---|
| Fast | 0.3 | (0.7, 0.2, 0.1) | (0.7, 0.2, 0.1) |
| Intermediate | 0.4 | (0.5, 0.5, 0.5) | (0.5, 0.5, 0.5) |
| Slow | 0.3 | (0.1, 0.2, 0.7) | (0.1, 0.2, 0.7) |

Figure 6.8 shows the resulting overall probability for all three type of crews whereas the detailed of the calculation of the probabilities for the fast, intermediate, and slow crew tendencies can be found in Appendix F.

In all the type of crews, the probability of the first 24 scenarios of each of the types of crews are larger compared to the others. This is due to the fact that the scenario after the $24^{th}$ are related to the failure of either HPI, steam dump valve, or both. Since their probability of failure is low, the scenario probability results low. Notice that since the values of the probability can vary of several orders of magnitude, the vertical axis is in logarithmic scale. The overall event tree is built up considering the fraction of types of crew shown in the second column of Table 6.2.

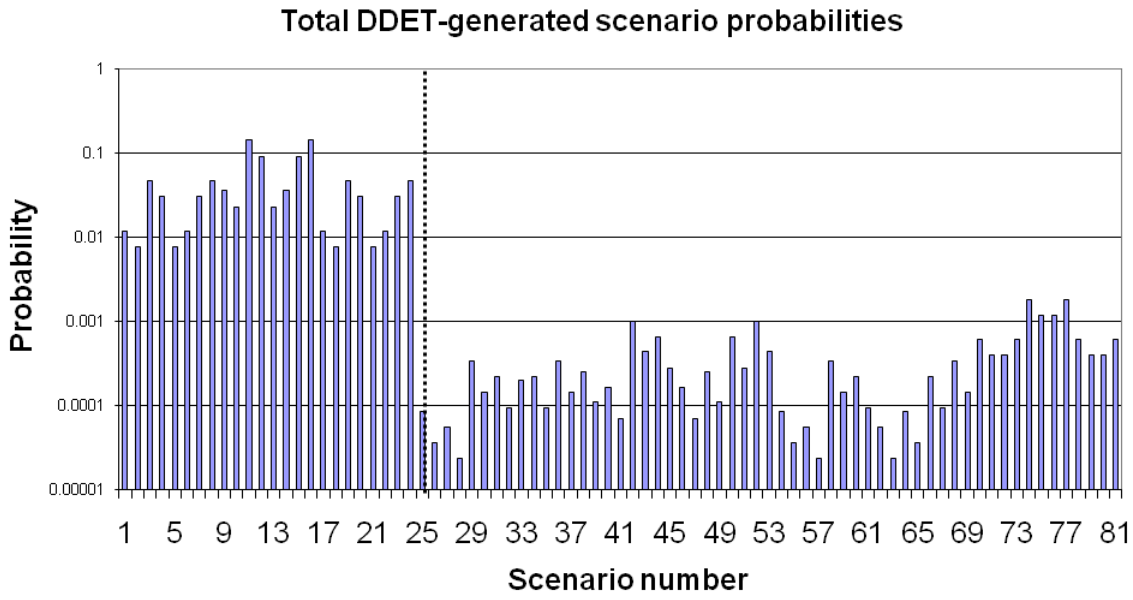



**Fig. 6.8:** Overall scenario probability for all three types of crews.

The overall scenario probabilities is represented in Figure 6.8. Those probabilities are the sum of the fast, intermediate, and slow type of crew probabilities weighted by the corresponding weights (or fraction of types of crews) listed in Table 6.2. In each sequence there is the contribution of the three types of crews therefore also extremely fast or slow behaviors can be observed.

The added value of calculating the scenario probabilities in the post-simulation phase is that the simulation is run only one time to explore all the possible scenarios due to human timing variability.The probabilities are set to 1 initially; then in the post-simulation phase real probabilities are recalculated and normalized considering as many types of crews as one wants. This allows the running of the thermal-hydraulic of the code only for one tree which, as already said, is the main bottleneck of the tool. In addition, the methodology allows a straightforward way of updating the DDET output probabilities in case new data are available. Finally, if one did not consider the concept of crew tendency only an average behavior would be modeled, which would tend to overlook some of the performance outcomes.

### High probability scenarios

In this section, the twelve scenarios with the highest probabilities are analyzed, in order to identify the main events contributing to those scenarios. Only the top twelve scenarios have been included in this analysis since they dominate the DDET-generated scenario probabilities, i.e., the probabilities of the subsequent scenarios are lower by one to two orders of magnitude. Table 6.3 shows the twelve high probability scenarios (notice that in all these sequences the HPI and steam dump valve did not fail).

The two highest probability scenarios are the ones including is the stop of the pressurizer spray at 5 m in addition to, first, the early transfer to SLOCA and, second, early stop of the last spray and late transfer to SLOCA and late stop of the spray.

Then, in the second group (the next four scenarios), there is the stop at 5 m of the pressurizer spray in addition with all the combinations of early and late for the two timing variability transfers. Next, the third group (the following four scenarios) are related to the stop of the pressurizer spray at 3 and 8 m in addition to early or late T1 and T2 transfers. Finally, the last group (last two scenarios) have the stop op the pressurizer spray at 5 m in addition to the stop of 2 HPIs with an early T1 and T2 transfers and stop of 1 HPI with early and late T1 and T2 transfers.

As a general result, one can say that the events leading to the highest probability scenarios are the stop of the pressurizer spray at 5 m, the stop of 1 HPI, and the early and early or late and late transfer for the two timing variability transfers.

**Table 6.3:** First twelve high probability scenarios for all crews. T1 = Timing variability in transfer to the SLOCA procedure. T2 = Timing variability in stopping the last HPI.

| Sc. Num | Prob. | Description |
|---|---|---|
| 11 | 0.0903 | Stop spray at 5 m, stop 1 HPI, early T1, and early T2 |
| 16 | 0.0903 | Stop spray at 5 m, stop 1 HPI, late T1, and late T2 |
| 12 | 0.0470 | Stop spray at 5 m, stop 1 HPI, early T1, and early T2 |
| 15 | 0.0470 | Stop spray at 5 m, stop 1 HPI, late T1, and early T2 |
| 3 | 0.0470 | Stop spray at 3 m, stop 1 HPI, early T1, and early T2 |
| 8 | 0.0470 | Stop spray at 3 m, stop 1 HPI, late T1, and late T2 |
| 19 | 0.0301 | Stop spray at 8 m, stop 1 HPI, late T1, and late T2 |
| 24 | 0.0301 | Stop spray at 8 m, stop 1 HPI, early T1, and early T2 |
| 9 | 0.0301 | Stop spray at 5 m, stop 2 HPIs, early T1, and early T2 |
| 14 | 0.0301 | Stop spray at 5 m, stop 2 HPIs, late T1, and late T2 |
| 4 | 0.02258 | Stop spray at 3 m, stop 2 HPIs, early T1, and late T2 |
| 7 | 0.02258 | Stop spray at 3 m, stop 1 HPI, late T1, and early T2 |

### 6.1.2 High-level scenario analysis

In this section, scenarios that have their end states close to failure are identified and analyzed. An example of undesired end state scenario is shown in Figure 6.5 where the subcooling margin (SCM) of all DDET-generated scenarios is plotted. As one can see, all scenarios have positive SCM, therefore saturation states are not reached. Nevertheless, there are some scenarios which have the SCM close to zero. An example is scenario 33 (Figure 6.9) where 90 minutes after the IE, the SCM margin starts to be below 5°C, i.e., close to saturation. Even if such scenarios do not lead to any system failure, for an HRA analyst they are interesting because one can identify a point in some scenarios where the crews may take an action to increase the subcooling margin. For instance, they may start injection and repressurize the system, thereby depleting the available injection water and delaying low-pressure conditions.

Scenario 33 is an interesting scenario because as further explained, it leads also to the minimum upper plenum mass with regard to the others. This scenario is characterized by the failure of one HPI, the stop of the pressurizer sprays at 3 meters, the late transfer

to the SLOCA procedures, and the stop of 2 HPIs. This means that after the stop of the 2 HPIs no HPIs are running since one is failed and two are manually stopped. Therefore, the pressure level quickly decreases but not to the level of the accumulators and LPI start and also the SCM follows the reduction of pressure. Due to the fact that it is a scenario with late transfer to the SLOCA procedures, the timing when the operators start to spray to reduce again the pressure to low pressure conditions is long and therefore, the SCM remains close to zero for a long time before the operators spray and the LPI system starts and then the inventory of the water makes the SCM no longer close to zero.

The probability associated to this scenario is $1.98{\cdot}10^{-4}$. Albeit in terms of probability this sequence has not a large weight, the associated consequence could have some impact for the safety of the system due to the possible creation of voids in the stream which can lead to pump cavitation. Therefore, from an HRA it is important to understand why low SCM is reached and how the crew must respond to avoid low SCM.

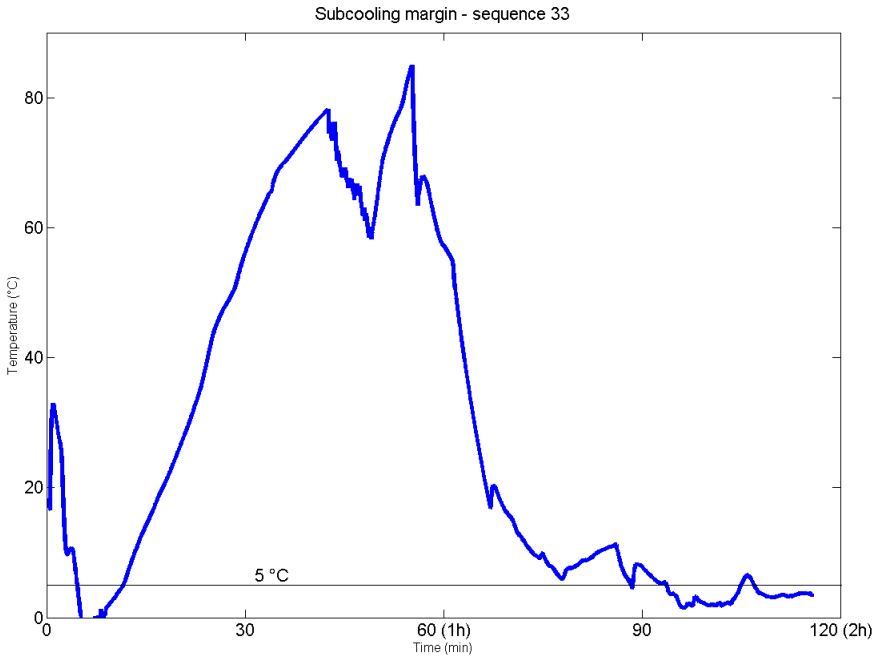



**Fig. 6.9:** Subcooling margin behavior of sequence 33.

In the same scenario 33, the amount of upper plenum water in the late phase of the

scenario, is the lowest of all the scenarios generated by the DDET tool (Figure 6.10). Also scenario 46 has a low amount of upper plenum water in the late phase of the scenario, as shown in Figure 6.10. Scenario 46 has similar occurring events as scenario 33. The difference is that the stop of the pressurizer sprays is at 5 meters and the dynamics of the system are faster in scenario 46 which lead the operators to spray before the scenario 33, slightly increasing the amount of water in the upper plenum. It is worthwhile to mention that again, these two scenarios do not lead any system to failure but if no actions are taken by the operators uncovery of the core might be reached.

The small amount of water of the upper plenum is mainly due to the fact that the three HPI pumps are not injecting water, combined with the slow crew dynamic which reduces the inventory of water and the delays in reaching the conditions for accumulators and LPIs.

The probability of scenario 46 is $1.63 \cdot 10^{-4}$. Also in this case the probability is low with regard to the others but the scenario is of interest due to the potential consequences.

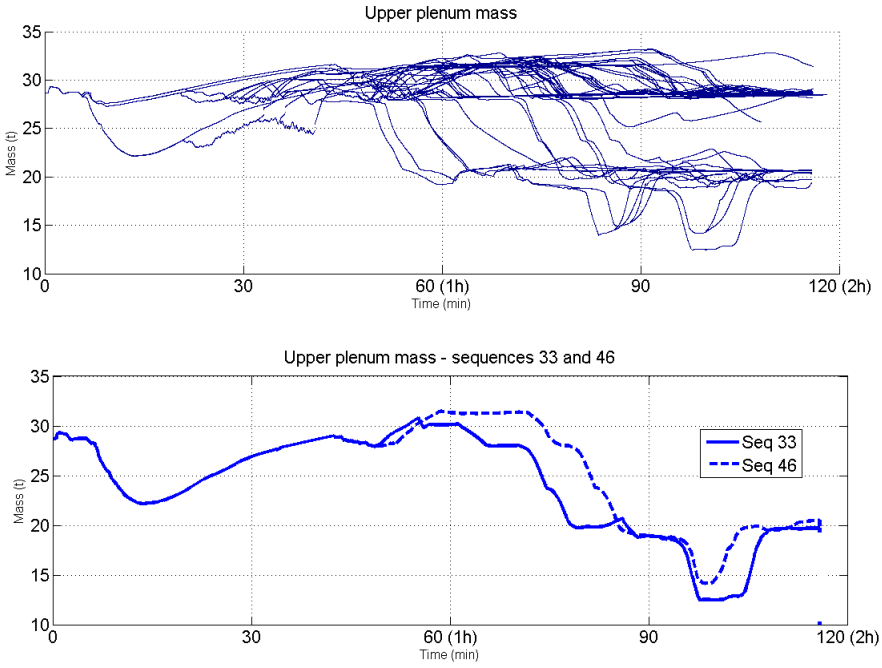



**Fig. 6.10:** Integral upper plenum mass for all scenarios (above) and for two selected scenarios.

## 6.2 Analysis of the results

In this section, the results achieved during this PhD are presented. Through the SLOCA case study, the following results have been obtained and will be described in detail in the following sections:

- the crew-plant simulation generates a distribution of the crew time response that account for crew tendencies;
- the analysis of scenarios from DDET-generated data provides a means to characterize the context for the success of critical actions, i.e., critical points in the procedures, dynamic constraints on operator actions, different strategies permissible in the procedures, and effect of concurring goals; and
- the dynamic results can be effectively used to inform HRA and to help the estimation of the human error probabilities.

### 6.2.1 Distribution of the crew response

The evolution of any plant parameter depends on the events that have occurred along the development of the accident scenario. Figure 6.11 shows as an example the behavior of the primary side pressure of a generic scenario and highlights several events that have occurred during the scenario evolution. In particular, there is a visible change in the pressure behavior when operators start the pressurizer spray and when they stop the HPI pumps. Those events, in addition to other not shown in Figure 6.11, guide the depressurization of the plant for that specific scenario.

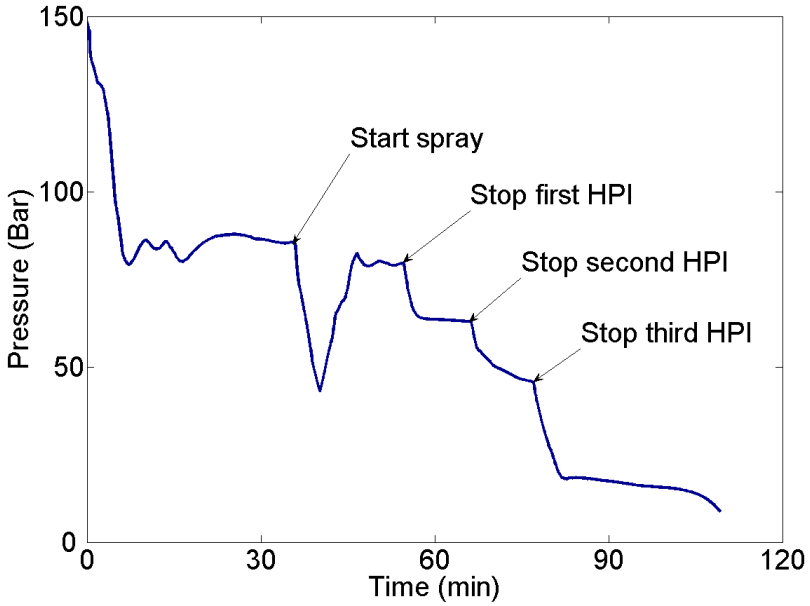



**Fig. 6.11:** Pressure history of one selected scenario with instants of the start of spraying and stop of high-pressure injection.

In the DDET, each sequence differs in terms of the events that occur in their timing, as shown in Figure 6.12.

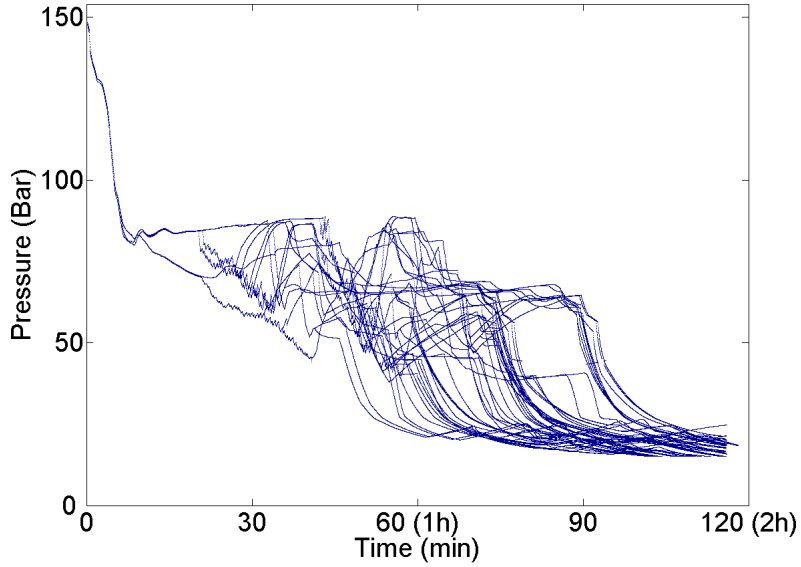



**Fig. 6.12:** Primary side pressure evolution of the DDET-generated scenarios.

As shown in Figure 6.12, each crew starts the depressurization of the system at different times (and thus also the cooldown) and is able to depressurize and cooldown the system at different times. Therefore, a distribution of depressurization or cooldown time is generated that mainly depends on the timing of the occurrence of the events.

Figure 6.13 shows the distribution of the crew time cooldown; in the vertical axis the cooldown time is shown (i.e., the delta time from when the operators start to cooldown until they reach 180°C) and in the horizontal axis the time in minutes. As one can see in Figure 6.13, the crews take from 60 to 100 minutes to cooldown the system. An interesting point is that both fast and slow behaviors can been observed due to the tendency method implemented in the DDET model. Those crew, which are observed in reality according to the studies in simulators, would have been truncated by the simulation as it has been described in Section 3.1.4 where the crew time model has been compared against empirical data.

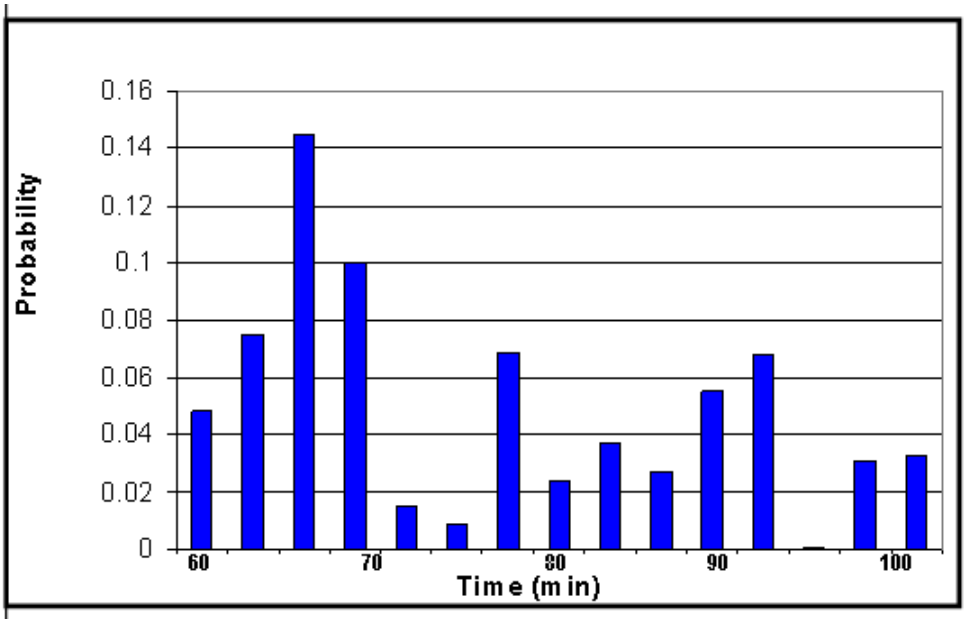



**Fig. 6.13:** Distribution of the cooldown crew responses.

One conclusion from this analysis, one can say that the events occurring along the scenario evolution will affect the behavior of the system and the timing when these events occurred will generate a range of responses. Due to the tendency method, a distribution

response where extreme behaviors can be observed is produced.

In the next Section, the scenarios are analyzed using the post-simulation techniques.

### 6.2.2 Insights from a dynamic HRA

The post-simulation strategy has been applied to the DDET-generated scenarios in order to analyze a PRA action against the reference PRA and to describe what makes the distribution of the crew response like the one identified in Section 6.2.1 for the characterization of the context. In particular, groups of scenarios based on similarities have been identified to obtain insights for HRA through the identification of failure or close to failure scenarios. The purpose is to demonstrate how the crew-plant modeling provides a tool to characterize the operator tasks, context, and challenges the operators are faced to during the accident scenario evolution.

The action analyzed in this section is the depressurization of the plant. From the reference PRA the main challenges of the operators are: *a*) depressurization of the system before losing makeup from the HPI tanks, i.e., fast depressurization; *b*) avoid boiling of water in the primary system, i.e., maintain SCM; and *c*) maintain the pressurizer level avoiding dryout and overfill. In addition, from the task analysis (analysis of procedures), the operators have to cooldown through the SG PORVs and shutdown the HPI pumps in order to reduce the pressure and minimize the break flow, and spray with the pressurizer sprays to increase the pressurizer level to compensate for the pressurizer level decrease during the cooldown. Therefore, three features are considered for the analysis of the results: primary pressure, subcooling margin, and pressurizer level.

#### Analysis of depressurization action against reference PRA

In classical PRAs, plant-specific, transient thermal-hydraulic calculations are usually performed for each type of accident initiating event. For certain types of initiating events, a few calculations are performed for each proposed success criterion to demonstrate its

validity over the entire range of conditions the initiating event is intended to represent. In addition to the comprehensive assessment of system success criteria, calculations are performed to evaluate the time available for plant operators to perform certain manual actions represented in the PRA. These actions generally represent manual actuation of key safety systems if, for some reason, automatic safety system response(s) fails to occur. Some of this information could be derived from the baseline system success criteria calculations from design basis accidents. But separate calculations are performed for this specific purpose to refine the available time frames for operator actions, and provide a rigorous technical basis for them.

Based on thermal-hydraulic calculations from the reference PRA, the operators have to depressurize the system in 90 minutes. This time was calculated based on deterministic calculations.

This action, in combination to all the actions taken by the operators in NPPs, can be identified in the simulated data from the DDET outcomes. After the generation of the DDET with the ADS tool, the following step is to identify prototypes of the action based on expert judgment for the groups of similarities. For example, we can assume three groups, i.e., fast, intermediate, and slow depressurization. Most interesting are slow depressurization scenarios which might not meet the criterion of 90 minutes of depressurization time which has been chosen according to the reference PRA model timing.

Then, the classifier must be trained with a small set of scenarios (for instance 3 for each class, see Section 4.3.1) and the test of all scenarios can be performed. The pattern considered for this type of analysis is the sampling of the pressurizer level at certain time points (every 100 seconds) after half an hour of simulation.

Table 6.4 summarizes the results of the classification and Figure 6.14 the corresponding pressurizer pressure behavior traces for each class.

As shown in Table 6.4 the classifier has been able to identify scenarios belonging to

the three foreseen groups plus several unforeseen scenarios. The unforeseen scenarios are scenarios which are near the boundary between two classes (green sequences in Figure 6.14). They cannot be classified as ambiguous. Those scenarios have a very low probability, i.e., 0.0014 they will not contribute that much to the scenarios that do not meet the depressurization criterion.

The probabilities of all the generated scenarios are calculated based on the values in Table 6.1 and they represent the probability of occurrence of the scenarios based on branching probability events.

From Table 6.4, the probability of class 1 is two times higher than the probability of class 2 even if the number of scenarios for each class is similar. This tells that the weight in terms of probability of the red and blue traces in Figure 6.14 are different and the red trace weights (class 1) are bigger that the blue ones (i.e., class 2).

