



Evaluation of the Performance of a Safety Instrumented System by the “Fault Tree” Method Using GRIF Software

Fateh Berrah^{1*}, Fares Innal²

¹ LRPCSI Laboratory of Skikda, University of 20Août 1955, Skikda 21000, Algeria,

Faculty of Technology, University of 20Août 1955, Skikda 21000, Algeria

² Automatic Laboratory of Skikda, University of 20Août 1955, Skikda 21000, Algeria

Corresponding Author Email: fberrah@univ-skikda.dz

ABSTRACT

Received: April 21st 2024

Accepted: April 23rd 2024

Published: June 30th 2024

Keywords:

Instrumented safety system, fault tree, Grif software (tree module), safety integrity.

This study aims to analyze the performance of an safety instrumented system operational in terms of safety integrity utilizing the "fault tree" method, it is one of the most common failure analysis techniques that reveals potential paths that lead to failure of systems or components. This occasional fire-fighting system contains multiple components, requiring careful consideration of different associated architectures. The quantitative analysis of the fault tree is conducted employing the Grif software to ensure high accuracy.

1. INTRODUCTION

Industrial development and modern industrial processes create different hazards for people, the environment, and assets, leading to significant accidents similar to those in Seveso, Bhopal, Toulouse, Feyzin, etc. Therefore, industrial operators are obligated to apply various safety measures. Among the most critical measures is the Safety Instrumented Systems (SIS), which generally constitutes the first layer of protection designed to control potentially dangerous deviations. For this reason, the performance verification of SIS, as defined in the IEC 61508 standard, is crucial to ensure that they meet a safety objective referred to as "Safety Integrity" or Safety Integrity Level (SIL). SIL is regarded as a parameter or measure of performance and confidence, demonstrating the level of assurance with which the SIS can be expected to achieve its intended safety function.

The performance of the Safety Instrumented System (SIS) is measured quantitatively based on its operating mode (Low demand, High demand, and continuous demand):

PFD_{avg} : is the average unavailability of an SIS for the low-demand mode.

PFH: is the average frequency of hazardous failure of an SIS for the high-demand or continuous-demand mode.

Markov Chain and Fault Tree are two well-known quantitative methods used to calculate these indicators. The Fault Tree Analysis (FTA), employed in this article, is a widely used engineering technique in safety and reliability studies. It includes two integrated parts to provide the probability of the occurrence of a desirable event: the first part involves graphical representation, and the second part entails mathematical treatment.

To facilitate the process and calculations, Grif is a software platform for system analysis and determining essential safety indicators.

2. SAFETY INSTRUMENTED SYSTEMS

2.1 Definition

A Safety Instrumented System (SIS) is a range of components guaranteeing the safe state of processes when predetermined conditions are fulfilled. According to the IEC 61508 standard, the SIS is an electrical/electronic/programmable electronic system related to safety applications [1]. According to the IEC 61511 standard, the SIS is a system to implement one or more Safety Instrumented Functions (SIF) [2]. A SIS is composed of any combination of sensor(s), logic solver, and final element(s), as represented in the following figure:

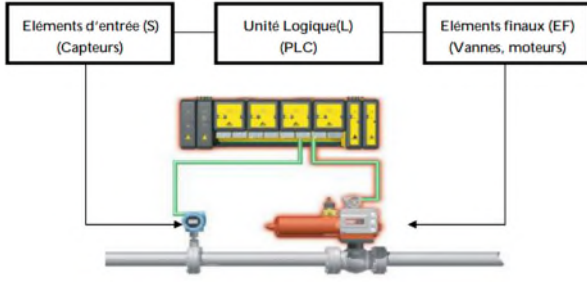


Figure. 1 Safety Instrumented System.[3]

The IEC 61508 standard sets the Safety Integrity Level (SIL), illustrating the ability of a Safety Instrumented System (SIS) to conduct required Safety Instrumented Functions (SIF) satisfactorily. The higher the SIL value, the greater the risk reduction. SIL is determined based on either PFDavg or PFH, as shown in the following Table :

Table 1. SIL Levels .[2]

SIL	Average Probability of Failure on Demand (PFDavg)	Failure Frequency per Hour (PFH)
1	$[10^{-2}, 10^{-1}]$	$[10^{-6}, 10^{-5}]$
2	$[10^{-3}, 10^{-2}]$	$[10^{-7}, 10^{-6}]$
3	$[10^{-4}, 10^{-3}]$	$[10^{-8}, 10^{-7}]$
4	$[10^{-5}, 10^{-4}]$	$[10^{-9}, 10^{-8}]$

2.2 SIS FAILURE

Two types of failures can affect a Safety Instrumented System (SIS) and lead to the loss of safety integrity: random failures and systematic failures. For the former, we have safe failures (λ_s) that occur in the absence of demand on the Safety Instrumented Function (SIF) and the latter (λ_d) that inhibit the SIF in case of demand.

