Introduction and Demonstration of the I&AB Quantification Method as Implemented with RiskSpectrum PSA

Ola Bäckström[a], Marc Bouissou[b], Rory Gamble[a]*, Pavel Krčál[a], Johan Sörman[a] and Wei Wang[a]

[a] Lloyd's Register, Stockholm, Sweden
[b] EDF, Paris, France

Abstract: Current practice for Probabilistic Safety Assessment (PSA) of nuclear power plants translates accident scenarios into a static model where the exact timing of failures leading to the analysed consequence is not taken into account. Components that are required to operate during the transient are often required to operate for the whole accident duration, and can be modelled by mission time basic events, yielding again a static failure probability. The size of real-life PSA models renders a fully dynamic analysis of non-trivial accident scenarios computationally intractable. The I&AB method allows for an efficient analysis of dynamic features in full-scale PSA studies, namely: repairs of components and modelling of the safe state by repairs of initiating events. Accidents where an analysis of a longer duration is of interest might benefit from this method as it incorporates a realistic assessment of repairs. For example, Loss of Offsite Power scenarios caused by an external event might require longer time for grid recovery than the usually assumed 24 hours. We report on an implementation of the I&AB method in RiskSpectrum and its evaluation on large scale PSA models.

Keywords: Dynamic PSA, Repair, I&AB, Large scale PSA models.

1 INTRODUCTION

Standard PSA methodology typically calls for the use of a mission time in calculations. International consensus is to use a 24 hour mission time. What such a calculation really means is that if the undesirable event has not occurred within 24 hours after an initiating event, the system is considered to be in a "safe state", and can no longer fail; the initiating event itself is considered to be repaired. This approach has a number of drawbacks: the choice of the mission time is somewhat arbitrary, and its extension to PSA studies of systems with long sequences due to initiating events with potentially long repair times (such as Loss of Offsite Power at external events), or grace delay times (such as fuel cooling pools) can be excessively conservative. Such systems can be accurately described by dynamic models which use component repair times rather than mission times, and incorporate deterministic failure times (grace delays and deterministic failures due to tanks or batteries with limited capacity). However, dynamic models for PSA of large systems quickly become intractable as the model size increases: analytic solutions using Markov methods suffer from an excessively large state space which cannot be solved with current computers, while Monte Carlo methods suffer from large simulation times because of the high reliability of the system.

The I&AB (Initiator and All Barriers) method developed by EDF [1,2] belongs to recently developed approaches [1,2,8,9] which combine selected dynamic aspects of accidents with existing static PSA models for analysis specification. On the calculation side, they utilise the efficient decomposition of the combinatorial structure into minimal cutsets. Individual cutsets are then quantified by new algorithms which take the dynamic behavior of certain components into account, even though only in an approximate manner. These methods decrease conservatism of the static model while retaining the scalability to real-life PSA studies by efficiency of the static analysis.

The I&AB method provides a way to include repair times of basic events, and captures much of the dynamic behaviour without suffering from the state space blow up of a fully dynamic model. It provides a conservative analytic estimate of the theoretical dynamic solution and therefore offers the

*Rory.Gamble@lr.org

potential to improve the accuracy of results from PSA models. The method operates on cutsets, and uses the relevant repair times for each basic event instead of a generic mission time. The possibility of multiple failure-and-repair cycles of cutset events is considered.

An I&AB quantification package will soon be available for use within the RiskSpectrum family as a collaboration with EDF. This will allow the method to easily be applied to large PSA problems. Existing PSA models may be quantified with only the addition of a small amount of information (repair times for basic events whenever applicable).

We examine the benefits and performance of the algorithm on a number of models: the study of a generic data centre power supply and real, full-scale PSA models from the nuclear industry (modified for confidentiality). We demonstrate the improvement in results that I&AB quantification yields for the reliability estimate of these systems, and explore the sensitivity to accident duration. A comparison of quantification times with standard RiskSpectrum PSA calculations is also made.

This article is organised as follows: the next section recalls the characteristics of current modelling and calculation methods, both in traditional PSA and in dynamic system analysis. Then the main principles of I&AB are explained, and the last section is a demonstration of benefits of the I&AB implementation in RiskSpectrum on various examples, by comparison with dynamic methods on the data centre example, and with traditional PSA calculation on full-scale PSA examples.

2 CURRENT METHODS

2.1 Traditional PSA, Static Methods

Contemporary PSA studies typically apply fault-tree/event-tree analysis to build a static model of the facility. Some dynamic information is encoded in sequences within event trees, with frequency events initiating the sequences and function events capturing the broad dynamic structure. A master fault tree is built, which is then solved to produce an MCS (minimal cutset) list, and these are then in turn quantified and combined to give an overall reliability. Each cutset therefore contains an initiating event, and probability events modelling barrier failures. Their probability can be calculated from a failure rate and a mission time. For events modelling components supposed to function during the whole accident, the mission time is typically 24 hours, by international consensus. The barriers listed in a given cutset are assumed to start functioning at the time of the initiating event. This implies that if any of the barriers of the cutset does not fail during its mission time, then the initiating event has been mitigated, and the system moves to a "safe state". The initiating event is then considered to be repaired.