**Table 6.4:** Results of the classification of the DDET-generated scenarios based on pressurizer pressure.

| | **Class 1** | **Class 2** | **Class 3** | **Ambiguous** |
|---|---|---|---|---|
| **Probability** | 0.64 | 0.32 | 0.04 | 0.0014 |
| **Number of scenarios** | 90 | 108 | 27 | 18 |

From an HRA, the most interesting scenarios are those of class 3, where the criterion of depressurization in 90 minutes is not met. This is shown in Figure 6.14 by the scenarios with black traces. In addition, also some of the ambiguous scenarios should contribute to not meeting the criterion that are scenarios between class 2 and 3 where the operators are not able to depressurize the system in 90 minutes. Since their probability is very low compared to class 3, their contribution to the failure scenarios is effectively negligible.

A further step in the analysis is the identification of the contributors to the class 3 scenarios looking at the DDET. From the review of the DDET using the DDET-parser, the main contributors identified to class 3 are: late transfer for the SLOCA procedure, late stop of HPI, stopping of the HPIs one per time, and all HPIs working or 1 HPI failed plus steam dump failed. These information help the HRA in identifying the combination

of events that lead to failure.

Furthermore, the pressurizer pressure behaviors have been cross-compared with the SCM behaviors considering the classes identified by the pressurizer pressure behavior analysis. The goal is to identify whether there are scenarios belonging to class 1 or 2 which are failure scenarios in the SCM feature. The SCM has been chosen because it is one of the safety parameters that must be controlled by the operators during accidents. In other words, the three foreseen classes and the ambiguous class have been matched with the SCM behavior. The resulting classification in the SCM feature is shown in Figure 6.15.

It is interesting to note that in the SCM feature, class 3 scenarios (i.e., failure scenarios with respect to the depressurization in 90 minutes) are scenarios where there is enough SCM margin. Notice that enough subcooling is an indication that in the reactor there is no boiling.

With regard to the achievement of the depressurization of the system, class 3 scenarios are the worst in the primary pressure feature but with regard to the SCM, class 3 is the best. Therefore, it is important to underline that success or failure of an action is relative to a particular goal that must be achieved and it is not a global result.

The subset of scenarios that do not meet the criterion of the low SCM level belonging to class 1 and 2 have been identified and quantified in terms of probability. The main contributors to the unsafe scenarios from the analysis of the DDET with the DDET-parser are the stop of the pressurizer spray at 3 and 5 m and the stop of 2 HPIs when enough SCM. This tells that the combination of these two main types of events lead to low SCM margin.

In addition, the pressurizer level behavior have been analyzed in order to identify scenarios that can lead to overfill of the primary side and eventually leak through the pressurizer PORVs. In fact, as shown in Figure 6.3, there are some scenarios where the pressurizer level is close to overfill.

Figure 6.16 shows the behavior of the class 3 pressurizer level. The scenarios we are interested in are highlighted in red. Those scenarios are the ones close to failure, i.e., close to 100% of level. The main contributors to them are the stop of pressurizer spray at 8 m in addition with a late transfer to the SLOCA procedure. As one can see, the contribution of these sequences is very low in terms of probability but the consequence can be important for the plant safety.

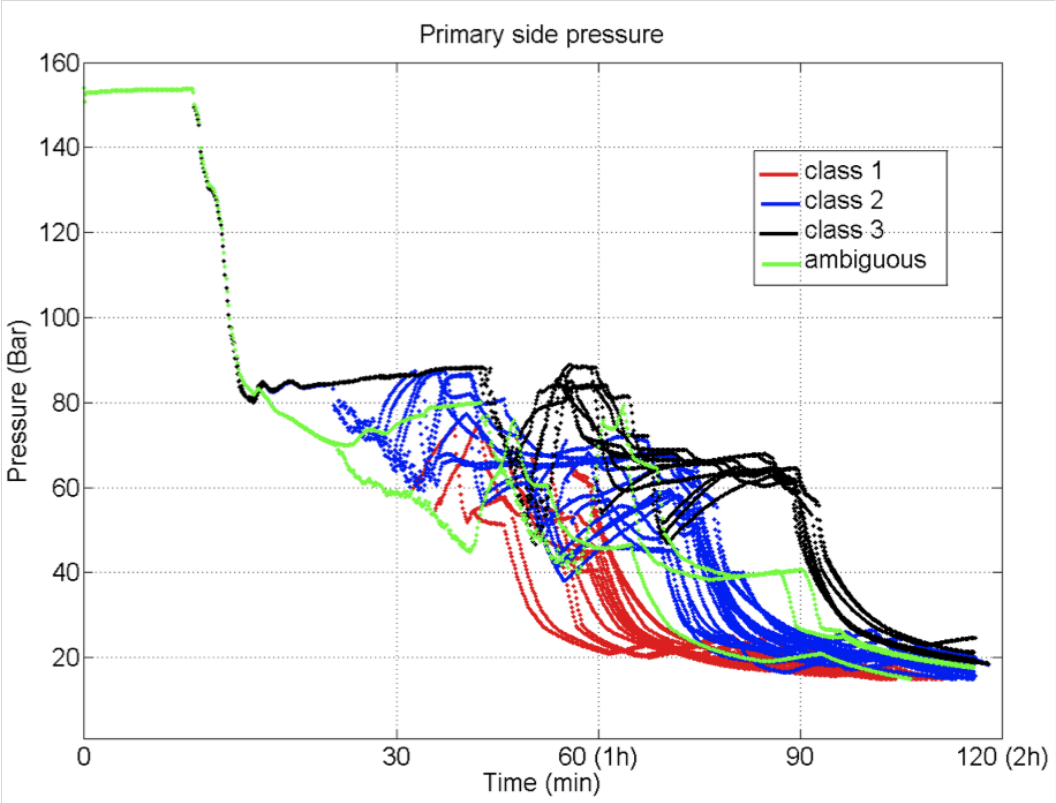



**Fig. 6.14:** Primary side pressure traces.

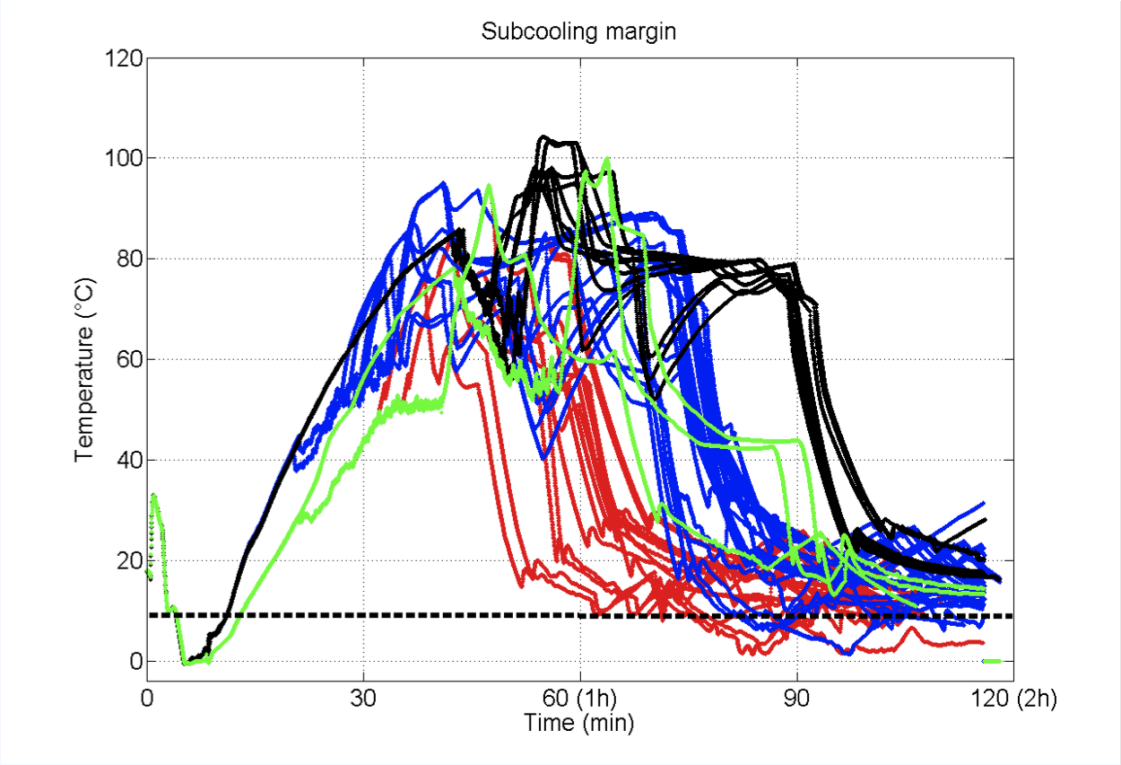



**Fig. 6.15:** Subcooling margin traces (red = class 1, blue = class 2, black = class 3, and green = ambiguous).

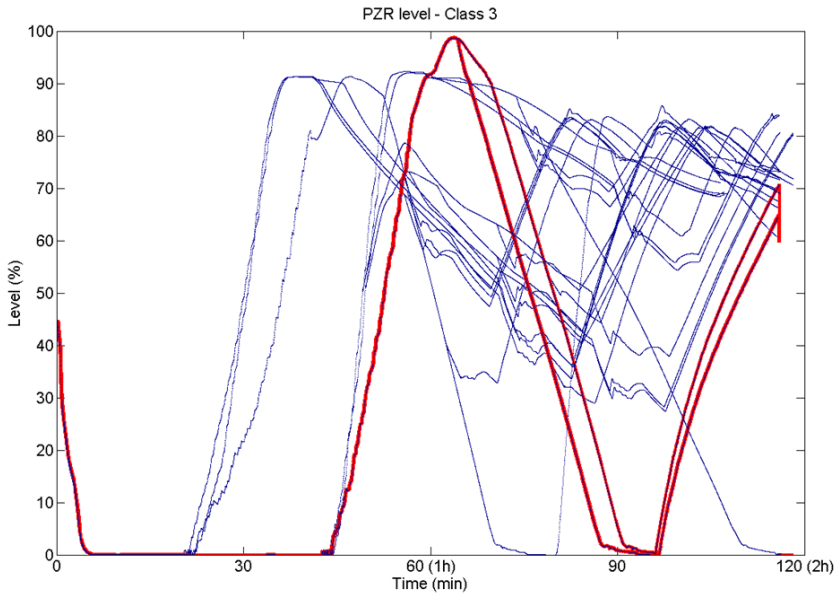



**Fig. 6.16:** Pressurizer level traces. The red traces correspond to scenarios close to pressurizer overfill.

In this analysis, it has been demonstrated that by using a dynamic approach, it is possible to model a spectrum of scenarios based on different strategies in executing actions. Additionally, one can directly see the effect of actions on the plant parameters. The timing in execution of actions and therefore the performance of the crew, may impact the next phase of the scenario and the following criterion or criteria that can be met. For example, if the next criterion to be analyzed is the success of the LPI, the fact that the operators did a fast or slow depressurization is relevant. In fact, if the operators were fast to depressurize and there is LPI failure, they would have more time to take recovery actions (like starting the firewater system) with regard to slow crews. Once again, the timing in executing actions and the strategy utilized impact the system response but also the dynamic execution of the next series of operator actions.

**Safety insights from failure scenarios** Safety insights can be drawn from the identification of failure scenarios in the three features, i.e., primary pressure, subcooling margin, and pressurizer level. In fact, by combining scenarios leading to failure in the three features, a list of events or type of events leading to undesired situations can be made.

Figure 6.17 presents the combination of events leading to failure in the three features. They are represented in a tree logic in order to see the type of relationship between different events.

From this dynamic analysis, some conclusions can be drawn for the specific depressurization action.

The 90-minute criterion taken in isolation may be not a bounding criterion for the safety of the system as stated in the reference PRA. The fact that the operators are not able to meet the 90 minute for the depressurization, does not mean that the system goes in an unsafe region. On the other hand, there are situations where the criterion is met but the system goes in unsafe regions if other features (the SCM feature for instance) are considered. When considering the operator action for depressurization or any other action, one should consider also other important failure modes like the failure to main-

tain subcooling margin and overfilling of the pressurizer. This shows that the dynamic approach allows safety to be assessed in terms of multiple interacting criteria.

Using a 90-minute time window as a model of failure does not reflect the context where the action is taken and other important insights about what makes this action difficult. The characterization of the context due to the variability in dealing with the scenario gives insights to be taken into account for a comprehensive analysis of the human actions as it will be shown in the next Section.

As a general conclusion, the depressurization of the system appears more challenging than expected in classical HRA, which did not address important features of the action. The main difficulties identified are:

- if there is enough SCM and the operators decide to stop two HPIs but the spray has been stopped at 3 or 5 meters, the system goes to an unsafe region;
- in case of failure of steam dump, at the most 1 HPI working, and the operators are too late to transfer to the SLOCA procedures, it is better to be fast in stopping the HPI in order to have safe conditions; and
- a slow transfer to the LOCA procedure combined with slow stopping of the HPI pumps leads to system failure.

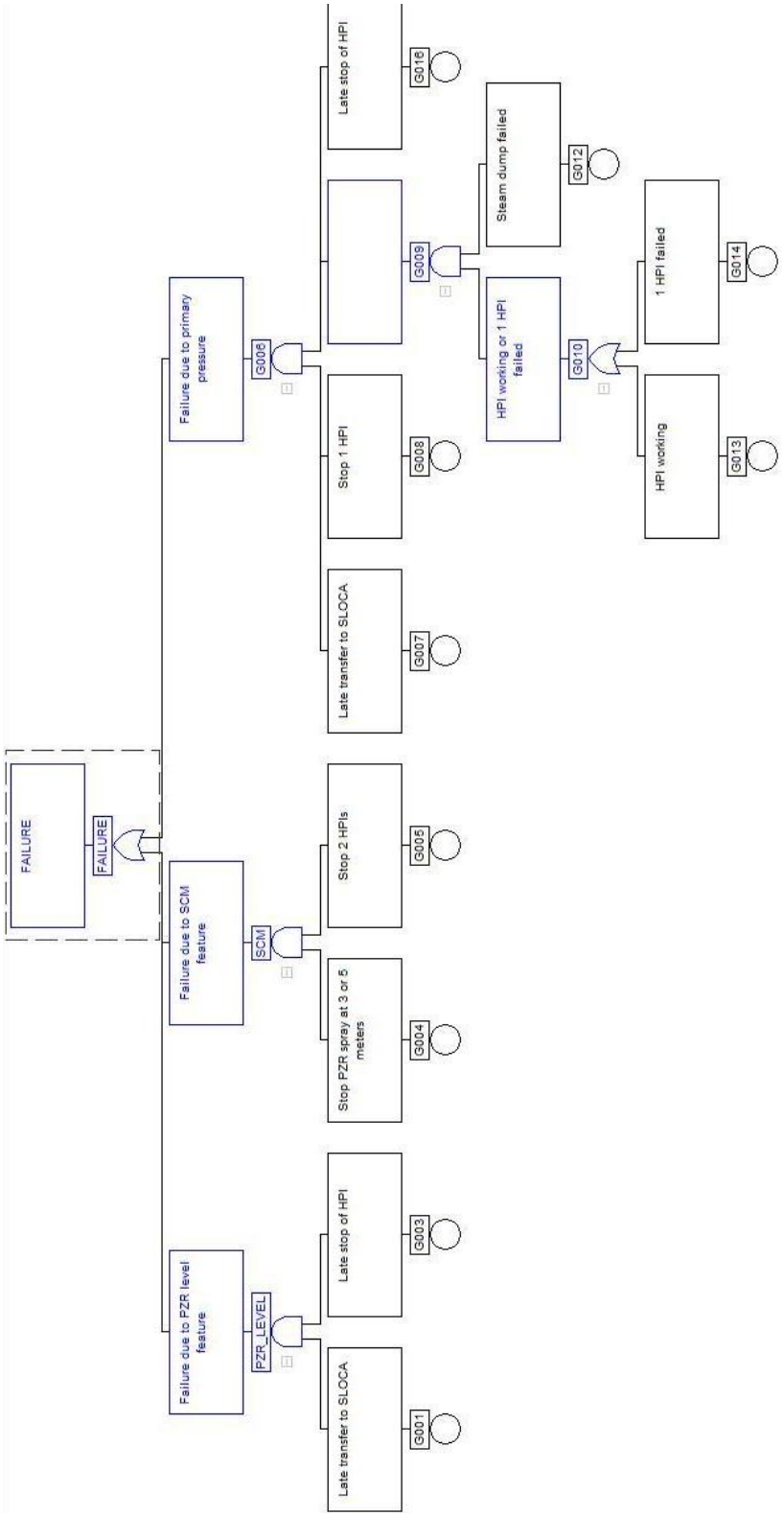



**Fig. 6.17:** Combination of events leading to failure in a fault tree format.

**Characterization of the context of the operator actions**

The analysis of the DDET-generated results from the previous Section, has demonstrated that the 90-minute rule for the depressurization action may not be a sufficient indicator of safety. The context which the operator actions takes place, is relevant for the success of the operator action and was not identified as a significant factor in the reference PRA.

The analysis of the fast crew behaviors, shows that those crews are mainly characterized by the fast time to start depressurization and by the stop of two HPI pumps instead of one. For some of them, these actions have generated a loss of SCM (with a probability of occurrence of 0.0014) with the risk of having boiling in the primary system. This situation will influence the next task: in such a situation, the operators may restart one HPI pump in order to increase the SCM; this will lead the crews to behave overall like slow crews with the risk of delaying the completion of the depressurization.

On the other hand, slow crews are characterized mainly by the stopping of one HPI pump at a time (since at the point in the procedure when they have to stop the HPI system operators have decided to stop only one HPI pump because of low SCM); they prioritize keeping the PZR level and hesitate to stop the last HPI. Therefore, these dynamic constraints will delay the completion of the depressurization.

From the analysis of the results the following issues related to the depressurization action have been identified:

- the dynamic constraints influence the crew response, i.e., operators cannot shut down two HPI pumps when there is not enough SCM and they will behave as slow crews;
- different crews may privilege different strategies. For instance fast crews give precedence to the fast depressurization (with the risk for some of them to lose SCM) as opposed to slow crews that concentrate on maintaining SCM; and
- the crews during the scenario evolution have to deal with competing goals. In

particular, they would like to depressurize as fast as possible, maintain SCM, and maintain the pressurizer level; but in order to accomplish these goals they have to perform competing actions: shut down to pumps (reducing pressure but losing SCM), stop one pump per time (maintain SCM but slowing the depressurization and losing more mass through the break), and spray long (maintaining the pressurizer level but losing SCM).

All these issues highlighted in the dynamic analysis were not addressed in the reference PRA and may make the scenarios more challenging than anticipated.

Furthermore, the variability of the scenarios as represented in Figure 6.13 depends on the timing of occurrence of events in addition to dynamic constraints, different strategies, and competing goals provided by the crew-plant dynamic integrations.

All of these results have an impact on the HRA results as will be demonstrated in Section 6.2.3.

**Other important results from a dynamic approach**

Other results important to inform HRA is the understanding of the performance of the operators to control the plant. Especially, the timing of performing procedure steps by different crews will be explored. The classifier developed in Section 4.4 has been used to help the analysis of the DDET-generated scenarios. This will also inform HRA on the factors that make the scenario more complex than expected.

The control of the plant by control room operators is an important aspect because depending on the plant control there might be situations where the context leads the operators in different directions than expected. This does not mean that failure scenarios necessarily follow but different performance conditions may arise, which need to be considered in the PSFs.

In this analysis, the classifier has been applied to identify scenarios which are similar in terms of procedure step timing. This explains how different crews are able to perform

the procedure steps and the impact of their performance on the plant control.

In this analysis the timing of entering into nine procedure steps has been considered. The actions in the steps are: *start the cooldown*, *start spraying*, *stop spraying*, *stop first HPI*, *stop second HPI*, *stop third HPI*, *start charging*, *start spraying again*, and *stop spraying*. These steps have been chosen because they comprise the main actions that operators must take during the scenario evolution. In Figure 6.18 the timing for the different steps is shown.

In Figure 6.19 four main characteristic types of behavior are shown which are used as prototype for the classification. There are crews that start fast and keep performing fast (class A), others that start fast and slow down later (class B), crews that start slow and keep performing slow (class C), and crews that start slow and later speed up (class D).

In order to give an idea of the crew speed, the plot shows the distance between the procedure steps in time. The larger the vertical distance and the slope of the lines, the slower the crew is.

The two classes of crews A and B perform the first steps rather quickly (until the *start charging* step and *start spraying*) then in the late phase their speed decreases quite fast with regard to the two other classes C and D. This is an indication of the workload of the different crews. In case of crews C and D, in the beginning of the scenario they start rather slow in entering the procedures; this means that they have more time to control other parameters like the cooldown rate and the SG levels. In contrast, the A and B crews control those parameters in the late phase of the scenario (then they have to slow down the performance of the procedures).

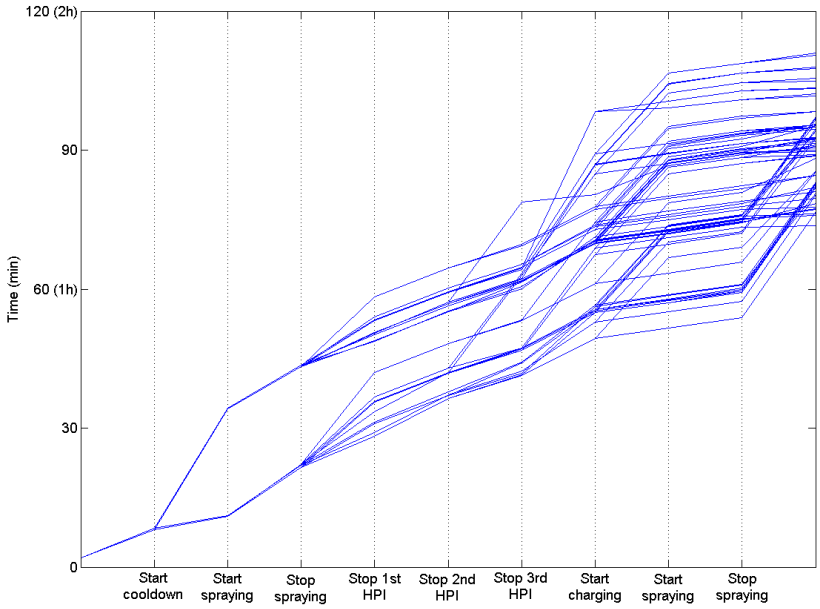



**Fig. 6.18:** Procedure step timing.

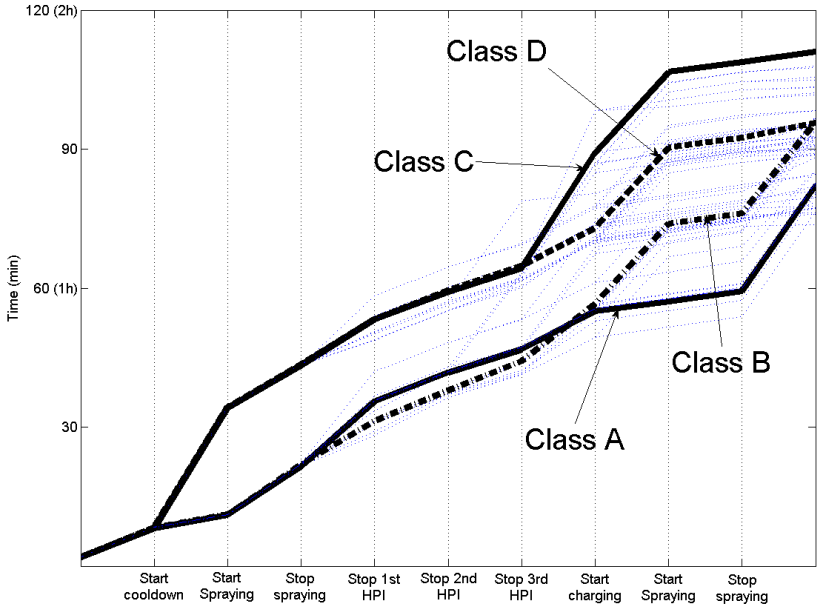



**Fig. 6.19:** Procedure step timing for the four identified prototypes of classes A, B, C, and D (marked lines).

Using the classifier, the crews that have behaviors like class A, B, C, D, or none of them have been identified. In the training phase a set of 12 patterns have been given. Then the 81 DDET-generated sequences have been tested in order to identify the four classes A, B, C, and D and also unknown scenarios (i.e., scenarios not belonging to any of the four classes). The classifier recognizes 11 class-A scenarios, 16 class-B scenarios, 12 class-C scenarios, and 21 class-D scenarios. The remaining 21 scenarios have been classified as unknown.

The unknown scenarios are scenarios that have an intermediate behavior. In fact, 12 of them start belonging to the class D (they are slow crews initially) and then they became class B (they speed up more than the average speed of the late phase of the class D crews). Six of them perform in the other way around (they start fast and slow down in the late phase of the scenario). The other remaining two are behaviors between class A and B and between class C and D. They are basically in the edge of the two classes (A-B and C-D).