Another classification partition or classification by detection: the first is detected failures (by online tests), and the second is undetected failures, performed at each period = T1. It represents the possibility of detecting failures by online tests through the Diagnostic Coverage factor (DC).

There are also Common Cause Failures (CCF), which result from one or more events causing the simultaneous failure of two or more channels. Various models are available to quantify the effects of CCF (λ_{ccf}), and the model employed by IEC 61508 is the β -factor model.

$$\begin{cases} \lambda_x = \lambda_{x_{ccf}} + \lambda_{x_{ind}} \\ \lambda_{x_{ccf}} = (1 - \beta_x) \cdot \lambda_x \\ \lambda_{x_{ind}} = \beta_x \cdot \lambda_x \end{cases} \quad (1)$$

All these failures can be summarized in the diagram shown in the following figure:

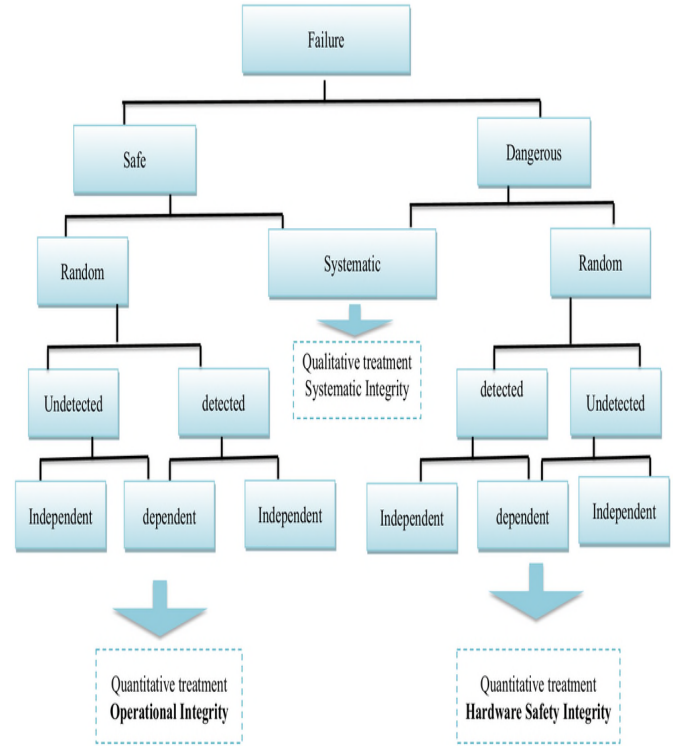


Figure. 2 SIS Failures Classification.[4;5]

As mentioned earlier, a SIS is composed of three subsystems in series, thus [6]:

$$PFD_{avg}^{sis} \approx PFD_S + PFD_{LS} + PFD_{FE} \quad (2)$$

$$PFH_{sis} \approx PFH_S + PFH_{LS} + PFH_{FE} \quad (3)$$

3. GRIF MODULE TREE

3.1 GRIF

The Grif tool is a software platform for system analysis that determines fundamental indicators of operational safety: reliability, availability, performance, and security. Grif was developed under the care of Total Energies and is the result of 40years of research and development [7].

Software consisting of 12 modules dedicated to calculations for operational safety; these modules are distributed among three packages:

- The simulation package includes the modules Pétri (Petri net), BStock (stochastic block diagrams), Petro (Block diagrams for Oil and gas systems), and Flux (utilized to model multi-flow diagrams with a user prototype created in Petri nets).
- The Markov package includes the Markov module (Markov graphs).
- The Boolean package consists of the modules tree (fault trees), BGiab (reliability block diagrams), ETree (event trees), SIL (instrumented safety loop modeling), Resede (reliability networks),

Bool (which links all Boolean approaches in the package), and the Risk module dedicated to risk. These modules are shown in figure 3

The Tree module permits modeling a system as a fault tree, providing a simple and cross-domain modeling approach through its Boolean logic. The Tree module relies on ALBIZIA, the calculation engine employing Binary Decision Diagrams (BDD) developed by Total Energies. ALBIZIA offers the advantage of performing precise analytical calculations and quickly providing comprehensive information about the system under study. You can easily draw the tree, input information, and get results efficiently.

