Integrated Deterministic and Probabilistic Safety Assessment

Durga Rao Karanki

Deterministic safety analyses as well as probabilistic safety assessments are widely used in risk management of complex engineering systems such as nuclear and process plants. Challenges to these approaches include modeling of dynamic interactions among physical process, safety systems, and operator actions as well as propagation of these model uncertainties. Dynamic Event Tree (DET) analysis allows for integrated deterministic and probabilistic safety assessment (IDPSA) by coupling thermal-hydraulic/process system models with safety system and operator response models. This chapter introduces the concept of IDPSA, highlights the benefits of the approach as well as its limitations. Case study on a medium loss of coolant accident in a nuclear power plant is presented, which focuses on a comparison between IDPSA and traditional approaches considering impact of accident dynamics.

1 Introduction to Integrated Deterministic and Probabilistic Safety Assessment

In the safety analysis of complex engineering systems, we develop accident sequence models to quantify the risk. In this process, it is a challenge to consider dynamic interactions and capture their impact on accident models. Such dynamics (time dependent interactions) can arise due to human interactions, digital control systems, & passive system behavior [1–4]. The main objective is to increase realisam in modeling dynamics while quantifying risk [5]. In this section, an integrated deterministic and probabilistic safety analysis approach (IDPSA) is introduced including its basic elements and their relationships.

D. R. Karanki (✉)
Siemens Mobility AG, Hammerweg 1, 8304 Wallisellen, Switzerland
e-mail: durga.karanki@siemens.com

D. R. Karanki et al. (eds.), *Advances in RAMS Engineering*,
Springer Series in Reliability Engineering,
https://doi.org/10.1007/978-3-030-36518-9_18

1.1 Probabilistic and Deterministic Safety

In the Risk Analysis of Nuclear Power Plants (NPPs), we primarily address these questions: What is the hazard? How likely is it? What are the consequences? How to improve the level of safety? We use a systematic and comprehensive methodology Probabilistic safety assessment (PSA) to evaluate the risk associated with complex engineering systems like NPPs. Here are the high level tasks of PSA: (1) Identify accident initiators (2) developing accident models including sequence delineation (sequence delineation—which sequences lead to core damage) and success criteria definitions. Success criteria—identifying the requirements for success of the safety systems. For example, what is the success criteria of safety equipment. These requirement concern how many systems or pieces of equipment must operate, the latest time by which the operators must intervene, how long the equipment must function. (Typical questions to identify Success Requirements: *How many systems must operate? *How long they must function? *Latest time for operator intervention). (3) Quantifying the risk then corresponds to estimating the likelihood that the requirements are not met and an accident follows.

How is it done with the classical approach?

Risk/Safety assessments are widely performed to evaluate risks associated with complex engineering systems such as aeronautical systems, nuclear power plants, marine systems, etc. This is called PRA in aerospace and PSA in nuclear industry. Figure 1 shows elements of a typical PSA. Methods are quite common. Classical combination of event tree and fault trees are used to build risk models. Quantification of risk models require inputs such as data, simulations, etc. Typical results include risk, contribution of sequence, basic events to risk.

Offline (with predefined boundary conditions) thermal hydraulic/process analysis are performed for determination of sequence outcome and defining success criteria (deterministic safety analysis). Probability safety models (classical combination of event tree and fault tree models) address the probability that these criteria are not met. Figure 2 illustrates high level tasks in the current PSA practice. Accident scenario is simulated with a standalone tool, for instance thermal hydraulic code in case of nuclear power plants. Typically, few sequences with predefined boundary conditions are simulated to investigate if sequences lead to a safe state or an undesirable consequence.

1.2 Issues in Current Approach

How complex engineered system works in normal conditions is well known. What about in an accident scenario? What are the accident dynamics? Process behavior evolves with the time; i.e. the process parameters change with respect to time influencing the response of safety systems. Operator response may influence the

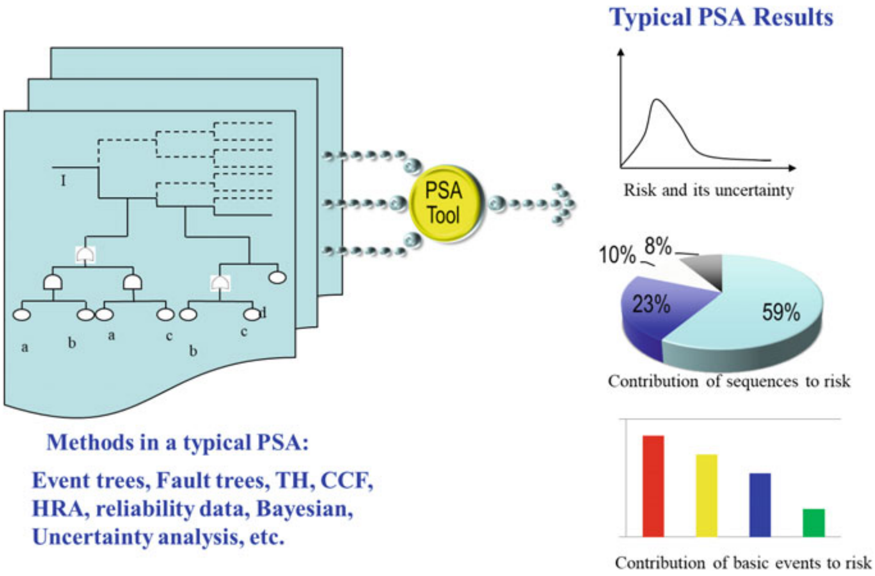

Typical PSA Results
I
a
b
a
c
b
c
d
PSA Tool
Risk and its uncertainty
10%
8%
23%
59%
Contribution of sequences to risk
Contribution of basic events to risk
Methods in a typical PSA:
Event trees, Fault trees, TH, CCF, HRA, reliability data, Bayesian, Uncertainty analysis, etc.

