Treating support system dependencies among safety functions in dynamic event tree quantification

Durga Rao Karanki · Vinh N. Dang

Received: 12 April 2013 / Published online: 12 February 2014

© The Society for Reliability Engineering, Quality and Operations Management (SREQOM), India and The Division of Operation and Maintenance, Lulea University of Technology, Sweden 2014

Abstract Dependencies are present among the safety systems in a nuclear power plant; for example, shared support systems such as power supply, service water, component cooling water, etc. The unavailability of the support systems contributes to the failure of the frontline systems. The solution and quantification of the event trees and fault trees that make up PSA models account for these dependencies. These dependencies must also be treated in dynamic risk assessments using the dynamic event tree framework, in which plant simulations are coupled to the stochastic models. The approaches from classical PSA for dealing with this issue can be adapted to the dynamic event tree work. While the principles are clear, the implementation is complex because of the need to couple the Boolean (logical) algorithms and probabilistic computations with the dynamic progression of the analysis. As an alternative to a fully integrated (online) treatment of the issue within the DET algorithm, this paper presents and demonstrates a post-simulation treatment based on conditional probability calculations. The obtained results are analyzed and compared to a reference solution based on a classical PSA approach.

Keywords Dynamic event tree analysis · Probabilistic safety assessment · Accident dynamic simulator · Loss of coolant accident

1 Introduction

Probabilistic safety assessment (PSA) is extensively used to evaluate the risks associated with complex engineering systems like nuclear power plants (NPPs). A combination of event tree and fault tree analyses are used to develop risk models in PSA of NPPs. In order to determine the sequence outcomes (e.g. core damage or not) and the success criteria for event tree headers, thermal-hydraulic (TH) calculations that simulate the physical processes of the NPP are performed. For NPP scenarios, such calculations must account for the interactions among the physical processes, safety system response, and operator responses. When stochastic variabilities in these responses and their impact on the scenario dynamics and outcomes are considered, defining success criteria and event tree models may become cumbersome and complex. Dynamic risk assessment approaches based on dynamic event tree (DET) analysis have been found to be useful to assess the impact of such variabilities and scenario dynamics on success criteria and ultimately on the results of the PSA model of the scenario (Karanki et al. 2012). DET implementation by ADS-TRACE (Karanki et al. 2011) was used in the application to medium break loss of coolant accident (MLOCA) scenario. Other DET implementation tools include MCDET (Kloos and Peschke 2006), ADAPT (Hakobyan et al. 2008), and SCAIS (Hakobyan et al. 2009).

In our earlier work on DET application to MLOCA scenario (Karanki et al. 2012), event tree models (including sequence outcomes and safety system success criterion) were developed based on the DET simulations and the final risk quantification was done in the PSA framework. The PSA framework allows fault trees to be used to quantify the event trees, thereby modeling dependencies. The

D. R. Karanki (✉) · V. N. Dang
Paul Scherrer Institute, Villigen PSI, Switzerland
e-mail: durga.karanki@psi.ch

V. N. Dang
e-mail: vinh.dang@psi.ch

dependencies are due to the shared support systems or shared components among the safety systems; for example—power supply, service water, and component cooling water are shared support systems in NPP. There are also shared components such as check valves in injection trains. Nevertheless, quantification of risk in PSA framework demands grouping of sequences and defining bounding success criteria. On the other hand, quantification of CDF in the DET framework needs to treat dependencies and also all the sequences generated by DET(s) must be evaluated to quantify the total risk. This paper primarily focuses on treating dependencies in DET framework.

The PSA approach accounts for dependencies by determining minimal cut sets (MCS) of each sequence with the fault trees of event tree headers; Boolean algebra and probability computations are used for the same (IAEA 1992). This approach from classical PSA for dealing dependencies can be adapted to the DET framework. However, implementation in DET framework is complex because of the need to integrate Boolean algorithms and probabilistic computations into dynamic progression of the analysis. As an alternative to a fully integrated (online) treatment of the issue within the DET algorithm, this paper presents and demonstrates a post-simulation treatment based on conditional probability calculations.

The impact of support system dependencies on top event and sequence probabilities is explained in Sect. 2. The proposed approximate conditional probabilities are first verified on a simple event tree example. Section 3 then presents an application. The classical PSA approach and the proposed DET approach to handle dependencies among safety functions are compared with a case study on MLOCA scenario. Conclusions are given in Sect. 4.

2 Support system dependencies in DET quantification

2.1 Impact of support system dependencies on top event or sequence probabilities

The shared support systems induce dependencies among the front line safety systems in NPPs. The unavailability of such shared systems contributes to the failure of front line systems. Hence such dependencies must be accounted in calculating top event or sequence probabilities. The impact of ignoring such dependencies is explained below with a simple example.

