Probabilistic risk assessment considering parameter and model uncertainties

Florent Brissaud, Elsa Rosner

Probabilistic risk assessment considering parameter and model uncertainties

F. Brissaud
FMDS industrie (.fr) / RAMS industry (.eu), France

E. Rosner
DNV GL, Paris, France

ABSTRACT: Probabilistic risk assessment (PRA) has become a widely used and accepted tool for managing risk in several industry sectors. The present paper focuses on parameter and model uncertainties within PRA that combine event trees and fault trees. To this end, a PRA is applied to a case study from oil and gas activities. Parameter uncertainties concern frequencies of initiating events, failure rates of safety barriers, factors of common cause failures, test coverages, and conditional probabilities. To perform these uncertainty analyses, a classical approach based on probability density functions and Monte Carlo simulations is used. On the other hand, model uncertainties concern effectiveness and architecture of safety barriers. To perform these uncertainty analyses, an approach based on fictitious events is proposed, which aims at transferring model uncertainties to parameter uncertainties. Resulting frequencies of occurrence of each accidental scenario are then assessed considering both parameter and model uncertainties. The impact of these results on risk management, notably in terms of risk acceptability, are then discussed, considering the selection of testing policy (including proof and partial tests) as example.

1 PROBABILISTIC RISK ASSESSMENT

Probabilistic risk assessment (PRA) (or "probabilistic safety assessment" (PSA)) is an important part of risk analysis, and more specifically of quantitative risk analysis (QRA). It is performed after hazard identification and, then, it is an essential tool for risk management. Therefore, PRA has become a widely used and accepted tool for managing risk in several industry sectors such as nuclear power plants, aerospace and aeronautics, oil and gas activities, and chemical process industries.

PRA aims at characterising a risk following their components: identifying possible accidental scenarios (i.e. sequences of events that could lead to an accident or to any other undesired event); quantifying their frequencies (based on combinations of frequencies and probabilities); and evaluating their consequences (i.e. severity). To this end, the most common method combines event trees and fault trees (Rausand, 2011). The event trees develop the possible events following an initiating event, taking safety barriers (which perform safety functions) into account, while the fault trees express the failures of safety barriers as combinations of basic events, using logic gates.

Probabilities in PRA should be interpreted as subjective (Apostolakis, 1990). Therefore, even if a probability cannot be "true" (by nature), important criteria allow the PRA to be an efficient tool for risk management. These criteria include coherence, substantiality, and robustness (Brissaud *et al.*, 2010). Coherence and substantiality can be achieved by using approaches such as event trees and fault trees, and by taking most of relevant information into account. Moreover, robustness is verified if results are trustworthy in spite of uncertainties in input information.

2 PARAMETER AND MODEL UNCERTAINTIES

2.1 *Uncertainty analyses*

Uncertainty analyses aims at determining the uncertainty in analysis results that derives from uncertainty in analysis inputs (Helton *et al.*, 2006). When performing a PRA, uncertainties come from different sources (US NRC, 2002): the model uncertainty, which is linked to the goodness-of-fit of the model to represent the real world; the parameter uncertainty, which is related to the input values used in the given model; and the completeness uncertainty, which is due to significant phenomena or relationships which may not be considered in the model. By nature, completeness uncertainty is not really possible to quantify (Reinert *et al.*, 2006) and could be mainly reduced by using appropriate methodologies properly. The present paper therefore focuses on parameter and model uncertainties.

Uncertainty analyses regarding parameters are quite common, including the use of probability density functions and Monte Carlo simulations (Helton *et al.*, 2006). This approach is applied in the present paper, regarding input data of the case study.

On the other hand, uncertainty analyses regarding models are less common. Within a PRA, such uncertainties appear, notably: when the effectiveness of a safety barrier is not sure; or when the architecture of a safety barrier is undetermined. To deal with these two types of model uncertainties, approaches based on fictitious events, as described in the following subsections, are proposed.

2.2 *Uncertainty regarding the effectiveness of safety barriers*

To deal with uncertainties regarding the effectiveness of safety barriers, it is proposed to introduce dedicated events for fault trees. For each set of a safety barrier k (of which failure is modelled by event SB_k) and an initiating event j (of which occurrence is modelled by event IE_j), an "effectiveness" $e_{k,j}$ is assigned, with $0 \leq e_{k,j} \leq 1$. $e_{k,j}$ is defined by the probability that safety barrier k prevents the assumed hazardous event in case of occurrence of initiating event j. The resulting fault tree is depicted in Figure 1 (with one initiating event and one safety barrier but it can be easily extended to more events and barriers), using events $EFF_{k,i}$ to model the "effectiveness" (then connected with NOT-gates). (In Figure 1, failure of safety barrier k is modelled by a transfer-gate because it is not developed on the current page.) It is therefore set that an event $EFF_{k,i}$ occurs with a probability equal to $e_{k,j}$. Model uncertainties related to effectiveness of safety barriers are therefore transferred to parameter uncertainties, through the values of $e_{k,j}$.

