Comparison of MCUB and MCS BDD Fault Tree Solution Algorithms using Leibstadt Nuclear Power Plant Model

Pavol Zvoncek[a*] and Olivier Nusbaumer[a]
[a] Leibstadt Nuclear Power Plant, 5325 Leibstadt, Switzerland

Abstract: This paper summarizes the benchmark calculations recently undertaken at Leibstadt nuclear power plant (KKL) with a goal of comparing two fault tree quantification algorithms available in the RiskSpectrum PSA software, namely Min Cut Upper Bound (MCUB) and the more recently implemented Minimal Cut Set Binary Decision Diagram (MCS BDD) approach.

The benchmark is primarily focused on the most common risk metrics, Core Damage Frequency (CDF) for full power and Fuel Damage Frequency (FDF) for low power and shutdown states, which are the pivotal outcomes of Level 1 Probabilistic Safety Assessment (PSA). Moreover, in order to appraise the accuracy of the algorithms, three simple generic Fault Tree (FT) topologies representing fundamental modelling concepts in PSA are analyzed as well. Finally, in view of the existence of high probability basic events in Containment Phenomenological Event Trees (CPETs), an additional comparison up to Level 2 PSA end states is also performed.

The improved accuracy of MCS BDD approach over MCUB was demonstrated for the generic cases, while a substantial reduction in CDF/FDF was achieved for KKL PSA model, highlighting a potential for reduction of these risk metrics also at other nuclear power plants worldwide. Not to mention that this approach is especially important for obtaining unbiased risk profiles and risk insights, as required in risk-informed applications.

Keywords: PSA, Fault Tree, Minimal Cut Set Analysis, Binary Decision Diagram.

1. INTRODUCTION

The safety and reliability analysis generally deals with quantification of a defined undesired event, labelled as top event, while credible possibilities (cut sets) leading to the undesired state are graphically represented by a fault tree model. The quantification of the top event frequency/probability is based on finding minimal cut sets (MCSs), each representing such combination of component failures (i.e. basic events) which, if all occur, the undesired state will be reached. A removal of any single basic event from a minimal cut set makes the combination no longer a cut set [1].

A generalized system reliability upper bound, known as Min Cut Upper Bound (MCUB), was derived in the 60's for coherent systems with statistically independent basic events [2]. The term coherent system is defined as a system, whose components are all relevant and its structure function is monotone; while a structure function is considered monotone when fixing of a failed component does not worsen system's state [3]. The MCUB method is an accurate approximation of the exact solution for instances with low component failure probabilities, but introduces conservatism as probabilities approach unity. The advantage of MCUB over the plain summation of individual MCSs (rare event approximation) lies in its treatment of simultaneous concurrence of minimal cut sets. The latter approach can be derived as first order expansion of the MCUB expression [4].

Nowadays, Probabilistic Safety Assessment (PSA) of nuclear power plants includes detailed modelling of external initiating events that generally lead to significantly larger component failure probabilities than those of random nature. Besides, by expanding the scope of industrial PSA models to Level 2, relatively high occurrence probabilities of relevant phenomena (e.g. hydrogen deflagration,

* Corresponding author, pavol.zvoncek@kkl.ch

gross containment failure) in the range of p ~ 0.1 demand accurate treatment of these high probability events in top event quantification.

To address these challenges, more rigorous approaches, such as Binary Decision Diagram (BDD) method [5,6], are required. These can eliminate the conservatism of MCUB method as well as produce unbiased hazard profiles. The latter is particularly important for risk-informed applications that might not provide credible insights when the quantification method at hand introduces disproportionately distributed level of conservatism. In that case, risk categories with largest level of conservatism yield unrealistically high importance and thus might impair risk-informed recommendations. The goal of this paper is to compare the two quantification algorithms available in RiskSpectrum PSA using the large-scale model of Leibstadt nuclear power plant (KKL).

1.1. BDD Implementation in RiskSpectrum PSA

In June 2017, Lloyd's Register released version 1.3.2 of RiskSpectrum PSA software (with RSAT 3.4.0 quantification engine), which now includes an implementation for construction of BDD from MCSs, so-called MCS BDD. The key features of this implementation are described in [7].

As far as settings of the MCS BDD implementation are concerned, to limit the size of the problem (provide fast and yet sufficient accuracy), RiskSpectrum enables the user to define what fraction of the cut set list should be treated with the conventional (MCUB) approach, so called MCS limit. To make the BDD algorithm scalable it also uses exact BDD nodes and approximate BDD nodes (the approximate BDD nodes are comparable to but more exact than Zero-suppressed Binary Decision Diagram (ZBDD)). The selection of the node type is governed by basic event's Fussell-Vesely (FV) importance metric and/or its probability (Q) [6].

1.2. Success Treatment in a Nutshell

Before moving to benchmark cases, two principal success treatments available in RiskSpectrum PSA shall first be outlined, as they can produce different minimal cut set lists. The default success treatment method called "*Logical ET Success*" (LETS) considers basic event failures in a consistent way across multiple function events, thus having logical property, however it assumes success probability of 1.0. This assumption is reasonable for highly reliable functions leading to success path probabilities very close to 1.0, but becomes conservative as failure probability increases. On the other hand, "*Logical and Simple Quantification*" (LASQ) makes a numerical estimate of the success probability ($1 - p_{failure}$), while still having the logical property.

From the practical standpoint, accurate success treatment becomes even more important in Level 2 PSA, not only due to the presence of high probability basic events, but also due to the fact that release categories cover the entire spectrum of end-states, hence necessitate quantification of sequences on success branches of Containment Phenomenological Event Trees (CPETs).

2. GENERIC COMPARISON

Three distinct fault tree topologies representing typical modelling approaches in PSA are analyzed in this section. The performance of rare event approximation, MCUB and MCS BDD approach are appraised against exact analytical solution for the cut sets with high probability basic events. The results of the two principal success treatments are distinguished as well.

