Extensions of the I&AB method for the reliability assessment of the spent fuel pool of EPR

Marc Bouissou

Extensions of the I&AB method for the reliability assessment of the spent fuel pool of EPR

M. Bouissou
EDF Lab Saclay, 7 Bd Gaspard Monge, Palaiseau 91120

ABSTRACT: The I&AB (Initiator and All Barriers) method was first introduced at ESREL 2016, as an efficient means to calculate, thanks to closed form formulae, the reliability of a very large repairable system with dependencies among components. The mathematical support of I&AB is continuous time Markov chains, and therefore it cannot be used for modeling the spent fuel pool of a nuclear power plant, because for this system, there are two kinds of *deterministic delays* that must be taken into account: grace times (for example, after the total loss of cooling of the pool, it takes exactly 14 hours for the water to start boiling), and deterministic failures due to the limited capacity of water tanks. In the present paper, we extend the I&AB method to account for deterministic delays. We explain how we could apply this method in the case of the fuel pool of the EPR (European Pressurized Reactor) starting from a model in the form of a BDMP (Boolean logic Driven Markov Process), and how results and computation times compare to a Monte Carlo simulation of the same BDMP.

1 INTRODUCTION

The standard PSA method (based on fault tree linking) is not well suited for the reliability assessment of the spent fuel pool of a nuclear power plant, for several reasons. Firstly, the dynamics of the phenomena to be modeled are relatively slow because of the large amount of water available in the pool itself and in the safety systems. It is thus not sufficient to look at what can happen in only 24 hours after an initiator. Secondly, the fact that components are repairable, and the existence of multiple standby redundancies cannot be ignored.

EDF has developed several tools for creating and quantifying dynamic models, better suited for this kind of system study. In particular, BDMPs (Boolean logic Driven Markov Processes) are a powerful modeling tool for the dependability analysis of dynamic systems (Bouissou & Bon 2003). For more than ten years, they have been used for assessing the reliability, availability, and safety of complex reconfigurable systems. BDMPs have a graphical representation close to fault trees, yet they specify (potentially very large) CTMCs (continuous time Markov chains). A BDMP model with the same detail level as fault trees of a standard PSA would not be quantifiable by analytical methods, even with classical approximations. On the other hand, it would require too large computation times with Monte Carlo simulation, because the probability of reaching a too low level in the spent fuel pool is very small.

For these reasons, we have developed a new approximate method for the quantification of very large BDMPs, and more generally any model able to generate minimal products containing one initiating event and the failures of the barriers activated after it in order to avoid the undesirable event. This is why the main foreseen application domain is nuclear PSA, all the more so as existing PSA models will be very easy to adapt to I&AB, merely by adding repair rates to component data. In a PSA context, I&AB can be used to take repairs into account instead of postulating that 24 hours after an initiating event, either the undesirable event is unavoidable, or the system is in a safe state. The I&AB (Initiator and all barriers) main principles were published in a paper at ESREL 2016 (Bouissou & Hernu 2016). In the present paper, we give all analytical formulae of I&AB and of its extension in the case of grace times and deterministic failures. We also give some numerical application examples, comparing the I&AB approximation to "exact" calculations performed on a dynamic model via Monte Carlo simulation.

2 THE INITIAL I&AB METHOD (2016)

2.1 Hypothesis on the system and definitions

Suppose we want to calculate the reliability of a repairable system with standby redundancies; it may be a good approximation to take into account only one level of dependences between the components. In

other words, one is capable to distinguish failures of "normal" components (they are called "initiating events") and failures of components in standby (that function only in case of failures of normal components). But one cannot discriminate between a component of "primary standby" (that assures the functioning of the system after a failure of the corresponding normal component) and a component of "secondary standby" (that operates only after a failure of the primary standby component).

The I&AB method relies on the two following approximations:

A0: When an initiating event occurs, all standby components are supposed to start functioning (or maybe refuse to start) immediately after the initiating event; then, they may fail and be repaired independently from each other until the initiating event is repaired.

A1: Once an initiating event is repaired, the system cannot anymore fail, whatever happens.

