UNIVERSITÀ DI PISA
Scuola di Dottorato in Ingegneria "Leonardo da Vinci"

Corso di Dottorato di Ricerca in
SICUREZZA NUCLEARE E INDUSTRIALE
Tesi di Dottorato di Ricerca
XXII Ciclo

Approaching Dynamic PSA within CANDU 6 NPP

Autore:
MARIAN MARIUS LONTOS

Relatori:
Prof. Ing. Marino Mazzini
Prof. Ing. Marco Carcassi
Dr. Ing. Davide Mazzini

SSD ING-IND/19

Anno 2012

OUTLINE OF DISSERTATION

The outline of this dissertation is going to present the applications that are the subject of the work and also the lay down of work content.

Chapter 1 reviews the conventional PSA main concepts, summarizes a short introduction history of Dynamic PSA (DPSA) and presents a non-exhaustive DPSA state-of-the-art with the recent and future developments.

Chapter 2 presents the first application of the thesis, which is actually an introduction in the context of the Integrated Dynamic Decision Analysis (IDDA) code, that represents the main tool used in the attempt of approaching the Dynamic PSA.

Starting from a description that reflects the level of knowledge about the system, IDDA code is able to develop all the scenarios of events compatible with the description received, from both points of view: either logical construction, or probabilistic coherence. By describing the system configuration and operation in a logically consistent manner, all the information is worked out by the code and is made available to the analyst as results in terms of system unavailability, minimal cut sets, uncertainty associated. The code allows also the association of different consequences that could be of interest for the analyst. The consequences could be of any type, such as economical, equipment outage time, etc.; for instance it can be considered an outage time for certain components of the system and then is calculated the “expected risk”. The association of consequences provides the inputs for a good decision making process.

Chapter 3 represents the core applications of the present work. The applications purpose is the coupling between the logic probabilistics of the system or plant and associated phenomenology of primary heat transport system of a generic CANDU 6 NPP.

First application is the coupling between the logic-probabilistic model of EWS system and associated phenomenology of primary heat transport system of CANDU 6 NPP. The considered plant transient is the total Loss of Main Feed-water with or without the coincident failure of the Emergency Water Supply System.

The second application is considering the CANDU 6 Station Blackout as plant transient-consequential condition, moreover the loss of all AC power sources existing on the site. The transient scenarios development consider the possibility to recover the offsite grid and the use of mobile diesel generators in order to mitigate the accident consequences. The purpose is to challenge the plant design and response and to check if the plant conditions of a severe accident are reached. The plant response is challenged for short and long periods of time.

The IDDA code allows interfacing the logic-probabilistic model of the system with the plant response in time, therefore with the evolution in time of the plant process variables. This allows raising sequences of possible events related in cause-consequence reasoning, each one giving place to a scenario with its development and its consequences. Therefore this allows acquiring the knowledge not only of which sequences of events are taking place, but also of the real environment in which they are taking place.

Associating the system sequences that lead to system unavailability on demand with the resulting phenomenology proves to be a useful tool for the decision making process, both in the design phase and for the entire power plant life time.

Chapter 4 presents future possible applications that could be developed with the present Dynamic PSA approach. A particular application could be the optimization or development of robust plant emergency operating procedures. In fact it consists in the coupling between the logic-probabilistics of the plant configurations corresponding to the Emergency Operating Procedure (EOP) and the associated phenomenology of the primary heat transport systems with the consideration for the plant safety systems.

The application could highlight those situations where the plant fails either because of hardware failures or system dynamics and furthermore to reveal those situations where changing of the hardware states brings the process variables of the system state out of the system domain.

A timeline course should be created for the process variables characterizing the plant state and that should reveal the time windows that operators have at disposition for intervention, in order to avoid potentially catastrophic conditions. Some week points in the EOP could be identified and then resolutions to be provided for their improvement, on the basis of sensitivity analyses.

Chapter 5 presents the conclusions and the insights of the work and outlines possible improvements in terms of the present methodology proposed.

Table of Contents

Acknowledgments

First and foremost, I would like to express my sincere gratitude to my principal advisor Prof. Marino Mazzini for the continuous support of my Ph.D study, for his patience and immense knowledge. His guidance and understanding helped me in all the time of research and writing of this thesis.

I would like to show my gratitude to Dr.Ing. Davide Mazzini who gave me the necessary support to pass over the critical moments in the development of the work. Thanks to his very nice and valuable friendship my stay and my research experience in Pisa was full of pleasant moments.

It is a pleasure to thank those who made this thesis possible and I am very grateful to Eng. Remo Galvagni and Dr.Ing. Mariagrazia Semenza. Due to their help my understanding for the use of IDDA code was possible.

I would like to thank and to show my gratitude to my family: my parents Constantin and Ioana for guiding me throughout life and helping me to choose the path toward a successful nuclear engineering career, encouraging me to carry on a project such as doctoral studies, and to my wife Narcisa for her continuous understanding and support to pursue and bring this work to the end.

Last but not the least, I offer my regards to all of those who supported me in any respect during the completion of this work.

List of acronyms

AC - Alternative Current

ADS - Accident Dynamic Simulator

ASDV - Atmospheric Steam Discharge Valve

BPC - Boiler Pressure Control

CANDU - Canadian Deuterium Uranium

CCDF - Complementary Cumulative Distribution Function

CCF - Common Cause Failure

CDF - Cumulative Distribution Function

CSDV - Condenser Steam Discharge Valve

CSN - Consejo de Seguridad Nuclear

D2O -Heavy Water

DC - Degasser Condenser

DDET - Dynamic Decision Event Tree

DETAM - Dynamic Event Tree Analysis Method

DPSA - Dynamic Probabilistic Safety Assessment

DYLAM - Dynamic Event Logic Analytical Methodology

ECCS - Emergency Core Cooling System

EOP - Emergency Operating Procedure

EPS - Emergency Power Supply

ET - Event Tree

ETA -Event Tree Analysis

EWS - Emergency Water System

FT - Fault Tree

FORTRAN - Formula Translation

GRS - Gesellschaft für Anlagen- und Reaktorsicherheit

HTS - Heat Transport System

IAEA - International Atomic Energy Agency

IDA - Integrated Decision Analysis

IDDA - Integrated Dynamic Decision Analysis

IE - Initiating Event

ISA - Integrated Safety Approach

KTH - Royal Institute of Technology

LOCA - Loss of Coolant Accident

MCS - Minimal Cut Sets

MC - Monte Carlo

MCDET - Monte Carlo Dynamic Event Tree

MCR – Main Control Room

MDG – Mobile Diesel Generator

MSSV - Main Steam Discharge Valve

MTTR – Mean Time To Repair

NPP - Nuclear Power Plant

PSA - Probabilistic Safety Assessment

PHTS – Primary Heat Transport System

PHWR – Pressurized Heavy Water Reactor

RCW - Recirculated Cooling Water

RPV - Rector Pressure Vessel

SBO - Station Blackout

SDE - Site Design Earthquake

SDCS - Shutdown Cooling System

SDG - Stand-by Diesel Generators

SDS - Safety Shutdown System

SG - Steam Generator

TLOMFW - Total Loss of Main Feedwater

UO2 - Uranium dioxide

VTT - Vattenfall Nuclear Power

List of tables

List of figures

INTRODUCTION

Nuclear safety focuses the unintended conditions or events that could lead to radiological releases from authorized activities. It relates mainly to intrinsic problems or hazards.

Nuclear safety deploys nuclear safety analyses which are an essential element to the safety assessment of a nuclear power plant.

Safety assessment is the systematic process that is carried out throughout the design process to ensure that all relevant safety requirements are met by the proposed or actual design of the plant. Safety assessment includes, but is not limited to, the formal safety analysis.

Safety analysis involves deterministic and probabilistic analyses in support of the sitting, design, commissioning, operation and decommissioning of a nuclear power plant. Safety analyses demonstrate that the overall plant design is capable of meeting the prescribed and acceptable limits for radiation doses and releases for each plant condition category and that the defense –in – depth is achieved.

Deterministic analysis aims to demonstrate that a nuclear facility is tolerant to identified faults/hazards that are within the "design basis", thereby defining the limits of safe operation. Probabilistic analysis aims to provide a realistic estimate of the risk presented by the nuclear facility. This can also be used to confirm the validity of the deterministic safety assessment.

These two types of analysis can complement one another to provide additional insights to the hazard or risk problem.

Probabilistic Safety Assessment (PSA) has been applied to large complex systems for more than thirty years. Many nuclear power plant (NPP) operators have performed probabilistic safety assessments to identify and understand key plant vulnerabilities. As a result of the availability of these PSA studies, there is a desire to use them to enhance plant safety and to operate the plants in the most efficient manner practicable.

PSA is an effective tool for this purpose as it assists plant management to target resources where the largest benefit for plant safety can be obtained. However, any PSA which is to be used to support decision making at NPPs must have a credible and defensible basis [1].

The PSA methods have also been used in other industry sectors and military applications. The first full scale application of PSA methods was the Reactor Safety Study WASH-1400[1].

[1] WASH-1400, 'The Reactor Safety Study', is a report produced in 1975 for the US Nuclear Regulatory Commission by a committee of specialists under supervision of Professor Norman Rasmussen from MIT. The report is considered nowadays obsolete.

The PSA applications are numerous, and spans from plant design phase throughout entire plant operational lifetime, including the area of incident and accident mitigation and management.

The well-established PSA techniques integrate various reliability modeling tools, such as fault trees and event trees that numerically quantify the probability of accident occurrences.

The PSA methods typically rely on the risk analyst to identify the risk scenarios. With the growth of the size of the dynamic systems and the complexity of the interactions between hardware, software and humans, it is extremely difficult to enumerate the risky scenarios by the traditional ET/FT methods [2].

It is already commonly agreed by the international PSA practitioners that conventional standalone Probabilistic Safety Assessment (PSA) has a number of fundamental limitations. Specifically, PSA can help to quantify probability of what is known as a safety issue, but it is not capable in revealing unknown issues. During abnormal transients and accidents, the complexity of nuclear power plant may drive the system non-linearly with respect to the safety parameters.

Therefore it appeared as a necessity to evolve from the conventional PSA toward an integrated approach, that considers in one platform the deterministic - probabilistic approaches. In this way one can perform comprehensive safety analyses which can tackle the complexity of the power plants. The integrated approach is called also Dynamic Probabilistic Safety Assessment.

The present work is an attempt to approach the Dynamic PSA (DPSA) throughout a coupled use of the Boolean logic integrated by the IDDA code and thermal-hydraulic analysis supported by the RELAP 5 code. The work attempts approaching Dynamic PSA throughout three different applications within the general CANDU 6 NPP operational context, without making reference to any particular CANDU 6 NPP that is operated by the CANDU owners' group countries.

CHAPTER 1

1.1 Probabilistic Safety Assessment

Probabilistic Safety Assessment (PSA) provides a tool for systematic and logical modeling of accident progression, is a comprehensive, structured approach for identifying failure scenarios; it constitutes a conceptual and mathematical tool for deriving numerical estimates of risk, including uncertainties estimation.

PSA methodology integrates information about plant design, operating practices, operating histories, component reliabilities, human behavior, thermal hydraulic plant response, accident phenomena, and brings to its conclusion at the evaluation of potential environmental and health effects.

The analysis (i.e. PSA), is done using a logical and systematic approach that makes use of realistic assessments of the performance of the equipment and plant personnel as a basis for the calculations. This in principle has the potential to produce an understanding of the inherent risk of operating the plant over a much wider range of conditions than the traditional deterministic methods, which generally define what is assumed to be a bounding set of fault conditions, [3].

The classical PSA approach deploys the event tree/fault tree methods. An *event tree analysis* (ETA) is an inductive procedure that shows all possible outcomes resulting from an accidental (initiating) event, taking into account whether installed safety barriers and systems are functioning or not, and additional events and factors. By studying all relevant accidental events the ETA can be used to identify all potential accident scenarios and sequences in a complex system. Design and procedural weaknesses can be identified, and probabilities of the various outcomes from an accidental event can be determined [4].

The fault tree itself is a graphic model of the various parallel and sequential combinations of faults that will result in the occurrence of the predefined undesired event. The faults can be events that are associated with component hardware failures, human errors, software errors, or any other pertinent events which can lead to the undesired event. A fault tree thus depicts the logical interrelationships of basic events that lead to the undesired event, the top event of the fault tree [5].

Fault tree analysis techniques were first developed in the early 1960's. Since this time they have been readily adopted by a wide range of engineering disciplines as one of the primary methods of performing reliability and safety analysis.

The relative size (i.e., complexity) of the event trees and fault trees is largely a matter of preference of the PSA analysts and also depends on the features of the software used. The most used PSA approaches employed are named Large Event Tree-Small Fault Tree and respectively Small Event Tree-Large Fault Tree.

In international practice, three levels of PSA are generally recognized:

- Level 1 PSA: the design and operation of the plant are analyzed in order to identify the sequences of events that can lead to core damage and the core damage frequency is estimated. Level 1 PSA provides insights into the strengths and weaknesses of the safety related systems and procedures in place or envisaged as preventing core damage. The detailed methodology of Level 1 PSA is presented in references [6] and [7].

- Level 2 PSA: the chronological progression of core damage sequences identified in Level 1 PSA is evaluated, including a quantitative assessment of phenomena arising from severe damage to reactor fuel. Level 2 PSA identifies ways in which associated releases of radioactive material from fuel can result in releases to the environment. It also estimates the frequency, magnitude and other relevant characteristics of the release of radioactive material to the environment. This analysis provides additional insights into the relative importance of accident prevention and mitigation measures and the physical barriers to the release of radioactive material to the environment (e.g. a containment building and associated Engineering Safety Features). The detailed methodology of Level 2 PSA in presented in IAEA guideline, reference [8].

- In Level 3 PSA, public health and other societal consequences are estimated, such as the contamination of land or food from the accident sequences that lead to a release of radioactivity to the environment. The detailed methodology of Level 3 PSA in presented in IAEA guideline, reference [9].

Level 1 PSA, Level 2 PSA and Level 3 PSA are sequential analyses, where the results of each assessment usually serve as a basis for the PSA at the next level.

Level 1 PSAs have now been carried out for most nuclear power plants worldwide. In recent years, a trend has emerged for Level 2 PSAs or limited Level 2 PSAs (e.g. Level 2 PSAs in which the large early release frequency is estimated) to be carried out for many types of nuclear power plant. In addition, Level 3 PSAs have been carried out in several States, [6].

The PSA applications cover a broad field of uses, either for design or in connection with the NPP operation, either for a regulatory perspective. The use of PSA concerns the most the NPP design and operation, but applications are done also in support of regulatory bodies, in order to ensure a risk informed decision making.

The PSA applications in connection with the plant design and operation are the following:

- Use of PSA to support NPP design
- Use of PSA to support NPP upgrade and back fitting activities and plant modifications
- Use of PSA in NPP maintenance
- Use of PSA in connection with NPP technical specifications
- Risk based configuration control

- Risk based safety indicators
- PSA based evaluation and rating of operational events
- Use of PSA to evaluate safety issues
- Use of PSA to support NPP periodic safety review
- Use of PSA to improve emergency operating procedures (EOPs)
- Use of PSA to support NPP accident management
- Use of PSA to support NPP emergency planning
- Use of PSA to improve operator training programs.

For a better understanding of PSA applications, it is recommended the technical document of IAEA, reference [1].

1.2 Dynamic PSA – a state of the art

PSA methodology has been successfully applied in different projects, but it has been recognized that it is hard to characterize some complex dynamical systems by solely applying such techniques as Event Tree/ Fault Tree analysis. Event trees or fault trees are implementations of logic. Primarily, the Boolean logic-based models are limited in terms of their capability to specify the timing of events or even the order in which events occur. It is also difficult to model the dependency of the probability or rate of occurrence of events on scenarios or time.

The classical combinatorial fault tree does not capture the potentially critical significance of the temporal ordering of failure events in a system and neither the relevant process variables with reference to the failure sequence identified (i.e. MCS).

Acknowledging such difficulties, a set of new methodologies were developed under the name of “Dynamic reliability” or “Dynamic PSA”. Because of the diverse background of people working on this problem, it is sometimes hard to define the term “dynamic reliability”.

Nevertheless, it is widely accepted that the following points list the basic characteristics of dynamic reliability/PSA modeling:

- The dynamic phenomena have a strong influence on the system’s response (e.g. the operation of control/protection devices upon reaching assigned thresholds of the process variables values);
- The hardware components failure behavior and the human operator actions depend on the process dynamics;
- The complex interactions between human operator actions and hardware components influence the system’s response and failure behavior;
- There are a variety of degraded modes related to multiple failure modes and to the process dynamics.

The analysis performed by Reina and Amendola in the end of 80ies, see [10], explored at that time the possibility of global treatment of the dynamic PSA. Then few years later the DYLAM and ADS implementations were applied to treat DPSA problems in nuclear power plants and other areas, see references [11], [12] and [13].

During that time beginning of 90ies, a more general mathematical framework was introduced for probabilistic dynamics that has been interpreted as equivalent to neutron transport theory and it was proposed to be solved by Monte Carlo simulation, see references [14], [15]. But, however the mathematical formulation for the dynamic PSA problem was first time attempted by Smidts C. and Devooght J, see [16] and then expanded by Izquierdo and Labeau, see references [16], [17] and [18].

The wide acceptance of traditional ET/FT methods has led some authors to propose extension to include some dynamic features in the FT framework. Others have introduced different graphical tools to capture the dynamical features, some of which have been used in applications. Examples are Petri Nets, Dynamic Flow-graphs, and Event Sequence Diagrams [2]. A detailed discussion of these techniques can be found in the following sub-chapters.

However for a broader overview of the dynamic PSA methodology, there are few several review papers of the DPSA, such as references [19] and [20]

Dynamic reliability methods are powerful mathematical frameworks capable of handling interactions among components and process variables explicitly. In principle, they constitute a more realistic modeling of systems for the purposes of reliability, risk and safety analyses. Although there is a growing recognition in the risk specialists community of the potentially greater correctness of these methods, no serious effort has been undertaken to utilize them in industrial applications [21].

Several dynamic approaches to reliability problems have been propounded during the last decade. They all turn out to be different numerical treatments with different assumptions of a unified theory called probabilistic dynamics. The two main candidate techniques for solving large problems are the Monte Carlo (MC) and Dynamic Discrete Event Tree (DDET) methods. Each of them has specific advantages and drawbacks, mainly related to the required memory and computation time [22].

1.2.1 Monte Carlo (MC) Simulation

While DDETs require the events to occur at predefined discrete time only, the Monte Carlo simulation approaches allow events to happen at any time. This avoids the combinational explosion of DDETs. Monte Carlo methods are insensitive to the complexity and dimension of the system. Any modeling assumption could be included, the non-fixed failure rate assumption, random delays, interaction between components and process dynamics, etc.

Generally the MC methods estimate the system safety or reliability directly, expressed in form of a probabilistic distribution function and the behavior of systems is governed by an underlying transport equation. The state explosion makes the analytical solution of the transport equation prohibitively difficult and the Monte Carlo simulation is seen as almost the only feasible solution, see reference [15].

The quantity that is of interest is defined as being the expected value of a random variable associated to the process, an estimator is obtained for each selected situation and then is averaged on the whole sample. As a Monte Carlo estimate relies on the expected value, the effect of uncertain parameters can be directly assessed during the simulation; this actually enlarges the number of variables on which the average is performed.

However, only Monte Carlo treatments for industrial applications within dynamic reliability domain are still expected to come, so far.

1.2.2 Discrete Dynamic Event Tree (DDET)

Discrete Dynamic Event Trees (DDETs) are simulation methods implemented by forward branching event trees, the branch points are restricted at discrete times only. The knowledge of the physical system under study is contained in a numerical simulation, written by the analyst. The components of the system are modeled in terms of discrete states, see references [23] and [24] All possible branches of the system evolution are tracked systematically.

One restriction of DDET is that the events (branches) only happen at predefined discrete time intervals. It is assumed that if the appropriate time step is chosen, DDETs would investigate all possible scenarios. It is a straightforward extension of the classical event trees. The binary logic restriction of the classical event trees is removed.

An example of a DDET is given in Figure 1.1, below:

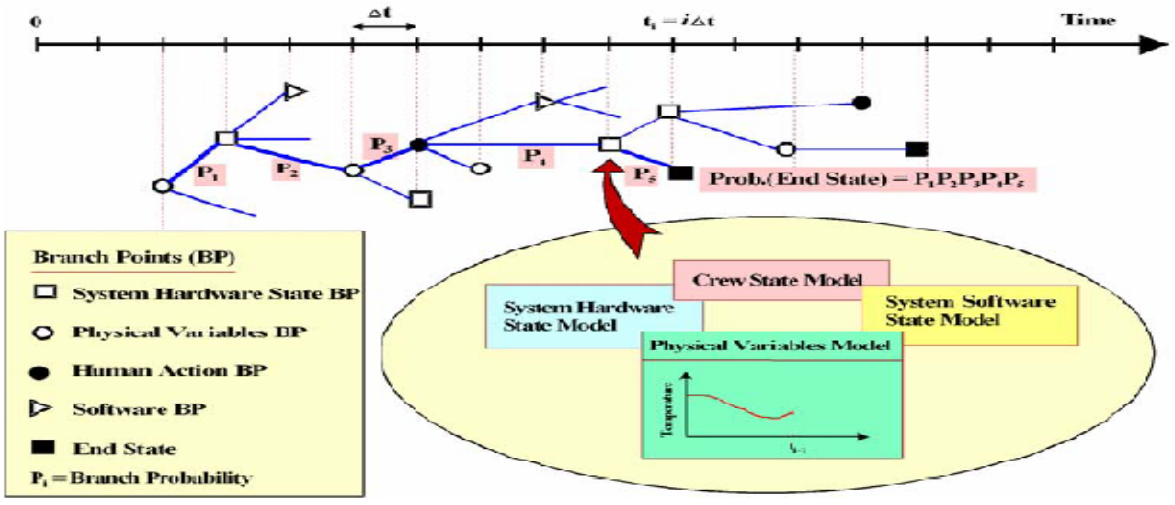


Figure 1.1 Example of a Discrete Dynamic Event Tree

The systematic branching would easily lead to such a huge number of sequences that the management of the output Event Tree becomes awkward. Measures have been taken to eliminate the explosion of branches. It can be done by increasing the length of the time step, but this may be at the expense of the accuracy of the analysis.

A cut-off probability was introduced in some implementations. The branches with a probability lower than cut-off would be discarded. Amendola in reference [25] suggested that when the number of failures in a sequence exceeds a user-defined value, further evolution along this sequence would be stopped

Implementations of DDETs include methodologies such as DYLAM, see [26], [27] and ADS in reference [28] and ADS-IDA in reference [29].

1.2.3 GO method

The GO method [30, 31] is a success-oriented system analysis that uses seventeen operators to aid in model construction. It was developed by Kaman Sciences Corporation during the 1960s for reliability analysis of electronics for the Department of Defense in U.S.

The GO model can be constructed from engineering drawings by replacing system elements with one or more GO operators. Such operators are of three basic types: (1) independent, (2) dependent, and (3) logic. Independent operators are used to model components requiring no input; the dependent operators require at least one input in order to have an output. Logic operators, on the other hand, combine the various operators into the success logic of the system being modeled. With the probability data for each independent and dependent operator, the probability of successful operation can then be calculated.

The GO method is used in practical application where the boundary conditions for the system to be modeled are well defined by a system schematic or other design documents. However, the failure modes are implicitly modeled, making it unsuitable for detailed analysis of failure modes beyond the level of component events shown in the system drawing. Furthermore, it does not treat common cause failures, nor provide structural information (i.e. the minimum cut sets) regarding the system. A brief description of GO flow, which is based on GO method, is documented in literature , see reference [30].

1.2.4 Digraph/Fault Graph

The fault graph method/digraph matrix analysis [30, 31] uses the mathematics and language of graph theory such as “path set” (i.e. a set of models traveled on a path) and “reach-ability” (i.e. the complete set of all possible paths between any two nodes), according to reference [31].

This method is similar to a GO chart but uses AND and OR gates instead. The connectivity matrix, derived from adjacency matrix for the system, shows whether a fault node will lead to the top event. These matrices are then computer analyzed to give singletons (single components

that can cause system failure) or doubletons (pairs of components that can cause system failure). Digraph method allows cycles and feedback loops which make it attractive for dynamic system.

1.2.5 Markov Modeling

Markov modeling [31] is a classical modeling technique used for assessing the time-dependent behavior of many dynamic systems [30]. In a 'Markov chain' processes, transitions between states are assumed to occur only at discrete points in time. On the other hand, in a 'discrete Markov process', transitions between states are allowed to occur at any point in time. For process system, the discrete system states can be defined in terms of ranges of process variables as well as component status.

This methodology also incorporates time explicitly, and can be extended to cover situations where problem parameters are time independent. The state probabilities of the system P(t) in a continuous Markov system analysis are obtained by the solution of a coupled set of first order, constant coefficient differential equations :

$$dP/dt = M.P(t)$$

where M is the matrix of coefficients whose off-diagonal elements are the transition rate and whose diagonal elements are such that the matrix columns sum to zero. An application of Markov modeling to a hold-up tank problem is discussed in literature [30], while Pate-Cornell used the technique to study the fire propagation for a subsystem on board a off-shore platform in [32].

1.2.6 Combined methods

In the following the two most important developments in the field of dynamic PSA will be presented; mainly, there are two centers were the research has been carried progressively to bring the most to the industrial applications. However, so far there are not any industrial applications of the dynamic PSA, only isolated applications that proved to be beneficial to the problem understanding and for decision making.

Probably, the most advanced application of the dynamic PSA methodologies has been developed by the nuclear safety authority of Spain – CSN. The research has been started in the 1980's and has involved few other institutions, such as universities and engineering companies.

The methodology is called Integrated Safety Approach (ISA) and is a systematic verification approach which can be considered as an extension of PSA and accident analysis techniques, supported by a simulation system.

The classical PSA static event trees are replaced by a generalized dynamic event-tree concept based on the theory of probabilistic dynamics (DDETs), see references [33] and [34]. Both

components of the risk, damage and likelihood are considered in this approach in a balanced and simultaneous way.

The main steps of this methodology are:

- Identification of damage variables and definition of risk acceptable regions in a frequency-damage plot.
- Initiating event (IE) and initial state selection.
- Modeling the deterministic characteristics of the plant (plant dynamics modeling) including crew procedures.
- Modeling the stochastic characteristics of the plant (reliability modeling).
- Event sequence generation.
- Analysis of the results and verification of the risk requirements.

Mainly the methodology has been employed in the delineation of the event trees, which were related to EOPs execution when combined with the complex plant dynamics involved and the large number of branches, see reference [35].

This software tool consists of a closed-loop plant/operator simulator: a thermal hydraulic code for simulating the plant transient (TRETA for PWR NPPs and TIZONA for BWR NPPs) and the procedures processor (COPMA III) to simulate the operator actions requested by the procedures, both coupled by a data communication system which allows the information exchange (SWBus). TRETA and TIZONA are modular simulation systems that are able to simulate virtually all the plant systems, including control, protection and balance of plant, and both include the necessary models to simulate PWR and BWR plants, according to reference [36].

The thermal-hydraulic modules are based on elaborated models that combine a good representation of most of single and two phase water regimes with a relatively fast solution algorithm. The modules are capable to incorporate also other single-application oriented codes (i.e. RELAP5, MAAP, CONTAIN) as modules using parallel computing techniques , see reference [37].

Another advanced application has been developed by Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) from Germany; this Institute coupled the Monte Carlo simulation and DDET, the coupled approach has been called MCDET. MCDET was realized as a set of software modules which were suitably connected with the integral accident analysis code MELCOR. The MCDET methodology was developed to consider time dependent interactions of stochastic events and the process dynamics. Within this application a sample of approximately 9800 accident sequences were computed. To each accident sequence the respective set of events and the probability of occurrence are attached. Since these approach needs much computing resources, its application was restricted to the in-vessel phase of a station blackout (SBO) accident up to RPV failure, see reference [38].

Currently there is an ongoing joint program of VTT Technical Research Centre of Finland and Royal Institute of Technology (KTH) from Stockholm to develop an integrated platform of combined Dynamic Deterministic/Probabilistic Safety Assessment for performing comprehensive safety analysis which can tackle with multifaceted complexity of the power plants. The program is meant to develop a plan for collaborative activities between KTH and VTT for the period 2012-2014.

1.2.7 Summary

The Dynamic Probabilistic Safety Assessment (DPSA) methodology has been evolving in the last two decades. DPSA methodologies are capable of handling interactions between components and the process variables; they provide more realistic modeling of the dynamic systems for the purpose of risk analysis. There is a growing recognition in the risk community of the potentials of these methods. Discrete Dynamic Event Tree and Monte Carlo simulation are two classes of methods that have been widely used.

The techniques discussed above address the deficiencies found in fault/event tree methodologies when analyzing dynamic scenarios. However, there are also limitations to their usage. The digraph and GO techniques model the system behavior and deal, in limited extends, with changes in model structure over time. On the other hand, Markov modeling requires the explicit identification of possible system states and the transitions between these states. This is a problem as it is difficult to envision the entire set of possible states prior to scenario development. DYLAM and DETAM can solve the problem through the use of implicit state-transition definition. With the large tree-structure generated through the DYLAM and DETAM approaches, large computer resources are required. The second problem is that the implicit methodologies may require a considerable amount of analyst effort in data gathering and model construction.

However, so far there are not any tools or methodologies to be used for industrial application purpose, the research and people involved in development of DPSA is still proposing and new attempts are ongoing.

1.3 Integrated Dynamic Decision Analysis (IDDA)

Integrated Dynamic Decision Analysis (IDDA) is a code developed by the Italian engineer Remo Galvagni in the 1980's, and since that period has been continuously improved its features and capabilities. The developer has been the former Director of the Technical Commission for Licensing Operators of Research and Prototype Nuclear Plant within Italian National Committee for Nuclear Energy and also the former member of many IAEA working groups.

IDDA code is an enhanced decision-dynamic event tree. IDDA approach is based on a consistent application of Boolean logic and can be considered a methodology that allows the systematic and complete exploration of alternatives of plant states that are possible within the formulated assumptions.

Integrated Dynamic Decision Analysis provides a full representation of the plant states, as well as all the possible occurrences patterns, expressed in a set of mutually self-excluding sequences. Availability of the full set of alternatives allows the complete spectrum of possible probability-consequence conditions to be used as a basis for decisions in risk reduction. Furthermore it is possible to interface with the logic-probabilistic model a process simulator, in order to assess the status of each relevant process variable with reference to the failure sequence identified, allowing the mutual interactions of the hardware components and the physical evolution of the plant to be taken into account [39].

Starting from a description, reflecting the level of knowledge that the analyst has about the system, IDDA is able to develop all the sequences of events compatible with the description received, from the point of view both of the logical construction, as of the probabilistic coherence. The system description has the form a binary chart, where the real logical and chronological sequence of the events is described; the direction of each branch is characterized by a probability of occurrence that can be modified by the boundary conditions, and in particular by the same development of the events themselves (probabilities conditioned by the events dynamics). As a matter of fact, in dynamic cause-consequence logic, in addition to the direct logical interactions characterizing it, each event can influence the subsequent events, depending on deterministic cause-consequence relations or stochastic dependences.

At the end of the analysis, the full set of the possible alternatives in which the system could evolve is obtained. These alternatives represent a “partition” since they are mutually exclusive; they are all and the sole possible alternatives, this allowing the method to guarantee the completeness and the coherence of the analysis.

Employment of IDDA to generate alternatives and quantify their probabilities and consequences greatly eases the analyst’s task and also supplies him with tools and recordings that fully support his conclusions. Simplification of the logical-probabilistic model can reduce the set of alternatives to only few that further obviously facilitates investigation of the corrective measures best able to bring the plant into conformity with acceptable safety standards [40].

The methodology has been mainly deployed in chemical installations applications, but also in nuclear and thermal facilities. The following chapters will present the features and capabilities of the methodology.

1.4 References

[1] Applications of Probabilistic Safety Assessment for nuclear power plants, IAEA-TECDOC-1200

[2] A guided simulation methodology for dynamic probabilistic risk assessment of complex systems, Yunwei Hu, 2005

[3] Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 1), 50-P-4, IAEA, 1992

[4] System Reliability Theory, Marvin Rausand, University of Science and Technology, Norway, 2005

[5] Fault Tree Handbook with Aerospace Applications, NASA, 2002

[6] Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, SSG-3, IAEA, 2010

[7] Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 1), 50-P-4, IAEA, 1992

[8] Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 2): Accident Progression, Containment Analysis and Estimation of Accident Source Terms: A Safety Practice, 50-P-8, IAEA, 1995

[9] Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 3): Off-Site Consequences and Estimation of Risks to the Public: A Safety Practice, 50-P-12, IAEA, 1996

[10] DYLAM-2 Description and how to use, Reina G. and Amendola A., , Commission of the European Communities, JRC Ispra (Italy), Euratom, PER1393/87, Technical Note I.87.128, 1987

[11] Dynamic accident sequence simulator for probabilistic safety assessment, Hsueh K.S. and Mosleh A, Proceedings of PSA'89, pp. 661-666, 1989

[12] The DYLAM approach for the reliability analysis of systems with dynamic interaction, Cojazzi G. and Cacciabue P.C., Reliability and safety assessment of dynamic process systems, NATO ASI Series 120, Springer Verlag, Berlin, 1994

[13] Dynamic PRA using ADS with RELAP5 code as its thermal hydraulic module, Chang Y.H. and Mosleh A., Proceedings of PSAM-IV, Volume 4, pp. 2468–2473, 1998

[14] Probabilistic reactor dynamics. I. The theory of continuous event trees, Devooght J. and Smidts C, Nuclear Science and Engineering 111, pp. 229-240, 1992

[15] Towards dynamic PSA via Monte Carlo methods, Marseguerra M. and Zio E, Proceedings of Esrel'93, pp. 415-427, 1993

[16] Probabilistic reactor dynamics. III. A framework for time dependent interaction between operator and reactor during a transient involving human error, Smidts C. and Devooght J, Nuclear Science and Engineering 112, pp. 101–113, 1992

[17] The Stimulus-Driven Theory of Probabilistic Dynamics as a Framework for Probabilistic Safety Assessment , Izquierdo J.M. and Labeau P.E, Proceedings of PSAM7 – Esrel'2004, Volume 2, pp. 687-693, 2004

[18] Relationships between probabilistic dynamics, dynamic event trees and classical event trees, Izquierdo J.M., Meléndez E. and Devooght J., Reliability Engineering and System Safety 52, pp. 197-209, 1996

[19] Dynamic reliability: towards an integrated platform for probabilistic risk assessment, P.E. Labeau, C. Smidts, S. Swaminathan, 2000

[20] Dynamic reliability, Jacques Devooght, Université Libre de Bruxelles, 2000

[21] Dynamic reliability: towards an integrated platform for probabilistic risk assessment, P.E. Labeau, C. Smidts, S. Swaminathan, 2000

[22] DDET and Monte Carlo simulation to solve some dynamic reliability problems, S. Marchand, B. Tombuyses, P.E. Labeau

[23] The DYLAM approach to the dynamic reliability analysis of systems, Cojazzi G, Reliability Engineering and System Safety 52 (3), pp. 279-296, 1996

[24] The development and application of the accident dynamic simulator for probabilistic risk assessment of nuclear power plants, Hsueh K.S. and Mosleh A, Reliability Engineering and System Safety 52 (3), pp. 297-314, 1996

[25] Accident sequence dynamic simulation versus event trees, Amendola A., Reliability Engineering and System Safety 22, pp. 3-25, 1988

[26] The DYLAM approach to the dynamic reliability analysis of systems, Cojazzi G, Reliability Engineering and System Safety 52 (3), pp. 279-296, 1996

[27] A human factor methodology for safety assessment based on the DYLAM approach Cacciabue P.C. and Cojazzi G, Reliability Engineering and System Safety 45, pp. 125-138, 1994.