2.1. Pure Reliability FT

The pure reliability model represents a coherent situation consisting of several basic events (without negation). For the sake of simplicity, all basic events are assumed to have same failure probability ($p_{failure}$ = 0.2 in the default case). The fault tree structure and the minimal cut sets are provided in

Appendix A.1. Since the fault tree does not feature any negative logic, the two success treatment methods provide identical minimal cut sets. The exact solution can be derived analytically, as follows:

$$p_{top}^{exact} = C+\left(1 - C\right)\cdot[(A_1 + (1 - A_1)\cdot A_2)\cdot(B_1 + (1 - B_1)\cdot B_2)] = p + \left(1 - p\right)\cdot\left(2p - p^2\right)^2 \xrightarrow{p = 0.2} 0.30368 \quad (1)$$

As shown in Appendix A.1, both algorithms (MCUB and MCS BDD) quantify the exact solution of the model, independently of the underlying failure probability, whereas rare event approximation diverges from the exact solution as the failure probability increases. That means the widely used default setting of MCUB in conjunction with minimal cut set list generated under Logical ET Success treatment is appropriate for this coherent problem.

2.2. FT with negative logic

Fault trees with negative logic are often used in PSA to represent "*If-Then-Else*" situations. This modelling approach comes in handy especially for initiating event-specific success criteria. As an example, different number of emergency core cooling systems is required to prevent core damage under Large Liquid Loss-of-Coolant-Accident (LL-LOCA) as compared to smaller diameter LOCAs, e.g. *If* initiating event is LL-LOCA *Then* 4 spray/injection systems are required *Else* 1 spray/injection system is required.

This situation is analyzed on the generic fault tree shown in Appendix A.2. Similarly like above, all basic events are assumed to have same failure probability ($p_{failure}$ = 0.2 in the default case). Due to the presence of negative logic, the two success treatments lead to two distinct minimal cut set lists, see Appendix A.2. The exact solution can be derived analytically, as follows:

$$p_{top}^{exact} = C + \left(1 - C\right)\cdot[X\cdot A + (1 - X)\cdot B)] = p + \left(1 - p\right)\cdot[p^2 + \left(1 - p\right)\cdot p] = p + (1 - p)\cdot[p] \xrightarrow{p = 0.2} 0.36000 \quad (2)$$

The following observations can be made from the results in Appendix A.2, namely: (i) both algorithms produce the same solution when applied to the coherent cut set list generated under LETS success treatment, however the result is conservative, (ii) MCUB algorithm in conjunction with LASQ success treatment produces optimistic top event result[†], which is undesirable, and lastly (iii) only the MCS BDD algorithm applied on minimal cut set list generated under LASQ success treatment can quantify the exact solution for this fault tree, independently of the underlying component failure probability.

In conclusion, the widely used approach of MCUB in conjunction with LETS success treatment lead to somewhat conservative results wherever negative logic exists in fault trees, or where quantification of success branch sequences is of interest. The MCS BDD with LASQ success treatment is therefore recommended for this type reliability problems.

2.3. FT with configurations

Fault trees with configurations represent in practice cases where simultaneous administrative failure mode, i.e. planned maintenance unavailability, of multiple redundant safety systems is precluded, as often stipulated in nuclear power plant's Technical Specifications.

Since there exist also other failure modes of the safety systems (e.g. random, external event induced failures), which are relevant when the systems is not in maintenance, basic events compounding all the other remaining failure modes are included in the exemplary "two-train" fault tree, see Appendix A.3. As outlined above, the modelling assumes that maintenance of component A cannot coexist with

[†] Due to presence of the negated basic event in the LASQ cut set list (Table A.2-1), thus making cut sets No. 2 and No. 3 mutually exclusive. This artefact of the MCUB algorithm is to be eliminated in next release of RSAT engine, such that LASQ default will only have treatment of success modules, and not negated basic events, which in turn will make the result of MCUB with LASQ for this example conservative.

planned maintenance of component B, hence the basic events are mutually exclusive. The mutual exclusivity is emulated by modelling the administrative failure of component A together with negation of the other administrative failure of B under an AND gate, and vice versa, see Fig. A.3-1.

The compound basic events are assumed to have same failure probability ($p_{failure}$ = 0.2 in the default case) and the fractional probability of component A/B being in planned maintenance is assumed constant, $u_{A/B}$ = 0.05. The minimal cut sets for both success treatment options are shown in Appendix A.3. The exact analytical solution consists of three terms:

$$p_{top}^{exact} = u_A \cdot B + u_B \cdot A + (1 - u_A - u_B) \cdot A \cdot B = 2up + (1 - 2u) \cdot p^2 \xrightarrow{p = 0.2;\ u = 0.05} 0.05600 \quad (3)$$

The individual terms in Eq. 3 represent respectively the administrative unavailability of component A and failure of B, the administrative unavailability of B and failure of A, and lastly, the failure of A and B during the "remaining time" of no planned maintenance. It is important to note that for two non-intersecting events, the "overlap" term $u_A \cdot u_B$ of the expansion becomes zero, see Eq. 4.

$$p_{remainder} = (1 - u_A) \cdot (1 - u_B) = 1 - u_B - u_A + u_A \cdot u_B \xrightarrow{u_A, u_B \in MUX} 1 - u_B - u_A \quad (4)$$

Before discussing the results presented in Appendix A.3, the full truth table solution listing all combinations of the basic event states is shown in Table 1. From the truth table, the exact solution can also be derived, see Table 2, where two mutual exclusivity (MUX) cases, namely "*w/o* MUX_{BE}" and "*w/* MUX_{BE}" are distinguished.

