Leaving mission times backstage and taking repair into account in long term scenarios

Anders Olsson[a]
[a] Lloyd's Register, Malmoe, Sweden

Abstract: In a standard PSA for an at-power nuclear reactor it is common practice to use mission time of 24 and 48 hours for PSA level 1 and 2 respectively without taking repair of failed components into account. In a shutdown/refueling PSA or a spent fuel pool PSA the time until fuel damage occurs is normally much longer compared to the at-power reactor PSA due to lower decay heat. The challenge with this is how to define the safe end state that in turn defines the mission time(s) to use. At the same time it enables for taking credit of repair of failed components as the available time to succeed with this has increased significantly.

In this paper the dynamic methodology Initiators and All Barriers (I&AB) is tested on a full scope PSA spent fuel facility. The main purpose with the paper is to investigate how a dynamic approach can be applied with emphasis on what is required in terms of realistic repair times and definition of safe end states. In order to demonstrate the usefulness of the dynamic versus the static (traditional PSA technique) a specific scenario is chosen and analyzed using both techniques. The results presented are from a pilot study on a full scale model the and is therefore to be seen as indicative only.

Keywords: Repair times, Dynamic methods, Long term scenarios, Repair, I&AB.

1. INTRODUCTION

It is common practice in PSA to define the time it takes to reach a safe end state after an initiating event as the sequence mission time. Furthermore the mission time is often defined as a "global" parameter in a PSA for a nuclear power plant. A question that you as a PSA analyst should ask yourself is of course what the **basis for the chosen mission time** is, e.g. has it been verified through MAAP or MELCOR analysis or is it based upon a deterministic criteria.

Another common approach in a "standard PSA" is that **no credit is taken for repair** of component failures unless you can demonstrate that you have much time available in order for the repair to be successful. In an at-power PSA it is not unusual that core damage can occur within a very short time (few hours) from the initiating event but it can also be that it takes much longer time (>10 hours) depending on what is causing the core damage and in such long term scenarios a "no credit for repair" assumption is of course more conservative. Again, as a PSA analyst you should be aware of this often "global" assumption, the basis for it in terms of **mission time versus required repair times** and the importance of the assumption in terms of impact on core damage frequency.

Initiators and All Barriers (I&AB) is a dynamic methodology developed by EDF (Industrial Risks Management Department, France), and which is presented in [1] and which is implemented in RiskSpectrum® PSA. It enables taking repair into account in a practical way in a full scope PSA application at the same time as you can actually define sequence specific time intervals referring to the available time to repair failed components until the undesirable end state occurs, hereinafter referred to as "grace time" or "grace delay". Implementation of I&AB in RiskSpectrum® PSA is further described in [2].

The objective with this paper is to apply the dynamic approach on a full scale PSA and thereyby investigate the importance of:

1. The basis for definition of safe and stable end states.
2. The importance of realistic repair times and how those correlates to probabilities of failed repair which may be defined in a PSA.

In section 1.1 below a theoretical example is given on how long term scenarios may be modelled using traditional PSA technique.

1.1 PSA modelling of long term scenarios

When long term scenarios are modelled in a traditional PSA one should take relaxed system requirements due to reduced decay heat into account and the likelihood that components may be repaired. In order to reflect that system requirements may be different depending on how long ago the initiating event occurred it may be necessary to divide the scenario into different time intervals with different systems requirement as illustrated in Figure 1 with different mission time basic events.