In Table 6.5 the relative probability of each class are reported with also the number of scenario per class and the sequence number belonging to the class. As one can see, the contribution in term of probability of occurrence of the class C crews is very low (0.283 %) even if the number of scenarios of that class is comparable to the number of scenarios of the other classes. This means that there are a few crews that perform for the entire scenario evolution as very slow crews in performing procedures. Vice versa the probability of the class A crew is the highest, that is many crews start the scenarios fast and they finish fast in performing procedures. It is worthwhile to underline again that the plots which have been shown in Section 6.1 do not take into account the probability of occurrence; this means that the probabilities associated to the traces are different.

The scenarios belonging to the classes A and D are the ones with highest conditional probability. Scenarios belonging to these two classes are further analyzed to identify the main contributors. In particular, for class A scenarios one of the main contributors is the timing in performing the two steps where time variability is modeled, i.e., transfer

to the SLOCA procedures and stopping the last HPI pump. The opposite is not true meaning that the fact that the operators perform as fast does not imply that they perform procedure steps quickly, i.e., they do not belong to class A scenario. There are definitely other factors to be taken into consideration that lead the scenario to belonging to another class and not to the class A. In fact, scenarios where the operators perform fast but there is failure of one HPI are classified to other classes than class A (even in scenario where there is recovery of the HPI). Those scenarios are mainly classified as class B, i.e., fast at the beginning but slow in the second phase of the scenarios. This is due to the fact that when the operators responding according to the procedures have to stop the HPI (which is failed), they try to restart or recover it, delaying the execution of the subsequent procedure steps.

With regard to the class D scenarios, the main contributor to that group is a slow timing performance in executing the procedure steps, i.e., all the class D scenario have a slow timing performance in executing the procedures pattern. As in the case of class A, the reverse does not apply. There are several scenarios belonging to this class that are particular in the sense that it is not the timing variability that lead them to the class but the fact that one HPI is failed (e.g., sequence number 26). As in the previous case, the failure of the HPI influences the timing in the following phase of scenario leading it to class D.

The same type of analysis can be done also for the class B scenarios even if the associated probability is lower than the other two classes. The class B has not been considered because the associated probability is very low.

Based on this classification the main contributors to the different classes are the timing of executing procedure steps and the success or failure of one HPI system. This give some information about what must be taken into consideration when performing an HRA, i.e., the time to perform a task is not only a function of the crews but can also be strongly influenced by the scenario.

**Table 6.5:** Probability of each class, number of scenarios belonging to the class, and sequence number.

| | **Class A** | **Class B** | **Class C** | **Class D** | **Unknown** |
|---|---|---|---|---|---|
| **Probability** | 0.301 | 0.166 | 0.00283 | 0.303 | 0.227 |
| **Number of scenarios** | 33 | 48 | 36 | 63 | 63 |
| **Sequence number** | 1, 3, 9, 11, 17, 19, 58, 59, 70, 74, 78 | 2, 10, 12, 18, 20, 29, 30, 42, 43, 54, 55, 60, 61, 71, 75, 79 | 27, 28, 36, 37, 40, 41, 46, 47, 48, 49, 52, 53 | 6, 8, 14, 16, 22, 24, 25, 26, 33, 34, 35, 38, 39, 50, 51, 65, 68, 69, 73, 77, 81 | 4, 5, 7, 13, 15, 21, 23, 31, 32, 44, 45, 56, 57, 62, 63, 64, 66, 67, 72, 76, 80 |

### 6.2.3 Input to HRA

The analysis of the results from Section 6.2.2 will be used in this section for the calculation of the HEP for the depressurization. In particular, the issues identified based on the dynamic analysis about the dynamic constraints, different crew strategies, and competing goals are used to inform the HRA analyst on the evaluation of the factors that influence the human performance, i.e., the so called Performance Shaping Factors (PSFs).

PSFs are factors that influence the human performance in complex systems. Table 6.6 presents a set of representative PSFs for post-interaction human failure events; these are used in the SPAT-H HRA method [NUREG/CR-6883, 2005]. The rating of the PSF is a multiplier where a multiplier less than one has a positive effect on the operator action whereas a multiplier larger than one has a negative effect.

**Table 6.6:** List of Performance Shaping Factors for HFEs.

| **Performance Shaping Factors** | **Description of the PSF** |
|---|---|
| Adequacy of time | Measure of time required to act compared with the time available |
| Stress and workload | Rate the impact of the environment on the performance of the operator in doing the action |
| Task complexity | Rate the effect of multiple requirements on task success |
| Training and experience | Measure the effect of the familiarity and confidence of the operators with the action |
| Procedural guidance | Rate the plant procedures to enhance the operator's ability to perform the action |
| Plant interface and indications of conditions | Rate the impact of the man-machine interface on the likelihood of success |
| Fitness for Duty | Measure whether the individual performing the task is physically and mentally fit to perform the task at the time |
| Work Processes | Refer to aspects of doing work, including inter-organizational, safety culture, work planning, communication, and management support and policies. |

The action chosen for the calculation of its HEP is the cooldown (and therefore the depressurization) of the system and it will be analyzed with the SPAR-H method [NUREG/CR-6883, 2005]. The method is briefly described in Appendix G where also the detail of the calculation of the PSFs and the HEPs with a classical approach and a dynamic approach are presented. In the SPAR-H method, the operator action is divided in diagnosis and execution and an HEP for both the diagnosis and the execution is calculated. The HEP for the action ($HEP_{ACTION}$) is the sum of the diagnosis HEP ($HEP_{diag}$) and the execution HEP ($HEP_{exec}$):

$$HEP_{ACTION} = HEP_{diag} + HEP_{exec} = f(PSFs)_{diag} + f(PSFs)_{exec} \tag{6.1}$$

The reference PRA states that operators have about 10 minutes for the decision to cooldown and about 80 minutes to execute the relative actions to cooldown. Based on this input and on the knowledge of the HRA analyst on the plant behavior, on the procedures,

and on the PRA, the multiplier to the PSF can be assigned.

Table 6.7 summarizes the HEP values identified using the classical SPAR-H method (second column) and with dynamic insights (third column). In particular, the value calculated with the classical SPAR-H is $3.5 \cdot 10^{-2}$ whereas the HEP with dynamic insights is $7.5 \cdot 10^{-2}$, i.e., about two times higher than the one predicted by the classical HRA.

The difference between the two approaches comes from the value of the PSF complexity multiplier. In fact, based on the results of Section 6.2.2 about the dynamic constraints, different strategies, and competing goals, the PSF related to complexity in the execution phase increases, which makes the $HEP_{exec}$ about two times higher than the one from the classical SPAR-H.

Notice that the results from Section 6.2.2 will inform only the execution HEP and not the diagnosis. In fact, the main issues the operators are faced to are not problems in the diagnosis of the accident but in the execution of the system cooldown and the depressurization which is more challenging than stated in the reference PRA according to the analysis of dynamic results.

The details of the calculations can be found in Appendix G.

**Table 6.7:** HEP values calculated with the classical SPAR-H method and the SPAR-H method with safety insights.

| | **classical SPAR-H** | **SPAR-H with dynamic insights** |
|---|---|---|
| $HEP_{diagosis}$ | $2.5 \cdot 10^{-2}$ | $2.5 \cdot 10^{-2}$ |
| $HEP_{execution}$ | $1.0 \cdot 10^{-2}$ | $5.0 \cdot 10^{-2}$ |
| $HEP_{ACTION}$ | $\mathbf{3.5} \cdot 10^{-2}$ | $\mathbf{7.5} \cdot 10^{-2}$ |

With regard to how to use the results from the calculation of the HEP, the two approaches give different important results in this specific case study. If one calculates the HEP based on the classical SPAR-H method, the diagnosis part of the HEP is more important than the execution ($2.5 \cdot 10^{-2}$ vs. $1.0 \cdot 10^{-2}$). This suggests that to decrease the probability of failure for this specific HFE, improvement on the diagnosis of the accident must be done; for instance, improve the alarm systems or the aids to the operators to

diagnose the SLOCA. On the contrary, based on the dynamic simulation of the scenario, the main issues for the operators are related to the execution of the action ($5.0 \cdot 10^{-2}$ vs. $2.5 \cdot 10^{-2}$). This means that in order to decrease the probability of failure of this specific action, the execution of the action must be improved; for instance, the procedures can be improved or additional automatic controls must be added.

The better characterization of the context of the action will help the HRA analyst on the estimation of the HEP through the information on the PSF.

### 6.2.4 Analysis of a second PRA action to obtain HRA insights

In this Section, other results from a dynamic approach about a second PRA action from the reference PRA are analyzed to obtain HRA insights. This addresses the actions to cooldown the RCS, in SLOCA scenarios with HPIs and accumulators not available. This analysis refers to an additional 22 sequences generated by the DDET tool. These sequences differ from the already described 81 sequences because in this case the HPIs and accumulators are guaranteed failed, meaning that they do not inject water into the reactor. Thus, the goal is to reduce the pressure as fast as possible to allow injection from the accumulators (at 26 bars).

In this case, the required actions and success criteria are, in contrast to the sequences with HPI discussed in Section 6.2.2, that the operators have cooldown at the maximum cool down rate rather than at 100K per hour. The maximum cooldown rate is limited by the secondary pressure rate of -4 bar/minute. If the secondary pressure decreases at a rate exceeding 4 bar/minute (an indication of a possible steam line break), a steam line isolation signal will isolate the steam generators, causing the loss of heat removal through the secondary side.

Classical PRA calculations are made in order to identify the cognitive time window available for operators to take the decision to start the fast cooldown. If the operators start the rapid cooldown within the maximum time window, the primary temperature of

the system can be reduced to 180 °C and the primary pressure to 10 bar avoiding core uncovery.

The classical PRA approach is to identify the maximum $T_{max}$ time necessary to cooldown the plant to safe conditions, meaning that the isolation signal and core uncovery are both not reached. The time is calculated considering that the operators are able to depressurize the system exactly at -4 bar/min. Based on that maximum time, the available cognitive time $T_{cog}$ is therefore calculated. The $T_{max}$ is calculated based on thermal-hydraulic calculations and it is fixed. The $T_{max}$ is associated with maximum point where the criteria for the actual operator action are met (e.g., no significant core uncovery and secondary pressure reduction less than 4 bar/min when reaching the target pressure $P_{target}$). Therefore, following the criterion of -4 bar/min backward, the point where the action starts is identified and then also the available time to take the decision to cooldown, i.e., the cognitive time $T_{cog}$, is characterized.

According to the reference PRA model, the maximum time to reach 10 bars of primary pressure ($T_{max}$) is 30 minutes with no core uncovery and activation of the steam line signal. The calculations show also that the cognitive time ($T_{cog}$) is 10 minutes since it takes 20 minutes to cooldown at the maximum possible rate.

The dynamic analysis of the operator action has been divided in three parts: first the correct aperture of the PORVs has been identified for the nominal scenario, second the effect of the timing variability in starting the cooldown has been analyzed, and third HRA insights are derived from the analysis.

**Identification of the correct cooldown rate**

According to the operating procedures, the control room operators are instructed to normally cooldown the system at a rate of 100 K/h through the steam dump valves or the safety valves. In case the HPIs are not available, the operators must increase the cooldown rate. In the PRA the rate is not specified but it says that the operators must initiate a

rapid cooldown for low pressure injection (10 bar) or to 26 bar when the accumulators are available. The cooldown rate must be equivalent to a secondary pressure reduction of about 3.5 bar/min in order to avoid the steam line isolation signal (-4 bar/min). The second criterion that must be met is that there should not be a significant core uncovery.

This first analysis is the identification of the correct aperture of the steam dump valves (PORVs) to meet the -4 bar/min of secondary pressure reduction criterion. In this case study, during the accident it has been assumed that the operators do not actuate a manual control of the cooldown rate continuously monitoring the secondary pressure reduction. Therefore, a manual control of this parameter has not been added in the analysis but within the DDET framework only the identification of the correct aperture of the valves has been performed.

Using the current plant model, the three steam dump valves (one per secondary side loop) have been opened at 0.5%, 5%, 10%, 20%, 50%, and 100% of the total capacity. As soon as those valves are required, i.e., at the procedure step to start the cooldown, six branches are generated. The idea of this run is to identify to correct opening of the valves for a correct cooldown rate to be further used for modeling the crew timing variability in starting the cooldown rate.

Figure 6.20 and Figure 6.21 show the behavior of the primary and secondary side pressures for the different scenarios due to different apertures of the steam dumps. As one can see, different apertures of the valves lead to different behaviors. For example, if the valves are opened at 0.5% there is no way to depressurize the system whereas if they are fully opened, the decreasing of the pressure is quite fast and the constrain of -4 bar/min is not fulfilled (Figure 6.21). The same applies for apertures of 10%, 20%, and 50%. In these situations, due to extreme plant parameter behaviors, the plant model is not properly working and the sequences are truncated by the tool.

Therefore, the correct aperture of the valves has been identified as 5%. With these apertures, the operators are able to cooldown the plant in safe conditions with the constrain of -4 bar/min for the secondary side cooldown. This opening of the valves is then

further used to model the timing variability in starting the cooldown.

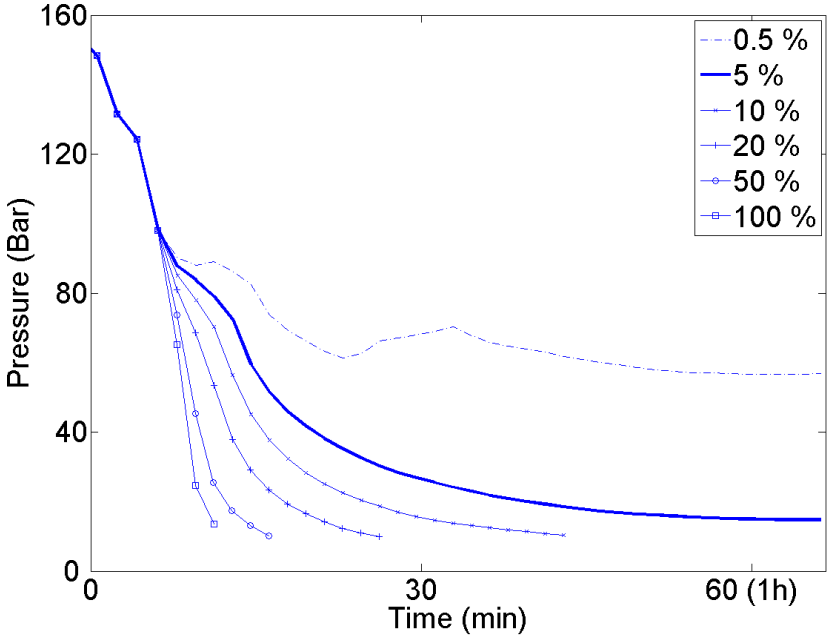



**Fig. 6.20:** Primary side pressures.

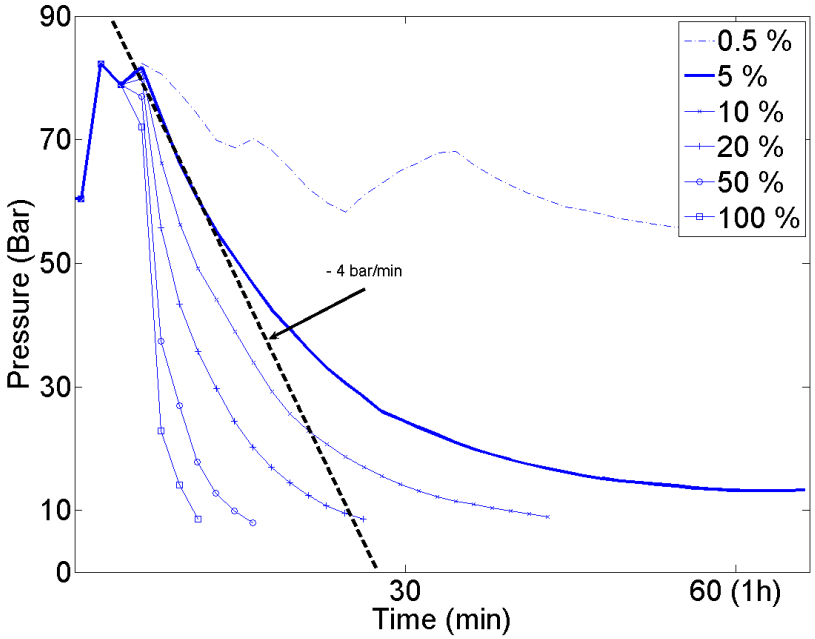



**Fig. 6.21:** Secondary side pressures.

Figure 6.22 shows the behavior of the temperature in the primary side. In case of 0.5% the decreasing of the temperature is almost zero whereas if the aperture of the valves is too large the gradient of the temperature is too large and problems in the structure of the components may occur. In all the other sequences the operators are able to cooldown the system below 225 °C according to the PRA action.

In a classical PRA analysis, the calculation of the amount of time available for the operator to take the decision to start the cooldown is based on the assumption that the operator is actually following the cooldown rate that correspond to the -3.5 bar/h of depressurization in the secondary side. As one can see in the previous plots, the system is not able to be depressurized at -3.5 bar/h as said in the classical PRA but in the late phase of the scenario, the depressurization decreases due to the dynamics of the system. Therefore, the calculation of the available time for the operators to take the decision and in particular the time to cooldown the system must consider the dynamic behavior of the system.

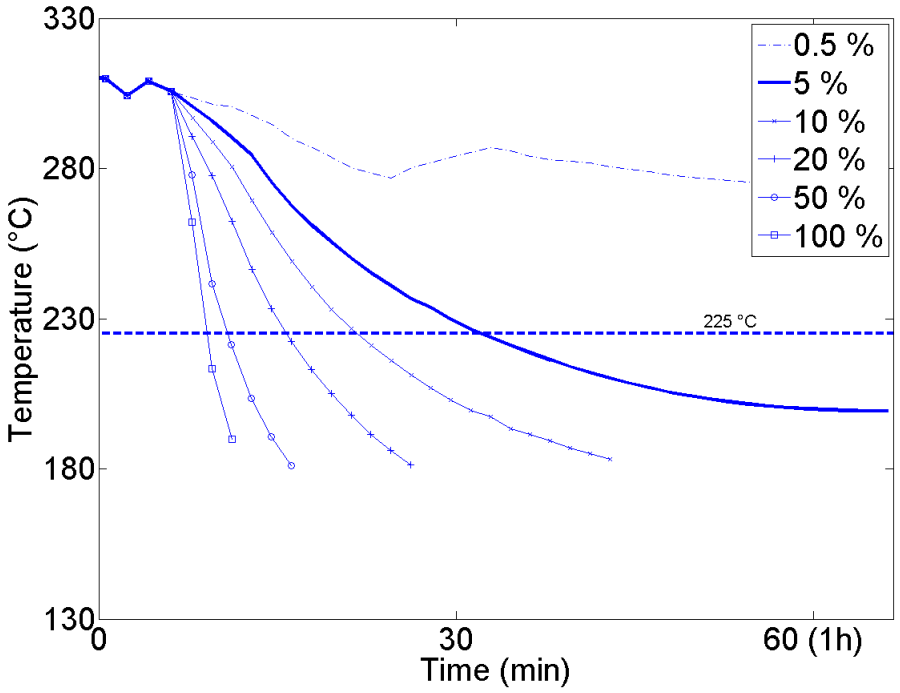



**Fig. 6.22:** Primary side temperatures.

### Timing variability in starting the cooldown

The second part of this work has been the modeling of the variability in the starting of the fast cooldown by the operators. The considered operator response has been chosen to be a Weibull distribution with shape parameter 500 and scale parameter 1.5. This distribution with the previous parameters have been chosen because the average of the distribution is about 7.5 minutes, i.e., a value of time slightly lower than the time identified by the classical HRA. Using a value less than the one calculated from the classical HRA the mass of the distribution is in the area covered by the classical HRA but at the same time, some variability of the response is given considering also extreme slow behaviors.

In this case study, 16 branching points due to the timing have been considered. The 16 modeled timings corresponding to 16 branches when the operators start the cooldown after they enter in the corresponding procedure step and the probabilities calculated by the given distribution are shown in Table 6.8. As one can see, the nominal scenario number, that is the highest probability scenario is the number 4.

**Table 6.8:** Scenarios number, timing, and probabilities for the fast cooldown rate.

| Scenario Number | Timing (s) | Probability |
|---|---|---|
| 1 | 50 | 0.0311 |
| 2 | 100 | 0.0545 |
| 3 | 200 | 0.1379 |
| 4 | 300 | 0.1482 |
| 5 | 400 | 0.1394 |
| 6 | 500 | 0.121 |
| 7 | 600 | 0.0993 |
| 8 | 700 | 0.0778 |
| 9 | 800 | 0.0587 |
| 10 | 900 | 0.0427 |
| 11 | 1000 | 0.0303 |
| 12 | 1100 | 0.0208 |
| 13 | 1200 | 0.014 |
| 14 | 1300 | 0.0092 |
| 15 | 1400 | 0.0059 |
| 16 | 1500 | 0.0037 |

Figure 6.23 shows the behavior of the primary side pressures for the generated five sequences. In several sequences, the pressure can be reduced to around 20 bar where the accumulators start. In several others, the simulations are truncated before reaching the desired pressure level because of extreme dynamic behaviors due to the fast cooldown rate.

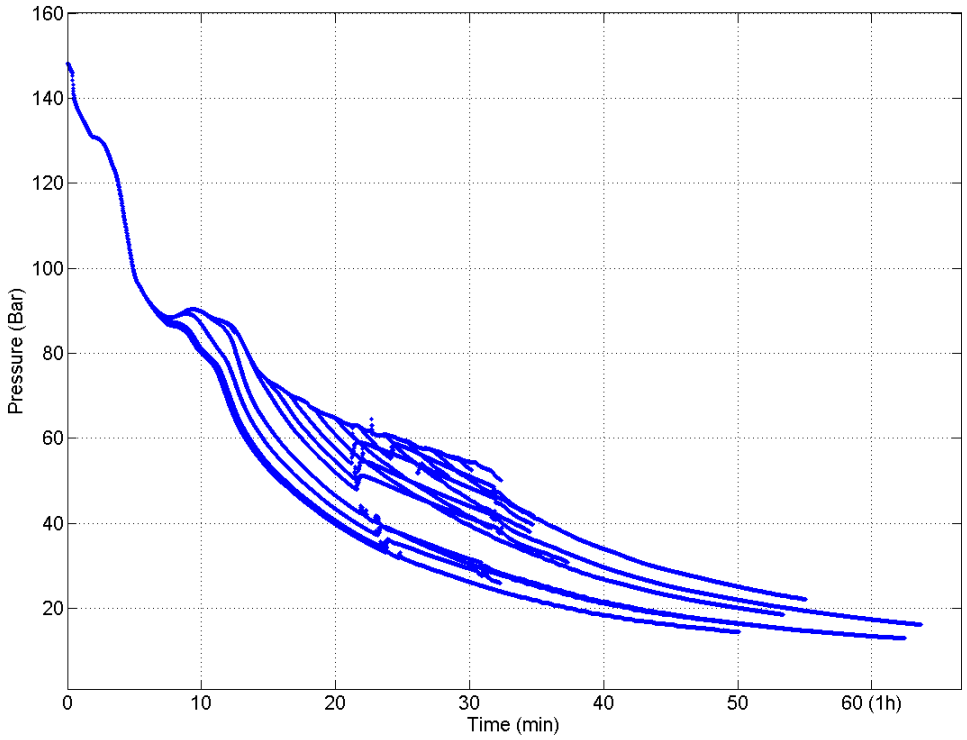



**Fig. 6.23:** Primary side pressures.

Figure 6.24 shows the behavior of the secondary side pressure. As one can see, there are two groups of sequences. The first one (blue traces) are scenarios where the criterion of -4 bar/min of depressurization is met whereas the second one (red traces) are scenario where the same criterion is not met. Therefore, for red scenarios the steam line isolation signal is triggered, which will delay the completion of the depressurization. The operator will have to reopen the steam line to continue cooling one of the steam generators or align alternative means for cooldown.

Those failure scenarios are the scenarios numbered 8 to 16. The probability of having a failure for the considered operator action is the sum of the probability of each red scenario, which is 0.2631. This probability can be interpreted as the error probability in the execution of the considered PRA operator action.