We suppose that the real system is described by a CTMC where the initial, "perfect" state is the state into which the system always returns, until it is absorbed by a failure state. Then its unreliability can be estimated from the following formula (Bouissou & Bon 1992):

$$\bar{R}(t) \leq 1 - \exp(-\Lambda p t) \quad (1)$$

where Λ is the frequency of initiating events (sum of rates of all transitions exiting the initial state) and p is the probability that the initiating events lead to an accident before the system goes back to the perfect state.

In I&AB, in order to estimate p we use the "minimal content of (failure) sequences" (MCS) of the Markov chain, as it was defined in (Bouissou 2006). The formal definition of a MCS is given ibid, but it can be defined informally as the result of a Boolean reduction of the following fault tree: a single OR gate with one son per failure sequence, each son being presented as an AND gate over the events appearing in the sequence. Initiating events must be distinguished from other events, so that for example, the MCS of a system made of 2 components Y and Z in active redundancy is {Y_init, Z} {Z_init, Y} and not simply {Y, Z}.

For real, complex systems, the MCS can be obtained in (at least) two ways: by building a PSA type model made of event trees and fault trees, and calculating its minimal cut sets, or by building a BDMP and applying the steps described in (Bouissou & Hernu 2016) to transform it into a standard fault tree whose minimal cut sets are the MCS of the Markov chain specified by the BDMP. In the remainder of the paper, we will therefore suppose that we have the MCS of the studied system at hand, and we will call its elements "minimal products".

2.2 I&AB general formulae

Let us suppose that there are n initiating events that can lead out the system from its perfect state. Then, according to (1), the system unreliability at time t can be found from

$$\bar{R}(t) \leq 1 - \exp(-t \sum_{ie=1}^{n} \lambda_{ie} p_{ie}) \quad (2)$$

where λ_{ie} is the failure rate of initiating event ie and p_{ie} includes probabilities for all k minimal products corresponding to it.

In calculations we distinguish two time intervals. The first interval is the mission time figuring in (2). The second time interval is *infinite* and starts once an initiating event takes place. The probability that all components in a minimal product c fail within time interval $[0, \infty[$ is simply the unreliability of a parallel system made of these components $\overline{R_c}(\infty)$; then we can use the following upper bound for p_{ie}, that will be a good approximation when all failure probabilities are small:

$$p_{ie} \leq \sum_{c=1}^{k} \overline{R_c}(\infty) \quad (3)$$

Using the Murchland approximation, we obtain:

$$p_{ie} \leq \sum_{c=1}^{k} \mathrm{E}\big(N_c(\infty)\big) \quad (4)$$

where $N_c(\infty)$is the number of failures of the minimal product c on an infinite horizon. What keeps p_{ie} small is the fact that in the initial state considered for c, the initiating event is realized with probability 1, but once repaired, it never fails again, contrary to other elements of the product. (this is the approximation *A1*).

In order to calculate $\mathrm{E}\big(N_c(t)\big)$ we need to give first a few definitions. We will utilize the following reliability characteristics:

- Unavailability $Q(t)$ – the probability that a component is in a failure state at time t;
- Unconditional failure intensity $W(t)$: $W(t)\Delta t$ is the mean number of failures of a component between t and $t + \Delta t$.

For markovian basic events, depending on their type, these quantities are given by the following expressions:

- Initiating event (the repair is definitive)

$$Q(t) = \exp(-\mu t)$$

$$W(t) = 0$$

- Failure in operation (it can fail several times)

$$Q(t) = \frac{\lambda}{\lambda + \mu}[1 - \exp(-(\lambda + \mu)t)]$$

$$W(t) = \lambda\big(1 - Q(t)\big)$$

- Failure on demand (the repair is definitive)

$$Q(t) = \gamma \exp(-\mu t)$$

$$W(t) = 0$$

Because of the lack of space, we will not recall here the demonstration given in (Bouissou & Hernu 2016) that leads to the following formula, written for a minimal product *c* containing *l* failures on demand and *m* failures in function.

$$\mathrm{E}\big(N_c(t)\big) = \prod_{i=1}^{l} \gamma_{c,i} \times \int_0^t \exp\big(-\mu_{c,ie}x\big) f(x)dx \qquad (5)$$

with

$$f(x) = \exp\big(-x\sum_{j=1}^{l}\mu_{c,j}\big)\sum_{i=1}^{m} W_{c,i}(x)\prod_{\substack{j=1\\ j\neq i}}^{m} Q_{c,j}(x).$$