Fig. 1 Elements of a typical PSA/PRA

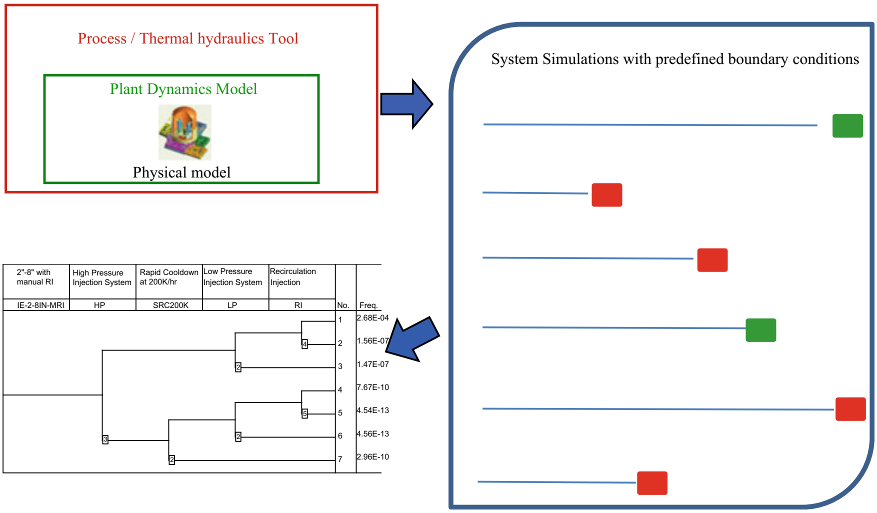


Fig. 2 Flow of high level tasks in a classical PSA

physical process. A typical accident scenario in a Nuclear Power Plant (NPP) involves complex interactions among process, safety equipment, and operator actions. The big question is: In current practice of plant simulations by independent thermal hydraulic codes (which don't have operator or equipment models), or A matrix of calculations) with pre-decided states of the systems and operator times, do we consider the complex interactions properly? For example, total operator time is dynamic, it is difficult to predict it offline. In addition to that, when stochastic variabilities in those responses are considered, defining success criteria will be cumbersome and complex. Also, the detrimental effects of binning; bounding assumptions are necessary while enveloping sequences and defining the success requirements in PSA; bounding is not only difficult but also produces modeling artifacts in certain cases. One of the major issues in current PSA practice is epistemic uncertainty in physical/process models [6–8]. PSA Model parameters (failure rates or failure probabilities) are already accounted, but uncertainties in physical model parameters (e.g. thermal hydraulic models) also needs to be addressed while building risk models. These may impact sequence outcomes, success requirements, subsequently risk estimates and contributors.

1.3 IDPSA Using Dynamic Event Trees

Dynamic Event Tree (DET) analysis provides a framework for integrated accident simulation of physical process, equipment, and operator actions. In other words, DET provide the means to simulate physical system evolutions, the evolution of system states due to stochastic events, and the dynamic interactions between these evolutions (DET simulates the dynamic interactions among physical process, safety system responses, and operator responses). DET models include deterministic (physical) as well as Stochastic Models.

Accident scenario is simulated considering dynamic interactions and stochastic variabilities to generate sequences. The outcome of sequences are labelled based on the values of physical parameters. Risk is estimated considering all the undesired sequences.

In the dynamic event tree: The transient is simulated in deterministic dynamic model and the process parameter values are obtained from plant dynamic model with respect to time. Scheduler has the integrated model of the plant describing the behavior of the various elements as a set of rules. When the process parameter reaches a level, it would fire one of these rules. As a result, event sequences are generated based on the rules (scheduler). When the process parameter demands intervention of safety system or human action, one of the rule in scheduler gets fired, and branching takes place in the DET.

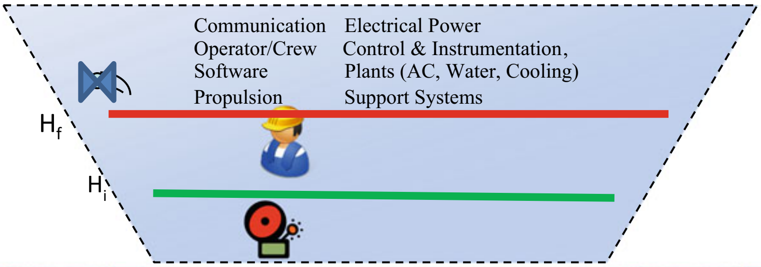
Several DET implementations tools and their applications can be seen in the literature. Interested readers may refer the following works in the literature [9–18].

2 A Simple Example: Water Leaks into a Ship/Vessel

Flooding is one of the important hazards for ship safety and stability. This example (see Fig. 3) is extremely simplified version of that problem. A Ship/vessel begins to accumulate water due to leak, which could be due to valve/pipe. The objective is to estimate the likelihood of vessel reaching the critical level, considering the stochastic variabilities and time dependent interactions. The tank will accumulate to a critical level if the operator does not isolate the leak in time. The operator receives a cue from an alarm caused by the rise in level, in response the operator should close the valve. System failure depends on the failures on demand of alarm and valve, as well as human response. The time dependent element in the problem is the human response time completing with the time taken by the tank to reach the critical level, which depends on leak size and location.

How do we solve this problem with the classical method? In the current practice, offline TH/physical process simulation-based analysis are performed to determine the sequence outcomes and define success criteria in developing accident sequence models. Success criteria analysis involved identifying the requirements on safety systems associated with the success branch for a function. These requirements concern how many components must operate, how long they must function, the latest time by which operator must intervene. The developed accident sequence model is typically an event tree with coupled fault trees, which are quantified to obtain risk. In the process of developing event tree models, bounding assumptions are necessary to envelop the sequences and define the success requirements. The accident dynamics complicate such grouping.

Figure 4 shows a classical event tree modeling of the vessel problem. Event trees are graphical models that order and reflect events according to the requirements for the mitigation of initiating events. Event trees are used to determine the sequences of system failures that can lead to undesired consequences.



A Vessel begins to accumulate water due to a leak. An alarm alerts the operator, who has to take a necessary action before the levels raises to a critical level. Estimate the risk of the vessel?

Fig. 3 An accumulating vessel with an initial level H_i and a critical level H_f

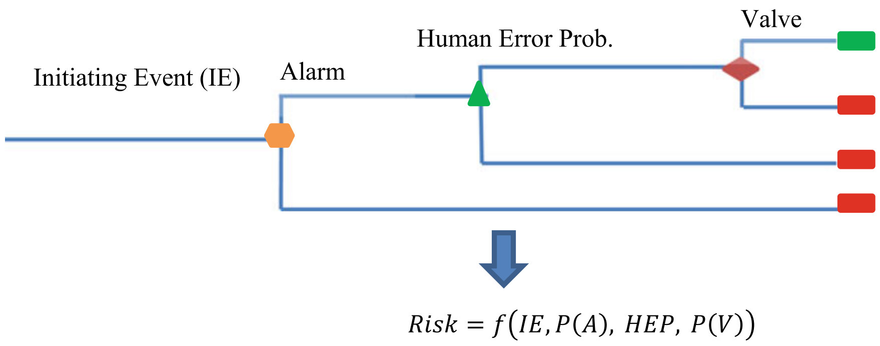
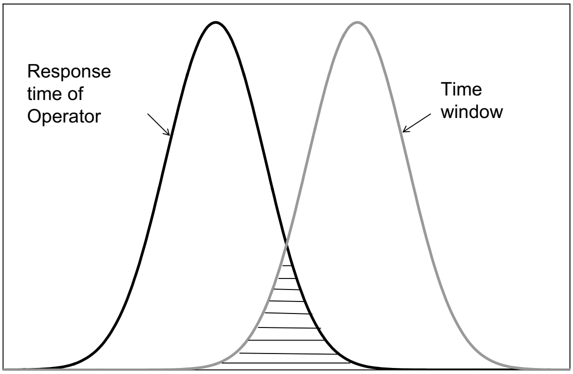