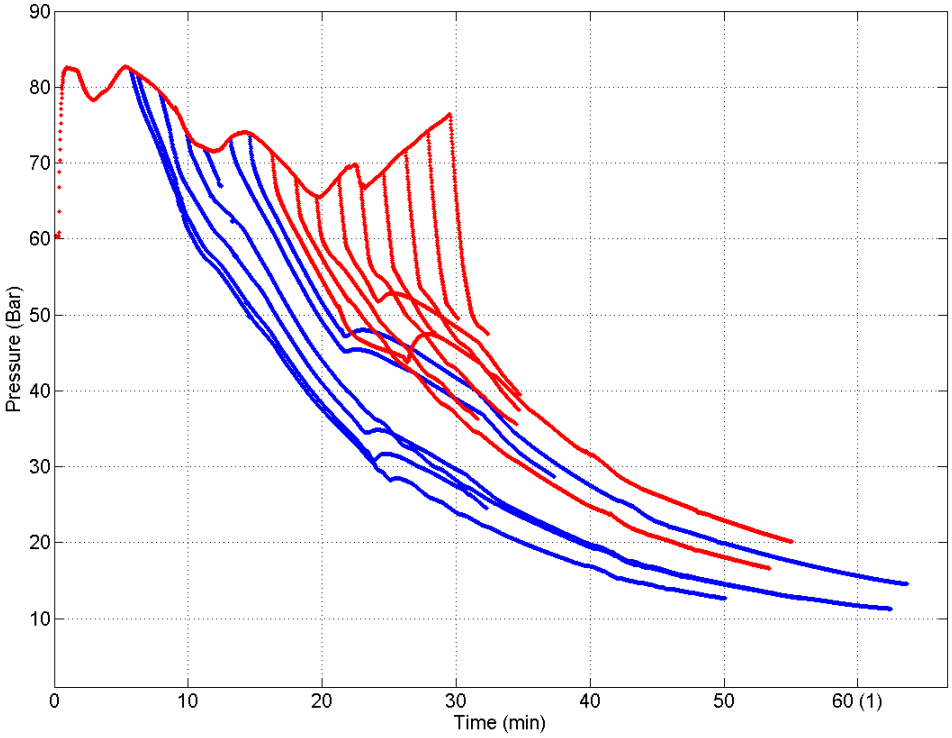



**Fig. 6.24:** Secondary side pressures.

According to this analysis, the system can be depressurized to about 20 bar until the operators take around 17 min to start the cooldown (sequence number 7). After that, due to the dynamic of the system, the depressurization becomes faster and the criterion of -4 bar/min cannot be met. These results show also that the time to depressurize the system is about 40 min in nominal conditions and 50 min at maximum (when the operators take about 17 minutes to start the cooldown). These results are less conservative than classical results where the available time to start the cooldown is 10 minutes.

In a dynamic approach, a better interaction between system and operators can be

modeled giving also a variability in the execution the PRA action. From this dynamic PRA approach there are mainly two results. The first one is that due to the dynamics of the plant, it is not possible to depressurize the system strictly following the -3.5 bar/min criterion because, as shown in Figure 6.24, after about 20 minutes, the depressurization rate decreases. This is because a fixed aperture of the steam dump valves is used. This assumption underscores that the operators need to adjust the steam dump valves during cooldown which could be a contributor to the HFE. The following insights can obtained: the operators have to start with a small aperture of the steam dump valves (above 5% it results in isolation of the steam dump valves and they risk to isolate the steam lines, thereby aggravating the scenario) then the operators need to open the dump valves later in the scenario, as the depressurization rate of the secondary decreases. If they delay in doing so, the cooldown takes longer. This means that the classical HRA has to consider that the operators start the cooldown within $T_{cog}$ but fail to depressurize at a sufficient rate overall (which means a steam dump valve aperture that does not trigger isolation, then a larger aperture later). So there is a possibility of omission.

A second result is the failure probability of this PRA action can be calculated as shown in the next section. The added value of a dynamic approach is the capacity to directly simulate the human-machine system interaction and then the response of the operator without the need of using studies available in literature based on other scenarios or generic scenarios. Therefore, the HEP for the specific action can change based on the direct simulation of the operator response in the context of DDET.

Many HRA methods focus on time constraint. Operators have only 10 minutes to take the decision to start the cooldown. This time constraints leads to a high value for the probability of failure. Using a dynamic approach, the context is better characterized and the direct effect of the variability of the operator actions on the plant can be seen and quantified. In addition, various allocations of time to decision and execution, respectively, may be accounted for.

**Analysis of the action to obtain HRA insights**

From the analysis if the PRA action modeled in a dynamic framework performed in the previous Sections, an HRA can be done using the SPAR-H method. In particular, some PSFs are informed by the analysis results and will be used for the estimation of the HEP.

Table 6.9 shows the results from a classical SPAR-H analysis and a SPAR-H analysis with dynamic insights. The details of the calculations can be found in Appendix G. In particular, both the diagnosis and execution HEPs decrease with the dynamic insights than the classical SPAR-H method. This reduces the final HEP of about three times, from 0.34 to 0.1.

**Table 6.9:** HEP values calculated with the classical SPAR-H method and the SPAR-H method with safety insights.

| | **classical SPAR-H** | **SPAR-H with dynamic insights** |
|---|---|---|
| $HEP_{diagosis}$ | 0.25 | 0.05 |
| $HEP_{execution}$ | 0.09 | 0.048 |
| $HEP_{ACTION}$ | **0.34** | **0.10** |

The dynamic insights used to support the HRA analysis are the complexity of the action and the available time for diagnosis and execution. The complexity the cooldown at the maximum allowed rate is higher than the one considered in the reference PRA. Therefore, the complexity PSF is evaluated more negatively in the case of SPAR-H with dynamic insights. On the contrary, both the available time for the execution and the complexity of the action is higher in a dynamic framework which make the diagnosis and execution PSFs related to the time lower that the classical PRA. The overall result is that the final HEP with dynamic insights based on the increase of the PSF of complexity in the execution and the available time in diagnosis and execution is lower than classical SPAR-H.

Therefore, in this specific case study, the HEP of the fast depressurization actions is decreased compared to the HEP based on the assumptions of the reference PRA.

The fact that an HEP increases or decreases with dynamic insights depends on the

specific case study and on the specific action. The DDET tool helps only the analyst to evaluate the PSF multipliers.

## 6.3 Methodology for HRA characterization

It has been demonstrated in the previous sections and chapters that the approach and methodologies developed during this PhD work can be used for a dynamic HRA. In particular, the ADS software tool with an operator or crew model can be used to model the mutual interaction between operators and systems in a NPP. This is done developing scenarios following any human-machine system interaction that could lead to different outcomes. The output is a DDET where several sequences are generated based on different interactions between operators and plant at discrete points in time.

Several issues arise from this mutual interaction and have been handled and solved during this PhD work: the crew timing variability, the probability calculation in DDET, and the grouping of DDET-generated scenarios to identify events making the most important groups for HRA. The latter is a step towards the development of importance measures for dynamic PRA.

The dynamic approach in addition with the post-simulation strategy, are important for the identification and characterization of failure scenarios and the context. In fact, failure scenarios or scenarios close to failure might show up during the evolution of the simulation based on the mutual human-plant interaction. Those scenarios, difficult to capture without a systematic approach, can be easily identified with a post-simulation approach. Once identified, they are subject of a further analysis whose scope is to identify the most important contributor to the scenarios and quantify their probability of occurrence. The probability of occurrence is strictly related to the HEP for a given action. Then using the developed methods, the HEPs for the actions modeled in the PRA can be estimated by applying an HRA method informed by the dynamic results.

It is worth to underline that groups of failure scenarios in one feature might not be

failed scenarios in others. This means that focusing on one success criterion does not represent very well a given HFE. The dynamic analysis helps to evaluate multiple criteria at once.

The approach developed during this PhD work can also be used for the characterization of the control of the plant by crews and the context for the assessment of the PSFs. This is based on a quantitative analysis of the DDET-generated scenarios in terms of probability. Groups of responses have been identified and probabilistically quantified based on their similarity in terms of different plant behaviors. The highest group probability has been therefore analyzed in details to understand and identify the main events leading to the highest probability groups. In particular, groups based on different timing on performing procedure steps have been labeled and probabilistically quantified. Groups based on particular parameter behaviors have also been identified and quantified. These results, can be used as a support to the HRA analyst in the assessment of some PSFs like complexity or timing of actions.

The approach based on many tools developed during this PhD thesis can be used for a human reliability analysis. In particular, a qualitative analysis for the identification of undesired situation and a quantitative analysis for the calculation of the failure probability for a given action can be done. Furthermore, a characterization of the context where the operators have to work can be done with this dynamic approach and conclusion about how the operators have to deal in handling the accident scenario can be drawn. For example how different actions impact the evolution of the next scenarios or the effect of the timing in executing particularly important actions.

Additionally, a dynamic approach can lead to a complete modeling of the crew-system interaction since what the operators see and what are their response can be directly simulated. Direct simulations of the crew-system interaction can lead to a reevaluation of success criteria and in some cases, to a reduction of some of the conservatism in the modeling of operator actions. The strength of a dynamic approach is to better characterize the context of operator actions especially when several factors and their interactions need

to be taken into account at the same time.

Through the analysis of the DDET simulation data of the current case study, the added value of a dynamic approach can be summarized as: *i*) reliable representation of the crew-system responses with respect to classical HRA because of the direct modeling of the operator behavior response at the level of plant interactions (based on both procedures and the training underlying the operators' responses) and the effect of their responses directly on the plant, i.e., on-line simulation; *ii*) usability of tools and methodologies for obtaining insights from NPP accident scenario simulations in DDETs; and *iii*) ability to inform HRA on several PSFs and calculation of HEPs.

The strategy used for obtaining these goals, after the scenario identification and input preparation, consists in the *a*) running of the DDET software tools; *b*) grouping accident sequences that are similar in terms of plant response and/or events; *c*) identifying the critical events that are key to the sequences with undesired outcomes or low safety level; and *d*) screening out events that lead to variability without affecting the outcome.

In order to demonstrate the capability of dynamic approaches, tools, techniques, and methodologies have been developed for obtaining a strategy for the analysis of scenarios of the human-machine system interaction. The main goals of the analysis of scenarios are:

- identification of the characteristics of the sequences that lead to failure based on plant evolution, hardware events, and operator actions;
- characterization of the causes that lead the operators to perform actions in the way they do within groups of similar scenarios. This focuses on what is causing the operators to perform actions or omit actions in the failure scenarios in the procedures, trained rules, and variability in trained rules;
- quantification of failure situations in the dynamic framework as opposed to classical approaches; and
- analysis of operator time window for operator actions from a dynamic point of view.

This PhD work is a further step towards dynamic PRAs in which the dynamic of the system is directly simulated along with the operator response The application of the developed techniques and strategy in the case study will demonstrate different ways in which operator-plant simulations can support HRA.

## Chapter 7

# Summary and conclusions

## Contents

## 7.1 General conclusions

Classical Probabilistic Risk Assessments (PRAs) and in particular Human Reliability Analyses (HRAs), treat accident sequence dynamics using quasi-static models. In addition, the interactions between crew and plant are treated considering only a small set of scenarios and the representation of the variability of the crew response is therefore limited. These are weaknesses of classical approaches than can be addressed with dynamic approaches.

Dynamic scenario analysis models that explicitly account for these crew-system interactions, are appropriate tools to help understanding the performance conditions under which human actions are required. Understanding these conditions is a fundamental input to HRA in particular with regard to the identification and quantification of failure scenarios, identification of events contributing to these failure scenarios, assessment of the Performance Shaping Factors (PSFs), estimation of the human error probabilities. In other words, this understanding is relevant to the prediction of how operators can fail in the situation assessment and of the likelihood of these failures.

The problems which have been addressed during this work are: *a*) identification of the key features of the crew response and implementation of a crew model in the DDET framework; *b*) development of an approach for time variability; *c*) improvement of a classification tool to address the post-simulation analysis; *d*) development of a method for biasing the DDET probabilities for avoiding the truncation of evolutions of potential interest; and *e*) application of the model in a case study for the evaluation of its impact and comparison with HRA.

As a result of this research project, the following has been learned:

1. Dynamic operator modeling provides the analyst a tool to characterize the performance of context and issues relevant to success of critical operator actions in NPP scenarios. In the case study performed in this work, the application of the tools led to the identification of the following types of issues:

- the variability in reaching critical points in the procedures which depends on how fast operators work, what are the scenario characteristics, and what is the current status of the plant;
- the dynamic constraints on operator actions;
- the different strategies that are permissible within procedures; and
- the effect of competing goals on the operator response.

2. The previous issues can be reflected in the HRA and can change the estimated failure probabilities.

   - Such issues were not identified in the PRA/HRA analysis of the case study scenario. Accounting for these issues in the HRA had a significant impact on the failure probabilities.

3. Some HRA data support the 'tendency' model for the representation of the crew response.

   - a few characteristic values of the response distribution are adequately to represent a wide spectrum of crew variabilities through the sequences;
   - the model is able to represent extreme behaviors, i.e., fast and slow crew responses, which would have been truncated by the DDET tool due to the regression to average behaviors.

4. For the analysis of DDET results, scenario diagnosis techniques, i.e., techniques for fault classification, can be adapted for DDET output data classification.

   - similar crew responses can be identified in the DDET output data; and
   - the output analysis can be substantially reduced due to the approach of grouping the sequences and analyzing only the prototype of the group.

5. An approach to prevent the truncation of potentially interesting scenarios is to boost the probabilities of crew-variability-related events. The actual sequence probabilities can be calculated in the post-simulation phase.

    - An approach to calculate the sequence probabilities during post-simulation was implemented by combining the classifier with a DDET parser; and
    - this can be useful if new information which leads to modifications of the stochastic event probabilities becomes available.

## 7.2 Significance and contribution of this research

The main objective of this study was to model and analyze the crew-plant interactions during accident scenarios in a Nuclear Power Plant. This study provides tools and methodologies for the treatment and analysis of the dynamic interactions between control room operators and plant and for the use of the dynamic approaches as a technique to inform the HRA. The NPP and the control room crew responses are simulated jointly through the ADS model. The novel aspect of the crew model in ADS is that it is based on a procedure-guided operator response, i.e., a combination between procedure-following and training-based responses.

For safety assessment, predicting and assessing crew performance involves understanding the indications available to the operators, and the procedures and training that support decision-making and performance in a given situation. In order to obtain a comprehensive understanding of the impact of the variability in the crew response and of the timing of the operator actions in a range of scenarios, dynamic simulation models where the operator response and the plant and its systems are jointly simulated like ADS are needed as demonstrated in this work.

The integrated modeling of the plant-operator response achieved in this study provides new capabilities to obtain insights by identifying interactions between the operators' re-

sponse and the system response as well as between procedure instructions and trained knowledge and rules. The understanding of these interactions provides an improved basis for HRA, by supporting the analysis of tasks and performance contexts, the quantification of HEPs, and the evaluation of PSFs for given actions.

The significance of this work is that with the use of dynamic tools such as ADS in addition with post-simulation tools, the response of the control room crews can be modeled giving some variability in the crew performance and evaluating the safety of the system due to hardware events and operator actions. Besides the simulation of different crews and the analysis of the impact on the safety of the plant, another strength of a dynamic approach is the use of the output scenarios analysis for informing HRA concerning the events leading to failure and also as an input for the quantification of PSFs and HEPs.

## 7.3 Outlook

Although this project demonstrated the practicability of using a dynamic simulation-based approach with a crew model in support of human reliability analysis, there are areas of potential further developments.

The crew model as currently implemented in ADS can support the HRA for the calculation of the HEPs. A step forward would be to improve the capability of the crew model adding the possibility to obtain as output the actual value of the HEP; this could be done including in the input of the model some parameters that take into consideration other variables like the level of training of the operators, the type of the available indications, the type of procedures in use, etc. In addition, a new feature of the model could be the calculation of the dependence level and therefore the probability of failure of two or more actions.

Currently, the model is able to identify events leading to failure from the DDET-generated data. A further step could be the development and implementation of a tool able to quantify the contribution of the events to the final state. This would open up an

interesting research branch in the direction of importance measures for dynamic HRA, i.e., prime implicants.

Moreover, extending the capability of the model to handle accident scenarios subsequent to core damage (level 2 PRA) is another issue. The main problem is to couple to ADS a thermal-hydraulic code able to model scenarios for level 2 PRA like MELCOR or MAAP. From a point of view of the crew modeling in ADS this is straightforward since the procedure framework developed in this work considered with the model of for rule-based actions should be adequate for the simulation of crew responses guided by the Severe Accident Management Guidelines (SAMGs).

Nevertheless, it must be underlined that the simulation requirements in terms of memory and CPU are an issue for this type of simulation. As already stressed, the main bottleneck is the thermal-hydraulic part of the model. Parallel computing or cluster computers can allow a more detailed and precise analysis increasing the number and the length of the generated scenarios due to the higher speed of calculation. With additional speed, more characteristic values of continuous stochastic variables (task durations, system responses) can be considered and impact of the number of trains of a system that are available can be examined.

## Appendix A

# List of operator models

A summary of several operator models with the main characteristics is listed below.

Task simulation. It is based on tasks which have to be performed in certain available time. It models only the human part in the human-machine system interactions [Siegel and Wolf, 1969].

MICROCREWS. It has been derived from task simulation and it simulates the flow actions across time. It is the first direct application of task simulation to NPP [Gertman and Blackman, 1993].

PROCRU (Procedure Oriented Crew Model). It is directly based on task simulation but the machine is explicitly modeled in a human-machine system interaction. It models the knowledge-based of the operator. It contains four elements: monitoring process, assessment on the current situation, procedure selection, and action execution [Baron et al., 1982].

INTEROPS. It is a conceptual model based on task simulation. It includes a knowledge-based models for fault diagnosis, situation assessment, decision-making, and procedure generation. The operator may respond by selecting or identifying a procedure from a procedural knowledge base or generating procedure [Schryver, 1982].

TBNM (Team Behavior Network Model). It analyzes the cognitive process of a crew

in complex dynamic context. The cognitive process of the crew consists in: identification of the symptoms, decision making, planning, and execution [Shu et al., 2002].

CES (Cognitive Environmental Simulation). It treats mainly knowledge-based cognitive behavior addressing: situation assessment, diagnosis, formation of information-seeking interactions. The machine system is not fully integrated in the human-machine system model [Woods et al., 1987].

COSIMO (COgnitive Simulation Model). It is a model of a single operator that simulates situation assessment, response generation, and execution [P. C. Cacciabue, 1992].

NPPCREW. It models a NPP operating crew. It is based on the knowledge-based assessment. Each operator generates ands reviews expectations concerning the plant response and the response of other operators [Dang et al., 1992].

JACOS. It models both the knowledge-based behavior and the rule-based behavior. A multilevel flow model represents the operator's cognitive activities [Yoshida et al., 1996].

IDAC-2006 (Information, Diagnosis/Decision, Action and Crew). It is based on a cognitive simulation developed to predict the response of a crew in a control room of a NPP during an accident [Chang and Mosleh, 1999].

OPSIM (operator-plant dynamic simulator). It is a cognitive model of an individual operator. The cognitive model considers rule-based cognitive behavior in the following procedure as well as in responses based on the operator's knowledge-based [Dang, 1996].

DETAM (Dynamic Event Tree Analysis Method). It is based on the dynamic event tree approach in which branches are stochastically generated. It includes, as an integral part of the approach, an operator crew that also stochastically generates branches. An important feature is that the past states could affect the likelihood of a future state [Acosta, 1991].

SYBORG (Simulation sYstem for the Behavior of an OpeRating Group). It simulates the behavior of a crew during an accident scenario. In particular, it studies severe accidents involving human factors. The operator behavior model within SYBORG has

no learning mechanism and the knowledge about a plant is fixed; therefore it cannot take suitable actions when unknown situations occur, nor can it learn anything from the experience [Yoshimura and Takayanagi, 1999].

## Appendix B

# The supervised evolutionary possibilistic clustering algorithm for classification

This Appendix describes the classification technique adopted in the work. The combination of the fuzzy clustering classification with a possibilistic clustering for recognizing unknown patterns has been recently introduced by some of the authors in connection with the classification of nuclear plants transients, in an effort to aid the plant operators in diagnosing the causes of the transients [Zio and Baraldi, 2005a,b, Zio et al., 2005]. The approach was developed to avoid misclassification of scenarios that were possibly overlooked in the a priori identification step. As a result of the introduced approach, the unknown transients are labeled as unknown by the evolutionary possibilistic FCM clustering algorithm.

## B.1 Fuzzy and possibilistic clustering

Fuzzy clustering algorithms have been widely studied and applied in various domains such as taxonomy, medicine, geology, business, engineering, image processing and others

[Yang, 1993].

Fuzzy clustering classification is based on the fuzzy partition of each pattern $\vec{x_k}$, $k$ = *1, 2,...N*, into $c$ available classes:

$$0 \leq \mu_{ik} \leq 1,\ i = 1, 2, ..., c, k = 1, 2, ..., N \tag{B.1}$$

$$\sum_{i=1}^{c} \mu_{ik} = 1, k = 1, 2, , N \tag{B.2}$$

In particular, the "probabilistic" constraint B.2, that the memberships $\mu_{ik}$ of a given pattern must sum up to 1, is a generalization of the condition which ensures that in a "hard" (crisp) partition a pattern is a member of one class only and avoids the trivial solution of all memberships equal to 0. As a result of this constraint, the membership of a pattern to a cluster depends on the memberships to all other clusters, i.e., geometrically speaking, it depends on where the pattern is located with respect to not only that cluster but also the others. Hence, in the framework of fuzzy clustering the membership functions take the meaning of degrees of sharing, i.e., they measure how much a pattern belongs to a cluster relatively to the others.

The values of the found memberships can serve as a confidence measure in the classification [Keller et al., 1985]: for example, if a pattern is assigned 0.9 membership in one class and 0.05 membership in two other classes we can be reasonably sure that the class of 0.9 membership is the class to which it belongs. On the other hand, if a pattern is assigned 0.55 membership in class A, 0.44 membership in class B, and 0.01 membership in class C, then we should be hesitant to assign it to a specific class based on these results.

Under these conditions, two major drawbacks arise [Dubois and Prade, 1988]:

1. The constrained memberships cannot distinguish between "equal evidence" and "ignorance" or, in other words, between "equally likely" and "unknown" membership to a cluster.

2. Since most distance functions used in fuzzy clustering are geometric in nature, "noisy" patterns, i.e., lying far from the clusters, can drastically influence the estimates of the clusters prototypes and, hence, the final partition and the resulting classification.

In this situation, an "unknown", atypical pattern not belonging to any cluster would still belong more to one cluster than to the others, relatively speaking, even if it lies far from all clusters in the feature space and thus it may receive high membership values to some clusters. On the contrary, in our application it is required that unknown, atypical patterns be recognized as such, i.e., bear low membership to all clusters. In this respect, thus, the "conservation of total membership" constraint B.2 is too restrictive since it gives rise to relative membership values, dependent on the number of clusters.

To overcome the above limitations, the clustering problem can be recast into the framework of possibility theory [Dubois and Prade, 1988], [Klir and Folger, 1988]. In this view, the memberships of representative (typical) patterns are high, while unrepresentative (atypical) points bear low memberships to all clusters. In this interpretation, the membership function $\mu_{ik}$ represents the degree of compatibility of the pattern $\vec{x_k}$ with the prototypical member $v_i$, i.e., the center, of cluster $i$. If the classes represented by the clusters are thought of as a set of fuzzy sets defined over the Universe of Discourse (UOD), then there should be no constraint on the sum of the memberships. The only constraint is that the membership values do represent degrees of compatibility, or possibility, i.e., they must lie in [0,1]. This is achieved by substituting the fuzzy clustering constraints B.1 B.2 with the following [Krishnapuram and Keller, 1993]:

$$0 \leq \mu_{ik} \leq 1,\ i = 1, 2, ..., c, k = 1, 2, ..., N \tag{B.3}$$

$$\max_i\ \mu_{ik} > 0, k = 1, 2, ..., N \tag{B.4}$$

where constraint B.4 simply ensures that the set of fuzzy clusters covers the entire UOD.

A possibilistic distributions (and the corresponding fuzzy subsets) over the UOD [Krishnapuram and Keller, 1993].

## B.2 The evolutionary possibilistic FCM clustering

The traditional, unsupervised possibilistic algorithm based on a Euclidean metric to measure compatibility leads to spherical clusters that rarely are adequate to represent the data partition in practice. A significant improvement in classification performance is achieved by considering a different Mahalanobis metric for each cluster, thus obtaining different ellipsoidal shapes and orientations of the clusters that more adequately fit the a priori known data partition [Zio and Baraldi, 2005b], [Yuan and Klir, 1997].

The information on the membership of the available patterns $\vec{x_k}$, *k=1, 2,..., N*, to the $c$ a priori known classes, can be used to supervise the algorithm for finding the optimal Mahalanobis metrics such as to achieve geometric clusters as close as possible to the a priori known physical classes. Correspondingly, the possibilistic clustering algorithm is said to be constructed through an iterative procedure of "training" based on a set of available patterns, pre-labeled with their possibilistic memberships to the a priori classes. The training procedure for the optimization of the metrics is carried out via an evolutionary procedure, presented in the literature within a supervised fuzzy clustering scheme [Yuan et al., 1995] and further extended to diagnostic applications [Zio and Baraldi, 2005a]. Here, the procedure is employed within the possibilistic clustering scheme.