[28] Risk assessment for dynamic systems: An overview, Siu N, Reliability Engineering and System Safety 43, pp. 43-73, 1994

[29] The development and application of the accident dynamic simulator for probabilistic risk assessment of nuclear power plants, Hsueh K.S., Mosleh A, Reliability Engineering and System Safety 52 (3), pp. 297-314, 1996

[30] Risk assessment for dynamic systems: an overview, N. Siu, 1994

[31] Ralph R. Fullwood & Robert E. Hall. Probabilistic Risk Assessment in the Nuclear Power Industry. 1st Ed, Pergamon Press, 1988

[32] M. E. Pate-Cornell. “Risk Analysis and Risk Management for Offshore Platforms: Lessons from the Piper Alpha Accident”. Journal of Offshore Mechanics and Arctic Engineering, Vol. 115, Aug 1993, pg 179-190

[33] Probabilistic dynamics as a tool for dynamic PSA, J. Devooght, C.Smidts, Reliability Engineering and System Safety 52(3), pp. 185-196, 1996

[34] Relationships between probabilistic dynamics, dynamic event trees and classical event trees, J.M. Izquierdo, E. Meléndez, J.Devooght, Reliability Engineering and System Safety 52, pp. 197-209, 1996

[35] Development of a software tool for the analysis and verification of emergency operating procedures through the integrated simulation of plant and operators actions, A. Esposito, C. Queral, J. Hortal, A. Quiroga, A. Ibarra, J.E. Hulsund, I. Gonzalez, G. Jimenez

[36] DENDROS: A second generation scheduler for dynamic event trees, Munoz R., Minguez E., Melendez E., Izquierdo J.M. and Sanchez-Perea M., Proceedings of M&C’99, Volume 2, pp. 1358-1367, 1999

[37] Development of a software tool for the analysis and verification of emergency operating procedures through the integrated simulation of plant and operators actions, A. Exposito , C. Queral , J. Hortal , A. Quiroga , A. Ibarra , J.E. Hulsund , I. Gonzalez , G. Jimenez

[38] Classical Event Tree analysis and Dynamic Event Tree Analysis for High Pressure Core Melt Accidents in a German PWR]. H. Loeffler, J. Peschke, M. Sonnenkalb

[39] Integrated Dynamic Decision Analysis: a method for PSA in dynamic process system, M. Demichela, N. Piccinini

[40] Integrated Dynamic Decision Analysis of a gas drying plant: phenomenological analysis, N. Piccinini, M. Demichela

CHAPTER 2

2.1 Introduction of CANDU 6 design

CANDU is an acronym for Canada Deuterium Uranium. A unique design, the CANDU system uses deuterium oxide (heavy water) as moderator and natural uranium as fuel. The core of the nuclear steam supply system of a CANDU 6 power plant is inside a large cylindrical vessel called the calandria. This vessel is filled with cool, low-pressure heavy water. The vessel houses 380 horizontal tubes, loaded with natural uranium fuel bundles.

The CANDU 6 plant layout can be seen below in Figure 2.1.

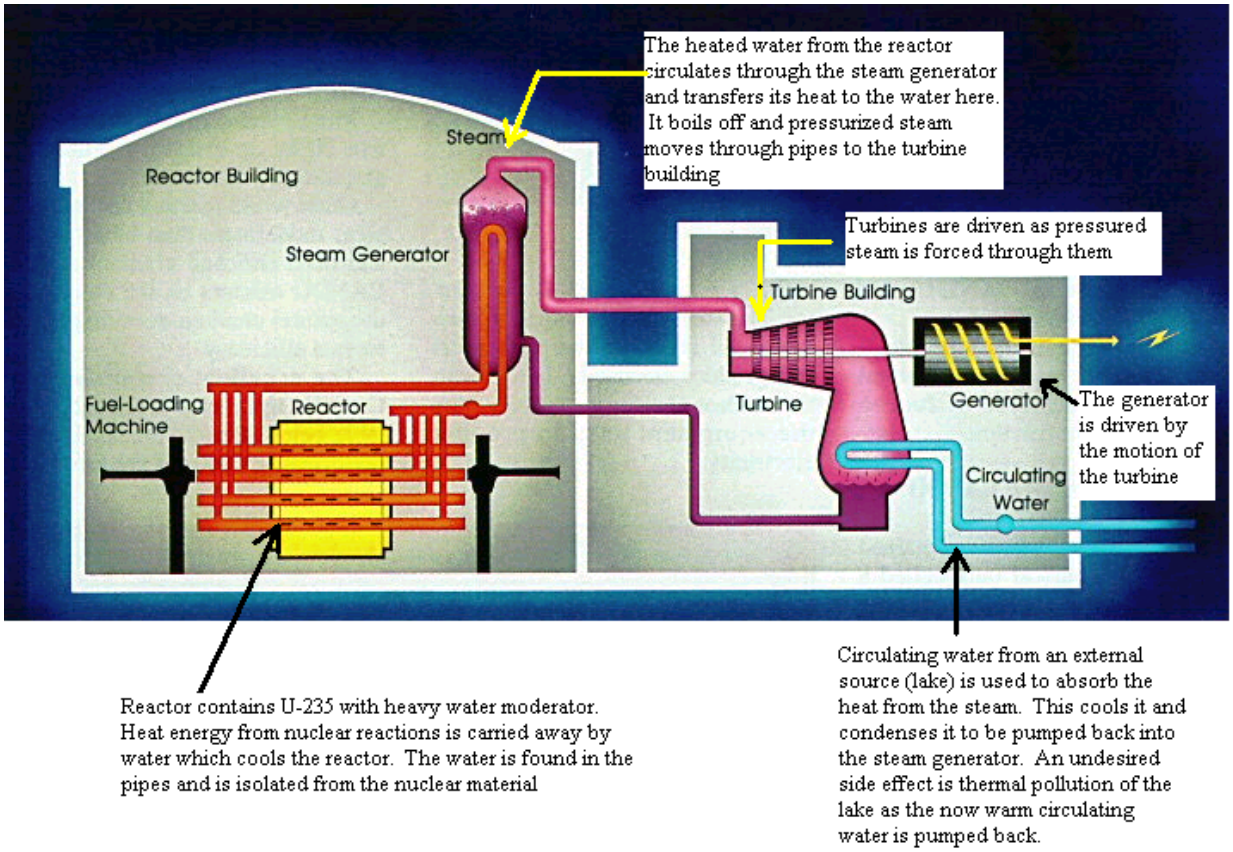


Figure 2.1 Simplified CANDU 6 plant layout

Originally licensed in Canada, the CANDU 6 design has also been licensed in every country where it has been sold. The first of the CANDU 6 series entered commercial service in 1983. The initial design of CANDU 6 was derived as a single-unit version of the successful Pickering A station in Ontario - Canada, an integrated four-unit plant operated by Ontario Hydro. Many

evolutionary improvements have been made in the design since these first units entered service, based on improved technology and the feedback of operating experience. Also, many of these later improvements have been back-fitted to the older plants, [1].

Fuel channels are the primary high-technology element of the CANDU design. A closed loop containing pressurized heavy water transports reactor heat to conventional U-tube steam generators and then to the steam turbine.

CANDU features such as natural uranium fuel and on power refuelling provides independence in fuel supply and respectively high capacity factors.

All CANDU 6 power plants are highly automated, requiring only a minimum of manual operator action. Each plant has two independent digital computers which operate continuously, one operating and one on standby. All aspects of the plant's operation are monitored and controlled from the control room. In case that the main control room is not available, the station can be shut down and kept in a safe condition from a secondary control room in another part of the plant.

CANDU 6 has four special safety systems: two independent fully capable and passively initiated shutdown systems (SDS1 and SDS2), the containment system, and the emergency core cooling system (ECCS).

The two safety shutdown systems (Shutdown System No. 1 and Shutdown System No. 2) are physically and functionally separate from each other and from the reactor regulating system. Each of the two shutdown systems is independently capable of shutting down the reactor and maintaining the reactor shutdown for all design basis events. The relatively long prompt neutron generating time inherent in CANDU 6 reactors retards power excursions and reduces the speed required for shutdown system action, even for large hypothetical reactivity increases.

The containment system, which includes the reactor building and the containment isolation system, provides a post-accident environmental barrier.

The emergency core cooling system provides fuel cooling in the event that the normal reactor coolant (D2O) is lost from the heat transport system due to a loss of coolant accident. The reactor may not be operated without all of the special safety systems being available.

Systems that provide reliable services, such as electrical power, cooling water, and air supplies to the special safety systems are referred to as safety support systems. To guard against cross-linked and common mode events, all plant systems, including the safety system are assigned to one of two available Groups (Group 1 and Group 2).

In case of accident conditions (e.g. LOCA), either Group can perform the necessary safety functions to maintain the plant in a safe state despite loss of the other Group.

Table 2.1 gives the list of systems that belong to each Group.

Safety Function	**Group 1**	**Group 2**
Reactor shutdown	*Shutdown System 1*	*Shutdown System 2*
Fuel Cooling	*Emergency Core Cooling System*	Emergency Water System Emergency Power Supply
Radioactivity Containment	Reactor Building Air Coolers	*Containment system*
Plant Monitoring	Main Control Room	Secondary Control Area

Table 2.1 Grouping of CANDU 6 Special safety systems

The Special Safety Systems and standby safety related systems have been physically separated by their assignation into two groups (Group 1 and Group 2) in order to provide adequate protection against common cause failures from events such as:

- Turbine disintegration and resultant missiles;
- Fires that can lead to uninhabitable control centre, wide spread system damage, etc.;
- Aircraft crash;
- Failure of a common process e.g. Electrical Power Systems, Service Water System, etc.;
- Common adverse environment e.g. extremes of temperature, pressure, humidity, radiation, toxic gases, etc.

The CANDU safety philosophy is based on the concept of single/dual failures. “Single failure” is a failure of any process system which is required for the normal operation of the plant and “dual failure” represents a combination of the single failure events and a simultaneous failure or impairment of one of the special safety systems. Coincident failure analysis is a systematic assessment of postulated dual failures.

Consideration of dual failures (i.e. single failure + failure of a safety system) at the design stage gives the fundamental design requirements for the safety systems, such as reliability- to ensure that the frequency of a dual failure is very low; therefore, the reliability of the safety systems is required to be high.

CANDU6 Electrical Power Systems

The power supply sources for a generic CANDU 6 plant are as follows, [2]:

- Redundant offsite sources, which provide electrical power required during startup and shutdown of the unit and can also, supply power during normal operating conditions;
- The turbine generator (onsite), which provides electrical power required during normal operation;
- On site standby sources which provide the electrical power required in case of loss of the normal power supply: Class III Standby Diesel Generator (SDG), batteries, Emergency Diesel–generator (EPS, Emergency Power Supply).

The onsite power distribution system is divided into redundant load groups (EVEN and ODD), so that the loss of any one group does not prevent the minimum safety function from being performed. Furthermore the onsite station service power supplies are classified as four classes that range from uninterruptible power to that which can be interrupted with limited and acceptable consequences, provided as follows:

- **Class I:** Uninterruptible direct current (dc) supplies for essential auxiliaries, control, protection and safety equipment. Batteries provide uninterruptible power for 8 hours.

- **Class II:** Uninterruptible alternating current (ac) supplies for essential auxiliaries, control, protection and safety equipment. Uninterruptible power is provided by batteries, through inverters or by Class III during unavailability of the inverters.

- **Class III:** Power supplies to the safety-related systems. Normal supply of Class III distribution system is from Class IV via the service transformers, and it is backed-up by 100% redundant standby diesel generators with 100% redundancy. Any interruption of power is of a short duration (i.e. maximum 180 s), which is necessary for start-up and loading of the standby diesel generators. Also, Class III is the charging source to the Class I batteries and back-up supply to Class II loads.

- **Class IV:** Normal alternating current supplies to auxiliaries and equipment, which can tolerate long duration interruptions without affecting nuclear safety, personnel or equipment safety. A complete loss or a loss of either odd or even division of Class IV power will initiate a reactor shutdown. Partial and total loss of Class IV power, including loss of offsite power are design basis events which do not pose any safety threat to the plant.

  Emergency Power Supply System: A completely independent, seismically qualified, emergency power supply (EPS) system designed to 100% redundancy and separation requirements is also provided to cope with common mode events, ensuring the safety functions are maintained. This system is intended for back-up supply supporting essential safety functions when all the others electrical supplies are unavailable or when the main control room is uninhabitable.

  Considering that the EPS buses could allow an electrical connection for the mobile Diesel Generator as those provided by the fire fighters, then in accident conditions the mobile diesel generator could recover the plant conditions. The fuel supply should be provided until the plant gets stable or the offsite grid is recovered.

2.2 Emergency Water System (EWS) description

Emergency Water System (EWS) is a safety support system of the special safety systems that belongs to the second Group of the safety systems. EWS ensures an adequate heat sink for decay heat removal following the loss of normal heat removal systems. Facilities are provided

for a separate water supply to the steam generators, emergency core cooling (ECC) heat exchangers and heat transport system.

A schematic diagram of the Emergency Water Supply (EWS) system is shown in Figure 2.2, from reference [3].

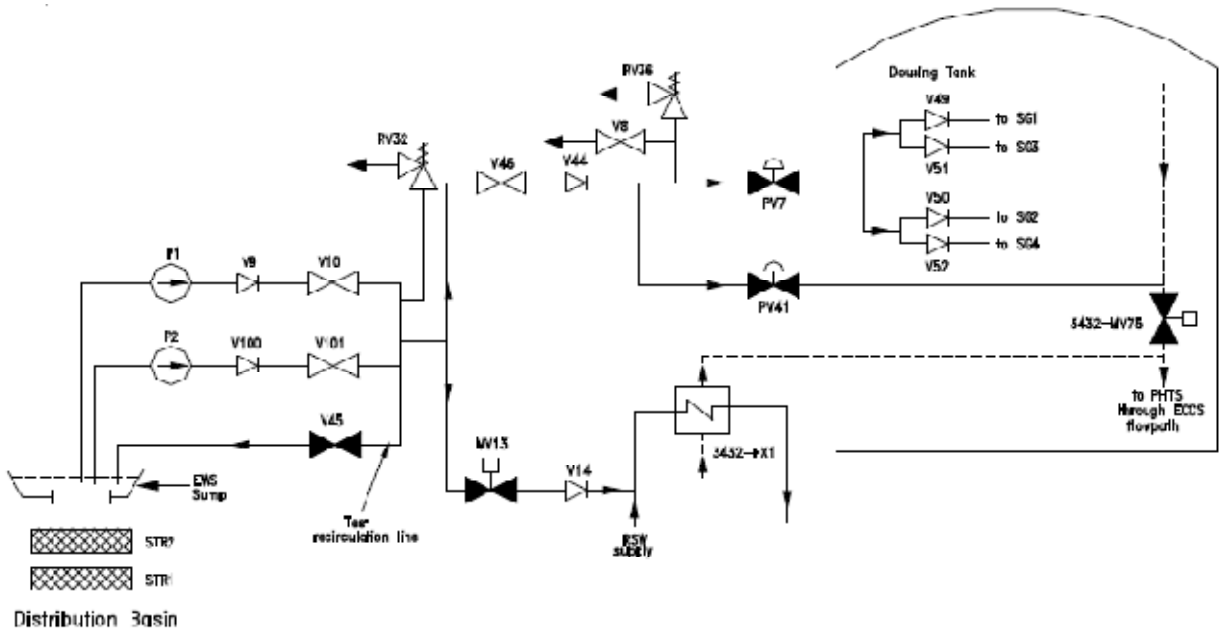


Figure 2.2 The simplified scheme of the EWS system

In the following points, the functions that are performed by EWS are described.

2.2.1 Emergency water supply to Steam Generators

In case the power system is lost or breaks in the feedwater – main and auxiliary - trains occur, the EWS provides an independent source of water for the steam generators of up to 30 kg/s. From EWS pump a pipeline discharges water into four pipelines inside the reactor building, each connecting to an EWS nozzle of the steam generator. Emergency water is ordinary water from any considerable water source.

Air-operated valves outside containment plus check valves at the steam generators inside containment provide the necessary segregation between the EWS and steam generator secondary side.

Valve connections to the dousing tank ECC line also allow water to be available for steam generator cooling purposes. This provides water to the steam generators until the EWS pumps have been started; preferable is to use the demineralised water to the largest possible extent from dousing tank instead of the untreated water of the EWS system. As long there is no need, either the dousing or the medium pressure ECC system to be available during the accident modes, the water from dousing tank can be used for an extended period of time.

On short term basis the water for the steam generators can be obtained by opening the valves and connecting the ECC injection line to the steam generators. This makes the medium pressure ECCS (dousing tank) water available until the EWS pumps have been started.

2.2.2 Emergency water supply to the primary heat transport system

EWS is initially provided from the dousing tank (500 m^3) via the emergency core cooling piping. The ECC valves can be powered by the EPS system to ensure that the ECC piping path is available.

Emptying the dousing tank leaves 1.8 m of water in the reactor building. Water from the main EWS pumps is subsequently provided for the heat transport system. One of the ECC recovery pumps (0.605 m^3/s) is used to re-circulate the water accumulated in the reactor building back into the dousing tank until the dousing tank is refilled.

The water in the dousing tank can then provide makeup to the heat transport circuit by opening the supply path as soon as the heat transport pressure falls below the dousing tank head.

2.2.3 Emergency water supply to ECCS heat exchangers

The EWS system backs up the Recirculated Cooling Water (RCW) system to ensure the reliability of supply of cooling water to the ECC heat exchangers during long term ECC operation. Long term ECC is required for a period of up to 3 months after a loss of coolant accident (LOCA).

The failure of the RCW system after a SDE should not fail the EWS. A flow of more than 85 l/s from the EWS is supplied to the ECC heat exchangers for decay heat removal. This flow is supplied from the EWS pump into the recirculated cooling water side of the ECC heat exchangers for long term ECC cooling.

The specific requirement for backup to the RCW for long term ECC operation occurs following a LOCA and subsequent failure of the Class IV and Class III power and/or cooling water systems due to an earthquake or system unavailability. For this sequence of events, EWS to the ECC heat exchangers is not required until a time later than 24 hours after the LOCA.

2.3 EWS system unavailability analysis

The EWS function unavailability that will be considered for the study is the main EWS function, which is the emergency water supply to steam generators. The unavailability study considers many simplifications in system configuration due to the lack of official data. The EWS function unavailability study considers two different system configurations, which evolved due to such studies and feedback operating experience. Currently these configurations are available on different CANDU 6 operating units.

The current application is meant to demonstrate some of the features and capabilities of IDDA code. The goal of the application is to calculate the function unavailability by the use of logical statements, probabilistic and logical constraints and not by the use of logical gates as with the use of the classical fault trees.

IDDA approach provides a full representation of the plant states during operation (ordinary, incidental or irregular operating conditions), as well as all the possible occurrences (logical and phenomenological description of events), expressed in a set of mutually self excluding sequences, said constituents.

The information provided can condition the graph development and allow a right application of theory of probability, as inductive logic, often said Bayesian approach. Also the information can condition the knowledge about states of successive aleatory events and the development of sequences, [4].

2.3.1 IDDA input file syntax

IDDA approach is based on consistent application of Boolean Logic. The development of the universe of the problem and identification of its constituents are done by use of an open graph method. The graph development is in comply with the imposed constraints, either logic or probabilistic.

Every branch of graph represents a possible time-trajectory of events with consequent progressive increase of logic and phenomenological information. The information can condition the graph development and allow a right application of theory of probability, as inductive logic.

The nodes or pivotal points of each graph are formed by aleatory events. The information about the state of nodes can condition the knowledge about states of successive aleatory events and the development of their scenarios.

The information contained by the universe of the problem allows obtaining self-consistent solutions, either from phenomenological and/or logic-probabilistical points of view.

The analyst is required to describe the whole system in a logically consistent manner. Description is in form of questions regarding all significant random events related to the operation of the system itself, which are called “levels”.

The level represents the elementary matter of the logical model and also a node in the event tree. It describes an uncertainty situation, a pivotal point where the logical path can take different courses.

Each pivotal point (level or question) has:

- a probability, that represents its expectation degree
- an uncertainty ratio, that represents the data dispersion, when using failure rate statistics to assign the probability

- next level addresses, that link to the following questions depending on the answer to the current one
- a comment string that allows the user to read the logical development of a sequence
- constraints allow the analyst to modify the input according to the current knowledge status.

The levels or questions are characterized by their possible logical constraints or possible probabilistically conditions regarding the given events. In particular the constraints can be logical and probabilistically; both of them present a twofold typology.

The logical constraints have the following functions:

- Change of address of the following questions or levels in case of success or failure, of the considered question or level (i.e. requested change of the logical algorithm).
- Determination of state (i.e. success or failure) of the following questions or levels, in case of success or failure of the considered question or level (i.e. constraints on states of the following levels).

The probabilistically constraints are related to probability evaluations along the event trajectories (or time trajectories) that characterize each constituent (scenario).

The probabilistically constraints have the following twofold typology:

- A first conditioning type of probabilities is assigned to the single events due to knowledge of success or failure states of former events.
- A second conditioning type is related to variations as mission time or waiting times in which event probabilities have to be evaluated. The capability to introduce variations allows in particular dealing in a simple way with problems where we need to take into account single component reparability and restoration times.

The process of ordering the questions, on the basis of the information available to the analyst, is an inductive one by trials and successive corrections. The developed IDDA methodology has as fundamental purpose to make systematic and complete exploration of alternatives that are possible inside the formulated assumptions, [5].

An example of the syntax file with few lines of the input is shown below:

```
:SV7 fails to open
10   5.E-3    0.720    11   17   3   'SV7'   'Works'   'dnWork'


:PV7 properly failure to open
11   1.11E-03   0.466    12   901   3   'PV7PF'   'Open'   'dnOpen'
16   8   0.   0.


:CV49 failure to open
12   1.3E-05   0.720   100   901   3   'CV49.O'   'Open'   'dnOpen'
```

IDDA syntax file corresponding to the first system configuration is given in the Annex A, while the Annex B contains the file that translates the IDDA syntax into normal language that makes easier to understand the numbers used to define the logic algorithm of the input file.

The unavailability analysis considers two system configurations with the goal of showing what could be the differences in terms of function unavailability. The first configuration is shown in Figure 2.2; a second system configuration is considered, as outlined below.

The emergency water supply is considering two injection paths or sources. First is the injection line from the dousing tank to the secondary side of the steam generator through the two pneumatic valves in series. The second alternative from the water source through one out of two EWS pumps to the secondary side of the steam generators.

The second system configuration analyzed considers one more pneumatic valve in parallel for each pneumatic valve disposed in series for the first system configuration.

2.3.2 Study Assumptions for System Unavailability

The present study considers the assumptions presented below. The study is simplified and does not have the objective of evaluating the complex and detailed system unavailability.

- The power supply of the EWS pumps is credited;
- The water intake necessary for EWS pumps is credited;
- The pipe intake clogging or pump strainer clogging are not considered;
- The EWS support systems are credited as available;
- It is credited that the SGs are depressurized and the EWS pumped supply is possible.

2.3.3 EWS – Generation of the universe

The problem that has to be solved should be described in the language of the code that after develops the Partition (Universe) and its constituents (i.e. event trajectories) in a clear, univocal and complete way. The problem is modelled by a sequence of questions, related to *true* or *false* of subsequent *random events.*

Once the system configuration and operation is described, then the software generates the universe of the problem (i.e. all the possible scenarios that can occur). The generated scenarios reflect the status of knowledge that the analyst has available.

Table 2.2 presents the results of this application, without and with the application of a cut-off of 1.E-12.

	# Scenarios Generated	Residual Probability	Partition Entropy
No cut-off applied	725	0.00	3.119E-01
Cut-off applied (i.e. 1.E-12)	282	3.576E-11	3.119E-01

Table 2.2 Application of IDDA code to the evaluation of EWS unavailability.

In case of the first system configuration there are 725 generated scenarios, in the conditions of no cut-off applied. In case that a classical cut-off of 1.E-12 which normally is applied in the common practices of system unavailability analysis, then the resulted scenarios are 282.

2.3.3.1 Entropy

Entropy is ubiquitous in physics, and it plays important roles in numerous other disciplines ranging from logic and statistics to biology and economics. Entropy is defined differently in different contexts, and even within the same domain different notions of entropy are at work. Some of these are defined in terms of probabilities, others are not.

The concept of entropy , besides the entropy from thermodynamics, comes from the Information theory. Information theory is a branch of applied mathematics and electrical engineering involving the quantification of information. Information theory was developed by Claude E. Shannon to find fundamental limits on signal processing operations such as compressing data and on reliably storing and communicating data. Since its inception it has broadened to find applications in many other areas.

The most general interpretation of entropy is as a measure of our uncertainty about a system and the entropy quantifies the uncertainty involved in predicting the value of a random variable.

The entropy general formula is the following:

$$Entropy(s) = -\sum_{i=1}^{C} p_i \log_2 p_i$$

If it is measured the entropy of a dataset S, with respect to one attribute, in this case the target attribute is calculated with formula given above, where p_i is the proportion of instances in the dataset that take the i^{th} value of the target attribute.

High *Entropy* means that the sampling comes from a uniform distribution with a flat histogram, therefore having an equal chance of obtaining any possible value.

Low *Entropy* means that the distribution varies, it has peaks and valleys. The histogram of frequency distribution would have many lows and maybe one or two highs. Hence it is more predictable.

Entropy values ranges from 0 (i.e. all instances of a variable have the same value) to 1 (i.e. equal number of instances of each value).

2.3.3.2 Entropy applicability within IDDA

The total number of constituents or event trajectories developed within the universe of problem (i.e. partition) is characterized by the *entropy* of partition that indicates how difficult could be to single out the true constituent among all those that have been defined. In case there is a reduction in entropy due to some additional information provided then the value shown confirms that a pre-existing dominant event has become even more dominant. On the other hand the increase of entropy confirms that the function unavailability is shared into a larger number of constituents (i.e. scenarios) and therefore presumably into a larger number of causes, too.

Hence, the entropy measures the degree to which the probability of the system is spread out over different possible microstates (constituents or scenarios).

The entropy concept is shared by the decision trees analyses, which are the bases of development of IDDA code.

2.3.3.3 Unavailability Analysis Results

The unavailability analyses were performed for the two system configurations considered. In the following paragraphs are presented the results obtained. In order to outline the form of constituents or scenarios generated within the universe of the problem, the most contributing scenarios are shown in the following for the two system configurations.

The constituent/scenario is simply the combination of events that brings to the top event. In comparison with the Fault Tree technique, IDDA code gives the constituents set instead of fault-tree cut set. The difference is that the fault tree cut set is the set of failures that are bringing to the Top Event occurrence and on the other side, IDDA constituent set is a set of successes and failures that cause the Top event, therefore it is logically incompatible with all the constituents.

Below are presented the most contributing scenarios to the top event unavailability corresponding to both system configurations.

System configuration 1 – most contributing scenario

```
----------------------------
CONSTITUENT Ordinal :      2

  1   IE         Occurs     -  V    1.0000E+00
  2   Pre.Sens   Calibr.    +       9.7000E-01          3.0000E-02
  3   MSSVs      Success    +  V    9.7000E-01
  4   3.45bar    Success    +  V    9.7000E-01
  5   DTank      No Leak    +       9.7000E-01          9.4300E-07
  6   PV41MNT    No.MNTC    +       9.7000E-01          1.0000E-06
  7   SV41       Works      +       9.6515E-01          5.0000E-03
  8   PV41PF     Open       +       9.6408E-01          1.1100E-03
  9   PV7MNT     No.MNTC    +       9.6408E-01          1.0000E-06
 10   SV7        Works      +       9.5926E-01          5.0000E-03
 11   PV7PF      dnOpen     -       1.0648E-03          1.1100E-03
901   EWS        Failure    -  V    1.0648E-03

          PROBABILITY equal to   :   1.0648E-03
```

System configuration 2 – most contributing scenario

```
----------------------------
CONSTITUENT Ordinal :      1

  1   IE         Occurs     -  V    1.0000E+00
  2   Pre.Sens   Calibr.    +       9.7000E-01          3.0000E-02
  3   MSSVs      Success    +  V    9.7000E-01
  4   3.45bar    Success    +  V    9.7000E-01
  5   DTank      No Leak    +       9.7000E-01          9.4300E-07
  6   PV41MNT    No.MNTC    +       9.7000E-01          1.0000E-06
  7   SV.41      Works      +       9.6515E-01          5.0000E-03
  8   PV.41.PF   Open       +       9.6408E-01          1.1100E-03
  9   PV7.MNT    No.MNTC    +       9.6408E-01          1.0000E-06
 10   SV.7       Works      +       9.5926E-01          5.0000E-03
 11   PV.7.PF    Open       +       9.5819E-01          1.1100E-03
 12   CV49.O     dnOpen     -       1.2456E-05          1.3000E-05
901   EWS        Failure    -  V    1.2456E-05

          PROBABILITY equal to   :   1.2456E-05
```

Table 2.3 presents the results obtained for the two system configurations considered.

Analyses Results	**Configuration 1**	**Configuration 2**
Number of scenarios (cut-off 1.E-12)	282	362
Number of scenarios that lead to Top Unavailability	212/282	206/362
Q [f/demand] - Unavailability	1.168E-03	2.196E-05
Entropy	3.119E-01	3.122E-01
Most contributing scenario on the total Q top unavailability	1.0648E-03 (91.1%)	1.245E-05 (56.7%)
Minimal Cut Sets	212	206

Table 2.3 Results of the application of IDDA code to the evaluation of EWS unavailability

The results obtained proof the fact that the system configuration 2 is categorically an improvement, because corresponds to a system unavailability decrease by 2 orders of

magnitude. Figure 2.4 shows graphically these results for the function unavailability of the top event analyzed.

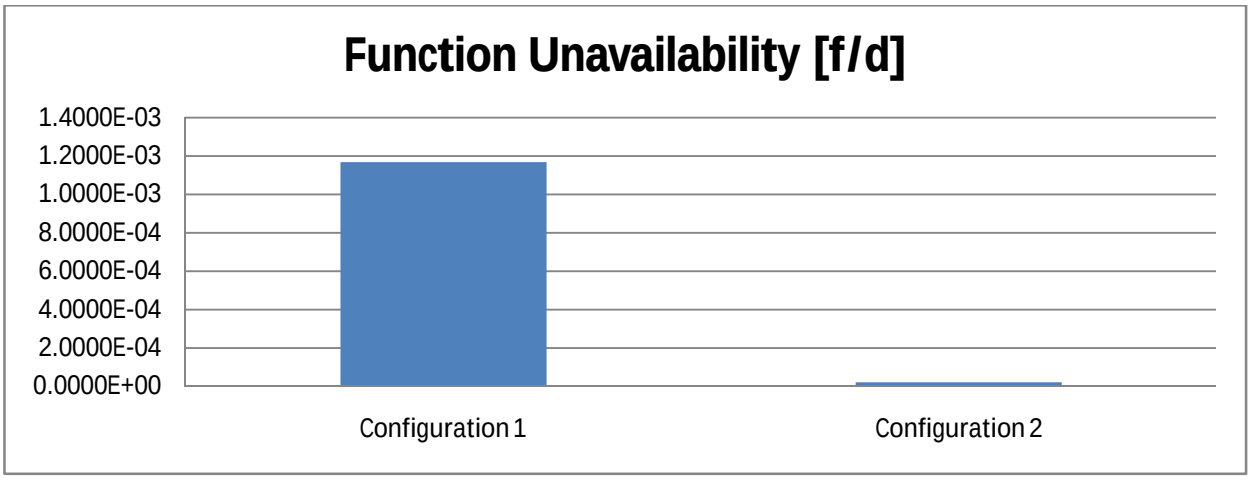


Figure 2.4. Unavailability of the two EWS system configurations

Also, the entropy values obtained for the two partitions resulted confirms that for configuration 2 there is an increase of entropy, i.e. the function unavailability is shared into a larger number of constituents (i.e. scenarios) and therefore into a larger number of causes, too.

The same as the Fault tree method, the IDDA code can give the Minimal Cut Sets (MCS) of the top events analyzed. The number of MCS resulted is the same as the number of scenarios that lead to top event unavailability. As it has been said previously IDDA constituent is a set of successes and failures that cause the Top event, removing the random events that are successful remain in fact the minimal cut set.

Below are presented the first three minimal cut sets resulted for the both system configurations.

System configuration 1

```
Minimal Cut       1]
                     PV7PF    dnOpen     (  11)        1.110000E-03
                                                       ------------
                     Failure Probability    1]        1.110000E-03

Minimal Cut       2]
                     SV41     dnWork     (   7)        5.000000E-03
                     EWSPs.HE Failure    (  80)        6.000000E-03
                                                       ------------
                     Failure Probability    2]        3.000000E-05

Minimal Cut       3]
                     CV49.O   dnOpen     (  12)        1.300000E-05
                                                       ------------
                     Failure Probability    3]        1.300000E-05
```

System configuration 2

```
Minimal Cut      1]
                    CV49.O    dnOpen     (  12)        1.300000E-05
                                                       ------------
                    Failure Probability     1]        1.300000E-05

Minimal Cut      2]
                    SV.7      dnWork     (  10)        5.000000E-03
                    PV107PF   dnOpen     (  59)        1.110000E-03
                                                       ------------
                    Failure Probability     2]        5.550000E-06

Minimal Cut      3]
                    Pre.Sens Mis.Calb    (   2)        3.000000E-02
                    HS41.HE  Failure     (  15)        1.000000E-02
                    EWSPs.HE Failure     (  80)        6.000000E-03
                                                       ------------
                    Failure Probability     3]        1.800000E-06
```

2.4. EWS - "RISK" Analysis

The definition of risk over the years took various forms among the people involved in the risk assessment, but common agreement has been found for the following formula, expressed below:

Risk = Probability of occurrence * Consequence

The present sub-chapter presents some specific capabilities of IDDA code. The purpose is to present a risk analysis in respect to the reparation times of the components of the EWS systems. The analyses consider the two system configurations of the main function that have been analyzed in the previous sub-chapter.

Therefore the analyses are meant to quantify the risk resulted/expected once consequences as reparation times are associated to the components of EWS system.

In case of a CANDU 6 plant transient, EWS system might be requested to mitigate accident consequences. EWS system is a safety support system that could be used over long term periods, i.e. more than 24 hours, so the possibility of components reparation should be considered.

Usually, such analyses are not possible with the existing codes available on the market and used in the probabilistic safety assessments of the nuclear power plants. Currently, some studies were performed on systems, such as spent fuel pool cooling systems, using the Markovian approach, but it cannot handle too many components**.**

The present application considers the reparation of all active components of the EWS system configuration.

The input data that have been used for the analysis are given in Table 2.4.

