CHEMICAL ENGINEERING TRANSACTIONS
VOL. 32, 2013
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at: www.aidic.it/cet
Chief Editors:SauroPierucci, JiříJ. Klemeš

ISBN 978-88-95608-23-5; **ISSN** 1974-9791
DOI: 10.3303/CET1332040

Performance Assessment of an Emergency Plan Using Petri Nets

Rachida Hamzi*[a], Fares Innal[a], Mohamed A.Bouda [a,b], Makhlouf Chati [a,b]

[a]Laboratoire de Recherche en Prevention Industrielle (LRPI), Institut d'Hygiène et Sécurité Industrielle, Université El Hadj Lakhdar-Batna, Avenue Chahid M. Boukhlouf 05000, Batna, Algeria
[b] SONATRACH, Division Production, BP 64 Hassi R'mel 03300, Laghouat, Algeria
Hamzi_hr@yahoo.fr

Emergency plans (EP) are complex systems which incorporate elements of three different natures: technical, human and organizational. In addition, they must be executed under time and efficiency constraints. This inherent complexity may leads to a number of failures, such as unavailability of critical personnel or technical assets and inappropriate operators' actions. In this paper we present a Petri Net-based approach to model and evaluate the performance of an EP related to condensate storage tank fire scenario. In fact, Petri Nets are a powerful tool to describe complex systems and their inherent interactions. Due to the model complexity, results are obtained thanks to Monte Carlo simulation.

1. Introduction

The failure of nowadays industrial installations may result in major hazard accidents. In order to limit their consequences, regulatory bodies require the establishment of Emergency Plans (EP) in accordance to the identified accident scenarios. Within the framework of Algerian Oil and gas industries, many factors played a major role in crisis management policy, including:

- Increasing number of major accidents occurred during the last decade, particularly: Skikda refinery fire (2004, 2005) and Skikda LPG Unit explosion (2004),
- Lack of the experience feedback (often referred to as "lessons learned"),
- Insufficiency of local regulatory related to the major hazard accidents.

Regarding this statement, the Algerian authorities – according to the article 2 of the executive decree 09-335/ 20October 2009 - required the establishment of so-called "Internal Emergency Plan (IEP)", which describes the measures to be taken inside the establishment in case of a major industrial accident aiming to protect people, property and the environment. The structure of the IEP is shown in Figure 1. The different plans that can be triggered when an emergency situation has occurred and according to its magnitude are successively the Internal Emergency Plan (IEP), the External Emergency Plan (EEP) and Crisis Plan (CP). There are four steps after detection and alert of an accidental situation: the two first steps which are the intervention team on site and the Operational command Post that concern the IEP, the third one is represented by the Tactic Command Post for EEP and the last one by the Strategic Command Post for the CP.

According to the IEP structure, it may be considered as a complex system which requires powerful modelling and analysis tools in order to assess its effectiveness. In this context, Petri Nets, in particular due to their graphical representation, have been widely used in the modeling and the performance assessment of nowadays complex systems. A brief presentation of PNs is given in section 2. The object of Section 3 is twofold. First, we describe the accident scenario and the related IEP used to demonstrate our approach. Secondly, the modelling and the performance evaluation of this IEP are presented. Section 4 summaries our concluding remarks.

Please cite this article as: Hamzi R., Innal F., Boudaa A., Chati M., 2013, Performance assessment of an emergency plan using petri nets, Chemical Engineering Transactions, 32, 235-240 DOI: 10.3303/CET1332040