Equation (5) assumes that a minimal product contains at least one basic event with a failure in operation. However, sometimes minimal products are only composed of basic events corresponding to failures on demand (plus one initiating event, as usually). In such a case, we suppose that these events happen at $t = 0$ and the unreliability for minimal product *c* is given by:

$$\overline{R_c}(\infty) = \Pr(\text{top} = \text{true at } t = 0) = \prod_{i=1}^{l} \gamma_{c,i}. \qquad (6)$$

2.3 I&AB formulae in the markovian case

The general equation (5) yields a closed form formula in the purely markovian case, where all components have constant failure and repair rates.

In order to simplify notations, we will omit the index *c* in the remainder of this section: we will implicitly give formulas for a single minimal product.

Taking an infinite time horizon and replacing $W_i(x)$ by its expression given in section 2.2 for a failure in operation, equation (5) becomes:

$$E\big(N(\infty)\big) = \prod_{i=1}^{l} \gamma_i \times \int_0^{\infty} \exp(-\mu_{ie}x) f(x)dx \qquad (7)$$

with

$$f(x) = \exp\big(-x\sum_{j=1}^{l}\mu_j\big)\sum_{i=1}^{m}\lambda_i\big(1 - Q_i(x)\big)\prod_{\substack{j=1\\ j\neq i}}^{m} Q_j(x) =$$

$$\exp(-x\sum_{j=1}^{l}\mu_j)\sum_{i=1}^{m}\lambda_i\left[\prod_{\substack{j=1\\ j\neq i}}^{m} Q_j(x) - \prod_{j=1}^{m} Q_j(x)\right].$$

Here we need to introduce new notations in order to simplify upcoming formulas. Let:

$$\mu = \mu_{ie} + \sum_{j=1}^{l}\mu_j$$

$$r_i = \lambda_i + \mu_i$$

Hence, replacing the functions Q_j by their definitions and using these new notations, we obtain:

$$E\big(N(\infty)\big) = \prod_{i=1}^{l}\gamma_i \sum_{i=1}^{m}\lambda_i \times$$

$$\left(\prod_{\substack{j=1\\ j\neq i}}^{m}\frac{\lambda_j}{r_j}\int_0^{\infty} e^{-\mu x}\prod_{\substack{j=1\\ j\neq i}}^{m}(1-e^{-r_j x})\,dx - \prod_{j=1}^{m}\frac{\lambda_j}{r_j}\int_0^{\infty} e^{-\mu x}\prod_{j=1}^{m}(1-e^{-r_j x})\,dx\right). \qquad (8)$$

Each integrand includes a product of functions, which can be represented in the following way:

$$\prod_{j=1}^{m}(1-e^{-r_j x}) =$$

$$= 1 - \sum_{i=1}^{m} e^{-r_i x} + \sum_{i=1}^{m} e^{-r_i x}\sum_{j>i}^{m} e^{-r_j x} - \sum_{i=1}^{m} e^{-r_i x}\sum_{j>i}^{m} e^{-r_j x}\sum_{k>j}^{m} e^{-r_k x} + \cdots +$$

$$(-1)^m \exp(-\sum_{i=1}^{m} r_i x). \qquad (9)$$

Hence, after the integration from 0 to infinity, we obtain an alternating series, every term of which, in its turn, is a sum of fractions. For instance, the second integral results in:

$$\int_0^{\infty} e^{-\mu x}\prod_{j=1}^{m}(1-e^{-r_j x})\,dx = \frac{1}{\mu} - \sum_{i=1}^{m}\frac{1}{\mu+r_i} + \sum_{i=1}^{m}\sum_{j>i}^{m}\frac{1}{\mu+r_i+r_j} - \sum_{i=1}^{m}\sum_{j>i}^{m}\sum_{k>j}^{m}\frac{1}{\mu+r_i+r_j+r_k} + \cdots$$

$$\ldots + (-1)^m(\mu + \sum_{i=1}^{m} r_i)^{-1}. \qquad (10)$$

The first integral is calculated in a similar way, the only difference is that one should exclude current element i from the product.

