Journal of Loss Prevention in the Process Industries 31 (2014) 56–69

Contents lists available at ScienceDirect

Journal of Loss Prevention in the Process Industries

journal homepage: www.elsevier.com/locate/jlp

Probability and frequency calculations related to protection layers revisited

Fares Innal [a, *], Pierre-Joseph Cacheux [b], Stéphane Collas [b], Yves Dutuit [c], Cyrille Folleau [d], Jean-Pierre Signoret [e], Philippe Thomas [d]

[a] Batna University, IHSI-LRPI, Avenue Chahid M. Boukhlouf, 05000 Batna, Algeria
[b] TOTAL EP, CSTJF, Avenue Larribau, 64000 Pau, France
[c] TOTAL Associate Professors, 38, rue du Prieuré, 33170 Gradignan, France
[d] SATODEV, 25 rue Marcel Issartier, 33700 Mérignac, France
[e] TOTAL Technology Specialist, 2 route de Garlin, 64160 Sedzère, France

ARTICLE INFO

Article history:
Received 11 August 2013
Received in revised form
3 June 2014
Accepted 7 July 2014
Available online 15 July 2014

Keywords:
Independent and dependent protection layers
Safety instrumented systems
Failure frequency
Fault tree
Markov model

ABSTRACT

This article casts a new glance over some methods dedicated to the calculation of the likelihood (probability or frequency) of failure of systems and, in particular, safety-related systems working alone or in association with other protection layers. It consists first in examining with a critical eye the relevancy of the aforementioned methods, which are still often used in spite of their restrictive limitations, and second in proposing an alternative approach for each of them. The correctness of the examinated methods is tested by applying them to very simple systems modeled by fault tree models, with intent to show why these methods are debatable and how they can be replaced by other ones, more appropriate. The particular case of several protection layers having to react on the demand resulting from the global failure of their associated control system is considered. That case leads to revisit the common assumption of the independence between the above protection layers and control system, by taking into account the order of their respective failures from a qualitative and quantitative point of view.

1. Introduction

Risk management approaches are aimed primarily at reducing the current risk, generated by a given application, to an acceptable or tolerable level and to maintain that level over time. This reduction is often achieved by interposing several layers (or barriers) of protection between the hazard source, which can be the monitored process, and the potential targets (people, plant and environment). The typology of these layers covers a wide variety and is increasingly supplemented by extra layers known as safety instrumented systems (SISs). These safety-related systems have sparked off and continue to cause a growing interest from industrial users, contractors and academics as well. This general interest is shown by the abundant literature dealing with this topic and by the second edition of IEC 61508 (2010) and IEC 61511 (2012) standards devoted to functional safety. The first one is already published, whilst the second one is still in the draft stage. The protection layers based-technique carried out to reduce risk is well-known and has been looked at in detail in (Center for Chemical Process Safety (CCPS), 2001) and in annexes B and F of the first edition of IEC 61511-3 standard (IEC 61511, 2003), respectively entitled *"Semi-quantitative method"* and *"Layer Of Protection Analysis (LOPA)"*. This protection technique has been abundantly presented, commented on, implemented, and the formula given in this standard to calculate the so-called mitigated event likehood, also known as hazardous-event rate (HER) or hazard event frequency (HEF) (Misumi & Sato, 1999), has been applied by many authors (see, for instance, Babu, 2007; Delvosalle, Fiévez, Pipart, Londiche, & Debray, 2004; Dowell, 1998; Dowell & Hendershot, 2002; Gowland, 2005; Marszal, 2000). But, since that time, the use of this formula and several other calculation methods in the same domain seem debatable (Innal, 2008; Innal, Dutuit, Rauzy, & Signoret, 2010) and then deserve to be further analyzed. This is the object of the present paper which is organized as follows. Section 2 is devoted to the critical analysis of two fault tree-based methods sometimes used to calculate the failure probability or the failure frequency of systems. These methods are applied on an elementary fault tree model to focus more easily on their intrinsic limitations by comparing the results they give with those provided by a right method. On the basis of a basic process control system (BPCS) associated to a paire of safety

* Corresponding author. Tel.: +213 669290488.
E-mail address: innal.fares@hotmail.fr (F. Innal).

http://dx.doi.org/10.1016/j.jlp.2014.07.001
0950-4230/

instrumented systems working together on demand, Section 3 shows that the formula proposed by IEC 61511 standard to calculate the average hazard event frequency, gives only an approximate result which is unfortunately non conservative, i.e., optimistic. In this section the BPCS and SISs are considered as independent, and the demand (initiating event) is characterized by the average failure frequency of the BPCS control valve. It is not the case in Section 4 where the initiating event is characterized by the BPCS time-dependent failure frequency. In this condition a correct calculation of the HEF requires to take into account a systemic dependency between BPCS and SISs. To complete and reinforce the conclusions given in Sections 3 and 4, the proposed procedure is finally applied, in Section 5, to a system comprising three subsystems (a control system and two associated protection layers) clearly dependents. Finally a short conclusion ends this article.

It is worth noticing that numerical values allocated to all reliability parameters in this article are only proposed for illustration purpose. Moreover in the sequel, physical items (sytems and component) are labeled by right letters (A, B, …), while their failure are labeled by the correponding italic letters (*A*, *B*, …) and their good functioning by the same italic letters with an asterisk (A^*, B^*, …).