Fig. 4 Classical event tree modeling of vessel problem

Fig. 5 Analytical Solution of the vessel problem

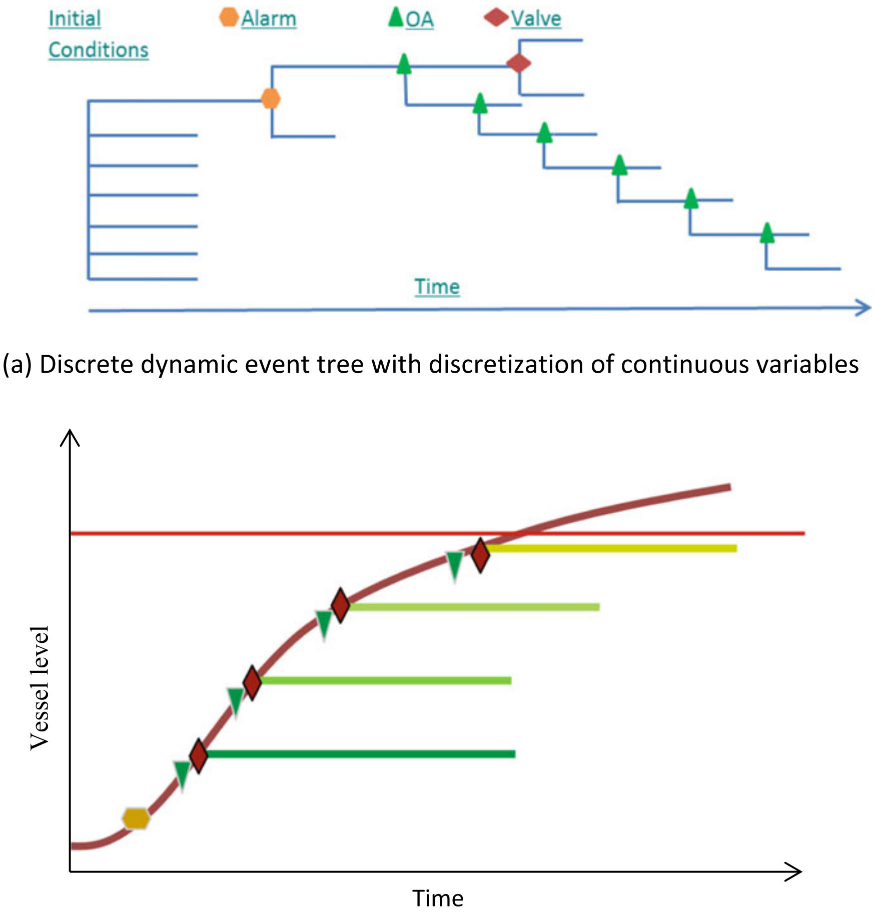


How do we solve this dynamic risk problem? There are several methods available in the literature such as analytical solution, analog Monte Carlo simulation, Dynamic Flowgraph Methodology, and DET, etc. As this is a simple problem, an analytical solution can be derived, which can be solved with a numerical integration method. Figure 5 shows the elements of the analytical solution of this problem, adapted from [6].

$$HEP = \int_{0}^{\infty} f_R(r) \int_{0}^{\left(\frac{r+k_2}{k_1}\right)^2} f_H(h)dh \cdot dr \tag{1}$$

where $k_1 = \frac{A}{aC}\sqrt{\frac{2}{g}}$ and $k_2 = \sqrt{H_f} \times k_1$

As depicted in Fig. 6, DET simulation framework integrates both deterministic and probabilistic models. In response to an accident in the vessel, several safety systems and crew actions are demanded by the process. The transient is simulated in deterministic dynamic model and the process parameter values are obtained from



(a) Discrete dynamic event tree with discretization of continuous variables

(b) Physical parameter evolution over time for different DET sequences

Fig. 6 DET solution of the vessel problem

vessel dynamic model with respect to time. The branches represent the possible states of the safety systems or/and crew. The sequences and vessel parameters with respect to time are obtained from the DET simulations.

3 IDPSA Methodologies

This section describes two IDPSA methodologies available in the literature, namely, DET Informed PSA [19] and quantified DET [20].

3.1 DET Informed PSA

Figure 7 shows the high level tasks of DET Informed PSA approach, which include DET Modeling, accident simulations with DET simulator, and success criteria analysis to develop event tree models and their evaluation. Primarily DET models consists of physical models of system behavior, stochastic models of the equipment, and operator response models.

Focusing on the detailed tasks involved in this approach, firstly the scope of the overall analysis is defined including the boundary conditions of initiating event, safety functions to be considered and the variabilities to be addressed, end sequence criteria (undesirable consequence), etc. The simulation models for physical process, response of safety functions, and operator responses are developed. The accident scenarios are simulated with Simulators considering the random variabilities. The results from the simulations are analyzed to understand the accident dynamics and identify the evolutions that lead to undesirable consequence. The success criteria are identified by examining the sequences generated by DETs, initially for the individual safety functions and initiating events. Initiators and sequences with similar success criteria for each safety function are then grouped, as a basis for defining one or more event trees to represent the overall variability of initiating event. Finally, the success criteria for these trees are defined. For operator actions, additional DET simulations are used to estimate time windows (TWs) in order to calculate the Human Error Probabilities (HEPs) in consideration of the sequence boundary conditions. The overall risk is quantified and important contributors are also identified.

The quantification of event trees requires various tasks such as fault tree modeling, common cause failure modeling, human reliability analysis, and failure data

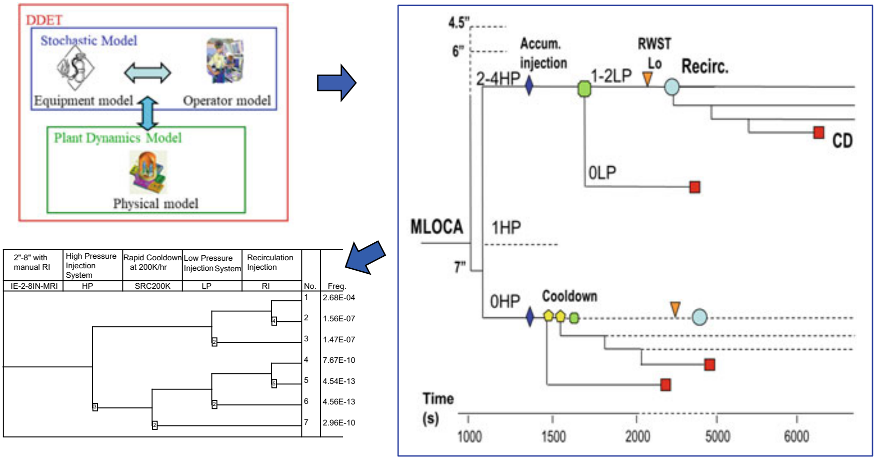


Fig. 7 Macro tasks of DET informed PSA

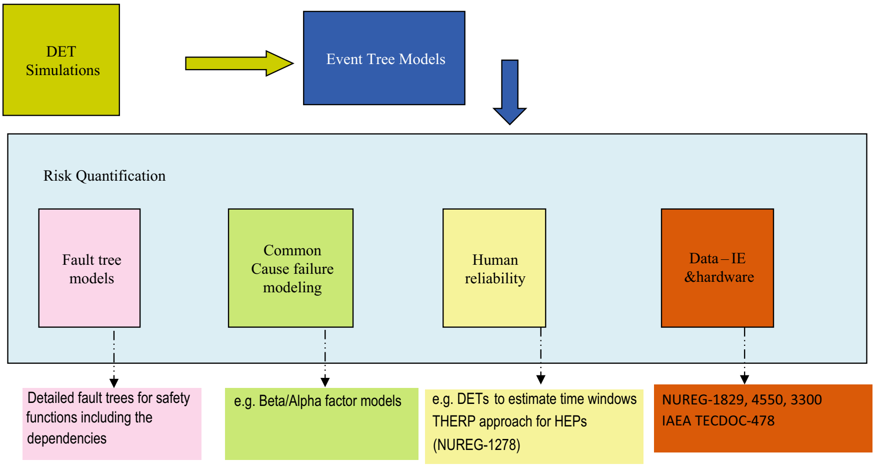

DET Simulations
Event Tree Models
Risk Quantification
Fault tree models
Common Cause failure modeling
Human reliability
Data – IE &hardware
Detailed fault trees for safety functions including the dependencies
e.g. Beta/Alpha factor models
e.g. DETs to estimate time windows THERP approach for HEPs (NUREG-1278)
NUREG-1829, 4550, 3300 IAEA TECDOC-478