3.2 Fault Tree

The Fault Tree Analysis (FTA) method was developed in 1962 to evaluate and enhance the Minuteman missile system [8], it is a well-known technique in reliability engineering and risk assessment that supports decision-making processes and the management of complex systems [9]. This method is based on deduction, which is employed for the predictive analysis of failures in physical systems. Using a distinctive graphical symbolism (For more information, it is recommended to refer to references [10] and [11]) permits the results to be presented in a tree-like arrangement. The main objective of this method is to identify combinations of events, i.e., component failures, starting from a predefined undesirable event (also called the top event, as it is placed at the highest level of the FTA).

This analysis permits hierarchical tracing of the potential causes of the undesirable event. It can extend down to essential events (the tree leaves). These primary events are independent and will not be decomposed into more straightforward elements due to a lack of information or interest or because it is impossible. Logical operators (AND, OR, etc.) establish connections between events.

This method is common in many fields and research such as [12;13;14]

Fault Tree Analysis (FTA) is primarily based on a minimal cut set, illustrating the smallest combination (logical intersection) of primary events that can lead to an undesirable event. Through quantitative analysis and based on the probabilities of occurrence of essential events, one can deduce the probability value of the occurrence of this undesirable event.

The following diagram is a guide for developing a fault tree. The idea is to determine all elementary causes that lead to the dreaded event.

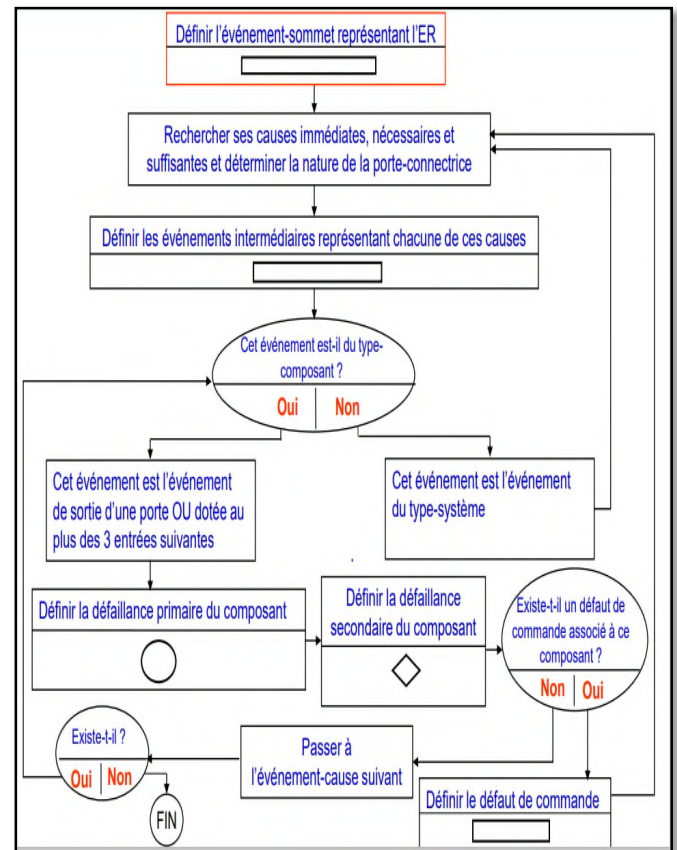


Figure. 4 Procedure for constructing a Fault Tree Analysis [11]



Figure. 3 The modules of GRIF software[7]

4. EXAMPLE OF APPLICATION

4.1 Presentation

We suggest studying a Safety Instrumented System that we consider a CO₂ fire suppression system designed to extinguish fires by rapidly reducing the oxygen content in the air to below 15% within seconds after receiving signals from detectors. A massive injection of CO₂ is provided by the initial discharge system into the machine compartments to reach the concentration necessary for extinguishment quickly. The extended discharge system maintains this concentration for a longer or shorter period, gradually raising additional amounts of CO₂.