IDDA Level	Eq. - Failure mode	λ [1/h]	λ [1/d]	T_M [h]	T_i [days]	EF	CoVar	MTTR [h]	Q_M	Source(s)
5	External Large Leak	3.93E-08		24		8.4	0.720	No MTTR for passive equipment.	9.43E-07	[6], [7]
6	PV41MNT		1.E-06			10	0.795		1.E-06	
7	SV41		9.54E-04			8.4	0.720	5	9.54E-04	[6], [7]
8	PV41PF	1.5E-06			672	4.3	0.466	4	5.04E-04	[6], [7]
9	PV7MNT		1.E-06			10	0.795		1.E-06	
10	SV7		9.54E-04			8.4	0.720	5	9.54E-04	[6], [7]
11	PV7PF	1.5E-06			672	4.3	0.466	4	5.04E-04	[6], [7]
12	CV49.O		1.30E-05			8.4	0.720	9	1.30E-05	[6], [7]
15	HS41.HE		1.E-02			10	0.795		1.E-02	
16	HS41	4.6E-07			672	5	0.520	3	1.5E-04	[6], [7]
17	HS7.HE		1.E-02			10	0.795		1.E-02	
18	HS7	4.6E-07			672	5	0.520	3	1.5E-04	[6], [7]
80	EWSPs. HE		6.E-03			10	0.795		6.E-03	[6], [7]
90	P1.MNTC		2.E-02			5	0.520		2.E-02	[6], [7]
105	P1Fs.CCF		8.E-05			5	0.520		8.E-05	
110	P1Fst		2.23E-03			4.7	0.497	150	2.23E-03	[6], [7]
120	P1Fr.CCF		8.4E-05			5	0.520		8.4E-05	
130	P1Frun	4.54E-06		24		3.3	0.375	21	1.08E-04	[6], [7]
140	V9V11CCF		2.47E-06			5	0.520		2.47E-06	
150	V9.O		1.30E-05			8.4	0.720	8	1.30E-05	[6], [7]
160	V10.O		2.5E-03			10	0.795	4	2.5E-03	
170	V45.C		7.E-05			8.4	0.720	6	7.E-05	
180	V44.O		1.30E-			8.4	0.720	6	1.30E-	

			05						05	
190	V47.C		7.E-05			8.4	0.720	6	7.E-05	[6], [7]
260	P2Fs.CCF		8.E-05			5	0.520		8.E-05	
270	P2Fst		2.23E-03			4.7	0.497	150	2.23E-03	
280	P2Fr.CCF		8.4E-05			5	0.520		8.4E-05	
290	P2Frun	4.54E-06		24		3.3	0.375	21	1.08E-04	
300	V11V9CCF		2.47E-06			5	0.520		2.47E-06	
310	V11.O		1.30E-05			8.4	0.720	8	1.30E-05	
320	V12.O		2.5E-03			10	0.795	4	2.5E-03	

Table 2.4 Input data considered for unavailability and risk analyses

For calculating the component unavailability in case there is no test interval considered, the following formula has been applied:

$$Q_m = \lambda * T_M$$

where:

Q_m – average unavailability

λ – component failure rate

T_M – mission time

The components that have been considered subjected to testing have applied the following formula for quantification of the component unavailability:

$$Q_m = \lambda * T_i/2$$

where:

Q_m – average unavailability

λ – component failure rate

T_i – test interval

For the redundant components, group of two, an approximation method has been used for the quantitative evaluation of CCFs. The method used was the β factor method.

In this method, the likelihood of the CCF is evaluated in relation to the random failure rate for the component. A β factor is estimated such that β% of the failure rate is attributed to the CCF and (1- β) % to the random failure rate of the component. The beta value used was β = 0.1

2.4.1 Complementary cumulative density function (CCDF)

The *complementary cumulative density function* is called also the "Risk curve". The IDDA code through the use of the different sets of commands and following the consideration of associated consequences, such reparation times, economical costs or any type of consequence can give in output the CCDF that characterizes the partition, in particular EWS system configurations. CCDF is a feature of IDDA and is a common used tool in the risk assessment.

In particular, for the EWS risk assessment, the CCDF consists of plots on log-log graph that indicates the probability versus consequence.

The knowledge of the CCDF allows the risk analyst to see what is the probability to have a certain consequence either below or above a given limit, and moreover to consider if the probability is acceptable or not acceptable.

2.4.1.1 CCDF – Theoretical considerations

In probability theory and statistics, the cumulative distribution function (CDF) describes the probability that a real-valued random variable X with a given probability distribution will be found at a value less than or equal to x.

For every real number x, the cumulative distribution function of a real-valued random variable X is given by:

$$F_X(x) = \mathrm{P}(X \leq x),$$

where:

The right-hand side represents the probability that the random variable X takes on a value less than or equal to x.

The CDF of a continuous random variable X can be defined in terms of its probability density function f as follows:

$$F(x) = \int_{-\infty}^{x} f(t)\,dt.$$

Complementary cumulative distribution function – sometimes it is useful to study the opposite question and ask how often the random variable is above a particular level. This is called the complementary cumulative distribution function (CCDF) or simply the tail distribution or exceedance, and is defined as:

$$\bar{F}(x) = \mathrm{P}(X > x) = 1 - F(x).$$

Area to the right of the x = b line is: G_X (b), this is the probability that X is greater than b.

Below, Figure 2.5 shows the graphical meaning of a complementary cumulative distribution function.

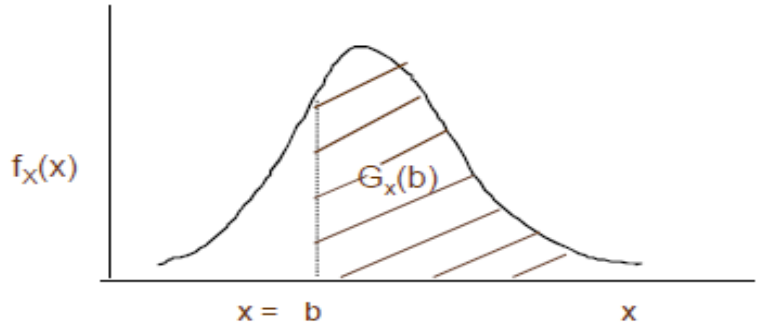


Figure 2.5 Complementary cumulative distribution function

2.4.1.2 Complementary cumulative distribution functions (CCDF) results

An ordering by decreasing consequence allows getting the Complementary Cumulative Distribution Function (CCDF) of that quantity that is the consequence (e.g. reparation times) by progressively cumulating constituent probabilities. In fact, it gives for each consequence value the probability of having a consequence not lower than this value. The complementary cumulative distribution function resulted after the consideration of all input data for the first system configuration is shown in the Figure 2.6.

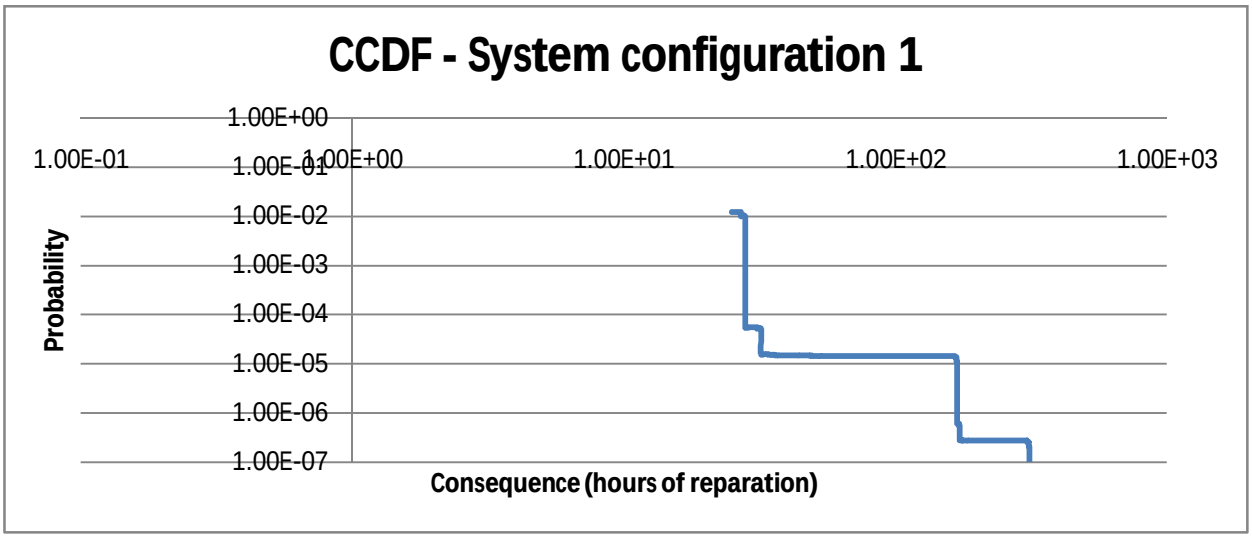


Figure 2.6. CCDF resulted for the first EWS system configuration

As it has been said before the CCDF helps the risk analyst to see what could be the probability to have a certain consequence. For instance, the probability to have a high consequence like 100 hours unavailability due to equipment reparations is very low and on the reverse when the probability is quite high the consequence is low.

The compared CCDFs obtained for both system configurations are shown below in Figure 2.7.

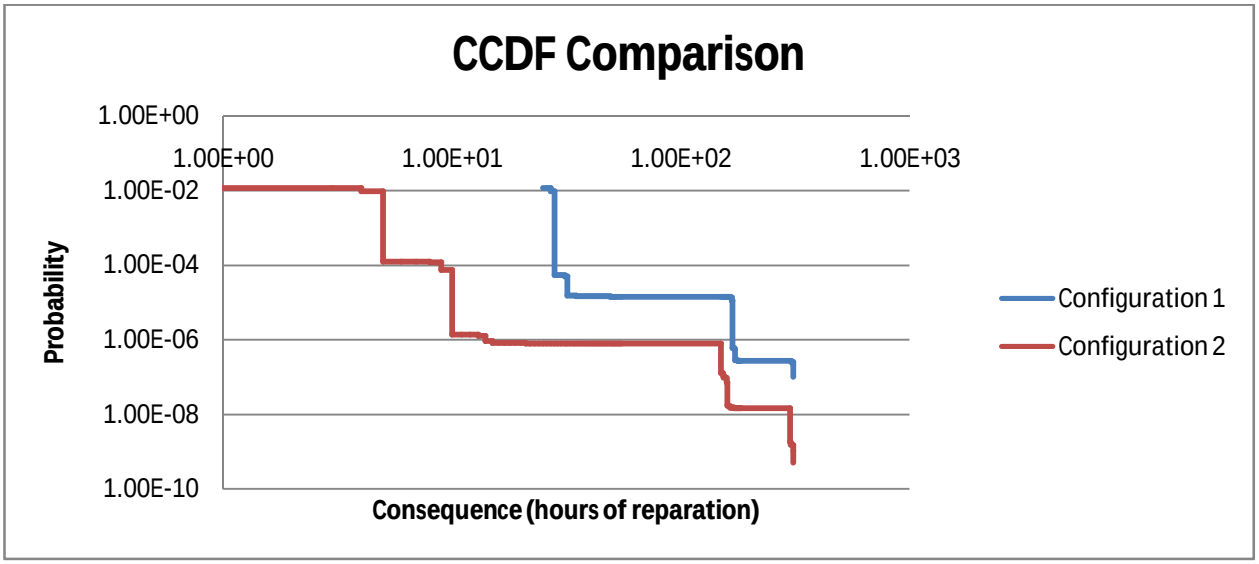


Figure 2.7. CCDFs comparison for the both EWS system configurations

The CCDF comparison of the two system configuration shows that the system configuration with redundancy for the two pneumatic valves presents lower consequences and lower probabilities; therefore the improvement of system configuration is worthy and brings evident benefits.

2.4.1.3 Identification of the critical aleatory events

Another feature of IDDA code is that it allows the risk analyst to identify the critical aleatory events that have significant contribution to the total risk within the considered partition.

Once the consequence is given (i.e. associated) to the basic events, whatever they are, either different type of consequence or different type of basic event (e.g. equipment, human action) the code generates the results in respect of the interested issue. The most significant aleatory events that contribute to the total risk could be presented in the form of single failures, the same as MCS of one order or in combination with other basic events failures, again the same as the MCS of great orders. As would be expected the combination of multiple basic events failure has less contribution as the failure of a single basic event.

For instance, for the two system configurations proposed, once the reparation times have been given to the code, it was of special interest to identify which are the critical components that have the most significant contribution to the total “risk”.

The results obtained for the first system configuration are shown below in the Figure 2.8.

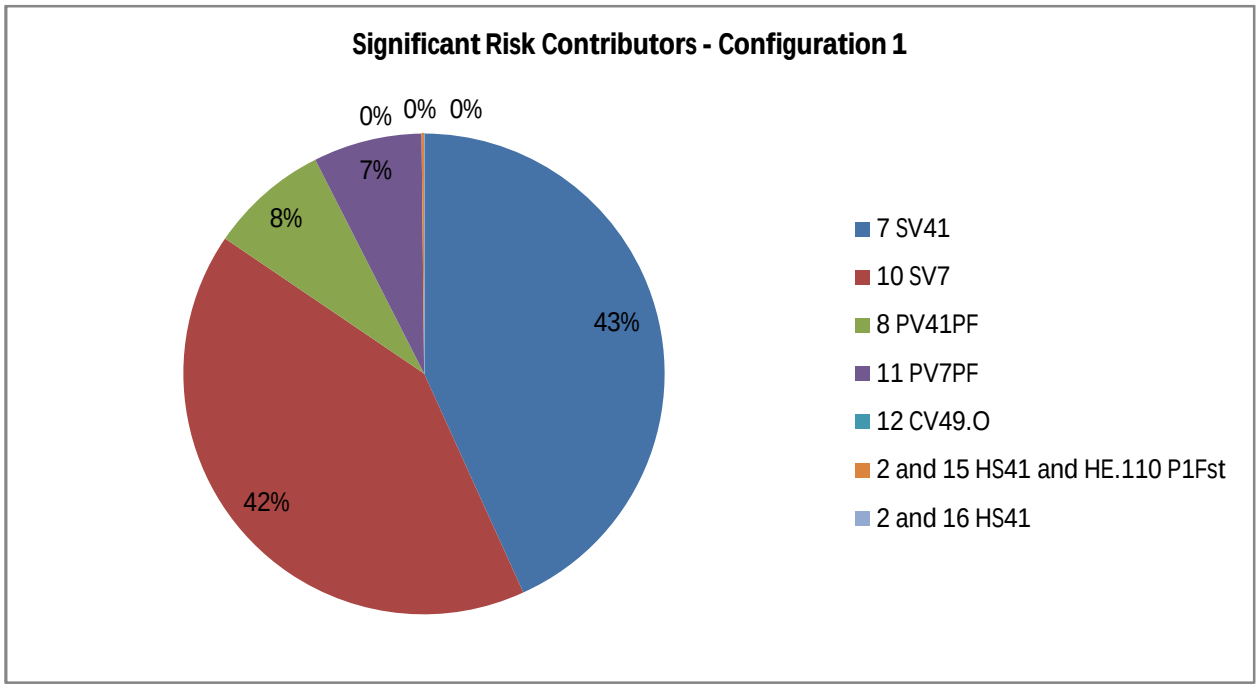


Figure 2.8 Significant risk contributors for EWS Configuration 1

The IDDA code output has the following format, shown below. In particular, the two most important basic events failure that have significant risk contribution are presented. The output file lists the causes that contribute to the risk in the decreased order. The output file registers the mnemonic that reminds the name of basic event, the level assigned in the input file, the value with which contributes to the risk, the percentual contribution to the total risk and the number of scenarios involved with the failure of the specific basic event(s); moreover they are presented in the decreased order of their contribution to the risk, see below Figure 2.9.

```
FAILURES          RISK            RISK %          MIN. CUT.

   7 SV41      dnWork
----------------------

                2.601E-02      4.31221E+01 %         2
                               4.31221E+01 %      ----
   8,    98,    36,     5,    35,    22,    81,    46,    12,    30,
  50,    16,    45,   349,   108,   346,   296,    72,   452,    14,
 375,    71,   228,    41,    65,   331,   141,   385,    38,   103,
 252,    27,   169,   373,    75,    89,   151,   104,   263,    37,
  66,   212,   262,    88,   102,   430,    17,   168,   208,   348,
 191,   199,   214,   347,    86,   106,   243,   286,   303,   132,
 147,   211,   352,   146,   224,   236,   239,    55,   291,   345,
 110,   164,   152,   282,    68,   145,   578,   618,   520,   614,
 305,   356,   218,   355,   445,   489,   367,   487,   561,   602,
 490,   519,   598,   554,   440,   371,   552,   418,   284,   416,
       Numb. of Involved Constit. :  101          (    1 -  101)

  10 SV7       dnWork
----------------------

                2.487E-02      4.12227E+01 %         1
                               8.43448E+01 %      ----
   6,    19,    28,    15,    44,    48,    74,    39,    96, /
Numb. of Involved Constit. :   10          (  102 -  111)


   8 PV41PF    dnOpen
----------------------
```

Figure 2.9 IDDA output – risk contribution for the failure of the first two significant basic events of EWS configuration 1

Again for comparison purpose, it has been analyzed also the system configuration 2 and its critical aleatory events that lead to risk, presented below in Figure 2.10.

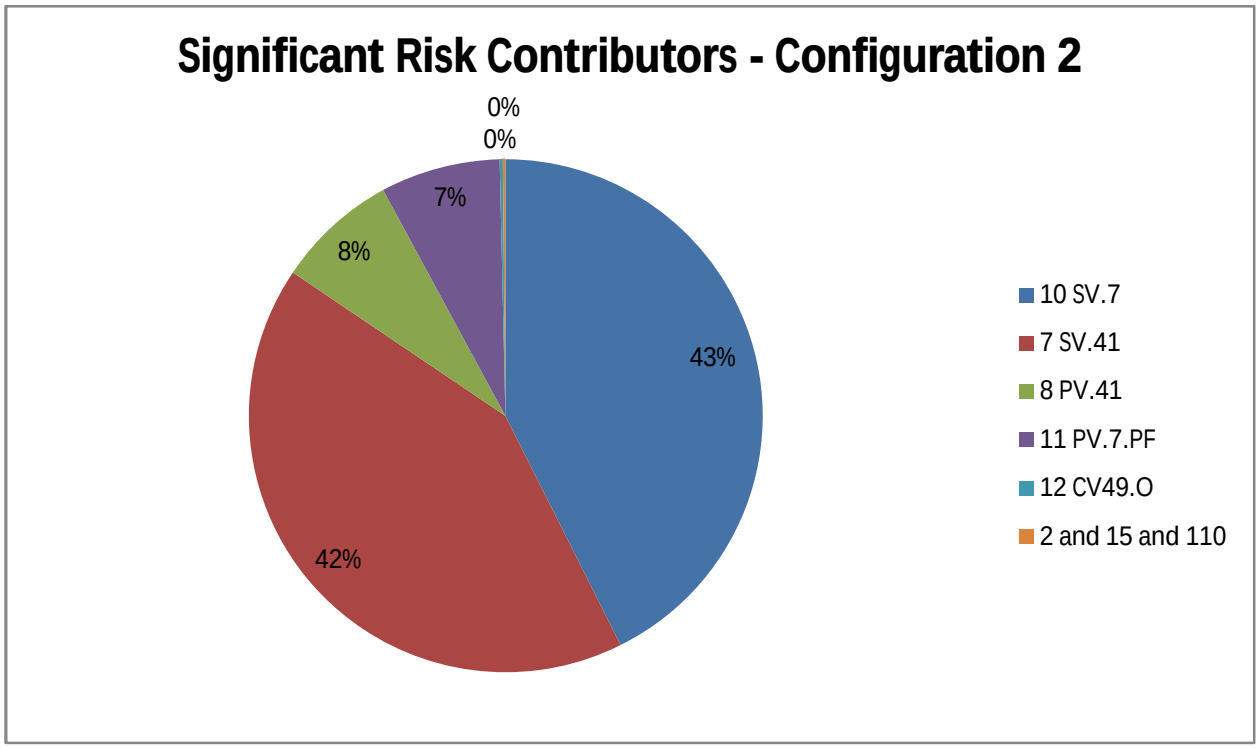


Figure 2.10. Significant risk contributors for EWS Configuration 2

Below in Figure 2.11 is shown the IDDA output for the failure of the first two significant basic events.

```
FAILURES          RISK              RISK %          MIN. CUT.

  10 SV.7      dnWork
----------------------

                2.499E-02      4.25809E+01 %         2
                               4.25809E+01 %
   5,    94,     6,    13,    40,    24,    33,    91,   246,   322,
 557,    57,    79,    44,   127,   122,   166,   113,   259,   651,
 747,   612,   931, /
Numb. of Involved Constit. :   24           (    1 -   24)
```

```
   7 SV.41     dnWork
----------------------

                2.455E-02      4.18248E+01 %         1
                               8.44057E+01 %      ----
   7,    15,    95,     8,    17,    39,    37,   248,    52,    99,
  23,   329,    98,   147,   245,    30,    75,   321,    32,   146,
 211,   556,    45,   101,   134,    41,    46,   129,   282,    69,
  90,   190,    61,   137,   187,    48,   130,   128,   195,    73,
 185,   842,   306,   840,   728,   969,   208,   393,   652,  1128,
  49,   746,   936,   966,   207,   559,   611,   846,   126,   171,
 197,   267,   808,   930,  1256,    78,   226,   375,   947,  1077,
 119,   153,   266,   284,   614,   670,    97,   178,   232,   251,
 344,   441,   932,   938,   210,   260,   301,   399,   453,  1093,
 169,   215,   288,   362,   663,   737,   115,   138,   198,   426,
 532,   543,   659,  1071,   258,   272,   281,   339,   486,  1059,
  58,   365,   442,   536,   783,   861,   162,   254,   494,   503,
 546,   644,   777,   862,   253,   300,   333,   361,   600,   713,
 745,  1187,    85,   345,   390,   534,   540,   636,   875,   988,
 389,   553,   589,   591,   598,   602,   650,   989,   152,   154,
 323,   379,   715,   722,   833,   858,   863,   217,   303,   430,
 434,   470,   640,   999,   395,   428,   469,   661,   695,   708,
 711,   189,   214,   219,   838,   984,   292,   382,   385,   518,
 401,   511,   025,   241,   463,  1551,  1600,  1354,  1604,  1001,
1683,  1137,  1815,   773,  1486,  1488,   915,  1802,   577,  1139,
 912,  1267,   318,   898,  1598,   408,  1035,   681,   688,  1142,
1033,  1280,   409,   656,   925,   499,   761,  1277,  1500,   496,
 596,   805,  1116,  1270,  1626,   585,   699,  1283,  1401,   478,
 764,  1046,  1056,  1337,  1615,   766,   883,   928,  1397,  1475,
1613,   593,   700,  1064,  1120,  1232,  1740,   690,   813,   923,
1406,  1408,  1463,   572,   770,  1061,  1174,  1457,  1728,   707,
 887,   896,  1065,  1586,  1053,  1190,  1240,  1244,   433,  1048,
1522,  1571,   515,   900,  1183,   819,   826,  1023,  1171,  1374,
 516,   623,   953,  1747,  1853,  1552,  2075,  1678,  1540,  1855,
1856,  1944,  1686,  2131,   974,  1794,  1105,  1667,   762,  1461,
1947,   893,   753,  1106,  1119,  1203,  1221,  1323,   880,  1179,
1563,  1013,  1343,  1520,   873,  1465,  1135,  1234,  1327,  1799,
1261,  1441,  1123,  1311,  1681,  1467,  1477,  1645,  1796,  1503,
1573,  2032,  1259,  1610,  1885,  1383,  1479,  1526,  1242,  1651,
1797,  1800,  1336,  1583,  1888,  1933,  1450,  1618,  2090,  1121,
1315,  1724,  1237,  1590,  1652,  1657,   922,  1576,  1758,  1891,
1043,  1455,  2009,   895,  1557,  1238,  1245,  1437,  1368,  1767,
1050,  1697,  1162,  1021,  1375,  2111,  2172,  2106,  2241,  2173,
2218,  2167,  2267,  1532,  1665,  1521,  1852,  1658,  1774,  1642,
1938,  1860,  1954,  1848,  2077,  2081,  1952,  2144,  2022,  2072,

 1936,  2221,  2135,  1993,  2061,  2145,  1986,  2191,  2127,  2166,
 2248,  1674,  1780,  2062,  1654,  2118,  1935,  2053,  2211,  1783,
 1873,  1761,  2012,  /
 Numb. of Involved Constit. :  424          (   25 -  448)
```

Figure 2.11 IDDA output – risk contribution for the failure of the first two significant basic events.

The risk results obtained for both system configurations show the importance of the solenoid valves that actuate the pneumatic valves, and also the importance of the pneumatic valves in the system configuration for ensuring the water supply to the secondary side of the steam generators. The results also highlight the importance of the check valve that is before the entrance to the steam generator. The results are expectable due to the fact that the components that proved to be important for the risk belong to the common water header before the water supply is split.The difference registered between the two system configurations in terms of risk is that the number of scenarios involved is bigger for the system configuration 2, that is due to the bigger partition number generated once the redundancy has been considered.

However in this mode the risk analyst is provided with the necessary tools and information for a complete “risk” analysis that could be a very useful input for the decision making process. The analyst is provided with the necessary information in regard to the random events on which to intervene with priority in order to decrease the risk. It should be reminded that the product probability by consequence in not the risk (in decision sense), it’s simply the contribution to the expected consequence value. In fact it lacks the utility factor that changes the expected consequence into decision risk. Only by considering the utility factor the expected value could be effectively transferred in decisional parameter, risk.

2.5. Conclusions

The set of codes that constitutes IDDA analysis methodology is a very articulate system that has the right answers to almost all analysis requests and needs. The methodology has been designed for complex situations and actually in those the code shows its real potentialities.

These types of results have a great importance to orient the course of the analysis or to be considered as valuable inputs for the decision making process.

The present applications have proved only partly the potentialities of the code, mainly the most important features, but there are still features that were not presented due to the lack of space and scope of the applications.

Other IDDA potentialities that are worthy to be mentioned are the following:

- Evaluation of weight of uncertainties
- Single component reliability vs. time
- Availability of reparable components vs. time
- CCDF for system/component unavailability
- Out of service times

The scope of applications was only to show some of the potentialities of the IDDA methodology in the given framework of the input data limits, and not to underline and weaknesses of any existing risk assessment methodology. Due to the fact there is not an official input data in regard to system operation and exact configuration, no specific conclusions could be withdrawn in respect to the EWS system or CANDU 6 plant design.

2.6. References

[1] Introduction to the Qinshan Phase III CANDU Nuclear Power Plant, Zhang Yanfa, B.A. Shalaby, Nuclear Power Engineering Magazine # 06, 1999

[2] National Report on the Implementation of the Stress Tests, CNCAN, Romania, 2011

[3] Incorporating Ageing Effects into System Reliability Models, Alexandru Stoian, Ageing PSA Network, Bucharest, Romania, 2006

[4] Integrated Decision Dynamic Analysis, Marius Lontos, Marino Mazzini, Open PSA Initiative, IAEA, 2007

[5] Integrated Dynamic Decision Analysis (IDDA) user manual, DOS-F77 FORTRAN Version, Remo Galvagni, 2007

[6] Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants, NUREG/CR-6928, 2007

[7] Component reliability data for use in Probabilistic Safety Assessment, IAEA-TECDOC-478, 1988

CHAPTER 3

3. 1 Introduction

Chapter 3 represents the core applications of the present work. The applications purpose is the coupling between the logic probabilistics of the system or plant and associated phenomenology of primary heat transport system of a generic CANDU 6 NPP.

The first application consists in the coupling between the logic-probabilistic model of EWS system and the associated phenomenology of primary heat transport system of CANDU 6 NPP. The considered plant transient is the total Loss of Main Feed-water with or without the coincident failure of the Emergency Water Supply System.

The second application is considering the CANDU 6 Station Blackout as plant transient, moreover the loss of all AC power sources existing on the site. The transient scenarios development considers the possibility to recover the offsite grid and the use of mobile diesel generators in order to mitigate the accident consequences. The purpose of the analysis is to challenge the plant design and response and to check if the plant conditions of a severe accident are reached. The plant response is challenged for short and long periods of time.

The IDDA code allows interfacing the logic-probabilistic model of the system with the plant response in time, therefore with the evolution in time of the plant process variables.

This allows raising sequences of possible events related in cause-consequence reasoning, each one giving place to a scenario with its development and its consequences. Therefore this allows acquiring the knowledge not only of which sequences of events are taking place, but also of the real environment in which they are taking place. Associating the system sequences that lead to system unavailability on demand with the resulting phenomenology proved to be a useful tool for the decision making process, both in the design phase and for the entire power plant life time.

3.2 CANDU 6 Design - Safety philosophy

The safety philosophy of CANDU reactors, based upon the principle of defense-in-depth, employs redundancy (i.e. using at least two components or systems for a given function), diversity (i.e. using two physically or functionally different means for a given function), separation (i.e. using barriers and/or distance to separate components or systems for a given function), and protection (seismically and environmentally qualifying all safety systems, equipment, and structures).

An important aspect of implementing defense-in-depth in the CANDU 6 design is the provision of a series of physical barriers to confine radioactive material at specified locations. As usual, in CANDU 6 design these barriers are the fuel matrix, the fuel sheath (clad), the Heat Transport

System (HTS), and the Containment. An additional administrative barrier is the exclusion area boundary, [1].

The following points are briefly listing the key safety features[2] of CANDU 6 design:

- CANDU 6 reactors have two separate, redundant fail-safe shutdown systems, (one seismically qualified); also the secondary control room is seismically qualified;

- Large volume of cooling water is contained in the dousing tank of the reactor building (approx. 3000 tonnes), ready to suppress the containment pressure or to cool by gravity the reactor core;

- CANDU 6 reactor core includes a large volume of low-temperature, low pressure moderator water (approx 260 tonnes), which provides an inherent backup heat sink. The large thermal capacity of this water and the surrounding shielding vault water (approx 600 tonnes) provides an interim heat sink.

- Feedwater shutdown cooling and moderator systems operate under CLASS IV and CLASS III power (independent diesel generators);

- If CLASS IV and CLASS III power are unavailable, seismically qualified EPS (Emergency Power Supply) will be started, in this case, pumped Emergency Water Supply (EWS) operating under EPS can ensure long term fuel cooling;

- Following total loss of off-site (CLASS IV) and on-site (CLASS III) power, the steam generator heat sink is maintained by make-up to steam generators by gravity from the dousing tank (EWS supply by gravity from dousing tank), after steam generator rapid cooldown;

- The natural uranium fuel bundles of CANDU 6 are gradually discharged during reactor operation and are stored in the bay for about 6 years, before they can be moved to passive air-cooled dry storage.

3.3 CANDU 6 NPP – Total Loss of Main Feedwater (TLOMFW) transient

3.3.1 Total Loss of Main Feedwater (TLOMFW) transient description

The Total Loss of Main Feedwater is an internal event plant transient that corresponds to a failure of the secondary side plant circuits. Initial Event (IE) can be a loss of the three main feed water pump trains (including valves), but conservatively is considered that also the auxiliary feedwater pump is lost.

[2] http://enformable.com/2011/11/nuclear-electrica-cernavoda-nuclear-candu-6/

The cause of loss could be due to loss of power supply to the main feedwater pumps, or due to a pipe break. The break could be located in the feedwater header. The break is conservatively assumed to be symmetric and consequently affects all steam generators in the same manner.

Table 3.1, presents the plant response associated to the accident of Total Loss of Main Feedwater (TLOMFW)

Table 3.1 Plant response associated to the TLOMFW accident

Plant response	**Description**
1	All the systems of the power plant are available. Immediately after initial occurrence, due to pressure drop of the feedwater flow a reactor trip occurs. Following the reactor trip, the heat rate transfer to secondary side decreases and this causes a drop in secondary circuit pressure. The turbine is isolated by the closure of the governor valves in the attempt to maintain constant boiler pressure. The main feedwater pumps are also tripped immediately after IE occurrence, on high motor current due to the excessive flow. Auxiliary Feedwater pump will automatically start but it cannot supply sufficient water to the steam generators because a part of feedwater flow will be lost through the break. Auxiliary Feedwater pump will trip on high pump motor current due to the excessive flow. Boiler pressure is controlled by using condenser steam discharge valves (CSDV's) or atmospheric steam discharge valves (ASDVs) to relief steam and boiler level by Boiler Level Control (BPC) program. If ASDV's or CSDV's are unavailable then MSSV's will be used for steam relief. Due to the feedwater supply failure to the SG's, the operator should initiate cooldown process. The cooldown process can be made in two ways: with BPC and SG's until the SG's level drop below -8 meters and after that continuing with SDCS down to 54 °C or directly with SDCS from 260 °C down to 54 °C. When the PHTS temperature drops below 90 °C, the PHTS can be depressurized from 6.5 MPa to 1.0 MPa. EWS short term system is blocked every time when SDCS system is brought into service. As long as SDCS is available, the plant remains in a stable end state (6.5 MPa and 125 °C or 1.0 MPa and 54 °C).
2	If SDCS system is unavailable, the operator must initiate SG's depressurization in order to bring into service low pressure water supply systems to SG's: Boiler Make-up Water (EWS short term) or pumped Emergency Water Supply (EWS

	long term) system. The operator will open 8 out of 16 main steam safety valves (MSSV's) and when the steam generators pressure decrease below 345 kPa, the water from the dousing tank will feed by gravity the SG's. If the operator does not depressurize the boilers, then boiler auto-depressurization is automatically initiated. Auto-depressurization will be enabled if the level in at least two steam generators will be below -2.6 m for 20 consecutive minutes and is conditioned by the feedwater header pressure below 4.93 MPa. If the EWS short term system fails, the operator will initiate EWS pumped (i.e. long term water supply) system to provide water supply to the SG's. The end stable state for this sequence is at 120 °C.
3	In case EWS systems (i.e. short term and long term water supplies) fail and concomitant with the feedwater supply lost, and without SDCS, then the plant end state will be core damage.
4	In case that secondary side water make up cannot be ensured, then primary water makeup is considered via emergency core cooling systems (ECCS). If ECCS make-up to primary circuit fails, then the operator initiates the EWS system to primary in order to ensure full primary heat transport system inventory. The same number of MSSV's (8 out of 16, or 4 out of 8 for one loop reactor) is required to depressurize the primary circuit that further allows the EWS make-up.
5	Without any make-up to primary circuit, the primary circulation is ensured by two-phase thermosyphoning. This heat removal mechanism requires two SG's per loop available and supplied continuously with low pressure feedwater (i.e. emergency water supply - EWS). As long as both SG's per loop are effective in heat removal the plant will be into a stable end state.

3.3.2 Thermal-hydraulic model assumptions

The main assumptions that stay at the basis of the thermal-hydraulic model are the following:

- Only one loop out of two, half reactor is modeled;
- The Shutdown Cooling System (SDCS) is not credited as available, therefore it is not modeled in the thermal-hydraulic model;
- The Degasser/Condenser (DC) is not modeled. The PHTS inventory discharged from Pressurizer through the Liquid Relief Valves to the Degasser/Condenser (DC) tank is credited as successful;

- The Auxiliary Feedwater pump operation is neither credited, nor modeled in the thermal-hydraulic model.
- The ECCS system to provide make-up to PHTS is not credited, nor modeled in the thermal-hydraulic model;
- CLASS IV and CLASS III power are credited as available;
- The moderator is not credited as ultimate heat sink, therefore it is not modeled in the thermal-hydraulic model.
- The Atmospheric Steam Discharge Valves (ASDV) and Condenser Steam Discharge Valve (CSDV) are considered conservatively as unavailable.
- The 2 SGs of the loop are credited as available, therefore no need for EWS make-up to the PHTS.