Table 1: Truth table of the fault tree with configurations

BE \ No.	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
A	1	0	0	0	1	1	1	0	0	0	1	1	1	0	1
B	0	1	0	0	1	0	0	1	1	0	1	1	0	1	1
u_A	0	0	1	0	0	1	0	1	0	1	1	0	1	1	1
u_B	0	0	0	1	0	0	1	0	1	1	0	1	1	1	1
Cut set?	-	-	-	-	Y	-	Y	Y	-	-	Y	Y	-	-	Y

Table 2: Quantification of the truth table solution and corresponding MUX treatment

Cut set No.	**A**	**B**	**u_A**	**u_B**	**w/o MUX_{BE}**	**w/ MUX_{BE}**
5	p_A	p_B	$(1 - u_A)$	$(1 - u_B)$	$p_A \cdot p_B \cdot (1 - u_A - u_B + \mathbf{u_A \cdot u_B})$	$p_A \cdot p_B \cdot (1 - u_A - u_B + \mathbf{0})$
7	p_A	$(1 - p_B)$	$(1 - u_A)$	u_B	$p_A \cdot (1 - p_B) \cdot (u_B - \mathbf{u_B \cdot u_A})$	$p_A \cdot (1 - p_B) \cdot (u_B - \mathbf{0})$
8	$(1 - p_A)$	p_B	u_A	$(1 - u_B)$	$(1 - p_A) \cdot p_B \cdot (u_A - \mathbf{u_A \cdot u_B})$	$(1 - p_A) \cdot p_B \cdot (u_A - \mathbf{0})$
11	p_A	p_B	u_A	$(1 - u_B)$	$p_A \cdot p_B \cdot (u_A - \mathbf{u_A \cdot u_B})$	$p_A \cdot p_B \cdot (u_A - \mathbf{0})$
12	p_A	p_B	$(1 - u_A)$	u_B	$p_A \cdot p_B \cdot (u_B - \mathbf{u_B \cdot u_A})$	$p_A \cdot p_B \cdot (u_B - \mathbf{0})$
15	p_A	p_B	u_A	u_B	$p_A \cdot p_B \cdot \mathbf{u_A \cdot u_B}$	**0**
Exact Solution					**0.05520**	**0.05600**

2.3.1. MCUB

The MCUB algorithm cannot reproduce the exact solution for this reliability problem, neither with LETS nor with LASQ success treatment. The MCUB expressions of the LETS cut set lists from Table A.3-1 are outlined in Eq. 5 and Eq. 6 for situations without mutual exclusivity ($u_A, u_B \notin MUX$) and with MUX ($u_A, u_B \in MUX$) of the two basic events, respectively. Likewise, the MCUB expressions of the LASQ cut set list from Table A.3-1 are outlined in Eq. 7 and Eq. 8 for situations without mutual exclusivity ($u_A, u_B \notin MUX$) and with MUX ($u_A, u_B \in MUX$) of the two basic events, respectively.

The numerical result values in the below equations correspond to the top event probability calculated by RiskSpectrum PSA software, see Table A.3-2.

$$p_{top}^{MCUB,\ LETS,\ w/o\ MUX} = 1 - [(1 - p^2) \cdot (1 - pu) \cdot (1 - pu)] \xrightarrow{p = 0.2;\ u = 0.05} 0.059104 \quad (5)$$

$$p_{top}^{MCUB,\ LETS,\ w/\ MUX} = 1 - [(1 - p^2)\cdot(1 - 2\,pu)] \xrightarrow{p = 0.2;\ u = 0.05} 0.059200 \quad (6)$$

$$p_{top}^{MCUB,\ LASQ,\ w/o\ MUX} = 1 - [(1 - p^2)\cdot(1 - pu\cdot(1 - u))\cdot(1 - pu\cdot(1 - u))] \xrightarrow{p = 0.2;\ u = 0.05} 0.058153 \quad (7)$$

$$p_{top}^{MCUB,\ LASQ,\ w/\ MUX} = 1 - [(1 - p^2)\cdot(1 - 2\,pu\cdot(1 - u))] \xrightarrow{p = 0.2;\ u = 0.05} 0.058240 \quad (8)$$

2.3.2. MCS BDD

By applying the MCS BDD on minimal cut set list generated under LETS success treatment, Fig. 1, an interesting observation was made, namely that the exact solution was produced even without information on mutual exclusivity of the u_A and u_B basic events.

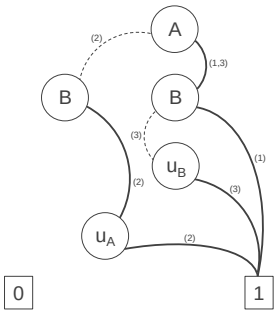

Figure 1: Representation of the Logical ET Success minimal cut set list in BDD. The numbers in brackets correspond to the cut set numbers from Table A.3-2

The explanation for this somewhat surprising behavior is provided in Eq. 9, which represents the mathematical form of the above-mentioned binary decision diagram. By expanding this equation and minor rearrangement the exact analytical solution (as shown in Eq. 3) is recreated. Therefore, for this fault tree, the combination of MCS BDD with LETS produces the exact solution, irrespectively of u_A and u_B mutual exclusivity.

$$p_{top}^{MCS\ BDD,\ LETS} = A\cdot B + \left(1 - A\right)\cdot B\cdot u_A + A\cdot(1 - B)\cdot u_B \quad (9)$$

$$p_{top}^{MCS\ BDD,LETS} = A\cdot B + B\cdot u_A - A\cdot Bu_A + A\cdot u_B - A\cdot B\cdot u_B = B\cdot u_A + A\cdot u_B + A\cdot B\cdot(1 - u_A - u_B)$$

As far as the LASQ minimal cut set list is concerned, its success modules enable the BDD algorithm to quantify the exact solution. As a matter of fact, the MCS BDD in conjunction with LASQ success treatment can replicate both exact solutions of the truth table, see the translation of the minimal cut set list and the truth table cut sets in Table 3. In order to produce the desired analytical solution, that precludes coexistence of the two planned maintenance unavailabilities, a MUX set containing both basic events needs to be explicitly specified in RiskSpectrum PSA software in this case.