Fig. 8 Flow of tasks in DET informed PSA

(See Fig. 8). Fault trees for safety functions are developed and linked to event trees. The common cause failure modeling accounts for any implicit dependencies among similar safety equipment. DET simulations provide useful information to estimate time windows for operator actions, which are used to estimate human error probabilities. PSA parameters including probabilities and frequencies of the initiating events, hardware, and operator actions are also necessary. Finally, PSA tools are used for quantification of accident sequence models to obtain risk results including point risk estimate and important contributors to risk basic events and sequences.

3.2 *Quantified DET Based IDPSA*

Figure 9 shows the high level tasks of DET quantification approach, which are DET modeling, simulation, and evaluation. DET Modeling and simulation task are quite similar to DET Informed approach. DET Evaluation replaces success criteria and bounded compact event trees modeling in this approach. In DET evaluation, all of the individual sequences that are generated are explicitly quantified. The DET sequences whose outcomes lead to undesirable consequences are identified and the frequencies for each of these failure sequences as well as total risk from the scenario are estimated.

Figure 10 shows a comparison between both IDPSA methodologies. Both DET Informed approach and DET quantification use the same integrated DET simulation tool. Although the DET tool and models are same, the simulations in DET-informed are with bounding while the latter approach perform simulations without bounding.

DET Informed PSA provides an integrated framework to account for complex dynamic interactions and stochastic variabilities among physical process, safety

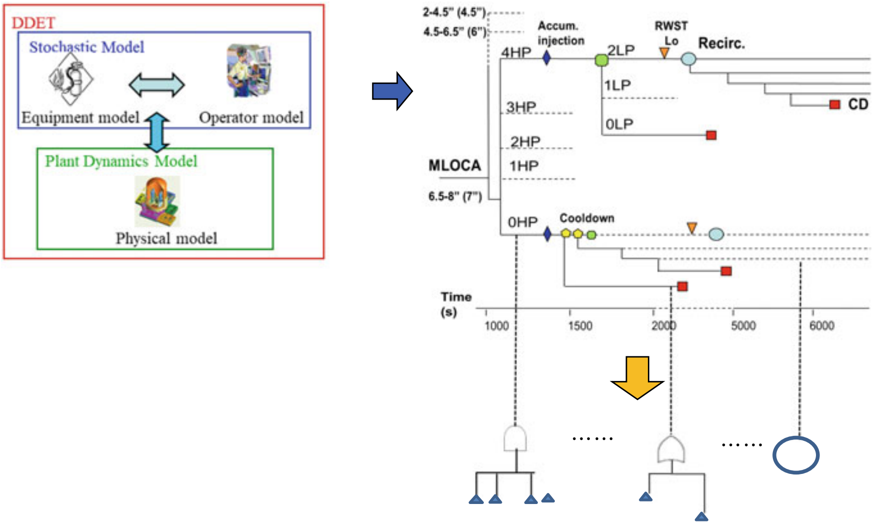


Fig. 9 Macro tasks of DET quantification

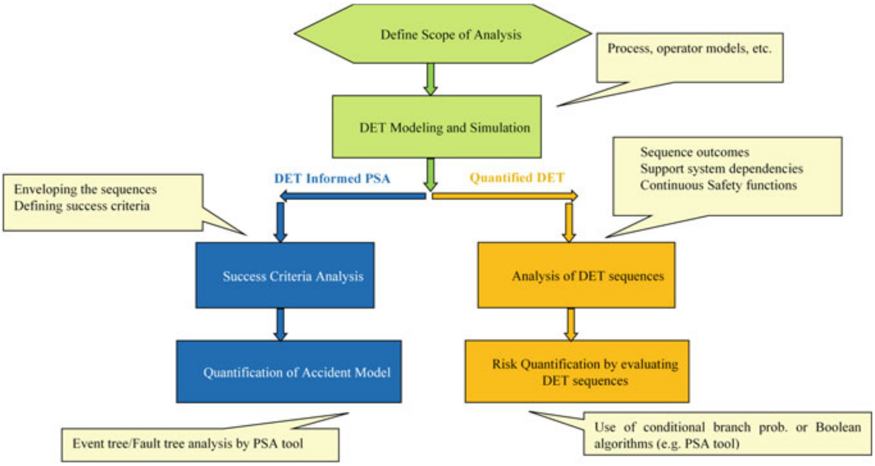

Define Scope of Analysis
Process, operator models, etc.
DET Modeling and Simulation
DET Informed PSA
Quantified DET
Sequence outcomes
Support system dependencies
Continuous Safety functions
Enveloping the sequences
Defining success criteria
Success Criteria Analysis
Analysis of DET sequences
Quantification of Accident Model
Risk Quantification by evaluating DET sequences
Event tree/Fault tree analysis by PSA tool
Use of conditional branch prob. or Boolean algorithms (e.g. PSA tool)

Fig. 10 Comparison of the tasks in the IDPSA methodologies

equipment, and operator actions. DET Informed PSA helps to get Success criteria definitions and to build a compact event tree which is quite practical in large scale PSAs of complex engineering systems. On the flipside, in DET informed PSA, bounding assumptions are inevitable to envelop the sequences and define the success requirements. Some detrimental effects of bounding may arise due to accident dynamics, which could be overlooked. Quantified DET approach does not need any bounding assumptions, thus bypassing issues associated with bounding effects. However additional computations are necessary.

DET-informed approach yields classical event trees that is compatible with the current PSA practice. Usually the classical event trees contain binary branches. On the other hand, Quantified DET approach may generate several branches for safety systems representing various combinations of conditions among the safety functions. Regarding quantification of risk, both approaches differ how safety systems are handled whose response involves a continuous aleatory variable. For example, recovery time of power supply or response time of operator actions. In classical event trees, the human error probability or recovery probability are estimated offline, then used as inputs to quantification of binary branches. In contrast, Quantified DET does not require the time windows to estimate these probabilities.

Quantified DET approach has to deal with the following practical issues: it must evaluate all generated sequences, treat support system dependencies among safety functions, as well as account for safety systems whose response is continuous. Some possible solutions for these issues were proposed in [20].

4 Case Study—MLOCA Scenario

This section presents a case study on Medium Loss of Coolant Accident (MLOCA) scenario. The application of both IDPSA approaches presented in preceding Section are described. The analysis of results primarily focuses on impact of accident dynamics as well as impact of bounding. This accident scenario is particularly chosen because its break range has strong effect on the sequence dynamics and consequently on the requirements on the safety function (success criteria). The DET models and some of the simulations of MLOCA accident scenario are adapted from the references [19, 20].

4.1 Description

The accident scenario is derived from the Zion Pressurized Water Reactor (PWR), a decommissioned 4-loop PWR with a thermal power of 3250 MW and one of the plants addressed in the NUREG-1150 study of severe accident risks [21].