3.3.3 RELAP 5 – CANDU 6 thermal-hydraulic model description

Four half circuits complete the two figure of 8 that are designed for heat removal and steam generation. A half circuit contains a main circulation pump and a steam generator. The main circulation pump takes heavy water that has passed through the steam generator, pumps it through the inlet headers, the reactor core and the outlet headers, and back into the steam generator. Heavy water flows through the steam generators and transfer heat to water to form steam. The steam flows out of the top of the steam generator to the turbines. The inlet headers distributes the heavy water to individual fuel channels and the outlet header collects heavy water from the individual fuel channels and directs it to the steam generator, [2].

A typical CANDU heat transport system is shown in Figure 3.1 below.

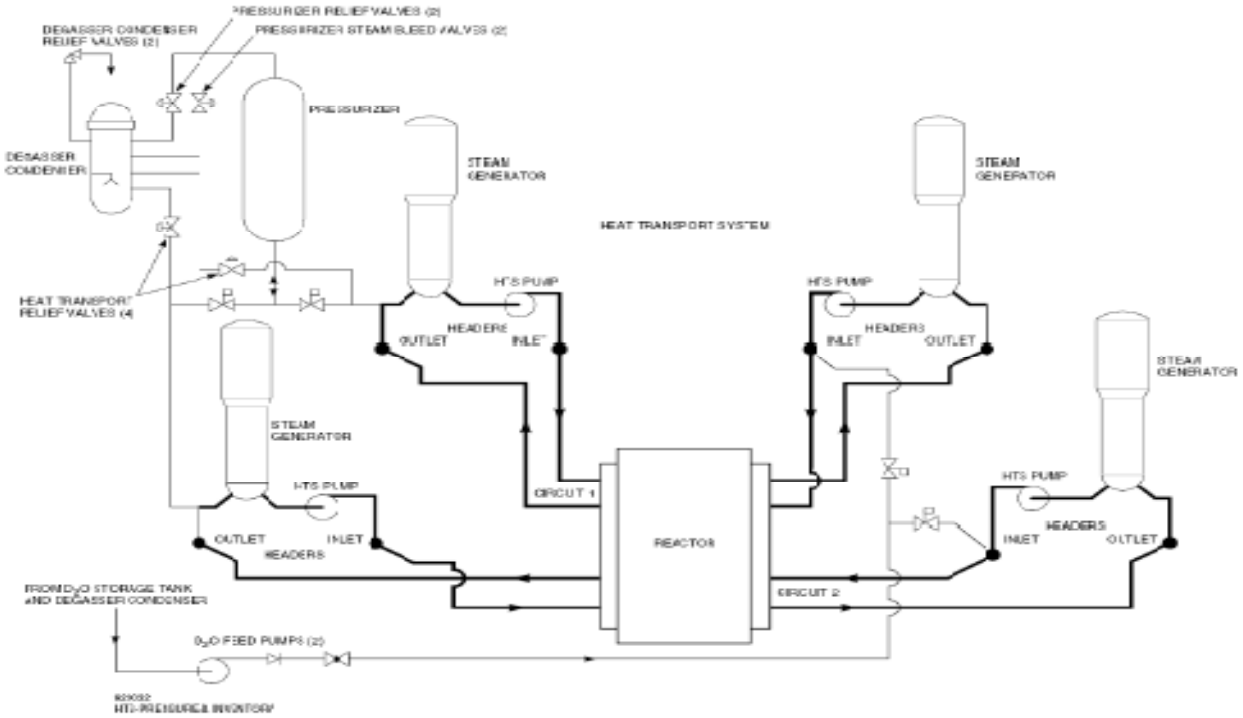


Figure 3.1. CANDU 6 Primary Heat transport system and pressure inventory control system

The RELAP5/Mod.3.3 input model of the CANDU 6 reactor design has been developed independently in the frame of the present work. The geometrical and process data correspond to a full vertical-scale representation of a CANDU 6 heat transport system.

The input model is designed so that reactor typical conditions, such as fluid mass flux, pressure and enthalpy, can be achieved in the primary and secondary side for both forced and natural circulation. The thermal-hydraulic model considers half of reactor, only one loop of the "figure-of-eight" geometry of a CANDU 6 design. The model considers one horizontal channel per pass and a 1:1 scaling of the vertical elevations throughout the loop.

Each six-meter-long fuel channel is connected to the end-fitting, i.e. inlet and outlet feeders. One fuel channel is simulating 95 fuel channels, actually one quarter from the total number of fuel channels that pass the Calandria vessel.

The steam generators are scaled approximately 1:1 with typical CANDU steam generators, in terms of tube diameter, mass and heat fluxes. The secondary-sides of the steam generators contain an internal pre-heater and an external down-comer. Primary fluid circulation is provided by two centrifugal pumps. These deliver full reactor typical head (about 210 m) at flow rates similar to a single reactor channel. Primary circuit pressure is maintained by the pressuriser**.**

The thermal-hydraulic model is equipped with the Emergency Water System (EWS) that provides water make-up to the secondary side of steam generators under postulated conditions of consequent failure of main and auxiliary feedwater systems. The EWS system is actuated by the secondary side pressure with the water injection when pressure drops below a predetermined value, i.e. 345 kPa.

The half loop modeled is made of the following main components:

- 2 steam generators
- 2 reactor coolant pumps
- 2 horizontal fuel channels
- 2 reactor inlet headers
- 2 reactor outlet headers
- Inlet feeders
- Outlet feeders

The thermal-hydraulic RELAP5 nodalization has been achieved through a number of volumes and inter-connecting junctions, valves, heat slabs and component-specific models such as pump, separator, etc.

The system controls are modeled through trip cards, which accept logical inputs based on time, pressure and other thermal-hydraulic parameters. The power trip, steam generators depressurization, EWS pump activation, etc., are controlled also through the trip cards.

In the following it is presented the modeling of main components of the primary and secondary circuits, such as:

- *Header, Feeder and Fuel Channel Modeling*

Each fuel channel is discretised into 12 axial volumes to obtain the axial distribution of thermal-hydraulic parameters. Each fuel element that transfers heat to the coolant, is modeled with a RELAP5 specific heat generating heat structure component. The fuel pins are combined into a single fuel pin heat structure maintaining the surface area, mass and equivalent heated perimeter corresponding to the 95 fuel channels simulated. The power ramp down during the transient is given in a tabular form in the code.

The heat structure that models the fuel element is at the external side in contact with the primary coolant. Moreover another heat structure has been put in place to model the pressure tube that is in contact at internal side with the primary coolant and at the external side directly with the moderator – heavy water that has imposed a constant water temperature of 70 °C.

The present thermal-hydraulic model of the fuel channel did not consider the modeling neither of calandria tube and, consequently, nor of the annulus gas that is between the pressure tube and the calandria tube. Thus the simulation of pressure tube drop on the calandria tube when the pressure tube heat-up is not modeled, fact that could lead to optimistic temperature values for the primary coolant, fuel sheath and moderator.

However, the phenomenon, i.e. pressure tube deformation takes place under certain postulated conditions, such as LOCAs with concomitant loss of ECCS when the complete voiding had occurred. The transients studied in the present work do not present these conditions (at least in the considered time period for the Station Black-out) and consequently the phenomenon is disregarded.

The inlet and outlet feeders nodalised have 11 volumes maintaining the pipe length and elevation. In the setup, the intake and off-take branches such as reactor coolant pump injection, feeder connection, etc., are connected to the header at different axial locations. Accordingly the main header is discretised into four axial volumes.

- *Steam Generator Modeling*

The steam generator U-Tubes are segregated into ten volumes including inlet and outlet plenum volumes. The U-Tube volumes are attached with heat slabs, forming the thermal linkage between the primary and secondary system. The secondary system consists of riser, drum and downcomer volumes.

A RELAP5 specific separator component, attached with the drum volume, is used to separate out steam and water.

The drum volume is modeled using a pipe component. The U-Tube heat slabs are connected to the two volumes of the riser portion. One single volume downcomer connects the drum inlet to the secondary riser inlet.

The main feedwater from a time-dependent volume is injected into the riser portion and mixes with the saturated water from the downcomer. It picks up heat from the U-tubes, converts into a two-phase mixture and rises in the riser volume. At the exit of the riser this two-phase mixture enters the separator volume. The steam from the separator moves to the upper portion of the drum volume and the saturated liquid falls back into the lower portion of the drum volume. The bottom volume of the drum is connected to the downcomer. The feed flow and temperature are given as time dependent boundary conditions.

- *Primary Heat Transport Pump Modeling*

The primary heat transport pump is modeled using the RELAP5 in-built Bingham Pump characteristics. The rated flow, speed and head are provided.

- *Emergency Water Supply/Auxiliary Feedwater System Modeling*

The emergency water and auxiliary feedwater system the same as the main feedwater system is considered as being a time-dependent volume. The emergency/auxiliary water flow and temperature are given as time dependent boundary conditions.

The EWS pumps are simulated using time-dependent junctions whose flow characteristics are given as functions of downstream discharge pressure.

- *Pressurizer Modeling*

The pressuriser is made of a time dependent volume and a pipe discretized in 9 volumes. The connection between the pressuriser and pipe is done via a trip valve, which should close after steady state

- *Calandria (Moderator) Modeling*

The Calandria, actually the moderator is modeled through the use of heat structures modules. The temperatures are given for the left and right sides. One external side to the fuel sheath (represented also with heat structures) is the moderator temperature (70 Celsius degrees) that keeps constant, and one internal side that cools down the fuel sheath temperature. Therefore the moderator temperature follows the trend of the fuel sheath temperature, but acts as a heat sink.

The main purpose of heavy water moderator in calandria vessel is to provide a mean to slow down high energy fission neutrons to the appropriate thermal energy level to promote further nuclear fission. Moreover the moderator removes the heat that is continuously generated in the moderator as a result of heat production associated with neutron moderation and gamma ray absorption processes, transfers the heat from the pressure tubes across the annular gap to the calandria tubes, and lastly transfers the heat from reactor structures.

The moderator thus constitutes a distributed, low pressure emergency heat sink surrounding each fuel channel, [3].

- *Others Modeling*

The steam produced in the steam generators can be directed either to the turbine, modeled by a time dependent volume through a valve connection, either can be released to the atmosphere through a valve connection that has the same flow area as 4 main steam safety valves. The steam released through the main steam safety valves is discharged in a time dependent volume.

The nominal initial conditions for the thermal-hydraulic model and the temperature and pressure distributions along the circuit are given in Table 3.2.

Main Parameters	Thermal-hydraulic model parameters
Reactor headers	
Reactor Inlet Header temperature [K]	539.15
Reactor Outlet Header temperature [K]	583.15
Reactor Inlet Header pressure [bar]	113.5
Reactor Outlet Header pressure [bar]	99.9
Steam Generators	
SG inlet pressure [bar]	97.4
SG inlet temperature [K]	582.15
SG inlet enthalpy [kJ/kg]	1395
SG outlet pressure [bar]	94.7
SG outlet temperature [K]	539.15
SG outlet enthalpy [kJ/kg]	1163
Heat transferred to secondary side/SG [MWth]	516
SG steam flowrate [kg/s]	254
Pressure at drum nozzle [bar]	47
Temperature at drum nozzle [K]	533.15
Enthalpy [kJ/kg]	2808
Quality at drum exit [%]	99.75
Pressure at turbine [bar]	45.5
Primary pump	
Suction pressure [bar]	95.4
Discharge pressure [bar]	113.4
Flowrate [kg/s]	2224
Head [m]	210
Main feedwater	
Temperature [K]	460.15
Pressure [bar]	48
Enthalpy [kJ/kg]	794
Flowrate [kg/s]	254
Emergency water	

Emergency water temperature [K]	305.15
Emergency water pumped pressure [bar]	10
Emergency water dousing tank pressure [bar]	4.8

Table 3.2 Main input data used for the thermal-hydraulic model

The RELAP5 model, that simulates the CANDU 6 power plant transient, is supposed to be in the following conditions and generates the resulting events sequence, see below Table 3. In order to see the trends of PHTS temperature and SG Downcomer Level, the total time for which the transients have been simulated is 5000 seconds.

By applying the energy balance equation (see below) between the primary and secondary side process parameters resulted following the steady state conditions, confirms that the system is well balanced and furthermore the different accident situations can be simulated.

$$Q_{\text{primary flowrate}} * (H_{\text{SG outlet}} - H_{\text{SG inlet}}) = Q_{\text{secondary flowrate}} * (H_{\text{steam}} - H_{\text{feedwater}})$$

Table 3.3, presents the comparison between the parameters obtained in the frame of the present work and the operational parameters for Cernavoda unit 2.

	Primary side		Secondary side		
THERMAL BALANCE	**SG in**	**SG out**	**STEAM**	**FEED WATER**	**CERNAVODA NPP**
P [bar]	97.8	94.7	45.5	48.26	
T [°C]	309	266	260	187	
H [kJ/kg]	1395	1163	2805	796	
M [kg/s]	2224	2224	257	257	
Q [MWth]	515.968		516.313		
THERMAL BALANCE	**SG in**	**SG out**	**STEAM**	**FEED WATER**	**2EXPERIMENTAL TH Model**
P [bar]	100	97	45.5	48	
T [°C]	309	266	260	187	
H [kJ/kg]	1395	1162	2808	794	
M [kg/s]	2214	2212	254	254	
Q [MWth]	515.862		511.556		

Table 3.3 Thermal balance comparison

Table 3.4, presents the pressure losses along the circuits, for both the thermal-hydraulic model and operational CANDU 6 of Cernavoda, unit 2.

ΔP - Pressure Losses (bar)	**CERNAVODA 2 NPP**	**MODEL**
R Inlet Header - R Outlet Header	13.6	13.2
Pump Discharge-Suction	18.1	17.8
SG in-out	3.1	3

Table 3.4 System pressure losses comparison

The RELAP5 thermal-hydraulic input that reproduces the steady state conditions of a CANDU6 reactor is given in Annex C, i.e. the nodalization of the thermal-hydraulic model.

The following graphs will confirm the steady state conditions of the thermal-hydraulic model developed. In order to confirm that the plant conditions are stable, a computation of 1000 seconds is performed. The following figures present the plant parameters for a period of 1000 seconds.

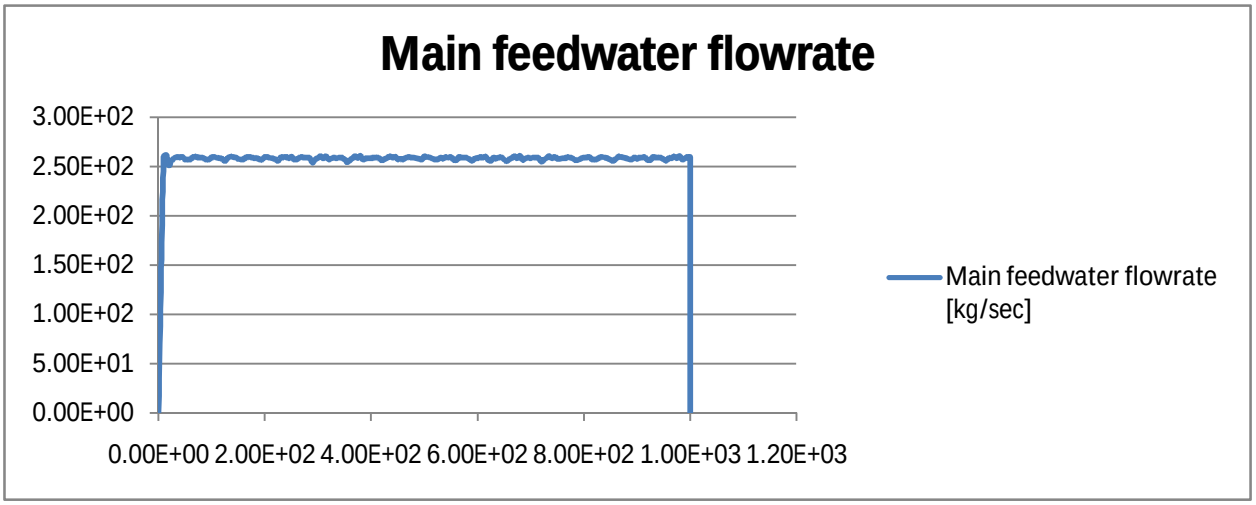


Figure 3.2. Main feedwater flowrate

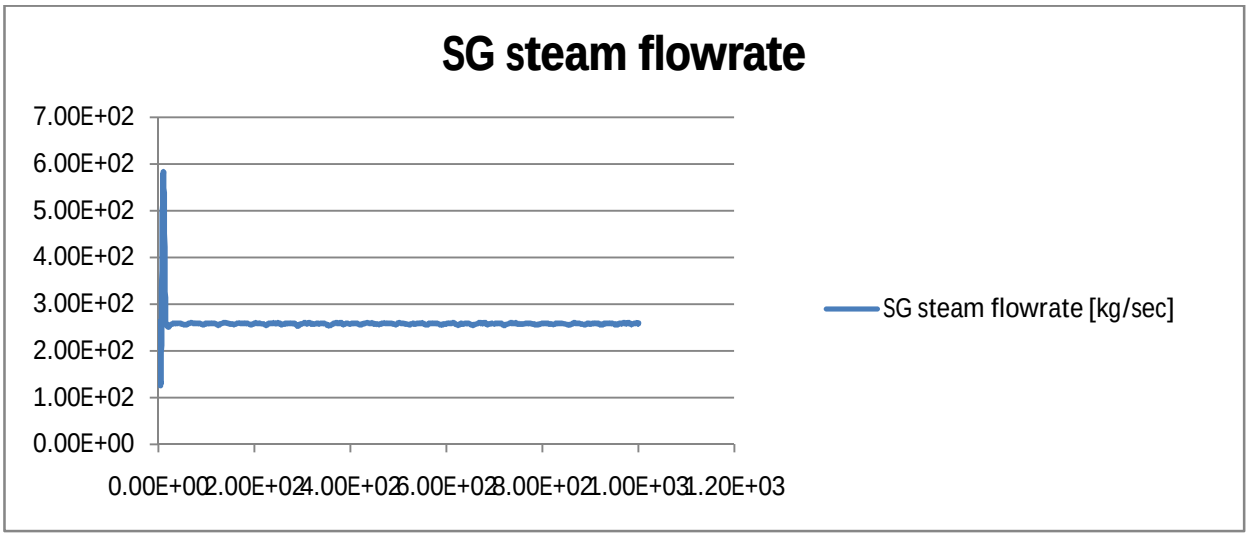


Figure 3.3 SG steam flowrate

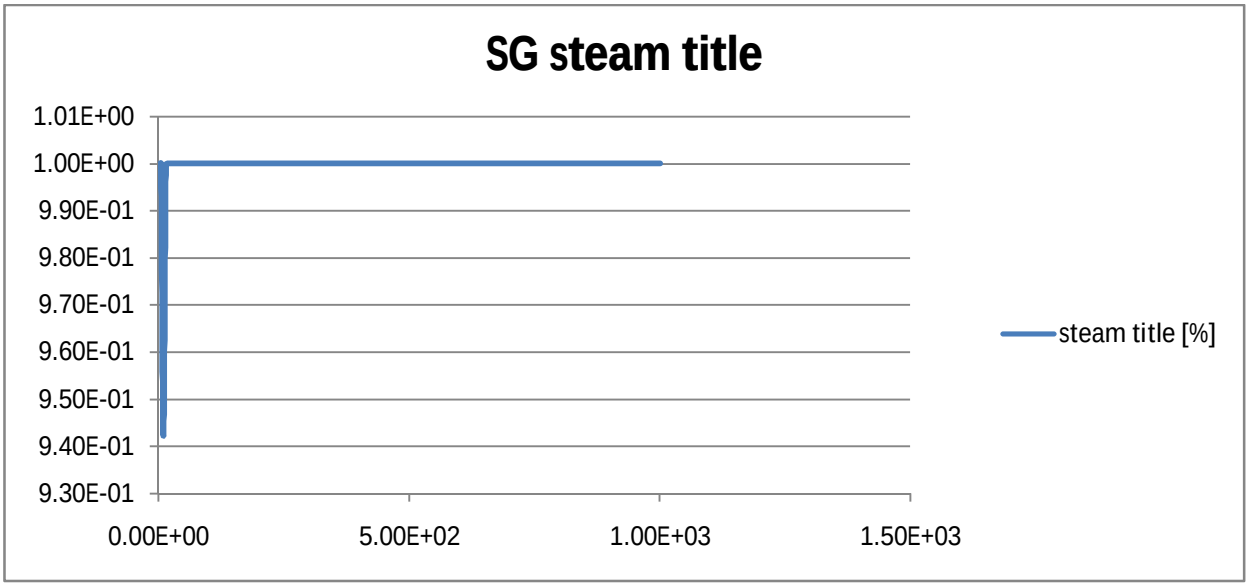


Figure 3.4 Steam Generator steam title

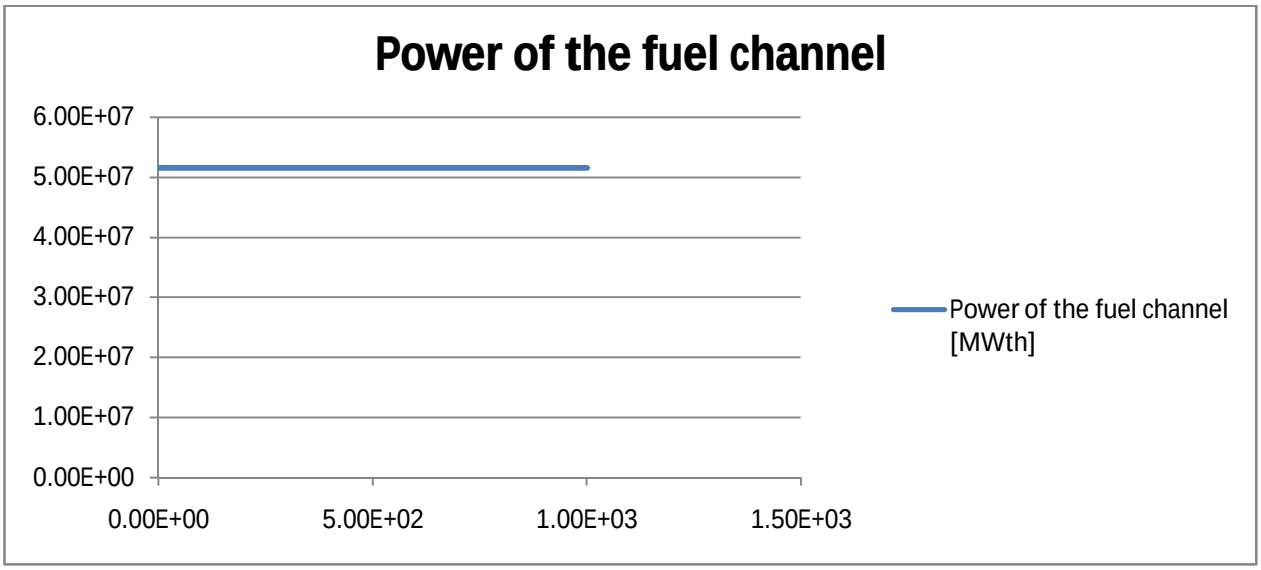


Figure 3.5 Power of one equivalent fuel channel

The above mentioned figures shows that the thermal-hydraulic model is a balanced plant, confirmed by the energy balance between the primary and secondary side circuits, the quality of steam supplied to the turbine and the power developed by the reactor, i.e. a quarter of the total core of a CANDU6 reactor.

3.3.4 IDDA Input – Logic-probabilistics model

For this application the EWS system availability is considered, with the two possibilities of emergency water supply for short and long term. For the short term supply, the emergency water is supplied by gravity from dousing tank that is contained in the upper side of the reactor building, while for the long term supply the emergency water is pumped from whatever water source.

The present application considers the EWS configuration 1 presented in the previous chapter (i.e. chapter 2), with the difference (between the input syntax files) is that the current one is considering also the impact of the instrumentation and control equipment on the actuation of the pneumatic valves that are on the path of water supply to the steam generator.

The differences introduced between the two input files have led to differences in system unavailability and number of scenarios (i.e. constituents) generated; the unavailabilities obtained for the two system possibilities of emergency water supply are shown below in Table 3.6. The same as for the previous application, a cutoff of 1.E-12 has been applied to the end state probabilities of the constituents generated inside the partition.

Table 3.5 Top events unavailabilities for short and long term emergency water supply

	Number of constituents	Q –Unavailability [unavailability/demand]
EWS short term	1751/2712	3.282E-02
EWS long term	805/2712	2.118E-04

For the current application the results that have been highlighted during the first application are not anymore of interest. Special attention is given to the scenarios with the highest unavailability for short and long term emergency water supply that yield within the given system configuration.

For instance the scenario with the highest unavailability for the short term emergency water supply is shown below in Figure 3.6.

```
---------------------------
CONSTITUENT Ordinal :      3

  10  Start      Analysis    +  V    1.0000E+00
  20  DTank      DNBreak     +       1.0000E+00        6.2400E-07
  30  PV41MNT    open        +       1.0000E+00        1.0000E-06
  40  FU227A41   Succes      +       9.9998E-01        2.0000E-05
 801  FU228A41   Succes      +       9.9995E-01        2.6400E-05
 802  BobRL8Q    Succes      +       9.9984E-01        1.1400E-04
 803  Cts2324Q   Succes      +       9.9982E-01        1.3500E-05
 811  CalerrP    Succes      +       9.9383E-01        6.0000E-03
 819  BoRL10H    Succes      +       9.9371E-01        1.1400E-04
 820  CT12RL10   Succes      +       9.8905E-01        4.6900E-03
 821  HEPMT      Succes      +       9.8312E-01        6.0000E-03
 822  CPosHS41   Succes      +       9.8297E-01        1.5000E-04
 823  FRuRL11H   Success     +       9.8286E-01        1.1400E-04
 824  RL11HCts   Success     +       9.7825E-01        4.6900E-03
 825  ChPHS41H   Succes      +       9.7810E-01        1.5500E-04
 826  HErHS41H   Success     +       9.6832E-01        1.0000E-02
 827  SV41       Success     +       9.6767E-01        6.7200E-04
  50  PV41PF     open        +       9.6718E-01        5.0000E-04
  70  FU231A7    Succes      +       9.6716E-01        2.6400E-05
 701  FU232A7    Succes      +       9.6713E-01        2.6400E-05
 702  BobRL8N    Succes      +       9.6702E-01        1.1400E-04
 703  Cts2324N   Succes      +       9.6701E-01        1.3500E-05
 711  CalerrP    Succes      +       9.6120E-01        6.0000E-03
 719  BoRL10H    Succes      +       9.6110E-01        1.1400E-04
 720  CT12RL10   Succes      +       9.5659E-01        4.6900E-03
 721  HEPMT      Succes      +       9.5085E-01        6.0000E-03
 722  ChPosHS2   Succes      +       9.5070E-01        1.5500E-04
 723  FRuRL11H   Success     +       9.5059E-01        1.1400E-04
 724  RL11HCts   Success     +       9.4613E-01        4.6900E-03
 725  ChPHS7H    Succes      +       9.4599E-01        1.5500E-04
 726  HErHS7H    Failure     -       9.4599E-03        1.0000E-02
 901  EWS-ST     Failure     -  V    9.4599E-03

          PROBABILITY equal to  :   9.4599E-03
```

Figure 3.6 Most contributing scenario for the system unavailability

3.4 DYNAMIC PSA procedure description

The dynamic PSA approach is achieved through the use of the I.D.D.A (Integrated Dynamic Decision Analysis) code. IDDA allows interfacing the logic-probabilistic model of the system at study with the plant response in time, therefore with the evolution in time of the plant process variables.

The Dynamic PSA coupling procedure is sketched in Figure 3.7 below.

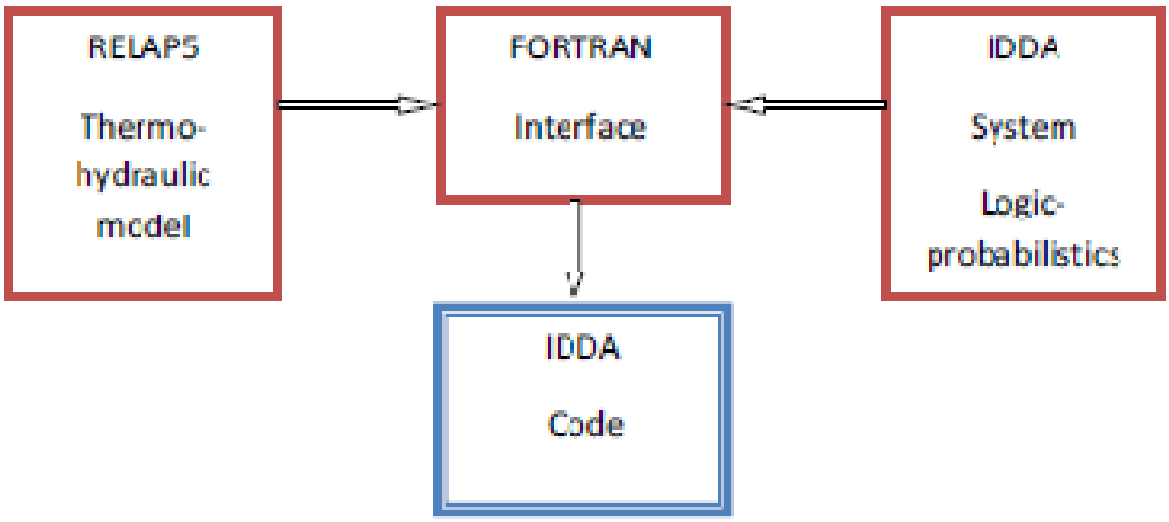
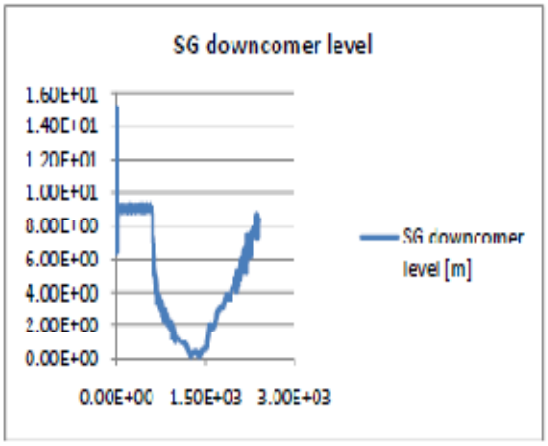


Figure 3.7 The dynamic PSA coupling procedure

The aim is to obtain for each accident sequence of the partition developed by IDDA the associated plant or system phenomenology. The process variables that are of interest for the analyst and further for the decision making process are identified, selected, and transferred from the thermal-hydraulic code to the special created subroutine in FORTRAN.

The phenomenology that corresponds to a certain transient could be described in a FORTRAN simulator either physically; giving a set of equations that describes the variable as a function of time, or by giving the corresponding polynomial equation of different parts of the curve which represents the process variable as a function of time.

An example of particular result and also the conceptual type of results is shown below in Figure 3.8.




```
-------------------------
CONSTITUENT Ordinal :     2

  1  IE         Occurs     - V    1.0000E+00
  2  Pre.Sens   Calibr.    +      9.7000E-01        3.0000E-07
  3  MSSVs      Success    + V    9.7000E-01
  4  3.45bar    Success    + V    9.7000E-01
  5  DTank      No Leak    +      9.7000E-01        9.4300E-07
  6  BV41MNT    No.MNTC    +      9.7000E-01        1.0000E-06
  7  SV41       Works      +      9.6515E-01        5.0000E-03
  8  BV41PT     Open       +      9.6408E-01        1.1100E-03
  9  BV7MNT     No.MNTC    +      9.6408E-01        1.0000E-06
 10  SV7        Works      +      9.5926E-01        5.0000E-03
 11  BV7PT      Unopen     -      1.0648E-03        1.1100E-03
901  RWS        Failure    - V    1.0648E-03

        PROBABILITY equal to  :  1.0648E-03
```

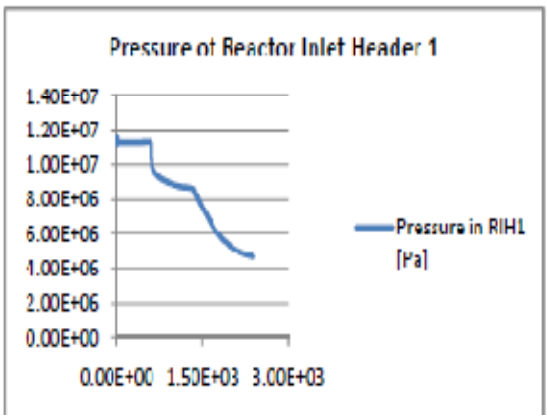


Figure 3.8. Example of results generated by the dynamic PSA methodology

IDDA can be considered a methodology that has as fundamental purpose the systematic and complete exploration of alternatives that are possible inside the formulated hypotheses [4].

The logic-probabilistic model can be interfaced with a phenomenological model of an associated system in order to obtain for each alternative sequence the following elements that represent the basis for a decision making process:

- Probability of occurrence of that alternative (i.e. constituent)
- The physical evolution in time of the particular process variable
- Class of consequence to which the event is belonging

The analysis of the constituents, in terms of logical congruence and correspondence with the knowledge of the plant, is made easier by their representation as concatenations of events that are placed along a well defined time trajectory [5].

3.4.1. DYNAMIC PSA approach results

By making use of the thermal–hydraulic model of a CANDU 6 NPP built in RELAP5 Mod.3.3 code, it has been simulated the total Loss of Feed-Water supply on the secondary side of steam generators, transient that in the normal plant operating conditions would require EWS system intervention, see plant response at subparagraph 3.3.1.

The RELAP5 model, that simulates the CANDU 6 power plant transient, is supposed to be in the following conditions and generates the resulting events sequence:

- Steady state conditions for - 600 s
- Reactor initially at 103% full power
- Total LOFW occurs at 0.0 s
- CLASS III and IV Power not available
- Reactor trip at 0.87 s
- PHTS pumps trip 1 s after reactor trip
- Turbine isolation valves close 2 s after reactor trip
- MSSV are immediately open by the operator as boiler upper head reaches a pressure value equal to 5 MPa; alternatively, MSSV cycles discharge steam for 20 consecutive minutes, maintaining the pressure in the range 4.8-5.0 MPa and after that open automatically.
- When SG secondary side pressure reaches 3.5 bar, EWS can supply water. This occurs respectively at 552 s and 1493 s after reactor trip, depending on the operator intervention or not.
- In order to see the trends of PHTS temperature and SG downcomer level, the total time for which the transients have been simulated is 5000 seconds.

As the goal of the present application is to see what would be the CANDU 6 reactor phenomenology (both primary and secondary side circuits) associated to a total loss of main feedwater transient concomitant with the unavailability of the emergency short and long water supply and along with the specific plant response, the resulted number of important scenarios that were simulated by the thermal-hydraulic code were eight.

For simplicity and a better visibility of the scenarios that were analyzed by the thermal hydraulic an event tree has been created, see below Figure 3.9.