Table 3: Relation of the LASQ minimal cut sets and the truth table solution

Logical and Simple Quantification					Cut set No.
No.	**Probability**	**Event 1**	**Event 2**	**Event 3**	**from Table 2**
1	4.0000E-01	3_A	3_B		**5** + **15**
2	9.5000E-03	3_B	3_UA	-3_UB	**8** + **11**
3	9.5000E-03	3_A	3_UB	-3_UA	**7** + **12**

To summarize the key observations of the generic benchmark, it can be concluded that the MCS BDD algorithm in conjunction with LASQ success treatment delivers the exact top event probability for all three modelling cases, though for fault tree modelling with configurations, mutual exclusivity of non-intersecting basic events needs to be explicitly specified.

Finally, the "conventional" approach of MCUB in conjunction with LETS success treatment produces the exact analytical solution only for the pure reliability model, while somewhat conservative results are obtained for cases featuring negative logic and/or configurations. To get a quick overview of the two approaches, please refer to grayed out cells of Table A.1-2, Table A.2-2 and Table A.3-2.

3. INDUSTRIAL BENCHMARK USING KKL PSA

The MCUB and MCS BDD benchmark calculations with industrial scale PSA model of Leibstadt nuclear power plant are presented in this section. The KKL PSA model is fully coupled, all states, all hazards RiskSpectrum model capable of quantifications up to Level 2 stage. The focus of the benchmark is primarily set on the most common risk metrics, Core Damage Frequency (CDF) for full power and Fuel Damage Frequency (FDF) for low power and shutdown states, which are the pivotal outcomes of Level 1 PSA.

In the benchmark, a comparison is made between the widely applied MCUB with Logical ET Success treatment approach and the MCS BDD in conjunction with Logical and Simple Quantitative success treatment. Also, the impact of the quantification algorithm on the breakdown of risk for both scopes (CDF and FDF) is presented. All quantifications were performed with MCS absolute cutoff of 1.0E-14 [1/a]. The absolute frequencies listed in this section are of indicative nature, however the relative differences correspond to the effectively observed changes.

3.1. Core Damage Frequency

The benchmark result for the KKL's core damage frequency is shown in Table 4. The breakdown of core damage frequency into hazard categories is provided in Table 5.

Table 4: Results of the KKL CDF Benchmark

	MCUB with LETS	MCS BDD with LASQ[1]	Rel. Diff.
Core Damage Frequency [1/a]	1.55E-06	1.03E-06	-33.5%
[1]RiskSpectrum MCS BDD settings: MCS limit = 5.0E-02, FV limit = 2.5E-02, Q limit = 2.5E-02			

Table 5: Breakdown of the KKL CDF, [1/a]

	MCUB with LETS	$CDF_{fraction}$	MCS BDD with LASQ[1]	$CDF_{fraction}$	Rel. Diff.
Transients	1.19E-07	7.7%	1.13E-07	10.6%	-5.5%
LOCAs	1.39E-07	9.0%	1.32E-07	12.3%	-5.2%
Fires	4.86E-08	3.1%	4.00E-08	3.7%	-17.6%
Floods	2.98E-08	1.9%	2.83E-08	2.6%	-5.0%
Earthquakes	9.75E-07	63.0%	5.54E-07[2]	51.8%	-43.2%
Winds	1.61E-07	10.4%	1.37E-07	12.8%	-14.9%
Tornadoes	6.39E-09	0.4%	5.37E-09	0.5%	-15.9%
Aircraft crashes	4.24E-08	2.7%	3.67E-08	3.4%	-13.4%
Lightning	8.32E-09	0.5%	7.38E-09	0.7%	-11.3%
Heavy rains	1.03E-11	0.0%	9.39E-12	0.0%	-8.6%
Sun storms	9.02E-09	0.6%	7.72E-09	0.7%	-14.4%
SWS inlet plugged	9.81E-09	0.6%	8.44E-09	0.8%	-14.0%
River diversion	1.68E-12	0.0%	1.55E-12	0.0%	-7.6%
[1]RiskSpectrum MCS BDD settings: MCS limit = 5.0E-02, FV limit = 2.5E-02, Q limit = 2.5E-02 [2]RiskSpectrum MCS BDD settings: MCS limit = 7.3E-02, FV limit = 2.5E-02, Q limit = 2.5E-02 due to memory constraint					

The most significant reduction of risk between the two algorithms exists in seismic hazard category, which features seismic fragility basic events having often relatively high failure probabilities. On the other hand, internal events (transients, LOCAs) see only minor risk reduction, since their risk is dominated by random component failures or Common Cause Failures (CCFs), which are usually of very low probability.

Additionally, in order to study the sensitivity of CDF on the fraction of minimal cut sets being developed into BDD, the FV and Q limits were kept constant at 2.5E-02 and only the MCS limit was varied. Figure 2 shows that by increasing the fraction of cut sets being treated by BDD, the core damage frequency decreases. A memory handling limitation of RiskSpectrum quantification engine prohibited calculation with MCS limit below 2.5E-02, corresponding to 97.5% of MCS being developed into BDD, though the limitation was already addressed to the development team. At very

small MCS fractions, the frequency exhibits a plateau, since the basic event-based limits in FV and Q became the governing parameters, thus further decrease in MCS limit did not have any impact on the end result. On the other hand, the CDF keeps steadily decreasing at large MCS fractions, thus suggesting that smallest achievable MCS limit shall be recommended for productive calculations.