To this purpose, the distance $D(\Gamma_i^t, \Gamma_i^*)$ between the set $\Gamma_i^t$ (t = true) of memberships of the $N$ available patterns to the a priori known class $i$ and the corresponding set $\Gamma_i^*$ of the possibilistic memberships to cluster *i=1, 2,..., c*, is computed by:

$$D(\Gamma_i^t, \Gamma_i^*) = \sum_{i=1}^{N} \frac{|\mu_{ik}^t - \mu_{ik}^*|}{N} \tag{B.5}$$

where $0 \leq \mu_{ik}^t \leq 1$ is the a priori known (possibilistic) membership of the *k-th* pattern to the *i-th* physical class and $0 \leq \mu_{ik}^* \leq 1$ is the possibilistic membership to the corresponding geometric cluster in the feature space.

The target of the supervised optimization is the minimization of the distance $D(\Gamma_i^t, \Gamma_i^*)$ between the a priori known physical class partition $\Gamma_i^t \equiv (\Gamma_1^t, \Gamma_1^t, ..., \Gamma_c^*)$ and the obtained geometric cluster partition $\Gamma_i^* \equiv (\Gamma_1^*, \Gamma_1^*, ..., \Gamma_c^*)$:

$$D(\Gamma^t, \Gamma^*) = \sum_{i=1}^{c} \frac{D(\Gamma_i^t, \Gamma_i^*)}{c} = \sum_{i=1}^{c} \sum_{i=1}^{N} \frac{|\mu_{ik}^t - \mu_{ik}^*|}{N \cdot c} \tag{B.6}$$

The optimal membership functions $\mu_{ik}^*$, *i = 1, 2,..., c, k = 1, 2,..., N*, result from the minimization of the objective function:

$$J_m(\Gamma, \vec{v}) = \sum_{i=1}^{c} \sum_{k=1}^{N} (\mu_{ik})^{r_m} s_{ik} + \sum_{i=1}^{c} \eta_i \sum_{k=1}^{N} (1 - \mu_{ik})^{r_m} \tag{B.7}$$

where $\eta_i$ are suitable positive numbers and $r_m$ is an index that determines the fuzziness of the final possibilistic partition and the shape of the possibility distribution ($r_m \to 1$, the membership functions are hard, $r_m \to \infty$ they are maximally possibilistic).

The distance $s_{ik} \equiv s_i(\vec{x_k}, \vec{v_i^*})$ in Equation B.3 between the pattern $\vec{x_k}$ and the optimal cluster center $\vec{v_i^*}$ is computed by:

$$s_i(\vec{x_k}, \vec{v_i^*}) = (\vec{x_k}, \vec{v_i^*})^T \cdot \underline{\underline{M_i}} \cdot (\vec{x_k}, \vec{v_i^*}) \tag{B.8}$$

$\underline{\underline{M_i}}$ being the metric for the cluster $i$ proposed by the evolutionary supervised procedure and $T$ denoting the transpose operator.

**The classification algorithm**

When fed with a new pattern $\vec{x}$ the classification algorithm provides the values of the membership functions $\mu_i^*(\vec{x})$, *i=1, 2,..., c*, to the possibilistic clusters:

$$\mu_{ik}^* = \frac{1}{1 + \left(\frac{s_{ik}}{\eta_i}\right)^{\frac{1}{r_m - 1}}} \tag{B.9}$$

These values give the degree of compatibility or "typicality" of $\vec{x}$ to the $c$ clusters. In practice, three situations may arise (Figure B.1):

1. $\vec{x}$ does not belong to any cluster with enough membership, i.e., all the membership values are below a given threshold $\epsilon_f$ (degree of ignorance): this means that $\vec{x}$ is an unanticipated (unknown) pattern with respect to the training patterns.

2. at least two membership values are above the threshold $\epsilon_c$ (degree of confidence): $\vec{x}$ is thus ambiguous. In this case, the ambiguity must be regarded as "equal evidence", i.e., the pattern is typical of more than one class and thus cannot be assigned to a class with enough confidence. This situation occurs if $\vec{x}$ is at the boundary between two classes.

3. $\vec{x}$ belongs only to a cluster with a membership value greater than the threshold $\epsilon_c$: in this case, it is assigned to the corresponding class.

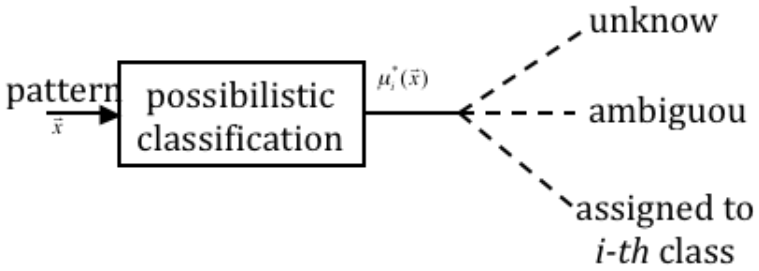



**Fig. B.1:** Classification of pattern $\vec{x}$.

## Appendix C

# Summary of work developed for this PhD work

This appendix summarizes the work that has been done during the PhD thesis. In particular, work the pure research in addition with development of tools, methodologies, and approaches to achieve the research goals introduced in Section 1.3. The following tables condensate the topics that have been developed and a short discussion about them. They are divided in five main groups: operator/crew model, plant model, accident dynamic simulator software tool, DDET modeling, and output analysis.

**Table C.1:** Operator and crew model topics and description.

| **Topic** | **Description** |
|---|---|
| Literature review of existing operator models | - A review of all the existing operator models and in addition the typical control room operator behavior has been also review in order to relate and compare the developed model with the existing one in literature. |
| Conceptual model | - A conceptual model ha been developed and integrated with the existing one in the ADS tool |
| Procedure-guided response | - A new procedure-guided model has been integrated into the operator model. |
| New crew operator | - A new operator has been added in the model, i.e., the supervisor who checks the safety functions to transfer to the SAMGs |
| HRA data handling and modeling | - HRA data has been used to validate the model developed in 3.1.4 for handling data related to crew performances. |
| Crew timing variability | - The crew timing variability issue has been considered and analyzed as explained in Section 3.1.4 |

**Table C.2:** Plant model topics and description.

| **Topic** | **Description** |
|---|---|
| Add new components, systems, and controls in the input deck | - In order to construct the case study an existing input deck has been used and many new components, systems, and controls have been introduced. |
| Modeling of the case study | - In order to decide which scenario to model, a review of the existing PRA documentation has been done. Then, the SLOCA event has been modeled based on some criteria described in Section 5.3. |

**Table C.3:** ADS tool topics and description.

| **Topic** | **Description** |
|---|---|
| Study of C++ programming language | - Self tutorial in studying the C++ programming language, i.e., the programming language of ADS |
| Analysis and study of the ADS code without operator model | - In order to understand the structure of the ADS code, the existing operator model has been removed and the framework of ADS code has been analyzed. |
| New input and output structure based on XML | - The input and output data structure has been rebuilt based on XML programming language. This language allows validation mechanisms reducing the likelihood of input errors and making the code more user friendly. |
| Debugging of the code | - An big effort has been done in debugging the code and solving a lot of existing bugs in the previous model. In particular part of the code has been reengineered to allow the integration with the new data structure a also lots of code conflicts has been solved. |
| Compiled RELAP with the Intel Visual Fortran compiler | - The RELAP thermal-hydraulic code has been compiled with the new Intel Fortran compile on window platform. |
| Compiled ADS with Microsoft Visual C++ 2005 and 2008 | - The compiler of ADS has been upgraded to the new Microsoft Visual C++ 2005 and 2008 in order to keep the code updated with the evolution of software compilers. |

**Table C.4:** DDET topics and description.

| Topic | Description |
|---|---|
| Literature review of DDETs | - In order to get familiar with the DDET concept a literature review of existing DDET model and also on dynamic models in general has been performed. |
| Branching generation due to expectations in the procedures | - Branching generation due to expectation within procedure steps has been added. This allow the operator to expect different values and to generate branches due to different expectations. |
| Branching generations due to skipping of procedure steps | - The possibility to skip procedure steps or entire procedures generating branching has been added into the model. |
| Branching generation due to different level of component level | - In the model, branches can be also generated if the operator for instance decides to open a valve at different levels. |
| Probability handling in the DDET | - A new approach and methodology to calculate the DDET probabilities at the end of the simulation has been implemented and validated. |
| DDET generation | - In ADS, a new way to generate the DDET based on XML has been introduced. This allows the possibility to parse the code with the developed DDET-parser. |

**Table C.5:** Output related topics and description.

| Topic | Description |
|---|---|
| Approach for output analysis | - An approach for the analysis of DDET-generated scenarios has been developed and applied in for the case study of this work. |
| DDET-parser | - A DDET-parser has been developed. The DDET-parser allows the possibility to visualize the DDET in different way, acting like a filter which extracts only information important for the analyst. |
| Output data analysis | - The analysis of the data has been dune using the approach developed in this work in addition with a classifier able to group scenarios based on similarity. |

## Appendix D

# Control Panel

This appendix shows the control panel implemented in the SLOCA case study.

...version="1.0" encoding="UTF-8"

...href="ControlPanelStyles.xsl" type="text/xsl"

...http://www.w3.org/2001/XMLSchema-instance

...file:/C:/XMLSchema/ADSSchemaFiles/ControlPanel.xsd

DisplayParameterValue

| | DisplayName | SystemName | ParameterName | CheckTime | ValueWhenFail |
|---|---|---|---|---|---|
| 1 | Waiting | CV_020 | Value | 20.0 | 0.0 |
| 2 | Time | CV_020 | Value | 20.0 | 0.0 |
| 3 | Watchdog_Timer | CV_019 | Value | 20.0 | 0.0 |
| 4 | Core_Power | CV_009 | Value | 20.0 | 0.0 |
| 5 | SUR | CV_008 | Value | 20.0 | 0.0 |
| 6 | del_k | CV_744 | Value | 20.0 | 0.0 |
| 7 | Clad_Temp_Max | CV_121 | Value | 20.0 | 0.0 |
| 8 | Fuel_Temp_Max | CV_122 | Value | 20.0 | 0.0 |
| 9 | RCS_T_Max | CV_731 | Value | 20.0 | 0.0 |
| 10 | RATE_RCS_T_Max | CV_731 | Value | 20.0 | 0.0 |
| 11 | Level_Core_Channel_Med | CV_114 | Value | 20.0 | 0.0 |
| 12 | Level_Core_Channel_Hot | CV_115 | Value | 20.0 | 0.0 |
| 13 | Level_Core_Channel_Side | CV_116 | Value | 20.0 | 0.0 |
| 14 | Level_Core_Channel_Min | CV_120 | Value | 20.0 | 0.0 |
| 15 | Loop_1_Thot | HV_201 | Liquid_Temperature | 20.0 | 0.0 |
| 16 | Loop_1_Tcold | HV_245 | Liquid_Temperature | 20.0 | 0.0 |
| 17 | Loop_1_Tav | CV_200 | Value | 20.0 | 0.0 |
| 18 | RATE_Loop_1_Tav | CV_204 | Value | 20.0 | 0.0 |
| 19 | Loop_2_Thot | HV_301 | Liquid_Temperature | 20.0 | 0.0 |
| 20 | Loop_2_Tcold | HV_345 | Liquid_Temperature | 20.0 | 0.0 |
| 21 | Loop_2_Tav | CV_300 | Value | 20.0 | 0.0 |
| 22 | RATE_Loop_2_Tav | CV_304 | Value | 20.0 | 0.0 |
| 23 | Loop_3_Thot | HV_401 | Liquid_Temperature | 20.0 | 0.0 |
| 24 | Loop_3_Tcold | HV_445 | Liquid_Temperature | 20.0 | 0.0 |
| 25 | Loop_3_Tav | CV_400 | Value | 20.0 | 0.0 |
| 26 | RATE_Loop_3_Tav | CV_404 | Value | 20.0 | 0.0 |
| 27 | SCM_Min | CV_725 | Value | 20.0 | 0.0 |
| 28 | Containment_Pressure | HV_950 | Pressure | 20.0 | 0.0 |
| 29 | PZR_Pressure | HV_540 | Pressure | 20.0 | 0.0 |
| 30 | RATE_PZR_Pressure | HV_540 | Pressure | 20.0 | 0.0 |
| 31 | PZR_Level_Meters | CV_512 | Value | 20.0 | 0.0 |
| 32 | PZR_Level | CV_511 | Value | 20.0 | 0.0 |
| 33 | RATE_PZR_Level | CV_511 | Value | 20.0 | 0.0 |
| 34 | PZR_Fluid_Mass | CV_501 | Value | 20.0 | 0.0 |
| 35 | PZR_Level_Setpoint | CV_833 | Value | 20.0 | 0.0 |
| 36 | PZR_PORV_VPI | CV_921 | Value | 20.0 | 0.0 |
| 37 | PZR_Spray_Mass_FLow | CV_561 | Value | 20.0 | 0.0 |
| 38 | PZR_Spray_FLow_VPI | CV_563 | Value | 20.0 | 0.0 |
| 39 | Total_ECCS_Loop_1_Flow | CV_278 | Value | 20.0 | 0.0 |
| 40 | Total_ECCS_Loop_2_Flow | CV_378 | Value | 20.0 | 0.0 |
| 41 | Total_ECCS_Loop_3_Flow | CV_478 | Value | 20.0 | 0.0 |
| 42 | Total_ECCS_Flow | CV_275 | Value | 20.0 | 0.0 |
| 43 | Total_ECCS_Loop_1_Fluid_Mass | CV_279 | Value | 20.0 | 0.0 |
| 44 | Total_ECCS_Loop_2_Fluid_Mass | CV_379 | Value | 20.0 | 0.0 |
| 45 | Total_ECCS_Loop_3_Fluid_Mass | CV_379 | Value | 20.0 | 0.0 |
| 46 | HPI_Loop_1_Flow | CV_267 | Value | 20.0 | 0.0 |
| 47 | HPI_Loop_2_Flow | CV_367 | Value | 20.0 | 0.0 |
| 48 | HPI_Loop_3_Flow | CV_467 | Value | 20.0 | 0.0 |
| 49 | LPI_Loop_1_Flow | CV_277 | Value | 20.0 | 0.0 |
| 50 | LPI_Loop_2_Flow | CV_377 | Value | 20.0 | 0.0 |
| 51 | LPI_Loop_3_Flow | CV_477 | Value | 20.0 | 0.0 |
| 52 | ACC_1_HL_Pressure | HV_295 | Pressure | 20.0 | 0.0 |
| 53 | ACC_1_CL_Pressure | HV_285 | Pressure | 20.0 | 0.0 |
| 54 | ACC_2_HL_Pressure | HV_395 | Pressure | 20.0 | 0.0 |
| 55 | ACC_2_CL_Pressure | HV_385 | Pressure | 20.0 | 0.0 |
| 56 | ACC_3_HL_Pressure | HV_495 | Pressure | 20.0 | 0.0 |
| 57 | ACC_3_CL_Pressure | HV_485 | Pressure | 20.0 | 0.0 |

Continue on page 2

| | | | | | |
|---|---|---|---|---|---|
| 57 | ACC_3_CL_Pressure | HV_485 | Pressure | 20.0 | 0.0 |
| 58 | ACC_1_HL_Level | CV_295 | Value | 20.0 | 0.0 |
| 59 | ACC_1_CL_Level | CV_285 | Value | 20.0 | 0.0 |
| 60 | ACC_2_HL_Level | CV_395 | Value | 20.0 | 0.0 |
| 61 | ACC_2_CL_Level | CV_385 | Value | 20.0 | 0.0 |
| 62 | ACC_3_HL_Level | CV_495 | Value | 20.0 | 0.0 |
| 63 | ACC_3_CL_Level | CV_485 | Value | 20.0 | 0.0 |
| 64 | Steam_Pressure | HV_900 | Pressure | 20.0 | 0.0 |
| 65 | RATE_Steam_Pressure | HV_900 | Pressure | 20.0 | 0.0 |
| 66 | SG_Level_Setpoint | CV_010 | Value | 20.0 | 0.0 |
| 67 | SG_1_Level | CV_605 | Value | 20.0 | 0.0 |
| 68 | SG_2_Level | CV_705 | Value | 20.0 | 0.0 |
| 69 | SG_3_Level | CV_805 | Value | 20.0 | 0.0 |
| 70 | RATE_SG_1_Level | CV_605 | Value | 20.0 | 0.0 |
| 71 | RATE_SG_2_Level | CV_705 | Value | 20.0 | 0.0 |
| 72 | RATE_SG_3_Level | CV_805 | Value | 20.0 | 0.0 |
| 73 | SG_1_Level_Deviation | CV_842 | Value | 20.0 | 0.0 |
| 74 | SG_2_Level_Deviation | CV_843 | Value | 20.0 | 0.0 |
| 75 | SG_3_Level_Deviation | CV_844 | Value | 20.0 | 0.0 |
| 76 | Air_Ejector_Rad_Monitor | CV_847 | Value | 20.0 | 0.0 |
| 77 | SG_1_Pressure | HV_650 | Pressure | 20.0 | 0.0 |
| 78 | SG_2_Pressure | HV_750 | Pressure | 20.0 | 0.0 |
| 79 | SG_3_Pressure | HV_850 | Pressure | 20.0 | 0.0 |
| 80 | RATE_SG_1_Pressure | HV_650 | Pressure | 20.0 | 0.0 |
| 81 | RATE_SG_2_Pressure | HV_750 | Pressure | 20.0 | 0.0 |
| 82 | RATE_SG_3_Pressure | HV_850 | Pressure | 20.0 | 0.0 |
| 83 | SG_1_Main_FW_Flow | CV_694 | Value | 20.0 | 0.0 |
| 84 | SG_1_FW_Flow | CV_620 | Value | 20.0 | 0.0 |
| 85 | SG_2_Main_FW_Flow | CV_794 | Value | 20.0 | 0.0 |
| 86 | SG_2_FW_Flow | CV_720 | Value | 20.0 | 0.0 |
| 87 | SG_3_Main_FW_Flow | CV_894 | Value | 20.0 | 0.0 |
| 88 | SG_3_FW_Flow | CV_820 | Value | 20.0 | 0.0 |
| 89 | SG_1_Steam_Flow | CV_665 | Value | 20.0 | 0.0 |
| 90 | SG_2_Steam_Flow | CV_765 | Value | 20.0 | 0.0 |
| 91 | SG_3_Steam_Flow | CV_865 | Value | 20.0 | 0.0 |
| 92 | SG_1_PORV_Flow | CV_666 | Value | 20.0 | 0.0 |
| 93 | SG_2_PORV_Flow | CV_766 | Value | 20.0 | 0.0 |
| 94 | SG_3_PORV_Flow | CV_866 | Value | 20.0 | 0.0 |
| 95 | SG_1_Safety_Valve_Flow | CV_667 | Value | 20.0 | 0.0 |
| 96 | SG_2_Safety_Valve_Flow | CV_767 | Value | 20.0 | 0.0 |
| 97 | SG_3_Safety_Valve_Flow | CV_867 | Value | 20.0 | 0.0 |
| 98 | SG_1_PORV_VPI | CV_977 | Value | 20.0 | 0.0 |
| 99 | SG_2_PORV_VPI | CV_987 | Value | 20.0 | 0.0 |
| 100 | SG_3_PORV_VPI | CV_997 | Value | 20.0 | 0.0 |
| 101 | SG_1_MSIV_VPI | CV_634 | Value | 20.0 | 0.0 |
| 102 | SG_2_MSIV_VPI | CV_644 | Value | 20.0 | 0.0 |
| 103 | SG_3_MSIV_VPI | CV_654 | Value | 20.0 | 0.0 |
| 104 | SG_1_FWRV_VPI | CV_695 | Value | 20.0 | 0.0 |
| 105 | SG_2_FWRV_VPI | CV_795 | Value | 20.0 | 0.0 |
| 106 | SG_3_FWRV_VPI | CV_895 | Value | 20.0 | 0.0 |
| 107 | SG_1_EFWV_VPI | CV_687 | Value | 20.0 | 0.0 |
| 108 | SG_2_EFWV_VPI | CV_787 | Value | 20.0 | 0.0 |
| 109 | SG_3_EFWV_VPI | CV_887 | Value | 20.0 | 0.0 |
| 110 | Steam_Dump_VPI | CV_937 | Value | 20.0 | 0.0 |
| 111 | Total_FW_Flow | CV_286 | Value | 20.0 | 0.0 |
| 112 | Turbine_Governor_VPI | CV_912 | Value | 20.0 | 0.0 |
| 113 | CL_Break_Mass_Flow | CV_960 | Mass_Flow_Rate | 20.0 | 0.0 |
| 114 | CL_HL_and_Safety_Mass_Flow | CV_962 | Mass_Flow_Rate | 20.0 | 0.0 |
| 115 | CL_HL_and_Safety_Integral_Mass | CV_963 | Value | 20.0 | 0.0 |
| 116 | CTP_ON_OFF | CV_550 | Value | 20.0 | 0.0 |
| 117 | PZR_Heaters | CV_562 | Value | 20.0 | 0.0 |
| 118 | CTP | CV_560 | Value | 20.0 | 0.0 |
| 119 | Makeup_Flow | CV_251 | Value | 20.0 | 0.0 |
| 120 | Tot_Loop_1_Mass_Flow | CV_250 | Value | 20.0 | 0.0 |
| 121 | Tot_Loop_2_Mass_Flow | CV_350 | Value | 20.0 | 0.0 |
| 122 | Tot_Loop_3_Mass_Fl | CV_450 | Value | 20.0 | 0.0 |

Continue on page 3

Continue on page 2

| | | | | | | |
|---|---|---|---|---|---|---|
| 122 | Hot_Loop_3_Mass_Flow | CV_450 | Value | 20.0 | 0.0 | |
| 123 | Upper_Plenum_Mass | CV_101 | Value | 20.0 | 0.0 | |
| 124 | Downcomer_1_Mass | CV_102 | Value | 20.0 | 0.0 | |
| 125 | Downcomer_2_Mass | CV_103 | Value | 20.0 | 0.0 | |
| 126 | Downcomer_3_Mass | CV_104 | Value | 20.0 | 0.0 | |
| 127 | Lower_Plenum_Mass | CV_105 | Value | 20.0 | 0.0 | |
| 128 | Medium_Channel_Mass | CV_106 | Value | 20.0 | 0.0 | |
| 129 | Hot_Channel_Mass | CV_107 | Value | 20.0 | 0.0 | |
| 130 | Side_Channel_Mass | CV_108 | Value | 20.0 | 0.0 | |
| 131 | Bypass_Channel_Mass | CV_109 | Value | 20.0 | 0.0 | |

DisplayComponentState

| ... | DisplayName | SystemName | ParameterName | CheckTime | StateWhenFail | ActivationOperator | ActivationTh... |
|---|---|---|---|---|---|---|---|
| 1 | Main_Steam_Isolation | LT_1514 | Trip_Time | 20.0 | ON | GREATER_THAN_ON | 1.0E-5 |
| 2 | Turbine_Trip | LT_1618 | Trip_Time | 20.0 | ON | GREATER_THAN_ON | 1.0E-5 |
| 3 | Reactor_Trip | LT_1616 | Trip_Time | 20.0 | ON | GREATER_THAN_ON | 1.0E-5 |
| 4 | Containment_Isolation | LT_1614 | Trip_Time | 20.0 | ON | GREATER_THAN_ON | 1.0E-5 |
| 5 | Safety_Injection | LT_1614 | Trip_Time | 20.0 | OFF | GREATER_THAN_ON | 1.0E-5 |
| 6 | SG_1_EFW_Pump_On | LT_1685 | Trip_Time | 20.0 | ON | GREATER_THAN_ON | 1.0E-5 |
| 7 | SG_2_EFW_Pump_On | LT_1686 | Trip_Time | 20.0 | ON | GREATER_THAN_ON | 1.0E-5 |
| 8 | SG_3_EFW_Pump_On | LT_1687 | Trip_Time | 20.0 | ON | GREATER_THAN_ON | 1.0E-5 |
| 9 | Low_SG_1_Level_Trip | VT_0301 | Trip_Time | 20.0 | ON | GREATER_THAN_ON | 1.0E-5 |
| 10 | Low_SG_2_Level_Trip | VT_0302 | Trip_Time | 20.0 | ON | GREATER_THAN_ON | 1.0E-5 |
| 11 | Low_SG_3_Level_Trip | VT_0303 | Trip_Time | 20.0 | ON | GREATER_THAN_ON | 1.0E-5 |
| 12 | Low_SG_Pressure_Isolation | LT_1511 | Trip_Time | 20.0 | ON | GREATER_THAN_ON | 1.0E-5 |
| 13 | High_Reactor_Power_Trip | VT_0304 | Trip_Time | 20.0 | ON | GREATER_THAN_ON | 1.0E-5 |
| 14 | Lo_PZR_Pressure_Trip | VT_0451 | Trip_Time | 20.0 | ON | GREATER_THAN_ON | 1.0E-5 |
| 15 | Hi_PZR_Pressure_Trip | VT_0459 | Trip_Time | 20.0 | ON | GREATER_THAN_ON | 1.0E-5 |
| 16 | Lo_PZR_Level_SI | VT_0455 | Trip_Time | 20.0 | ON | GREATER_THAN_ON | 1.0E-5 |
| 17 | Hi_Cont_Pressure_SI | VT_0456 | Trip_Time | 20.0 | ON | GREATER_THAN_ON | 1.0E-5 |
| 18 | Lo_PZR_Pressure_SI | VT_0453 | Trip_Time | 20.0 | ON | GREATER_THAN_ON | 1.0E-5 |
| 19 | HPI_Pump_1_On | LT_1760 | Trip_Time | 20.0 | OFF | GREATER_THAN_ON | 1.0E-5 |
| 20 | HPI_Pump_2_On | LT_1775 | Trip_Time | 20.0 | OFF | GREATER_THAN_ON | 1.0E-5 |
| 21 | HPI_Pump_3_On | LT_1782 | Trip_Time | 20.0 | OFF | GREATER_THAN_ON | 1.0E-5 |
| 22 | LPI_Pump_1_On | LT_1756 | Trip_Time | 20.0 | OFF | GREATER_THAN_ON | 1.0E-5 |
| 23 | LPI_Pump_2_On | LT_1778 | Trip_Time | 20.0 | OFF | GREATER_THAN_ON | 1.0E-5 |
| 24 | LPI_Pump_3_On | LT_1793 | Trip_Time | 20.0 | OFF | GREATER_THAN_ON | 1.0E-5 |
| 25 | FLAG_SGTR_SG_1 | VT_0951 | Trip_Time | 1.0 | ON | GREATER_THAN_ON | 1.0E-5 |
| 26 | FLAG_SGTR_SG_2 | VT_0952 | Trip_Time | 1.0 | ON | GREATER_THAN_ON | 1.0E-5 |
| 27 | FLAG_SGTR_SG_3 | VT_0953 | Trip_Time | 1.0 | ON | GREATER_THAN_ON | 1.0E-5 |