RiskSpectrum PSA [7] is an advanced tool for constructing and solving fault tree/event tree models of system reliability. The tool allows for full-scale probabilistic safety analysis of entire nuclear power plants, and is licensed for use at more than half of the world's nuclear power plants. The calculation engine RSAT is heavily optimised and allows efficient quantification of a master fault tree containing tens of thousands of basic events, and resulting in hundreds of thousands of minimal cutsets, while using reasonable computational resources. Appropriate use of a cutoff value ensures that a result which identifies the most significant cutsets can be achieved in a reasonable amount of computing time.

The traditional, static PSA method also has a number of drawbacks. In particular, the choice of a mission time is somewhat arbitrary, and is not necessarily related to the repair times of the components in a particular sequence, or the initiating event. Repairs of components in the cutset are not considered, even though in reality a failed component might have the opportunity to be repaired during the mission time. The rationale of this approach leads to increasing the mission time for problems with relatively long sequences, such as cooling pool problems, up to perhaps hundreds of hours. But neglecting the possibility to make repairs during the mission time is likely to make the assessment much too conservative.

*Rory.Gamble@lr.org

In order to illustrate differences between the calculation methods quoted in this section and the next one dedicated to I&AB, we will take a very simple example and show the interpretation of the methods in terms of state graphs. Let us consider a system consisting of three components S1, S2, and S3, with constant failure and repair rates ($\lambda = 10^{-4}$ h^{-1} and $\mu = 0.1$ h^{-1}). In the perfect state, component S1 is in operation and components S2 and S3 are in standby. As soon as S1 fails, S2 starts functioning. When both S1 and S2 are failed, S3 replaces them.

A truly dynamic model, that takes all these hypotheses into account, is the Markov chain of Figure 1. We use a bold font for components in operation and a regular font for those in standby; numbers with bars indicate failed components. Notice that there is only one functioning component in each state. This Markov chain takes into account repairs of all components and, consequently, the fact that the system can repeatedly go back to the perfect state during the mission time. The only possible trajectory (without loop) resulting in the top event is successive failures of S1, S2, and S3.

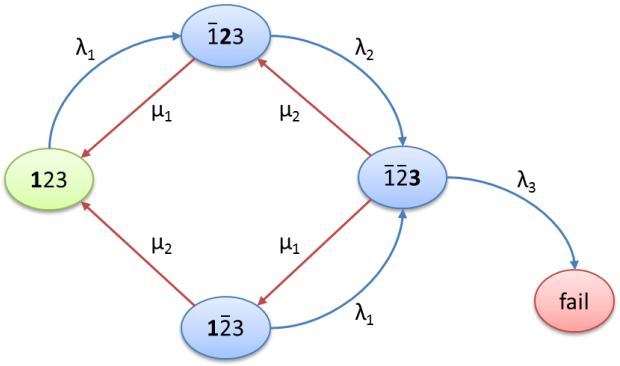

Figure 1. Markov chain modelling the system.

This system can be represented in various ways in RiskSpectrum, for example like Sequence No. 4 in Figure 2.

S1	S2	S3	No.	Freq.	Conseq.	Code
			1			
			2			S3
			3			S2
			4			S2-S3

Figure 2. System representation in RiskSpectrum.

This representation does not capture the fact that S3 is a standby component for S2. Its state graph is presented in Figure 3.

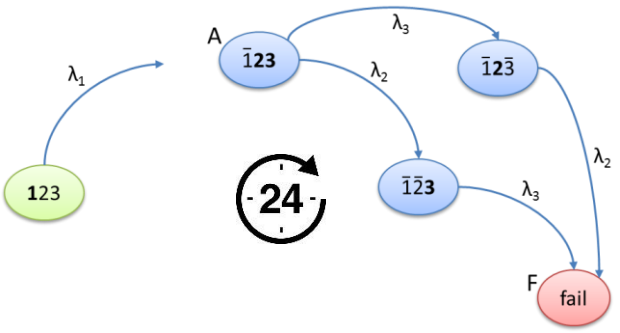

Figure 3. State graph giving the semantics of the PSA model, which excludes repairs

*Rory.Gamble@lr.org

First of all, no repairs are implied. Once an initiating event occurs, the failures of all other components in minimal products corresponding to it are supposed to be independent. In the state graph, we intentionally separate the perfect state from the rest in order to explicitly demonstrate this assumption. Also, the occurrence of the top event given that the initiating event took place is limited by 24 hours.

2.2 Dynamic Methods

Dynamic models capture the full dynamic behaviour of the system, including e.g. the order of component failures in a failure sequence, repair times that are specific to each failing component, the possibility of considering successive failures and repairs, and dependencies between components due to standby redundancies. Importantly, repair rates for individual components are used instead of requiring a mission time that is uniformly applied after a given initiating event.