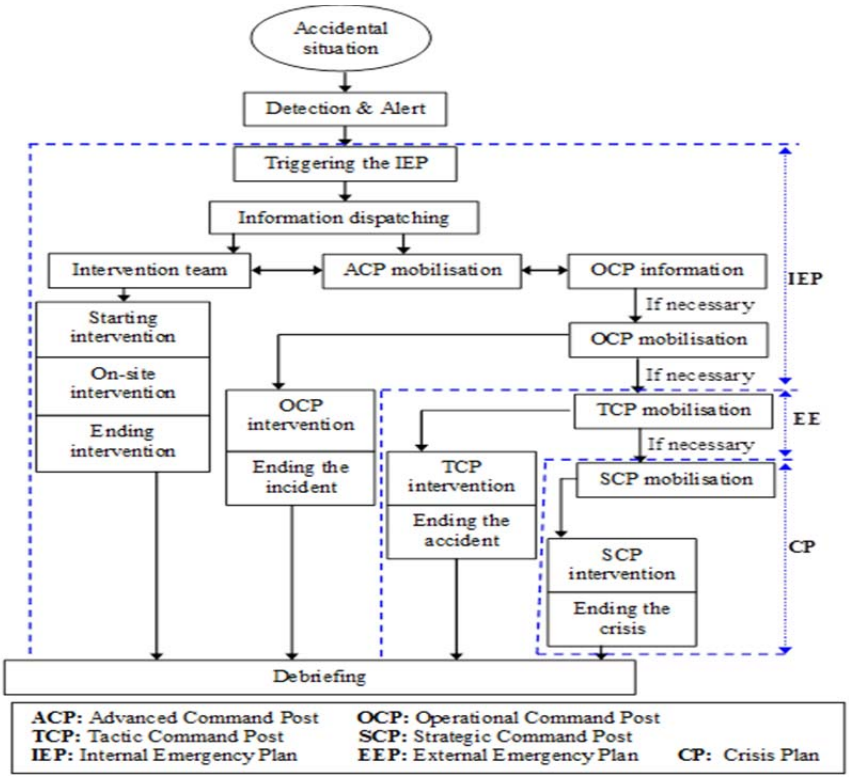

Figure 1: IEP structure (DNV, 2010)

2. Overview of Petri Nets (PNs)

Petri Nets were developed by Carl Adam Petri during his PhD thesis on communication with automata (Gu and Bahri, 2002). Their purpose was initially the description of causal relationships between conditions and events in a computer system. Since then, many extensions related to PNs have been made in order to enlarge their modelling capabilities. In this article, the Petri Net presentation is deliberately limited to the necessary concepts which are used in the following sections. For the interested readers, a detailed description of PNs theory is given in (David and Alla, 2010).

A Petri net is a graphical notation with an underlying mathematical structure suited to model event-driven systems (discrete event systems)(Huang and Liang, 2004). It may be identified as a particular kind of bipartite directed graph which contains two parts (IEC 61508, 2010) (Blume et al., 2007):

(i) *Static part* which include three objects:

- *places*, depicted as circles or ovals in the graphical representation, are states of system components.
- *transitions*, drawn as bars or boxes, corresponding to potential events that change the state of a Petri net. Delays may be assigned to transitions (e.g. required time to carry out a given task).
- *oriented arcs* connecting places to transitions (*upstream* or *input arcs*) and transitions to places (*downstream*or *output arcs*). Arcs are *weighted* with a positive number. For example, the weight of an upstream arc may indicate the required resources to achieve a given action whereas that of a downstream arc may indicate the amount of the output resulted from this action. This weight equals to one if it is not explicitly mentioned on the graph.

(ii) *Dynamic part*:

- *tokens* pictured by small solid dots. Each place may potentially hold either none or a positive number of tokens which illustrate that the corresponding place is currently allocated. The distribution of tokens in places is referred as the *marking*. Tokens move through transitions when events occur. A token may, for example, represent the presence or absence of a resource.
- *predicates*or *guards*, any formula which may be true or false, *enabling* transitions.
- *assertions*, any equation, updating some variables when a transition is *fired*.

It is useful to make a distinction between '*enabling*' and '*firing*' of transitions:

- A transition is enabled when all input places contain at least the number of tokens required by each input arc (indicated by its weight) and all predicates must be 'true'.
- A transition is fired when all preconditions are satisfied (i.e. it is enabled) and a required delay is elapsed (duration from the enabling until the firing). This delay may be deterministic or stochastic (random delay, e.g. negative exponential). If no delays exist (delay = 0) then enabling coincides with firing.

On the firing of a transition:

- input places lose as many tokens as specified by the weights of input arcs.
- output places gain as many tokens as specified by the weights of output arcs.
- assertions are updated.