In a PWR, the primary coolant (water) is pumped under high pressure to the reactor core where it is heated by the energy generated by the fission of atoms. The heated water then flows to a steam generator where it transfers its thermal energy to a secondary system where steam is generated and flows to turbines which, in turn, spin an electric generator. This is about the physical process during the normal operation of NPP. In accident conditions, we need safety systems like Emergency Core Cooling System (ECCS) to prevent core damage. When automatic systems don’t function, operator has to intervene. Figure 11 shows a simplified schematic

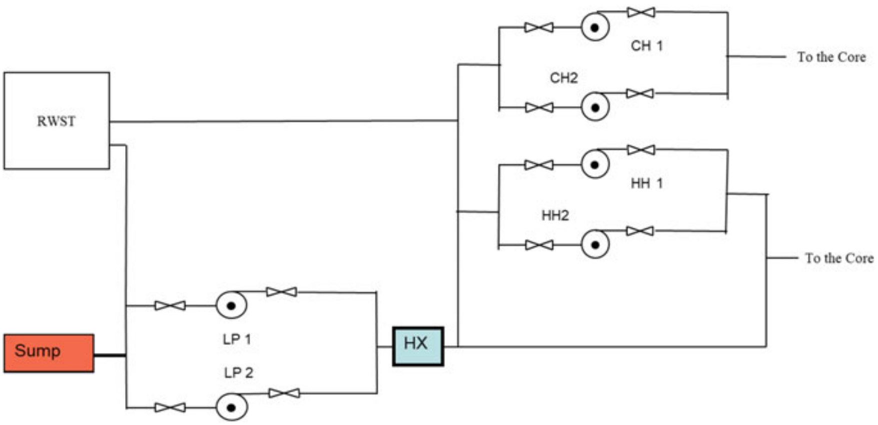


Fig. 11 A schematic diagram of the ECCS of a PWR

diagram of the ECCS of the PWR. ECCS consists of a high-pressure injection (HPI) system, a low-pressure injection (LPI) system, and an accumulator in each loop (not shown); HPI consists of two charging (CH) pumps as well as two high head (HH) injection pumps and theirs associated Valves. LPI includes two Low Pressure (LP) pumps in their injection trains. All these injection trains take suction from Refueling Water Storage Tank (RWST). When the water level in RWST tank reaches low level, an alarm prompts operator in control room to manually switch the injection to recirculation from containment sump.

If HPI fails, operator must perform rapid cooldown to depressurize reactor coolant system to low pressures conditions, which allows LP injection system to prevent core damage. This rapid cooldown is manual action using steam generator dump valves. Figure 12 shows operator actions during this accident sequence, which include reactor trip alerts operator in control room, emergency procedures will be examined, required action to depressurize must follow.

Figure 13 shows an Event Sequence Diagram (ESD) of MLOCA scenario. The sequence of events occurring, and their interactions are shown at a high level. Following reactor trip and turbine trip, the response to a MLOCA scenario begins with a HPI phase. Subsequently, the RCS pressure drops below the set point of the accumulators (40 bars) and finally to the low pressure injection (LPI) set point (15 bars). The summary of events and their potential stochastic variabilities are also depicted in Fig. 13.

Figure 14 presents ESDs during Secondary Rapid Cooldown (SRC) and Recirculation Injection (RI) phases.

The pivotal events involved in MLOCA scenario can be represented with a simplified event tree as shown in Fig. 15. There are four safety functions and seven sequences. Each header will have a fault tree (Fault trees are used to identify all combinations of component failures/events that can lead to system failure). Event tree represents sequences of system failures and associated consequences. The

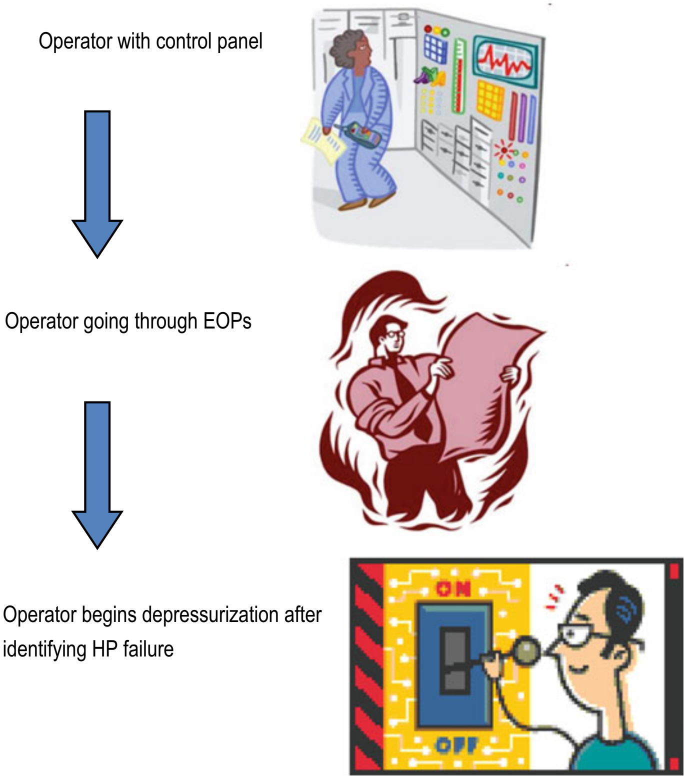

Operator with control panel
Operator going through EOPs
Operator begins depressurization after identifying HP failure
ON
OFF

Fig. 12 Operator actions to initiate rapid cooldown

success criteria definitions of safety functions (which decide their respective probabilities) are input to the fault tree (in order to calculate their branch probabilities) modeling. The important elements of success requirements are: number of injection trains, rate and timing of cooldown, timing of recirculation. Irrespective of what method (PSA or IDPSA) we choose, plant simulations are designed (scope is defined) to provide information to know the answers to these questions which give SC definitions.

Figure 16 shows the computational framework for MLOCA scenario. Simulation of accident scenario with different break sizes results in about 1000 sequences. A typical event tree for this scenario may have about 7 sequences as shown in Fig. 15, which is compact and of practical use with cut sets, importance measures, etc. Classical PSA approach usually based on a single limiting break, which may ignore the dynamic interactions, or in principle we could also take hybrid of most challenging criteria (it gives unnecessary conservatism and it does not represent any physical break). To account for dynamics, variabilities, and diversity in success requirements, split break range model can be used, which has about 30 sequences; additional sequences and appropriate success criteria