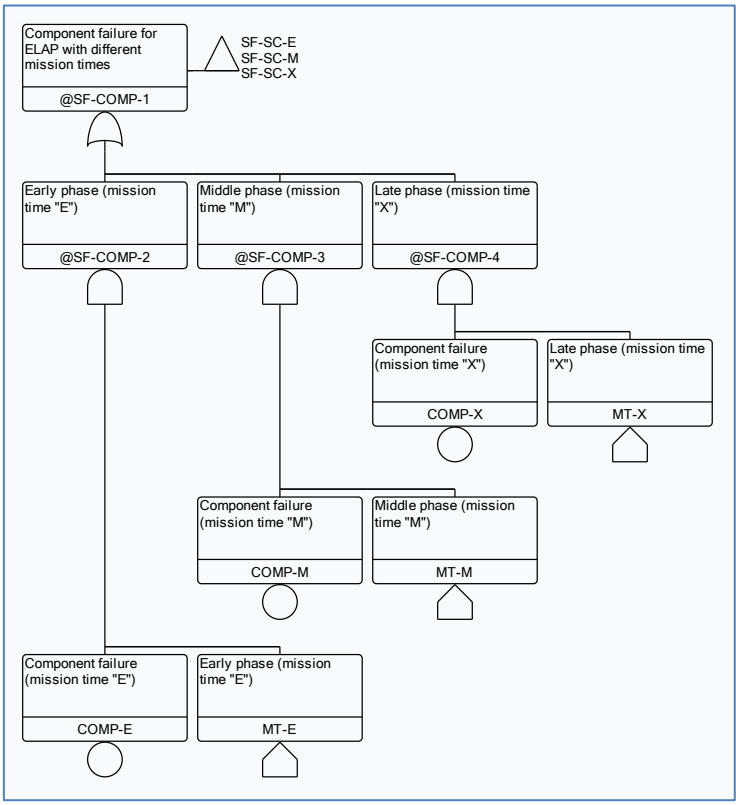

Figure 1: Division of long term scenarios into time intervals with different system requirements here illustrated by different mission time basic events.

In long term scenarios when repair is taken into account it is also quite likely that some components may be considered as non-repairable while other may be considered as repairable. This may depend on their respective importance to the results (less important components may be treated conservatively as non-repairable) and their estimated repair times (if no spare parts are available for a certain component it may be treated as non-repairable due to long repair time). As a PSA analyst you often want to focus on what is important to the result and it may not be in your interest to take repair into account for all component failures in the PSA. In Figure 2 it is illustrated how repair may be modelled in the fault tree structure for selected component failure modes.

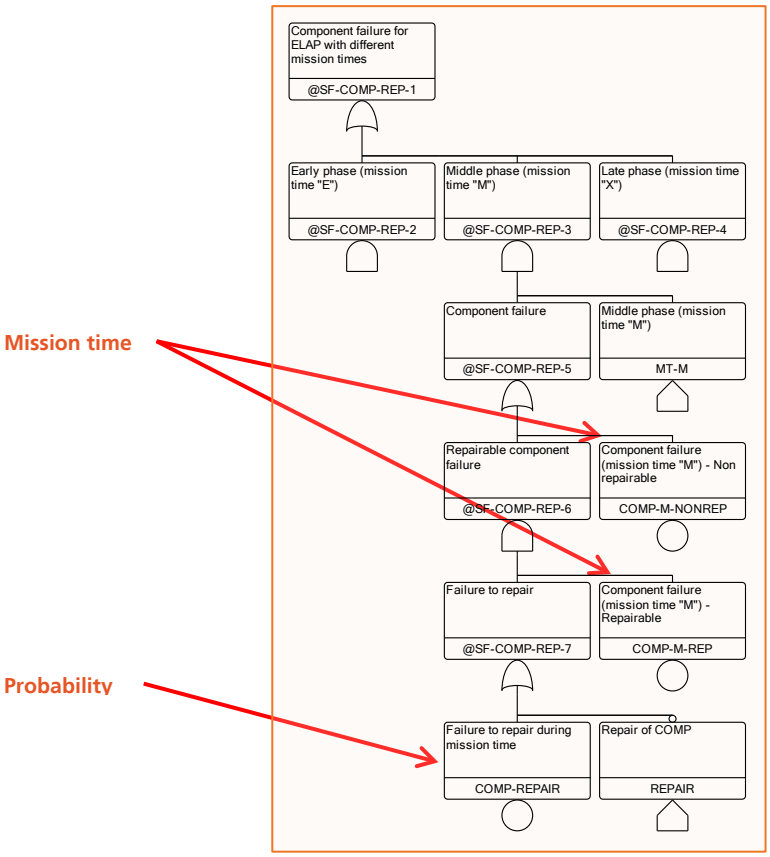

Figure 2: Example of how repair may be considered for selected component failures.

2. PSA FOR SPENT FUEL FACILITY

As we do not want to disclose exactly what facility the trial application of I&AB has been applied to, no exact details will be given about the facility or the PSA results. Some basic facts are however presented in Table 1 below with the purpose to allow the reader to have a basic understanding of the PSA in question.