ControlValue

| ... | ControlName | IndicatorName | CheckTime | OnOrOpen... | OffOrCloseValue | NeutralStateValue | DisplayValue... |
|---|---|---|---|---|---|---|---|
| 1 | X_ACC_1_CL | IC_852 | 1.0 | 1.0 | 0.0 | -1.0 | 0.0 |
| 2 | X_ACC_1_HL | IC_853 | 1.0 | 1.0 | 0.0 | -1.0 | 0.0 |
| 3 | X_ACC_2_CL | IC_856 | 1.0 | 1.0 | 0.0 | -1.0 | 0.0 |
| 4 | X_ACC_2_HL | IC_857 | 1.0 | 1.0 | 0.0 | -1.0 | 0.0 |
| 5 | X_ACC_3_CL | IC_860 | 1.0 | 1.0 | 0.0 | -1.0 | 0.0 |
| 6 | X_ACC_3_HL | IC_861 | 1.0 | 1.0 | 0.0 | -1.0 | 0.0 |
| 7 | X_SG_1_FWRV | IC_843 | 1.0 | 1.0 | 0.0 | -1.0 | 0.0 |
| 8 | X_SG_2_FWRV | IC_845 | 1.0 | 1.0 | 0.0 | -1.0 | 0.0 |
| 9 | X_SG_3_FWRV | IC_847 | 1.0 | 1.0 | 0.0 | -1.0 | 0.0 |
| 10 | X_SG_1_MSIV | IC_842 | 1.0 | 1.0 | 0.0 | -1.0 | 0.0 |
| 11 | X_SG_2_MSIV | IC_844 | 1.0 | 1.0 | 0.0 | -1.0 | 0.0 |
| 12 | X_SG_3_MSIV | IC_845 | 1.0 | 1.0 | 0.0 | -1.0 | 0.0 |
| 13 | X_PZR_Spray_Valve | IC_823 | 1.0 | 1.0 | 0.0 | -1.0 | 0.0 |
| 14 | X_PZR_Spray_Valve1 | IC_823 | 1.0 | 1.0 | 0.0 | -1.0 | 0.0 |
| 15 | X_Watchdog_Timer | IC_950 | 1.0 | 9999. | 0.0 | -1. | 0.0 |
| 16 | X_Stm_Dump | IC_818 | 1.0 | 1.0 | 0.0 | -1.0 | 0.0 |
| 17 | X_Stm_Dump_Pressure_Setpoint | IC_819 | 1.0 | 6.9e6 | 0.0 | 6.9e6 | 6.9e6 |
| 18 | X_SG_1_PORV | IC_824 | 1.0 | 1.0 | 0.0 | -1.0 | 0.0 |
| 19 | X_SG_2_PORV | IC_826 | 1.0 | 1.0 | 0.0 | -1.0 | 0.0 |
| 20 | X_SG_3_PORV | IC_828 | 1.0 | 1.0 | 0.0 | -1.0 | 0.0 |
| 21 | X_SG_1_PORV_Setpoint | IC_825 | 1.0 | 7.07e6 | 0.0 | 7.07e6 | 7.07e6 |
| 22 | X_SG_2_PORV_Setpoint | IC_827 | 1.0 | 7.07e6 | 0.0 | 7.07e6 | 7.07e6 |
| 23 | X_SG_3_PORV_Setpoint | IC_829 | 1.0 | 7.07e6 | 0.0 | 7.07e6 | 7.07e6 |
| 24 | X_PZR_PORV | IC_835 | 1.0 | 0.33 | 0.0 | -1.0 | 0.0 |

Continue on page 4

Continue on page 3

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 25 | X_PZR_PORV_Setpoint | IC_836 | 1.0 | 16.5e6 | 0.0 | -1.0 | 0.0 |
| 26 | X_SG_1_EFW_Pump | IC_870 | 1.0 | 1.0 | 0.0 | -1.0 | 0.0 |
| 27 | X_SG_1_EFWV_Throttle | IC_871 | 1.0 | 1.0 | 0.0 | -1.0 | 0.0 |
| 28 | X_SG_2_EFW_Pump | IC_872 | 1.0 | 1.0 | 0.0 | -1.0 | 0.0 |
| 29 | X_SG_2_EFWV_Throttle | IC_873 | 1.0 | 1.0 | 0.0 | -1.0 | 0.0 |
| 30 | X_SG_3_EFW_Pump | IC_874 | 1.0 | 1.0 | 0.0 | -1.0 | 0.0 |
| 31 | X_SG_3_EFWV_Throttle | IC_875 | 1.0 | 1.0 | 0.0 | -1.0 | 0.0 |
| 32 | X_HPI_Loop_1_Throttle | IC_881 | 1.0 | 1.0 | 0.0 | -1.0 | 0.0 |
| 33 | X_HPI_Loop_2_Throttle | IC_883 | 1.0 | 1.0 | 0.0 | -1.0 | 0.0 |
| 34 | X_HPI_Loop_3_Throttle | IC_885 | 1.0 | 1.0 | 0.0 | -1.0 | 0.0 |
| 35 | X_HPI_Loop_1_Pump | IC_880 | 1.0 | 1.0 | 0.0 | -1.0 | 0.0 |
| 36 | X_HPI_Loop_2_Pump | IC_882 | 1.0 | 1.0 | 0.0 | -1.0 | 0.0 |
| 37 | X_HPI_Loop_3_Pump | IC_884 | 1.0 | 1.0 | 0.0 | -1.0 | 0.0 |
| 38 | X_LPI_Loop_1_Throttle | IC_891 | 1.0 | 1.0 | 0.0 | -1.0 | 0.0 |
| 39 | X_LPI_Loop_2_Throttle | IC_893 | 1.0 | 1.0 | 0.0 | -1.0 | 0.0 |
| 40 | X_LPI_Loop_3_Throttle | IC_895 | 1.0 | 1.0 | 0.0 | -1.0 | 0.0 |
| 41 | X_LPI_Loop_1_Pump | IC_890 | 1.0 | 1.0 | 0.0 | -1.0 | 0.0 |
| 42 | X_LPI_Loop_2_Pump | IC_892 | 1.0 | 1.0 | 0.0 | -1.0 | 0.0 |
| 43 | X_LPI_Loop_3_Pump | IC_894 | 1.0 | 1.0 | 0.0 | -1.0 | 0.0 |
| 44 | X_Charging | IC_899 | 1.0 | 1.0 | 0.0 | -1.0 | 0.0 |

ControlState

| ... | ControlName | IndicatorName | CheckTime | OnOrOpen... | OffOrCloseValue | NeutralStateValue | DisplayState... |
|---|---|---|---|---|---|---|---|
| 1 | X_RCP_1 | IC_831 | 1.0 | 1.0 | -1.0 | -1.0 | ON |
| 2 | X_RCP_2 | IC_832 | 1.0 | 1.0 | -1.0 | -1.0 | ON |
| 3 | X_RCP_3 | IC_833 | 1.0 | 1.0 | -1.0 | -1.0 | ON |
| 4 | X_Control_Rods_In | IC_814 | 1.0 | 1.0 | -1.0 | -1.0 | ON |
| 5 | X_Control_Rods_Out | IC_815 | 1.0 | 1.0 | -1.0 | -1.0 | ON |
| 6 | X_Turb_Trip | IC_840 | 1.0 | 1.0 | 0.0 | -1.0 | ON |
| 7 | X_Increase_Turbine_Load | IC_816 | 1.0 | 1.0 | -1.0 | -1.0 | ON |
| 8 | X_Decrease_Turbine_Load | IC_817 | 1.0 | 1.0 | -1.0 | -1.0 | ON |
| 9 | X_SCRAM | IC_820 | 1.0 | 1.0 | 0.0 | -1.0 | OFF |
| 10 | X_PZR_Safety_Valve_1 | IC_821 | 1.0 | 1.0 | 0.0 | -1.0 | OFF |
| 11 | X_PZR_Safety_Valve_2 | IC_822 | 1.0 | 1.0 | 0.0 | -1.0 | OFF |
| 12 | X_LOCA_Cold_Leg | IC_811 | 1.0 | 1.0 | -1.0 | -1.0 | ON |
| 13 | X_LOCA_Hot_Leg | IC_812 | 1.0 | 1.0 | -1.0 | -1.0 | ON |
| 14 | X_SGTR_1 | IC_898 | 1.0 | 1.0 | -1.0 | -1.0 | ON |
| 15 | X_Steam_Line_Break | IC_813 | 1.0 | 1.0 | -1.0 | -1.0 | ON |
| 16 | X_SIAS | IC_830 | 1.0 | 1.0 | -1.0 | -1.0 | ON |
| 17 | X_Letdown | IC_896 | 1.0 | 1.0 | 0.0 | -1.0 | ON |
| 18 | X_Makeup | IC_897 | 1.0 | 1.0 | 0.0 | -1.0 | ON |
| 19 | X_MSIV_Isolation_Block | IC_848 | 1.0 | 1.0 | 0.0 | -1.0 | ON |
| 20 | X_FLAG_SGTR_1 | IC_951 | 1.0 | 1.0 | -1.0 | -1.0 | ON |
| 21 | X_FLAG_SGTR_2 | IC_952 | 1.0 | 1.0 | -1.0 | -1.0 | ON |
| 22 | X_FLAG_SGTR_3 | IC_953 | 1.0 | 1.0 | -1.0 | -1.0 | ON |

AlarmParameter

| ... | AlarmName | IndicatorName | AlarmImportance | CheckTime | ActivationOperator | ActivationThreshold |
|---|---|---|---|---|---|---|
| 1 | A_HPI_Loop_1_Flow | HPI_Loop_1_Flow | 0.5 | 20.0 | GT | 0.01 |
| 2 | A_HPI_Loop_2_Flow | HPI_Loop_2_Flow | 0.5 | 20.0 | GT | 0.01 |
| 3 | A_HPI_Loop_3_Flow | HPI_Loop_3_Flow | 0.5 | 20.0 | GT | 0.01 |
| 4 | A_PZR_Lo_Level | PZR_Level | 0.5 | 20.0 | LT | 10.0 |
| 5 | A_PZR_Hi_Level | PZR_Level | 0.5 | 20.0 | GT | 80.0 |
| 6 | A_PZR_Level_Lo_Dev | PZR_Level | 0.5 | 20.0 | LT | 45.0 |
| 7 | A_PZR_Level_Hi_Dev | PZR_Level | 0.5 | 20.0 | GT | 60.0 |
| 8 | A_PZR_Spray_FLow | PZR_Spray_FLow_VPI | 0.5 | 20.0 | GT | 0.01 |
| 9 | A_SG_1_Lo_Level | SG_1_Level | 0.5 | 20.0 | LT | 25.0 |
| 10 | A_SG_2_Lo_Level | SG_2_Level | 0.5 | 20.0 | LT | 25.0 |
| 11 | A_SG_3_Lo_Level | SG_3_Level | 0.5 | 20.0 | LT | 25.0 |
| 12 | A_SG_1_Hi_Level | SG_1_Level | 0.5 | 20.0 | GT | 90.0 |
| 13 | A_SG_2_Hi_Level | SG_2_Level | 0.5 | 20.0 | GT | 90.0 |
| 14 | A_SG_3_HI_Level | SG_3_Level | 0.5 | 20.0 | GT | 90.0 |
| 15 | A_SG_1_Lo_Pressure | SG_1_Pressure | 0.5 | 20.0 | LT | 5500000.0 |
| 16 | A_SG_2_Lo_Pressure | SG_2_Pressure | 0.5 | 20.0 | LT | 5500000.0 |
| 17 | A_SG_3_Lo_Pressure | SG_3_Pressure | 0.5 | 20.0 | LT | 5500000.0 |
| 18 | A_SG_1_Hi_Pressure | SG_1_Pressure | 0.5 | 20.0 | GT | 6700000.0 |
| 19 | A_SG_2_Hi_Pressure | SG_2_Pressure | 0.5 | 20.0 | GT | 6700000.0 |

Continue on page 5

| | | | | | | |
|---|---|---|---|---|---|---|
| | 20 | A_SG_3_Hi_Pressure | SG_3_Pressure | 0.5 | 20.0 | GT | 6700000.0 |
| | 21 | A_ENDSEQ_PZR_Primary_Pressure_LOW | PZR_Pressure | 0.5 | 20.0 | LT | 1500000.0 |
| | 22 | A_PZR_Pressure_Lo_Dev | PZR_Pressure | 0.5 | 20.0 | LT | 15000000.0 |
| | 23 | A_PZR_Pressure_Hi_Dev | PZR_Pressure | 0.5 | 20.0 | GT | 15754000.0 |
| | 24 | A_PZR_Lo_Pressure | PZR_Pressure | 0.5 | 20.0 | LT | 14479000.0 |
| | 25 | A_PZR_Hi_Pressure | PZR_Pressure | 0.5 | 20.0 | GT | 15858000.0 |
| | 26 | A_ACC_1_CL_Lo_Pressure | ACC_1_CL_Pressure | 0.5 | 20.0 | LT | 2413000.0 |
| | 27 | A_ACC_1_CL_Hi_Pressure | ACC_1_CL_Pressure | 0.5 | 20.0 | GT | 2758000.0 |
| | 28 | A_ACC_1_HL_Lo_Pressure | ACC_1_HL_Pressure | 0.5 | 20.0 | LT | 2413000.0 |
| | 29 | A_ACC_1_HL_Hi_Pressure | ACC_1_HL_Pressure | 0.5 | 20.0 | GT | 2758000.0 |
| | 30 | A_ACC_2_CL_Lo_Pressure | ACC_2_CL_Pressure | 0.5 | 20.0 | LT | 2413000.0 |
| | 31 | A_ACC_2_CL_Hi_Pressure | ACC_2_CL_Pressure | 0.5 | 20.0 | GT | 2758000.0 |
| | 32 | A_ACC_2_HL_Lo_Pressure | ACC_2_HL_Pressure | 0.5 | 20.0 | LT | 2413000.0 |
| | 33 | A_ACC_2_HL_Hi_Pressure | ACC_2_HL_Pressure | 0.5 | 20.0 | GT | 2758000.0 |
| | 34 | A_ACC_3_CL_Lo_Pressure | ACC_3_CL_Pressure | 0.5 | 20.0 | LT | 2413000.0 |
| | 35 | A_ACC_3_CL_Hi_Pressure | ACC_3_CL_Pressure | 0.5 | 20.0 | GT | 2758000.0 |
| | 36 | A_ACC_3_HL_Lo_Pressure | ACC_3_HL_Pressure | 0.5 | 20.0 | LT | 2413000.0 |
| | 37 | A_ACC_3_HL_Hi_Pressure | ACC_3_HL_Pressure | 0.5 | 20.0 | GT | 2758000.0 |
| | 38 | A_ACC_1_CL_Lo_Level | ACC_1_CL_Level | 0.5 | 20.0 | LT | 70.0 |
| | 39 | A_ACC_1_CL_LoLo_Level | ACC_1_CL_Level | 0.5 | 20.0 | LT | 10.0 |
| | 40 | A_ACC_1_HL_Lo_Level | ACC_1_HL_Level | 0.5 | 20.0 | LT | 70.0 |
| | 41 | A_ACC_1_HL_LoLo_Level | ACC_1_HL_Level | 0.5 | 20.0 | LT | 10.0 |
| | 42 | A_ACC_2_CL_Lo_Level | ACC_2_CL_Level | 0.5 | 20.0 | LT | 70.0 |
| | 43 | A_ACC_2_CL_LoLo_Level | ACC_2_CL_Level | 0.5 | 20.0 | LT | 10.0 |
| | 44 | A_ACC_2_HL_Lo_Level | ACC_2_HL_Level | 0.5 | 20.0 | LT | 70.0 |
| | 45 | A_ACC_2_HL_LoLo_Level | ACC_2_HL_Level | 0.5 | 20.0 | LT | 10.0 |
| | 46 | A_ACC_3_CL_Lo_Level | ACC_3_CL_Level | 0.5 | 20.0 | LT | 70.0 |
| | 47 | A_ACC_3_CL_LoLo_Level | ACC_3_CL_Level | 0.5 | 20.0 | LT | 10.0 |
| | 48 | A_ACC_3_HL_Lo_Level | ACC_3_HL_Level | 0.5 | 20.0 | LT | 70.0 |
| | 49 | A_ACC_3_HL_LoLo_Level | ACC_3_HL_Level | 0.5 | 20.0 | LT | 10.0 |
| | 50 | A_Air_Ejector_Rad_Monitor | Air_Ejector_Rad_Monitor | 0.5 | 20.0 | GT | 25000.0 |
| | 51 | A_SCM_Low | SCM_Min | 0.5 | 20.0 | LT | 10.0 |
| | 52 | A_SCM_High | SCM_Min | 0.5 | 20.0 | GT | 30.0 |
| | 53 | A_SG_1_MFW_Off | SG_1_Main_FW_Flow | 0.5 | 20.0 | LT | 0.1 |
| | 54 | A_SG_2_MFW_Off | SG_2_Main_FW_Flow | 0.5 | 20.0 | LT | 0.1 |
| | 55 | A_SG_3_MFW_Off | SG_3_Main_FW_Flow | 0.5 | 20.0 | LT | 0.1 |
| | 56 | A_SG_1_PORV_VPI_Open | SG_1_PORV_VPI | 0.5 | 20.0 | GT | 0.01 |
| | 57 | A_SG_2_PORV_VPI_Open | SG_2_PORV_VPI | 0.5 | 20.0 | GT | 0.01 |
| | 58 | A_SG_3_PORV_VPI_Open | SG_3_PORV_VPI | 0.5 | 20.0 | GT | 0.01 |

| AlarmComponent | ... | AlarmName | IndicatorName | AlarmImportance | CheckTime | ActivationState |
|---|---|---|---|---|---|---|
| | 1 | A_Main_Steam_Isolation | Main_Steam_Isolation | 0.5 | 1.0 | ON |
| | 2 | A_Turbine_Trip | Turbine_Trip | 0.5 | 1.0 | ON |
| | 3 | A_Reactor_Trip | Reactor_Trip | 0.5 | 1.0 | ON |
| | 4 | A_Containment_Isolation | Containment_Isolation | 0.5 | 1.0 | ON |
| | 5 | A_Safety_Injection | Safety_Injection | 0.5 | 1.0 | ON |
| | 6 | A_SG_1_EFW_Pump_On | SG_1_EFW_Pump_On | 0.5 | 1.0 | ON |
| | 7 | A_SG_2_EFW_Pump_On | SG_2_EFW_Pump_O | 0.5 | 1.0 | ON |

Continue on page 6

Continue on page 5

| | | | | | | |
|---|---|---|---|---|---|---|
| 7 | A_SG_2_EFW_Pump_On | SG_2_EFW_Pump_On | 0.5 | 1.0 | ON | |
| 8 | A_SG_3_EFW_Pump_On | SG_3_EFW_Pump_On | 0.5 | 1.0 | ON | |
| 9 | A_Low_SG_1_Level_Trip | Low_SG_1_Level_Trip | 0.5 | 1.0 | ON | |
| 10 | A_Low_SG_2_Level_Trip | Low_SG_2_Level_Trip | 0.5 | 1.0 | ON | |
| 11 | A_Low_SG_3_Level_Trip | Low_SG_3_Level_Trip | 0.5 | 1.0 | ON | |
| 12 | A_High_Reactor_Power_Trip | High_Reactor_Power_Trip | 0.5 | 1.0 | ON | |
| 13 | A_Lo_PZR_Pressure_Trip | Lo_PZR_Pressure_Trip | 0.5 | 1.0 | ON | |
| 14 | A_Hi_PZR_Pressure_Trip | Hi_PZR_Pressure_Trip | 0.5 | 1.0 | ON | |
| 15 | A_Lo_PZR_Level_SI | Lo_PZR_Level_SI | 0.5 | 1.0 | ON | |
| 16 | A_Hi_Cont_Pressure_SI | Hi_Cont_Pressure_SI | 0.5 | 1.0 | ON | |
| 17 | A_Lo_PZR_Pressure_SI | Lo_PZR_Pressure_SI | 0.5 | 1.0 | ON | |

AlarmTwoParameterDifference

| ... | AlarmName | IndicatorName | AlarmImportance | CheckTime | SecondIndicator... | ActivationThreshold |
|---|---|---|---|---|---|---|
| 1 | A_SG_1_Level_Lo_Dev | SG_Level_Setpoint | 0.5 | 20.0 | SG_1_Level | 10.0 |
| 2 | A_SG_2_Level_Lo_Dev | SG_Level_Setpoint | 0.5 | 20.0 | SG_2_Level | 10.0 |
| 3 | A_SG_3_Level_Lo_Dev | SG_Level_Setpoint | 0.5 | 20.0 | SG_3_Level | 10.0 |
| 4 | A_SG_1_Level_Hi_Dev | SG_1_Level | 0.5 | 20.0 | SG_Level_Setpoint | 10.0 |
| 5 | A_SG_2_Level_Hi_Dev | SG_2_Level | 0.5 | 20.0 | SG_Level_Setpoint | 10.0 |
| 6 | A_SG_3_Level_Hi_Dev | SG_3_Level | 0.5 | 20.0 | SG_Level_Setpoint | 10.0 |

## Appendix E

# Test case study - SGTR event

The Steam Generator (SG) is an important component of a NPP not only because it transfers heat from the Reactor Coolant System (RCS) to the secondary steam system, but also because it is a barrier against the release of radioactive material to the secondary side, which in turn presents potential leakage paths outside the containment. In a SGTR accident this barrier is broken due to the rupture of one or more SG tubes.

In this study we consider a SGTR event in loop A of a two-loop Pressurized Water Reactor (PWR). The SGTR event is an accident Initiating Event (IE) which induces a number of abnormal conditions (e.g., low RCS pressure, high radiation in the secondary steam line, etc.), which automatically command: *1*) the actuation of the High Pressure Injection (HPI) system (after about 80 seconds) to inject cool water to cooldown the RCS and provide RCS inventory make-up; and *2*) trip of the reactor and of the Main Feed Water (MFW) system (after about 115 seconds). Upon the reactor trip, the turbine trips as well, the core power rapidly decreases, and the TBVs open to control the secondary side pressure.

The response of the control room operators is guided by the Emergency Operating Procedures (EOPs) and conditioned by their training. Upon the IE, the operators enter into EOP *immediate and subsequent manual actions*. The first steps entail checking the behavior of the key plant parameters and the status of the key plant safety systems.

Then, the operators must go through a number of decision points that would direct them to initiator-specific EOPs: the *loss of subcooling margin* EOP, the *excessive heat transfer* EOP, the *steam generator tube leak* EOP. In particular, the entry criteria for the steam generator tube leak EOP are: high radiation levels in the secondary side, incontrollable level increase in one SG, and mismatch in the FWs to the SGs.

Once the operators have entered the *steam generator tube leak* procedures, their main goals are to:

- maintain the pressurizer (pressurizer) level,
- maintain the subcooling margin,
- depressurize and cooldown the RCS (so as to minimize the leak from the RCS to the secondary side),
- isolate the ruptured SG,
- control and maintain key plant parameters.

