Design of complex safety-related systems in accordance with IEC 61508

Florent Brissaud, Dominique Charpentier, Anne Barros, Christophe Bérenguer

Design of complex safety-related systems in accordance with IEC 61508

F. Brissaud & D. Charpentier
Institut National de l'Environnement Industriel et des Risques (INERIS), Verneuil-en-Halatte, France

A. Barros & C. Bérenguer
Université de Technologie de Troyes (UTT) – Institut Charles Delaunay (ICD) – FRE CNRS 2848, Troyes, France

ABSTRACT: According to IEC 61508, a safety-related system is regarded as type B if it presents a high complexity (i.e. the failure mode of at least one component is not well defined, or the behaviour under fault conditions cannot be completely determined), or if there is insufficient data to support claims for failure rates. This paper proposes a modelling method adapted to the evaluation of failure probabilities for systems with uncertain behaviour under fault conditions. To this aim, weighted "continuous gates" are introduced in a fault tree framework. By acting on weight values, it is then allowed to continuously graduate system part architectures between series and parallel structures. An intelligent transmitter is used as example. Probabilities of failure on demand are assessed, with both failure rates and behaviour uncertainty analyses. Results tend to show that the lack of knowledge in system behaviour can be partially handled by this kind of approach.

1 INTRODUCTION & IEC 61508

Safety instrumented systems (SIS) play a major part in industrial risk management as risk reduction measures. The main European standard for functional safety of SIS, denoted electrical / electronic / programmable electronic (E/E/PE) safety-related systems, is the IEC 61508 (IEC, 2005a). The second edition will soon be adopted in 2009 (IEC, 2009). Objectives are to enable the design of SIS, and the development of application sector standards. Such examples are IEC 61511 (IEC, 2004) for process industry, and IEC 62061 (IEC 2005b) for machinery. One of the main contributions of IEC 61508 is to consider the overall system and software safety life cycle. The standard framework, with the corresponding normative parts and subclauses, is:

1 development of the overall safety requirements (SR): concept, scope definition, hazard and risk analysis, overall SR specification (Part 1: 7.2-7.5);
2 SR allocation to the designated SIS or other risk reduction measures (Part 1: 7.6);
3 SR specification for each SIS in order to achieve the required functional safety (Part 1: 7.10);
4 realisation phase for SIS design and development in accordance with SR specification, for system (Part 2) and software (Part 3);
5 installation, commissioning, safety validation, including planning (Part 1: 7.8-7.9 and 7.13-7.14);
6 operation, maintenance, modification, and decommissioning (Part 1: 7.7 and 7.15-7.18).

Other requirements, regarding all phases, are about documentation (Part 1: 5); management of functional safety (Part 1: 6); functional safety assessment (Part 1: 8); and verification (Part 1: 7.18). Part 4 gives definitions and abbreviations. The other parts are informative: guidelines to determine overall SR (Part 5), guidelines for realisation phase (Part 6), and an overview of techniques and measures (Part 7).

Safety requirements (SR) refer to safety function and safety integrity. A safety function has to be implemented by a SIS or other risk reduction measures to achieve or maintain a safe state of the equipment under control (EUC). The probability of a SIS satisfactorily performing the specified safety function is the safety integrity. Safety integrity values are arranged in four discrete levels, denoted safety integrity levels (SIL), according to target failure measures. For example, Table 1 applies to safety functions operating in low demand mode.

According to IEC, 2009, a safety-related system is regarded as low complexity if the failure modes of each individual component are well defined, and the behaviour of the system under fault conditions can be completely determined. This paper focuses on SIS to which this definition does not apply.

The realisation phase is investigated in Section 2. Some issues linked to the system complexity are discussed in Section 3, and a fault tree based approach is proposed. An intelligent transmitter is used as an example in Section 4, for both failure rates and behaviour uncertainty analyses. Finally, discussions are given in Section 5.

Table 1. SIL and corresponding target failure measures for a safety function operating in low demand mode

SIL	Average probability of dangerous failure of the safety function on demand (PFD_{avg})
SIL 4	$10^{-5} \leq PFD_{avg} < 10^{-4}$
SIL 3	$10^{-4} \leq PFD_{avg} < 10^{-3}$
SIL 2	$10^{-3} \leq PFD_{avg} < 10^{-2}$
SIL 1	$10^{-2} \leq PFD_{avg} < 10^{-1}$

2 DESIGN IN ACCORDANCE WITH IEC 61508

2.1 *Inputs and objectives of the realisation phase*

Before starting the SIS realisation phase, the overall safety requirements have been previously developed, as well as the SR allocation and specification. The following inputs are then available:

– the safety functions to carry out by the SIS;
– the mode of operation of each safety function;
– the target failure measures with associated SIL.

In the present paper, only the low demand mode of operation is assumed (i.e. the safety function is only performed on demand, and not more than one per year). The target failure measure is then defined by the average probability of dangerous failure on demand of the safety function (PFD_{avg}), and the associated SIL is determined by Table 1. Note that these definitions stem from IEC 61508, 2009 revision, which are more precise than in the first edition.

The objective of the realisation phase is then to create the SIS conforming to the specification, especially in terms of safety functions and allocating SIL. This paper focuses on system requirements (Part 2), and does not develop software aspects (Part 3). The realisation phase consists of design requirement specification (for subsystems and elements), design and development, integration (software integration refers to Part 3), operation and maintenance, validation, modification, and verification.