Table 1: Summary of PSA for spent fuel facility

Topic	Note
No. of Basic Events	>1200
No. of Event Trees	>30
No. of Fault Trees	>350
Scope	Internal events, Level 1 and 2
Consequences	Boiling, Fuel element uncovery, Mechanical damage of fuel damage
Mission time	30 days (based upon deterministic system requirements)
No. of MCS	~27,000 in consequence analysis case for fuel pool boiling
Consideration of repair	Yes, for important components and initiating events in long term scenarios

As can be seen from Table 1 the PSA model in question is a semi-large model, at least when comparing against a full scope model for a nuclear power plant. Depending on the potential off-site consequences (small, medium and large release) the numerical safety goals are defined. The “boiling” consequence is however more of a deterministic design criteria and one of the objectives with the PSA is to demonstrate that the frequency of reaching a boiling scenario in the spent fuel pools is within the defined numerical criteria (the criteria is not presented in this paper).

As the spent fuel pools are large and the decay heat of the fuel stored in them is low the time until boiling occurs after failed pool cooling is long (~1 week) and once boiling has started it will take approximately another 3 weeks before the fuel elements are uncovered. The design criteria for the fuel

pool cooling system is that it shall be possible to keep the fuel pools cooled during a period of 30 days after an initiating event which gives a mission time of 720 hours. The challenge with such a long mission time is illustrated in Figure 3 below and it can also be concluded that in this particular case all mission time basic events have a fractional contribution of ~50%, i.e. increased mission time will definitely increase the result.

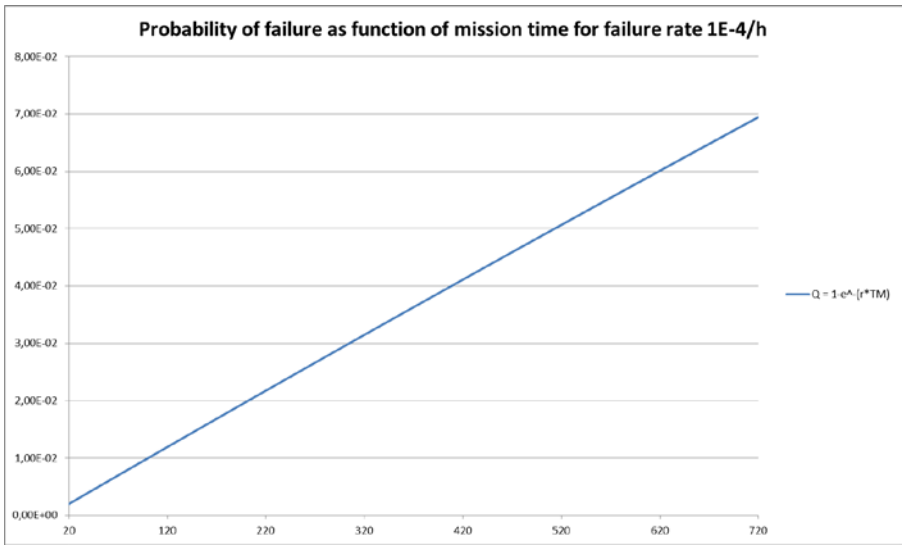

Figure 3: Probability of failure for a mission time basic event with failure rate equal to 1.0E-04/h as a function of mission time

In order to compensate for the long mission time, repair has been taken into account for a selection of component failures, i.e. those that can be found in the top cutsets. For the components where repair is considered, a probability of unsuccessful repair has been estimated based upon a study where it has been assessed if repair can be conducted within 7 days or not, i.e. the time until boiling starts. With this study as input probabilities of failed repair have been estimated to vary between 0.01 to 0.5 per demand. Repair is then modelled as illustrated in Figure 2 above.

2. APPLICATION OF DYNAMIC METHOD ON THE BOILING SCENARIO

When the I&AB methodology is applied on a PSA one needs to define what repair rates (1/[repair time]) shall be applied and what grace time to use. The grace time is defined as the time available in order for repair to be conducted between the initiating event and the undesirable consequence taking place. The options available given the input provided in the PSA are summarized in Table 2 below

Table 2: Options with respect to repair and grace times

Topic	#	Options
Repair time:	1	7 days for components where repair has been considered in the PSA, other components considered to be non-repairable
	2	7 days for components where repair has been considered in the PSA, other components considered to repairable within 30 days
	3	Conversion of used repair probabilities to repair rates
Grace time	1	No grace time considered
	2	Grace time of 7 days (time until boiling)
	3	Grace time of 30 days (time until fuel element uncovery)

As the survey that was conducted regarding repair times took on a “deterministic approach” and only concluded if repair can be successful within 7 days or not, no detailed information about the actual repair times was available. In the PSA some additional aspects were taken into account when assigning probabilities of unsuccessful repair, e.g. “repair is easy and can be made swiftly” which

yielded a probability of unsuccessful repair equal to 0.01/demand. For some components historical data revealed that there had been cases when spare parts were not available and therefore it was judged that for a certain fraction of the failures it might not be possible to repair the components within the time frame of 7 days which yielded a probability of unsuccessful repair >0.01/demand. The highest probability of unsuccessful repair used in the PSA was 0.5/demand.