These analytical formulae (8) and (10) seem very cumbersome; however, they permit to considerably reduce the processing time (in comparison with a numerical integration) while ensuring an excellent accuracy.

3 I&AB EXTENSIONS

3.1 Taking grace times into account

In this section, the focus is on systems such that, after the loss of all components subject to random failures in a minimal product, the undesirable event is delayed by some physical process that guarantees a deterministic grace time. The spent fuel pool is a good example: after the complete loss of the cooling system, the water will heat until it boils, but this process is deterministic and it would give an excessively conservative evaluation to replace the grace time by a random delay, exponentially distributed in order to stay in the markovian framework.

We first suppose that we need to quantify minimal products containing failures of components (with the same hypotheses as in § 2.3) and a single deterministic grace time. Let X_c be the failure time of the set A_c of markovian elements of the minimal product *c*, Y_c the time needed to repair at least one of the markovian components, starting from the state where they are all failed, and T_c the grace time. For sake of simplicity, we suppose that after a given occurrence of the initiator, the basic event corresponding to the grace time behaves like a Heaviside function: it becomes true at $X_c + T_c$ and stays true forever (it is "not repairable"). The probability p_{ie} to go from the state where the system is just after the initiator *ie* to the failure state can be estimated as:

$$p_{ie} \approx \sum_{c=1}^{k} E\big(N_c(\infty)\big)\cdot \Pr(Y_c > T_c). \qquad (11)$$

The total repair rate when all markovian components are failed is the sum of their repair rates. Hence

$$\Pr(Y_c > T_c) = \exp\left(-T_c \sum_{i \in A_c} \mu_i\right). \quad (12)$$

As for $E\left(N_c(\infty)\right)$, it can be computed using the formulae of §2.3.

To conclude this section, let us mention that the grace delay may depend on the minimal product, and that a minimal product can contain two or more grace delays: in this case, only the *last one* must be taken into account (cf. §4.1.2 for more details about this choice).

3.2 Taking deterministic failures into account

If, after a non-recovered loss of cooling, the water starts to boil in the fuel pool, there is a possibility to add water coming from tanks. However, the capacity of tanks is limited and after a given time the water flow is interrupted: this is what we call a deterministic failure. After a given initiator, such failures can be considered as non-repairable: it is impossible to replenish the tanks in a short amount of time (the same applies to batteries). However, in a dynamic model, they can be associated to a repair (with a small repair rate, see discussion on that topic in §4.1.2) in order to allow the model to return to its initial state. In order to be consistent with general assumptions of I&AB, we will suppose that the "timers" associated to deterministic failures start just after the initiating event; this is obviously conservative, as in fact they start after some failures. This assumption has an immediate consequence: if there are two or more deterministic failures in a minimal product, the one associated to the greatest delay suffices to prevent the minimal product from becoming true until it happens. So, without loss of generality, we will consider in this section that we want to quantify a minimal product containing *l* failures on demand, *m* failures in function, and one deterministic failure.

We define the unavailability *Q* and unconditional failure intensity *W*, needed in equation (5), for this type of basic event. *Q* is a Heaviside function and *W* a Dirac distribution:

$$Q(t) = \bar{R}(t) = \mathrm{H}(t_0) = \begin{cases} 0, t < t_0 \\ 1, t \geq t_0 \end{cases}$$

$$W(t) = \delta(t - t_0).$$

With these notations, equation (5) can be written as follows (with an infinite time horizon, and omitting the minimal product index *c*):

$$E\left(N(\infty)\right) = \prod_{i=1}^{l} \gamma_i \times \int_0^\infty \exp\left(-\mu_{ie} x - \sum_{i=1}^{l} \mu_i x\right) \times \sum_{i=1}^{m+1} W_i(x) \prod_{\substack{j=1 \\ j \neq i}}^{m+1} Q_j(x)\, dx \quad (13)$$