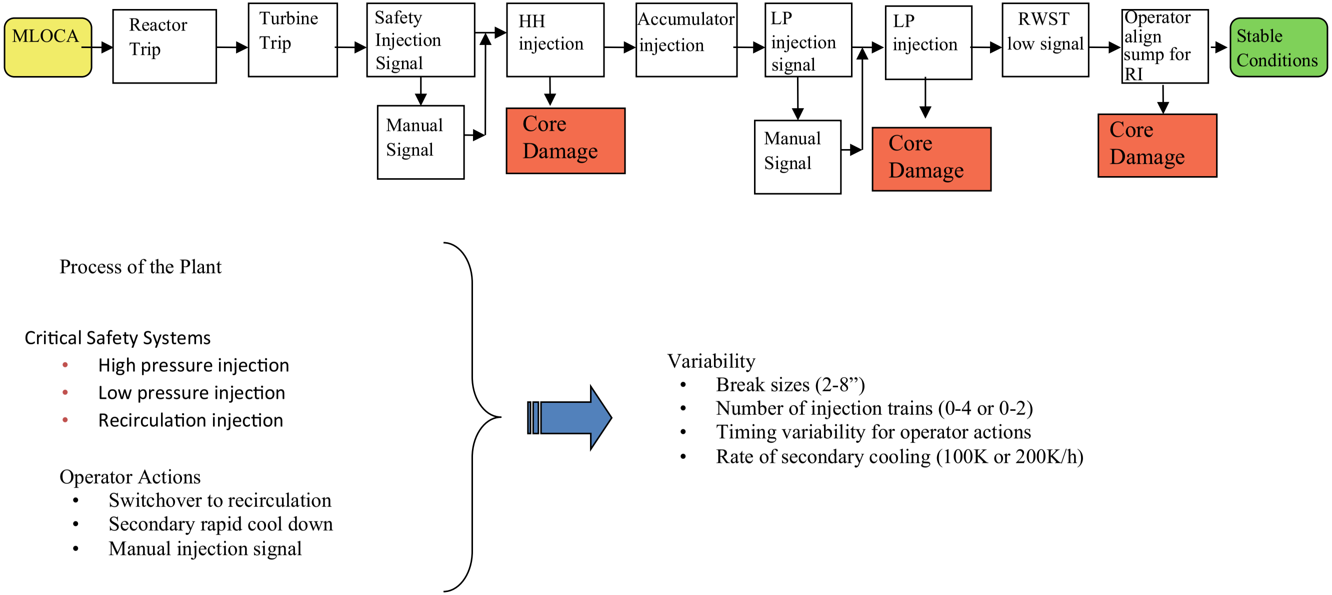


Fig. 13 Events and their interactions in the accident scenario (simplified ESD)

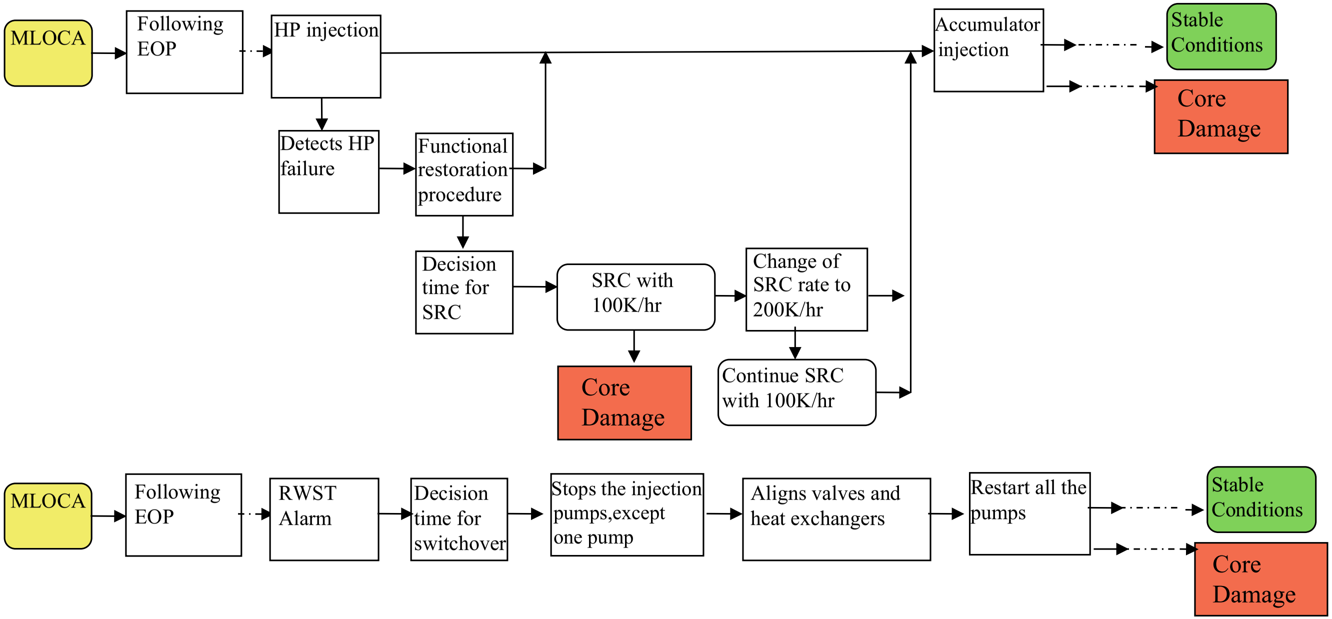


Fig. 14 Detailed events in secondary rapid cooldown and recirculation modes

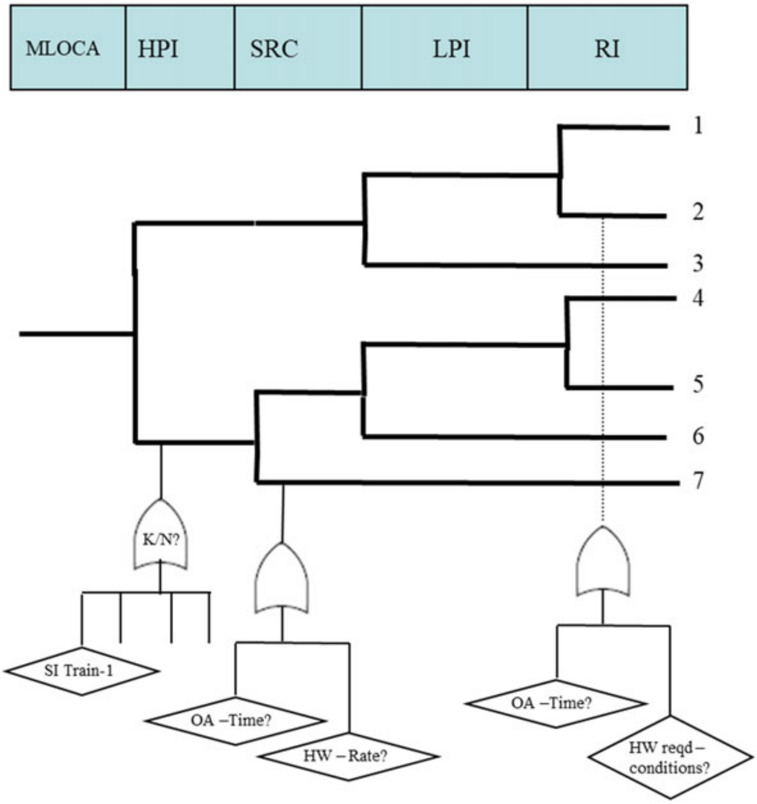


Fig. 15 Qualitative event tree of MLOCA scenario

definitions are used. To bypass issues associated with bounding, we can use DET quantification, meaning quantifying all the 1000 sequences.

4.2 Results—Comparison of IDPSA Approaches with PSA

The results obtained from the three methods, namely, classical PSA, DET informed PSA, and Quantified DET are considered for comparison. The obtained results include conditional core damage probabilities, core damage frequencies, critical sequences, and important basic events.