In the following sections, the SIS design and development is detailed, according to hardware, systematic, and other safety requirements.

2.2 *Hardware safety integrity requirements*

The requirements for hardware safety integrity contain architectural constraints and random hardware failure quantification. The former are based on:

– the hardware fault tolerance (HFT), equal to *N* if *N+1* is the minimum number of faults that could cause a loss of the safety function;
– the safe failure fraction (SFF), defined by the ratio of the average failure rates of safe or detected failures by diagnostic tests, to the total failures.

These two parameters are then used to determine the maximum allowable SIL for the safety function, according to system type A or B. For example, Table 2 applies to type B systems.

Table 2. Maximum allowable SIL for a safety function carried out by a type B safety-related system

Safe failure fraction (SFF)	Hardware fault tolerance (HFT)		
	0	1	2
SFF < 60%	-	SIL 1	SIL 2
60% ≤ SFF < 90%	SIL 1	SIL 2	SIL 3
90% ≤ SFF < 99%	SIL 2	SIL 3	SIL 4
99% ≤ SFF	SIL 3	SIL 4	SIL 4
Route 2_H*	SIL 1-2	SIL 3	SIL 4

*Alternative route proposed by IEC, 2009

Low complexity systems with available significant feedback data are regarded as type A. Conversely, type B systems are defined by at least one of these properties:

– the failure mode of at least one constituent component is not well defined;
– the behaviour of the system under fault conditions cannot be completely determined;
– there is insufficient dependable failure data to support claims for rates of failures for detected and undetected dangerous failures.

More insight into architectural constraints is provided by Lundteigen, 2009. SFF has been especially questioned by Innal, 2006 and Langeron, 2007. As a general conclusion, SFF is not an appropriate indicator for safety integrity. An alternative "route" is then proposed by the second edition of IEC 61508. It is based on reliability feedback data from end users, and does not consider SFF (see Table 2, "Route 2_H"). In that case, a special requirement for type B systems is a diagnostic coverage (i.e. proportion of average dangerous failure rates detected by diagnostic tests) equal to or greater than 60%.

Requirements for quantifying the effect of random hardware failures consist of a list a parameters to be taken into account: system architecture, dangerous failure rates which are detected or not by diagnostic tests, diagnostic test coverage and interval, common cause failures, proof tests interval and effectiveness, repair times (if EUC is not maintained in a safe state during repair), and random human error effects. Methods for the target failure measure evaluation are mentioned (e.g. fault trees, reliability block diagrams, Markov models, and Petri nets), and guidelines are given in Part 6, but for information only. Discussions about type B system issues for the evaluation of the average probability of dangerous failure on demand are proposed in Section 3.

2.3 *Systematic safety integrity requirements*

To prevent the introduction of faults during the design and development of the SIS hardware and software, requirements for the avoidance and control of systematic faults (i.e. related in a deterministic way to a certain cause) are introduced. Techniques and measures are given in Part 2: Annexes A and B.

The systematic safety requirements can also be fulfilled by demonstrating that the system is proven in use. Such criteria are discussed by Beurden, 2004.

2.4 *Other requirements*

Other requirements refer to system behaviour upon detection of a fault (basically, specified actions have to achieve or maintain a safe state of the EUC when a dangerous fault is detected); data communication processes (taking into account transmission errors, repetitions, delays etc.); and special architectures for integrated circuits with on-chip redundancy, if relevant (Part 2: Annex E).

3 MODEL FOR COMPLEX SYSTEMS

3.1 *Type B safety-related system issues*

The lack of data to support claims for failure rates is an issue which is widely investigated by data uncertainty analyses. For example, Hauptmanns, 2008 compares the use of reliability data stemming from different sources on probabilistic safety calculations, and tends to prove that results do not differ substantially. Wang, 2004 discusses and identifies the inputs that may lead to SIL estimation changes. Propagation of error, Monte Carlo, and Bayesian methods (Guérin, 2003) are quite common. Fuzzy set theory is also often used to handle data uncertainties, especially into fault tree analyses (Tanaka, 1983, Singer, 1990). Other approaches are based on evidence, possibility, and interval analyses (Helton, 2004).

The non-low complexity properties, used to describe type B systems (i.e. not well defined failure modes; undetermined system behaviour), are much less investigated in literature. However, research work is focusing on microprocessor or software based safety systems and aims to identify unknown hazards (Garrett, 2002), or evaluating parameters for SIL calculation (Camargo, 2001).

Models used to quantify probabilities of failure require setting the system responses to events (e.g. the choice of gates into fault trees, the state boundaries into Markov diagrams). The behaviour of the system under fault conditions therefore must be completely determined in most of the models, maybe apart from a few fuzzy approaches (Pan, 1997). Moreover, it is difficult to analyse the impact of model architecture (e.g. fault tree gates, Markov diagram states and transitions) on results in a coherent manner, as it is common to do with input data. In fact, these constraints are usually of a discrete nature and are very significant, since architecture changes could often yield unrealistic configurations.

The next section aims to define a reliability approach which fits the properties of type B systems, and allows both input data (i.e. failure rates) and behaviour uncertainty analyses.

3.2 *Continuous gate for fault tree*

Fault trees, which are equivalent to reliability block diagrams, are common in industry. Moreover, they provide an efficient tool for SIL calculations, under some quantification warnings (Signoret, 2007). A fault tree based approach is therefore chosen in the present paper.