Taking, as in § 2.3,

$$\mu = \mu_{ie} + \sum_{j=1}^{l} \mu_j \text{ and}$$

$$r_i = \lambda_i + \mu_i$$

$$E\left(N(\infty)\right) = \prod_{i=1}^{l} \gamma_i \times \int_0^\infty \exp(-\mu x) \sum_{i=1}^{m} W_i(x) \left(\prod_{\substack{j=1 \\ j \neq i}}^{m} Q_j(x) \times \mathrm{H}(t_0) \right) dx + \int_0^\infty \exp(-\mu x) \delta(x - t_0) \prod_{j=1}^{m} Q_j(x)\, dx$$

Finally,

$$E\left(N(\infty)\right) = \prod_{i=1}^{l} \gamma_i \times \int_{t_0}^\infty \exp(-\mu x) \sum_{i=1}^{m} W_i(x) \prod_{\substack{j=1 \\ j \neq i}}^{m} Q_j(x)\, dx + \exp(-\mu t_0) \prod_{j=1}^{m} Q_j(t_0) \quad (14)$$

The second term (the integral) of equation (13) can be written, using the same notations as in §2.3:

$$\sum_{i=1}^{m} \lambda_i \left(\prod_{\substack{j=1 \\ j \neq i}}^{m} \frac{\lambda_j}{r_j} \int_{t_0}^\infty e^{-\mu x} \prod_{\substack{j=1 \\ j \neq i}}^{m} (1 - e^{-r_j x})\, dx - \prod_{j=1}^{m} \frac{\lambda_j}{r_j} \int_{t_0}^\infty e^{-\mu x} \prod_{j=1}^{m} (1 - e^{-r_j x})\, dx \right). \quad (15)$$

After integration from t_0 to infinity, we obtain for the second integral the following alternate sum:

$$\int_{t_0}^\infty e^{-\mu x} \prod_{j=1}^{m} (1 - e^{-r_j x})\, dx = \frac{\exp(-\mu t_0)}{\mu} - \sum_{i=1}^{m} \frac{\exp(-(\mu + r_i) t_0)}{\mu + r_i} + \sum_{i=1}^{m} \sum_{j>i}^{m} \frac{\exp\left(-(\mu + r_i + r_j) t_0\right)}{\mu + r_i + r_j} - \sum_{i=1}^{m} \sum_{j>i}^{m} \sum_{k>j}^{m} \frac{\exp\left(-(\mu + r_i + r_j + r_k) t_0\right)}{\mu + r_i + r_j + r_k} + \cdots$$

$$\ldots + (-1)^m \left(\mu + \sum_{i=1}^{m} r_i\right)^{-1} \exp\left(-\left(\mu + \sum_{i=1}^{m} r_i\right) t_0\right).$$

Of course, taking $t_0 = 0$, we obtain again the formula (10) given in §2.3.

All these formulae are so complicated that it is necessary to carefully validate their implementation in a program. The next section has two purposes: give what we believe is the result of I&AB (we cannot guarantee that our Python implementation is totally bug free) and see how I&AB approximations compare to more precise calculations made by Monte Carlo simulation (the only possible method because of deterministic times) on a truly dynamic model.

4 ACCURACY TESTS OF I&AB EXTENSIONS

The small examples of this section were designed just to make comparisons between I&AB and "exact" calculations performed with Monte Carlo simulation. In practice the models were input graphically as BDMPs in KB3 (see Figure 1 for an example), then processed both by I&AB and by the Monte Carlo simulator YAMS. An overview of EDF tools including KB3 and YAMS is given in (Bouissou 2005).

In all calculations, failures are associated to a failure rate of 10^{-3}/h and repair rate of 2 10^{-2}/h. The grace times and delays of deterministic failures are indicated in § 4.1 and 4.2. Table 1 gives a synthesis of all comparisons. The numbers in the first column correspond to the numbers of sections below that explain the test cases. All calculations with I&AB require a negligible time, whereas some of the Monte Carlo simulations require a few minutes for sufficient precision.

Table 1. I&AB accuracy on various simple test cases. Columns 2 and 3 are the estimations of the unreliability at 10000 hours computed by I&AB and Monte Carlo simulation (the last column is the width half of the 90% confidence interval of the YAMS result).