2.3 *Uncertainty regarding the architecture of safety barriers*

To deal with uncertainties regarding the architectures of safety barriers, it is proposed to use the "continuous gates for fault tree" (Brissaud *et al.*, 2010). The so-called "C-gate" (Brissaud *et al.*, 2009) is depicted in Figure 2 (with two basic events but it can be easily extended to N basic events). For each basic event E_i, a weight p_i is assigned, with $0 \leq p_i \leq 1$. The top event of a C-gate with N basic events E_i then occurs if: any basic event E_i occurs and causes, with a probability equal to p_i, the top event to occur; or all the N basic events E_i occur. An equivalent fault tree for C-gate is then depicted in Figure 3, using fictitious events P_i to model the weighting of basic events, and repeated basic events E_i (coloured in grey). It is therefore set that a fictitious event P_i occurs with a probability equal to p_i.

When all the weights are equal to 0.0, a C-gate is equivalent to an AND-gate (i.e. parallel architecture) and when all the weights are equal to 1.0, a C-gate is equivalent to an OR-gate (i.e. series architecture). This approach then allows continuously graduation of system part architecture from parallel (for the most reliable case) to series (for the least reliable case), by acting on these probabilistic weights (Brissaud *et al.*, 2010). Model uncertainties related to architecture of safety barriers are therefore transferred to parameter uncertainties, through the values of p_i (i.e. the weights).

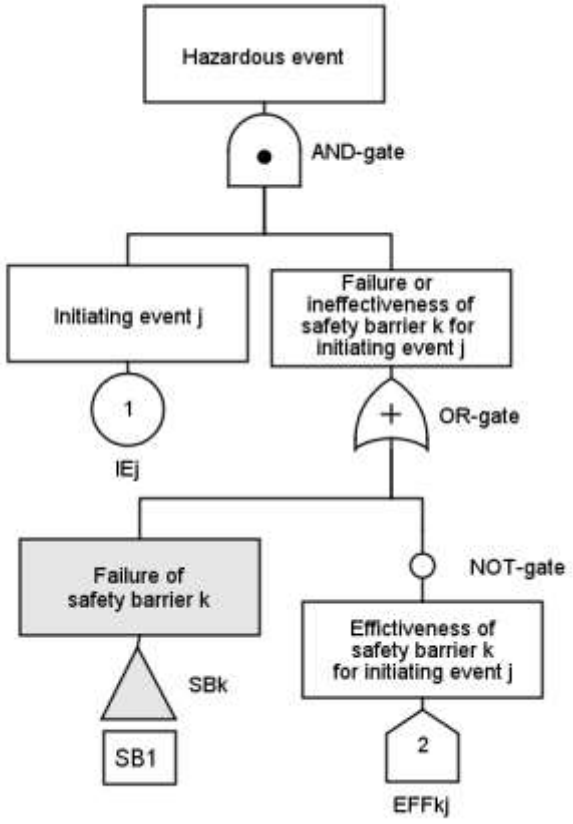

Figure 1. Fault tree with effectiveness of safety barriers (example with one barrier)

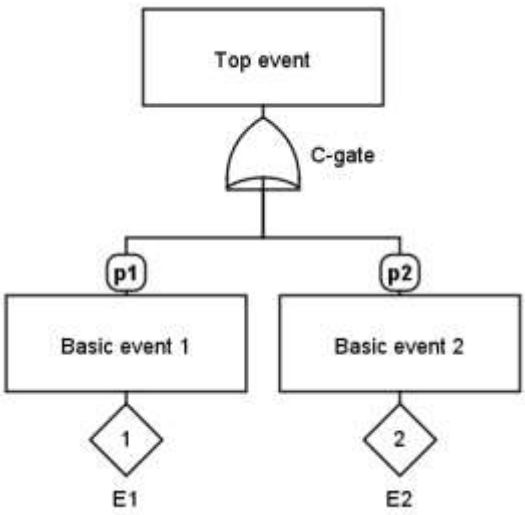

Figure 2. C-gate (example with two basic events)