It was of course of interest to compare the results from the pilot study using the dynamic approach with those obtained using the static (PSA) approach when conditions were kept as similar as possible. This is however not trivial as a the dynamic approach require specific repair times to be assigned while in a traditional PSA you can use more "qualitative" information when deriving and assigning probabilities for unsuccessful repair.

When it comes to definition of grace time it is more straightforward but still not trivial. As the consequence studied in this case was "boiling", a grace time of 7 days could be seen as the most obvious choice. However, remember that the PSA also had the ambition to verify the deterministic design criteria that pool cooling shall be maintained during 30 days. This can be compared with the normal mission time of 24 hours in a Level 1 PSA for a nuclear power plant during at-power, i.e. core damage may occur in only a few hours but still the criteria used is that all systems must work for 24 hours.

2.1 Results obtained with the inputs provided

In Table 3 below some results achieved with different assumptions on repair times and grace time are presented. As the dynamic approach takes repair into account one would assume that the results in general would be lower than the ones achieved in the PSA base case, at least for case No. #3 and #4 in Table 3. As this is not the case it is obvious that the repair times assumed most likely are conservative compared to the repair probabilities used in the PSA base case (ranging from 0.01 to 0.5 per demand).

Table 3: Results obtained using conservative assumptions on repair times

Case #	Assumptions on repair and grace times	Relative results compared to base case
1	• Repair only considered for same components as in the base case, repair time of 7 and 30 days used. • Components where repair is not taken into account in the base case are considered to be non-repairable. • No grace time taken into account	13xlarger
2	• Same as for case #1 except that instead of assuming "non-repairable" all components are assumed to be able to repair within 30 days. • No grace time taken into account	11x larger
3	• Same as for case #2. • A grace time of 7 days taken into account.	1.9x larger
4	• Same as for case #2 and in addition a repair time of 7 days assigned to additional components that can be found in top cutsets. • A grace time of 7 days taken into account.	1.8x larger

2.2. Judgment of less conservative repair time

First of all it is worth pointing out that a repair time as defined in the I&AB methodology is a mean repair time following an exponential distribution. So, 63% of repairs can be completed after one repair time T, 86% of repairs completed after time 2T, etc. Setting a repair time of T = 8 hours in does therefore not mean that all repairs must be able to be completed within 8 hours. In reality, setting a repair time to a certain value (assume 8 hours) is the same as stating that a significant number of

repairs (37%) will take longer than 8 hours which is much more conservative than setting 8 hours as the absolute longest repair time that can occur, see also [2].

In order to be able to achieve more realistic results using I&AB a first assessment was made on less conservative repair times compared to those used in Table 3 above, i.e. either 7 days (168 hours) or 30 days (720 hours). Below is a summary of the judgments made in order to achieve this:

- 8 h repair time assumed for measurement devices, transmitters etc. where it is noted that spare parts exist "in-house". Same repair time is used for pumps in operation where it is noted that stand-by pump can be activated swiftly, in case stand-by pump also fails it is assumed to have a repair time of 168 h (7 days).
- 24 h repair time assumed for all heat exchanger failure modes, spare parts are available.
- 48 h repair time assumed for exchange of check valve, spare parts are available.
- 96 h repair time is assumed for certain failure modes for bus bars and for pumps when it is stated that repair can be accomplished in less than 7 days.
- 168 h (7 days) repair time assumed for components that were added in case #4 in Table 3 above.
- 336 h (15 days) repair time is assumed for more complicated failures in bus bars.

As can be noted the repair times listed above still have some degree of conservatism, especially if one should consider that the scenario considered is one where there is a degree of emergency. The results when applying the above listed repair times are presented in Table 4.