The following diagram shows the components and operation method of the CO₂ fire extinguishing system:

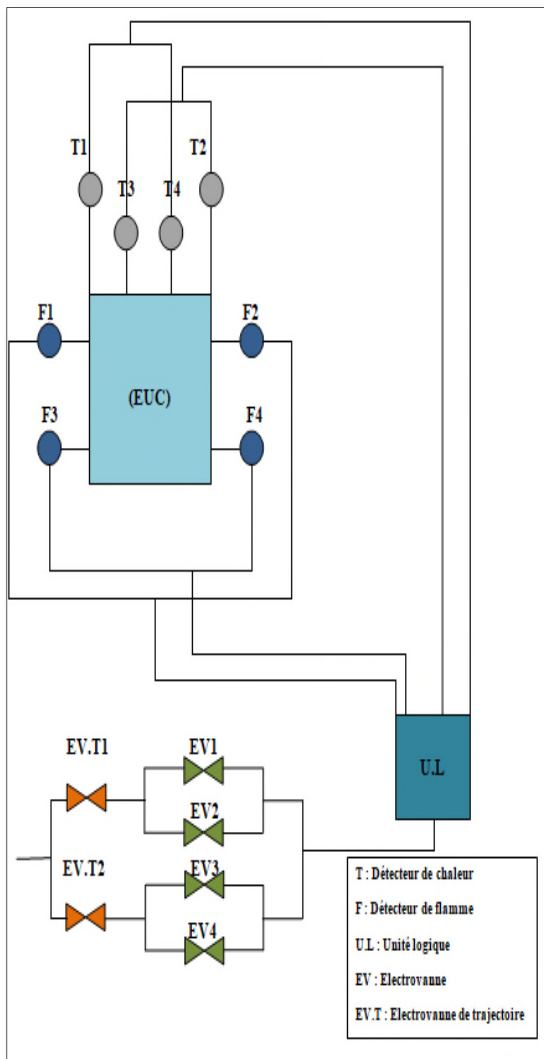


Figure. 4 Principle diagram of operation of the CO₂ fire fighting system

To simplify the concept, we suggest the decomposition of the Safety Instrumented System (SIS) in the form of a block diagram:

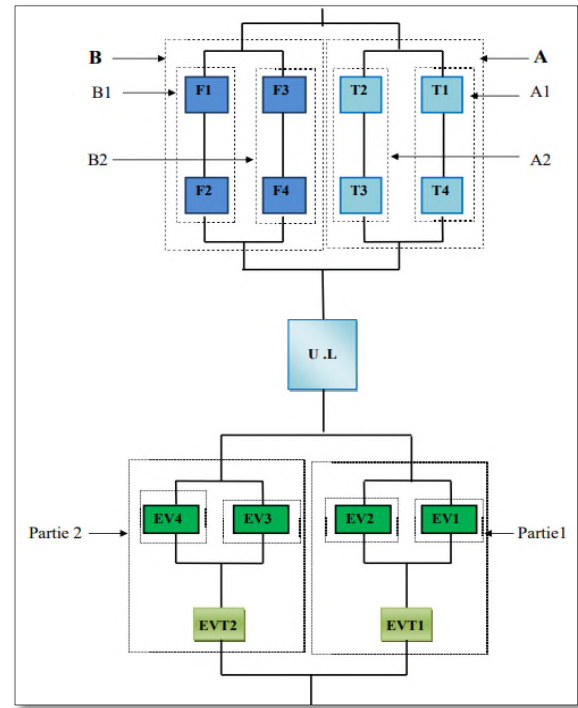


Figure. 5 Decomposition of (SIS) in the form of a block diagram

4.2 Arbre de défaillance du SIS (pour le module Tree)

To achieve this example, the following input data has been considered:

Table 2. Reliability parameters of fire-fighting system components

Parameters	λ_{DD} (10 ⁻⁶ h)	λ_{DU} (10 ⁻⁶ h)	MTTR (h)	T1 (h)	β
Heat Detector	0.4	0.6	8	8760	0.05
Optical Flame Detector	2.1	0.9	8	8760	0.05
Logic Unit (AFP-400)	0.9	0.003	8	8760	-
Solenoid Valve	0.39	0.91	8	8760	0.02

With :

$$\begin{cases} \lambda_x^{ccf} = \beta_x \cdot \lambda_x \\ \lambda_x^{ind} = (1 - \beta_x) \cdot \lambda_x \end{cases} \quad (3)$$

Table 3. The values of $\gamma\lambda^{ccf}$ et $\gamma\lambda^{ind}$ of the system components

Parameters	λ_{DD}^{CCF} (10 ⁻⁶ h)	λ_{DU}^{CCF} (10 ⁻⁶ h)	λ_{DD}^{IND} (h)	λ_{DU}^{IND} (h)
Heat Detector	0.02	0.03	0.38	0.57
Optical Flame Detector	0.105	0.045	1.995	0.855
Logic Unit (AFP-400)	-	-	0.9	0.009
Solenoid Valve	0.0078	0.0182	0.3822	0.8918