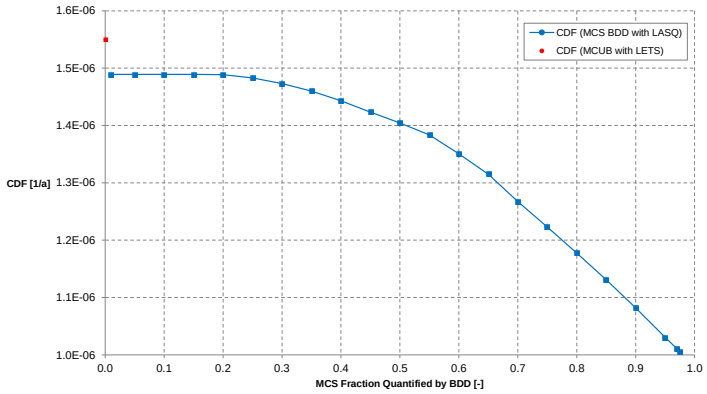

Figure 2: KKL Core Damage Frequency as a function of MCS fraction quantified by BDD

3.2. Fuel Damage Frequency

The benchmark result for the KKL's fuel damage frequency is shown in Table 6. The breakdown of fuel damage frequency into hazard categories is provided in Table 7.

Table 6: Results of the KKL FDF Benchmark

	MCUB with LETS	MCS BDD with LASQ[1]	Rel. Diff.
Fuel Damage Frequency [1/a]	4.52E-07	3.04E-07	-32.7%
[1]RiskSpectrum MCS BDD settings: MCS limit = 5.0E-02, FV limit = 2.5E-02, Q limit = 2.5E-02			

Table 7: Breakdown of the KKL FDF, [1/a]

	MCUB with LETS	$FDF_{fraction}$	MCS BDD with LASQ[1]	$FDF_{fraction}$	Rel. Diff.
Transients	1.36E-08	3.0%	1.26E-08	4.1%	-7.3%
LOCAs	1.54E-07	34.2%	1.17E-07	38.1%	-24.4%
Fires	3.79E-08	8.4%	1.30E-08	4.2%	-65.8%
Floods	7.56E-09	1.7%	7.11E-09	2.3%	-6.0%
Earthquakes	1.40E-07	31.1%	7.10E-08	23.2%	-49.4%
Winds	7.49E-08	16.6%	6.88E-08	22.5%	-8.1%
Tornadoes	1.34E-09	0.3%	1.23E-09	0.4%	-8.0%
Aircraft crashes	1.71E-08	3.8%	1.19E-08	3.9%	-30.7%
Lightning	6.64E-11	0.0%	6.17E-11	0.0%	-7.0%
Heavy rains	1.78E-13	0.0%	1.66E-13	0.0%	-6.9%
Sun storms	3.95E-09	0.9%	3.66E-09	1.2%	-7.4%
SWS inlet plugged	6.57E-10	0.1%	4.70E-10	0.2%	-28.4%
River diversion	2.11E-14	0.0%	2.11E-14	0.0%	0.0%
[1]RiskSpectrum MCS BDD settings: MCS limit = 5.0E-02, FV limit = 2.5E-02, Q limit = 2.5E-02					

Similarly like for CDF scope, the frequency of earthquake risk sees a significant reduction, due to some high probability seismic fragilities. Even more pronounced risk reduction exists for internal fire risk category in this case. A closer look into the cut sets revealed that important risk contributors, again having relatively high probabilities, such as planned maintenance-related time fraction of an important safety system and some human errors, were the main drivers of this considerable reduction.

3.3. A Level 2 PSA Case

In view of the existence of high probability basic events in CPETs, the benchmark is extended to Level 2 PSA scope by quantification of one release category. It should be noted that KKL PSA model

uses a simplified modelling approach for Level 2 PSA inside RiskSpectrum, such that, for each Key Plant Damage State (KPDS), a fully developed CPET is condensed into a set of basic events representing the contribution to corresponding release categories [8].

The release category (RC) analysed here has a sole KPDS contributor, whose entire frequency propagates to this release category, i.e. the "KPDS-to-RC" contribution probability equals to unity, while no other KPDS contributes to this release category. The minimal cut set list of the RC is therefore identical to that of the KPDS, with the exception of every minimal cut set containing additionally also the "KPDS-to-RC" contribution basic event with probability of 1.0. On that basis, the two frequencies should be the same, since $f(RC) = f(KPDS) \cdot 1.0$.

The MCUB algorithm, applied here on the minimal cut set list generated with LASQ success treatment provides consistent results, since the RSAT engine discards basic events with probability of 1.0 from minimal cut set list and thus leading to KPDS and RC frequencies to match perfectly, see Table 8.

Table 8: Results of the KKL Level 2 PSA Benchmark

	MCUB with LASQ	**MCS BDD with LASQ[1]**	**Rel. Diff.**
KPDS frequency [1/a]	3.133E-08	2.985E-08	-4.7%
RC frequency [1/a]	3.133E-08	2.985E-08	-4.7%
[1]RiskSpectrum MCS BDD settings: MCS limit = 1.0E-05, FV limit = 1.0E-04, Q limit = 1.0E-04			

Similarly, the MCS BDD algorithm, also applied on the minimal cut set list generated with LASQ success treatment, exhibits consistent performance. The frequencies are by several percent lower though, owing to the conservative characteristic of the MCUB algorithm as already observed also on the generic fault tree cases studied in Section 2.

4. CONCLUSIONS

The benchmark performed on the generic fault tree cases underlined the quantification accuracy of the newly implemented BDD based algorithm in RiskSpectrum PSA software. In conjunction with LASQ success treatment, the MCS BDD algorithm produced exact solutions for all generic cases, however special care had to be taken in case of fault trees with configurations, for which explicit information on mutual exclusivity of basic events was required.