Table 4: Result obtained when using less conservative assumptions on repair times

Case #	Assumptions on repair and grace times	Relative results compared to base case
5a	• Components where repair is considered in base case are assigned according to bullet list above. • Components where repair is not taken into account in the base case are assumed to have a repair time of 30 days (720 h). • Grace time of 7 days taken into account	0.15x, i.e. lower
5b	• Same as case 5a, first and last bullet • Components where repair is not taken into account in the base case are assumed to have a repair time of 7 days (168 h).	0.056x, i.e. lower

As can be concluded from the results presented in Table 4 compared to the ones presented in Table 3 the reduction of conservatism in terms of repair times had a very significant impact on the results. The other conclusion that can be made is of course that if it can be verified that the repair times applied are not optimistic then the dynamic approach would yield significantly lower results.

The obvious question that can be asked now is if the repair probabilities used in the base case (ranging from 0.01 to 0.5 per demand) can be converted into representative repair times. If that would be possible one would achieve a better comparison of the base case PSA results and the results obtained with I&AB. One would also achieve an assessment of how realistic the repair probabilities are, i.e. is it reasonable to be able to repair the failed components within a certain time. This is further elaborated in the next section.

2.3. Conversion of repair probabilities to repair times

As is presented in Table 2 selection of the repair times for the fuel pool case can only be made using conservative assumptions (7 days, 30 days or unrepairable). In Section 2.2 the impact of assigning less conservative repair times is demonstrated and the question is raised if and how a conversion can be made between used repair probabilities in the base case PSA into repair times.

In Figure 4 the results of a time dependent calculation of a basic event with reliability model *Repairable* and the following reliability data is presented:

- Probability of failed repair at time zero: 1.0
- Failure rate of 1E-05/h (*should be equal to the failure rate of the studied failure mode*)
- Repair time of 168 h (7 days)

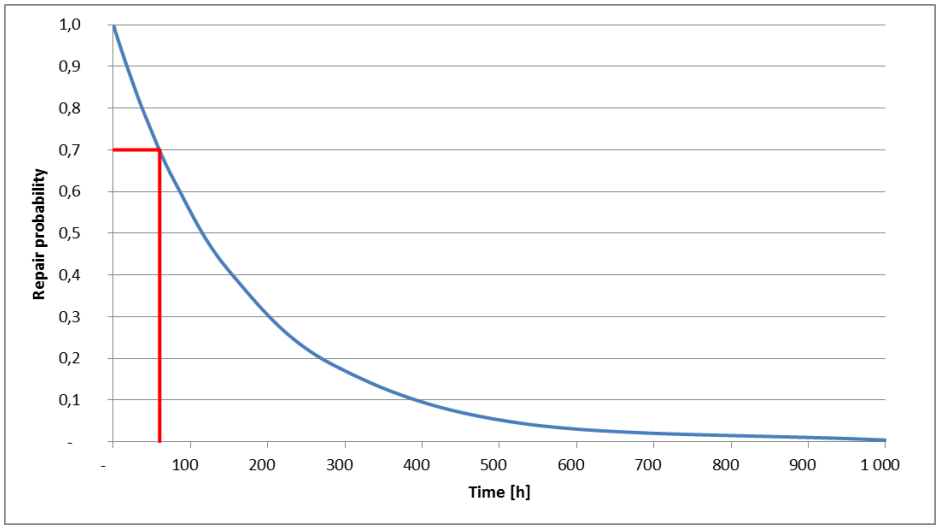

Figure 4: Conversion between likelihood of repair to repair time.

The conversion is then made in such a way where the probability of failed repair from the base case PSA first is converted to a probability of successful repair:

$$Q_{success} = 1 - Q_{failure} \quad (1)$$

This means that probability of failed repair of 0.3 would yield a probability of successful repair of 0.7 and this can be converted to a repair time of ~65 hours (red line in Figure 5). The conversion of repair probabilities into repair times is presented in Table 5 and Figure 5.

Table 5: Repair probabilities converted into repair times

Probability of failed repair	Probability of successful repair	Equivalent repair time
0.01	0.99	1 h
0.035	0.965	5 h
0.06	0.94	7 h
0.10	0.90	16 h
0.30	0.70	65 h
0.50	0.50	125 h

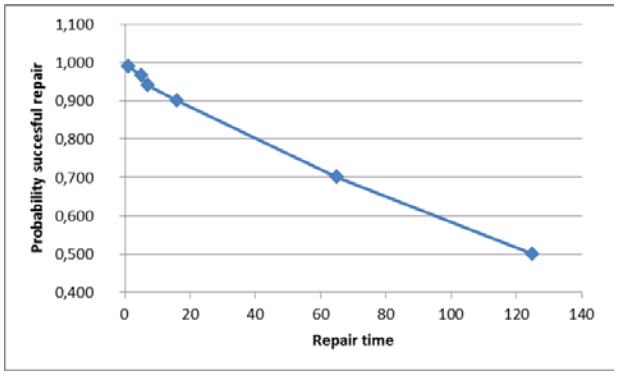

Figure 5: Repair probabilities converted into repair times.