Let the top event is the simultaneous failure of two frontline systems X and Y and there is a shared support system Z. There are two different ways of modeling the top event. In the first approach (a typical PSA calculation), the support system is a basic event present in both the intermediate events X and Y. Assuming ‘A’ and ‘B’ as the

Fig. 1 Fault tree models with and without mentioning support system as a basic event

Table 1 Comparison of results with different combinations

Event	Description	PSA	Direct
XY	Failure of both X and Y	1.0E-4	1.2E-6
X+Y	Failure of X or Y	2.1E-3	2.2E-3
X $\bar{Y}$	Failure of X and success of Y	1.0E-3	1.1E-3

independent contributions for X and Y respectively, the Boolean expression for the top event is determined as $T = AB + Z$ and its probability is $P(A)P(B) + P(Z)$. In the second approach (where frontline systems are treated independently), the support system is not considered as a separate basic event, but as an internal event of X and Y; the Boolean expression is $T = (X)(Y)$ and its probability is simply their product. Figure 1 shows the fault tree models for both the approaches. Let the probabilities of A, B, and Z are $1e-3$, $1e-3$, and $1e-4$ respectively. The quantification of the top event by the first approach gives $1.01e-4$ and the second approach gives $1.21e-6$. The second approach is much lower than the first approach and it clearly underestimates the probability. If the top event is failure of system X or system Y ($X+Y$) (refer Table 1), the second approach is marginally higher than PSA result. Similarly, if the top event is failure of X and success of Y ($X\bar{Y}$), the second approach is higher than PSA result (See Fig. 2). The second approach underestimates with the XY logic and overestimates with the other logics. This shows that the approach of directly multiplying the probabilities of event tree headers may underestimate sequence probability if support systems are present.

Fig. 2 Comparison of results

In order to overcome the above problem in the second approach, conditional probabilities of event tree headers should be used; for example, the conditional probability of Y failure given X failure. The use of conditional probabilities will be able to consider support system dependencies and match PSA results. The obvious question is how to calculate such conditional probabilities. Eq. 1 gives the mathematical expression for the conditional probability based on Kolmogorov definition. The conditional probability of Y given X successful based on this definition is

$$P\left(\frac{Y}{X}\right) = \frac{P(X \cap Y)}{P(X)} \quad (1)$$

But we still need Boolean expression to calculate the $P(X \cap Y)$. The next section explains how one can calculate the conditional probabilities.

2.2 Conditional probability calculations in event trees—steps involved

The steps involved in calculating conditional probabilities is explained with a small event tree (with simple fault trees X: A+Z; Y: B+Z) shown in Fig. 3. Sequence 1 has the success of X and Y after the occurrence of initiating event. Sequence 2 considers the failure of Y given X successful, where as the sequence 3 considers the failure of X and followed by success of Y. Sequence 4 represents the simultaneous failure of both X and Y. Seq1.1 denotes the sequence up to X available after the initiating event (prior to the demand of Y); similarly, Seq3.1 denotes the sequence up to X unavailable after the initiating event.

Using the Eq. 1, the conditional probability of Y failure given the occurrence of Seq3.1 (Br4.1 in Fig. 3) is

$$P\left(\frac{Y}{Seq3.1}\right) = \frac{P(Seq4)}{P(Seq3.1)} \quad (2)$$

Fig. 3 Simple event tree and fault tree model

There are two ways to get the Boolean expression for sequence 3.1: either re-run the PSA model with header Y removed/disabled or the Boolean sum of sequences 3 and 4 gives the expression for Seq3.1. In the second approach, MCSs of sequences 3 and 4 shall be added and simplified by the Boolean algebra rules. The probability over the simplified Boolean expression (MCS) of Seq3.1 gives its probability.

However, in event trees with several headers, the above approaches will take a lot of computations. In order to reduce the computational effort, we could use the following approximation. The probability/frequency of Seq3.1 is approximately equal to the sum of probabilities/frequencies of sequences 3 and 4. It is important to note that this assumption is valid only for rare events. In case of higher likely events, the probability of Seq3.1 would be higher than the real value, but the conditional probability would be underestimated as the $P_{seq3.1}$ is in denominator of Eq. 2.

$$P_{Seq3.1} \approx P_{Seq3} + P_{Seq4} \quad (3)$$

Substituting Eq. (3) in Eq. (2), we have

$$P\left(\frac{Y}{Seq3.1}\right) \approx \frac{P_{Seq4}}{P_{Seq3} + P_{Seq4}} \quad (4)$$

The above expression (Eq. 4) can be used to calculate the branch probability of Br4.1. Similarly the branch

Table 2 Comparison of approximate approach with exact method on branch probability—BR4.1