Figures 17 and 18 show event tree models from classical PSA and DET-informed approaches respectively. 7″ limiting break is assumed to represent MLOCA scenario in PSA approach, based on the results reported in [22]. DET-informed includes three split break range models, 2–4.5″, 4.5–6.5″, and 6.5–8″. Regarding event tree headers, they are different because of different time windows and high or low

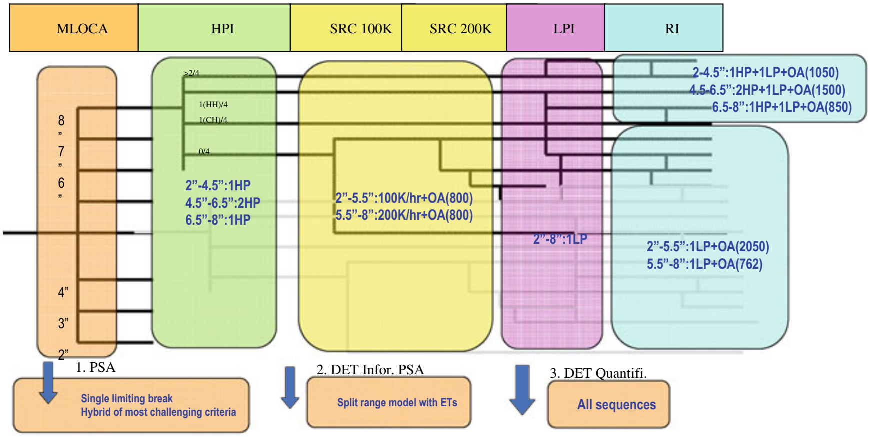


Fig. 16 Computational framework with three approaches

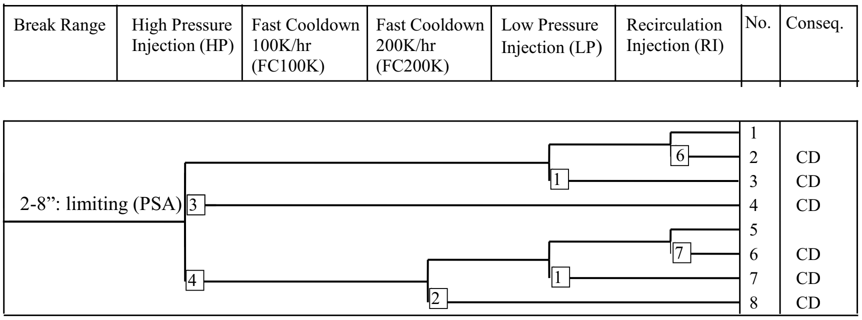

Break Range
High Pressure Injection (HP)
Fast Cooldown 100K/hr (FC100K)
Fast Cooldown 200K/hr (FC200K)
Low Pressure Injection (LP)
Recirculation Injection (RI)
No.
Conseq.
2-8": limiting (PSA)
3
4
2
1
1
6
7
1
2 CD
3 CD
4 CD
5
6 CD
7 CD
8 CD

Fig. 17 Event tree of classical PSA approach

pressure conditions leading to different events or probabilities in fault tree. Sequence 4 (1HP) in 4.5–6.5″ event tree leads to core damage (CD) as there is no cue for OA for cooldown. To quantify risk estimates, fault trees of safety systems, CCF models, HRA models, and failure data were plugged into the event trees. In Quantified DET approach, large event trees consisting of 1000 sequences were quantified (a section of DET can be seen in Fig. 9).

Figure 19 shows a comparison of the obtained core damage frequency (CDF) estimates among three methods. The core damage frequency (CDF) indicates the likelihood of an accident that would cause damage to reactor core, which also incorporates the probability of the breaks occurring. The results indicate the classical PSA approach is the most conservative, followed by DET-informed approach. The classical approach is significantly higher than quantified DET by a factor of 14 while DET-informed is higher by almost a factor

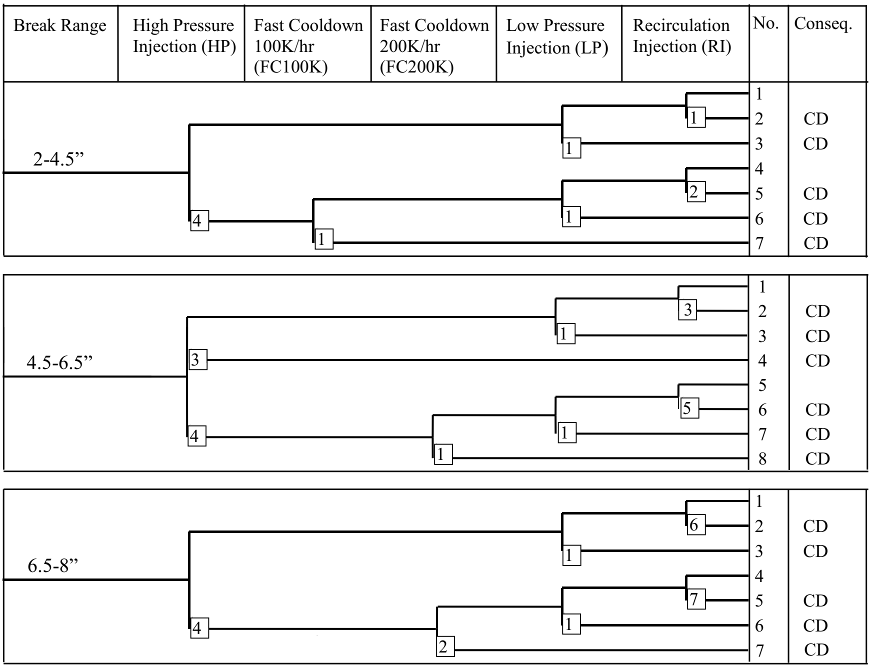
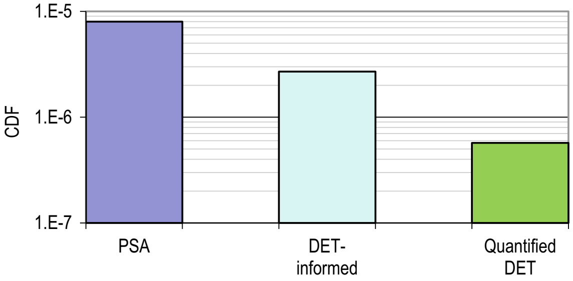

Break Range
High Pressure Injection (HP)
Fast Cooldown 100K/hr (FC100K)
Fast Cooldown 200K/hr (FC200K)
Low Pressure Injection (LP)
Recirculation Injection (RI)
No.
Conseq.
2-4.5”
4.5-6.5”
6.5-8”
1
2
3
4
5
6
7
8
CD
1
2
3
4
5
6
7

Fig. 18 Event trees of DET informed PSA approach

Fig. 19 Comparison of core damage frequencies among three methods



of 5. PSA and DET-informed estimates are higher than quantified DET, due to conservative bounding success criteria (limiting time windows).

Figure 20 shows a comparison of Fussel-Veseley importance measure of basic events. In PSA and DET-informed quantification, operator action during recirculation has the highest importance measure and none of the other basic events has comparable measure. Interestingly in quantified DET results, CCF event of LP injection is as important as operator action. Due to the conservative human error probability in PSA and DET-informed quantification, the importance of hardware events was underestimated. Quantified DET gave more realistic results as the impact of bounding is not present.