Test case	I&AB	YAMS	conf. interval
4.1.1 a	5.25 10^{-3}	5.05 10^{-3}	5.21 10^{-5}
4.1.1 b	1.17 10^{-3}	1.12 10^{-3}	5.50 10^{-5}
4.1.1 c	5.85 10^{-5}	5.72 10^{-5}	3.93 10^{-6}
4.1.2 a	7.08 10^{-3}	2.60 10^{-3}	2.64 10^{-4}
4.1.2 b	1.73 10^{-2}	3.90 10^{-3}	3.24 10^{-4}
4.1.2 c	2.89 10^{-3}	6.95 10^{-4}	4.33 10^{-5}
4.1.2 d	9.55 10^{-3}	1.03 10^{-3}	5.27 10^{-5}
4.1.2 e	3.54 10^{-4}	3.80 10^{-5}	1.01 10^{-5}
4.1.2 f	3.89 10^{-3}	1.00 10^{-4}	1.64 10^{-5}
4.2.1 a	1.87 10^{-1}	1.67 10^{-1}	8.67 10^{-4}
4.2.1 b	6.21 10^{-3}	5.44 10^{-3}	1.71 10^{-4}
4.2.1 c	1.65 10^{-3}	1.67 10^{-3}	9.50 10^{-5}
4.2.2 a	1.87 10^{-1}	1.42 10^{-2}	2.75 10^{-4}
4.2.2 b	1.87 10^{-1}	1.56 10^{-2}	2.88 10^{-4}
4.2.2 c	6.21 10^{-3}	9.86 10^{-4}	7.30 10^{-5}
4.2.2 d	6.21 10^{-3}	1.14 10^{-3}	7.86 10^{-5}
4.2.2 e	1.65 10^{-3}	8.28 10^{-4}	4.73 10^{-5}
4.2.2 f	1.65 10^{-3}	8.62 10^{-4}	4.83 10^{-5}

Below are the descriptions of the test cases and comments on the results.

4.1 Grace times

4.1.1 Single grace time

The minimal product to quantify is {Initiator, A, B, grace_time}. In the dynamic model, there are only two sequences: Initiator, A, B, grace_time and Initiator, B, A, grace_time (A and B are in active redundancy). The grace time is successively taken equal to 25h (line 4.1.1.a of Table 1), 50h (line b), 100h (line c).

In this case, I&AB works quite well, and it is not surprising, given the fact that the dynamic model corresponds exactly to the simplifying assumptions made in § 2.1.

4.1.2 Two grace times

The minimal product to quantify is {Initiator, A, grace_time_1, B, grace_time_2}. In the dynamic model, there is only one sequence: Initiator, A, grace_time_1, B, grace_time_2. The grace time is fractioned, and the component B can fail only after the failure of A and the end of grace_time_1. The two grace times (in hours) are successively taken equal to (5, 20) (line 4.1.2a of Table 1), (20, 5) (line b), (15, 35) (line c), (35, 15) (line d), (30, 70) (line e), (70, 30) (line f). Note that in the dynamic model, the basic event grace_time_1 is considered as repairable (with repair rate equal to 1/250h), so that after an initiating event, the system can return to its initial state provided it does not reach the undesirable event; the value chosen for the repair rate is not sensitive as long as the mean time to repair components is much smaller than the mean time to repair the grace time: in such a case, after a given occurrence of the initiator, the grace time can be considered as "not repairable" just like in I&AB. In the simulation model, the order of the two grace times makes a difference if they are not equal. In I&AB, it is also the case because only the last grace delay is taken into account. We have also tested the idea of taking the sum of the two grace delays like a single one in I&AB: it yields results much closer to those of the dynamic model, but this approximation can produce optimistic results in some cases (for case f the result is 5.85 10^{-5}). Intuitively, this is due to the fact that in the dynamic model only the last grace delay is competing with *all* repairs of the markovian elements of the cut set. Cf. also § 5.