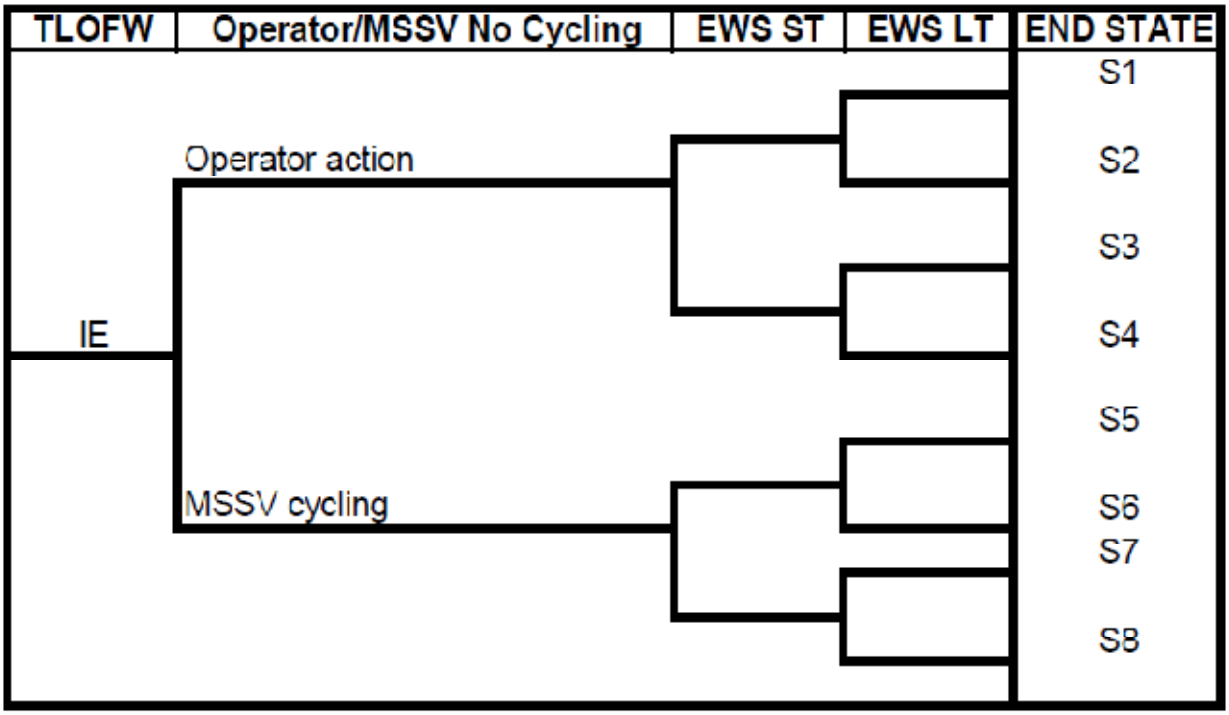


Figure3.9 The main scenarios analyzed within the RELAP5 thermal-hydraulic model

The thermal hydraulic model provides those process variables that along the transient are of interest in order to monitor plant evolution, such as SG's downcomer level, primary heat transport system pressure and temperature.

Through a FORTRAN programming interface the results that are given by RELAP5 code are extracted as data sets and, through piece by piecewise polynomial fit or only one polynomial fit, are forwarded to IDDA code, that couples the system logic probabilistic model with the thermal-hydraulic results. The System Process Simulator that has been built in FORTRAN was meant to find out the water level (water inventory) inside downcomer of steam generator along with all the system possible modes of occurrence of EWS short and long term water supply. One example of FORTRAN subroutine (i.e. interface between the logic-probabilistic model and RELAP output data) used is given in Annex D.

When EWS is employed, during a transient such as Total Loss of Feed-water, the operator in Main Control Room will require process information in order to monitor the status of the station. The following indicators are on the EWS control panel:

- Steam Generator Downcomer Level
- Heat Transport System Pressure
- Primary Heat Transport System Coolant Temperature

The two process variables that have been considered of special interest for the plant phenomenology and assessed were the steam generator down-comer level to see in which conditions the steam generator dry-out can be reached and the other parameter considered was the PHTS coolant temperature in order to see how much worsen the conditions.

3.4.2. Thermal-hydraulic results of the simulated transients scenarios

The following figures show the SG Down-comer Level and PHTS coolant temperature, the two process variables that are of interest for the plant operator in order to monitor the plant status along total LOFW transient in the above mentioned 8 different plant configurations:

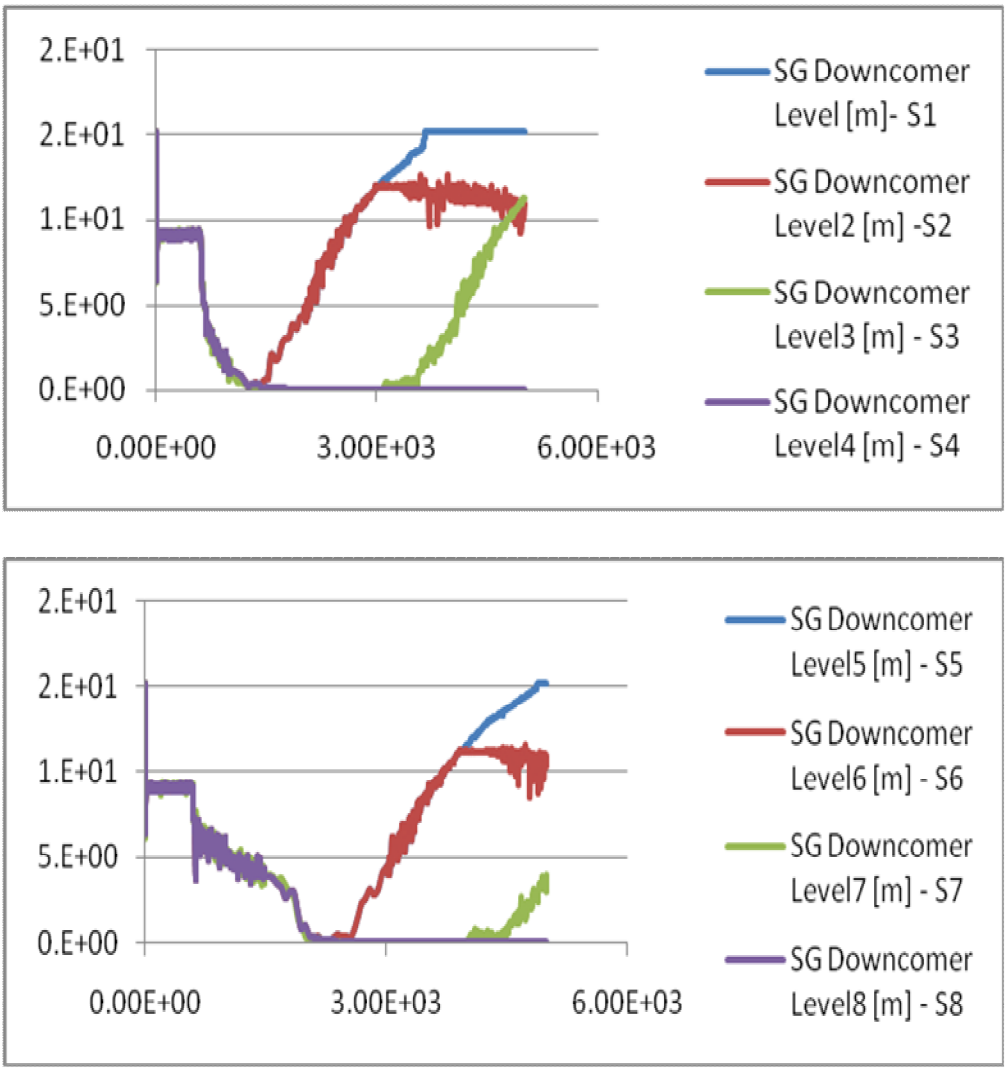


Figure 3.10 Scenarios 1 to 8, SG Downcomer Level

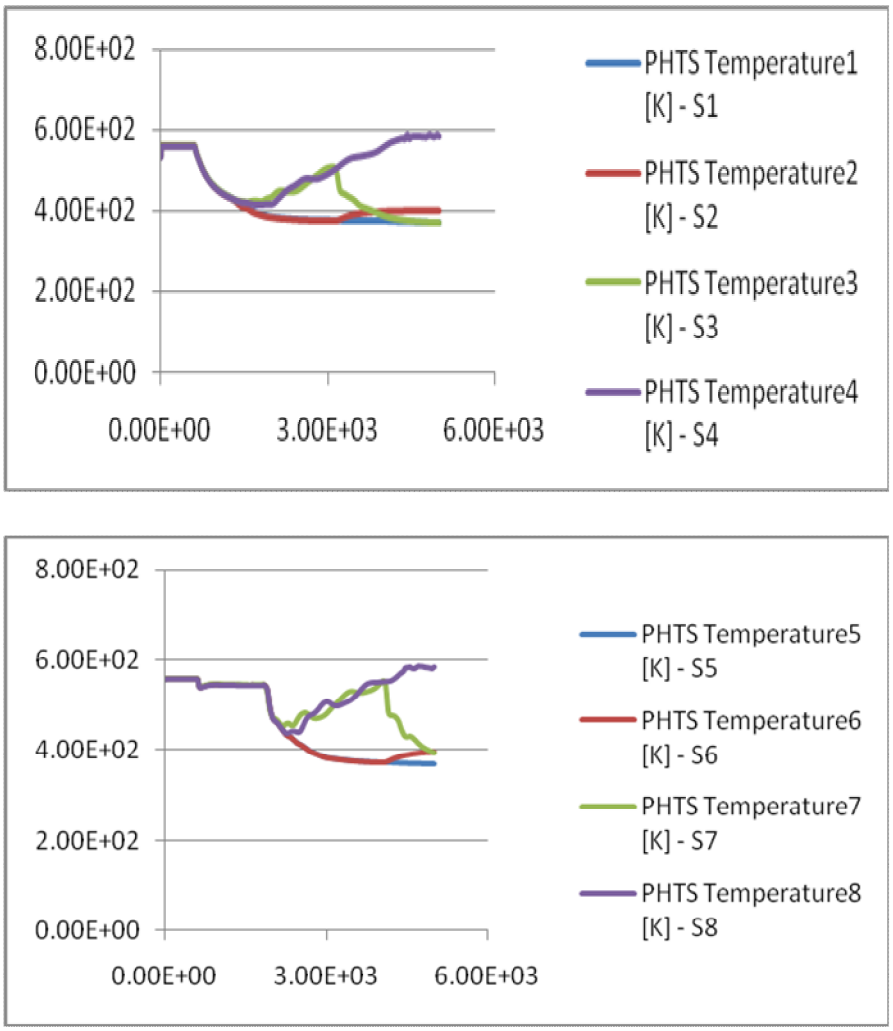


Figure 3.11 Scenarios 1 to 8, PHTS coolant temperature

3.4.3.FORTRAN programming code interface

The results of thermal-hydraulic analysis that are given by RELAP code are forwarded through a FORTRAN subroutine to IDDA code, see Annex D. The FORTRAN interface contains the polynomials that fit as much as possible the data sets of process variables of interest for a safely plant operation.

An example of the polynomial equation that fits the given process variable along the transient is shown in Figure 3.12, to be compared with Figure 3.10, Scenario 1.

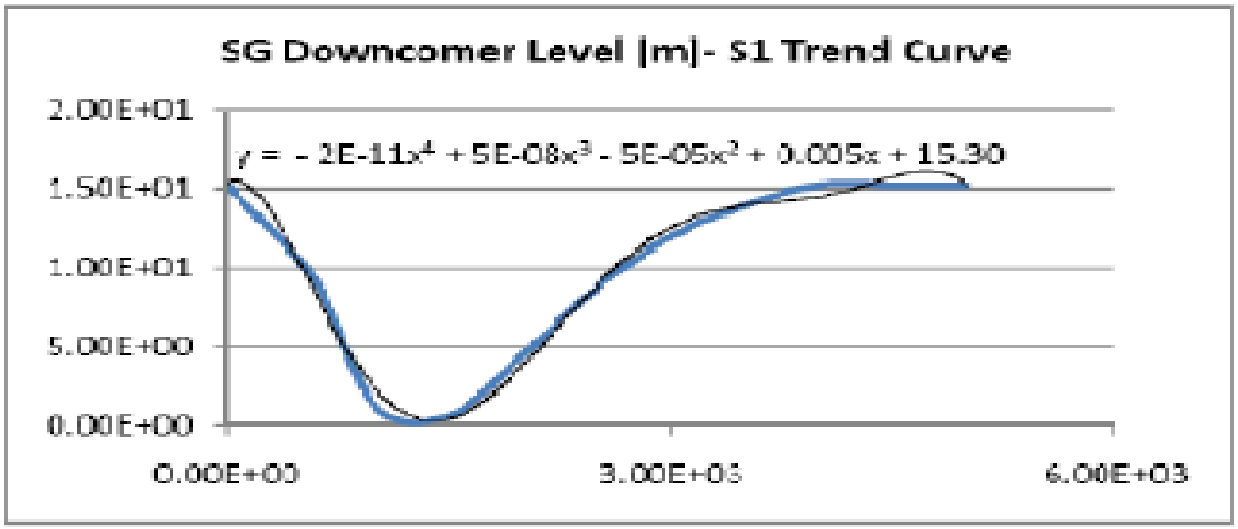


Figure 3.12 Trend Curve and Polynomial Fit

The FORTRAN interface contains the polynomials that fit as much as possible the data sets of interested process variables. Therefore, by use of logical operators and flags, the phenomenology that characterizes the constituent trajectory in subject is transferred.

3.4.4. DYNAMIC PSA approach results

The following figures 3.13 and 3.14 below show two snap-shots of the dynamic PSA approach. They are given by the IDDA code after the coupling procedure has been completed, and are self explanatory.

These figures show the evolution in time of the steam generator down-comer level and of the fuel sheath temperature, as well as the sequences of events that can lead to EWS system unavailability either for the short term, or for the long term.

In case of short term unavailability 1751constituents have as phenomenological consequences the conditions of scenario S2 and respectively for long term unavailability 805 constituents have as phenomenological consequences the conditions of scenario S3.

As it can be seen in Figure 12, EWS short-term failure can lead to SG dry out for more than 2000 s, but correct operation of long term EWS recovers the situation, bringing the plant in safe conditions.

Only total failure of the EWS system can produce dangerous plant conditions in the examined time period, as shown in Figure 13: fuel sheath temperatures become greater than nominal operating temperatures (scenarios 4 and 8). These sequences could bring to severe accidents conditions.

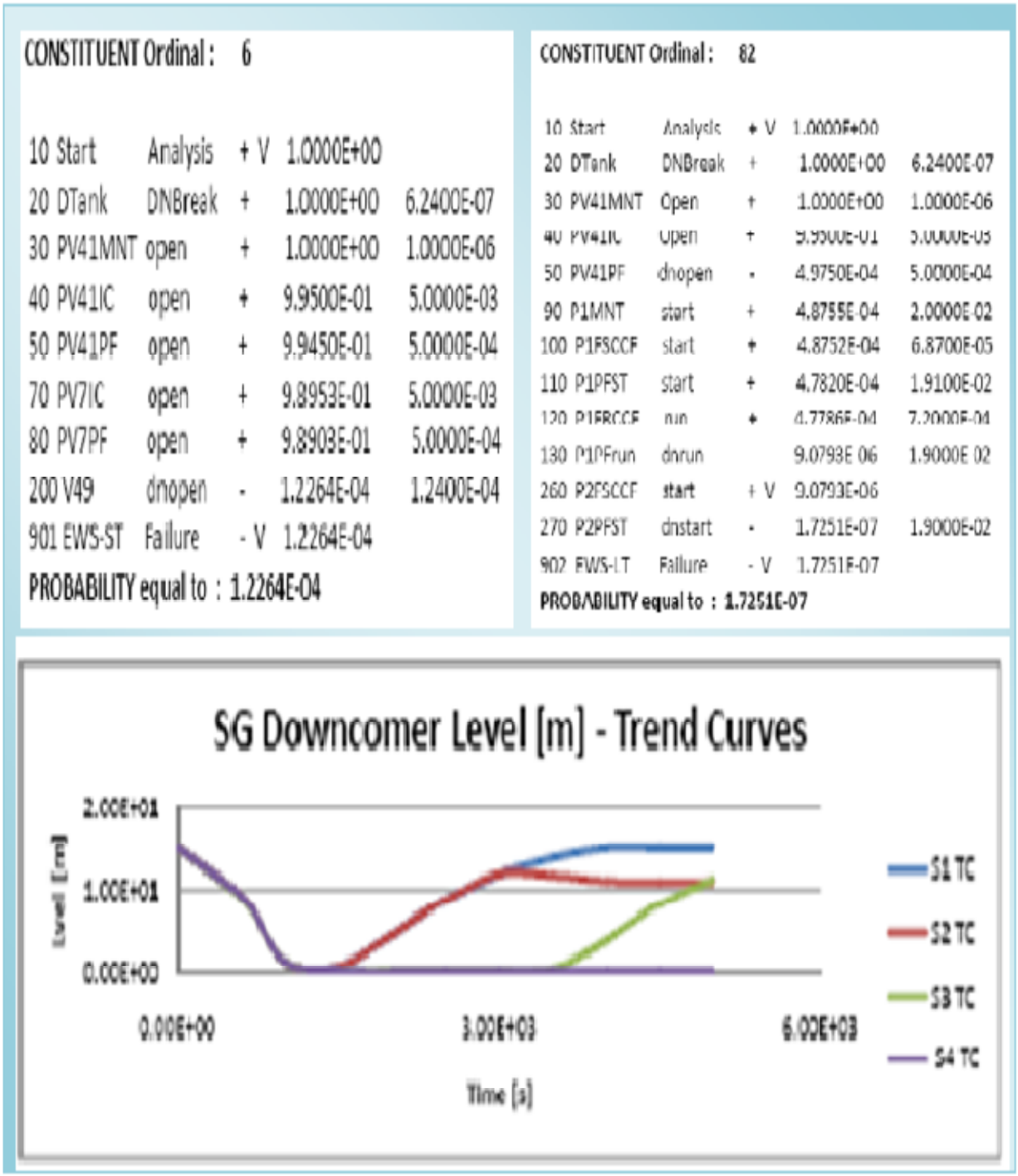


Figure 3.13 Trend Curves of SG Downcomer Level

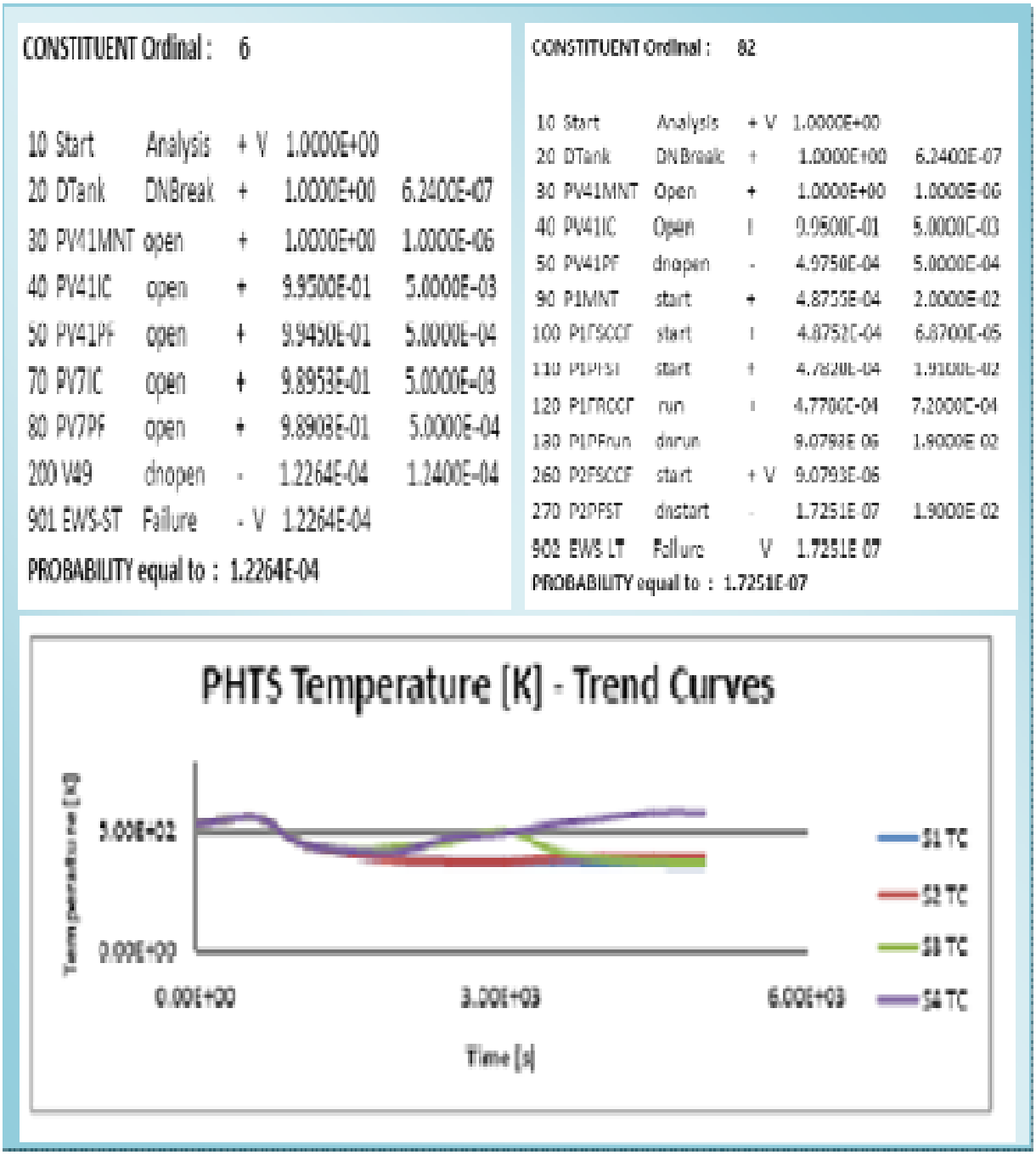


Figure 3.14. Trend curves of PHTS Coolant Temperature

3.5 Generic CANDU 6 plant response to a Station Blackout (SBO) accident

3.5.1 SBO Accident description

The Station Blackout (SBO) accident represents a beyond design basis case[3] scenario, a consequential condition following an earthquake for instance, which involves the loss of external grid, Stand-by Diesel Generators (SDGs) and Emergency Diesel Generators (EPS EDGs), therefore loss of all AC electric power generation sources of the plant.

The plant and operator response following this accident is described below, [1]:

- The reactor is shutdown immediately after the SBO, either by first shutdown system (SDS1) or second shutdown system (SDS2) on the process trip parameters. Both shutdown systems are designed to fail safe, in such a manner that if they are not supplied with electrical power the systems will perform their design function, i.e. reactor shutdown. Therefore the possibility to have an ATWS event as in the classical PWR design is discarded;

- The Loss of Class IV power determines the following event sequences: turbine trip, reactor trip, main coolant pump trip, main feedwater pump trip, SGs steam pressure increase with a consequently opening and closing of the Main Steam Safety Valve (MSSVs) for SG overpressure protection;

- The Loss of Class III power determines the loss of the auxiliary feedwater pump;

- In case of SBO the operator should initiate SGs depressurization in order to bring into service the low pressure water supply to SGs, i.e. the dousing tank water supply or pumped Emergency Water Supply. The operator will open MSSVs and when the SGs pressure decrease below 345 kPa, the water from the dousing tank will start to be fed by gravity into the SG;

- Considering that the Class I and II electrical power (batteries) are available, in case that the operator does not depressurize the SGs then the auto-depressurization is automatically initiated when specific conditions are reached. The secondary side SG pressure then oscillates at the MSSV set point as the safety valves open and close;

[3] The beyond design basis accidents are severe accidents characterized by multiple failures and their accident conditions are more severe than a design basis accident. They are normally identified by a systematic plant review or by a PSA, and are too low in frequency to merit inclusion in the design basis set. For instance, in CANDU 6 design the accidents that result in damage to the reactor core are of two classes, those for which the core geometry is preserved called also Limited Core Damage Accidents and those for which the core geometry is lost, called also Severe Core Damage Accidents. The Limited Core Damage Accidents are typically considered part of the design basis for PHWRs.

- In both cases, either manual or auto depressurization of the SGs, the water inventory will be available from the dousing tank that is located at the top of containment building;

- Since water is provided to the SGs, the thermo-siphoning process will ensure decay power removal and the fuel damage is not expected;

- SG depressurization causes a rapid depressurization of the PHT system and also the draining of the pressurizer due to shrinkage. The secondary side water level in SGs decreases as boil-off proceeds. The SGs reach the dry-out state and are no longer a heat sink to remove the decay heat from the PHTS;

- During this time, the plant operators will attempt to restore the EPS diesel generators in order to start EWS pumps that ensure the long-term heat sink. In case that EPS cannot be recovered, the plant procedures are directing the operator to use the mobile Diesels Generators. Once the mobile Diesel generators are operational, the EWS pumps can be used to provide water supply to SGs;

- The moderator temperature in the calandria vessel increases as a result of the loss of moderator cooling and heat transfer from the core.

- Containment isolation valves will fail close either on loss of their electrical power supply or loss of instrumentation air. Therefore the containment function considering the SBO accident is not affected;

- The monitoring of the critical safety parameters will be ensured by use of electrical power supplied from batteries (8 hours autonomy). After depletion of the batteries is considered that the mobile diesel generators can be connected.

3.5.2 SBO study assumptions

The study, both the logic-probabilistics model and the thermal-hydraulic model considered the following assumptions:

- AC power and all onsite standby/emergency electric power are unavailable;

- The batteries are credited as available;

- Reactor shutdown is initiated immediately after accident initiation. The possibility of an ATWS is not credit for CANDU 6 design;

- Moderator cooling and shield cooling are assumed unavailable;

- Shutdown cooling system is unavailable;

- Main and auxiliary feed water are assumed unavailable as a consequence of SBO event. The logic-probabilistic and the thermal-hydraulic analysis consider successive recovery attempts of the external grid after 1, 2 and 3 hours and recall of the auxiliary feedwater system, in case the external grid was successfully recovered;

- The injection flowrate is considered to be the same for AFW and EWS.

- Once the AFW pump is failed, no reparation is credited.

- Emergency Core Coolant System (ECCS), including high (HPI), medium (MPI) and low pressure (LPI) injection, are not credited in this analysis;

- Crash cool-down system (i.e. automatic opening of 8 out of 16 MSSVs) is not credited;

- Steam generator safety valves (i.e. MSSVs) are available; they open and close at the set point;

- Containment dousing system is initially available, but both the logic-probabilistic analysis and thermal-hydraulic analysis consider the possibility of failure of this system. The failure could be due to reclosure of the isolation valves that are on the path supply to the SGs;

- The main steam isolation valves are closed after accident initiation, therefore the turbine is tripped and isolated;

- All operator interventions are credited, excepting the immediate opening of the MSSVs following the SBO accident;

- As the thermal-hydraulic model of the generic CANDU 6 plant considers only one loop of the reactor, the triggering of the loop isolation is not considered;

- The opening and closure of the Liquid Relief Valves that are meant to protect the Calandria Vessel against overpressure are not credited in the analysis;

- In case that the EWS system cannot provide water to SGs, the fire water trucks or the possibility to provide water directly to the SGs through the EWS pipes is not credited;

- The mobile diesel generators connection to the EWS pumps is credited to be possible in approximately 3 hours; field experiments confirmed that, [1].

- The calandria vault is not considered.

3.5.3. IDDA logic-probabilistics model

According to the plant response in case of SBO accident and specific study assumptions presented at the previous paragraphs (see § 3.7.1. and § 3.7.2.) was created the corresponding IDDA logic-probabilistics model. The resulted scenarios are 33. The equivalent event tree that corresponds to the scenarios generated by IDDA is given at Figure 3.15, below.

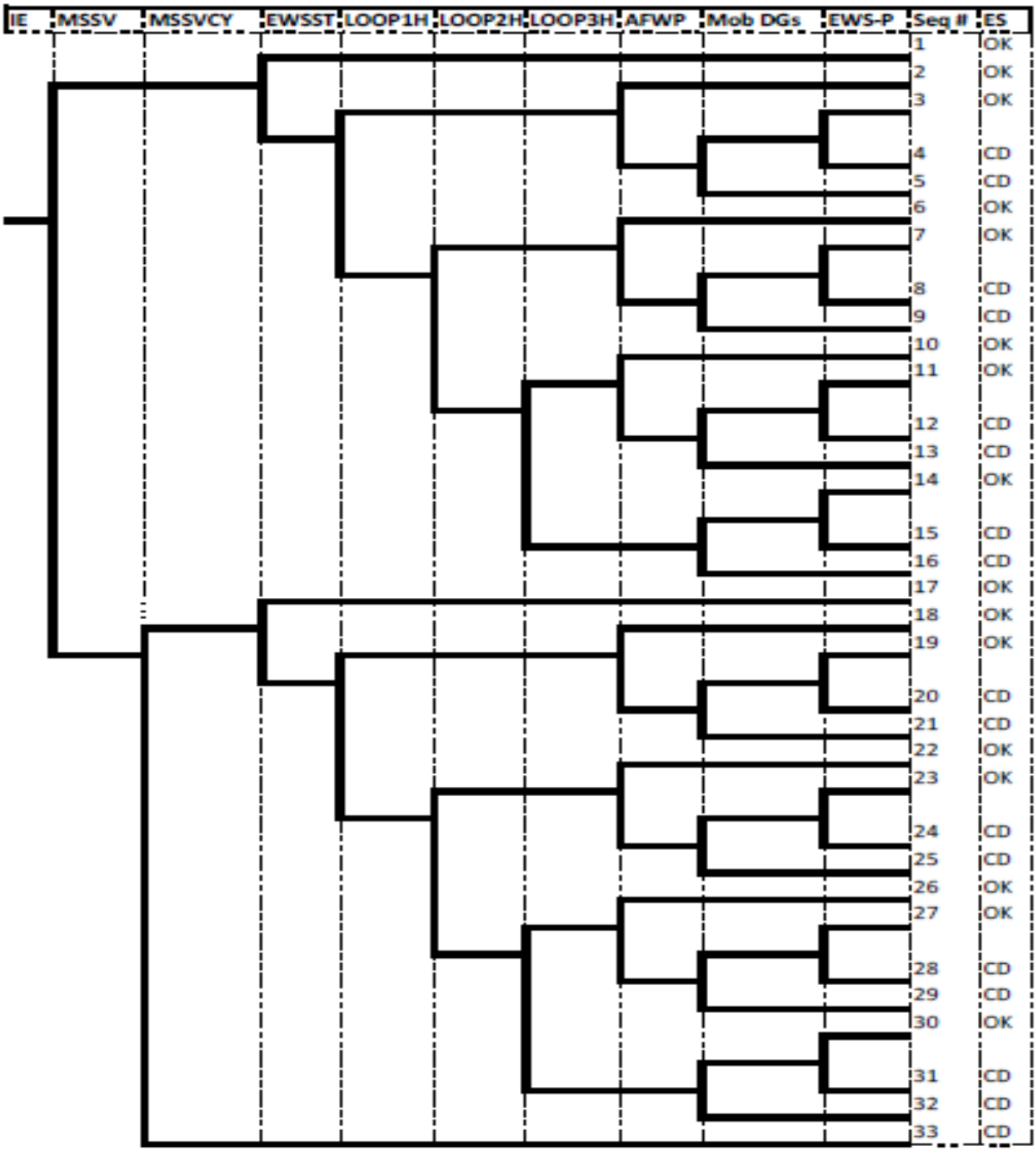


Figure 3.15 SBO Even Tree resulted

The SBO logic probabilistic input syntax file is given in Annex E and the resulted scenarios are given in Annex F.

If according to the SBO logic-probabilistics the plant response in terms of scenarios were resulted 33, then in terms of consequences that can rise within the spectrum of cause-consequence, the number of scenarios that develop different consequences are 10.

Table 3.6 given below summarizes the scenarios that have the same consequences or unique consequences.

Reference Scenario	**Scenarios with similar consequences as the reference scenario or unique consequences**	**Scenario summary**
1	NA	All the operator actions and mitigation systems are actuated as it should, the plant reaches stable conditions.
2	NA	Dousing tank system fails, the grid is recovered after one hour and the recall of AFW pump is successful.
3	Scenario 7, Scenario 11, Scenario 14.	All mitigation systems fail, even if the external grid was successfully recovered, but following the connection of mobile DG to the EWS pump connection the water injection is possible after 3 hours from the initiation of SBO accident.
4	Scenario 5 Scenario 8 Scenario 9 Scenario 10 Scenario 12 Scenario 13 Scenario 15 Scenario 16	Finally even if the external grid recovery was possible, then the failure comes either from the mobile DG or the failure of EWS system (e.g. fail to start of EWS pump)
6	NA	Dousing tank system fails, the grid is recovered after two hours and the recall of AFW pump is successful.
17	NA	All the mitigation systems are actuated as it should, the plant reaches stable conditions.
18	NA	MSSVs are cycling for a while until the SG pressure is decreased. Dousing tank system fails, the grid is recovered

		after one hour and the recall of AFW pump is successful.
19	Scenario 23 Scenario 27 Scenario 30	MSSVs are cycling for a while until the SG pressure is decreased. All mitigation systems fail, even if the external grid was successfully recovered, but following the connection of mobile DG to the EWS pump connection the water injection is possible after 3 hours from the initiation of SBO accident.
20	Scenario 21 Scenario 24 Scenario 25 Scenario 28 Scenario 29 Scenario 31 Scenario 32	MSSVs are cycling for a while until the SG pressure is decreased. Finally even if the external grid recovery was possible, then the failure comes either from the mobile DG or the failure of EWS system (e.g. fail to start of EWS pump)
22	NA	MSSVs are cycling for a while until the SG pressure is decreased. Dousing tank system fails, the grid is recovered after two hours and the recall of AFW pump is successful.

Table 3.6 SBO scenarios with unique consequences or similar consequences

3.5.4. SBO transient thermal-hydraulic results

The same as for the first application of Chapter 3, the scenarios split in those that are considering the intervention of the operator from main control room that opens the MSSVs in order to depressurize the steam generators and scenarios that are considering the MSSVs cycling until the pressure is decreased to the set point of actuation of the dousing tank, therefore the timing is different. As it has been shown above in Table 3.8, the scenarios with unique consequences are 8.