To deal with the uncertain behaviour of systems under fault conditions, a continuous fault tree gate, denoted C-gate, is introduced, and depicted in Figure 1. N basic events E_i are given with attributing weights p_i. The top-event gate then occurs if at least one of these options is fulfilled:

- option 1: any basic event E_i occurs and causes, with a probability equal to p_i, the top-event gate occurrence;
- option 2: all the basic events E_i occur.

By introducing fictitious events P_i which occur with constant probability equal to p_i, a C-gate is equivalent to the fault tree given by Figure 2. The "direct" or-gate refers to option 1, and the "logic" and-gate to option 2. Assuming all events independent, let:

- $F_i(t)$ be the probability that the basic event E_i occurs at time t;
- p_i be the constant probability that the fictitious event P_i occurs at time t.

The top-event gate probability of occurrence at time t, denoted $F_{top}(t)$, can then be expressed as follows (see proof in Appendix):

$$F_{top}(t) = 1 - \prod_{i=1}^{N} \left(1 - p_i \cdot F_i(t)\right) + \prod_{i=1}^{N} \left((1 - p_i) \cdot F_i(t)\right) \quad (1)$$

Figure 3 plots results of Equation (1) with $N=3$, $F_i(t)=1-e^{-0.001 \cdot t}$ for $i=1,\ldots,N$, and the weights p_i reported in Table 3.

Note that when all the weights are equal to 0, a C-gate is equivalent to an and-gate (i.e. parallel structure); and when all the weights are equal to 1, a C-gate is equivalent to an or-gate (i.e. series structure). Any coherent system reliability is comprised between parallel (for the most reliable case) and series (for the least reliable case) structure function (Rausand, 2004). By acting on the weights, a C-gate then allows continuous graduation of the system architecture (i.e. its behaviour under fault conditions). Moreover, the system analyses can be performed by classical tools, using equivalent fault trees.

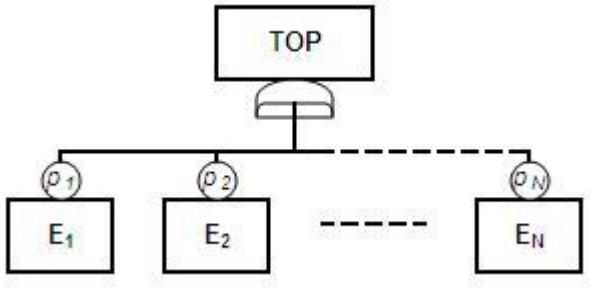

Figure 1. C-gate for fault tree

Table 3. C-gate unreliability functions, see Equation (1)

Weight			Unreliability function
p_1	p_2	p_3	
0	*0*	*0*	F[0.0](t) / parallel structure
0.5	*0*	*0*	F[0.5](t)
0.5	*0.5*	*0*	F[1.0](t)
0.5	*0.5*	*0.5*	F[1.5](t)
1	*0.5*	*0.5*	F[2.0](t)
1	*1*	*0.5*	F[2.5](t)
1	*1*	*1*	F[3.0](t) / series structure