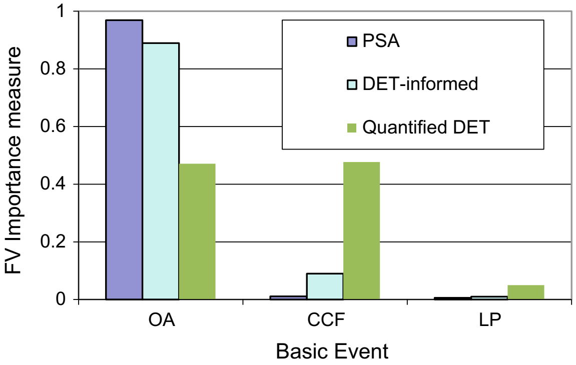


Fig. 20 Comparison of important events

5 Summary

In the current case study, bounding in PSA and DET informed quantification lead to conservative estimate of overall risk (core damage frequency), but it can be sensitive to bounding assumptions and their ability to capture accident dynamics. Also both quantifications underestimated the percentage risk contribution and importance of events due to bounding success criteria. Bounding gets complicated when we consider physical parameter uncertainties and epistemic uncertainties of failure and repair parameters. The IDPSA approach, quantified DET, improves the modeling of accident dynamics, eliminates the effects of bounding, and provides a framework propagate the epistemic uncertainties of the physical model, safety system model, and operator response models. However, quantified DET requires additional computations as well as the discretization of continuous stochastic responses.

Acknowledgements The author is grateful to Vinh N. Dang, Tae-Wan Kim, Saidur Rahman, and Omar Zerkak, for the guidance as well as the collaborative work at Paul Scherrer Institute.

References

1. Siu N (1994) Risk assessment for dynamic systems: an overview. Reliab Eng Syst Saf 43:43–73
2. Hsueh K-S, Mosleh A (1996) The development and application of the accident dynamic simulator for dynamic probabilistic risk assessment of nuclear power plants. Reliab Eng Syst Saf 52:297–314
3. Aldemir T (1989) Quantifying set point drift effects in the failure analysis of process control systems. Reliab Eng Syst Saf 24:33–50
4. Labeau PE, Smidts C, Swaminathan S (2000) Dynamic reliability: towards an integrated platform for probabilistic risk assessment. Reliab Eng Syst Saf 68:219–254
5. Siu N, Marksberry D, Cooper S, Coyne K, Stutzke M (2013) PSA technology challenges revealed by the great East Japan earthquake. In: PSAM topical conference in light of the Fukushima Dai-Ichi accident, Tokyo, Japan, 15–17 Apr 2013

6. Karanki DR, Rahman S, Dang VN, Zerkak O (2017) Epistemic and aleatory uncertainties in integrated deterministic-probabilistic safety assessment: tradeoff between accuracy and accident simulations. Reliab Eng Syst Saf (ISSN: 0951-8320) 162:91–102
7. Rahman S, Karanki DR, Zerkak O, Dang VN (2018) Deterministic sampling for propagating epistemic and aleatory uncertainty in DET analysis of a nuclear power plant. Reliab Eng Syst Saf 175:62–78
8. Karanki DR, Dang VN, MacMillan MT, Podofillini L (2018) A comparison of dynamic event tree methods—case study on a chemical batch reactor. Reliab Eng Syst Saf (ISSN: 0951-8320) 169:542–553
9. Amendola A, Reina G (1984) DYLAM-1, a software package for event sequence and consequence spectrum Methodology. EUR-924, CEC-JRC ISPRA, Commission of the European Communities, Ispra, Italy
10. Cacciabue PC, Amendola A, Cojazzi G (1986) Dynamic logical analytical methodology versus fault tree: the case of auxiliary feedwater system of a nuclear power plant. Nucl Technol 74:195–208
11. Cojazzi G (1996) The DYLAM approach to the dynamic reliability analysis of systems. Reliab Eng Syst Saf 52:279–296
12. Acosta C, Siu N (1993) Dynamic event trees in accident sequence analysis: application to steam generator tube rupture. Reliab Eng Syst Saf 41:135–154
13. Kloos M, Peschke J (2006) MCDET: a probabilistic dynamics method combining Monte Carlo simulation with the discrete dynamic event tree approach. Nucl Sci Eng 153:137–156
14. Hakobyan A et al (2008) Dynamic generation of accident progression event trees. Nucl Eng Des 238:3457–3467
15. Aldemir T (2013) A survey of dynamic methodologies for probabilistic safety assessment of nuclear power plants. Ann Nucl Energy 52:113–124
16. Hsueh KS, Mosleh A (1993) Dynamic accident sequence simulator for probabilistic safety assessment. In: PSA international topical meeting, conference proceedings, Florida, 26–29 Jan 1993
17. Catalyurek U et al (2010) Development of a code-agnostic computational infrastructure for the dynamic generation of accident progression event trees. Reliab Eng Syst Saf 95:278–294
18. Alfonsi A et al (2013) Dynamic event tree analysis through RAVEN. In: ANS PSA 2013 international topical meeting on probabilistic safety assessment and analysis, American Nuclear Society, CD-ROM, Columbia, SC, USA, 22–26 Sep 2013
19. Karanki DR, Kim T-W, Dang VN (2015) A dynamic event tree informed approach to accident sequence modeling: dynamics and variabilities in MLOCA. Reliab Eng Syst Saf (ISSN: 0951-8320) 142:78–91
20. Karanki DR, Dang VN (2016) Quantification of dynamic event trees—a comparison with event trees for MLOCA scenario. Reliab Eng Syst Saf (ISSN: 0951-8320) 147:19–31
21. USNRC (1990) Severe accident risks: an assessment for five US nuclear power plants, NUREG-1150
22. Karanki DR, Dang VN, Kim TW (2012) The impact of dynamics on the MLOCA accident model—an application of dynamic event trees. In: Proceedings of 11th probabilistic safety assessment and management/European safety and reliability (PSAM11/ESREL2012), CD-ROM, Helsinki, Finland, 25–29 June 2012

Dr. Durga Rao Karanki is currently working as a RAMS Manager at Siemens Mobility AG (Switzerland) since 2017. He is responsible for planning, coordination, and performing RAMS activities for development and execution of European Train Control System (ETCS) projects. Previously, he worked as a Scientist at Paul Scherrer Institute (PSI) from 2009 to 2017. His research at PSI primarily focused on dynamic safety assessment and uncertainty management. Prior to joining PSI, he worked as a Scientific Officer (2002–2009) at Bhabha Atomic Research Centre (India), where he conducted research on dynamic fault tree analysis, uncertainty analysis, and risk informed decision making of nuclear power plants. He is also a visiting faculty at several technical institutes. He has actively been involved in Reliability and Safety Assessment research and development for the last 17 years. His work resulted in more than 70 publications including 4 books, 15 first author journal papers, and several conference papers, with more than 900 citations. He received two awards for research Excellency from Society for Reliability Engineering, Quality and Operations Management (SREQOM). He is on the editorial board of three international journals in the area of reliability and risk analysis. He holds B.Tech in Electrical and Electronics Engineering from the Nagarjuna University (India), M.Tech in Reliability Engineering from the Indian Institute of Technology (IIT) Kharagpur and Ph.D. from the IIT Bombay.