The crew model implemented in the ADS includes three types of actions, in an effort to reproduce the operators behavior as realistically as possible: actions guided by the EOPs, actions guided by the so-called mental procedures, and cognitive actions.

The actions of the first type are directly taken from the EOPs and are intended to model the crew's following the procedures. Actions belonging to *immediate and subsequent manual actions* and *steam generator tube leak* EOPs have been implemented in this work (Table E.1). The second type of actions is carried out following the so-called mental procedures. These are plant operating procedures memorized by the operator and are based on formal procedures. Mental procedures are task-oriented, i.e., each mental procedure corresponds to a specific task. Table E.2 lists the modeled actions of this type.

Rule-based actions comprise a third type [Carvalho, 2006a]. These are intended to model the fact that, although during an accident (as well as during normal operations)

the typical control room operators' response is mainly guided by procedures, in many situations it has been observed that operators do not follow the procedure by rote. In other words, they do not apply these "mechanically" or without judgment. Even when guided by procedures, situation assessment and response planning based on the knowledge and training of the operators continue to be important for successful operator performance [Roth et al., 1994]. In this work, rule-based actions model this assessment or planning. These rules are instructions acquired by the operator through training, e.g., provided by supervisors. These are listed in Table E.3.

**Table E.1:** Crew actions directed by the Emergency Operating Procedures (EOPs) modeled in the SGTR scenario.

| **EOP** | **Modeled actions** |
|---|---|
| IMMEDIATE AND SUBSEQUENT MANUAL ACTIONS | - Manually trip the reactor<br>- Verify reactor shut down<br>- If emergency system is not required, maintain pressurizer level above 100 inches<br>- If any subcooling margin = 0 °F, go to LOSS OF SUBCOOLING procedures<br>- If the heat transfer is or has been excessive, go to EXCESSIVE HEAT TRANSFER procedures<br>- If any of the radiation alarms start, go to STEAM GENERATOR TUBE LEAK procedures |
| STEAM GENERATOR TUBE LEAK | - Identify the SG with the leak<br>- Maintain the pressurizer level > 80 inches<br>- Adjust the turbine bypass valves to maintain the steam pressure below 950 psig<br>- Depressurize the reactor coolant system to minimize the core subcooling margin<br>- Depressurize and cool down the RCS<br>-When the RCS is below 532 °F and if more than one RCP loop is operating then secure RCPs for one RCP/loop operation<br>- Check any subcooling margins<br>- If pressurizer level is above 375 inches reduce RCP pressure below 2000 psig and open the pressurizer relief block<br>- Isolate the SG with the larger tube leak<br>- Control the secondary side contamination |

**Table E.2:** Crew actions directed by the mental procedures.

| **Mental procedure** | **Action** |
|---|---|
| Pressurizer level < 100 inches | Maintain pressurizer level to 110 inches by manual control |
| Subcooling margin (SCM) less than 5 °F | Maintain SCM to 50 °F by manual control |

**Table E.3:** Rule-base cognitive actions.

| **Perceived information** | **Action** |
|---|---|
| Rate of power > 1 (or < -1) | Trip the reactor |
| Rate of the loop 1 (or 2) hot leg temperature is < -1 (or 1) | Trip the reactor |
| Pressurizer level > 320 inches and the rate of pressurizer level > 1 | Trip the reactor |
| Pressurizer level < 200 inches and the rate of pressurizer level < 1 | Trip the reactor |
| RCS pressure > 2350 psig and the RCS rate > 0.25 | Trip the reactor |
| RCS pressure < 2000 psig and the RCS rate < -0.25 | Trip the reactor |
| All the RCPs are not working | Trip the reactor |
| The SG operating range levels > 70 and alarm flow imbalance on | Trip the reactor |
| The SG operating range levels < 40, alarm flow imbalance on and MFWs has been tripped | Trip the reactor |
| Alarm flow imbalance on | Trip the reactor |
| The SG operating range levels > 80 | Trip the reactor |
| The SG operating range levels < 30 | Trip the reactor |
| The SG pressure < 900 psig | Trip the reactor |
| Pressurizer level < 200 inches | Turn on HPI |
| SCM less than 5 °F | Trip all RCPs |

# Appendix F

# DDET-generated scenario probabilities

In the following Figure F.1, F.2, and F.3, the resulting probabilities for each type of crew, i.e., fast, intermediate, and slow (which correspond to three sub-DDETs) are shown.

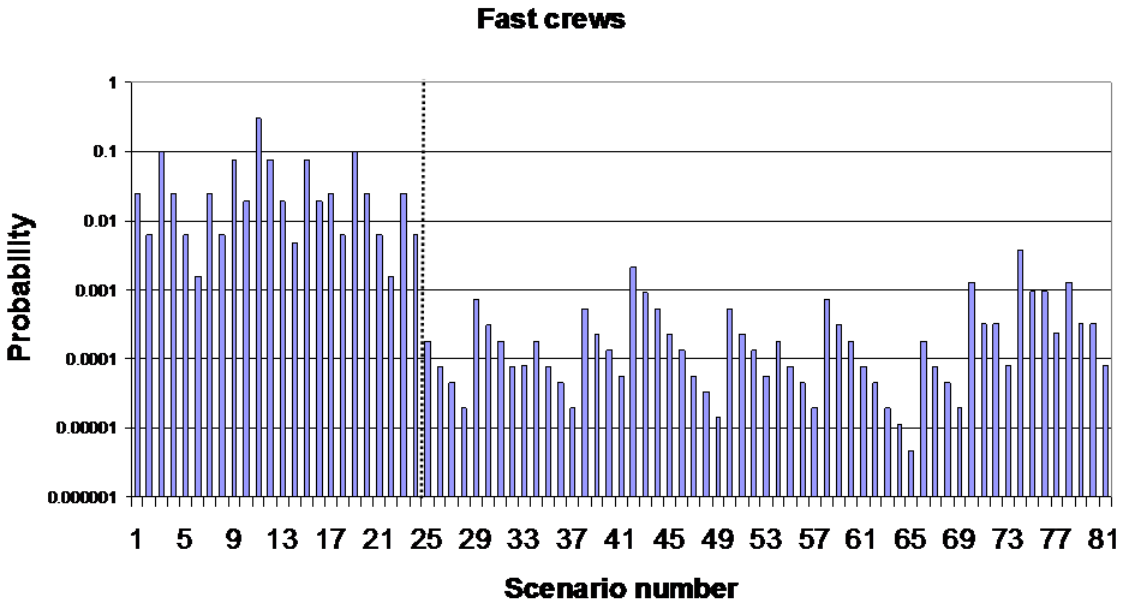



**Fig. F.1:** Scenario probabilities for fast type of crews.

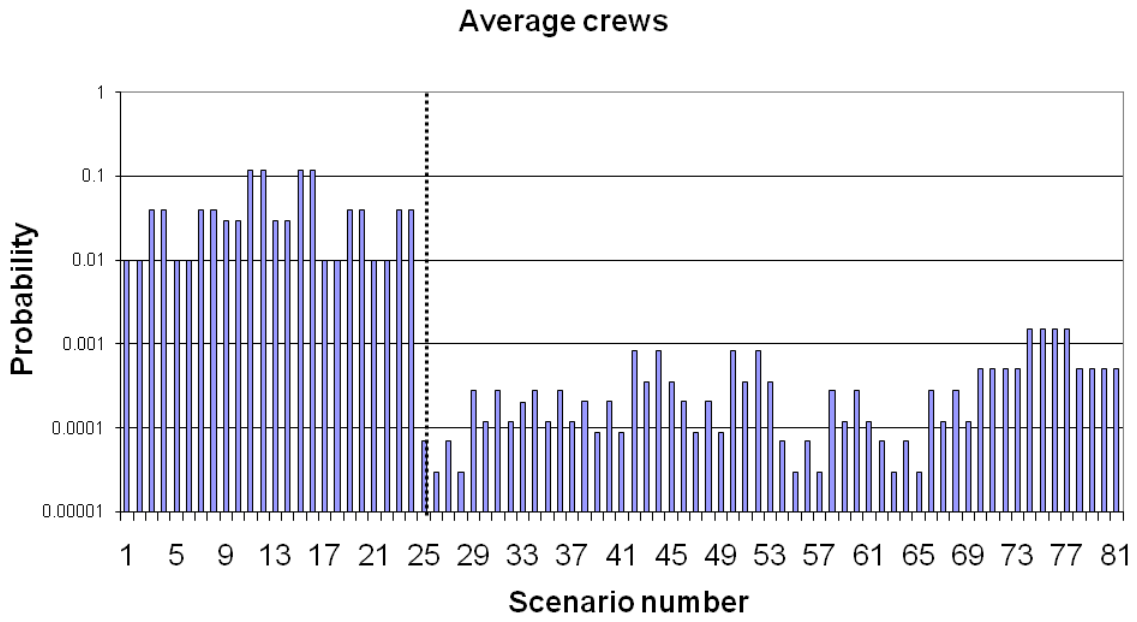



**Fig. F.2:** Scenario probabilities for intermediate type of crews.

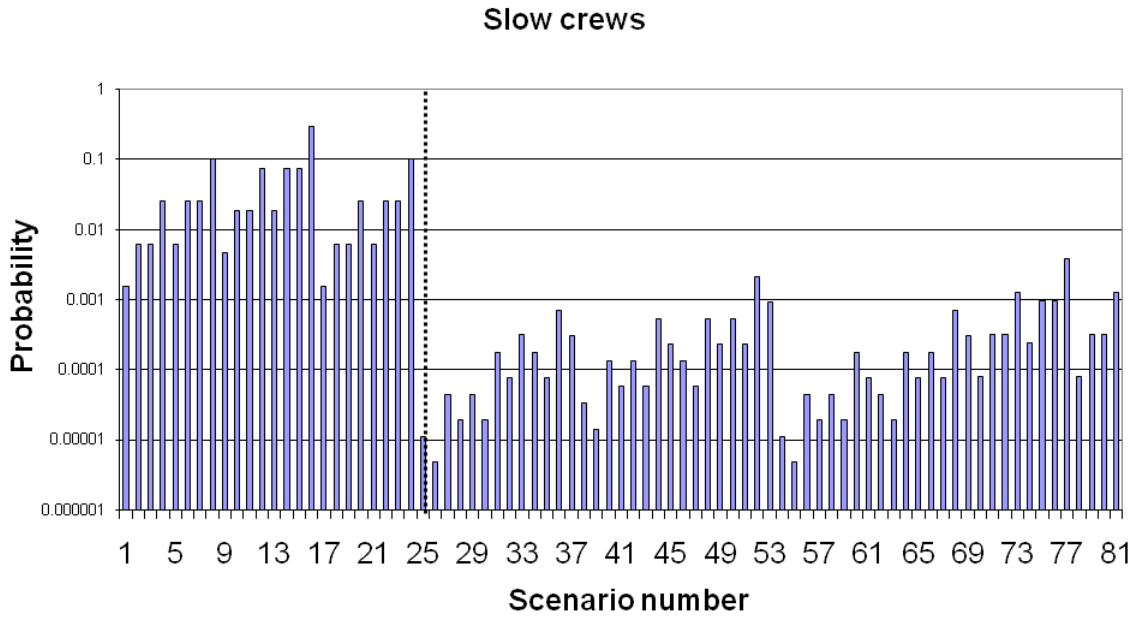



**Fig. F.3:** Scenario probabilities for slow type of crews.

As one can see, in all the type of crews, the probability of the first 24 scenarios of each of the types of crews are larger compared to the others. This is due to the fact that the scenario after the $24^{th}$ are related to the failure of either HPI, steam dump valve, or

both. Since their probability of failure is low, the scenario probability results low.

In general, looking at the results of the first 24 scenarios related to the intermediate type of crews, the associated scenario probabilities are more flat than the fast and slow types. This is an expected result because the intermediate crew behavior in the single task (almost symmetric distribution) affects the final distribution of the scenario probabilities making them symmetric. Whereas in the first 24 scenarios of fast and slow type of crews the distribution is not symmetric because the original timing distributions are skewed towards fast or slow crew behaviors.

In Figure F.1 for the fast type of crews, there are mainly three scenarios whose probabilities are clearly higher than the others (scenarios 3, 11, and 19). Those scenario probabilities are related to the crews that perform the timing variability steps with a fast tendency and the probability of the associated scenario is high. In addition, since the probability of not performing as fast is different than zero (in case of fast crew tendency is equal to 0.2), the scenario probability associated with non-fast crew type is different than zero (e.g., scenario 7).

The same pattern applies to the slow type of crews (Figure F.3). In that case, scenario 16 is the one where the crews perform as slow in the timing tasks. Since slow type of crews are considered in this case, the probability of performing as slow crew in the single task is higher than non-slow crew and therefore the associated scenario probability is high.

The first twelve high probability scenarios for each type of crew are analyzed, in order to identify the main events of those scenarios. Only the first twelve scenarios have been included in this analysis since they dominate the DDET-generated scenario probabilities, i.e., the following scenario probabilities decrease roughly by a couple of order of magnitudes. Table F.1, F.2, and F.3 show for each type of crew the first twelve high probability scenarios (notice that in all these sequences the HPI and steam dump valve did not fail).

With regard to the fast crews (Table F.1), number 11 is the highest probability scenario

with a rather high probability of 0.3. That scenario is characterized by a stop of the pressurizer spray at 5 m, an early transfer to the SLOCA procedure, and early stop of last HPI.

In the second position there are scenarios similar to the number 11 but with the stop of spray at 3 and 8 m (scenarios 3 and 19) with 0.1 of probability each. Then, in the next positions there are scenarios with the stop of the spray at 5 m and the stop of 2 HPIs, with early transfer for both the two timing variability transfers and then combination of early and late with the stop of 1 HPI. The same pattern applies for the stop of 3 and 8 m.

Looking at the results of fast crew behavior, one can say that the main events leading to high probability scenarios are the early transfer in case of both the two timing variability events in addition to the stop of HPI at 5 m as said in the procedure.

It is interesting to note that the variation of the probability between the first scenario and the twelfth scenario is about one order of magnitude. Therefore scenario 11 dominates the other scenarios in the DDET.

**Table F.1:** First twelve high probability scenarios for fast crews. (T1 = Timing variability in transfer to the SLOCA procedure. T2 = Timing variability in stopping the last HPI)

| **Sc. Num** | **Prob.** | **Description** |
|---|---|---|
| 11 | 0.301 | Stop spray at 5 m, stop 1 HPI, early T1, early T2 |
| 3 | 0.100 | Stop spray at 3 m, stop 1 HPI, early T1, and early T2 |
| 19 | 0.100 | Stop spray at 8 m, stop 1 HPI, early T1, and early T2 |
| 9 | 0.075 | Stop spray at 5 m, stop 2 HPIs, early T1, and early T2 |
| 12 | 0.075 | Stop spray at 5 m, stop 1 HPI, early T1, and late T2 |
| 15 | 0.075 | Stop spray at 5 m, stop 1 HPI, late T1, and early T2 |
| 1 | 0.025 | Stop spray at 3 m, stop 2 HPIs, early T1, and early T2 |
| 4 | 0.025 | Stop spray at 3 m, stop 1 HPI, early T1, and late T2 |
| 7 | 0.025 | Stop spray at 3 m, stop 1 HPI, late T1, and early T2 |
| 17 | 0.025 | Stop spray at 8 m, stop 2 HPIs, early T1, and early T2 |
| 20 | 0.025 | Stop spray at 8 m, stop 1 HPI, early T1, and late T2 |
| 23 | 0.025 | Stop spray at 8 m, stop 1 HPI, late T1, and early T2 |

In case of intermediate crews (Table F.2), the first twelve scenarios are divided in two parts in terms of probability, the first four scenarios with probability of 0.118 and the next eight scenarios with probability of 0.0392. This means that the resulting probability distribution of the DDET-generated scenarios is more symmetric than the case of fast crews since the original probability distribution functions of the branching points are symmetric. For example for the two timing variability branching points the probability is 0.5 for early behavior and 0.5 for late behavior, i.e., the probability of being early or late is the same.

In case of intermediate crews, what affects the end probability is only the stopping of the spray. In fact, in case of stop of spraying at 5m, the associated branching probability is higher that the other and therefore the scenarios probability results higher (first four scenarios). Whereas, with regard to the stop at 3 and 8 meters, since their associated probability is the same the resulting scenario probability results equal (last eight scenarios).

**Table F.2:** First twelve high probability scenarios for intermediate crews. (T1 = Timing variability in transfer to the SLOCA procedure. T2 = Timing variability in stopping the last HPI)

| **Sc. Num** | **Prob.** | **Description** |
|---|---|---|
| 11 | 0.118 | Stop spray at 5 m, stop 1 HPI, early T1, early T2 |
| 12 | 0.118 | Stop spray at 5 m, stop 1 HPI, early T1, and late T2 |
| 15 | 0.118 | Stop spray at 5 m, stop 1 HPI, late T1, and early T2 |
| 16 | 0.118 | Stop spray at 5 m, stop 1 HPI, late T1, and late T2 |
| 3 | 0.0392 | Stop spray at 3 m, stop 1 HPI, early T1, and early T2 |
| 4 | 0.0392 | Stop spray at 3 m, stop 1 HPI, early T1, and late T2 |
| 7 | 0.0392 | Stop spray at 3 m, stop 1 HPI, late T1, and early T2 |
| 8 | 0.0392 | Stop spray at 3 m, stop 1 HPI, late T1, and late T2 |
| 19 | 0.0392 | Stop spray at 8 m, stop 1 HPI, early T1, and early T2 |
| 20 | 0.0392 | Stop spray at 8 m, stop 1 HPI, early T1, and late T2 |
| 23 | 0.0392 | Stop spray at 8 m, stop 1 HPI, late T1, and early T2 |
| 24 | 0.0392 | Stop spray at 8 m, stop 1 HPI, late T1, and late T2 |

In case of slow crews (Table F.3), the same patter as the fast crews can be applied. The

only difference is that the dominating event is the late transfer to the SLOCA procedure and late stop of last HPI.

It is interesting to note that the scenario 11 which was the first one for the fast crews and in the first group in the intermediate crews, it is not in the first twelve of slow crews. This is due to the fact that in the scenario 11 the main events that contribute to the probability are the early transfer for the two timing variability transfers which have low probability in case of slow crews. In this case, the the main events leading to high probability scenarios are the early transfer in case of both the two timing variability events in addition to the stop of HPI at 5m as said in the procedure.

**Table F.3:** First twelve high probability scenarios for slow crews. (T1 = Timing variability in transfer to the SLOCA procedure. T2 = Timing variability in stopping the last HPI)

| **Sc. Num** | **Prob.** | **Description** |
|---|---|---|
| 16 | 0.301 | Stop spray at 5 m, stop 1 HPI, late T1, and late T2 |
| 8 | 0.100 | Stop spray at 3 m, stop 1 HPI, late T1, and late T2 |
| 24 | 0.100 | Stop spray at 8 m, stop 1 HPI, late T1, and late T2 |
| 12 | 0.075 | Stop spray at 5 m, stop 1 HPI, early T1, and late T2 |
| 14 | 0.075 | Stop spray at 5 m, stop 2 HPI, late T1, and late T2 |
| 15 | 0.075 | Stop spray at 5 m, stop 1 HPI, late T1, and early T2 |
| 4 | 0.025 | Stop spray at 3 m, stop 1 HPI, early T1, and late T2 |
| 6 | 0.025 | Stop spray at 3 m, stop 2 HPI, late T1, and late T2 |
| 7 | 0.025 | Stop spray at 3 m, stop 1 HPI, late T1, and early T2 |
| 20 | 0.025 | Stop spray at 8 m, stop 1 HPI, early T1, and late T2 |
| 22 | 0.025 | Stop spray at 8 m, stop 2 HPI, late T1, and late T2 |
| 23 | 0.025 | Stop spray at 8 m, stop 1 HPI, late T1, and early T2 |

It is also interesting to note that with regard to the single type of crews (fast, intermediate, and slow), the difference of the probabilities between a group and another is lower. This is due to the recalculation of the probabilities multiplying the type of crew to the relative fraction. This means that actually there is not a dominant scenario (or group of scenarios) on the others but the most probable scenarios are less dominant on the others giving more variability on the differentiation of scenarios due to probabilities.

# Appendix G

# Performance shaping factors estimation to support HRA

## G.1 Overview of the SPAR-H method

The Standardized Plant Analysis Risk Human Reliability Analysis (SPAR-H) is an HRA method for estimating the human error probabilities (HEPs) associated with operator and crew actions and decisions in response to initiating events in NPPs. In the SPAR-H method, the HEP is calculated considering the probability of failure in the diagnosis and in the execution. The HEP of the action is therefore the sum of the HEP for the diagnosis and the HEP for the execution.

The SPAR-H method is built on an explicit information-processing model of human performance derived from the behavioral sciences literature that was then interpreted in light of activities at NPPs [Blackman and Byers, 1994]. In 1999, further research identified eight PSFs capable of influencing human performance. These PSFs are accounted for in the SPAR-H quantification process. These factors include:

- Available time
- Stress and stressors

- Experience and training
- Complexity
- Ergonomics (including the human-machine interface)
- Procedures
- Fitness for duty
- Work processes.

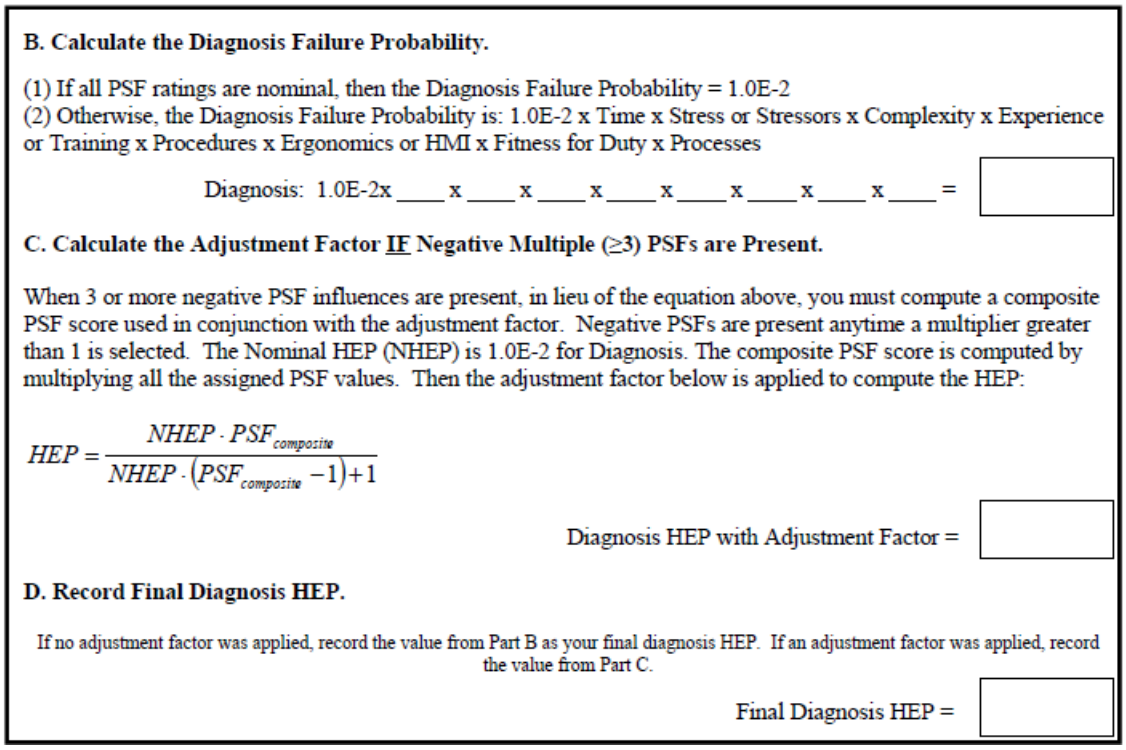
For each of this PSFs the HRA analyst has to assign a specific multiplier where a low multiplier has a positive effect on the operator action whereas a high multiplier has a negative effect.

Figure G.1 and Figure G.2 show an excerpt of the PSFs to be assigned for the calculation of the diagnosis HEP with the SPAR-H method [NUREG/CR-6883, 2005] and the final calculation of the HEP. In particular, for both the diagnosis and execution part of the HEP a table with PSFs and multiplier must be filled out by the analyst and the final HEP for both the execution and the diagnosis is a function of the multiplier of the PSFs [NUREG/CR-6883, 2005].