EDF has developed several methods and tools for creating and quantifying dynamic models. In particular, BDMPs (Boolean logic Driven Markov Processes) are a powerful modelling formalism for the dependability analysis of dynamic systems [3]. BDMPs have a graphical representation close to fault trees, yet they specify (potentially very large) CTMCs (continuous time Markov chains).

Solving dynamic models exactly requires significant resources, and becomes intractable for PSA studies of large systems due to a rapid expansion of the state space. Even the powerful method implemented in the tool Figseq, consisting of a search and quantification of sequences leading to a target state is not applicable for BDMPs with more than a few hundred basic events (this is a very rough statement: in fact the structure of the BDMP is as important as its size). Monte Carlo methods may suffer from excessive simulation times due to the high reliability of the systems under study: a very large number of simulations is required to produce a meaningful statistical picture of the failure modes. In such cases, the most-likely failure modes dominate, and it is difficult to see the contribution of the less-likely modes (this is illustrated in the example of section 4.1). Thus, a BDMP model representing a full-scale nuclear PSA would be intractable with the above cited tools.

But, by using the ability of KB3 [4] to convert various models into static fault trees, it is possible to transform automatically a BDMP into a RiskSpectrum PSA model suitable for quantification by I&AB, which offers a brand new way to quantify very large BDMPs.

3 THE I&AB METHOD

3.1 General principles of I&AB

The I&AB method offers a convenient balance between the static and dynamic methods described in the previous sections. The method was inspired by an insight of [5] noting that the majority of the behaviour of a fully dynamic model is captured by the first-order relationships between the failure of functioning components (i.e. the frequency events) and the standby components which act as barriers to the initial failure (i.e. the remaining basic events in a cutset). The initiating event is modelled as a repairable event which fails with rate λ_i. While it is failed and under repair (with repair rate μ_i), the barriers B_1, B_2, B_3,…, B_n are assumed to immediately begin to function. Barrier events may be either *failure on demand* or *failure in function* type events. Failure on demand events may fail with probability γ at the occurrence of the initiating event. If they fail, they are under repair (with repair rate μ_n), and once repaired they cannot fail again (the system moves to a safe state). Failure in function events fail with rate λ_n and are repaired with repair rate μ_n. Failure in function events continue to operate after repair, and may undergo successive cycles of failure and repair. If at any stage the initiating event is repaired, the system moves to a ‘safe state’ and cannot fail until the next initiating event.

These assumptions correspond to the state graph of Figure 4 for the three-component system introduced in the previous section. It can be seen that this graph is a sort of mixture of the graphs corresponding to the standard PSA and the fully dynamic quantification methods.

*Rory.Gamble@lr.org

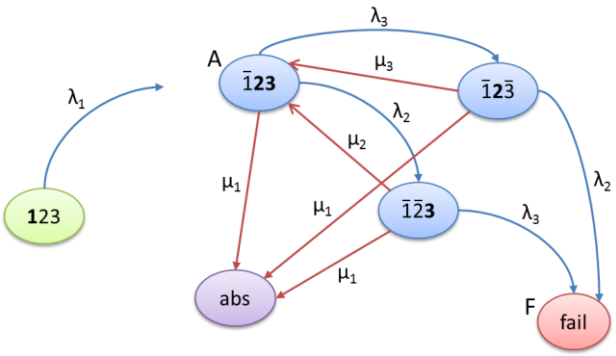

Figure 4. Markov chain corresponding to I&AB assumptions.

The PSA model is solved in the same way as for a static PSA, resulting in a minimal cutsets list to be quantified. These cutsets are then quantified using the I&AB method. This method is an analytic conservative approximation of the CTMC for the cutset. It captures the most important dynamic behaviour of a failure mode (that is, the first-order dependence between failures of barrier components), while offering an approximate analytical method. The reader is referred to [1] and [2] for a detailed description of the calculation. Reference [1] gives the generic equations for the quantification of a cutset, and the procedure to obtain automatically the relevant cutsets from a BDMP, using the fault tree generation function of KB3. Reference [2] gives the detailed analytical formulae for the quantification of a single cutset, and their extension in the case where there are deterministic delays.

It is interesting to look at the numerical results one can obtain on the small three-component system, using various approximations. In Table 1, each column corresponds to a calculation method and the different lines correspond to various hypotheses on the repair rates taken for all three components. The first column is an exact calculation performed on the Markov chain of Figure 1 representing the system unreliability at 10000 hours. The second column displays the system unreliability calculated by a static event/fault tree method which does not take repairs into account. Therefore, the value is the same for all rows. It uses the mission time of 24 hours. The last column shows the results of the I&AB method.