2. Probability and frequency calculations performed by using GbG and ABLA methods

2.1. Context

Two common practices devoted to the quantitative assessment of failure probabilities and failure frequencies performed by using fault tree model suffer from strong limitations and may seem formally erroneous, even if these practices sometimes provide rather good approximate numerical results. But it is worth noticing that these acceptable results are generally due to the predominant contribution of common cause failures (CCF) which mask the effects of the other contributions. The two methods previously mentioned are respectively known as *"Average Before Logic Approximation method"* (*ABLA*) and *"Gate-by-Gate method or technique"* (*GbG*).

The aim of this section is first to show that these two approaches are generally not able to give exact results, and second to explain where lie their respective weak points. The demonstration of the intrinsic limitations of the *ABLA* and *GbG*-approaches is made through their application to very simple examples, in order to focus mainly on the previously mentioned weak points, rather on a deep understanding of the functioning of the system under study. This system (S) is made up of three independent periodically tested components A, B and C and is operating if component A functions and at least one component among B and C functions. For sake of simplicity only a few reliability and mode of functioning parameters are taken into account:

- Only non detected failures are considered: λ_A = 1.5E-5 h^{-1}; λ_B = 1E-5 h^{-1}; λ_C = 2E-5 h^{-1}.
- Components A, B and C have the same test interval T = 1 year = 8760 h.
- The test duration and the restoration time required by these components are assumed negligible with regard to *T*.
- Once repaired the components are considered as good as new.

2.2. The Gate-by Gate fault tree method

This simple method is known and used for a long time. It is a "bottom-up" method described as follows in Center for Chemical Process Safety (CCPS) (2000):

> "The Gate-by-Gate technique starts with the basic events of the fault tree and proceeds upward toward the top-event. All inputs to a gate must be defined before calculating the gate output. All the bottom gates must be computed before proceeding to the next higher level".

The mathematical relationships used in the Gate-by-Gate technique are given in Table 1, where p_x and f_x stand respectively for the probability and the frequency of failure of item (component or system) X. The above failure frequency is also known as unconditional failure intensity $w_x(t)$ (Kumamoto & Henley, 1996), which is identical to the probability density function $f_x(t)$ of the time to failure of item X, when the latter is non repairable.

2.2.1. Probability calculations

The parameter of interest is the instantaneous unavailability $U_S(T)$ of system S at time *T*, which is obtained by applying the probability rules of Table 1 to the elementary fault tree models depicted hereafter.

The procedure inherent to the *GbG* method applied to the FT-model of Fig. 1a involves three steps. It starts with the definition of the input data of the first level-gates (the bottom-gates). They are the basic event probabilities (their unavailability at time *T* or their unreliability over [0, *T*]) which can be written as follows:

$$p_X(T) = U_X(T) = F_X(T) = 1 - \exp(-\lambda_X \cdot T), \quad \text{with X} = \text{A, B or C} \tag{1}$$

The probabilities of the intermediate events I_1 and I_2 are then calculated and are in turn used as the input data of the second level-gate, which is the top-gate. The output datum of the latter (and of the FT-model) is the value of the parameter of interest $U_S(T)$. The successive input data and the final output datum appear in Fig. 1a near each basic and intermediate event and the top-event. The same procedure is applied to the FT-model of Fig. 1b.

The results thus provided are different (2.99E-2 vs 2.85E-2) in spite of the fact that the two FT-models are equivalent (they have the same minimal cutsets) and correct. Then the key-point which can explain the above difference is the presence (see Fig. 1a) or the absence (see Fig. 1b) of repeated events (event *A*) within the examined FT-models. This hypothesis is confirmed by the detailed formulae dedicated to the probability calculations given in Table 1. They clearly show that the input events of any gate are assumed independent, but the input events (I_1 and I_2) of the top-gate are obviously dependent, because they share event *A*. So the *GBG* technique is not able to perform exactly the top-event probability of the FT-model depicted in Fig. 1a. Another way to claim that result provided by FT-model of Fig. 1b is the good one is to calculate the above probability via the minimal cutsets of this model as follows:

$$\begin{aligned} p_S(T) = U_S(T) = F_S(T) &= p(A \cdot B + A \cdot C) = p(A \cdot B + B^* \cdot A \cdot C) \\ &= p_A(T) \cdot p_B(T) + [1 - p_B(T))] \cdot p_A(T) \cdot p_C(T) \end{aligned} \tag{2}$$

Table 1
Rules for Gate-by-Gate fault tree calculation (Center for Chemical Process Safety (CCPS), 2000).

Gate	Input pairing	Calculation for output	Units
OR	p_A OR p_B	p(A OR B) = 1−(1−p_A)·(1−p_B) = p_A + p_B−p_A·p_B ≈ p_A + p_B	t^{-1}
	f_A OR f_B	f(A OR B) = f_A + f_B	
	p_A OR f_B	Not permitted	
AND	p_A AND p_B	p(A AND B) = p_A·p_B	t^{-1}
	f_A AND f_B	Unusual pairing, reform to f_A	
	f_A AND p_B	AND p_B f(A AND B) = f_A·p_B	