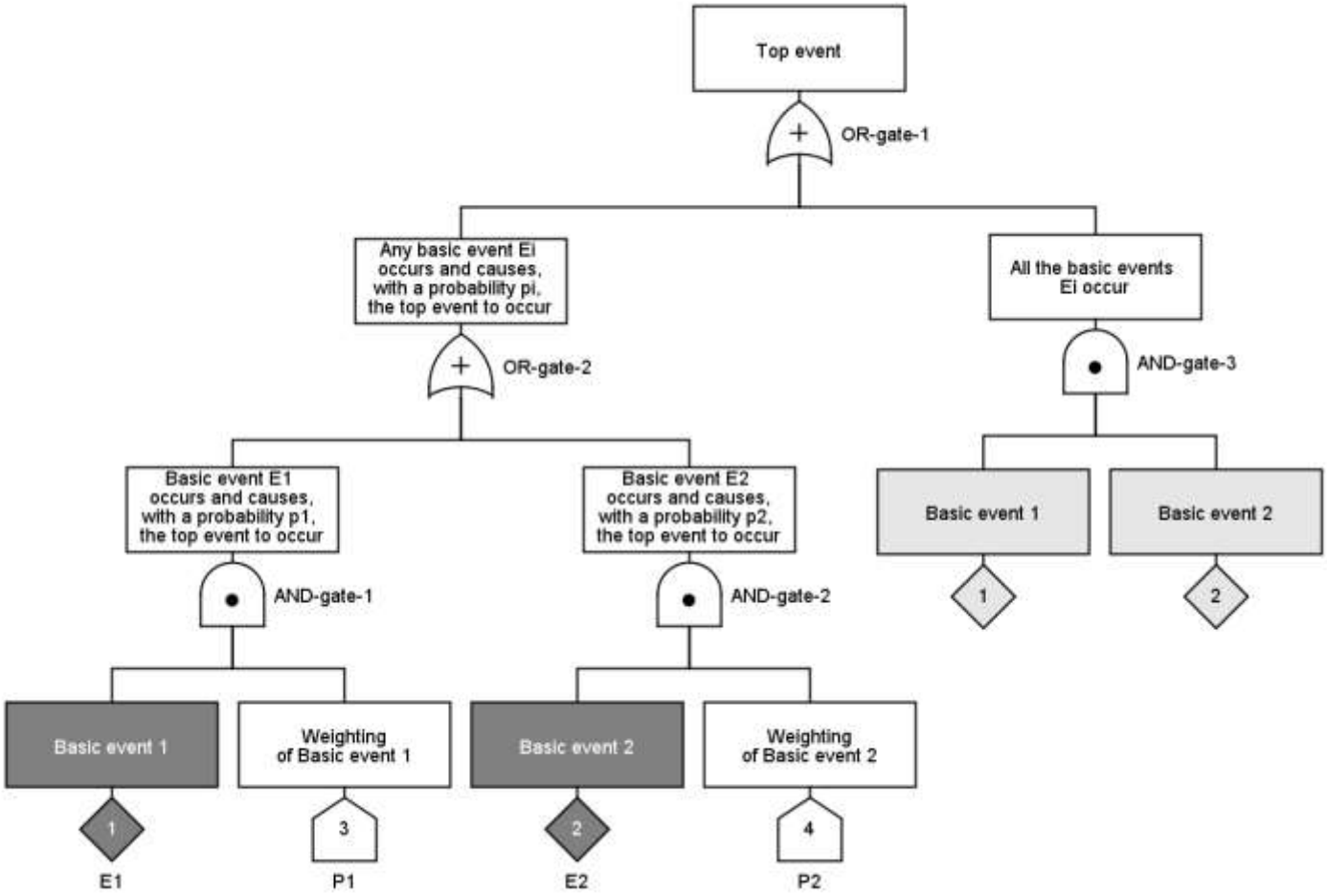

Figure 3. Equivalent fault tree for C-gate (example with two basic events)