In the following we present the thermal hydraulic results obtained for the different scenarios. The process variables that are of special interest for plant monitoring are the following:

- SG downcomer level

- PHTS coolant temperature
- Fuel sheath temperature

The following figures describe the SBO scenarios: the first four scenarios (i.e. S2, S3, S4 and S6) that are considering the successful MCR operator action to open the MSSVs and the last four scenarios (i.e. S18, S19, S20, S22) that do not credit the operator action and consider the MSSV cycling until MSSVs get depressurized at the set point of dousing tank gravitational feeding.

```
CONSTITUENT Ordinal :      2

  1  SBO        Occurs     -  V    1.0000E+00
  2  SCRAM      Success    +  V    1.0000E+00
  4  OpA-MSSV   Success    +       9.5000E-01        5.0000E-02
  6  3.45bar    Success    +  V    9.5000E-01
 10  EWS-ST     Failure    -       1.1970E-04        1.2600E-04
 20  Gridrec1   YES        +       1.1964E-04        5.0000E-04
 22  AFW-pump   Success    +       1.1904E-04        5.0000E-03
100  NPPSTATE   SUCCESS    +  V    1.1904E-04

          PROBABILITY equal to  :  1.1904E-04
```

Figure 3.16 SBO Event Tree - Scenario 2 – External grid recovery after one hour and then successful AFW running

```
CONSTITUENT Ordinal :      3

  1  SBO        Occurs     -  V    1.0000E+00
  2  SCRAM      Success    +  V    1.0000E+00
  4  OpA-MSSV   Success    +       9.5000E-01        5.0000E-02
  6  3.45bar    Success    +  V    9.5000E-01
 10  EWS-ST     Failure    -       1.1970E-04        1.2600E-04
 20  Gridrec1   YES        +       1.1964E-04        5.0000E-04
 22  AFW-pump   Failure    -       5.9820E-07        5.0000E-03
 50  MobileDG   Success    +       5.9521E-07        5.0000E-03
 60  EWS-pump   Success    +       5.9223E-07        5.0000E-03
100  NPPSTATE   SUCCESS    +  V    5.9223E-07

          PROBABILITY equal to  :  5.9223E-07
```

Figure 3.17 SBO Event Tree - Scenario 3 – No recovery of the external grid, but successful connection of MDGs after 3 hours and then running of one out of two EWS pumps

```
CONSTITUENT Ordinal :      4

  1   SBO         Occurs      -  V    1.0000E+00
  2   SCRAM       Success     +  V    1.0000E+00
  4   OpA-MSSV    Success     +       9.5000E-01          5.0000E-02
  6   3.45bar     Success     +  V    9.5000E-01
 10   EWS-ST      Failure     -       1.1970E-04          1.2600E-04
 20   Gridrec1    YES         +       1.1964E-04          5.0000E-04
 22   AFW-pump    Failure     -       5.9820E-07          5.0000E-03
 50   MobileDG    Success     +       5.9521E-07          5.0000E-03
 60   EWS-pump    Failure     -       2.9760E-09          5.0000E-03
900   R FUSION    OCCURS          V    2.9760E 09
```

Figure 3.18 SBO Event Tree - Scenario 4 – Neither successful recovery of the external grid, nor successful running of EWS pumps after 3 hours

```
CONSTITUENT Ordinal :      6

  1   SBO         Occurs          V    1.0000E+00
  2   SCRAM       Success     +   V    1.0000E+00
  4   OpA-MSSV    Success     +       9.5000E-01          5.0000E-02
  6   3.15bar     Success     +   V    9.5000E-01
 10   EWS-ST      Failure     -       1.1970E-04          1.2600E-04
 20   Gridrec1    NO          -       5.9850E-08          5.0000E-04
 30   Gridrec2    YES         +       5.9790E-08          1.0000E-03
 22   AFW-pump    Success     +       5.9491E-08          5.0000E-03
100   NPPSTATE    SUCCESS     +   V    5.9491E-08

          PROBABILITY equal to  :  5.9491E-08
```

Figure 3.19 SBO Event Tree - Scenario 6 – Successful recovery of the external grid after 2 hours, and then successful running of AFW pump

The Figure 3.20 presents the actuation of AFW or EWS after 1, 2 or 3 hours occurrence of the SBO,

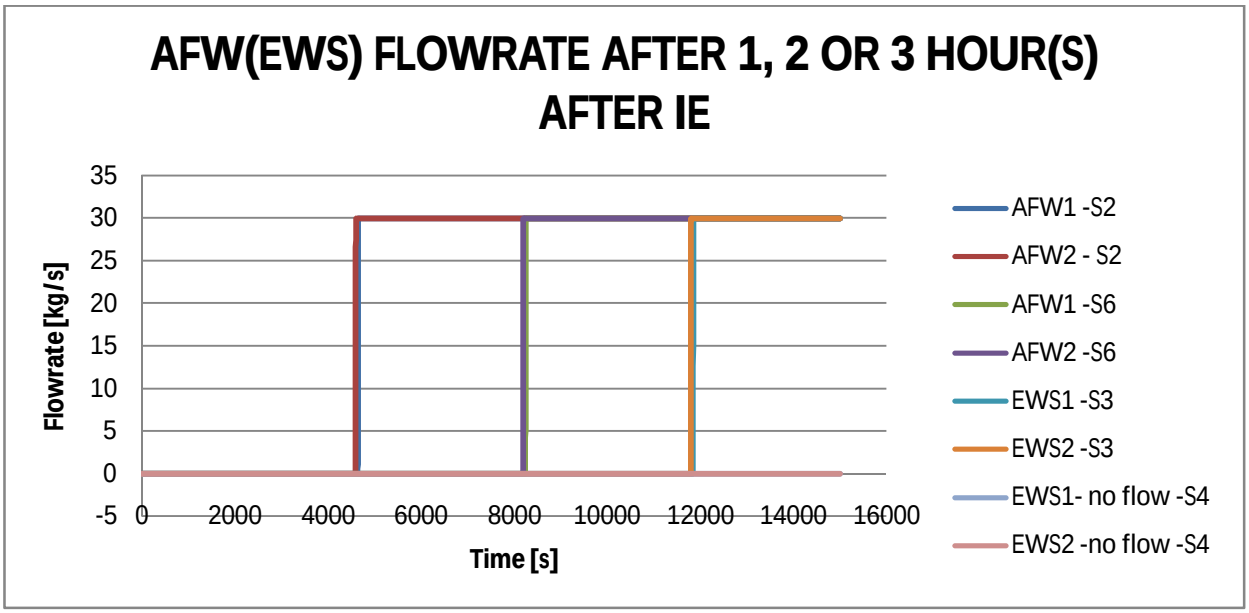


Figure 3.20 AFW (EWS) flowrate –operator actuates MSSVs

Figure 3.21 shows the SG downcomer level recovery or non recovery and the time when the SGs reach the dry-out conditions or complete refill.

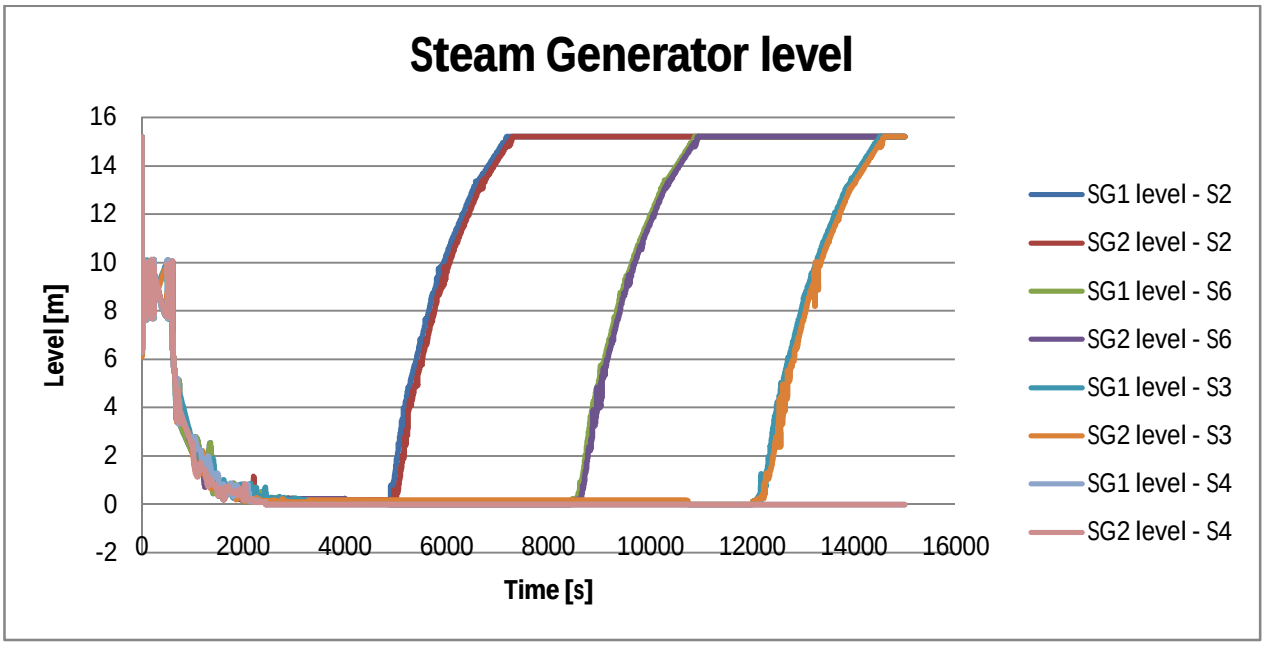


Figure 3.21 SG downcomer level - operator actuates MSSVs

The Figure 3.22 shows the fuel sheath temperature variations following the 4 scenarios with unique consequence that might occur considering that operator from MCR successfully actuates the MSSVs in order to depressurize the SGs. It is shown that in case the heat sink is missing

(see scenario 4) the temperature increases but not drastically, the moderator present in calandria vessel act as a ultimate heat and cut the eventual temperature rise.

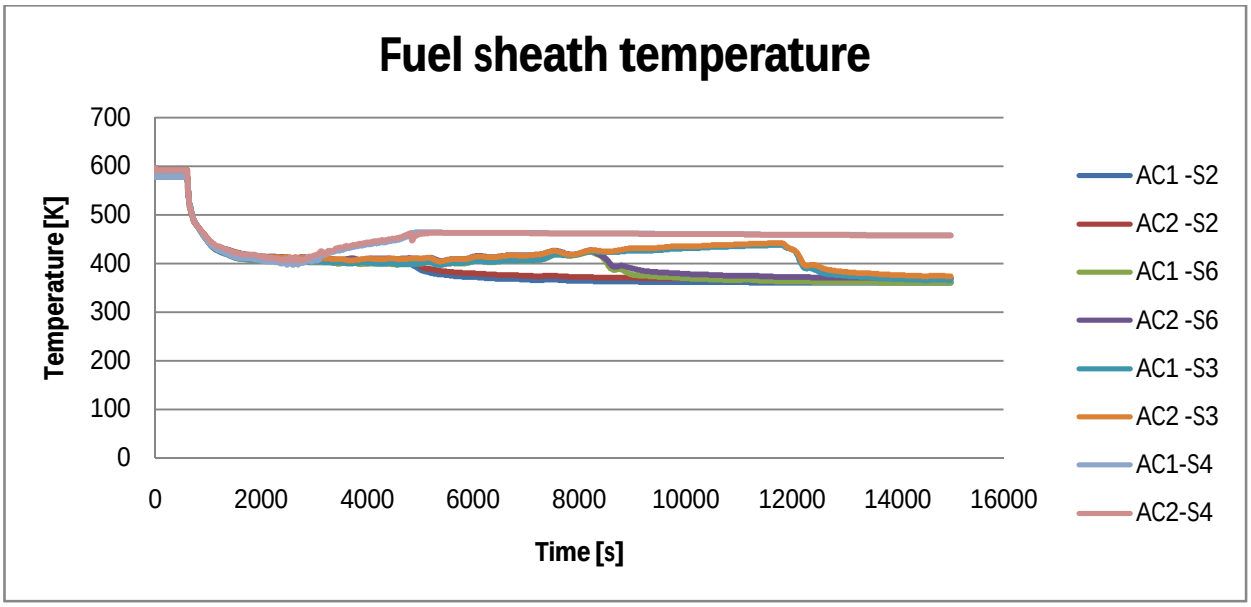


Figure 3.22 Fuel sheath temperature – operator actuates MSSVs

The Figure 3.23 shows the different trends that PHTS coolant temperature can take for the first four scenarios. The PHTS coolant temperature could have a small temperature increase due to delays in providing heat sink for 1, 2 or 3 hours (see scenarios S2, S6, S3) but however in case the heat sink is missing (i.e. SG water inventory) then moderator that surrounds the fuel channels acts as a ultimate heat sink, due to its low temperature, i.e. 343 K.

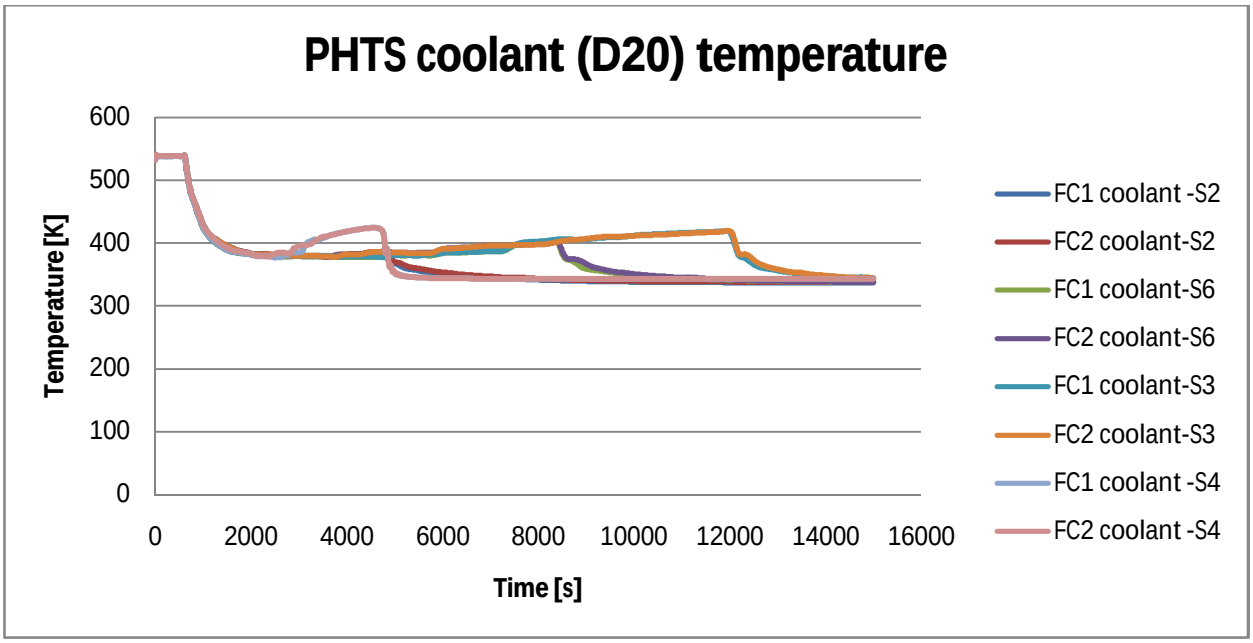


Figure 3.23 PHTS coolant (D2O) temperature – MSSVs operator action

The following figures present the other 4 scenarios of SBO event tree with unique consequences. These scenarios do not credit the operator action from MCR that actuates the opening of MSSVs, those latter are cycling and depressurize the SGs with a delay of approximately 1100 seconds.

```
CONSTITUENT Ordinal :     18

  1  SBO        Occurs     -  V    1.0000E+00
  2  SCRAM      Success    +  V    1.0000E+00
  4  OpA-MSSV   Failure    -       5.0000E-02        5.0000E-02
 90  MSSV-Cyc   Success    +       4.9975E-02        5.0000E-04
  6  3.45bar    Success    +  V    4.9975E-02
 10  EWS-ST     Failure    -       6.2969E-06        1.2600E-04
 20  Gridrec1   YES        +       6.2937E-06        5.0000E-04
 22  AFW-pump   Success    +       6.2622E-06        5.0000E-03
100  NPPSTATE   SUCCESS    +  V    6.2622E-06

          PROBABILITY equal to  :  6.2622E-06
```

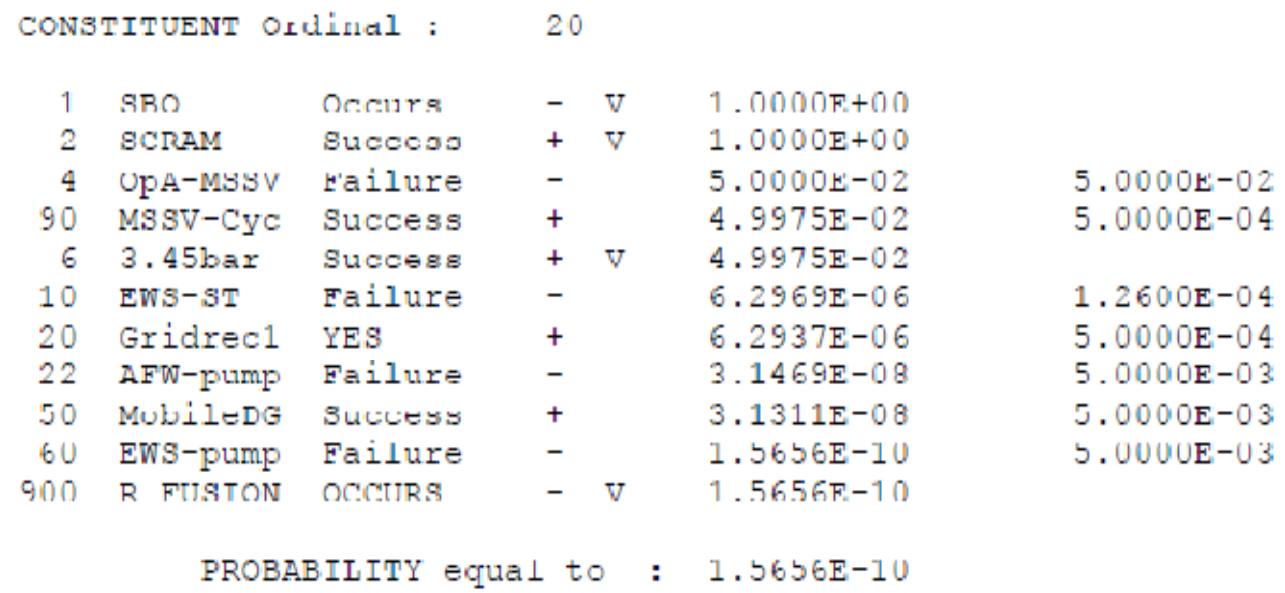
Figure 3.24 SBO Event Tree - Scenario 18 – External grid recovery after one hour and then successful AFW running

```
CONSTITUENT Ordinal :     19

  1  SBO        Occurs     -  V    1.0000E+00
  2  SCRAM      Success    +  V    1.0000E+00
  4  OpA-MSSV   Failure    -       5.0000E-02        5.0000E-02
 90  MSSV-Cyc   Success    +       4.9975E-02        5.0000E-04
  6  3.45bar    Success    +  V    4.9975E-02
 10  EWS-ST     Failure    -       6.2969E-06        1.2600E-04
 20  Gridrec1   YES        +       6.2937E-06        5.0000E-04
 22  AFW-pump   Failure    -       3.1469E-08        5.0000E-03
 50  MobileDG   Success    +       3.1311E-08        5.0000E-03
 60  EWS-pump   Success    +       3.1155E-08        5.0000E-03
100  NPPSTATE   SUCCESS    +  V    3.1155E-08

          PROBABILITY equal to  :  3.1155E-08
```

Figure 3.25 SBO Event Tree - Scenario 19 – No recovery of the external grid, but successful connection of MDGs after 3 hours and then successful running of one out two EWS pumps

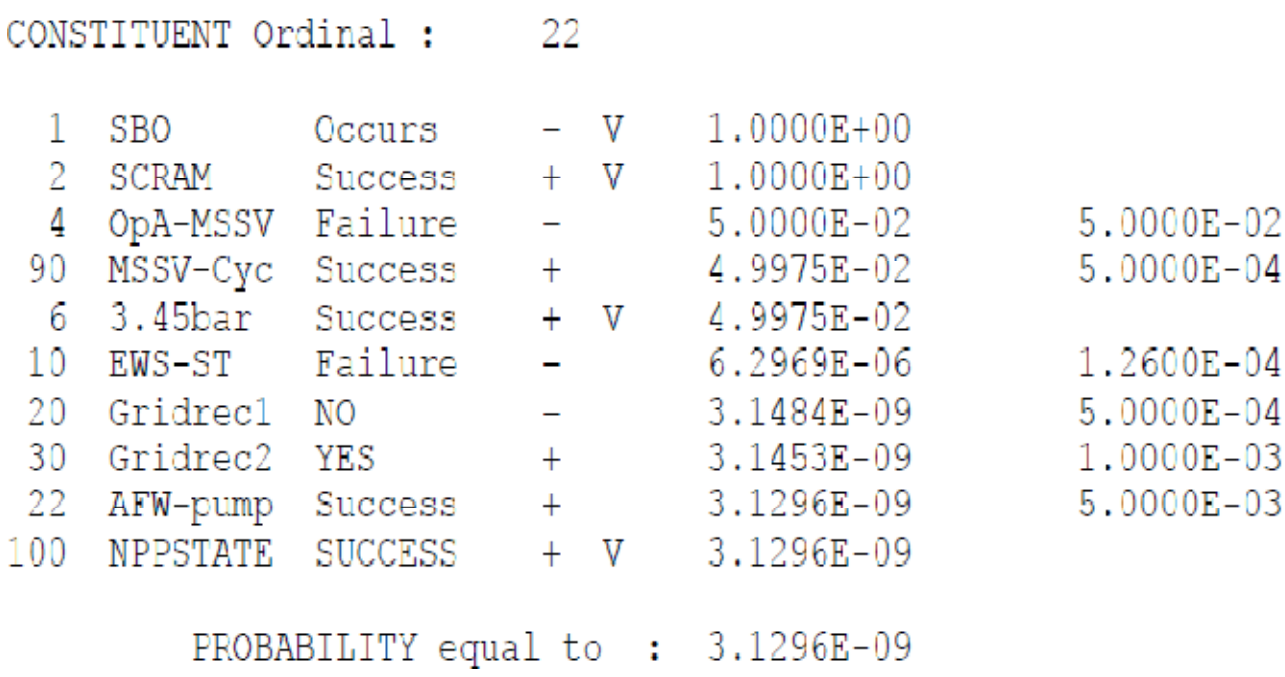


```
CONSTITUENT Ordinal :     20

  1  SBO         Occurs     -  V    1.0000E+00
  2  SCRAM       Success    +  V    1.0000E+00
  4  OpA-MSSV    Failure    -       5.0000E-02          5.0000E-02
 90  MSSV-Cyc    Success    +       4.9975E-02          5.0000E-04
  6  3.45bar     Success    +  V    4.9975E-02
 10  EWS-ST      Failure    -       6.2969E-06          1.2600E-04
 20  Gridrec1    YES        +       6.2937E-06          5.0000E-04
 22  AFW-pump    Failure    -       3.1469E-08          5.0000E-03
 50  MobileDG    Success    +       3.1311E-08          5.0000E-03
 60  EWS-pump    Failure    -       1.5656E-10          5.0000E-03
900  R_FUSTON    OCCURS     -  V    1.5656E-10

          PROBABILITY equal to  :   1.5656E-10
```

Figure 3.26 SBO Event Tree - Scenario 20 – Neither recovery of the external grid, nor successful running of one of the EWS pumps after 3 hours



```
CONSTITUENT Ordinal :     22

  1  SBO         Occurs     -  V    1.0000E+00
  2  SCRAM       Success    +  V    1.0000E+00
  4  OpA-MSSV    Failure    -       5.0000E-02          5.0000E-02
 90  MSSV-Cyc    Success    +       4.9975E-02          5.0000E-04
  6  3.45bar     Success    +  V    4.9975E-02
 10  EWS-ST      Failure    -       6.2969E-06          1.2600E-04
 20  Gridrec1    NO         -       3.1484E-09          5.0000E-04
 30  Gridrec2    YES        +       3.1453E-09          1.0000E-03
 22  AFW-pump    Success    +       3.1296E-09          5.0000E-03
100  NPPSTATE    SUCCESS    +  V    3.1296E-09

          PROBABILITY equal to  :   3.1296E-09
```

Figure 3.27 SBO Event Tree - Scenario 22 – Neither recovery of the external grid, nor successful running of EWS pumps after 3 hours

The Figure 3.28 presents the actuation of AFW (EWS) after 1, 2 or 3 hours occurrence of the SBO. It can be seen that the SGs depressurization occur later (approximately 1100 seconds) due to the low rate depressurization of MSSVs.

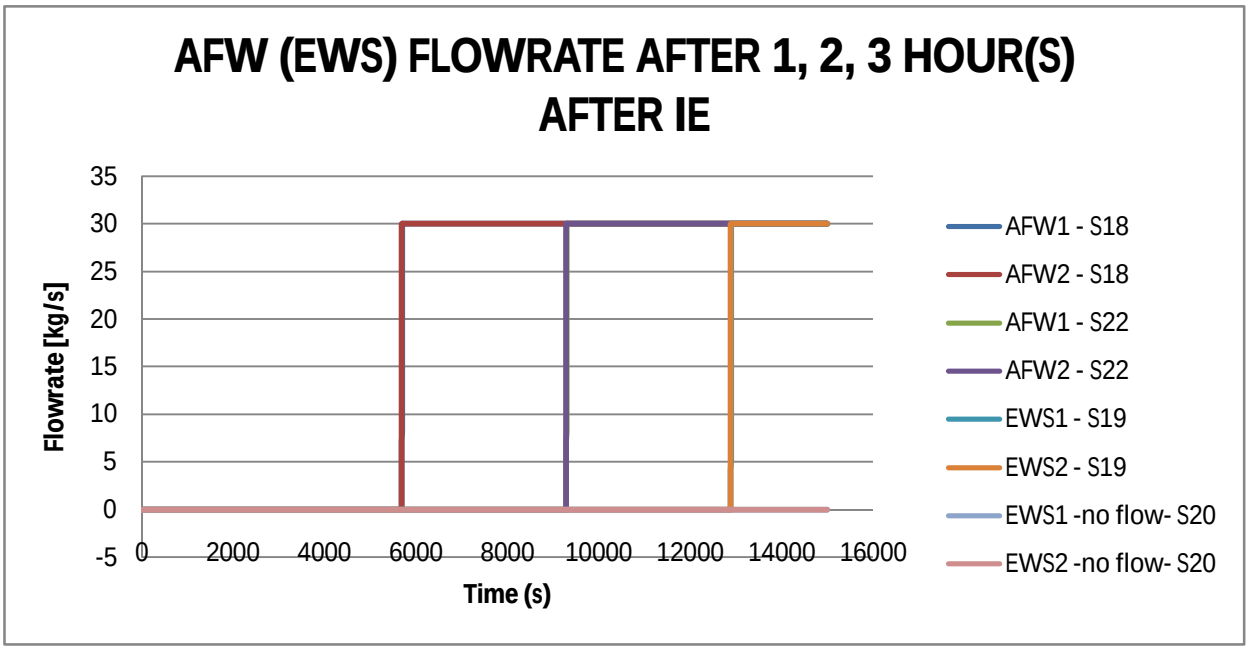


Figure 3.28 AFW (EWS) flowrate – MSSVs cycling

Figure 3.29 shows the SG downcomer level recovery or non recovery and the time needed for the SGs to reach the dry-out conditions. It can be seen that the SG dryout conditions are reached with some delay, approximately 20 minutes later.

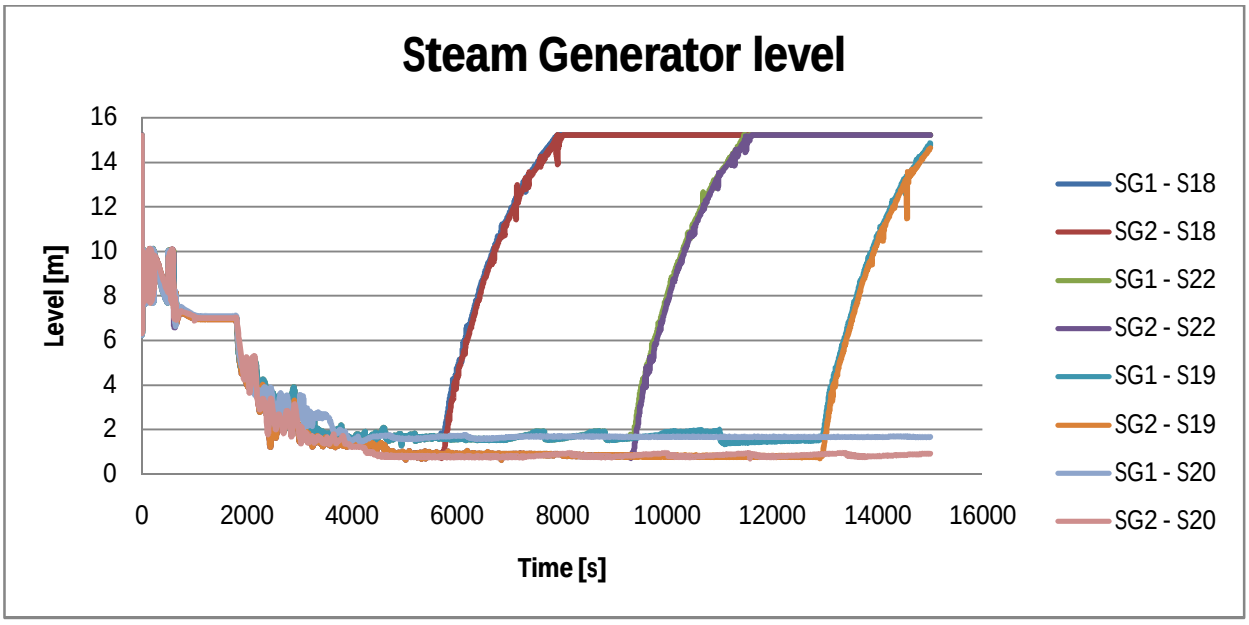


Figure 3.29 SG downcomer level – MSSVs cycling

Figure 3.30 shows the fuel sheath temperature, it is confirmed that the fast actuation (opening) by operator of the MSSVs induces a crash cooldown for the primary temperature and pressure and then the eventual lack of heat sink induces some temperature increases. On the contrary for the case when MSSVs are cycled until the SGs are depressurized, the temperatures have small increases in case of lack of heat sinks, but then the fact that the moderator is at low temperature and pressure makes the moderator to act as a successfully ultimate heat sink.

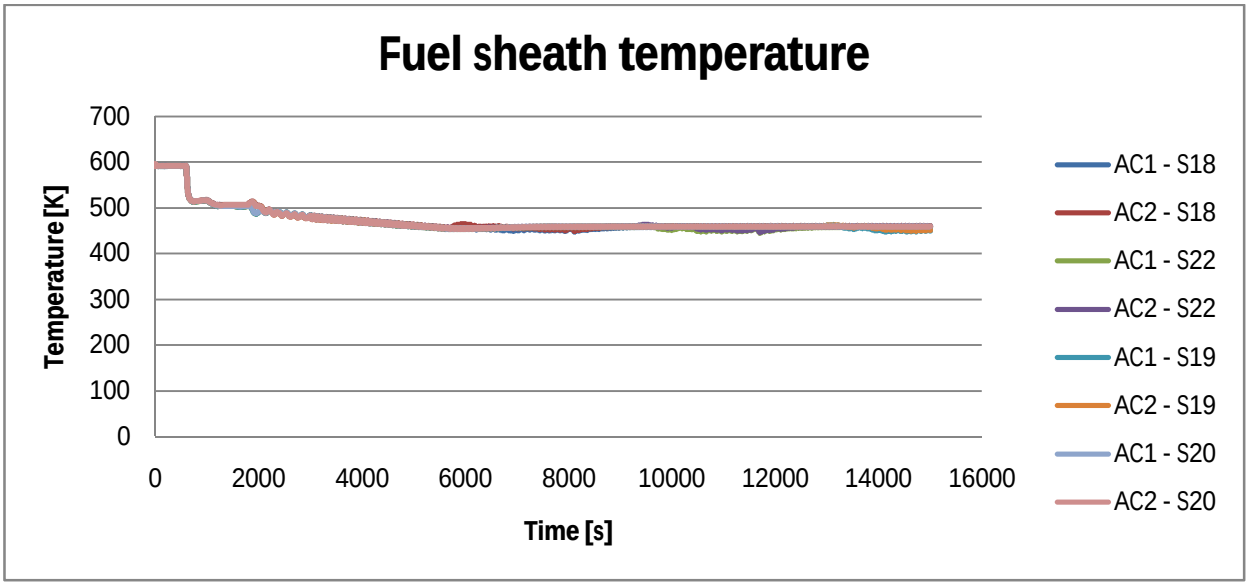


Figure 3.30 Fuel sheath temperature – MSSVs cycling

The Figure 3.31 shows the PHTS coolant (D2O) temperature variations along with the possible scenarios that might occur. It is shown that in case the heat sink is missing, then the temperature increases but not drastically, the moderator present in calandria vessel act as a ultimate heat and cuts successfully the eventual temperature rise.

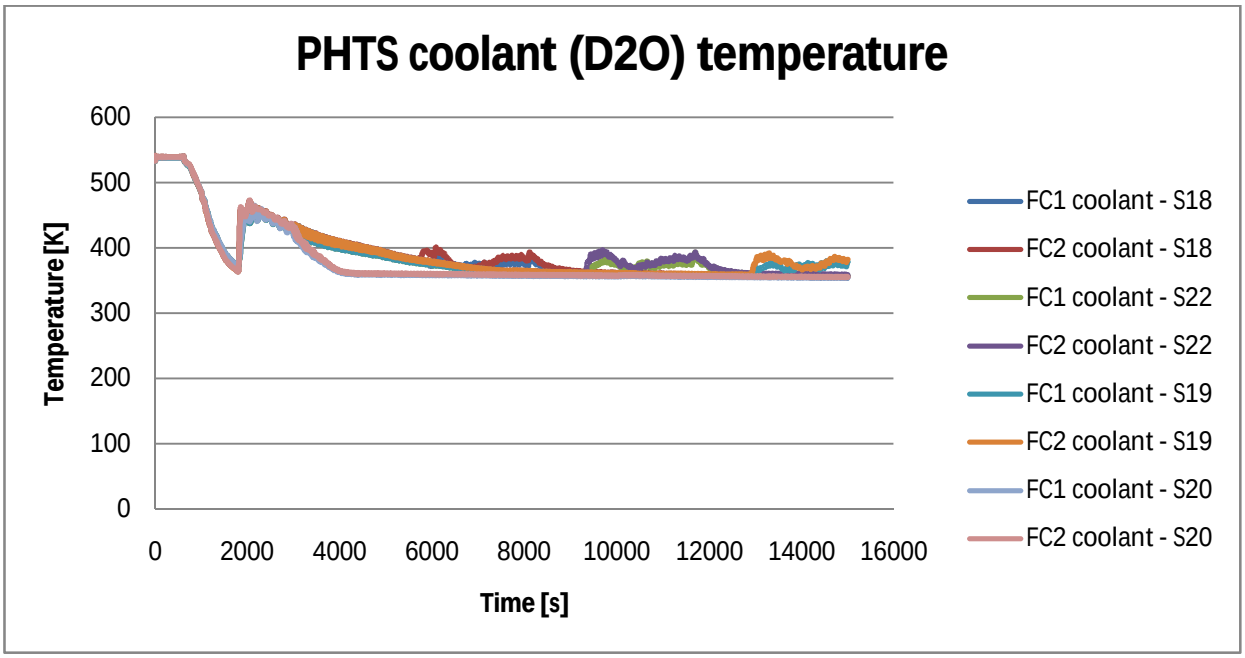


Figure 3.31 PHTS coolant (D2O) temperature – MSSVs cycling

3.6 Conclusions

The potential and interest of the present approach in comparison with the classical PSA approach is given by the methodology itself that uses the dynamic Event-Decision Trees. This allows raising sequences of possible events related in cause-consequence reasoning, each one giving place to a scenario with its development and its consequences. The latter is valid when very complex interactions take place between software-hardware and operator actions. So we can acquire the knowledge not only of which sequences of events are taking place, but also of the real environment in which they are taking place.