4.2 Deterministic failures

4.2.1 Barriers in active redundancy

Let us consider a little hydraulic system modeled by the BDMP below:

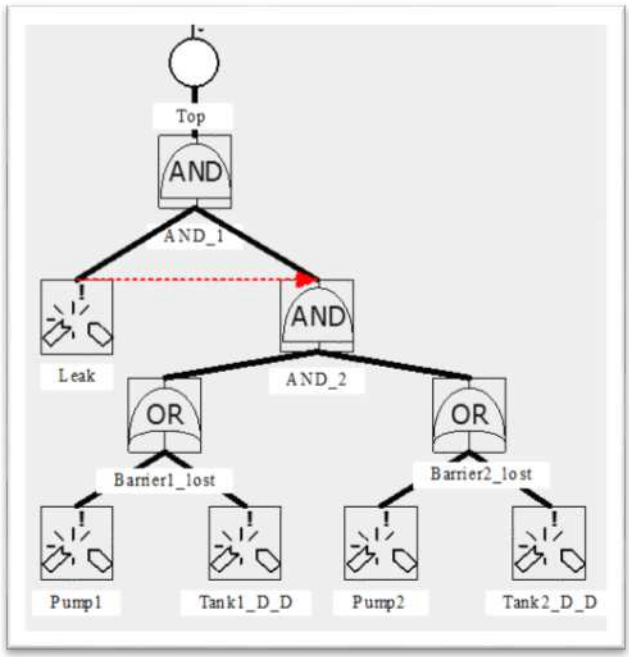

Figure 1. BDMP modeling a system with bounded capacities

When the initiator Leak occurs, the two barriers (each one composed of a pump and a tank) are activated. The undesirable event occurs if, before the repair of the leak, the two pumping systems are lost, either because of a random failure of the pump, or because the tank is empty. The failure and repair rates for random

events are as described at the beginning of §4, except that the repair rate of the Leak is 0.1/h in order to get small enough probabilities.

The results given in Table 1 correspond to the following values for the times after which Tank1 and Tank2 are empty: (40, 30) (line 4.2.1a), (80, 60) (line b), (150, 100) (line c). Note that the order of the two numbers is not important here, because of the symmetry of the two barriers. I&AB performs quite well on this example, where the minimal product containing the two deterministic failures is dominant. In the dynamic model as well as in I&AB, the amount of water in the biggest tank is the most influent parameter.

4.2.2 Barrier 2 activated on failure of barrier 1

In this case, in the dynamic model, the functioning times of the two tanks add up, unless a failure of pump1 forces to start barrier2 before depletion of tank1. It is therefore not surprising that I&AB is more conservative in this case than when the two barriers are in active redundancy. The BDMP corresponding to this case is not shown, because it is the BDMP of Figure 1 with just *one* additional trigger (red dotted line), going from gate Barrier1_lost to gate Barrier2_lost. There is no need to re-run the calculations with I&AB, since for this method, this case gives the same results as the previous one (active redundancy of barriers). But here, the capacities of the two tanks are not exchangeable in the dynamic model, this is why we ran YAMS with the following couples of values for deterministic delays: (40, 30) (line 4.2.2a), (30, 40) (line b), (80, 60) (line c), (60, 80) (line d), (150, 100) (line e), (100, 150) (line f). The unreliability increases a bit when the greatest delay is the last one. Going from line a to f, the results of I&AB range from extremely conservative (by a factor 10) to acceptably conservative (by a factor 2). On the other hand, using the sum of the delays instead of the greatest cannot be recommended because it could lead to optimistic results.

5 DIFFERENCES BETWEEN GRACE TIMES AND DETERMINISTIC DELAYS

In a dynamic model like a BDMP, both grace times and deterministic delays are represented as leaves associated to a deterministic time to failure. So the difference between those two concepts is not obvious. In essence, the difference between a grace delay and a deterministic failure is that:

- Once the grace delay has started, whatever happens on the system can only postpone (case of a repair) the undesirable event, or leave it unchanged (case of a failure);
- In the case of a deterministic failure, whatever happens on the system can only make the undesirable event happen sooner (case of a failure), or leave it unchanged (case of a repair).

The I&AB theory makes a very clear distinction between the two concepts, because it considers that the grace time starts when all other components of the cut set have failed, whereas the timer of a deterministic failure starts just after the initiator. An intermediate grace time such as in the example of § 4.1.2 corresponds to none of these cases, this is why in I&AB it should be simply ignored. It is the user's responsibility to mark leaves as grace delays, deterministic failures or "to be ignored" in the BDMP before transforming it into input data for I&AB.