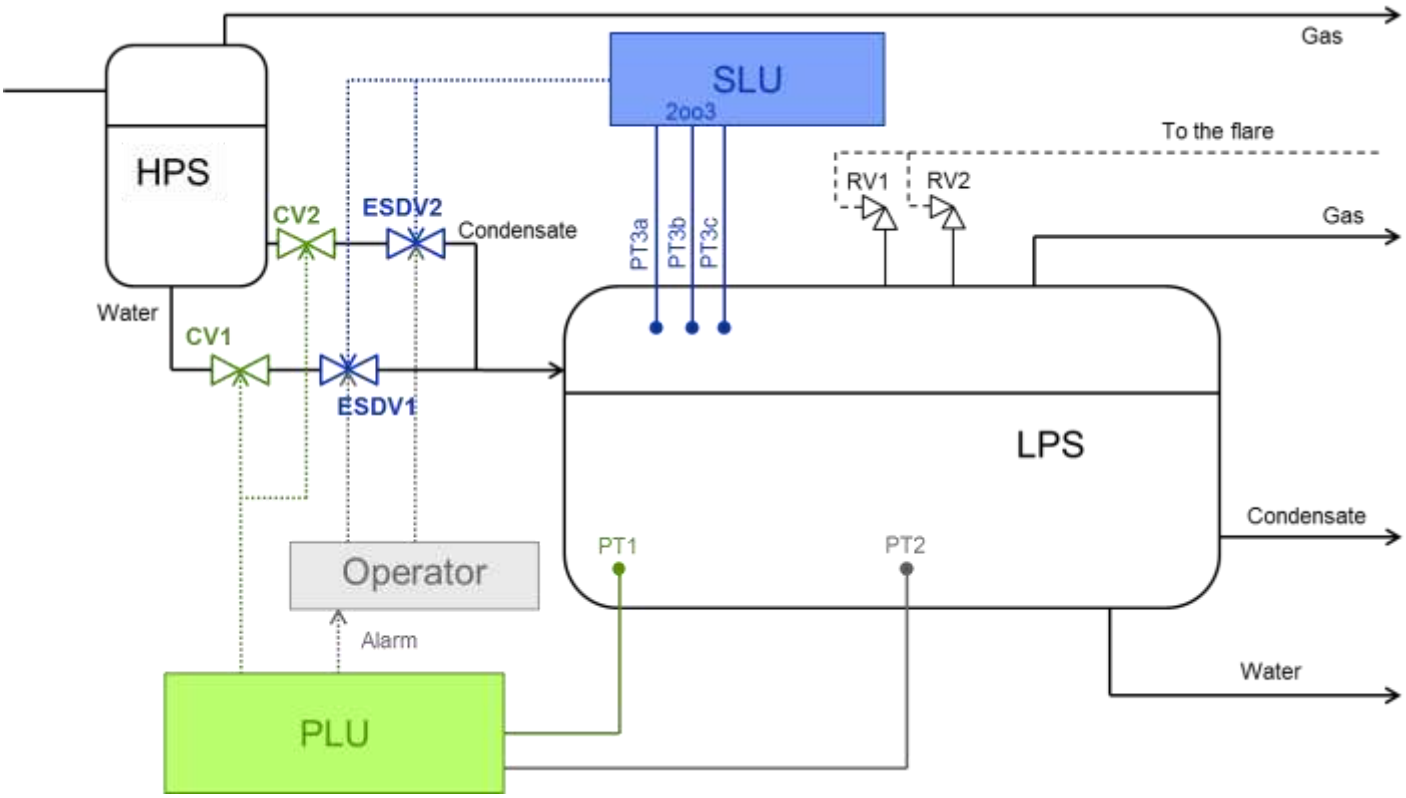

Figure 4. Equipment under control

3 CASE STUDY

3.1 *Equipment under control*

This case study originates from oil and gas activities. The equipment under control (EUC) is a low-pressure separator (gas, condensate, water) (LPS), downstream a high-pressure separator (HPS), as shown in Figure 4. Water and condensate are flowing from HPS to LPS by two separate lines. The flow is regulated by a pressure transmitter (PT1), a programmable logic unit (PLU), and one control valve for each line (CV1 for water and CV2 for condensate). The hazardous event to be prevented is a leakage from the LPS due to overpressure.

3.2 *Initiating events and preventive safety barriers*

To prevent the overpressure in LPS (i.e. the safety function), three safety barriers are implemented:

a. An alarm with operator action, based on a dedicated pressure transmitter (PT2) connected to the PLU, designed to alert an operator who should then close manually two emergency shutdown valves, one for each line (ESDV1 for water and ESDV2 for condensate);

b. A Safety Instrumented System (SIS), which consists of three dedicated pressure transmitters (PT3a, PT3b, and PT3c) that follows a 2-out-of-3 architecture (i.e. the functioning of two transmitters among three is sufficient to perform the safety function), a dedicated safety logic unit (SLU), and the two emergency shutdown valves (ESDV1 and ESDV2);

c. Two safety relief valves (RV1 and RV2).

ESDV1 and ESDV2 close the water and condensate lines, respectively. Depending on the (unknown) circumstances (according to the product flows), closing only one of these lines could be enough to prevent the hazardous event. Therefore, a C-gate is used to model the failure of the ESDVs to perform their safety function, as depicted in Figure 5. It is then assumed that the hazardous event is not prevented in the following cases: with a likelihood of 80%, if ESDV1 (on the water line) does not close; with a likelihood of 90%, if ESDV2 (on the condensate line) does not close; and with a likelihood of 100%, if both ESDV1 and ESDV2 do not close (according to the C-gate definition and parameters given in Figure 5).

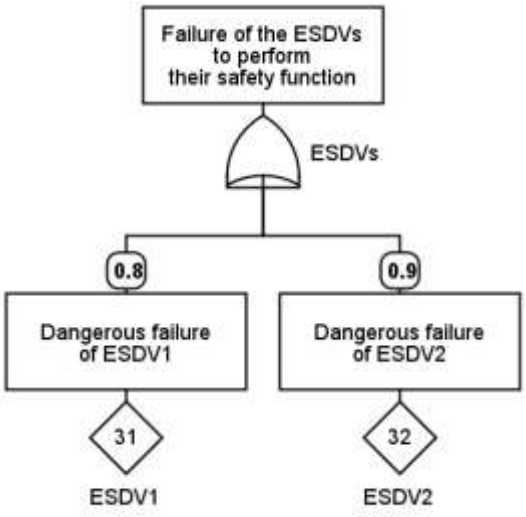

Figure 5. Modelling of ESDVs failure with a C-gate

The same approach is used to model the failure of the relief valves (RV1 and RV2) to perform their safety function, as depicted in Figure 6. In fact, depending on the circumstances (according to the degree of overpressure in LPS), opening only one of these relief valves could be enough to prevent the hazardous event.