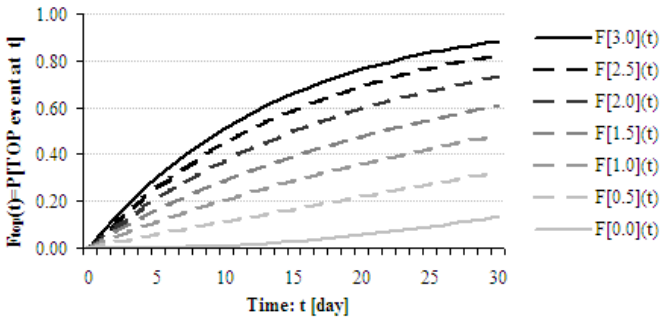

Figure 3. C-gate unreliability functions, see Table 3

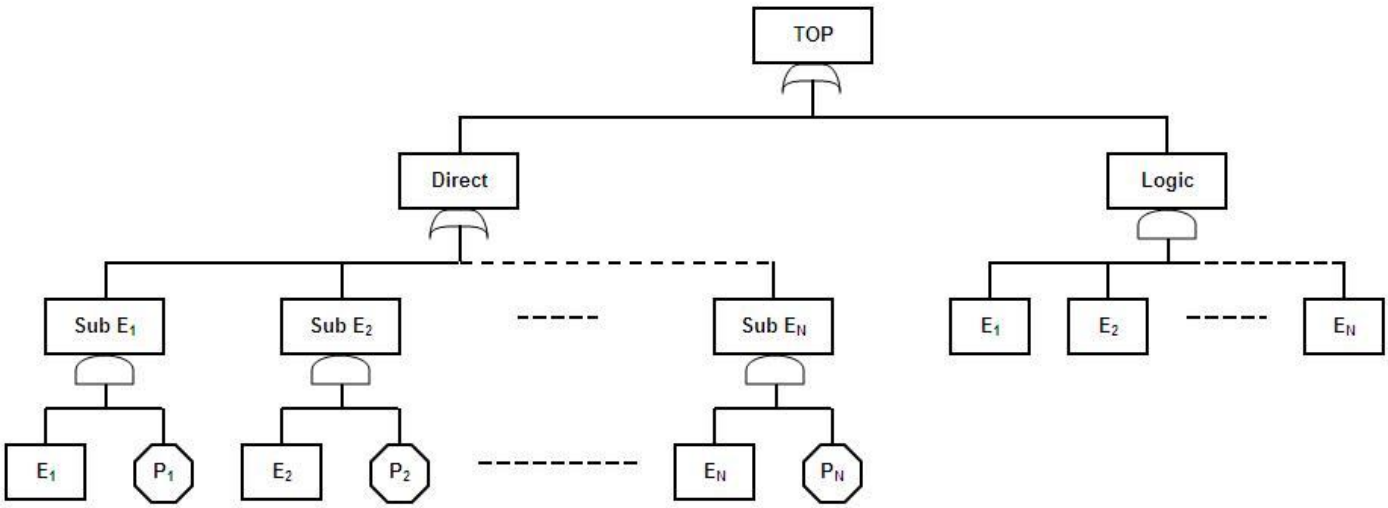

Figure 2. Equivalent fault tree for C-gate

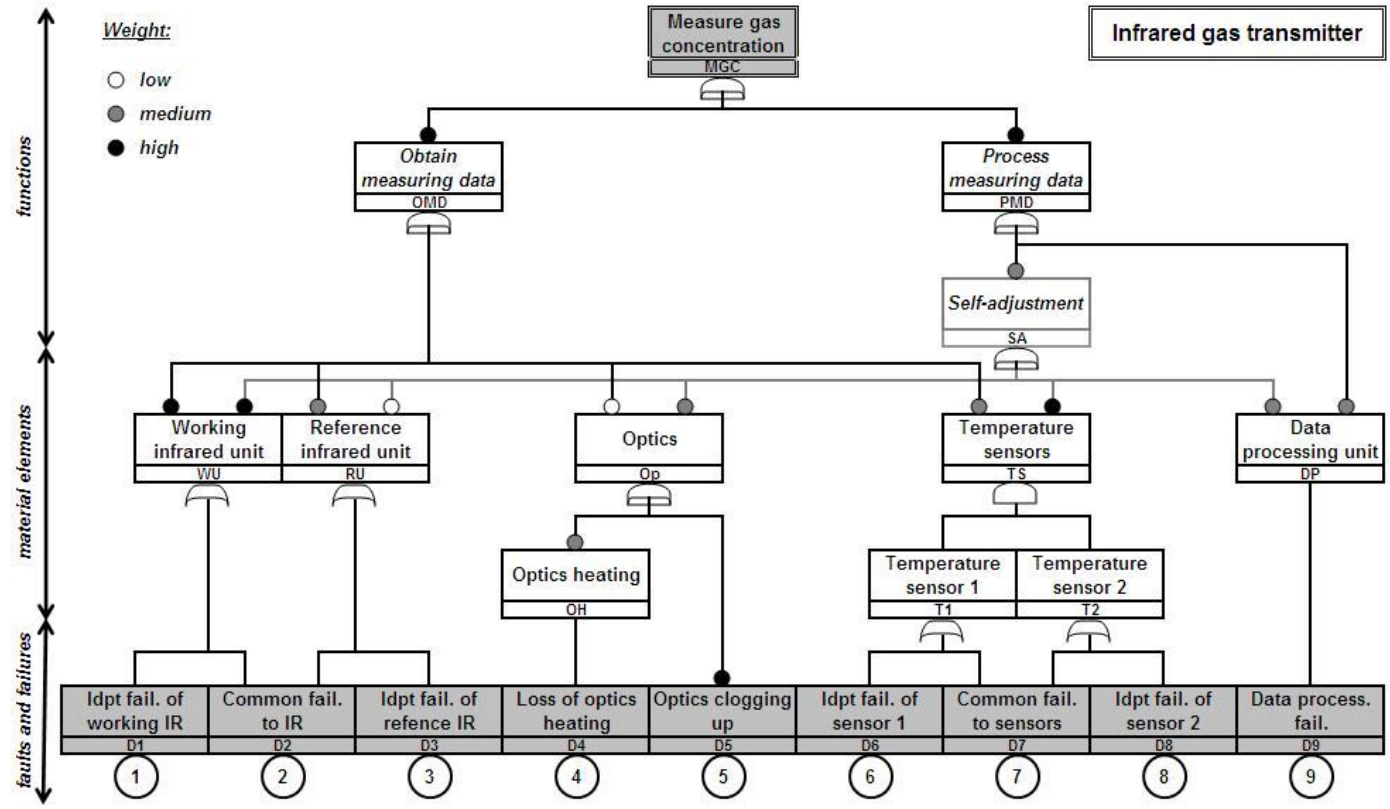

Figure 4. “3-step” (faults and failures–material elements–functions) fault tree for infrared gas transmitter, using C-gates

4 INTELLIGENT TRANSMITTER EXAMPLE

4.1 *Intelligent transmitter*

A transmitter can be described as "intelligent" according to its ability to modify its internal behaviour to optimize data collection and communicate them in a response manner to a host system (Brignell, 1996); and to the bi-directional communication for sending measurement and status information and receiving and processing external commands (IEC, 2006). Moreover, intelligent transmitters take advantage of digital technologies to allow specific functionalities (Brissaud, 2008): error measurement correction, self-adjustment, self-diagnosis and validation, on-line reconfiguration, and digital bidirectional communication. Such transmitters integrate programmable units and software, then the consequences of faults or failures on functions are difficult to predict. Intelligent transmitters are therefore examples of type B systems according to their behaviour under fault conditions which cannot be completely determined.