As for the industrial scale PSA model of Leibstadt nuclear power plant, a substantial reduction of about 30% was achieved in Level 1 PSA metrics (CDF, FDF) with the new algorithm, as compared to widely used MCUB approach with LETS success treatment. The impact on the individual hazard categories has also been studied on the KKL PSA model, concluding considerable risk reduction of seismic hazard (up to 43%) for full power scope and of internal fire hazard (up to 65%) for low power and shutdown scope. Furthermore, the sensitivity study on MCS BDD settings displayed the decreasing trend in CDF with the increasing fraction of MCSs processed by the BDD algorithm.

Lastly, the stability of the algorithm was tested on one Level 2 PSA problem featuring two minimal cut set lists, one of which contained a basic event with probability of 1.0 in every minimal cut set. The two minimal cut set lists were otherwise identical. Both algorithms produced consistent results, however the MCS BDD result ended up being lower by several percent, owing to the conservative nature of the MCUB algorithm.

Acknowledgements

The authors would like to thank our colleague Valerio Ariu for enriching technical discussions on generic fault trees, which greatly contributed to our understanding of these fundamental modelling approaches. We would also like to express our gratitude to Ola Bäckström and Pavel Krcal of RiskSpectrum development team for their continual technical assistance as well as insights on RSAT quantification engine and MCS BDD implementation.

References

[1] W. E. Vesely, F. F. Goldberg, N. H. Roberts and D. F. Haasl, "*Fault Tree Handbook*", U.S. Nuclear Regulatory Commission, NUREG-0492, January 1981.

[2] J. D. Esary and F. Proschan, "*Coherent Structures of Non-identical Components*", Boeing Scientific Research Laboratories, D1-82-0154, February 1962.

[3] F. J. Samaniego, "*System Signatures and their Applications in Engineering Reliability*". Springer, 2007, New York.

[4] H. E. Lambert, "*Fault Trees for Decision Making in Systems Analysis*", Ph.D. Thesis, UCRL-51829, October 9th 1975.

[5] R. Bryant. "*Graph-Based Algorithms for Boolean Function Manipulation*", IEEE Transactions on Computers, Volume C-35, pp. 677-691, (1986).

[6] A. Rauzy, "*Binary Decision Diagrams for Reliability Studies*". In: Misra K.B. (eds) Handbook of Performability Engineering, Springer, 2008, London.

[7] O. Bäckström, P. Krcal and W. Wang, "*MCS BDD - Description and Verification of the Method Implemented in RiskSpectrum*", 13th International Conference on Probabilistic Safety Assessment and Management (PSAM 13), 2-7 October, 2016, Seoul, Korea.

[8] P. Zvoncek, O. Nusbaumer and A. Torri. "*Development of a Fully-Coupled, All States, All Hazards Level 2 PSA at Leibstadt Nuclear Power Plant*", Nuclear Engineering and Technology, Volume 49, pp. 426-433, (2017).

APPENDIX A.1: Pure Reliability FT

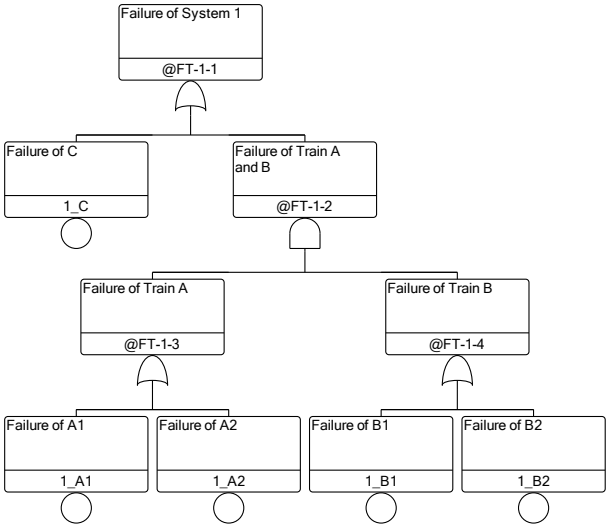

Figure A.1-1: Pure reliability fault tree model

Table A.1-1: Minimal cut set list for the pure reliability model

Logical ET Success			
No.	**Probability**	**Event 1**	**Event 2**
1	2.0000E-01	1_C	
2	4.0000E-02	1_A1	1_B1
3	4.0000E-02	1_A1	1_B2
4	4.0000E-02	1_A2	1_B2
5	4.0000E-02	1_A2	1_B1

Logical and Simple Quantification			
No.	**Probability**	**Event 1**	**Event 2**
1	2.0000E-01	1_C	
2	4.0000E-02	1_A1	1_B1
3	4.0000E-02	1_A1	1_B2
4	4.0000E-02	1_A2	1_B2
5	4.0000E-02	1_A2	1_B1

Table A.1-2: Comparison for the pure reliability model ($p_{failure}$ = 0.2)

	Rare Event	**MCUB**	**MCS BDD**	**Exact**
Log. ET Success	3.6000E-01	3.0368E-01	3.0368E-01	3.0368E-01
Log. and Simple Quant.	3.6000E-01	3.0368E-01	3.0368E-01	