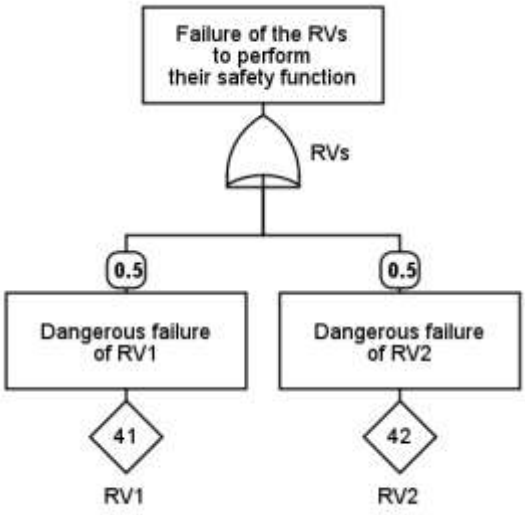

Figure 6. Modelling of RVs failure with a C-gate

Four initiating events (i.e. events that can lead to overpressure in LPS) are identified and reported in Table 1. This table also shows their frequency of occurrence, and the effectiveness of the safety barriers for each initiating event. For example, in case of gas blow by from HPS, there is a probability of 0.5 that the alarm with operator action is able to prevent the overpressure (notably because in 50% of these cases, the pressure is assumed to increase too fast for the operator to respond quickly enough). Note that the effectiveness does not consider failures of barriers. In fact, the probabilities of failures are modelled by fault trees in the following.

Table 1. Initiating events with frequencies of occurrence and effectiveness of safety barriers to prevent overpressure in LPS

		Effectiveness of safety barriers to prevent overpressure in LPS		
Initiating event	Frequency of occurrence	Alarm with operator action	Safety instrumented system	Relief valves
IE1: control loop failure	determined by fault trees	1	1	1
IE2: gas blow by from HPS	0.2 per year	0.5	1	1
IE3: human error	0.1 per year	0.5	1	1
IE4: external event (incl. fire)	0.005 per year	0.1	0.5	1

The frequency of occurrence of the control loop failure (as the first initiating event) is modelled by fault trees. The control loop includes CV1 and CV2 to regulate the water and condensate lines, respectively. Depending on the (unknown) circumstances (according to the product flows), the failure to regulate only one of these lines could be enough to initiate the hazardous event. Therefore, a C-gate is used to model the failure of the CVs to perform proper regulation, as depicted in Figure 7.

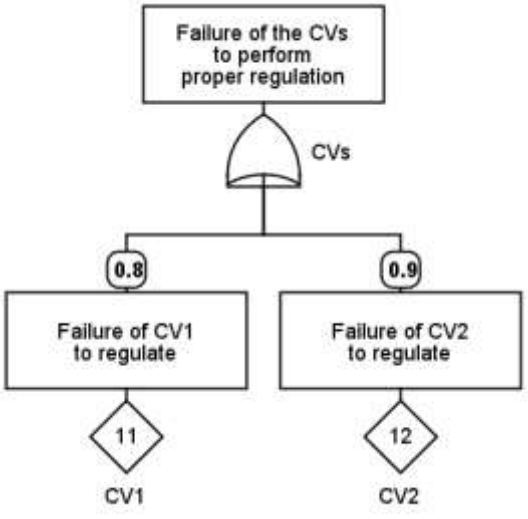

Figure 7. Modelling of CVs failure with a C-gate

For each material element, the failure mode and failure rates given in Table 2 are considered. It is assumed that any dangerous failure of a safety barrier element that is detected implies a shutdown of the EUC to perform the maintenance actions.

This is why only dangerous failure that are undetected online are considered (except for failures that are only part of initiating events), and no repair time. A proof test is performed periodically to detect and repair these failures. For emergency shutdown valves (ESDV1 and ESDV2), partial tests are also performed, with a partial test coverage given in Table 2. The selection of proof and partial test periods will be decided based on results. The pressure transmitters are subject to common cause failures (impacting all the transmitters), with a beta factor given in Table 2.