A transmitter for gas concentration measurement by infrared absorption is used as a case study. It is made up of two infrared units: the working unit sends a ray with a proportional wavelength to the gas concentration to be measured; and the reference unit sends a ray which does not respond to the gas. Through a wavelength ratio of the two receiving rays, the gas concentration quantity is obtained with a correction of the optics clogging up (mirror and plane), and power fluctuation of sending rays, if both are in acceptable ranges. Heating elements aim to prevent steam from building up on optics. Temperature is an important gas concentration influencing quantity. Two redundant sensors are therefore used for digital compensation of temperature while being in acceptable ranges. Finally, a data processing unit carries out all processing and calculations.

The safety function analysed in this paper is to *measure gas concentration*. It consists of obtaining measuring data (rays from working and reference infrared units, through the optics, and temperature) and processing them with appropriate digital corrections. This last function requires off-set and gain drift parameters which are defined by self-adjustments.

4.2 *Fault tree for intelligent transmitter*

A fault tree for the infrared gas transmitter example, using C-gates, is given by Figure 4. To deal with interactions between functions and material elements, a "3-step" approach is proposed (Brissaud, 2008). That is, the safety function to be evaluated (*measure gas concentration*) is broken up into subfunctions (*obtain measuring data* and *process measuring data*) and supporting functions (*self-adjustment*) which impact the former (self-adjustment aims to define parameters which are then used by the measuring data processing).

The second step of the fault tree represents the material elements which are required by the functions. Some elements are more critical than others for function fulfilments (attributed weights in C-gates differ). For example, temperature sensors are almost always essential to self-adjustment (this property is due to the algorithm of off-set and gain drift definition, which requires temperature as a main parameter), whereas in some cases, a failure of these sensors still allows obtaining of efficient measuring data (e.g. when temperature compensation is not significant). Similarly, depending on the failure of the data processing unit, it can yield a direct malfunction of the measuring data processing, or only an error in self-adjustment, which may also impact the measuring data processing as an indirect relationship.

The last step is a list of all potential faults and failures that the system may experience. Failures can be independent (i.e. impact only one element), or common to several material elements. Note that some faults or failures may have undetermined consequences on material elements, for example, due to not well defined failure modes (e.g. the degree of clogging up leading the optics into a failed state), or environmental constraints which are difficult to predict at any time (the loss of optic heating may have no impact on the system if, at that moment, the temperature and humidity are suitable).

4.3 *Fault tree analyses*

The weight values used for the C-gates are given in Table 4 (column "Base value"). The probability of fault or failure i at time t (i.e. occurrence of basic event D_i, see Figure 4), with $i=1,\ldots,9$, is equal to $F_i(t)=1-e^{-\lambda i \cdot t}$ with λ_i being the rate of fault or failure i, given in Table 5 (column "Base value").

The following assumptions are made:

- only dangerous failures which are not detected by online diagnostic test are taken into account;
- no maintenance action is performed in time interval *[0, 12 months]*;
- at the end of the 12^{th} month, test and maintenance actions are performed in such a way that the system is restored to an as good as new condition.

The fault tree analyses are performed using equivalent fault trees (see Figure 2), and SimTree, the fault tree module of the Aralia WorkShop software tool, distributed by Dassault Systemes. *249* minimal cut sets (MCS) have been obtained and are arranged by orders in Table 6. Probability of failure on demand of the safety function *measure gas concentration* (i.e. occurrence of the top-event gate MGC, see Figure 4) at time *t*, denoted *PFD(t)*, is depicted in Figure 5. The average value on time interval *[0, 12 months]*, denoted PFD_{avg}, is equal to $8.73 \cdot 10^{-3}$ and is also reported in Figure 5. According to Table 1, the safety function therefore fulfils SIL 2.

Table 4. Weight values

Type*	Name	Base value	Uncertainty analysis		
			law**	mean	variance
low	p_L	*0.10*	U[*0.0, 0.2*]	*0.10*	$3.3 \cdot 10^{-3}$
medium	p_M	*0.50*	U[*0.2, 0.8*]	*0.50*	$3.0 \cdot 10^{-2}$
high	p_H	*0.90*	U[*0.8, 1.0*]	*0.90*	$3.3 \cdot 10^{-3}$

* see Figure 4 caption
** U[*a*, *b*] is a uniform distribution between *a* and *b*

Table 5. Failure rates

Name	Base value	Uncertainty analysis		
	[hour^{-1}]	law*	mean	variance
λ_1	$4.0 \cdot 10^{-7}$	log-Normal	$4.0 \cdot 10^{-7}$	$3.2 \cdot 10^{-14}$
λ_2	$1.0 \cdot 10^{-7}$	log-Normal	$1.0 \cdot 10^{-7}$	$2.0 \cdot 10^{-15}$
λ_3	$4.0 \cdot 10^{-7}$	log-Normal	$4.0 \cdot 10^{-7}$	$3.2 \cdot 10^{-14}$
λ_4	$1.0 \cdot 10^{-6}$	log-Normal	$1.0 \cdot 10^{-6}$	$2.0 \cdot 10^{-13}$
λ_5	$3.0 \cdot 10^{-6}$	log-Normal	$3.0 \cdot 10^{-6}$	$1.8 \cdot 10^{-12}$
λ_6	$5.0 \cdot 10^{-7}$	log-Normal	$5.0 \cdot 10^{-7}$	$4.9 \cdot 10^{-14}$
λ_7	$1.5 \cdot 10^{-7}$	log-Normal	$1.5 \cdot 10^{-7}$	$4.5 \cdot 10^{-15}$
λ_8	$5.0 \cdot 10^{-7}$	log-Normal	$5.0 \cdot 10^{-7}$	$4.9 \cdot 10^{-14}$
λ_9	$5.0 \cdot 10^{-7}$	log-Normal	$5.0 \cdot 10^{-7}$	$4.9 \cdot 10^{-14}$