Table 1: comparison of methods precision

Repair rates (h^{-1}) \ Method	**Exact**	**PSA**	**I&AB**
1	5.00E-9	**5.75E-6**	1.00E-8
1/10	4.99E-7		9.99E-7
1/24	**2.86E-6**		**5.74E-6**
1/100	4.85E-5		9.88E-5

The PSA standard method with a fixed mission time yields a result that can be either optimistic or pessimistic compared to the exact value depending on the repair rates of components. I&AB is systematically conservative by a factor of 2 compared to the exact value. This can easily be explained by the fact that it considers both sequences S2, S3 and S3, S2 where only one is in fact possible.

3.2 Common Cause Failure models and repair

For CCF treatment of failure in function events in I&AB, we apply the CCF multiplier β to the failure rate λ of one of the basic events of the CCF group, analogous to the standard probabilistic treatment in PSA.
For CCF probabilities in static PSA:

$$P_{CCF} = \beta P \quad (1)$$

For failure rates of in function failures in I&AB:

$$\lambda_{CCF} = \beta \lambda \quad (2)$$

*Rory.Gamble@lr.org

For a CCF event representing the coupled failure of n in function components, we use a repair rate which is equivalent to summing the time needed to repair all of the basic event components:

$$\mu_{CCF} = \mu/n \qquad (3)$$

We term this a *consecutive* repair model for the CCF event. This is an extremely conservative assumption, for two reasons. First, the CCF event will begin to act as a functioning barrier again as soon as any single event in the CCF is repaired; it is not necessary to repair the entire CCF event to make the barrier function. Second, this model assumes that the repair crew cannot repair more than one component at a time. The entire repair crew is considered to be occupied with repairing one component, and only when that component is completely repaired can work begin on the second component in the CCF. Clearly this is a very conservative representation of a repair scenario in a real facility.

One alternative repair model would be a *concurrent* repair model, where the repair time for the CCF event is the same as for a single component: in this model, it takes no longer to repair the entire CCF than it does to repair just a single component. Equivalently, this could be interpreted as requiring only one component in the CCF event to be repaired in order to restore the function lost because of the CCF event. The first interpretation is potentially non-conservative, since it does not seem reasonable that repairing an entire CCF failure can take the same amount of time as a single event. The second interpretation is also non-conservative: since in function events may fail multiple times, we must ensure that a repair of a CCF event returns the entire CCF event to its initial state.

A full treatment would consider all the possible CCF combinations of failures that are possible for the CCF group to suffer once it has been repaired the first time. These possible failure groupings are higher-order details, and treating them properly falls within the area of fully dynamic modelling. We use the consecutive repair model for CCF repairs, and recognise that this is a conservative treatment, and that the real-world scenario for CCF repairs probably falls somewhere between the two extremes of strictly concurrent and strictly consecutive repairs, with repairs continuing after the first component is repaired and function is restored.

CCF events for failure of on demand components (probabilities) are treated in a straightforward way. The γ_{CCF} value is derived from that of the underlying basic event multiplied by the CCF multiplier β, in an identical way to static PSA. The repair rate for the CCF event is the same as that of the underlying basic event. In the case of on demand components, this is a suitable repair rate because in I&AB, the system moves to a safe state after the repair of on demand events (they cannot fail again).

$$\gamma_{CCF} = \beta\gamma, \qquad \mu_{CCF} = \mu \qquad (4, 5)$$

In section 4.2, we present the results of a large-scale PSA study using the more conservative consecutive repair strategy for CCF events. For the analysis cases shown in that section, the consecutive repair strategy results in a median increase in top value of 7% compared to the concurrent repair strategy. In the worst case, a 28% increase was observed. While this is significant, it should be noted that this analysis case still compares favourably with the corresponding static analysis case (Model 1, Analysis Case 5, 192h) even when using the more conservative consecutive repair strategy.

3.3 Implementation with RiskSpectrum PSA/RSAT

Changes to Quantification Method

All I&AB quantifications presented in this paper are made with an alpha version of RiskSpectrum PSA/RSAT which includes the I&AB quantification method as an add-on. In I&AB, the final quantified cutset value is not a simple product of values from the contributing basic events. This has practical consequences for the master fault tree generation algorithm in RSAT in relation to cutoff and modules. For cutoff, a conservative estimate of the value of a partially-generated cutset is made, and

*Rory.Gamble@lr.org

compared to the cutoff value. Since this value is not exact, it is incompatible with relative cutoff. Relative cutoff is therefore not used in these calculations. Similarly, module values cannot be calculated exactly; a conservative estimate for module values is also used in cutoff. Cutsets containing modules must be demodularised before they can be quantified with the I&AB method. A further cutoff check is applied to the cutset values during demodularisation, once the I&AB value has been calculated. Both of these changes result in a decrease in MCS generation performance compared to the quantification of the static method.

The I&AB quantification of MCS lists is also significantly more complex [1] than for static PSA quantification (which uses a simple product of basic event values) and this leads to corresponding increases in computation time. This is not a problem for single quantification of MCS lists where the quantification time is still quite manageable. Upcoming versions of RSAT will implement a quantification method which is efficient for the repeated calculations which are required for importance or uncertainty analysis of the MCS list.