Table 2. Failure data for material elements

	Failure mode	Failure rate	Other parameter
Pressure transmitters (PTx)	Dangerous (incl. fail to regulate) undetected	5.00×10^{-6}	Beta factor: 5%
Programmable logic unit (PLU)	Dangerous (incl. fail to regulate) undetected	3.00×10^{-6}	-
Safety logic unit (SLU)	Dangerous undetected	1.00×10^{-6}	-
Control valves (CVx)	Fail to regulate detected online	8.00×10^{-6}	-
Emergency shutdown valves (ESDVx)	Dangerous undetected	1.00×10^{-5}	Partial test coverage: 90%
Safety relief valves (RVx)	Dangerous undetected	2.00×10^{-6}	-

In addition to the data given in Table 2, a probability of operator not responding as required to the alarm (i.e. not attend to close the emergency shutdown valves) is assumed equal to 0.1.

3.3 *Protective safety barriers*

In case of overpressure in LPS, the hazardous event occurs and leads to scenarios (i.e. sequences) identified in the event tree depicted in Figure 8. This event tree assumes the following protective safety barriers: ignition control (to prevent leakage ignition), explosion control (to prevent explosion in case of leakage explosion), proof walls (to prevent people to be possibly exposed to the explosion), and controlled presence (to prevent possibly exposed people to be hurt). The conditional probabilities of success (top branch) and failure (down branch) of these barriers are reported in Figure 8.

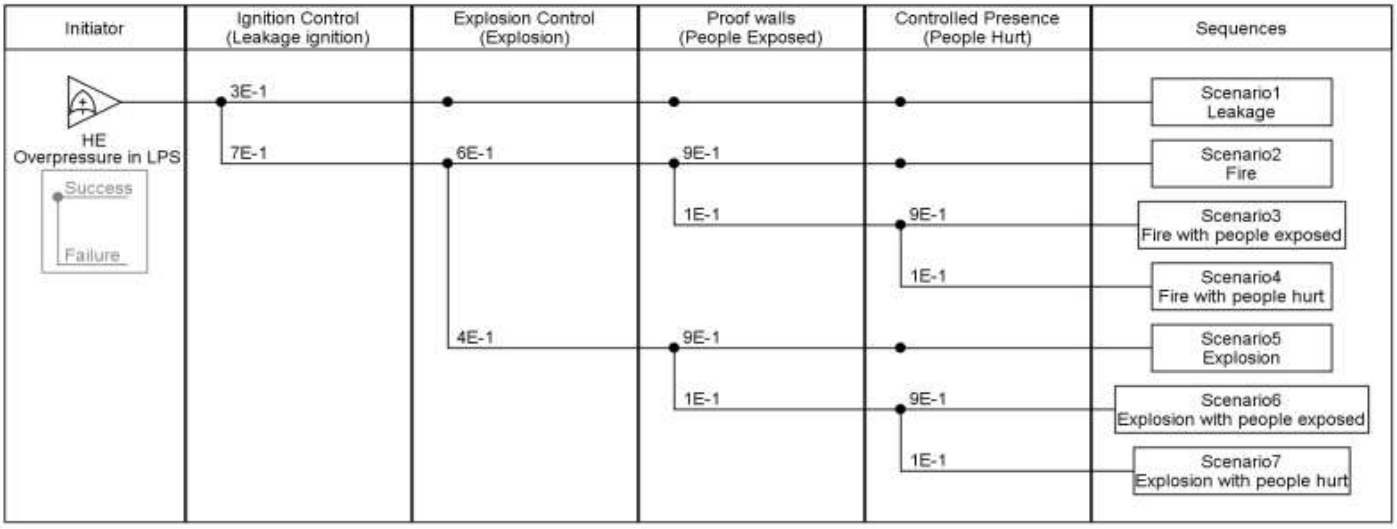

Figure 8. Event tree, following overpressure in LPS

4 ANALYSES

4.1 *Uncertainties in inputs*

The uncertainties in inputs are modelled using probability density functions, as defined in Table 3.

Table 3. Uncertainties in inputs

Data	Definition of uncertainties
Frequency f	Log-normal distribution such as the mean value is f and the 90% confidence interval is [f/5, f×5]
Failure rate λ	Log-normal distribution such as the mean value is λ and the 90% confidence interval is [λ/5, λ×5]
Beta factor β	Uniform distribution in the interval [0, β×2]
Partial test coverage PTC, with $0.1 \leq PTC \leq 0.9$	Uniform distribution in the interval [PTC-0.1, PTC+0.1]
Probability p (incl. effectiveness, weights, and conditional prob.), with p=0.5	Uniform distribution in the interval [p-0.3, p+0.3]
Probability p (incl. effectiveness, weights, and conditional prob.), with $0.1 \leq p \leq 0.9$ and $p \neq 0.5$	Uniform distribution in the interval [p-0.1, p+0.1]
Other	No uncertainty

4.2 *Modelling and analyses*

Modelling and analyses are performed using the Boolean package of the GRIF software tool, developed by Satodev for the account of TOTAL. Fictitious events are used, as depicted previously, to model the C-gates and the effectiveness of safety barriers. Given the inputs, fault tree analyses are "exact", based on Boolean algebra and Binary Decision Diagrams (BDD) algorithms. For the uncertainty analyses, Monte Carlo simulations are performed on the inputs (cf. Table 3) and then the results are obtained by fault tree analyses.