* the parameters $\{\mu,\sigma\}$ of the log-Normal distributions are equal to $\{ln(mean)-\sigma^2/2, ln(EF)/1.645\}$, with $EF=5$

Table 6. Minimal cut sets (MCS) arranged by orders

Order	Number of MCS	Cumulative number of MCS
1	000	000
2	000	000
3	007	007
4	038	045
5	050	095
6	100	195
7	042	237
8	012	249

Table 7. Uncertainty analysis configurations

Configuration	Uncertainty analysis on
Config.1	Failure rates only
Config.2	System behaviour (i.e. weight values) only
Config.3	Failure rates and system behaviour

Table 8. Uncertainty analysis results, obtained by 1,000,000 Monte Carlo simulations

Configuration	Mean	Variance	P[SIL2]	P[SIL1]
Config.1	$8.69 \cdot 10^{-3}$	$1.5 \cdot 10^{-5}$	*0.74*	*0.26*
Config.2	$8.73 \cdot 10^{-3}$	$2.9 \cdot 10^{-6}$	*0.78*	*0.22*
Config.3	$8.68 \cdot 10^{-3}$	$2.0 \cdot 10^{-5}$	*0.74*	*0.26*

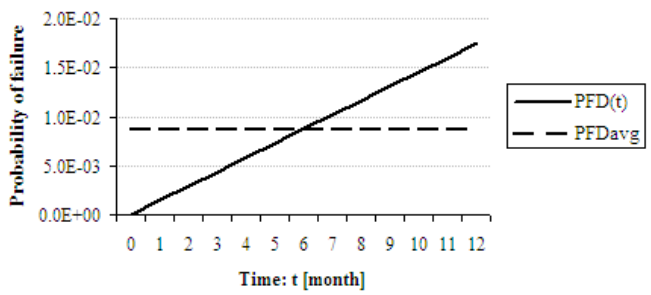

Figure 5. Probability of dangerous failure on demand at time *t*, *PFD(t)*, and on average, PFD_{avg}

4.4 *Uncertainty analyses*

System behaviour uncertainty can be translated into uncertainties in C-gate weight values (see Section 3.2). Uniform distributions are used to represent the uncertainties in weight values, according to weight type (i.e. low, medium, high), as reported in Table 4 (column "Uncertainty analysis"). It is assumed that extreme values (i.e. low and high weights) are more uncertain than the middle value (i.e. medium weight), as shown by the variances. Note also that these distributions are defined in such a way that the expectancies are equal to the base values.

To represent the uncertainties in failure rates, log-Normal distributions are more common. The parameters are defined in order to have a mean value equal to the base value, and an error factor equal to *5* (i.e. the lower and upper bounds of the *90%* centred confidence interval are obtained by dividing and multiplying the median value by *5*, respectively).

The uncertainty analyses are performed by Monte Carlo simulations. To make calculations faster, it is assumed that the *PFD(t)* is a linear function according to time, in interval *[0, 12 months]* (see Figure 5, the coefficient of determination has been computed at one minus $1.39 \cdot 10^{-5}$). The PFD_{avg} can therefore be obtained by the following approximation:

$$PFD_{avg} \approx \frac{PFD(12\ months)}{2} \qquad (2)$$

The three uncertainty configurations which are described in Table 7 are analysed. For each of them, 1,000,000 draws of Monte Carlo simulations have been performed to obtain several PFD_{avg} results by Equation (2). The resulting probability density functions of PFD_{avg} are depicted in Figure 6. The means and variances are given in Table 8 with the probability of being in SIL 2 or SIL 1, according to Table 1.

Note that in all of these configurations, the means are nearly equal to the PFD_{avg} value obtained in Section 4.3. The variances are of 10^{-5} to 10^{-6} order, and the probabilities of SIL fulfilments are very close among the configurations. Moreover, assuming the uncertainties in failure rates, the addition of system behaviour uncertainties does not have a significant effect.

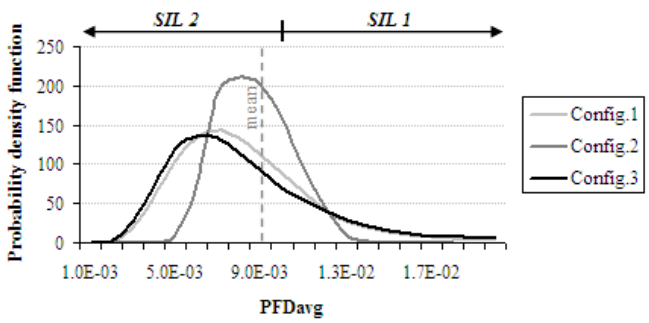

Figure 6. Probability density function of PFD_{avg} according to the configurations given in Table 8, obtained by Monte Carlo simulations, after smoothing

5 DISCUSSION

The previous analyses have shown that taking system behaviour uncertainties into account leads to an average probability of failure on demand with a relatively small variance (orders of magnitude lower than any of the weight variances). These results therefore tend to show that the uncertainties in inputs have not been increased through the proposed model but, on the contrary, are even sometimes partially mitigated. To give some explanations, the two operators used in the fault tree analyses (relating to an and-gate and to an or-gate) are investigated in this section, according to the expectancies *E[.]*, and the variances *V[.]*.