Model Conversion

The *Repairable* reliability model defined in RiskSpectrum PSA requires some extra consideration when using I&AB. This model represents the fraction of time that a normally-running component is unavailable due to maintenance or repairs. The model requires failure rate and repair rate (specified as a mean time to repair, MTTR) as mandatory parameters, which are used to calculate an unavailability:

$$Q(t) = \frac{\lambda}{\lambda+\mu}[1 - \exp(-(\lambda+\mu)t)], \qquad Q_{mean} = \frac{\lambda}{\lambda+\mu} \qquad (6, 7)$$

The intent of this model is not to include repairs to the component during the sequence. The I&AB interpretation of repairable events is complex. They behave as failure on demand events with well-defined failure probabilities Q_{mean}. In addition, the components that they describe are required to run continuously during the accident sequence and therefore can be interpreted as in function events. A future version of RiskSpectrum PSA will allow a convenient way for repairable events to express a combination of these characteristics, i.e. both a maintenance repair rate used for the static repairable model, and a sequence repair rate which is used in I&AB.

Conversion of all other basic event reliability models for use with I&AB is straightforward. Each basic event in the model requires a repair rate to be specified, and all other reliability data required for the calculation are already present in the static PSA model. There is a direct mapping of the RiskSpectrum PSA reliability models to the I&AB reliability models (initiators, failure in function and failure on demand).

4 DEMONSTRATION

We demonstrate the capabilities of the RiskSpectrum implementation of the I&AB method by comparing it to both fully dynamic calculations and to the standard static PSA method. First, we present a non-trivial dynamic model of a real system – electrical supply of a data centre. Its size allows for fully dynamic analysis methods, but it can be also translated into a fault tree and analysed in RiskSpectrum by the standard static method and by the I&AB method.

Secondly, we report results obtained from large real-life PSA models by the I&AB method. This illustrates precision gains one can obtain on full PSA studies when taking some dynamic aspects into account: the I&AB method is used to consider repairs of (some) components and models the safe state by a repair of initiating events rather than by a fixed mission time. Note that the size of these analyses is prohibitive for a fully dynamic analysis by the tools used on the data centre electrical supply system.

4.1 Comparison to a dynamic analysis: Electrical Supply of a Data Centre

*Rory.Gamble@lr.org

The purpose of this section is to show on a non-trivial example, how well the I&AB method performs in terms of precision when it is compared to a precise calculation, made by Markov analysis techniques or Monte Carlo simulation. The system to be studied is represented in Figure 5. Red dotted arrows indicate the priorities of various paths from the GRID to the bus bars BBA3 and BBB3 which power the servers of the data centre. The normal paths are through TA for both of them. The component denoted BAT (in fact a battery and a DC/AC converter) is used as a last resort, and provides a grace time of 2 hours when all other sources are lost. Its failure rate is neglected. The undesirable event to quantify is the simultaneous loss of supply on BBA3 and BBB3 before 10000 hours of system operation. This is the "top value" of Table 3.