In the case where deterministic and stochastic delayed transitions are involved, which is the case for real life systems, the resulting PNs cannot be solved using analytical approaches. Hence, a simulation approach has to be considered to efficiently asses the expected performance measures. This being the case, Monte Carlo simulation is an effective tool to deal with stochastic processes. The principle of Monte Carlo simulation is to use random numbers to animate a behavioural model of the real system. It is worth noting that PNs provide a very efficient support for performing Monte Carlo simulation (IEC 61508, 2010). The Monte Carlo simulation is run to produce a large statistical sample from which statistical results are obtained. For a given simulated parameter X, the basic statistics allow the calculation of the average, variance and confidence interval of the sample (X_i) which has been simulated:

$$\overline{X} = \sum_{i}^{n} x_i / n \tag{1}$$

$$\sigma^2 = \sum_{i}^{n} (x_i - \overline{X})^2 / n \tag{2}$$

$$\text{Confidence interval} = \left[\overline{X} - E \cdot (\sigma / \sqrt{n}),\ \overline{X} + E \cdot (\sigma / \sqrt{n}) \right] \tag{3}$$

where E = 1.6449 for confidence = 90 %.

3. Scenario description and its IEP analysis

3.1 Scenario description

The chosen accident scenario relies on the Loss Of Containment (LOC) in a condensate storage tank (appertaining to SONATRACH / DP Hassi R'mel: Algerian Oil company). We note that the description and the data given hereafter are provided by operational and intervention teams in charge of the installation where de condensate tank is located. The situation of the considered tank regarding the whole installation is depicted in Figure 2.

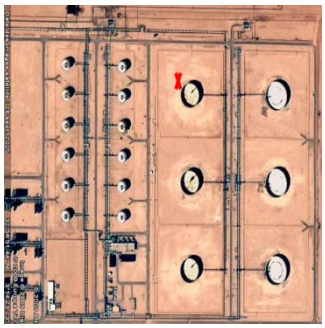

Figure 2: Condensate tank situation

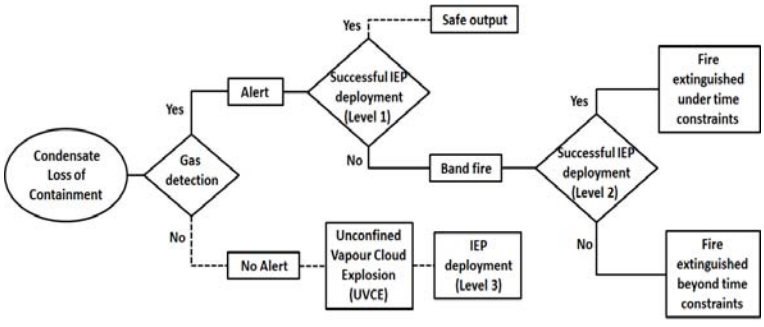

Figure 3: Scenario description

The studied scenario is described in Figure 3. A complete scenarios description resulting from a LOC is given in (Joaquim et al., 2012). We assume that the initiating event, the condensate Loss Of Containment (LOC), is produced on the piping enabling the storage tank filling (within a frequency of 3.11E-3/y). This LOC should be detected thanks to a gas detection system, made up of the following:

- 3 gas detectors (GD): at least the working of one GD is required. Also, each GD may fail under solicitation with a probability equals to 0.05.
- Programmable Logic Controller (PLC), which has a probability of failure equals to 0.022.
- Gas indicator (GI: situated in the control room), which has a probability of failure equals to 0.01.

In addition, the LOC could be detected by on-site operator (witness). According to portion of time the operator should be near the storage tank, he can fail to detect the incident with a probability equals to 0.2. Once the LOC is detected, the alert is triggered instantaneously in case of automatic detection, whereas it takes 4 min with operator detection. Then the IEP (level 1) is deployed. It aims to limit and therefore control the condensate LOC. For this level, the necessary emergency actions should be carried out with respect to the following chronological order.

- *Operational team intervention*. It consists in closing valves and pumps, allowing the filling of the condensate tank, in order to limit the condensate leakage amount. Note that this operation must be achieved in a specified time (Critical Time = 15 min). Beyond this time, the LOC may lead to a band fire which is difficult to master. One has to consider the following element:

- The closing of pumps may be achieved according to three ways: (1) instantaneously if the Emergency Shutdown Push Button works (probability of failure = 0.044), else (2) after 5 min if the whole operational team (team 1) is available or after 10 min if the team number is not sufficient.
- The closing of valves may be achieved according to three ways: (1) instantaneously if they work automatically (probability of failure = 3.28E-3), else (2) after 10 min if the whole operational team (team 2) is available or after 16 min if the team number is not sufficient.