**A. Evaluate PSFs for the Diagnosis Portion of the Task, If Any.**

| PSFs | PSF Levels | Multiplier for Diagnosis | Please note specific reasons for PSF level selection in this column. |
|---|---|---|---|
| Available Time | Inadequate time | P(failure) = 1.0 ☐ | |
| | Barely adequate time (≈2/3 x nominal) | 10 ☐ | |
| | Nominal time | 1 ☐ | |
| | Extra time (between 1 and 2 x nominal and > than 30 min) | 0.1 ☐ | |
| | Expansive time (> 2 x nominal and > 30 min) | 0.01 ☐ | |
| | Insufficient information | 1 ☐ | |
| Stress/ Stressors | Extreme | 5 ☐ | |
| | High | 2 ☐ | |
| | Nominal | 1 ☐ | |
| | Insufficient Information | 1 ☐ | |
| Complexity | Highly complex | 5 ☐ | |
| | Moderately complex | 2 ☐ | |
| | Nominal | 1 ☐ | |
| | Obvious diagnosis | 0.1 ☐ | |
| | Insufficient Information | 1 ☐ | |
| Experience/ Training | Low | 10 ☐ | |
| | Nominal | 1 ☐ | |
| | High | 0.5 ☐ | |
| | Insufficient Information | 1 ☐ | |
| Procedures | Not available | 50 ☐ | |
| | Incomplete | 20 ☐ | |
| | Available, but poor | 5 ☐ | |
| | Nominal | 1 ☐ | |
| | Diagnostic/symptom oriented | 0.5 ☐ | |
| | Insufficient Information | 1 ☐ | |
| Ergonomics/ HMI | Missing/Misleading | 50 ☐ | |
| | Poor | 10 ☐ | |
| | Nominal | 1 ☐ | |
| | Good | 0.5 ☐ | |
| | Insufficient Information | 1 ☐ | |
| Fitness for Duty | Unfit | P(failure) = 1.0 ☐ | |
| | Degraded Fitness | 5 ☐ | |
| | Nominal | 1 ☐ | |
| | Insufficient Information | 1 ☐ | |
| Work Processes | Poor | 2 ☐ | |
| | Nominal | 1 ☐ | |
| | Good | 0.8 ☐ | |
| | Insufficient Information | 1 ☐ | |

**Fig. G.1:** Example of table for the calculation of the HEP for diagnosis based on PSFs.



**B. Calculate the Diagnosis Failure Probability.**

(1) If all PSF ratings are nominal, then the Diagnosis Failure Probability = 1.0E-2
(2) Otherwise, the Diagnosis Failure Probability is: 1.0E-2 x Time x Stress or Stressors x Complexity x Experience or Training x Procedures x Ergonomics or HMI x Fitness for Duty x Processes

Diagnosis: 1.0E-2x ____ x ____ x ____ x ____ x ____ x ____ x ____ x ____ =

**C. Calculate the Adjustment Factor IF Negative Multiple (≥3) PSFs are Present.**

When 3 or more negative PSF influences are present, in lieu of the equation above, you must compute a composite PSF score used in conjunction with the adjustment factor. Negative PSFs are present anytime a multiplier greater than 1 is selected. The Nominal HEP (NHEP) is 1.0E-2 for Diagnosis. The composite PSF score is computed by multiplying all the assigned PSF values. Then the adjustment factor below is applied to compute the HEP:

$$HEP = \frac{NHEP \cdot PSF_{composite}}{NHEP \cdot (PSF_{composite} - 1) + 1}$$

Diagnosis HEP with Adjustment Factor =

**D. Record Final Diagnosis HEP.**

If no adjustment factor was applied, record the value from Part B as your final diagnosis HEP. If an adjustment factor was applied, record the value from Part C.

Final Diagnosis HEP =

**Fig. G.2:** Example of table for the final calculation of the HEP for diagnosis.

## G.2 Calculation of the HEPs with the SPAR-H method

The following two tables summarize the PSF multipliers used for the calculation of the HEP for the case study 1, i.e., SLOCA with the HPI systems available (Table G.1), and for the case study 2, i.e., SLOCA without any HPI system available (Table G.2).

**Table G.1:** Evaluation of PSFs for diagnosis and execution with classical SPAR-H and SPAR-H with dynamic insights. Case study 1 - SLOCA with HPI systems available.

| | **Classical SPAR-H** | | **SPAR-H with dynamic insights** | |
|---|---|---|---|---|
| PSF | Diagnosis | Execution | Diagnosis | Execution |
| Available time | 10 | 10 | 10 | 10 |
| Stress | 1.0 | 1.0 | 1.0 | 1.0 |
| Complexity | 1.0 | 2 | 1.0 | 5 |
| Training | 0.5 | 0.5 | 0.5 | 1.0 |
| Procedures | 1.0 | 1.0 | 1.0 | 1.0 |
| Ergonomics | 0.5 | 1.0 | 0.5 | 1.0 |
| Fitness for duty | 1.0 | 1.0 | 1.0 | 1.0 |
| Work processes | 1.0 | 1.0 | 1.0 | 1.0 |
| Total | $2.5 \cdot 10^{-2}$ | $1.0 \cdot 10^{-2}$ | $2.5 \cdot 10^{-2}$ | $5.0 \cdot 10^{-2}$ |

The final HEP calculated with the classical SPAR-H is given by:

$$HEP = HEP_{diagnosis} + HEP_{execution} = 2.5 \cdot 10^{-2} + 1.0 \cdot 10^{-2} = 3.5 \cdot 10^{-2} \tag{G.1}$$

The final HEP calculated with SPAR-H with dynamic insights is given by:

$$HEP = HEP_{diagnosis} + HEP_{execution} = 2.5 \cdot 10^{-2} + 5.0 \cdot 10^{-2} = 7.5 \cdot 10^{-2} \tag{G.2}$$

**Table G.2:** Evaluation of PSFs for diagnosis and execution with classical SPAR-H and SPAR-H with dynamic insights. Case study 2 - SLOCA without any HPI system available.

| | **Classical SPAR-H** | | **SPAR-H with dynamic insights** | |
|---|---|---|---|---|
| PSF | Diagnosis | Execution | Diagnosis | Execution |
| Available time | 10 | 10 | 1 | 1 |
| Stress | 1 | 2 | 1 | 2 |
| Complexity | 1 | 1 | 2 | 5 |
| Training | 0.5 | 1 | 0.5 | 1 |
| Procedures | 5 | 5 | 5 | 5 |
| Ergonomics | 1 | 1 | 1 | 1 |
| Fitness for duty | 1 | 1 | 1 | 1 |
| Work processes | 1 | 1 | 1 | 1 |
| Total | 0.25 | 0.09 | 0.05 | 0.0476 |

The final HEP calculated with the classical SPAR-H is given by:

$$HEP = HEP_{diagnosis} + HEP_{execution} = 0.25 + 0.09 = 0.34 \tag{G.3}$$

The final HEP calculated with SPAR-H with dynamic insights is given by:

$$HEP = HEP_{diagnosis} + HEP_{execution} = 0.05 + 0.0476 = \ 0.10 \tag{G.4}$$

# References


Technical basis and implementation guidelines for a technique for human event analysis (atheana). *NUREG-1624, Rev. 1*, 2000.

C. Acosta. *Dynamic Event Tree for Accident Sequence Analysis.* PhD thesis, Massachusetts Institute of Technology, June 1991.

C. Acosta and N. Siu. Dynamic event trees in accident sequence analysis: application to steam generator tube rupture. *Reliability Engineering and System Safety*, 41:135–154, 1993.

A. Amendola and G. Reina. Event sequence and consequence spectrum: a methodology for probabilistic transient analysis. *Nucl. Sci. Engng.*, 77:297–315, 1981.

D. Bader and R. Pennington. Cluster computing: Applications. *Georgia Tech College of Computing. Retrieved 2007-07-13*, 1996.

S. Baron, C. Feehrer, R. Muralidharan, R. Pew, and P. Horwitz. An approach to modeling supervisory control in a nuclear power plant. *NUREG/CR-2988, ORNL/SUB/81-70523/1*, 1982.

H. S. Blackman and J. C. Byers. Asp/spar-h methodology. *Internal EGG report for the USNRC*, 1994.

P.C. Cacciabue. Understanding and modelling man-machine interaction. *Nuclear Engineering and Design*, 165(3):351–358, 1996.

V.R. Paulo De Carvalho. Ergonomic field studies in a nuclear power plant control room. *Progress in nuclear energy*, 48:51–69, 2006a.

V.R. Paulo De Carvalho, L. Isaac dos Santos, and C. R. Mario Vidal. Nuclear power plant shift supervisor's decision making during microincidents. *International Journal of Industrial Ergonomic*, 35:619–644, 2005.

V.R. Paulo De Carvalho, L. Isaac dos Santos, and C. R. Mario Vidal. Safety implications of cultural and cognitive issues in nuclear power plant operation. *Applied Ergonomics*, 37:211–223, 2006b.

B. Ruttand U. Catalyurek, A. Hakobyan, K. Metzroth, T. Aldemir, R. Denning, S. Dunagan, and D. Kunsman. Distributed dynamic event tree generation for reliability and risk assessment. *CLADE 2006 Workshop Paris, France*, 2006.

Y. H. J. Chang and A. Mosleh. Cognitive modeling and dynamic probabilistic simulation of operating crew response to complex system accidents. part 1: Overview of the idac model. *Reliability Engineering and System Safety*, 2006a.

Y. H. J. Chang and A. Mosleh. Cognitive modeling and dynamic probabilistic simulation of operating crew response to complex system accidents. part 2: Idac performance influencing factors model. *Reliability Engineering and System Safety*, 2006b.

Y. H. J. Chang and A. Mosleh. Cognitive modeling and dynamic probabilistic simulation of operating crew response to complex system accidents. part 3: Idac operator response model. *Reliability Engineering and System Safety*, 2006c.

Y. H. J. Chang and A. Mosleh. Cognitive modeling and dynamic probabilistic simulation of operating crew response to complex system accidents. part 4: Idac causal model of operator problem-solving response. *Reliability Engineering and System Safety*, 2006d.

Y. H. J. Chang and A. Mosleh. Cognitive modeling and dynamic probabilistic simulation of operating crew response to complex system accidents. part 5: Idac dynamic

probabilistic simulation of the idac model. *Reliability Engineering and System Safety*, 2006e.

Y.H. Chang and A. Mosleh. Cognitive modeling and dynamic probabilistic simulation of operating crew response to complex system accident (ads-idacrew). 1999. Center for Technology Risk Studies, University of Maryland, College Park, MD, USA.

S. H. Chien, A. A. Dykes, J. W. Stetkar, and D.C. Bley. Quantification of human error rates using a slim-based approach. *IEEE Fourth Conference on Human Factors and Power Plants*, 1988.

G. Cojazzi. The dylam approach for the dynamic reliability analysis of the systems. *Reliability Engineering and System Safety*, 52:279–296, 1996.

K. Coyne. *A predictive model of nuclear power plant crew decision-making and performance in a dynamic simulation environment.* PhD thesis, University of Maryland, College Park, 2009.

K. Coyne and A. Mosleh. Implementation of a dynamic pra approach for the prediction of operator errors during abnormal nuclear power plant events. *Proc. Ninth International Conference on Probabilistic Safety Assessment and Management (PSAM-9)*, May 2008.

V. N. Dang. Frameworks for dynamic risk assessment and their implications for operator modeling. pages 43–75, 2000. in: C. Smidts, J. Devooght, P.E. Labeau (Eds.), "Dynamic Reliability - Future Directions", International Workshop Series on Advanced Topics in Reliability and Risk Analysis, Greenbelt, MD, USA, 19-20 Sept. 1998, Center for Reliability Engineering, University of Maryland, College Park, MD, USA.

V. N. Dang. *Modeling cognition for accident sequence analysis: development of a dynamic operator-plant simulation.* PhD thesis, Massachusetts Institute of Technology, May 1996.

V. N. Dang, Y. Huang, N. Siu, and J. S. Carrol. Analyzing cognitive errors using a dynamic crew-simulation model. *proceeding of the 1992 IEEE fifth conference on human factors and power plants*, 1992.

H Demmou, S Khalfaoui, E Guilhem, and R Valette. Critical scenarios derivation methodology for mechatronic systems. *Reliability Engineering and System Safety*, 84:33–44, 2004.

D Dubois and H Prade. *Possibility Theory: An approach to Computerized Processing of Uncertainty*. Plenum Press, New York, 1988.

D. E. Embrey, P. Humphreys, E. A. Rosa, B. Kirwan, and K. Rea. Slim-maud: An approach to assessing human error probabilities using structured expert judgment. *NUREG/CR-3518*, I and II, 1984.

G. Parry et al. An approach to the analysis of operator actions in pra. *EPRI TR-100259, Electric Power Research Institute*, 1992.

J. Forester, A. Kolaczkowski, E. Lois, and D. Kelly. Evaluation of human reliability analysis methods against good practices. *NUREG-1842*, 2006.

C. J. Garrett and G. E. Apostolakis. Automated hazard analysis of digital control systems. *Reliability Engineering and System Safety*, 77(1):1–17, 2002.

D. I. Gertman and H.S. Blackman. Development of a stochastic simulation method (microcrews) for nuclear power plant operations. *Proc. International topical mtg on Probabilistic Safety Assessment (PSA 93)*, 1993.

D. I. Gertman, L. N. Haney, and N. Siu. Representing context, cognition, and crew performance in a shutdown risk assessment. *Reliability Engineering and System Safety*, 52(3):261–278, 1996.

D.I. Gertman, H.S. Blackman, J. Byers, L. Haney, C. Smith, and J. Marble. The spar-h method. *NUREG/CR-6883*, 2005.

S. Glasstone and A. Sesonske. *Nuclear Reactor Engineering*. Chapman and Hall, Inc., 1994.

A. Hakobyana, T. Aldemir, R. Denning, S. Dunagan, D. Kunsman B. Rutt, and U. Catalyurek. Dynamic generation of accident progression event trees. *Nuclear Engineering and Design*, 238(12):3457–3467, 2008.

G. W. Hannaman, V. Joksimovich, D. H. Worledge, and A. J. Spurgin. The role of human reliability analysis for enhancing crew performance. *Proc. International ANS/ENS Topical Meeting on Advances in Human Factors in Nuclear Power Systems*, 1986.

E. Hofer, M. Kloos, B. Krzykacz-Hausmann, J. Peschke, and M. Sonnenkalb. Dynamic event trees for probabilistic safety analysis. *EUROSAFE-Berlin-2002*, 2:14, 2002. Gesellschaft fur Anlagen - und Reaktorwsicherheit, Cologne, Germany.

E. Hollnagel. Cognition as control: a pragmatic approach to the modeling of joint cognitive systems. *IEEE Transactions on Systems, Man and Cybernetics*, 2003.

E. Hollnagel. Reliability analysis and operator modeling. *Reliability Engineering and System Safety*, 52:327–337, 1996.

K. S. Hsueh and A. Mosleh. Dynamic accident sequence simulator for probabilistic safety assessment. *PSA International Topical Meeting*, 26 - 29 Jan 1993.

J. Itoh, S. Yoshimura, T. Ohtsuka, and F. Masuda. Cognitive task analysis of nuclear power plant operators for man-machine interface design. *American Nucle*, pages 96–102, 1990.

J. M Izquierdo-Rocha and M. Sanchez-Perea. Application of the intgrated safety assessemnt mothodology to the emergency procedures of a sgtr of a pwr. *Reliability Engineering and System Safety*, 45:159–173, 1994.

J. Julius, J. Grobbelaar, D. Spiegel, and F. Rahn. The epri hra calculator userŠs manual, version 3.0, product id 1008238. *Electric Power Research Institute*, 2005.

J Keller, M Gray, and J Givens. A fuzzy k-nearest neighbor algorithm. *IEEE Trans. Syst.,Man,Cybern*, 15(4):580–585, 1985.

G Klir and T Folger. *Fuzzy Sets, Uncertainty and Information.* Englewood Cliffs, Prentice Hall, New Jersey, 1988.

M. Kloos and J. Peschke. Mcdet: A probabilistic dynamics method combining monte carlo simulation with the discrete dynamic event tree approach. *Nuclear Science and Engineering*, 153:137–156, 2006.

R Krishnapuram and J M Keller. A possibilistic approach to clustering. *IEEE Trans. On Fuzzy systems*, 1(2):98–110, 1993.

PE Labeau, C. Smidts, and S. Swaminathan. Dynamic reliability: towards an integrated platform for probabilistic risk assessment. *Reliability Engineering and System Safety*, 68:219–254, 2000.

E. Lois, V. N. Dang, J. Forester, H. Broberg, S. Massaiu, M. Hildebrandt, P.Ø. Braarud, G. Parry, J. Julius, R. Boring, I. Männistö, and A. Bye. International hra empirical study - description of overall approach and first pilot results from comparing hra methods to simulator data. *HWR-844. OECD Halden Reactor Project, Norway*, 2008.

M. Marseguerra and E. Zio. Monte carlo approach to psa for dynamic process systems. *Reliability Engineering and System Safety*, 52:227–241, 1996.

T. Matsuoka. Reliability analysis of a self-holding type relay system by a dynamical event tree and the go-flow methodology. *Proceedings of the 8th International Conference on Probabilistic Safety Assessment and Management May 14-18*, 2006. New Orleans, Louisiana, USA.

D. Mercurio, L. Podofillini, E. Zio, and V.N. Dang. Identification and classification of dynamic event tree scenarios via possibilistic clustering: Application to a steam generator tube rupture event. *Accident Analysis and Prevention*, 7 Sep 2008. Available on line.

K. Metzroth, R. Denning, C. Sidts, and T. Aldemir. Incorporation of a human reliability model into the adapt pra methodology. *PSAM 9*, 18-23 May 2008.

D. Mosey. Reactor accidents: Nuclear safely and role of institutional failure. *Nuclear Engineering International Special Publication*, 1990.

R. Munoz, E. Minguez, E. Melendez, J. M. Izquierdo, and M. Sanchez-Perea. Dendros: A second generation scheduler for dynamic event trees. *Mathematics and Computation, Reactor Physics and Environmental Analysis in Nuclear Applications, Conference Proceedings*, 1999.

I. Munteanu and T. Aldemir. A methodology for probabilistic accident management. *Nuclear Plant Operations and Control*, 2003.

NUREG/CR-6883. The spar-h human reliability method. *NUREG/CR-6883(INL/EXT-05-00509)*, 2005.

et al. P. C. Cacciabue. Cosimo: a cognitive simulation model of human decision making and behavior in accident management of complex plants. *IEE Trans. Sys. Man, and Cybernetics*, 22:1058–1074, 1992.

J. Peschke and M. Kloos. Consideration of human actions in combination with the probabilistic dynamics code mcdet. *Journal of Risk and Reliability*, Sep 2008a.

J. Peschke and M. Kloos. Impact of epistemic uncertainties on the probabilistic assessment of the emergency operating procedure secondary side bleed and feed. *PSAM9*, 2008b.

L. Podofillini, D. Mercurio, V. N. Dang, and E. Zio. Dynamic safety assessment: Scenario identification via a fuzzy clustering approach. *Reliability Engineering and System Safety*, 95:534–549, 2010.

C. Queral, A. Exposito, J. A. Quiroga, A. Ibarra, and J. Hortal. Simulation of accident sequences including emergency operating procedures. *Proceedings of ICAPP 04*, June 2004.

J. Rasmussen. *Models of Mental Strategies in Process Plant Diagnosis.* J. Rasmussen and W. Rouse, Editors, Human Detection and Diagnosis of System Failures, p. 241, Plenum, New York, 1981.

J. Rasmussen. Skills, rules, knowledge: signals, signs and symbols and other distinctions in human performance models. *IEEE Transactions: Systems, Man and Cybernetics*, 13:257–267, 1983.

RELAP5/MOD3.3. Relap5/mod3.3 code manual. 2001. Prepared for the Division of Systems Research Office of Nuclear Regulatory Research U.S. Nuclear Regulatory Commission Washington, DC 20555. Information Systems Laboratories, Inc., Rockville, Maryland Idaho Falls, Idaho.

E. M. Roth, R. J. Mumaw, and P. M. Lewis. An empirical investigation of operator performance in cognitively demanding simulated emergencies. *NUREG/CR-6208*, 1994.

S. Sancaktar and D. R. Sharp. Living pra concept for plant risk, reliability, and availability tracking. *Proceedings of International Conference on Nuclear Power Plant Aging, Availability Factor and Reliability Analysis*, 1985.

J. C. Schryver. Operator model-based design and evaluation of advanced systems: computational model. *Proc. of the 1988 IEEE fourth conference on human factors and power plants*, pages 121–127, 1982.

K. S. Sheng and A. Mosleh. The development and application of the accident dynamic simulator for dynamic probabilistic risk assessment of nuclear power plats. *Reliability Engineering and System Safety*, 52(3):297–314, 1996.

Y. Shu, K. Furuta, and S. Kondo. Team performance modeling for hra in dynamic situations. *Reliability Engineering and System Safety*, 78(1):111–121, 2002.

A. I. Siegel and J. J. Wolf. *Man-machine system simulation model; psychosocial and performance interaction.* Wiley-interscience, New York, 1969.

N. Siu. Risk assessment for dynamic systems: An overview. *Reliability Engineering and System Safety*, 43(1):43–73, 1994.

M. Stamatelatos, G. Apostolakis, H. Dezfuli, C. Everline, S. Guarro, P. Moieni, A. Mosleh, T. Paulos, and R. Youngblood. Probabilistic risk assessment procedure guide for nasa managers and practitioners. *Prepared for Office of Safety and Mission Assurance NASA Headquarters Washington*, August 2002. www.hq.nasa.gov/office/codeq/doctree/praguide.pdf.

A. D. Swain. Accident sequence evaluation program human reliability analysis procedure. *NUREG/CR-4772/SAND86-1996*, 1996.

A. D. Swain and H. E. Guttmann. Handbook of human reliability analysis with emphasis on nuclear power plant applications. *NUREG/CR-1278/SAND80-0200*, 1983.

N. E. Todreas and M. S. Kazimi. *Nuclear Systems: Vol. I, Thermal Hydraulic Fundamentals*. Hemisphere, NY 1990, 3rd printing, Taylor and Francis, 2001.

N. E. Todreas and M. S. Kazimi. *Nuclear Systems: Vol. II, Elements of Thermal Hydraulic Design*. Hemisphere, NY 1990, 1990.

USNRC. Reactor safety study (wash-1400). *NUREG-75/014*, 1975.

USNRC. Reactor concepts manual - pressurized water reactor systems. 2003. www.nrc.gov/reading-rm/basic-ref/teachers/04.pdf.

W. E. Vesely. Incorporating aging effects into probabilistic risk analysis using a taylor expansion approach. *Reliability Engineering and System Safety*, 32(3):315–337, Sep 1991.

V. Volovoi. Modeling of system reliability petri nets with aging tokens. *Reliability Engineering and System Safety*, 84(2):149–161, 2004.

D. Wakefield, G. Parry, and and A. Spurgin G. Hannaman. Sharp1: A revised systematic human action reliability procedure. *EPRI TR-101711, Tier 2, Electric Power Research Institute*, 1992.

D. D. Woods. Some results on operator performance in emergency events. *Institute of Chemical Engineers Symposium Series*, 90:21–23, 1984.

D. D. Woods, H. Pople, and E. M. Roth. Cognitive environment simulation: an artificial intelligence system for human performance assessment. *NUREG/CR-4862*, 1987.

M Yang. A survey of fuzzy clustering. *Mathl. Comput. Modelling*, 18(11):1–16, 1993.

M. Yau, S. Guarro, and G. E. Apostolakis. Demonstration of the dynamic flowgraph methodology using the titan ii space launch vehicle digital flight control system. *Reliability Engineering and System Safety*, 49(3):335–353, 1995.

K. Yoshida, M. Yokobayashi, F. Tanabe, and K. Kawase. Development of ai-based simulation system for man-machine system behavior in accidental situations in nuclear power plant. *journal of nuclear science and technology*, 33(2):110–118, 1996.

S. Yoshimura and H. Takayanagi. Study on modeling of operator's learning mechanis. *Man, and Cybernetics. IEEE SMC '99 Conference Proceedings.*, 3:721–726, 1999.

B Yuan and G Klir. *Data driven identification of key variables*. In: Ruan, D. (Ed.), Intelligent Hybrid Systems Fuzzy Logic, Neural Network, and Genetic Algorithms. Kluver Academic Publishers, Ch. 7, 1997.

B Yuan, G Klir, and J Swan-Stone. Evolutionary fuzzy c-means clustering algorithm. *Proc. Fourth IEEE International Conference on Fuzzy Systems*, pages 2221–2226, 1995.

D. Zhu, Y. H. Chang, and A. Mosleh. The use of distributed computing for dynamic pra: The ads approach. *Proceedings of PSAM 9. CD-ROM Version, IAPSAM*, 2008.

E Zio and P Baraldi. Identification of nuclear transients via optimized fuzzy clustering. *Annals of Nuclear Energy*, 32:1068–1080, 2005a.

E Zio and P Baraldi. Evolutionary fuzzy clustering for the classification of transients in nuclear components. *Progress in Nuclear Energy*, 46, 2005b.

E Zio, P Baraldi, and D Mercurio. Fuzzy clustering classification of nuclear transients with a possibilistic filter for unknown conditions. *Enlarged Halden Programme Group Meeting, Radisson SAS Lillehammer Hotel, Norway 16-21*, 2005.