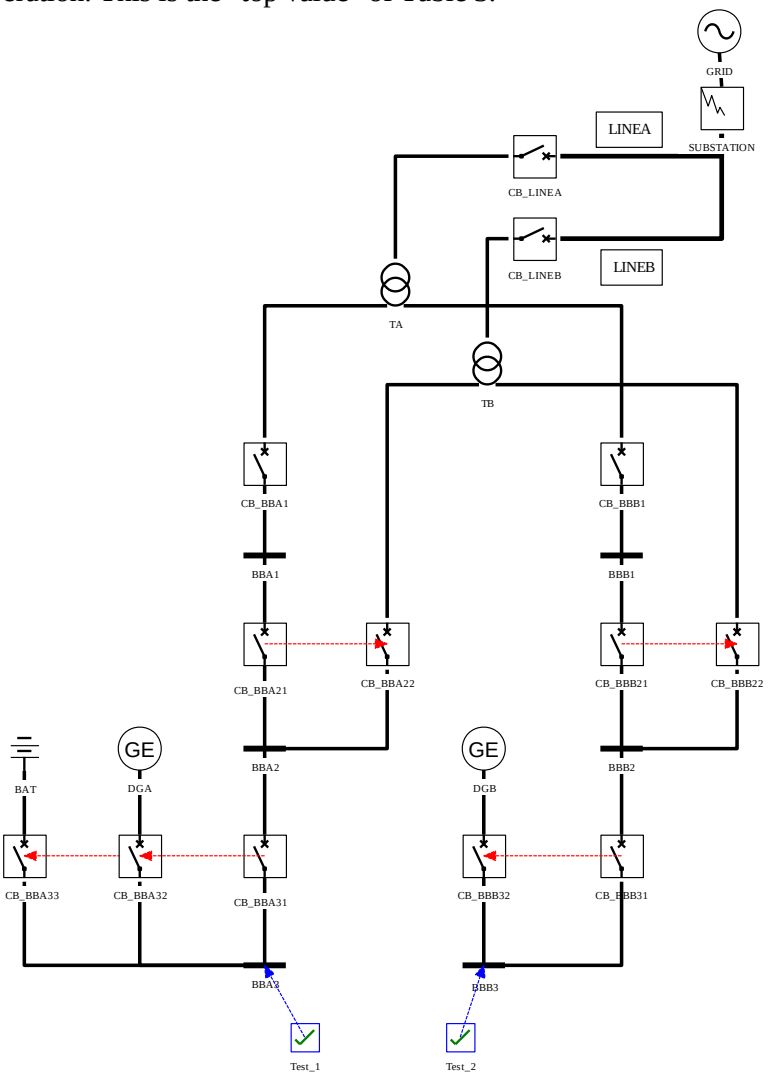

Figure 5. Generic architecture of a data centre power supply

*Rory.Gamble@lr.org

Table 2: reliability data of components of Figure 5.

Component type/failure mode	gamma Probability of failure on demand	lambda/h Failure rate (constant)	mu/h Repair rate (constant)
Circuit breaker/refuse to open	2E-4		1/5
Circuit breaker/refuse to close	2E-4		1/5
CB_LINEA, CB_LINEB short circuit		1E-7	1/5
Circuit breaker/short circuit (all other circuit breakers)		5E-7	1/5
Bus bar short circuit		2E-7	1/50
Transformer short circuit (TA, TB)		5E-6	1/200
Diesel generators long failures	2E-3	5E-4	1/200
Diesel generators short failures		2E-3	1/10
GRID failure in function		1E-5	1/10
SUBSTATION		1E-6	1/20
Lines LINEA, LINEB		2E-5	1/5
Simultaneous failure of DGA and DGB by CCF	2E-4	5E-5	1/400
Simultaneous failure of LINEA and LINEB by CCF		1E-6	1/200

The corresponding BDMP has 42 leaves and 25 gates. It is much simpler, but has a structure similar to the structure of the BDMP given exhaustively in [6]. Thanks to the KB3 workbench, this single model can be processed in four different ways: by Figseq, YAMS (Monte Carlo simulator), and transformation into a fault tree which can be quantified by RiskSpectrum, either by the dynamic I&AB method or by a standard static PSA. The fixed time transition (battery depletion) is replaced by an exponential transition in the Figseq analysis. The mission time considered in the static PSA calculation by RiskSpectrum was 24 hours. Table 3 compares the four kinds of calculation.

Table 3: I&AB compared to methods for dynamic models

Solver name	**Solver principle**	**CPU [s]**	**Top value**	**Absolute cutoff**	**Qualitative results**
Figseq	Search and quantification of sequences in Markov chain.	12	9.23E-4	1E-9	1542 first sequences
YAMS	Monte Carlo simulation	180	7.98E-4 +-4E-5		9 sequences **among** the first ones
KB3 + RiskSpectrum	Fault tree generation + I&AB	3	9.55E-4	0	68860 cutsets (exhaustive)
KB3+ RiskSpectrum	Fault tree generation + Static PSA	3	2.67E-3	0	68860 cutsets (exhaustive)

The results show that the I&AB method produces a result close to the fully dynamic methods in a fraction of the calculation time. It also generates substantially more cutsets which can be an advantage for, e.g., importance and uncertainty analyses. When compared to the static PSA, the I&AB method generates the same set of minimal cutsets and the top value is approximately three times lower. More importantly, *cutsets are not sorted in the same order as in the static analysis*. This means that basic events would get incorrect importance in the static analysis.

4.2 Large Scale PSA Models

The aim of the evaluation on large scale PSA models is to illustrate advantages of the I&AB method for real-life analyses in the nuclear industry. We calculate frequencies of serious consequences (mostly core damage) by the usual static method and by I&AB. The I&AB method brings two important features which make the comparison of top frequencies less straightforward: (i) the accident duration is not specified by an upper bound, but by a repair rate on the initiating event and (ii) one can let failed components be repaired by assigning repair rates to them.

*Rory.Gamble@lr.org

There is no simple relation between an upper bound on accident duration and a mean accident duration. If we compare results from an analysis which uses 24 hours mission time (upper bound) with another analysis which uses 24 hours MTTR then clearly the latter is more conservative. In an exponential distribution, the mean value is at the 63rd percentile. In 27 percent of accidents, the duration will exceed 24 hours. In fact, in 13 percent, it will exceed 48 hours, in 5 percent it will exceed 72 hours and in 2 percent it will exceed 96 hours. What is a reasonable upper bound in this case? We evaluate top frequencies with different mission times and different mean repair times of initiating events and allow readers to compare the results themselves.

The 24 hours bound on accident duration is appropriate in many scenarios, typically for certain classes of internal events. In other situations, a conservative analysis might require accounting for longer accident duration. For instance, a loss of offsite power (LOOP) caused by an external event might be impossible to repair within a short time. Counting with a horizon over 100 hours might be necessary. Level 2 analyses or analyses of other types of problems like spent fuel pool cooling also require a long mission time. An application of I&AB to pool cooling problems is presented in a separate paper [10]. Here, we especially focus on Level 1 LOOP accidents and evaluate frequencies of severe consequences, for longer mission times in the static model and longer MTTRs of the initiating event in I&AB.