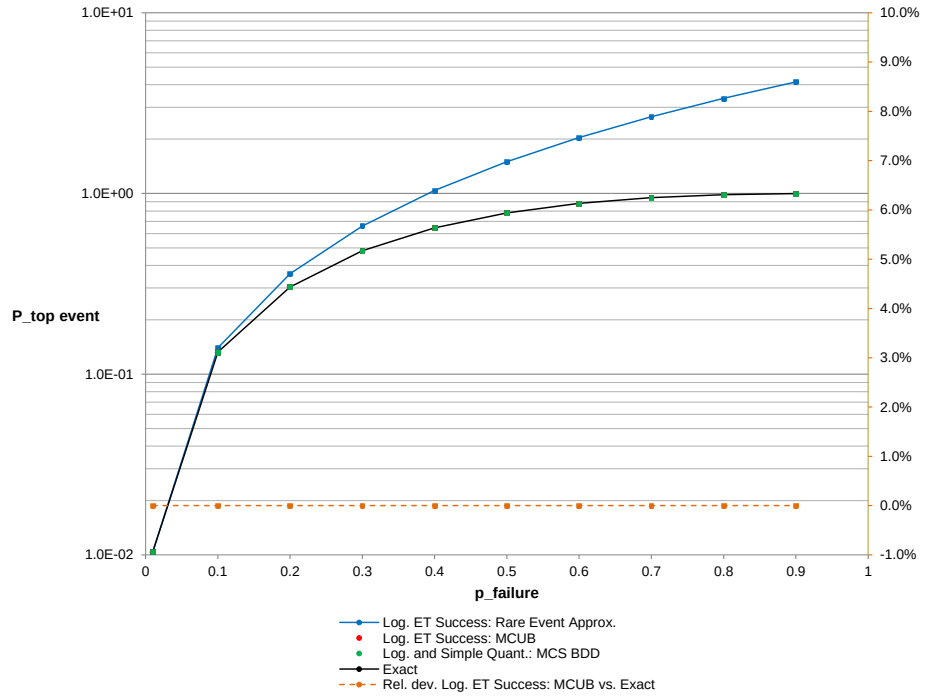

Figure A.1-2: Top event probability as a function of $p_{failure}$ for the pure reliability model

APPENDIX A.2: FT with negative logic

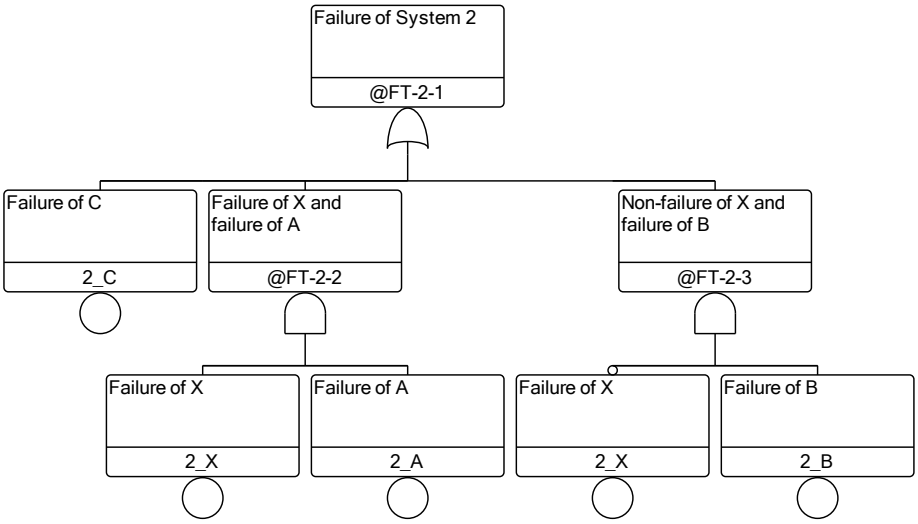

Figure A.2-1: Fault tree model with configurations

Table A.2-1: Minimal cut set list for the FT model with negative logic

Logical ET Success			
No.	**Probability**	**Event 1**	**Event 2**
1	2.0000E-01	2_C	
2	2.0000E-01	2_B	
3	4.0000E-02	2_A	2_X

Logical and Simple Quantification			
No.	**Probability**	**Event 1**	**Event 2**
1	2.0000E-01	2_C	
2	1.6000E-01	2_B	-2_X
3	4.0000E-02	2_A	2_X

Table A.2-2: Comparison for the FT model with negative logic ($p_{failure}$ = 0.2)

	Rare Event	**MCUB**	**MCS BDD**	**Exact**
Log. ET Success	4.4000E-01	3.8560E-01	3.8560E-01	3.6000E-01
Log. and Simple Quant.	4.0000E-01	3.5488E-01	3.6000E-01	

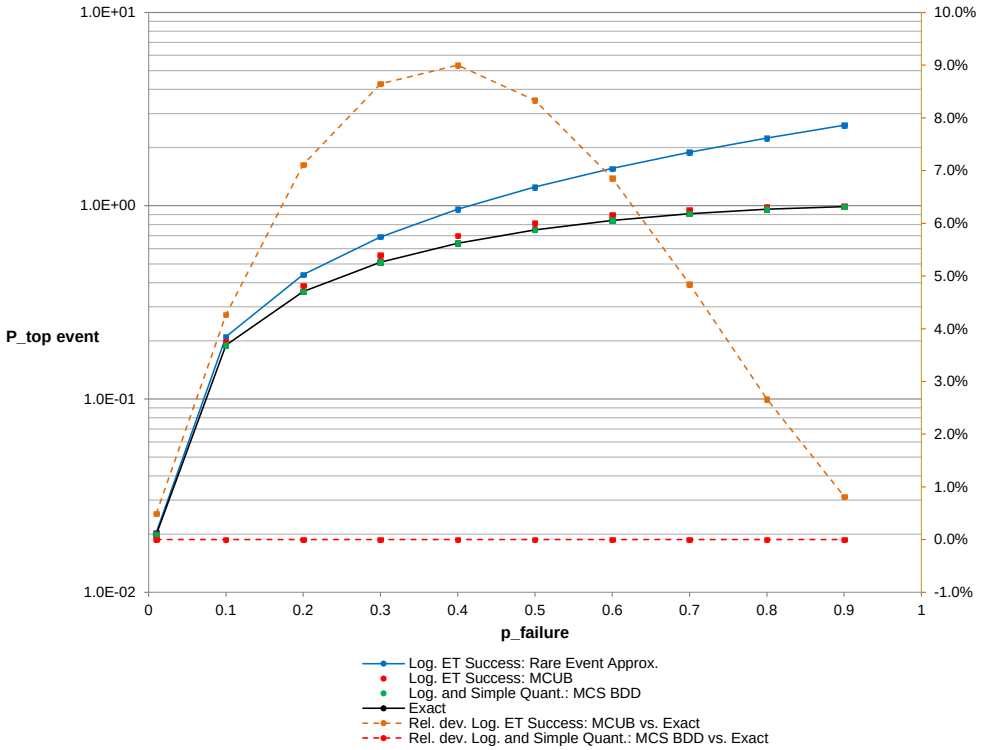

Figure A.2-2: Top event probability as a function of $p_{failure}$ for the FT model with negative logic