Coupling the two different outputs (e.g. deterministic and logic-probabilistic) it can be obtained a full representation of the system operational states, as well as all the possible occurring patterns that are expressed in a set of mutually self excluding sequences. Availability of the full set of alternatives allows the complete spectrum of probability-consequence conditions to be used as a basis of decision making process in order to mitigate and control risk with measures such as up-graded plant operating procedures, adding redundancy of protective equipment, and adding front line systems, and so on.

The possibility to interface the logic probabilistic model of a system with a process simulator allows the assessment of the status of each relevant process variable with reference to the failure sequence identified. In addition, this permits the mutual interactions of the hardware components and the physical evolution of the plant to be taken into account [6].

Further the methodology proposed makes possible revealing situations where the correct intervention of protective equipment or operator actions could bring even to unexpected events.

In particular, the present Dynamic PSA approach might be very useful in support of power plant safety improvements, either in plant hardware or in operating procedures.

No specific results have been yield following the first application due to lack of consistent and detailed input data in regard to system operation and configuration. The thermal-hydraulic model of the CANDU 6 reactor design and the associated transient phenomenology has been well reflected and consequently the results confirmed and stressed the importance of emergency water supply in both short and long term. However, it should be taken into account that very conservative assumptions have been considered for the thermal-hydraulic model of the CANDU6 design and a further reconsideration of them would give generous increase of the safety margins and grace periods observed along the calculations.

The results of the second application show that significant time is available for operator action during the Station Blackout accident to arrest the accident progression.

Experiments showed that significant sag of the CANDU fuel channel driven by creep occurs above 800 C degrees, following the accident scenarios that were analyzed; any of them did not reached those temperatures. Since creep deformation is a slow process, the core damage progression in a CANDU 6 core is expected to be a slow process.

Furthermore the progression of a severe core damage accident within the CANDU 6 calandria vessel could be analyzed by use of MELCOR or MAAP4 CANDU code, the latter contains CANDU-specific models, such as horizontal fuel channels within the core, calandria vessel and calandria vault.

The second application confirmed the importance of the moderator and its parameters, i.e. temperature 343 K and pressure of 1 bar, therefore the cold mass inventory of moderator serves as an important heat sink which can avoid or cut eventually temperature increases.

Assuming even total failure of active heat sinks, the moderator inventory of water dramatically slows down the progression of the accident, allowing time for recovery actions to be taken by operators and time for emergency planning.

It is confirmed that the moderator can preserve the fuel channel integrity and prevent gross melting of the UO2 for short and long term severe accident sequences, such as an SBO. In addition, the presence of the shield water around the calandria, (i.e. reactor vault), enables the calandria shell to be cooled and thereby serve for many hours as a core catcher in severe accident scenarios.

The onset of PHTS reaching saturation conditions and furthermore boil off is expected after many hours from the start of the event, [1].

3.7 References

[1] CNCAN, National Report on the Implementation of the Stress Tests, Romania, December 2011

[2] Fundamental Characteristics of CANDU System Thermal hydraulics: Model, Aaron Chiu , Danielle Major, Ishan Roy, Sophie Zhu. University Network of Excellence in Nuclear Engineering, 2010

[3] Safety Aspects of HWRs, IAEA Publications

[4] M.Demichela, N.Piccinini, Integrated Dynamic Decision Analysis: a method for PSA in Dynamic process system, CISAP3, 2008

[5] Approaching Dynamic PSA Within CANDU 6 NPPs, M.Lontos, M.Mazzini, D.Mazzini, 18th International Conference on Nuclear Engineering (ICONE18) ,May 17–21, 2010 , Xi'an, China, ISBN 978-0-7918-4931-6

[6] An application of Dynamic PSA approach to the Emergency Water System of CANDU 6 NPP, M.Lontos, M.Mazzini, D.Mazzini, 17th International Conference on Nuclear Engineering (ICONE 17), July 2009, Brussels, Belgium,

CHAPTER 4

4.1 Introduction

Chapter 4 presents future possible applications that could be developed with the present approach. The application objective could be the optimization of the emergency operating procedures (EOPs) in terms of operator grace windows and not only. The same as the previous applications presented in chapter 3, the approach consists in coupling the logic-probabilistics of the plant configurations corresponding to the Emergency Operating Procedures (EOPs) and the associated phenomenology of the primary heat transport systems with the consideration of the plant safety systems.

Emergency operating procedures (EOPs) are essential for maintaining the fundamental safety functions and for preventing core damage during both design basis accidents and beyond design basis accidents in nuclear power plants (NPPs), [1]. Emergency operating procedures (EOPs) in nuclear plants guide operators in handling significant process disturbances. In EOPs operators are required to simply follow the procedures without diagnosing the cause of the emergency situations. This means that the quality of EOPs is one of the most decisive factors in determining the safety of the plant.

The development of such an application could highlight those situations where the plant fails either because of hardware failures or system dynamics and reveal those situations where changing of the hardware states brings the process variables of the system state out of the system domain.

A timeline course needs to be created for the most important process variables characterizing the plant state. The timeline course could reveal the time windows that operators have at disposition for intervention, in order to avoid potentially catastrophic conditions.

The IDDA methodology can be utilized to identify how certain postulated top events may occur in a given system. The result is a set of prime implicants that represent system faults resulting from diverse combinations of possible system parameter, operator error and/or component state.

The associated plant phenomenology could be obtained from the usual deterministic codes employed in deterministic safety analysis. The code should be linked to IDDA in order to determine the evolution of each generated scenario.

4.2 The approach description

The approach itself provides in general the framework of the integrated safety analysis. According to reference [2], the integrated safety analysis should provide:

- a description of the structures, equipment, and process active at the facility/installation,
- an identification and systematic analysis of hazards at the facility
- a comprehensive identification of potential accident/event sequences that would result in unacceptable consequences, and the expected likelihoods of those sequences,
- an identification and description of controls (i.e., structures, systems, equipment, or components) that are relied on to limit or prevent potential accidents or mitigate their consequences,
- an identification of measures taken to ensure the availability and reliability of identified safety systems.

Although these techniques were established primarily as tools to analyze process hazards at chemical facilities, they were extended to address radiological and nuclear criticality hazards. Finally the major objectives of the approach are to find the dangerous scenarios in the plant event space, estimating their probability of occurrence.

The approach is briefly described in the following sub-chapters.

4.2.1 The Emergency Operating Procedure scenarios delineation

A tree structured simulation of the EOP scenarios is realized through the use of IDDA code in order to build up the event tree associated to the chosen emergency operating procedure. The number of scenarios generated within the EOP could rise in function of the complexity of transient to tens of thousands. However, applying a cutoff probability (e.g. 1.E-12 cut-off probability used in the classical PSA scenarios truncation) to the scenarios generated within the EOP, then the number of scenarios is reduced to a manageable number that the approach can be easily handled; furthermore this reduces significantly the computational efforts enabling the identification of rare, but potentially high consequence hazards.

The deterministic analysis should provide the trend of the most important process variables that have significant impact on the plant safety and then the parameters evolution is shown in function of time along with the different scenarios that occur for the given plant transient.

The following, Figure 4.1 simply sketches the approach intended for the optimization of the emergency operating procedures.

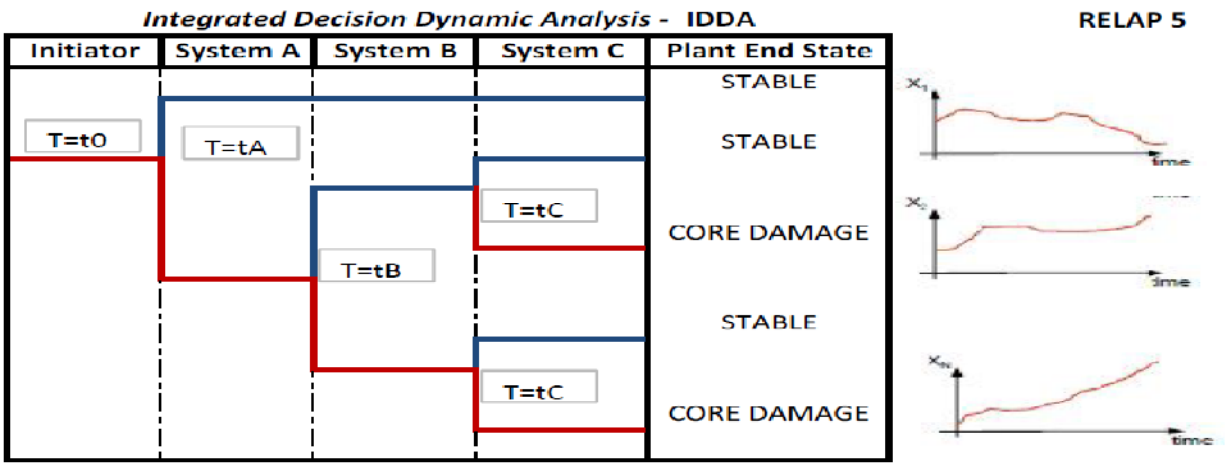


Figure 4.1 Dynamic PSA approach simple sketch

Through the use of IDDA code, the approach follows the traditional PSA techniques for problem decomposition, i.e. event tree, keeping the same overall structure and calculating the same type of results – scenario end state probability of occurrence.

4.2.2 Critical plant safety parameters

Following the deterministic analysis results, for each plant critical safety parameter chosen by the analyst, then the scenarios that are leading to plant/facility failure are identified; moreover the thermal hydraulic model associated confirms that the process variable is over its safety limit and within the failure domain. The correct timing in the successful activation of safety mitigation systems can ensure that the violation of plant safety margins is avoided. Also, the approach confirms that the interaction of physical processes and operator actions in time for the successful activation of the mitigation systems is crucial for plant safety.

The Figure 4.2 sketches what has been described previously.

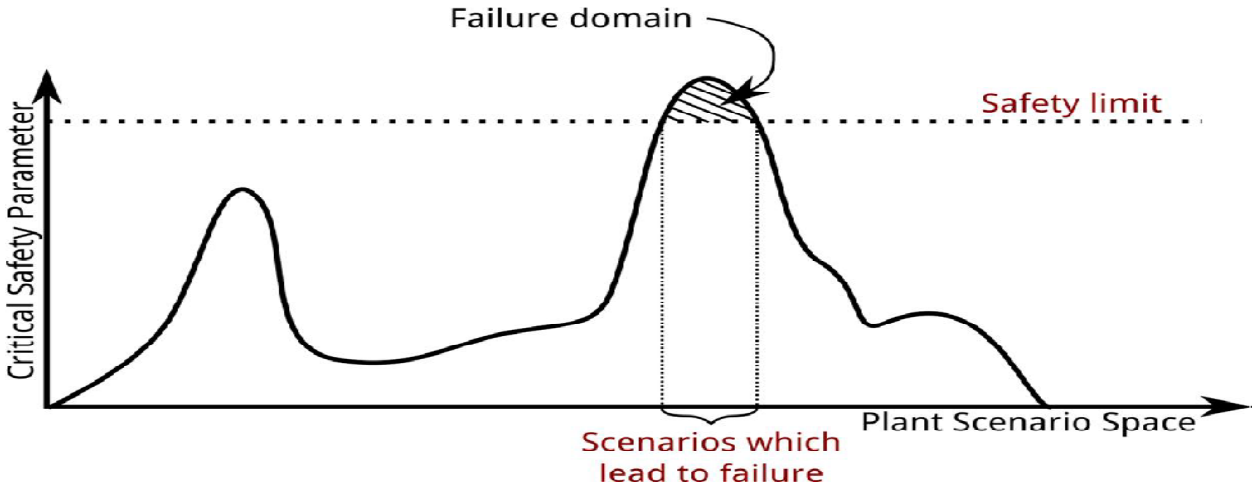


Figure 4.2 Critical safety parameter vs. plant scenario space

4.3 Conclusions

The proposed approach identifies the undesirable events or accidents with high or intermediate consequences and develops the needed safety measures to prevent or exclude the occurrence of such events.

The IDDA methodology could be utilized to identify how certain postulated top events may occur in a given system. The result is a set of prime implicants that represent system faults resulting from diverse combinations of possible system parameter, operator error and/or component state.

One of the results of the approach proposed is the identification of controls, both engineered and administrative, that are needed to limit or prevent accidents or mitigate their effects.

Application of methodology requires complete and consistent supporting analyses and data as well as a system model describing the system behavior under normal and upset conditions (e.g. process simulator). The high complexity of these modules makes that only experimental versions have been developed so far.

Once the dynamic PSA application provides some valuable insights on the system and process in subject, those further can be integrated and supplementary given to the Event Tree model. The results obtained could either complement the existing information; either to supplement the initial ET model.

Following the Fukushima events it appeared imperious the necessity for plant operators to develop new emergency operating procedures for response to Station Blackout and to total and extended loss of the spent fuel pool cooling system events. The application of the approach described in present chapter could help in improving and strengthening the development of the new emergency operating procedures since their very early phase. Using dynamic PSA approach the nuclear facilities and industrial installations can achieve and demonstrate safety in an effective and efficient manner.

The chemical industry has performed a number of dynamic/integrated safety analyses on process facilities, but because these studies contain proprietary information, few have been published or only cited in the open existing literature.

However the developments that could be carried out in the direction of the present work would be to consider the creation of an automatic tool in the way that IDDA commands RELAP5 scenarios to be analyzed and other way around.

4.4 References

[1] Development and Review of Plant Specific Emergency Operating Procedures, Safety Reports Series 48, IAEA

[2] Integrated Safety Analysis Guidance Document, NUREG 1513, May 2001

CHAPTER 5

The present work was intended to be an attempt in approaching Dynamic PSA. As the chapter 1 has shown there were many attempts and many methodologies proved to bring to some extents to the development of dynamic PSA. Even if its development commenced many years ago, beginning of 80ies, the applications and the applicability remained at the level of R&D, without any particular industrial application, so far.

The currently methodology employed for approaching the dynamic PSA did the use of codes coupling such as RELAP5 and IDDA. The application environment had considered the generic CANDU 6 plant design, in particular the PHTS response in case of plant specific accidents.

The applications proposed in the present work have shown the potentiality of tools involved and of such an approach and due to the lack of official data input in regard to the system/plant configuration and operation did not yield relevant results in terms of CANDU 6 design, but did confirmed the robustness of the plant in facing a beyond design basis accident, such as a Station Blackout.

The methodology proposed is not intended to replace the classical PSA method, but to complement it when is needed, for instance when too much conservative assumptions are involved. The classical PSAs models considered for the current operating nuclear power plants involve the different power operational states that need to be considered, i.e. at power and low power shutdown conditions. Often the plant power operational states should be split in order to consider the different plant configurations and/or plant conditions (e.g. the case of uncontrolled level drop with RPV head off and head on for PWR design), but the common PSA practice is to consider the configuration with the worse consequences. In this manner the intended scope of PSA to be a best estimate tool is not anymore preserved and introduces additional conservativeness. Following the coupling between the deterministic and probabilistic analysis could be identified those sleeping threats that usually stay in the residual risk, and could address the uncertainty that the analyst has it present, and in particular if the accident scenarios are the ones right addressed and what is the risk in using bounding conservative accident assumptions. In fact, the well known limitations of the classical PSA methodology could be used as useful case studies for the Dynamic PSA such as the modeling of logical loops.

So far, due to the fact that the collaboration between the plant operators and parties involved in the R&D dedicated to this topic is rather laking, the identification of risk-significant accident situations is not obtainable by the traditional approaches (e.g. DSA, PSA).

The applications developed and the future developments, in case data is made available, proofs the fact that the set of codes that constitutes IDDA analysis methodology is a very articulate system that has the right answers to almost all analysis requests and needs.

Also it should be mentioned that the current methodology has been designed for complex situations, such as hardware/software and operator actions, and actually in those the code shows its real potentialities. The types of results that could be provided in the conditions of valid

input data could have a great importance to orient the course of the analysis or to be considered as valuable inputs for the decision making process. But still, the present applications have proved only partly the potentialities of the IDDA code, mainly the most important features, and there are still features that were not presented due to the lack of space and scope of the applications of the current work.

The first application has shown that the same type of results in terms of system unavailability could be obtained by making use of IDDA code and not of the classical Fault Trees analysis. Moreover in the same application, has been shown the potentiality that IDDA code has in considering the possibility of risk analysis. The fact that different types of consequences could be associated to the random levels (i.e. basic events) could be a very valuable input for decision making situations when requested, as is the case of long term accident scenarios, plant outage periods, improvement of plant technical specifications in terms of Allowed Outage Times or/and Surveillance In service Testing, and so on.

The second and third applications have shown that the coupling between the deterministic and probabilistic models allowed raising sequences of possible events related in cause-consequence reasoning, with each one giving place to a scenario with its development and its consequences. Therefore to have the possibility to acquire the knowledge not only of which sequences of events are taking place, but also of the real environment in which they are taking place.

Hence, coupling the two different results it can be obtained the full representation of the system operational states, as well as all the possible occurring patterns that are expressed in a set of mutually self excluding sequences, that further allows the complete spectrum of probability-consequence conditions to be used as a basis of decision making process in order to mitigate and control risk with measures such as addition of redundancy on the protective equipment/ front line systems, up-graded plant operating procedures, improvement treatment of the operator actions and so on.

The possibility to interface the logic probabilistic model of a system with a process simulator allows the assessment of the status of each relevant process variable with reference to the failure sequence identified. In addition, this permits the mutual interactions of the hardware components and the physical evolution of the plant to be taken into account.

The application presented in chapter 4 as future development for the optimization of the plant EOPs could addresses the plant scenario space with time dependent events and plant state parameters, therefore addressing a more realistic structure of EOP and/or event trees.

The complementarities that exist between the deterministic and probabilistic analysis, i.e. the fact that the DSA identifies the safety margins but the accident sequences analyzed are only few and then the fact that PSA does not provide any information about safety margins, but considers the spectrum of many accident scenarios makes the development of Dynamic PSA necessary and needed in order to provide exhaustiveness in regards to the safety analysis of

the plant. Furthermore the consideration of such an approach gives the right frame of risk informed safety margins.

All the enumerated advantages could surely improve the plant emergency preparedness, give a more effective risk-informed regulation and an increased robustness of safety assessment.

However so far the present developments in the direction of dynamic PSA proved the high complexity of the models and not yet applied for industrial purposes, that currently only experimental versions have been developed. The best progress of the issue has been registered by the Spanish nuclear safety authority, CSN, that involved the participation of universities, research institutes and has started the work in the beginning of 80ies. The purpose of CSN was to develop an independent safety analysis review tool, such as DPSA that mainly delineates the ETs submitted in the frame of Spanish PSA studies.

Along with the many challenges that the dynamic PSA has to face in order to become applicable and worth considering it, the main question that remains still open for the industry is actually the cost-efficiency of considering the application or non-application of such methodologies for industrial purposes.

ANNEX A

:Start of analysis -Total Loss of Feed-water (2 main pumps + 1 auxiliary pump)

1 1. 0. 0 2 3 'IE' 'dnOccur' 'Occurs'

:Miscalibration error of the SG pressure detectors

;as the miscalibration error has higher failure rate than the sensor failure rate, the latter is not considered

2 3.E-02 0.795 3 15 3 'Pre.Sens' 'Calibr.' 'Mis.Calb'

: Main Steam Safety Valves open sure, there is no doubt, therefore no failure rate is assigned

3 0. 0. 4 4 3 'MSSVs' 'Success' 'Failure'

: Pressure on the secondary side of SG is below 3.45 bar

4 0. 0. 5 5 3 '3.45bar' 'Success' 'Failure'

:Dousing Tank fails - External large leak

5 9.43E-07 0.720 6 80 3 'DTank' 'No Leak' 'Leaks'

24 8 0. 0.

:PV41 fails to open, because the transient occurs during maintainance period of PV41

6 1.E-06 0.795 7 80 3 'PV41MNT' 'No.MNTC' 'MNTC'

:SV41 fails to open

7 5.E-3 0.720 8 80 3 'SV41' 'Works' 'dnWork'

:PV41 properly failure to open

8 1.11E-03 0.466 9 80 3 'PV41PF' 'Open' 'dnOpen'

;**********Water supply**********

:PV7 fails to open, because the transient occurs during maintainance period of PV7

9 1.E-6 0.795 10 901 3 'PV7MNT' 'No.MNTC' 'MNTC'

```
:SV7 fails to open
10  5.E-3   0.720   11  17  3  'SV7'  'Works'  'dnWork'
:PV7 properly failure to open
11  1.11E-03  0.466   12  901  3  'PV7PF'  'Open'  'dnOpen'
16  8  0.  0.
:CV49 failure to open
12  1.3E-05  0.720  100  901  3  'CV49.O'  'Open'  'dnOpen'
;*********************************PV41/7 Actuation ****************************
;operator action that actuates PV41 from MCR, therefore has to use the HS41
;is it assumed that he receives all necessary inputs, alarms
:Operator error to actuates PV41 HS41 from MCR
15  1.E-02  0.795  16  80  3   'HS41.HE'   'Success'   'Failure'
:HS41 does it work
16  1.E-04  0.520  8   80  3  'HS41'  'Works'  'DnWorks'
:Operator error to actuates the PV7 HS7 from MCR
17  1.E-03  0.795  18  901  3  'HS7.HE'  'Success'   'Failure'
:HS7 does it work
18  1.E-04  0.520  11  901  3  'HS7'  'Works'  'DnWorks'
;*******************************EWS Pumped*****************************************
: Field operator starts 1/2 EWS pumps
80  6.E-03  0.795  90  901  3  'EWSPs.HE'  'Success'   'Failure'
:P1 fails to start due to maintainance period
90  1.E-06  0.520  105  260  3  'P1.MNTC'  'No.MNTC'  'MNTC'
:P1 failure to start due to CCF
105  8.E-05  0.520   110  260   3  'P1Fs.CCF'  'No.CCF'  'CCF'
```

```
24   260  0.  0.
:P1 failure to start
110  2.23E-03  0.497   120   260  3  'P1Fst'  'Start'  'dnStart'
24  150  0.  0.
24  160  0.  0.
15  260  0.  0.
:P1 failure to run due to CCF
120  8.4E-05  0.520   130  260  3  'P1Fr.CCF'  'No.CCF'  'CCF'
24   280  0.  0.
:P1 failure to run
130  1.0E-04  0.375  140  260  3   'P1Frun'  'Run'  'dnRun'
15   280  0.  0.
:V9V11 CCF failure to open
140  2.47E-06  0.520  150  260  3  'V9V11CCF'  'No.CCF'  'CCF'
:CV9 fails to open
150  1.3E-05  0.720  160  260  3  'CV9.O'  'Open'  'dnOpen'
15   300  0.  0.
:V10  fails to open
160  2.5E-03  0.795  170  260  3   'SV10.O'  'Open'  'dnOpen'
:V45 failure to close
170  7.0E-05  0.720   180  190  3  'V45.C'  'Close'  'dnClose'
:V44 failure to open
180  1.30E-05  0.720   11  901  3  'V44.O'  'Open'  'dnOpen'
:V47 failure to close
190  7.0E-05  0.720   180  901  3  'V47.C'  'Close'  'dnClose'
```

```
:P2 failure to start due to CCF
260  8.0E-05  0.520  270   901   3  'P2Fs.CCF'  'No.CCF'  'CCF'
:P2 properly failure to start
270  1.9E-2  0.497   280  901   3  'P2Fst'  'Start'  'dnStart'
24   310  0.  0.
24   320  0.  0.
:P2 failure to run due to CCF
280  8.4E-05  0.520   290  901   3  'P2Fr.CCF'  'No.CCF'  'CCF'
:P2  failure to run
290  1.08E-04  0.375   300  901    3   'P2Frun'  'Run'  'dnRun'
:CCF to open of both V9V11
300  2.47E-06  0.520   310  901  3  'V11V9CCF'  'No.CCF'  'CCF'
:V11 failure to open
310  1.30E-05  0.720   320  901  3  'CV11.O'  'Open'  'dnOpen'
:V12 failure to open
320  2.5E-03  0.795   170  901  3  'SV12.O'  'Open'  'dnOpen'
;**********************************END STATES**************************************
:EWS  Failure
901  1.  0.  0   0   3  'EWS'  '  '  'Failure'
:EWS  Success
100  0.  0.  0   0   3  'EWS'  'Success'  '  '
;*****************************END of INPUT*****************************************
```

ANNEX B

FILE NAME : proba2.INP STARTING LEVEL : 1

1 Start of analysis -Total Loss of Feed-water (2 main pumps + 1 aux

[IE] [dnOccur] [Occurs]

Statement : [Occurs !]

If [dnOccur] Then End

If [Occurs] Then Following Event is : 2 [Pre.Sens]-[Calibr.]-[Mis.Calb]

---

2 Miscalibration error of the SG pressure detectors

[Pre.Sens] [Calibr.] [Mis.Calb]

Question : [Calibr. ?] or [Mis.Calb?]

If [Calibr.] Then Following Event is : 3 [MSSVs]-[Success]-[Failure]

If [Mis.Calb] Then Following Event is : 15 [HS41.HE]-[Success]-[Failure]

---

3 Main Steam Safety Valves open sure, there is no doubt, therefore

[MSSVs] [Success] [Failure]

Statement : [Success !]

If [Success] Then Following Event is : 4 [3.45bar]-[Success]-[Failure]

If [Failure] Then Following Event is : 4 [3.45bar]-[Success]-[Failure]

---

4 Pressure on the secondary side of SG is below 3.45 bar

[3.45bar] [Success] [Failure]

Statement : [Success !]

If [Success] Then Following Event is : 5 [DTank]-[No Leak]-[Leaks]

If [Failure] Then Following Event is : 5 [DTank]-[No Leak]-[Leaks]

---

5 Dousing Tank fails - External large leak

[DTank] [No Leak] [Leaks]

Question : [No Leak ?] or [Leaks ?]

If [No Leak] Then Following Event is : 6 [PV41MNT]-[No.MNTC]-[MNTC]

If [Leaks] Then Following Event is : 80 [EWSPs.HE]-[Success]-[Failure]

If [Leaks] Then it forces EVENT 8 on: ([PV.41.PF]-[dnOpen])

---

6 PV41 fails to open, because the transient occurs during maintaina

[PV41MNT] [No.MNTC] [MNTC]

Question : [No.MNTC ?] or [MNTC ?]

If [No.MNTC] Then Following Event is : 7 [SV.41]-[Works]-[dnWork]

If [MNTC] Then Following Event is : 81 [SV.141]-[Works]-[dnWork]

---

7 SV41 fails to open

[SV.41] [Works] [dnWork]

Question : [Works ?] or [dnWork ?]

If [Works] Then Following Event is : 8 [PV.41.PF]-[Open]-[dnOpen]

If [dnWork] Then Following Event is : 81 [SV.141]-[Works]-[dnWork]

---

8 PV41 failure to open

[PV.41.PF] [Open] [dnOpen]

Question : [Open ?] or [dnOpen ?]

If [Open] Then Following Event is : 9 [PV7.MNT]-[No.MNTC]-[MNTC]

If [dnOpen] Then Following Event is : 81 [SV.141]-[Works]-[dnWork]

---

81 SV141 fails to open

[SV.141] [Works] [dnWork]

Question : [Works ?] or [dnWork ?]

If [Works] Then Following Event is : 82 [PV141.PF]-[Open]-[dnOpen]

If [dnWork] Then Following Event is : 80 [EWSPs.HE]-[Success]-[Failure]

---

82 PV141 failure to open

[PV141.PF] [Open] [dnOpen]

Question : [Open ?] or [dnOpen ?]

If [Open] Then Following Event is : 9 [PV7.MNT]-[No.MNTC]-[MNTC]

If [dnOpen] Then Following Event is : 80 [EWSPs.HE]-[Success]-[Failure]

---

9 Event

[PV7.MNT] [No.MNTC] [MNTC]

Question : [No.MNTC ?] or [MNTC ?]

If [No.MNTC] Then Following Event is : 10 [SV.7]-[Works]-[dnWork]

If [MNTC] Then Following Event is : 58 [SV107]-[Works]-[dnWork]

---

10 SV7 fails to open

[SV.7] [Works] [dnWork]

Question : [Works ?] or [dnWork ?]

If [Works] Then Following Event is : 11 [PV.7.PF]-[Open]-[dnOpen]

If [dnWork] Then Following Event is : 58 [SV107]-[Works]-[dnWork]

---

11 PV7 properly failure to open

[PV.7.PF] [Open] [dnOpen]

Question : [Open ?] or [dnOpen ?]

If [Open] Then Following Event is : 12 [CV49.O]-[Open]-[dnOpen]

If [dnOpen] Then Following Event is : 58 [SV107]-[Works]-[dnWork]

If [Open] Then it forces EVENT 8 on: ([PV.41.PF]-[dnOpen])

---

58 SV107 fails to open

[SV107] [Works] [dnWork]

Question : [Works ?] or [dnWork ?]

If [Works] Then Following Event is : 59 [PV107PF]-[Open]-[dnOpen]

If [dnWork] Then Following Event is : 17 [HS7.HE]-[Success]-[Failure]

---

59 PV107 properly failure to open

[PV107PF] [Open] [dnOpen]

Question : [Open ?] or [dnOpen ?]

If [Open] Then Following Event is : 12 [CV49.O]-[Open]-[dnOpen]

If [dnOpen] Then Following Event is : 901 [EWS]-[ ]-[Failure]

---

12 CV49 failure to open

[CV49.O] [Open] [dnOpen]

Question : [Open ?] or [dnOpen ?]

If [Open] Then Following Event is : 100 [EWS]-[Success]-[ ]

If [dnOpen] Then Following Event is : 901 [EWS]-[ ]-[Failure]

---

15 Operator error to actuates PV41 HS41/141 from MCR

[HS41.HE] [Success] [Failure]

Question : [Success ?] or [Failure ?]

If [Success] Then Following Event is : 16 [HS41]-[Works]-[DnWorks]

If [Failure] Then Following Event is : 80 [EWSPs.HE]-[Success]-[Failure]

---

16 HS41/141 does it work

[HS41] [Works] [DnWorks]

Question : [Works ?] or [DnWorks ?]

If [Works] Then Following Event is : 8 [PV.41.PF]-[Open]-[dnOpen]

If [DnWorks] Then Following Event is : 80 [EWSPs.HE]-[Success]-[Failure]

---

17 Operator error to actuates the PV7 HS7/107 from MCR

[HS7.HE] [Success] [Failure]

Question : [Success ?] or [Failure ?]

If [Success] Then Following Event is : 18 [HS7]-[Works]-[DnWorks]

If [Failure] Then Following Event is : 901 [EWS]-[ ]-[Failure]

---

18 HS7/107 does it work

[HS7] [Works] [DnWorks]

Question : [Works ?] or [DnWorks ?]

If [Works] Then Following Event is : 59 [PV107PF]-[Open]-[dnOpen]

If [DnWorks] Then Following Event is : 901 [EWS]-[ ]-[Failure]

---

80 Field operator starts 1/2 EWS pumps

[EWSPs.HE] [Success] [Failure]

Question : [Success ?] or [Failure ?]

If [Success] Then Following Event is : 90 [P1.MNTC]-[No.MNTC]-[MNTC]

If [Failure] Then Following Event is : 901 [EWS]-[ ]-[Failure]

---

90 P1 fails to start due to maintainance period

[P1.MNTC] [No.MNTC] [MNTC]

Question : [No.MNTC ?] or [MNTC ?]

If [No.MNTC] Then Following Event is : 105 [P1Fs.CCF]-[No.CCF]-[CCF]

If [MNTC] Then Following Event is : 260 [P2Fs.CCF]-[No.CCF]-[CCF]

---

105 P1 failure to start due to CCF

[P1Fs.CCF] [No.CCF] [CCF]

Question : [No.CCF ?] or [CCF ?]

If [No.CCF] Then Following Event is : 110 [P1Fst]-[Start]-[dnStart]

If [CCF] Then Following Event is : 260 [P2Fs.CCF]-[No.CCF]-[CCF]

If [CCF] Then it forces EVENT 260 on: ([P2Fs.CCF]-[CCF])

---

110 P1 failure to start

[P1Fst] [Start] [dnStart]

Question : [Start ?] or [dnStart ?]

If [Start] Then Following Event is : 120 [P1Fr.CCF]-[No.CCF]-[CCF]

If [dnStart] Then Following Event is : 260 [P2Fs.CCF]-[No.CCF]-[CCF]

If [dnStart] Then it forces EVENT 150 on: ([CV9.O]-[dnOpen])

If [dnStart] Then it forces EVENT 160 on: ([SV10.O]-[dnOpen])

If [Start] Then it forces EVENT 260 on: ([P2Fs.CCF]-[No.CCF])

---

120 P1 failure to run due to CCF

[P1Fr.CCF] [No.CCF] [CCF]

Question : [No.CCF ?] or [CCF ?]

If [No.CCF] Then Following Event is : 130 [P1Frun]-[Run]-[dnRun]

If [CCF] Then Following Event is : 260 [P2Fs.CCF]-[No.CCF]-[CCF]

If [CCF] Then it forces EVENT 280 on: ([P2Fr.CCF]-[CCF])

---

130 P1 failure to run

[P1Frun] [Run] [dnRun]

Question : [Run ?] or [dnRun ?]

If [Run] Then Following Event is : 140 [V9V11CCF]-[No.CCF]-[CCF]

If [dnRun] Then Following Event is : 260 [P2Fs.CCF]-[No.CCF]-[CCF]

If [Run] Then it forces EVENT 280 on: ([P2Fr.CCF]-[No.CCF])

---

140 V9V11 CCF failure to open

[V9V11CCF] [No.CCF] [CCF]

Question : [No.CCF ?] or [CCF ?]

If [No.CCF] Then Following Event is : 150 [CV9.O]-[Open]-[dnOpen]

If [CCF] Then Following Event is : 260 [P2Fs.CCF]-[No.CCF]-[CCF]

---

150 CV9 fails to open

[CV9.O] [Open] [dnOpen]

Question : [Open ?] or [dnOpen ?]

If [Open] Then Following Event is : 160 [SV10.O]-[Open]-[dnOpen]

If [dnOpen] Then Following Event is : 260 [P2Fs.CCF]-[No.CCF]-[CCF]

If [Open] Then it forces EVENT 300 on: ([V11V9CCF]-[No.CCF])

---

160 SV10 fails to open

[SV10.O] [Open] [dnOpen]

Question : [Open ?] or [dnOpen ?]

If [Open] Then Following Event is : 170 [V45.C]-[Close]-[dnClose]

If [dnOpen] Then Following Event is : 260 [P2Fs.CCF]-[No.CCF]-[CCF]

---

170 V45 failure to close

[V45.C] [Close] [dnClose]

Question : [Close ?] or [dnClose ?]

If [Close] Then Following Event is : 180 [V44.O]-[Open]-[dnOpen]

If [dnClose] Then Following Event is : 190 [V47.C]-[Close]-[dnClose]

---

180 V44 failure to open

[V44.O] [Open] [dnOpen]

Question : [Open ?] or [dnOpen ?]