Basic event probabilities			RiskSpec—default options		RiskSpec—success by Demorgan, 3rd order approximation	
A	B	Z	Exact	Approx.	Exact	Approx.
1e-3	1e-3	1e-4	9.18e-2	9.17e-2	9.18e-2	9.18e-2
1e-1	1e-1	1e-2	0.1825	0.1659	0.1825	0.1825

probabilities of Br1.2, Br2.1 and Br3.2 are given by the expressions mentioned below (Eqs. 5–7).

$$P_{Br1.2} = P\left(\frac{\bar{Y}}{Seq1.1}\right) \approx \frac{P_{Seq1}}{P_{Seq1} + P_{Seq2}} \quad (5)$$

$$P_{Br2.1} = P\left(\frac{Y}{Seq1.1}\right) \approx \frac{P_{Seq2}}{P_{Seq1} + P_{Seq2}} \quad (6)$$

$$P_{Br3.2} = P\left(\frac{\bar{Y}}{Seq3.1}\right) \approx \frac{P_{Seq3}}{P_{Seq3} + P_{Seq4}} \quad (7)$$

When we have event trees with more number of headers, the sequence and branch probabilities can be calculated from right to left with this approach. This approximate conditional probability is easy to apply for large event trees without repeating PSA or Boolean arithmetic.

The approximate approach is worked out on the simple event tree example (Fig. 3) and compared with the exact approach. The conditional probability Br4.1 is chosen for comparison. The exact formula for conditional probability Br4.1 is given in Eq. (2) and approximate formula is in Eq. (4). Table 2 gives the summary of the results with two sets of data, one with low likely rare events (case-1) and other with higher likelihood. With the PSA tool-RiskSpectrum default options (success events by logical ET, rare event approximation), as expected in Case-2 there is a significant difference between the two approaches of conditional probability calculations. The approximation approach underestimated the probability of the sequence (shown in bold); this is considerable when there are common cut sets (as is the case here) between the sequences or chance for redundancy in Boolean expression. When the success events are treated by Demorgan in fault tree and event trees (option is available in RiskSpectrum), the approximate conditional probabilities match with the exact approach. It is important to note that success treatment option plays a role than the rare event approximation in RiskSpectrum; the tool would automatically do the higher order approximation when the events are high likely.

The following insights are worth to note from this exercise when calculating conditional probabilities:

- When all the events have lower likelihood (<1e-2), the approximate approach with RS default options can

simply be used. If any of the events have higher likelihood, we must use the option of Demorgan for fault tree and event tree with the approximate approach.

- The effort involved in calculations of conditional probabilities with the exact formula is larger than the approximate approach. The approximate approach does not need the repetition of any event tree analysis. This may be used for large scale problem to reduce the effort of calculating conditional probabilities with the exact formula.

3 Case study

3.1 Introduction to MLOCA accident scenario of Zion NPP

The analysis is performed for a decommissioned plant the Zion PWR, a 4-loop PWR with a thermal power of 3,250 MW and one of the plants addressed in the NUREG-1150 study of severe accident risks (U. S. Nuclear Regulatory Commission 1990), which is frequently used in international studies and allows the results of alternative methods to be compared. MLOCA scenario is considered here, i.e. accidents in which a medium sized coolant circuit pipe work fracture occurs. In an MLOCA scenario, automatic safety systems will trip the reactor and turbine and will start to inject water into the reactor coolant system (RCS), in order to compensate for the loss of coolant. For MLOCAs, high pressure injection systems are required initially. Next, the RCS pressure will drop, allowing the accumulators and, finally, the low pressure injection systems to inject. Two manual actions are often considered in MLOCAs: switching HPI or LPI to recirculation when the coolant reserve is low, and in scenarios in which HPI fails, a rapid cooldown to reduce pressure and allow LPI to inject. The nominal success sequence in MLOCA requires the availability of high pressure injection (HPI), accumulators, low pressure injection (LPI), and the recirculation.

3.2 Event tree model for MLOCA scenario

The event tree model is shown in Fig. 4. The pivotal events involved in the MLOCA scenario are HPI, Rapid cooldown, LPI, and recirculation. There are seven sequences in the event tree—sequence 1 and 4 lead to safe state of reactor core, and the rest of the sequences would be leading to core damage. The accumulators are assumed to be available as they are passive and have higher value of availability. Each header of the event tree has a fault tree representing the combination of basic events involved in its failure. The success criterion for HP injection is

Fig. 4 Event tree for MLOCA scenario**Table 3** Top event probabilities from fault tree analysis

Branch	Top event frequency/probability
Initiating event—MLOCA	2.68E-04
HP injection	2.86E-06
Rapid cooldown	3.85E-01
LP injection	5.50E-04
Recirculation with HP available	1.92E-03
Recirculation without HP	1.91E-03

Table 4 Conditional probabilities of branches

Branch	Conditional probability
RI failure given HP and LP success	1.39e-3
LP failure given HP successful	5.49e-4
RI failure given HP failure and LP successful	1.4e-3
LP failure given HP failure	5.94e-4

availability of 2 out of 4 trains, and the LP injection is 1 out of 2 trains; the time windows of manual recirculation and cooldown are 25 and 15 min respectively (Karanki et al. 2011). Three approaches are used here for CDF quantification—(1) Classical PSA approach, (2) Direct top event probabilities, and (3) Conditional top event probabilities.