APPENDIX A.3: FT with configurations

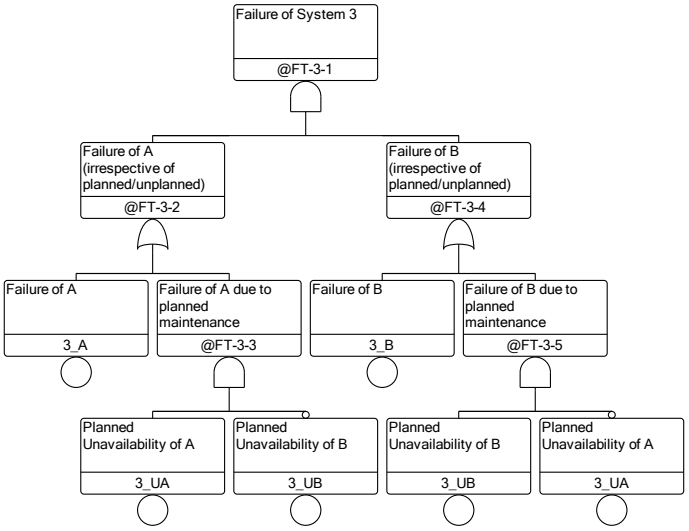

Figure A.3-1: Fault tree model with configurations

Table A.3-1: Minimal cut set list for the FT model with configurations

Logical ET Success			
No.	**Probability**	**Event 1**	**Event 2**
1	4.0000E-02	3_A	3_B
2	1.0000E-02	3_B	3_UA
3	1.0000E-02	3_A	3_UB

Logical and Simple Quantification				
No.	**Probability**	**Event 1**	**Event 2**	**Event 3**
1	4.0000E-02	3_A	3_B	
2	9.5000E-03	3_B	3_UA	-3_UB
3	9.5000E-03	3_A	3_UB	-3_UA

Table A.3-2: Comparison for the FT model with configurations ($p_{failure}$ = 0.2, $p_{maintenance}$ = 0.05)

	Rare Event	**MCUB w/o MUX_{BE}**	**MCUB w/ MUX_{BE}**	**MCS BDD w/o MUX_{BE}**	**MCS BDD w/ MUX_{BE}**	**Exact**
Log. ET Success	6.0000E-02	5.9104E-02	5.9200E-02	5.6000E-02	5.6000E-02	5.6000E-02
Log. and Simple Q.	5.9000E-02	5.8153E-02	5.8240E-02	5.5200E-02	5.6000E-02	

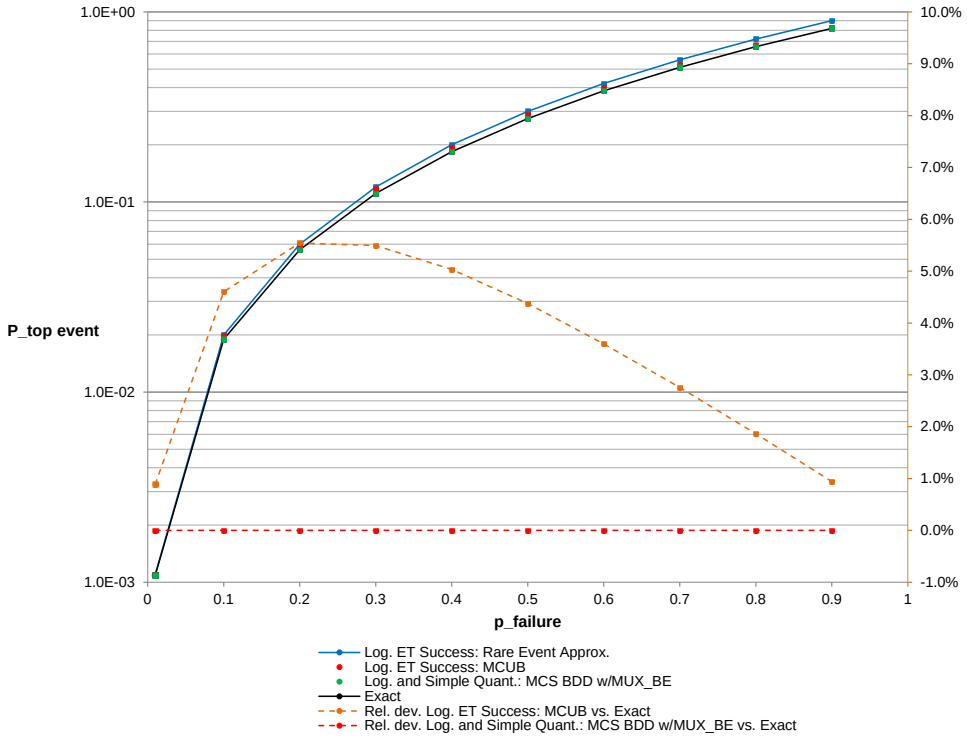

Figure A.3-2: Top event probability as a function of $p_{failure}$ for the FT model with configurations