On a large model, it is probable that the few minimal products with a too conservative quantification will be "hidden in the crowd" and that the global result will not be much affected.

6 APPLICATION TO THE SPENT FUEL POOL

To perform all our tests so far, we have used the implementation of I&AB that we described in (Bouissou & Hernu 2016). It is not the most efficient because it separates the search for minimal products from their quantification, therefore preventing the use of a probability threshold to discard at an early stage in the calculations most minimal products, as it is done by the MOCUS algorithm (Fussell & Vesely 1972). In spite of this limitation, we have been able to demonstrate impressive performances of I&AB in the spent fuel pool application.

We have built a model relative to the spent fuel pool of the European Pressurized Reactor and its support systems. Although less detailed than a classical PSA model, the BDMP we have built takes into account all dependances due to standby redundancies, common cause failures, sharing of electrical supplies… The model takes into account both the grace time of 14 hours before boiling of the water and deterministic failures of tanks used to replace evaporated water.

This BDMP (326 leaves, 77191 minimal products of order up to 6) could be processed by I&AB in a few minutes on a laptop. This model happened to be also quantifiable by YAMS: the Monte Carlo simulation gave a failure probability smaller than the result of I&AB by a factor around 2, but the calculation took 25 minutes to reach a 10% precision with 95% of confidence on the same machine.

Besides, with Monte Carlo simulation, it is very hard to get qualitative results: for that particular model, there is only one dominant sequence and all other sequences are much less probable: it would require many hours of simulation to get results comparable to the, say, 10 most probable minimal products that are easily identified by the I&AB method.

8 CONCLUSION

I&AB is an analytical method for the reliability calculation of large repairable systems with dependences between components. Two kinds of models can serve as input for this method: BDMPs or standard nuclear PSA models complying with the fault tree linking method. Both of them can be transformed into a set of minimal products that are the basis of the calculation. I&AB as it was described in (Bouissou & Hernu 2016) cannot readily be used for the fuel pool case, because for this system, there are two kinds of deterministic delays that must be taken into account: grace times, and deterministic failures due to the limited capacity of water tanks.

In the present paper, we have given two theoretical contributions: the analytical formulae of the I&AB method (so far, they were only available in the French patent file FR3044787) and their extension in the case of deterministic delays. In addition, we have shown on several examples that the extended method can yield reasonably conservative results, in times incomparably shorter than Monte Carlo simulation.

Thanks to a partnership between EDF and Lloyd's Register, I&AB will soon be available for the large community of users of the RiskSpectrum PSA tool. This could revolutionize PSA praxis in upcoming years.

9 ACKNOWLEDGEMENT

This paper is based on work done in collaboration with Olga Hernu, the co-author of the I&AB method and patent file (Bouissou & Hernu 2016).

REFERENCES

Bouissou, M. & Bon, J.-L. 1992. Fiabilité des grands systèmes séquentiels: résultats théoriques et applications dans le cadre du logiciel GSI. *Rev. Stat. Appl.* 40 (2).

Bouissou, M. & Bon, J.-L. 2003. A new formalism that combines advantages of fault-trees and Markov models: Boolean logic driven Markov processes. *Reliab. Eng. Syst. Saf.* 82: 149-163.

Bouissou M. & Hernu, O. 2016. Boolean approximation for calculating the reliability of a very large repairable system with dependencies among components. *Proc. ESREL 2016, Glasgow, 2016.*

Bouissou, M. 2005. Automated dependability analysis of complex systems with the KB3 workbench: the experience of EDF R&D. *Proc. CIEM 2005, Bucharest, 2005.*

Bouissou, M. 2006. Détermination efficace de scenarii minimaux de défaillance pour des systèmes séquentiels. *Proc. 15ème Colloque de fiabilité et maintenabilité, Lille, 2006.*

Fussell, J.B. & Vesely, W.E. 1972. A new methodology for obtaining cut sets for fault trees. *Trans. Amer. Nucl. Soc.* 15: 262-263.

Krcál, J. & Krcál, P. 2015. Scalable analysis of fault trees with dynamic features. *Proc. DSN 2015, Rio de Janeiro, 2015.*