- *Emergency team intervention*. Its actions are delayed 3 min regarding the first intervention and are the following:
  - Safety bounder establishment: this operation has an efficiency of 90% (the 10% of inefficiency is due to the large area to be prevented).
  - Ignition sources prevention: its efficiency = 91 % (due to mobiles, synthetic clothes, cars).
  - Foam film establishment: it depends on the water pumps and emulsifier. There are 5 water pumps (3 on-site and 2 off-site). The starting of Water pumps may be performed according to four ways: (1) Instantaneously if the ESD Push button works (probability of failure = 0.044) and the pumps work (with probability of failure for each pump = 0.019) or the off-site pumps work (probability of failure= 0.019), else (2) after 3.50 min if the whole operational team (team 3) is available or after 7 min if the team number is not sufficient. The emulsifier tank may fail according to a probability = 0.09 (provided after 5 min). In case of its failure, a rescue emulsifier is provided within 2 min.

If the first level emergency deployment fails in limiting the condensate LOC under the Critical Time constraint (15 min), a band fire may occur if both ignition sources and the failure of foam film establishment in due time (10 min). In that case, a second level emergency has to be implemented:

- *Cooling actions*, carried out by fixed means, to answer the protection of a LPG sphere and a Condensate tank in the vicinity of the damaged condensate tank. The cooling system success depends on the functioning of water system (described above) and two nozzles (sphere and tank). Each nozzles may fails according to a fixed probability equals to 0.023.
- Fire extinguishing actions using four trucks (two trucks among them are needed to control the fire). Each truck has a probability of failure = 0.01, due to: emulsifier storage failure or truck mechanical failure.

3.2 IEP analysis

The aim of this section is the performance assessment of the IEP described above. This evaluation is based on the duration taken to perform the two emergency levels. In particular, we are interested in the following three intervention phases:

- *IEP level 1*: condensate LOC emergency. As we have mentioned, we assume that operation should at most take 15 min. Beyond this critical time, the LOC could result in a fire band. The performance of this action is evaluated through the probability (P_1) that LOC control duration be lower than15 min.
- *IEP level 2*: fire extinguishing. This operation is assessed according to two phases:

- Temporization duration, i.e. the time elapsed between the band fire starting and the arrival of reinforcements extinguishing means (trucks). The related performance is computed towards the probability (P_2) that the duration between the fire starting and the temporization ending do not exceeds 30 min.
- Fire extinction duration, the time elapsed between the starting and the extinguishing of the band fire. Its performance is measured with respect to the probability (P_3) that this duration be lower than 60 min.
- Avoiding domino effects. Its performance is characterized by the probability (P_4) of either the fire extinction in due time (60 min) or that of cooling system working.

3.3 PNs models

In order to compute all the specified probabilistic quantities, PNs models relating to the described scenario have been established.Some explanations related to the syntax related to the PNs developed are given: *#i* (*i* is an integer > 0) is the marking of the place number *i* on the network; *jets* indicates the number of tokens; *!!* introduces a list of variables assignments (these assignments take place when the transition is

launched); *??* specifies a list of conditions that must be verified for the transition to be valid; *drc d* is Dirac's law of duration *d; @* (*k*) (e_1, e_2, …, e_n) is a the *k* out-of *n* Logic (e_i are Boolean expressions).
We present in the following some of these PNs.

• *Condensate LOC and Gas detection*. At time = 0, we made the assumption that the LOC is occurred. This fact is modeled by the PN of Figure 4(a). Figure 4(b) model the behavior of Gas detector 1 (GD1) under solicitation (*?? LOC==true*). Note that all component behaviours under solicitation are modelled according to the general scheme of figure 4(b). Once the detection is performed, the Alert must be given (*!! Alert = true*) to deploy the IEP of level 1, see Figure 4(c).