There is no natural way of specifying component repairs in standard PSA models. One could add basic events for failures to repair essential equipment or one could include the failure to repair a component into its original failure probability (i.e., a component has failed and an attempt to repair it has also failed). Both methods suffer from various drawbacks. The I&AB method allows engineers to specify repairs by a repair rate (or, equivalently, by a mean time to repair). The quantification then takes the dynamic behavior into account (in an approximate way). It accounts for failures at different time points, with repairs starting afterwards and in parallel with the repair of the initiating event, and possible subsequent failures of repaired components.

Clearly, one can expect lower top event frequencies from models with repairs compared to models which do not take repairs into account.

We have selected three large real-life PSA models for our evaluation and modified them for confidentiality:

- Model 1 and Model 2: Analysis cases chosen are those which make the biggest contribution to core damage.
- Model 3: Analysis cases with important Mission Time events are selected for analysis, i.e. those analyses for which I&AB is likely to have a large impact for long accident durations. (ACs 1, 2, 3). A Core Damage analysis over all initiators is added for comparison (AC 4).

These analysis cases each involve several thousand gates and basic events. Largest analyses have more than ten thousand gates and four thousand basic events. All analyses include CCF events and modules.

The numerical results we present illustrate differences between the static and I&AB methods and show situations in which gains from the I&AB method are significant. We investigate the behavior of models for accident durations t = 24h, 48h, 96h, 192h. Static PSA models are modified by changing all mission time parameters with value in the range [24h, t] to t. The same models are modified for use in I&AB by setting a corresponding repair rate on initiating events (μ=1/24, 1/48, 1/96, 1/192 h^{-1}). Repair rates for the other basic events are set to:

- 1/20 h^{-1} for failure in function events (for all initiating event repair rates)
- Zero (no repairs) for failure on demand events. An exception to this is analysis case 3 of Model 2.
- Mission time events less than or equal to 20 hours are assigned values from their static PSA interpretation (a Q value is calculated and considered as an on demand failure, without repair). This is because a component with a short mission time is considered to not be repairable during the accident sequence.

*Rory.Gamble@lr.org

- We treat all repairable events as in function events. The λ parameter is used directly, while the MTTR parameter defined for the repairable event is ignored: instead, μ is set in exactly the same way as for other in function basic events.
- CCF events are assigned repair rates according to the CCF model of Section 3.2.

Table 4: Summary of static calculations on large scale PSA models

Model	Analysis case	Top frequency (1/year), for Mission Time			
		24h	48h	96h	192h
M 1	AC 2	1.60E-07	1.76E-07	2.03E-07	2.40E-07
	AC 3	6.81E-09	1.12E-08	2.30E-08	5.62E-08
	AC 4	1.52E-08	2.63E-08	5.81E-08	1.59E-07
	AC 5	7.64E-09	1.47E-08	3.34E-08	9.52E-08
	AC 6	1.77E-10	2.64E-10	5.45E-10	1.98E-09
M 2	AC 1	1.17E-05	1.41E-05	2.01E-05	3.96E-05
	AC 2	1.08E-06	1.77E-06	3.72E-06	1.22E-05
	AC 3	2.05E-06	3.93E-06	7.91E-06	1.76E-05
M 3	AC 1	3.16E-07	4.10E-07	7.17E-07	2.05E-06
	AC 2	3.87E-08	7.54E-08	2.21E-07	9.58E-07
	AC 3	1.94E-07	2.97E-07	5.96E-07	1.65E-06
	AC 4	4.37E-06	4.85E-06	6.12E-06	1.03E-05

Table 5: Summary of I&AB calculations on large scale PSA models

Model	Analysis case	Top frequency (1/year), for IE MTTR			
		24h	48h	96h	192h
M 1	AC 2	1.57E-07	1.73E-07	1.96E-07	2.28E-07
	AC 3	6.16E-09	9.71E-09	1.70E-08	3.12E-08
	AC 4	1.37E-08	2.24E-08	4.06E-08	7.71E-08
	AC 5	7.25E-09	1.30E-08	2.52E-08	5.02E-08
	AC 6	1.61E-10	2.43E-10	3.89E-10	6.75E-10
M 2	AC 1	1.10E-05	1.20E-05	1.34E-05	1.69E-05
	AC 2	7.79E-07	1.09E-06	1.42E-06	2.36E-06
	AC 3	2.04E-06	3.89E-06	7.58E-06	1.48E-05 1.74E-06*
M 3	AC 1	3.15E-07	3.82E-07	5.09E-07	7.16E-07
	AC 2	3.82E-08	6.07E-08	1.07E-07	1.92E-07
	AC 3	1.91E-07	2.87E-07	4.74E-07	8.48E-07
	AC 4	4.33E-06	4.79E-06	5.54E-06	6.79E-06

A number of conclusions may be drawn by comparison of Tables 4 and 5, while bearing in mind the differences between an upper bound on accident duration and a mean accident duration (a 24h mean repair time includes a significant likelihood that the accident duration is >24h). For 24h accident durations, the results of the I&AB method are comparable to the static method, showing a modest decrease in top value across the analysis cases studied. This indicates that the static PSA method is sufficient in 24h mission time scenarios, though it does not hurt to use I&AB.