4.3 *Results*

Three testing policy are considered, depending on the period of proof tests (for all material elements), noted T1, and the period of partial tests (for ESDV1 and ESDV2), noted T2. The first testing policy is defined by T1=12 years and T2=3 years. The second testing policy is defined by T1=8 years and T2=1 year. And the third testing policy is defined by T1=4 years and T2=6 months.

The results depict the frequency of occurrence of each scenario (cf. Figure 8). Three criteria are defined. The first criterion is the average frequency computed on the proof test period. The second criterion is the maximum frequency within the proof test period (basically, this is the frequency reached just before the proof test, since the frequency increases until the test is performed). The third criterion considers the uncertainties, this is the 90% upper value of the average frequency (i.e. the average frequency is lower than this value with a certainty of 90%).

Tables 4-6 and Figures 9-11 report the results considering the first, second, and third testing policy. For each scenario, a maximum tolerable frequency is defined, based on the risk matrix depicted in Figures 9-11.

Table 4. Results: first testing policy
(T1=12 years and T2=3 years)

Scenario	Average frequency per year	Max. frequency per year	90% up. value of the av. fr. per year	Max. tolerable frequency per year
1	5,00E-03	1,12E-02	1,85E-02	1,00E-02
2	6,30E-03	1,42E-02	1,82E-02	1,00E-02
3	6,30E-04	1,42E-03	3,17E-03	1,00E-03
4	7,00E-05	1,57E-04	3,79E-04	1,00E-04
5	4,20E-03	9,43E-03	1,16E-02	1,00E-02
6	4,20E-04	9,43E-04	1,87E-03	1,00E-03
7	4,67E-05	1,05E-04	2,41E-04	1,00E-04

Table 5. Results: second testing policy
(T1=8 years and T2=1 year)

Scenario	Average frequency per year	Max. frequency per year	90% up. value of the av. fr. per year	Max. tolerable frequency per year
1	2,29E-03	6,21E-03	1,23E-02	1,00E-02
2	2,89E-03	7,82E-03	1,21E-02	1,00E-02
3	2,89E-04	7,82E-04	1,99E-03	1,00E-03
4	3,21E-05	8,69E-05	2,51E-04	1,00E-04
5	1,93E-03	5,21E-03	7,67E-03	1,00E-02
6	1,93E-04	5,21E-04	1,18E-03	1,00E-03
7	2,14E-05	5,79E-05	1,60E-04	1,00E-04

Table 6. Results: third testing policy
(T1=4 years and T2=6 months)

Scenario	Average frequency per year	Max. frequency per year	90% up. value of the av. fr. per year	Max. tolerable frequency per year
1	6,53E-04	1,94E-03	4,85E-03	1,00E-02
2	8,23E-04	2,45E-03	4,78E-03	1,00E-02
3	8,23E-05	2,45E-04	7,14E-04	1,00E-03
4	9,14E-06	2,72E-05	9,95E-05	1,00E-04
5	5,49E-04	1,63E-03	3,04E-03	1,00E-02
6	5,49E-05	1,63E-04	4,22E-04	1,00E-03
7	6,10E-06	1,81E-05	6,32E-05	1,00E-04

These results show that when considering the average frequency of occurrence of each scenario, the first testing policy is sufficient to decide that all scenarios are tolerable. However, when considering the maximum frequency, the first testing policy does not allow five scenarios over seven to be tolerable, but the second testing policy is sufficient. Finally, when considering uncertainties and the 90% upper value of the average frequency, only the third testing policy allows all the scenarios to be tolerable. In fact, using the second testing policy, there is a probability greater than 10% that the average frequencies of six scenarios over seven are greater than the maximum tolerable frequencies, even if the maximum frequencies (without consideration for uncertainties) meet these requirements. It is therefore concluded that making decisions in terms of risk management without consideration for uncertainties can lead to unsafe choices.