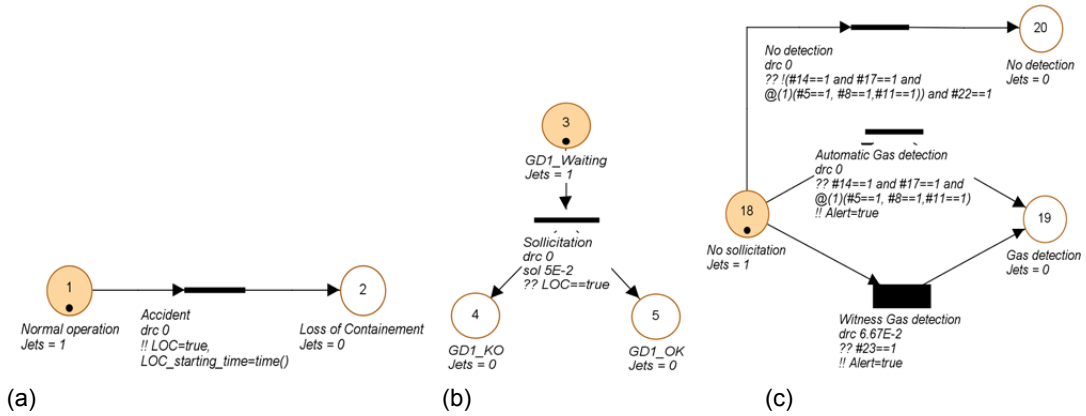

Figure 4: (a) Condensate LOC, (b) Gas Detector 1 (GD1) behaviour and (c) Gas detection system

• *Operational team intervention*. We recall that its function is to control the LOC through the closing of pumps and valves, see Figure 5.

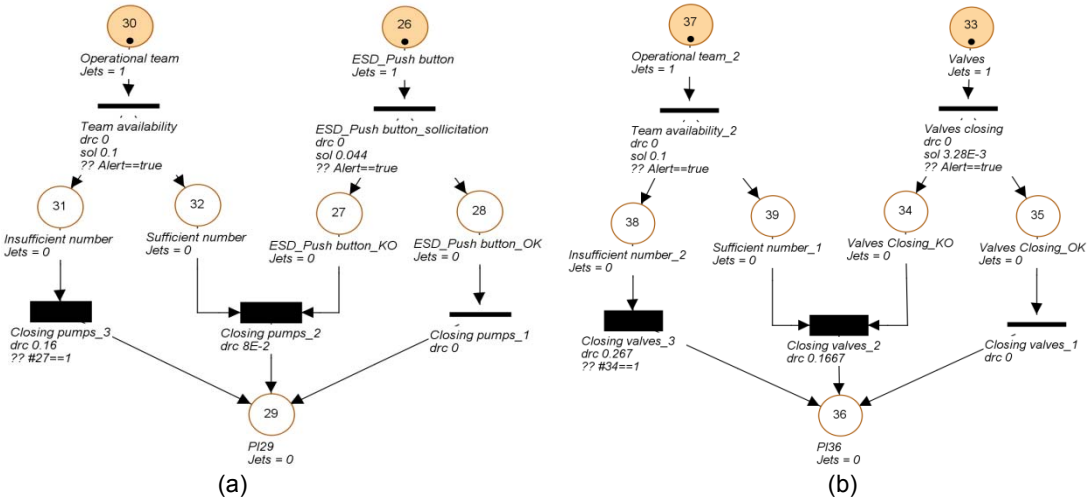

Figure 5: (a) Closing of pumps and (b) Closing of valves PNs models

• *Emergency team intervention*. We only present the foam film PNs models, which depends on water pumps (not depicted hereafter) and emulsifier availability: (??(#81==1 or #86==1) and #89==1).

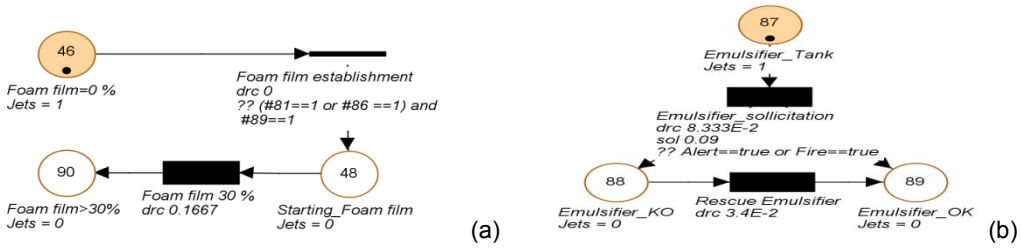

Figure 6: (a) Foam film and (b) Emulsifier availability

- *Fire starting and extinguishing*. Figure 7(a) presents the three conditions that the junction is required to trigger the fire: (ignition, foam insufficiency and uncontrolled LOC (within 15 min), whilst Figure 7(b) shows the fire extinguishing process. Note that trucks behaviorsare note depicted below.