As can be seen from Table 5 it can be questioned if a repair time of 1 hour is reasonable and what kind of alarms or indications would be necessary to introduce in order to achieve such a repair time. It may also be that some changes in procedures and in terms of spare parts need to be put in place in order to be able to assure that such repair time can be obtained as a maximum. On the other hand, it can be questioned in the same way if a probability of failed repair of 0.01 is reasonable. One benefit with a conversion like this is that it is much easier to discuss repair times with maintenance personnel than probabilities.

The results obtained when using the repair times given in Table 5 is presented in Table 6 for a grace time of 7 days (case #6a – 168 h) and 30 days (case #6b – 720 h).

Table 6: Result obtained when using repair probabilities converted into repair times

Case #	Assumptions on repair and grace times	Relative results compared to base case
6a	• Repair time according to Table 5 for components where repair is considered in base case. • Components where repair is not taken into account in the base case are assumed to have a repair time of 30 days (720 h). • Grace time of 7 days taken into account	0.013x, i.e. lower
6b	• Repair time according to Table 5 for components where repair is considered in base case. • Components where repair is not taken into account in the base case are assumed to have a repair time of 30 days (720 h). • Grace time of 30 days taken into account	0.0000013x, i.e. lower

The purpose with case #6b is to study the impact if the grace time is increased to the time it takes until the fuel elements start to be uncovered as an alternative safety goal compared to “fuel pool boiling” with the addition of “being able to keep fuel pool cooled during 30 days”.

The results from calculation cases presented in Tables 3, 4 and 6 have been summarized in Figure 6 below.

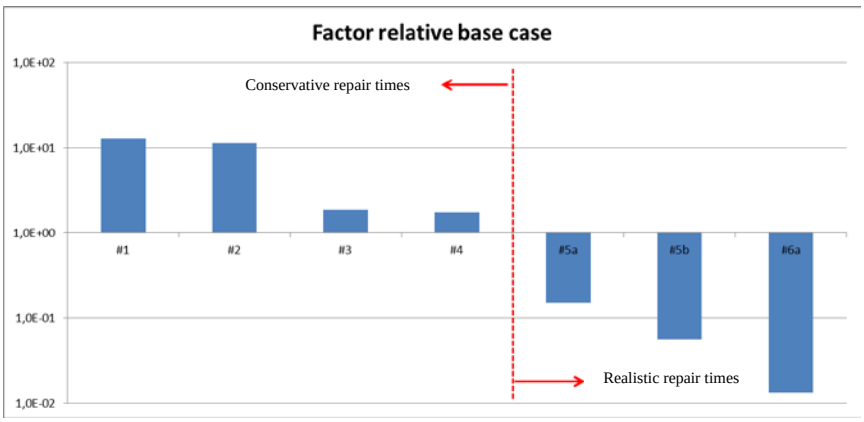

Figure 6: Summary of results when different repair times are used.

3. CONCLUSIONS

From the study presented in this paper there are several conclusions that can be made, the most important being:

1. Applying a dynamic approach such as the I&AB methodology, which takes repair and grace times into account can have a significant impact on the results in long term scenarios such as fuel pool cooling.

2. In order to get full benefit of the methodology it is important to be able to assign as realistic repair times as possible, at least to the most contributing components.

3. Using repair time instead of repair probabilities is easier to communicate with maintenance personnel and the possibility to convert between them can be useful also when performing a traditional PSA.

4. One of the challenges when defining mission times in a traditional PSA is to correlate them to physical properties which refer to safe and stable end states. When the mission time is defined from deterministic design criteria such as “a function must be maintained for a certain duration” it is difficult to understand what physical properties the PSA end states (consequences) are representing.

References

[1] M. Bouissou, O. Hernu, “*Boolean approximation for calculating the reliability of a very large repairable system with dependencies among components*”, ESREL 2016 proceedings (ISBN 978-1-138-02997-2)

[2] O. Bäckström, M. Bouissou, et.al. “*Introduction and Demonstration of the I&AB Quantification Method as Implemented in RiskSpectrum PSA*”, Paper #203 at PSAM14.