For long accident durations, the benefits of I&AB over the static PSA method can be very significant: in the most dramatic cases the I&AB results are approximately one fifth of the static values. Due to the differences in upper bound vs mean accident duration, it is relevant to compare the I&AB 96h and static 192h results also, in which case the I&AB results can be close to one tenth of the static results. This shows that I&AB can have a significant impact for long accident durations: because repair during the accident sequence is possible, and taking these repairs into account can have a drastic effect on the results obtained. Accidents caused by certain initiators, such as Loss of Offsite Power caused by external events, are appropriate to study with long accident duration times, as these events can take a long time to repair. Here, I&AB can greatly reduce the conservatism of the static approach.

*Rory.Gamble@lr.org

Comparing the differences in results across models and analysis cases chosen, we note that I&AB has a much more significant effect when it is applied to analysis cases which have mission time events with a high importance. The impact of the I&AB method is reduced (but still significant) when applied to the important analysis cases in a model (Models 1, 2 and AC 4 of Model 3) without deliberately targeting those analysis cases which show the greatest benefit with I&AB.

The impact of repairs on failure on demand events is not thoroughly investigated in this study. We did not have reliable repair information for these events, and allowing repair on these introduces yet another advantage to the I&AB method. The results show that the I&AB method can yield a significant improvement even when only considering repair of in function failures, which are central to the dynamic aspect of I&AB. Nonetheless, we were able to easily isolate an important failure on demand event in one case (the HRA event of Model 2, Analysis Case 3, marked with an asterisk). Allowing repairs for this event showed nearly an entire order of magnitude improvement in the result. Clearly these results show that the I&AB method can be used in a targeted way, allowing the modeller to concentrate efforts where there will be the most significant impact.

5 CONCLUSION

The I&AB method, implemented with RiskSpectrum PSA as a collaboration between Lloyd's Register and EDF, provides a means of analysing certain dynamic aspects in full-scale PSA studies. It replaces mission times by repairs of initiating events and it takes repairs of components into account, including repeated failures. Preparing existing PSA models for I&AB quantification requires only minor changes: repair times for initiating events and selected (by a PSA engineer) basic events in the model need to be provided. The method reduces the conservatism of the static model, especially when an analysis with longer accident duration is relevant. Decreases in the top frequency value between 50-90% are demonstrated for certain analyses with longer accident duration in large-scale contemporary PSA models. More importantly, as shown on the first example, I&AB has the potential to completely reorder the dominant cutsets if repair rates depend on components and do not have uniform values, like in the experiments we performed. This can greatly improve the optimisation of resources for improving the safety of nuclear power plants.

5.1 References

[1] M. Bouissou and O. Hernu. "*Boolean approximation for calculating the reliability of a very large repairable system with dependencies among components*", Proc. ESREL 2016, Glasgow, (2016).
[2] M. Bouissou. "*Extensions of the I&AB method for the reliability assessment of the spent fuel pool of EPR*" ESREL 2018, Trondheim, June 2018.
[3] M. Bouissou, J.L. Bon. "*A new formalism that combines advantages of fault-trees and Markov models: Boolean logic driven Markov processes*", Reliab. Eng. Syst. Saf. 82: 149-163, (2003).
[4] M. Bouissou, "*Automated dependability analysis of complex systems with the KB3 workbench: the experience of EDF R&D*", Proc. CIEM 2005, Bucharest, (2005).
[5] J. Collet, *"An extension of Boolean PSA methods"*. Proc. PSA'95, Seoul, 1995.
[6] M. Bouissou. "*A Benchmark on Reliability of Complex Discrete Systems: Emergency Power Supply of a Nuclear Power Plant*", Proc. of MARS 2017, Uppsala, 2017.
[7] RiskSpectrum PSA software, http://www.riskspectrum.com
[8] Krcal, J. & Krcal, P., "*Scalable Analysis of Fault Trees with Dynamic Features*", Proc. of the International Conference on Dependable Systems and Networks. DSN '15 (2015)
[9] Bäckström, O. & Butkova, Y. & Hermanns, H. & Krcal, J. & Krcal, P., "*Effective Static and Dynamic Fault Tree Analysis"*, Proc. of SAFECOMP'2016 (2016)
[10] A. Olsson, *"Leaving mission times backstage and taking repair into account in long term scenarios"*, #149 PSAM 14, (2018)

*Rory.Gamble@lr.org