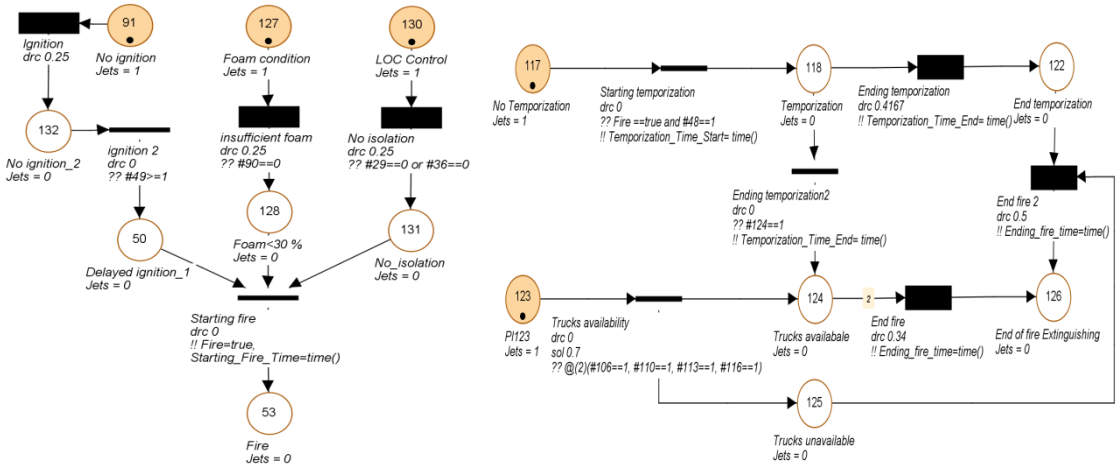

Figure 7: (a) Fire starting and (b) Fire extinguishing

4. Results and conclusion

The simulation of the developed PNs, 1E+6 trials have been performed, results in the numerical values provided in Table 1.

Table 1: Obtained results

Probabilities	Averages	Standard deviations (σ)	Lower bounds (CI 90%)	Upper bounds (CI 90%)
P_1	9.9329E-1	8.1621E-2	9.9316E-1	9.9343E-1
P_2	9.0267E-1	2.9638E-1	9.0220E-1	9.0317E-1
P_3	9.7099E-1	1.6781E-1	9.7072E-1	9.7127E-1
P_4	9.9862E-1	3.6731E-2	9.9858E-1	9.9871E-1

Table 1 shows that the performance indicators that we are looking for are very high, except P_2, ≈0.9, which indicates that the temporization duration, may be greater than the threshold value (30 min) within 10% of cases. Hence, that performance has to be improved, for example, by increasing the reliability of water pumps or that of the emulsifier storage tank. In a future work we expect to consider uncertainties related to some operation durations: e.g. closing valves or pumps in case of unavailability of operators. Note that uncertainties may reduce the above quantities and therefore decrease the IEP performance.

References

Blume H., Von Sydow T., Becker D. and Noll T.G., 2007, Application of deterministic and stochastic Petri-Nets for performance modeling of NoC architectures, Journal of Systems Architecture, 53, 466-476.

Casal J., Gomez-Mares M., Munoz M. and Palacios A., 2012, Jet Fires: a “Minor” Fire Hazard?, Chemical Engineering Transactions, 26, 13-20 DOI: 10.3303/CET1226003.

David R., Alla H., 2010, Discrete, continuous and hybrid Petri nets, 2nd ed, Springer Publishing Company, Berlin, Germany.

DNV (DET NORSKE VERITAS), 2010, Plan d'Intervention Interne (PII), Rapport N° EP002720 N° 6 – HRM Centre, SONATRACH (in French).

Gu T., Bahri P.A., 2002, A survey of Petri net applications in batch processes, Computers in Industry, 47, 99-111.

Huang C.-C., Liang W.Y., 2004, Object-oriented development of the embedded system based on Petri-nets, Computer Standards & Interfaces, 26, 187-203.

IEC 61508 standard, 2010, Functional safety of electrical/electronic/programmable electronic safety-related systems, 2nd ed, International Electrotechnical Commission, Geneva, Switzerland.