If [Open] Then Following Event is : 11 [PV.7.PF]-[Open]-[dnOpen]

If [dnOpen] Then Following Event is : 901 [EWS]-[ ]-[Failure]

---

190 V47 failure to close

[V47.C] [Close] [dnClose]

Question : [Close ?] or [dnClose ?]

If [Close] Then Following Event is : 180 [V44.O]-[Open]-[dnOpen]

If [dnClose] Then Following Event is : 901 [EWS]-[ ]-[Failure]

---

260 P2 failure to start due to CCF

[P2Fs.CCF] [No.CCF] [CCF]

Question : [No.CCF ?] or [CCF ?]

If [No.CCF] Then Following Event is : 270 [P2Fst]-[Start]-[dnStart]

If [CCF] Then Following Event is : 901 [EWS]-[ ]-[Failure]

---

270 P2 properly failure to start

[P2Fst] [Start] [dnStart]

Question : [Start ?] or [dnStart ?]

If [Start] Then Following Event is : 280 [P2Fr.CCF]-[No.CCF]-[CCF]

If [dnStart] Then Following Event is : 901 [EWS]-[ ]-[Failure]

If [dnStart] Then it forces EVENT 310 on: ([CV11.O]-[dnOpen])

If [dnStart] Then it forces EVENT 320 on: ([SV12.O]-[dnOpen])

---

280 P2 failure to run due to CCF

[P2Fr.CCF] [No.CCF] [CCF]

Question : [No.CCF ?] or [CCF ?]

If [No.CCF] Then Following Event is : 290 [P2Frun]-[Run]-[dnRun]

If [CCF] Then Following Event is : 901 [EWS]-[ ]-[Failure]

---

290 P2 failure to run

[P2Frun] [Run] [dnRun]

Question : [Run ?] or [dnRun ?]

If [Run] Then Following Event is : 300 [V11V9CCF]-[No.CCF]-[CCF]

If [dnRun] Then Following Event is : 901 [EWS]-[ ]-[Failure]

---

300 CCF to open of both V9V11

[V11V9CCF] [No.CCF] [CCF]

Question : [No.CCF ?] or [CCF ?]

If [No.CCF] Then Following Event is : 310 [CV11.O]-[Open]-[dnOpen]

If [CCF] Then Following Event is : 901 [EWS]-[ ]-[Failure]

---

310 V11 failure to open

[CV11.O] [Open] [dnOpen]

Question : [Open ?] or [dnOpen ?]

If [Open] Then Following Event is : 320 [SV12.O]-[Open]-[dnOpen]

If [dnOpen] Then Following Event is : 901 [EWS]-[ ]-[Failure]

---

320 V12 failure to open

[SV12.O] [Open] [dnOpen]

Question : [Open ?] or [dnOpen ?]

If [Open] Then Following Event is : 170 [V45.C]-[Close]-[dnClose]

If [dnOpen] Then Following Event is : 901 [EWS]-[ ]-[Failure]

---

901 EWS Failure

[EWS] [ ] [Failure]

Statement : [Failure !]

If [ ] Then End

If [Failure] Then End

---

100 EWS Success

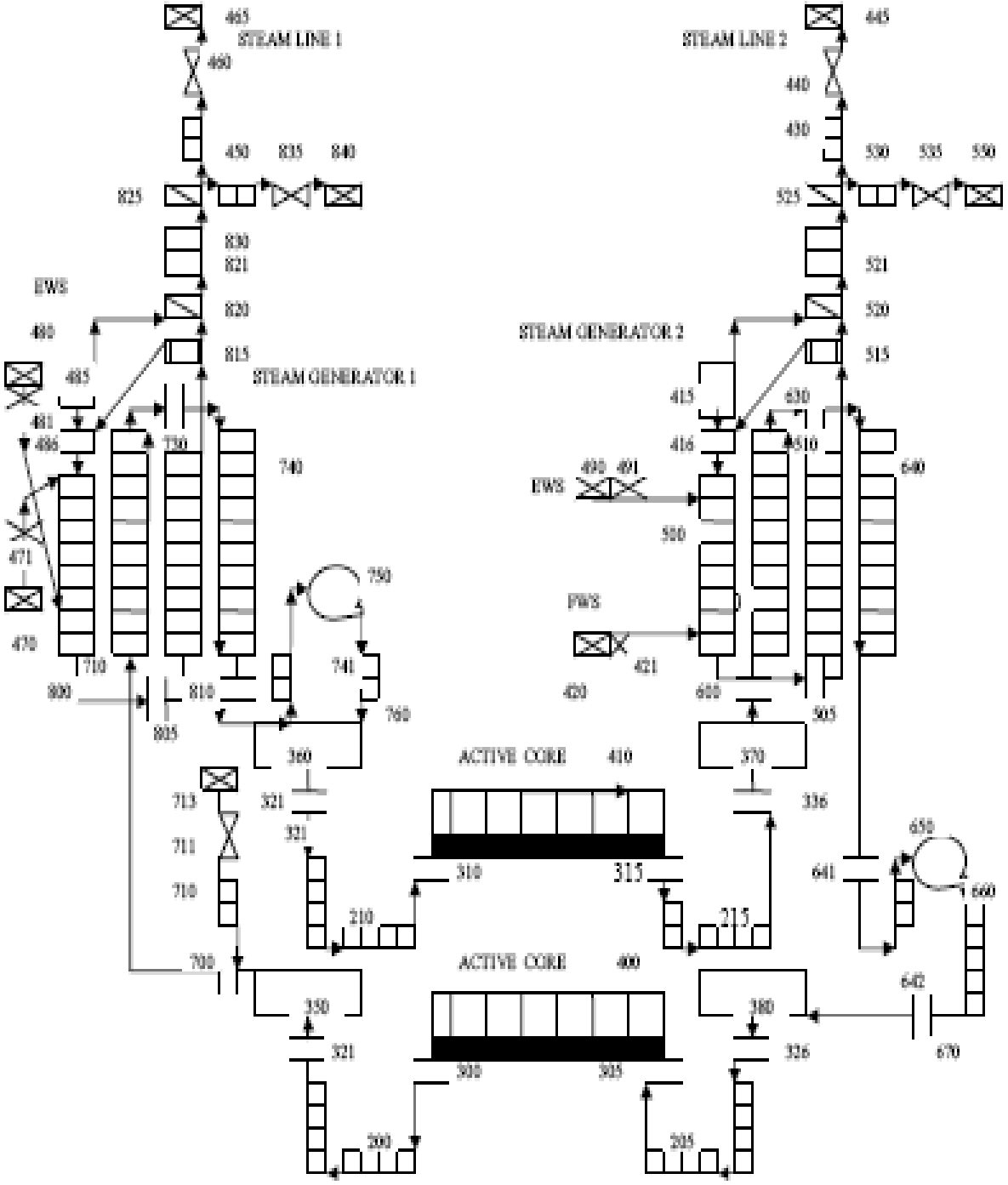
[EWS] [Success] [ ]

Statement : [Success !]

If [Success] Then End

If [ ] Then End

ANNEX C


465
STEAM LINE 1
460
450
835
840
825
830
821
EWS
820
480
815
485
STEAM GENERATOR 1
481
730
740
486
471
750
470
710
741
800
810
760
805
360
ACTIVE CORE
410
713
321
321
711
310
315
710
210
215
700
ACTIVE CORE
400
350
380
321
326
300
305
200
205
445
STEAM LINE 2
440
430
530
535
550
525
521
520
STEAM GENERATOR 2
515
415
630
416
510
640
490
491
EWS
550
PWS
421
420
600
505
570
336
650
641
660
642
670

ANNEX D

EXAMPLE OF FORTRAN SUBROUTINE PIECEWISE POLYNOM FIT.FOR

```
$STORAGE:2
$FLOATCALLS


      SUBROUTINE DOWNCC

      INTEGER      I
      REAL         Q1,Q2,L0,L,T,DT
      CHARACTER*14 TFIL1
      LOGICAL      FL1,FQ1,FQ2

      COMMON/FLG/FL1,FQ1
      COMMON/CHR/TFIL1

      Q1 = 30.
      Q2 = 7.
      L0 = 16.
      FQ2  = .TRUE.


    CALL CONCAT(TFIL1,'.GRF')
    OPEN(1,FILE=TFIL1,STATUS='NEW')

      I = 0
      T = 0.
      DT = 1.
      L  = L0

10     CONTINUE

       WRITE(1,11000)  T,L

      IF (T.GE.751.)  GOTO 100

      IF (T.LT.309.) THEN
      L = L0
      END IF

      IF (T.GE.310..AND.T.LE.420.) THEN
```

```
      L = -0.0996*T + 43.39
      ENDIF

      IF (T.GT.420..AND.T.LE.1500.) THEN
      L = 0.006*T - 1.8525
      ENDIF

      IF (.NOT.FQ1.AND.T.EQ.150) THEN
      L = L0
      ENDIF

     IF (.NOT.FQ1.AND.T.GT.150..AND.T.LE.751.) THEN
     L = - 3.09*T + 16
     END IF

     I = I+1
    T = I*DT
    GOTO 10

 100   CONTINUE
       CLOSE (1)
       IF (L.LT.1.)         THEN
          WRITE(0,10100)
       ELSEIF (L.GT.1.)     THEN
          WRITE(0,10101)

      ENDIF

11000 FORMAT(2(5X,1PE13.6))
10100 FORMAT(//,5X,'EWS FAILURE !!!',//)
10101 FORMAT(//,5X,'EWS SUCCES !!!',//)


      END
```

ANNEX E

1 1. 0. 2 2 3 'SBO' 'Dn-Occur' 'Occurs'

2 0. 0. 4 4 3 'SCRAM' 'Success' 'Failure'

4 5.E-2 0. 6 90 3 'OpA-MSSV' 'Success' 'Failure'

90 5.E-4 0. 6 900 3 'MSSV-Cyc' 'Success' 'Failure'

6 0. 0. 10 10 3 '3.45bar' 'Success' ' '

10 1.26E-4 0. 100 20 3 'EWS-ST' 'Success' 'Failure'

20 5.E-4 0. 22 30 3 'Gridrec1' 'YES' 'NO'

22 5.E-3 0. 100 50 3 'AFW-pump' 'Success' 'Failure'

12 30 0. 0.

12 40 0. 0.

30 1.E-3 0. 22 40 3 'Gridrec2' 'YES' 'NO'

40 5.E-3 0. 22 50 3 'Gridrec3' 'YES' 'NO'

50 5.E-3 0. 60 900 3 'MobileDG' 'Success' 'Failure'

60 5.E-3 0. 100 900 3 'EWS-pump' 'Success' 'Failure'

900 1. 0. 0 0 3 'R FUSION' ' ' 'OCCURS'

100 0. 0. 0 0 3 'NPPSTATE' 'SUCCESS' ' '

ANNEX F

CONST. sborec.PUN of PARTITION sborec.OUT

CONSTITUENT Ordinal : 1

1 SBO Occurs - V 1.0000E+00

2 SCRAM Success + V 1.0000E+00

4 OpA-MSSV Success + 9.5000E-01 5.0000E-02

6 3.45bar Success + V 9.5000E-01

10 EWS-ST Success + 9.4988E-01 1.2600E-04

100 NPPSTATE SUCCESS + V 9.4988E-01

PROBABILITY equal to : 9.4988E-01

CONSTITUENT Ordinal : 2

1 SBO Occurs - V 1.0000E+00

2 SCRAM Success + V 1.0000E+00

4 OpA-MSSV Success + 9.5000E-01 5.0000E-02

6 3.45bar Success + V 9.5000E-01

10 EWS-ST Failure - 1.1970E-04 1.2600E-04

20 Gridrec1 YES + 1.1964E-04 5.0000E-04

22 AFW-pump Success + 1.1904E-04 5.0000E-03

100 NPPSTATE SUCCESS + V 1.1904E-04

PROBABILITY equal to : 1.1904E-04

CONSTITUENT Ordinal : 3

1 SBO Occurs - V 1.0000E+00

2 SCRAM Success + V 1.0000E+00

4 OpA-MSSV Success + 9.5000E-01 5.0000E-02

6 3.45bar Success + V 9.5000E-01

10 EWS-ST Failure - 1.1970E-04 1.2600E-04

20 Gridrec1 YES + 1.1964E-04 5.0000E-04

22 AFW-pump Failure - 5.9820E-07 5.0000E-03

50 MobileDG Success + 5.9521E-07 5.0000E-03

60 EWS-pump Success + 5.9223E-07 5.0000E-03

100 NPPSTATE SUCCESS + V 5.9223E-07

PROBABILITY equal to : 5.9223E-07

CONSTITUENT Ordinal : 4

1 SBO Occurs - V 1.0000E+00

2 SCRAM Success + V 1.0000E+00

4 OpA-MSSV Success + 9.5000E-01 5.0000E-02

6 3.45bar Success + V 9.5000E-01

10 EWS-ST Failure - 1.1970E-04 1.2600E-04

20 Gridrec1 YES + 1.1964E-04 5.0000E-04

22 AFW-pump Failure - 5.9820E-07 5.0000E-03

50 MobileDG Success + 5.9521E-07 5.0000E-03

60 EWS-pump Failure - 2.9760E-09 5.0000E-03

900 R FUSION OCCURS - V 2.9760E-09

PROBABILITY equal to : 2.9760E-09

CONSTITUENT Ordinal : 5

1 SBO Occurs - V 1.0000E+00

2 SCRAM Success + V 1.0000E+00

4 OpA-MSSV Success + 9.5000E-01 5.0000E-02

6 3.45bar Success + V 9.5000E-01

10 EWS-ST Failure - 1.1970E-04 1.2600E-04

20 Gridrec1 YES + 1.1964E-04 5.0000E-04

22 AFW-pump Failure - 5.9820E-07 5.0000E-03

50 MobileDG Failure - 2.9910E-09 5.0000E-03

900 R FUSION OCCURS - V 2.9910E-09

PROBABILITY equal to : 2.9910E-09

CONSTITUENT Ordinal : 6

1 SBO Occurs - V 1.0000E+00

2 SCRAM Success + V 1.0000E+00

4 OpA-MSSV Success + 9.5000E-01 5.0000E-02

6 3.45bar Success + V 9.5000E-01

10 EWS-ST Failure - 1.1970E-04 1.2600E-04

20 Gridrec1 NO - 5.9850E-08 5.0000E-04

30 Gridrec2 YES + 5.9790E-08 1.0000E-03

22 AFW-pump Success + 5.9491E-08 5.0000E-03

100 NPPSTATE SUCCESS + V 5.9491E-08

PROBABILITY equal to : 5.9491E-08

CONSTITUENT Ordinal : 7

1 SBO Occurs - V 1.0000E+00

2 SCRAM Success + V 1.0000E+00

4 OpA-MSSV Success + 9.5000E-01 5.0000E-02

6 3.45bar Success + V 9.5000E-01

10 EWS-ST Failure - 1.1970E-04 1.2600E-04

20 Gridrec1 NO - 5.9850E-08 5.0000E-04

30 Gridrec2 YES + 5.9790E-08 1.0000E-03

22 AFW-pump Failure - 2.9895E-10 5.0000E-03

50 MobileDG Success + 2.9746E-10 5.0000E-03

60 EWS-pump Success + 2.9597E-10 5.0000E-03

100 NPPSTATE SUCCESS + V 2.9597E-10

PROBABILITY equal to : 2.9597E-10

CONSTITUENT Ordinal : 8

1 SBO Occurs - V 1.0000E+00

2 SCRAM Success + V 1.0000E+00

4 OpA-MSSV Success + 9.5000E-01 5.0000E-02

6 3.45bar Success + V 9.5000E-01

10 EWS-ST Failure - 1.1970E-04 1.2600E-04

20 Gridrec1 NO - 5.9850E-08 5.0000E-04

30 Gridrec2 YES + 5.9790E-08 1.0000E-03

22 AFW-pump Failure - 2.9895E-10 5.0000E-03

50 MobileDG Success + 2.9746E-10 5.0000E-03

60 EWS-pump Failure - 1.4873E-12 5.0000E-03

900 R FUSION OCCURS - V 1.4873E-12

PROBABILITY equal to : 1.4873E-12

CONSTITUENT Ordinal : 9

1 SBO Occurs - V 1.0000E+00

2 SCRAM Success + V 1.0000E+00

4 OpA-MSSV Success + 9.5000E-01 5.0000E-02

6 3.45bar Success + V 9.5000E-01

10 EWS-ST Failure - 1.1970E-04 1.2600E-04

20 Gridrec1 NO - 5.9850E-08 5.0000E-04

30 Gridrec2 YES + 5.9790E-08 1.0000E-03

22 AFW-pump Failure - 2.9895E-10 5.0000E-03

50 MobileDG Failure - 1.4948E-12 5.0000E-03

900 R FUSION OCCURS - V 1.4948E-12

PROBABILITY equal to : 1.4948E-12

CONSTITUENT Ordinal : 10

1 SBO Occurs - V 1.0000E+00

2 SCRAM Success + V 1.0000E+00

4 OpA-MSSV Success + 9.5000E-01 5.0000E-02

6 3.45bar Success + V 9.5000E-01

10 EWS-ST Failure - 1.1970E-04 1.2600E-04

20 Gridrec1 NO - 5.9850E-08 5.0000E-04

30 Gridrec2 NO - 5.9850E-11 1.0000E-03

40 Gridrec3 YES + 5.9551E-11 5.0000E-03

22 AFW-pump Success + 5.9253E-11 5.0000E-03

100 NPPSTATE SUCCESS + V 5.9253E-11

PROBABILITY equal to : 5.9253E-11

CONSTITUENT Ordinal : 11

1 SBO Occurs - V 1.0000E+00

2 SCRAM Success + V 1.0000E+00

4 OpA-MSSV Success + 9.5000E-01 5.0000E-02

6 3.45bar Success + V 9.5000E-01

10 EWS-ST Failure - 1.1970E-04 1.2600E-04

20 Gridrec1 NO - 5.9850E-08 5.0000E-04

30 Gridrec2 NO - 5.9850E-11 1.0000E-03

40 Gridrec3 YES + 5.9551E-11 5.0000E-03

22 AFW-pump Failure - 2.9775E-13 5.0000E-03

50 MobileDG Success + 2.9627E-13 5.0000E-03

60 EWS-pump Success + 2.9478E-13 5.0000E-03

100 NPPSTATE SUCCESS + V 2.9478E-13

PROBABILITY equal to : 2.9478E-13

CONSTITUENT Ordinal : 12

1 SBO Occurs - V 1.0000E+00

2 SCRAM Success + V 1.0000E+00

4 OpA-MSSV Success + 9.5000E-01 5.0000E-02

6 3.45bar Success + V 9.5000E-01

10 EWS-ST Failure - 1.1970E-04 1.2600E-04

20 Gridrec1 NO - 5.9850E-08 5.0000E-04

30 Gridrec2 NO - 5.9850E-11 1.0000E-03

40 Gridrec3 YES + 5.9551E-11 5.0000E-03

22 AFW-pump Failure - 2.9775E-13 5.0000E-03

50 MobileDG Success + 2.9627E-13 5.0000E-03

60 EWS-pump Failure - 1.4813E-15 5.0000E-03

900 R FUSION OCCURS - V 1.4813E-15

PROBABILITY equal to : 1.4813E-15

CONSTITUENT Ordinal : 13

1 SBO Occurs - V 1.0000E+00

2 SCRAM Success + V 1.0000E+00

4 OpA-MSSV Success + 9.5000E-01 5.0000E-02

6 3.45bar Success + V 9.5000E-01

10 EWS-ST Failure - 1.1970E-04 1.2600E-04

20 Gridrec1 NO - 5.9850E-08 5.0000E-04

30 Gridrec2 NO - 5.9850E-11 1.0000E-03

40 Gridrec3 YES + 5.9551E-11 5.0000E-03

22 AFW-pump Failure - 2.9775E-13 5.0000E-03

50 MobileDG Failure - 1.4888E-15 5.0000E-03

900 R FUSION OCCURS - V 1.4888E-15

PROBABILITY equal to : 1.4888E-15

CONSTITUENT Ordinal : 14

1 SBO Occurs - V 1.0000E+00

2 SCRAM Success + V 1.0000E+00

4 OpA-MSSV Success + 9.5000E-01 5.0000E-02

6 3.45bar Success + V 9.5000E-01

10 EWS-ST Failure - 1.1970E-04 1.2600E-04

20 Gridrec1 NO - 5.9850E-08 5.0000E-04

30 Gridrec2 NO - 5.9850E-11 1.0000E-03

40 Gridrec3 NO - 2.9925E-13 5.0000E-03

50 MobileDG Success + 2.9775E-13 5.0000E-03

60 EWS-pump Success + 2.9626E-13 5.0000E-03

100 NPPSTATE SUCCESS + V 2.9626E-13

PROBABILITY equal to : 2.9626E-13

CONSTITUENT Ordinal : 15

1 SBO Occurs - V 1.0000E+00

2 SCRAM Success + V 1.0000E+00

4 OpA-MSSV Success + 9.5000E-01 5.0000E-02

6 3.45bar Success + V 9.5000E-01

10 EWS-ST Failure - 1.1970E-04 1.2600E-04

20 Gridrec1 NO - 5.9850E-08 5.0000E-04

30 Gridrec2 NO - 5.9850E-11 1.0000E-03

40 Gridrec3 NO - 2.9925E-13 5.0000E-03

50 MobileDG Success + 2.9775E-13 5.0000E-03

60 EWS-pump Failure - 1.4888E-15 5.0000E-03

900 R FUSION OCCURS - V 1.4888E-15

PROBABILITY equal to : 1.4888E-15

CONSTITUENT Ordinal : 16

1 SBO Occurs - V 1.0000E+00

2 SCRAM Success + V 1.0000E+00

4 OpA-MSSV Success + 9.5000E-01 5.0000E-02

6 3.45bar Success + V 9.5000E-01

10 EWS-ST Failure - 1.1970E-04 1.2600E-04

20 Gridrec1 NO - 5.9850E-08 5.0000E-04

30 Gridrec2 NO - 5.9850E-11 1.0000E-03

40 Gridrec3 NO - 2.9925E-13 5.0000E-03

50 MobileDG Failure - 1.4963E-15 5.0000E-03

900 R FUSION OCCURS - V 1.4963E-15

PROBABILITY equal to : 1.4963E-15

CONSTITUENT Ordinal : 17

1 SBO Occurs - V 1.0000E+00

2 SCRAM Success + V 1.0000E+00

4 OpA-MSSV Failure - 5.0000E-02 5.0000E-02

90 MSSV-Cyc Success + 4.9975E-02 5.0000E-04

6 3.45bar Success + V 4.9975E-02

10 EWS-ST Success + 4.9969E-02 1.2600E-04

100 NPPSTATE SUCCESS + V 4.9969E-02

PROBABILITY equal to : 4.9969E-02

CONSTITUENT Ordinal : 18

1 SBO Occurs - V 1.0000E+00

2 SCRAM Success + V 1.0000E+00

4 OpA-MSSV Failure - 5.0000E-02 5.0000E-02

90 MSSV-Cyc Success + 4.9975E-02 5.0000E-04

6 3.45bar Success + V 4.9975E-02

10 EWS-ST Failure - 6.2969E-06 1.2600E-04

20 Gridrec1 YES + 6.2937E-06 5.0000E-04

22 AFW-pump Success + 6.2622E-06 5.0000E-03

100 NPPSTATE SUCCESS + V 6.2622E-06

PROBABILITY equal to : 6.2622E-06

CONSTITUENT Ordinal : 19

1 SBO Occurs - V 1.0000E+00

2 SCRAM Success + V 1.0000E+00

4 OpA-MSSV Failure - 5.0000E-02 5.0000E-02

90 MSSV-Cyc Success + 4.9975E-02 5.0000E-04

6 3.45bar Success + V 4.9975E-02

10 EWS-ST Failure - 6.2969E-06 1.2600E-04

20 Gridrec1 YES + 6.2937E-06 5.0000E-04

22 AFW-pump Failure - 3.1469E-08 5.0000E-03

50 MobileDG Success + 3.1311E-08 5.0000E-03

60 EWS-pump Success + 3.1155E-08 5.0000E-03

100 NPPSTATE SUCCESS + V 3.1155E-08

PROBABILITY equal to : 3.1155E-08

CONSTITUENT Ordinal : 20

1 SBO Occurs - V 1.0000E+00

2 SCRAM Success + V 1.0000E+00

4 OpA-MSSV Failure - 5.0000E-02 5.0000E-02

90 MSSV-Cyc Success + 4.9975E-02 5.0000E-04

6 3.45bar Success + V 4.9975E-02

10 EWS-ST Failure - 6.2969E-06 1.2600E-04

20 Gridrec1 YES + 6.2937E-06 5.0000E-04

22 AFW-pump Failure - 3.1469E-08 5.0000E-03

50 MobileDG Success + 3.1311E-08 5.0000E-03

60 EWS-pump Failure - 1.5656E-10 5.0000E-03

900 R FUSION OCCURS - V 1.5656E-10

PROBABILITY equal to : 1.5656E-10

CONSTITUENT Ordinal : 21

1 SBO Occurs - V 1.0000E+00

2 SCRAM Success + V 1.0000E+00

4 OpA-MSSV Failure - 5.0000E-02 5.0000E-02

90 MSSV-Cyc Success + 4.9975E-02 5.0000E-04

6 3.45bar Success + V 4.9975E-02

10 EWS-ST Failure - 6.2969E-06 1.2600E-04

20 Gridrec1 YES + 6.2937E-06 5.0000E-04

22 AFW-pump Failure - 3.1469E-08 5.0000E-03

50 MobileDG Failure - 1.5734E-10 5.0000E-03

900 R FUSION OCCURS - V 1.5734E-10

PROBABILITY equal to : 1.5734E-10

CONSTITUENT Ordinal : 22

1 SBO Occurs - V 1.0000E+00

2 SCRAM Success + V 1.0000E+00

4 OpA-MSSV Failure - 5.0000E-02 5.0000E-02

90 MSSV-Cyc Success + 4.9975E-02 5.0000E-04

6 3.45bar Success + V 4.9975E-02

10 EWS-ST Failure - 6.2969E-06 1.2600E-04

20 Gridrec1 NO - 3.1484E-09 5.0000E-04

30 Gridrec2 YES + 3.1453E-09 1.0000E-03

22 AFW-pump Success + 3.1296E-09 5.0000E-03

100 NPPSTATE SUCCESS + V 3.1296E-09

PROBABILITY equal to : 3.1296E-09

CONSTITUENT Ordinal : 23

1 SBO Occurs - V 1.0000E+00

2 SCRAM Success + V 1.0000E+00

4 OpA-MSSV Failure - 5.0000E-02 5.0000E-02

90 MSSV-Cyc Success + 4.9975E-02 5.0000E-04

6 3.45bar Success + V 4.9975E-02

10 EWS-ST Failure - 6.2969E-06 1.2600E-04

20 Gridrec1 NO - 3.1484E-09 5.0000E-04

30 Gridrec2 YES + 3.1453E-09 1.0000E-03

22 AFW-pump Failure - 1.5726E-11 5.0000E-03

50 MobileDG Success + 1.5648E-11 5.0000E-03

60 EWS-pump Success + 1.5570E-11 5.0000E-03

100 NPPSTATE SUCCESS + V 1.5570E-11

PROBABILITY equal to : 1.5570E-11

CONSTITUENT Ordinal : 24

1 SBO Occurs - V 1.0000E+00

2 SCRAM Success + V 1.0000E+00

4 OpA-MSSV Failure - 5.0000E-02 5.0000E-02

90 MSSV-Cyc Success + 4.9975E-02 5.0000E-04

6 3.45bar Success + V 4.9975E-02

10 EWS-ST Failure - 6.2969E-06 1.2600E-04

20 Gridrec1 NO - 3.1484E-09 5.0000E-04

30 Gridrec2 YES + 3.1453E-09 1.0000E-03

22 AFW-pump Failure - 1.5726E-11 5.0000E-03

50 MobileDG Success + 1.5648E-11 5.0000E-03

60 EWS-pump Failure - 7.8239E-14 5.0000E-03

900 R FUSION OCCURS - V 7.8239E-14

PROBABILITY equal to : 7.8239E-14

CONSTITUENT Ordinal : 25

1 SBO Occurs - V 1.0000E+00

2 SCRAM Success + V 1.0000E+00

4 OpA-MSSV Failure - 5.0000E-02 5.0000E-02

90 MSSV-Cyc Success + 4.9975E-02 5.0000E-04

6 3.45bar Success + V 4.9975E-02

10 EWS-ST Failure - 6.2969E-06 1.2600E-04

20 Gridrec1 NO - 3.1484E-09 5.0000E-04

30 Gridrec2 YES + 3.1453E-09 1.0000E-03

22 AFW-pump Failure - 1.5726E-11 5.0000E-03

50 MobileDG Failure - 7.8632E-14 5.0000E-03

900 R FUSION OCCURS - V 7.8632E-14

PROBABILITY equal to : 7.8632E-14

CONSTITUENT Ordinal : 26

1 SBO Occurs - V 1.0000E+00

2 SCRAM Success + V 1.0000E+00

4 OpA-MSSV Failure - 5.0000E-02 5.0000E-02

90 MSSV-Cyc Success + 4.9975E-02 5.0000E-04

6 3.45bar Success + V 4.9975E-02

10 EWS-ST Failure - 6.2969E-06 1.2600E-04

20 Gridrec1 NO - 3.1484E-09 5.0000E-04

30 Gridrec2 NO - 3.1484E-12 1.0000E-03

40 Gridrec3 YES + 3.1327E-12 5.0000E-03

22 AFW-pump Success + 3.1170E-12 5.0000E-03

100 NPPSTATE SUCCESS + V 3.1170E-12

PROBABILITY equal to : 3.1170E-12

CONSTITUENT Ordinal : 27

1 SBO Occurs - V 1.0000E+00

2 SCRAM Success + V 1.0000E+00

4 OpA-MSSV Failure - 5.0000E-02 5.0000E-02

90 MSSV-Cyc Success + 4.9975E-02 5.0000E-04

6 3.45bar Success + V 4.9975E-02

10 EWS-ST Failure - 6.2969E-06 1.2600E-04

20 Gridrec1 NO - 3.1484E-09 5.0000E-04

30 Gridrec2 NO - 3.1484E-12 1.0000E-03

40 Gridrec3 YES + 3.1327E-12 5.0000E-03

22 AFW-pump Failure - 1.5663E-14 5.0000E-03

50 MobileDG Success + 1.5585E-14 5.0000E-03

60 EWS-pump Success + 1.5507E-14 5.0000E-03

100 NPPSTATE SUCCESS + V 1.5507E-14

PROBABILITY equal to : 1.5507E-14

CONSTITUENT Ordinal : 28

1 SBO Occurs - V 1.0000E+00

2 SCRAM Success + V 1.0000E+00

4 OpA-MSSV Failure - 5.0000E-02 5.0000E-02

90 MSSV-Cyc Success + 4.9975E-02 5.0000E-04

6 3.45bar Success + V 4.9975E-02

10 EWS-ST Failure - 6.2969E-06 1.2600E-04

20 Gridrec1 NO - 3.1484E-09 5.0000E-04

30 Gridrec2 NO - 3.1484E-12 1.0000E-03

40 Gridrec3 YES + 3.1327E-12 5.0000E-03

22 AFW-pump Failure - 1.5663E-14 5.0000E-03

50 MobileDG Success + 1.5585E-14 5.0000E-03

60 EWS-pump Failure - 7.7925E-17 5.0000E-03

900 R FUSION OCCURS - V 7.7925E-17

PROBABILITY equal to : 7.7925E-17

CONSTITUENT Ordinal : 29

1 SBO Occurs - V 1.0000E+00

2 SCRAM Success + V 1.0000E+00

4 OpA-MSSV Failure - 5.0000E-02 5.0000E-02

90 MSSV-Cyc Success + 4.9975E-02 5.0000E-04

6 3.45bar Success + V 4.9975E-02

10 EWS-ST Failure - 6.2969E-06 1.2600E-04

20 Gridrec1 NO - 3.1484E-09 5.0000E-04

30 Gridrec2 NO - 3.1484E-12 1.0000E-03

40 Gridrec3 YES + 3.1327E-12 5.0000E-03

22 AFW-pump Failure - 1.5663E-14 5.0000E-03

50 MobileDG Failure - 7.8317E-17 5.0000E-03

900 R FUSION OCCURS - V 7.8317E-17

PROBABILITY equal to : 7.8317E-17

CONSTITUENT Ordinal : 30

1	SBO	Occurs	-	V	1.0000E+00	
2	SCRAM	Success	+	V	1.0000E+00	
4	OpA-MSSV	Failure	-		5.0000E-02	5.0000E-02
90	MSSV-Cyc	Success	+		4.9975E-02	5.0000E-04
6	3.45bar	Success	+	V	4.9975E-02	
10	EWS-ST	Failure	-		6.2969E-06	1.2600E-04
20	Gridrec1	NO	-		3.1484E-09	5.0000E-04
30	Gridrec2	NO	-		3.1484E-12	1.0000E-03
40	Gridrec3	NO	-		1.5742E-14	5.0000E-03
50	MobileDG	Success	+		1.5663E-14	5.0000E-03
60	EWS-pump	Success	+		1.5585E-14	5.0000E-03
100	NPPSTATE	SUCCESS	+	V	1.5585E-14	

PROBABILITY equal to : 1.5585E-14

CONSTITUENT Ordinal : 31

1	SBO	Occurs	-	V	1.0000E+00	
2	SCRAM	Success	+	V	1.0000E+00	
4	OpA-MSSV	Failure	-		5.0000E-02	5.0000E-02

90 MSSV-Cyc Success + 4.9975E-02 5.0000E-04

6 3.45bar Success + V 4.9975E-02

10 EWS-ST Failure - 6.2969E-06 1.2600E-04

20 Gridrec1 NO - 3.1484E-09 5.0000E-04

30 Gridrec2 NO - 3.1484E-12 1.0000E-03

40 Gridrec3 NO - 1.5742E-14 5.0000E-03

50 MobileDG Success + 1.5663E-14 5.0000E-03

60 EWS-pump Failure - 7.8317E-17 5.0000E-03

900 R FUSION OCCURS - V 7.8317E-17

PROBABILITY equal to : 7.8317E-17

CONSTITUENT Ordinal : 32

1 SBO Occurs - V 1.0000E+00

2 SCRAM Success + V 1.0000E+00

4 OpA-MSSV Failure - 5.0000E-02 5.0000E-02

90 MSSV-Cyc Success + 4.9975E-02 5.0000E-04

6 3.45bar Success + V 4.9975E-02

10 EWS-ST Failure - 6.2969E-06 1.2600E-04

20 Gridrec1 NO - 3.1484E-09 5.0000E-04

30 Gridrec2 NO - 3.1484E-12 1.0000E-03

40 Gridrec3 NO - 1.5742E-14 5.0000E-03

50 MobileDG Failure - 7.8711E-17 5.0000E-03

900 R FUSION OCCURS - V 7.8711E-17

PROBABILITY equal to : 7.8711E-17

CONSTITUENT Ordinal : 33

1 SBO Occurs - V 1.0000E+00

2 SCRAM Success + V 1.0000E+00

4 OpA-MSSV Failure - 5.0000E-02 5.0000E-02

90 MSSV-Cyc Failure - 2.5000E-05 5.0000E-04

900 R FUSION OCCURS - V 2.5000E-05

PROBABILITY equal to : 2.5000E-05