The event tree has been quantified by the three approaches. PSA tool RiskSpectrum (2006) was used for fault tree and event tree analysis. First approach is based on the classical PSA approach. In the second approach, top event probabilities were obtained from their respective fault trees (shown in Table 3); the sequence frequency is simply the product of initiating event frequency and top event probability of safety functions involved in the sequence or in other words, the top event probabilities are directly given to event trees instead of fault trees. In the third approach, conditional probabilities were calculated based on the approach discussed in the Sect. 2.2. Similar to

Fig. 5 Frequencies of sequences and CDF from the three approaches

the second approach, the conditional probabilities are assigned to the branches of event trees instead of fault trees. The computed conditional probabilities for the event tree branches are shown in Table 4.

3.3 Results and discussion

Figure 5 shows the frequencies of sequences (only core damage sequences are shown) from the three approaches and their respective total CDF. For sequences 2 and 5, the frequency from PSA approach is lower than the second approach; on the other hand, second approach values for the remaining sequences are lower or equal to PSA approach. The sequence 2 represents availability of LP injection and unavailability of recirculation. In PSA calculations of sequence 2, the common cut sets of LP injection and recirculation gets eliminated as LP is available, leading to reduction in the sequence frequency. For sequence 6, support system dependencies are properly accounted in PSA calculations but they are treated as independent contribution in the second approach. Although we have mixed effect of support system dependencies, the

higher likelihood of sequence 2 made the MLOCA CDF from second approach higher than the PSA approach. The conditional probability approach gave the same results as that of PSA approach as it accounts for the support system dependencies. As the events are low likely in the scenario, approximate conditional probabilities approach is sufficient.

Although integrating fault tree models in dynamic event tree simulations accounts for support system dependencies, but the implementation of Boolean and probabilistic computations into DET simulations is complex. The conditional probabilities for various combinations of front lines can be made offline with a PSA tool and the results can be used in DET quantifications. This information will be useful in DET simulations for directly computing the sequence frequency and the scenario CDFs.

4 Conclusions

The way support system dependencies are treated impact the risk estimates of the accident scenarios. The PSA approach accounts for these dependencies in minimal cut set calculations. The simple example and the case study demonstrate that ignoring such dependencies would bias the risk estimate. For sequences having all the headers unavailable, the direct top event probability approach will give smaller values than PSA approach. For other combination of event tree headers, the direct top event probability approach will be conservative than PSA. As PSA type calculations are not possible in DET simulations yet, a conditional probability approach has been proposed. The approach is found to give same results as that of PSA results. In large scale problems, the computational efforts involved in calculation of conditional probabilities with the

exact approach are larger than the approximate approach. The options to be used in PSA tools while using approximate conditional probability approach have also been explored. When any of the basic events have higher likelihood ($>1e-2$), Demorgan option must be used with the approximate approach; otherwise, default options can simply be used.

References

- Hakobyan et al (2008) Dynamic generation of accident progression event trees. *Nucl Eng Des* 238:3457–3467
- Durga R. Karanki, Vinh N. Dang, Tae-Wan Kim (2011) Discrete dynamic event tree analysis of MLOCA using ADS-TRACE, ANS PSA 2011 International topical meeting on probabilistic safety assessment and analysis on CD-ROM, American Nuclear Society, LaGrange Park, Wilmington, 13–17 Mar 2011
- Durga R. Karanki, Vinh N. Dang, Tae-Wan Kim (2012) The impact of dynamics on the MLOCA accident model—an application of dynamic event trees”. In: 11th International probabilistic safety assessment and management conference & The annual european safety and reliability conference (PSAM11-ESREL2012), Helsinki, 25–29 June 2012
- 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
- Izquierdo JM et al. (2009) SCAIS (Simulation code system for integrated safety assessment): current status and applications,” ESREL 2008, safety, reliability and risk analysis. In: Martorell et al. (eds.) NUREG report—MLOCA Zion PSA, Taylor & Francis Group, London, pp 121–128
- IAEA (1992) Procedure for conducting probabilistic safety assessment of nuclear power plants (level 1), International Atomic Energy Agency, Vienna, Safety Series No. 50-P-4, 1992
- U. S. Nuclear Regulatory Commission (1990) Severe accident risks: an assessment for five U.S. nuclear power plants, NUREG-1150
- RiskSpectrum—PSA professional software (2006), version 2.10.4, Scandpower AB, Sweden