Let p_a and p_b be two independent random variables (in accordance with the hypotheses given in Section 3.2), then:

$$E[p_a \cdot p_b] = E[p_a] \cdot E[p_b] \tag{3}$$

$$V[p_a \cdot p_b] = E^2[p_a] \cdot V[p_b] + E^2[p_b] \cdot V[p_a] + V[p_a] \cdot V[p_b] \tag{4}$$

$$E[p_a \amalg p_b] = E[p_a] \amalg E[p_b] \tag{5}$$

$$V[p_a \amalg p_b] = (1 - E[p_a])^2 \cdot V[p_b] + (1 - E[p_b])^2 \cdot V[p_a] + V[p_a] \cdot V[p_b] \tag{6}$$

With the following operator:

$$\alpha \amalg \beta = 1 - (1 - \alpha) \cdot (1 - \beta) \tag{7}$$

Equations (3) and (5) explain that the mean values of PFD_{avg} obtained in Section 4.4 are nearly equal to the value obtained in Section 4.3. Moreover, the following statements can be deduced from Equations (4) and (6), (see proof in Appendix):

$$V[p_a \cdot p_b] \le \min\{V[p_a], V[p_b]\} \Leftrightarrow \frac{E^2[p_a]}{V[p_a]} + \frac{E^2[p_b]}{V[p_b]} \le \frac{1}{\max\{V[p_a], V[p_b]\}} - 1 \tag{8}$$

$$V[p_a \amalg p_b] \le \min\{V[p_a], V[p_b]\} \Leftrightarrow \frac{(1 - E[p_a])^2}{V[p_a]} + \frac{(1 - E[p_b])^2}{V[p_b]} \le \frac{1}{\max\{V[p_a], V[p_b]\}} \tag{9}$$

Equations (8) and (9) give the necessary and sufficient conditions on two input random variables so that the corresponding operation gets a lower variance than any of the inputs. Because these conditions are often fulfilled by the random variables of Tables 4 and 5, resulting variances of PFD_{avg} are relatively small. Due to dependencies between MCS, it is, however, difficult to recursively apply Equations (4) and (6) to obtain PFD_{avg} variance by calculations.

6 CONCLUSION

This paper has presented safety requirements for the SIS design in accordance with IEC 61508. Special issues of type B systems are discussed. While several research works have been undertaken to deal with uncertainties in failure rates for reliability evaluation, modelling the uncertain behaviour of the system under fault conditions has been less investigated. This paper therefore proposes a modelling method adapted to the evaluation of failure probabilities for these complex systems.

Within the fault tree modelling framework, the key feature of the method is the use of weighted "continuous gates". By acting on the weight values, it is possible to continuously graduate the system part architecture between parallel and series structures. The behaviour of the system under fault conditions is therefore parameterised so that the uncertainty on the system architecture can be translated into a parametric uncertainty. Moreover, such analyses can be performed by classical fault tree tools using equivalent fault trees with classical gates and fictitious events.

An intelligent transmitter is used as example. The probability of failure on demand is assessed, and both failure rates and behaviour uncertainty analyses are performed by Monte Carlo simulations. The resulting average probabilities of failure on demand are used to determine the probability of safety integrity level (SIL) fulfilment, according to IEC 61508, and taking the undetermined system behaviour under fault conditions into account. The resulting uncertainties in probabilities of failure are orders of magnitude lower than the uncertainties in any of the input weights, as shown by the variance results. Some discussions are proposed to give some explanations of this property. These analyses therefore tend to show that the lack of knowledge in system behaviour can be accounted for and partially compensated for by this kind of fault tree, in order to evaluate probabilities of system failure on demand.

7 APPENDIX

7.1 *Proof of (1)*

According to Figure 2:

$$F_{top}(t) = P\left[\left(\bigcup_{j=1}^{N}\left(E_j \cap P_j\right)\right) \cup \bigcap_{i=1}^{N} E_i\right]$$

Using the conditional probability definition:

$$F_{top}(t) = P\left[\bigcup_{j=1}^{N}\left(E_j \cap P_j\right)\right] + P\left[\bigcap_{i=1}^{N} E_i\right] - P\left[\bigcap_{i=1}^{N} E_i\right] \cdot P\left[\bigcup_{j=1}^{N}\left(E_j \cap P_j\right) \Big/ \bigcap_{i=1}^{N} E_i\right]$$

$$F_{top}(t) = P\left[\bigcup_{j=1}^{N}\left(E_j \cap P_j\right)\right] + P\left[\bigcap_{i=1}^{N} E_i\right] - P\left[\bigcap_{i=1}^{N} E_i\right] \cdot P\left[\bigcup_{j=1}^{N} P_j\right]$$

$$F_{top}(t) = P\left[\bigcup_{j=1}^{N}\left(E_j \cap P_j\right)\right] + P\left[\bigcap_{i=1}^{N} E_i\right] \cdot \left(1 - P\left[\bigcup_{j=1}^{N} P_j\right]\right)$$

$$F_{top}(t) = P\left[\bigcup_{j=1}^{N}\left(E_j \cap P_j\right)\right] + P\left[\bigcap_{i=1}^{N} E_i\right] \cdot P\left[\bigcap_{j=1}^{N} \overline{P_j}\right]$$