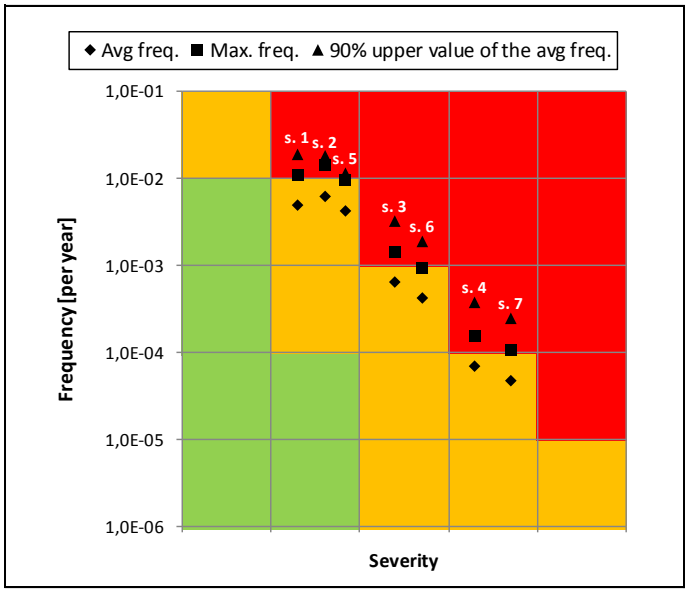

Figure 9. Risk matrix: first testing policy

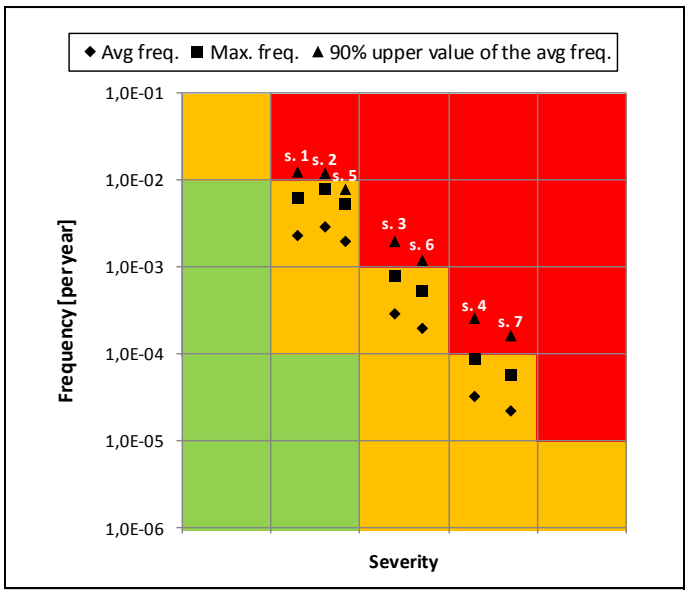

Figure 10. Risk matrix: second testing policy

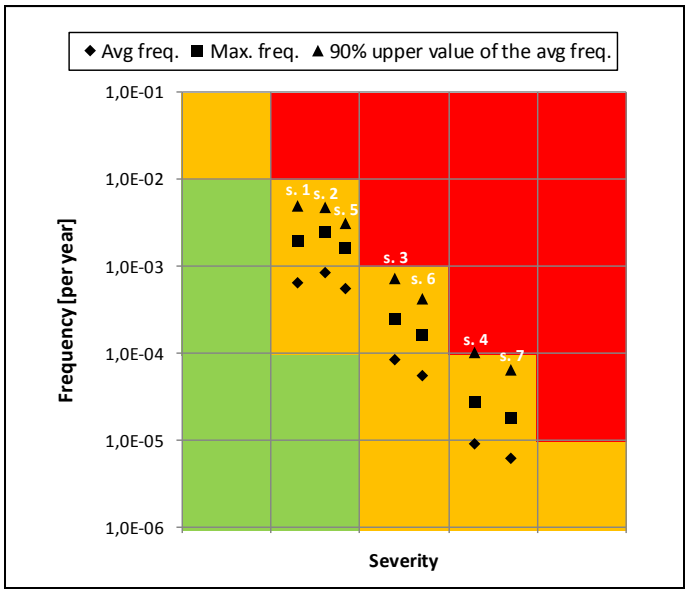

Figure 11. Risk matrix: third testing policy

5 REFERENCES

Apostolakis, G. 1990. The concept of probability in safety assessment of technological systems. *Science* 250: 1359-1364.

Brissaud, F., Barros, A., Bérenguer, C. & Charpentier, D. 2009. Design of complex safety-related systems in accordance with IEC 61508. *Proceedings of the 18th European Safety and Reliability Conference, Prague, Czech Republic 7-10 September 2009.*

Brissaud, F., Barros, A. & Bérenguer, C., 2010. Handling Parameter and Model Uncertainties by Continuous Gates in Fault Tree Analyses. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, special issue on Uncertainty in Engineering Risk and Reliability* 224(4): 253-265.

Helton, J.C., Johnson, J.D., Sallaberry, C.J. & Storlie, C.B. 2006. Survey of sampling-based methods for uncertainty and sensitivity analysis. *Reliability Engineering & System Safety* 91: 1175-1209.

Rausand, M. 2011. *Risk Assessment: Theory, Methods, and Applications*. Wiley.

Reinert, J.M. & Apostolakis, G.E. 2006. Including model uncertainty in risk-informed decision making. *Annals of Nuclear Energy* 33: 354-369.

US Nuclear Regulatory Commission. 2002. *An approach for using probabilities risk assessment in risk-informed decisions on plant-specific changes to the licensing basis (Regulatory guide 1.174)*, Revision 1. US Nuclear Regulatory Commission.