And, according to notations given in Section 3.2:

$$F_{top}(t) = 1 - \prod_{i=1}^{N}\left(1 - p_i \cdot F_i(t)\right) + \prod_{i=1}^{N} F_i(t) \cdot \prod_{j=1}^{N}(1 - p_i)$$

$$F_{top}(t) = 1 - \prod_{i=1}^{N}\left(1 - p_i \cdot F_i(t)\right) + \prod_{i=1}^{N}\left((1 - p_i) \cdot F_i(t)\right)$$

7.2 *Proof of (8)*

According to (7):

$$V[p_a \cdot p_b] \le V[p_a] \Leftrightarrow \frac{E^2[p_a]}{V[p_a]} \le \frac{1}{V[p_b]} - \frac{E^2[p_b]}{V[p_b]} - 1$$

$$V[p_a \cdot p_b] \le V[p_p] \Leftrightarrow \frac{E^2[p_a]}{V[p_a]} \le \frac{1}{V[p_a]} - \frac{E^2[p_b]}{V[p_b]} - 1$$

Then:

$$V[p_a \cdot p_b] \le \min\{V[p_a], V[p_b]\} \Leftrightarrow$$

$$\frac{E^2[p_a]}{V[p_a]} + \frac{E^2[p_b]}{V[p_b]} \le \frac{1}{\max\{V[p_a], V[p_b]\}} - 1$$

REFERENCES

Beurden, I. van & Amkreutz, R. 2004. 'Proven-in-use' criteria for safety instrumented systems. *Hydrocarbon processing* 81(11): 61-70

Brignell, J. E. 1996. The future of intelligent sensors: A problem of technology or ethics? *Sensors And Actuators A-Physical* 56: 11-15

Brissaud, F. et al. 2008. Capteurs intelligents : nouvelles technologies et nouvelles problématiques pour la sûreté de fonctionnement. In IMdR (ed). *16e Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement*. Bagneux: IMdR

Camargo, J.B. et al. 2001. Quantitative analysis methodology in safety-critical microprocessor applications. *Reliability Engineering and System Safety* 74: 53-62

Garret, C.J. & Apostolakis, G.E. 2002. Automated hazard analysis of digital control systems. *Reliability Engineering and System Safety* 77: 1-17

Guérin, F. et al. 2003. Reliability estimation by Bayesian method: definition of prior distribution using dependability study. *Reliability Engineering and System Safety* 82: 299-306

Hauptmanns, U. 2008. The impact of reliability data on probabilistic safety calculations. *Journal of Loss Prevention in the Process Industries* 21: 38-49

Helton, J.C. et al. 2004. An exploration of alternative approaches to the representation of uncertainty in model predictions. *Reliability Engineering and System Safety* 85: 39-71

Innal, F. et al. 2006. An attempt to understand better and apply some recommendations of IEC 61508 standard. In Langseth, H. & Cojazzi, G. (eds). *30th ESReDA seminar; Proc., Trondheim, 7-8 June 2006*. Ispra: ESReDA

International Electrotechnical Commission [IEC] (1st) 2004. *IEC 61511, Functional safety – Safety instrumented systems for the process industry sector – All parts*. Geneva: IEC

International Electrotechnical Commission [IEC] (1st) 2005a. *IEC 61508, Functional safety of electrical / electronic / programmable electronic safety-related systems – All parts*. Geneva: IEC

International Electrotechnical Commission [IEC] (1st) 2005b. *IEC 62061, Safety of machinery – Functional safety-related electrical, electronic and programmable electronic control systems*. Geneva: IEC

International Electrotechnical Commission [IEC] (1st) 2006. *IEC 60770-3, Transmitters for use in industrial-process control systems – Part 3*. Geneva: IEC

International Electrotechnical Commission [IEC] (2nd) 2009. *IEC 61508, Functional safety of electrical / electronic / programmable electronic safety-related systems – All parts*. Geneva: IEC

Langeron, Y. et al. 2007. Safe failures impact on Safety Instrumented Systems. In Aven, T. & Vinnem, J. (eds). *Risk, reliability, and societal safety*: 641-648. London: Taylor & Francis

Lundteigen, M.A. & Rausand, M. 2009. Architectural constraints in IEC 61508: Do they have the intended effect? *Reliability Engineering and System Safety* 94: 520-525

Rausand, M. & Høyland, A. (2nd ed.) 2004. *System reliability theory; models, statistical methods, and applications*. New York: Wiley

Pan, H.S. & Yun, W.Y. 1997. Fault Tree Analysis with Fuzzy Gates. *Computers ind. Engng* 33: 569-572

Signoret, J.P. et al. 2007. High Integrity Protection Systems (HIPS): Methods and tools for efficient Safety Integrity Levels (SIL) analysis and calculations. In Aven, T. & Vinnem, J. (eds). *Risk, reliability, and societal safety*: 663-669. London: Taylor & Francis

Singer, D. 1990. A fuzzy set approach to fault-tree and reliability analysis. *Fuzzy Sets and Systems* 34: 145-155

Tanaka, H. et al. 1983. Fault-tree analysis by fuzzy probability. *IEEE trans. Reliability* 32: 453-457

Wang, Y. et al. 2004. The impact of data uncertainty in determining safety integrity level. *Process Safety and Environmental Protection* 82(B6): 393-397