After creating the fault tree of the system studied, illustrated in Figure 5, we move on to the event configuration step, in this step, we introduced a heat detector as an example to demonstrate the event configuration method:

For independent failures:

Figure. 6 Configuration of heat detector T1 (Detected Failure)

Figure.7 Configuration of heat detector T1 (undetected Failure)

For common cause failures (CCF):

Figure. 8 Configuration of heat detector A (CCF detected failures)

Figure.9 Configuration of heat detector A (CCF undetected Failure)

Results :

The obtained results demonstrate that the PFD_{avg} of the CO2 fire fighting system is equal to $1,2065.10^{-4}$, corresponding to a real SIL of level 3. This is graphically illustrated in Figures 11 and 12.

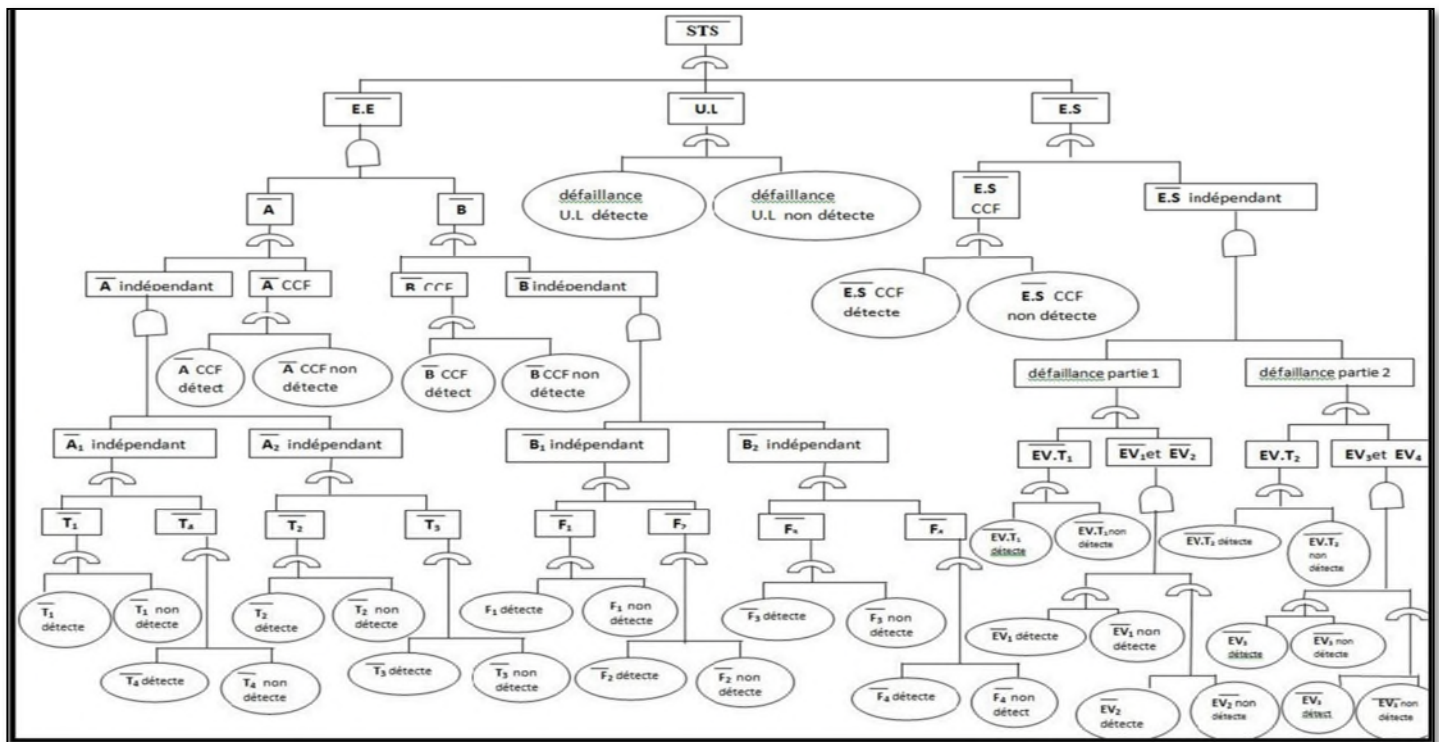


Figure. 10 The fault tree of the SIS

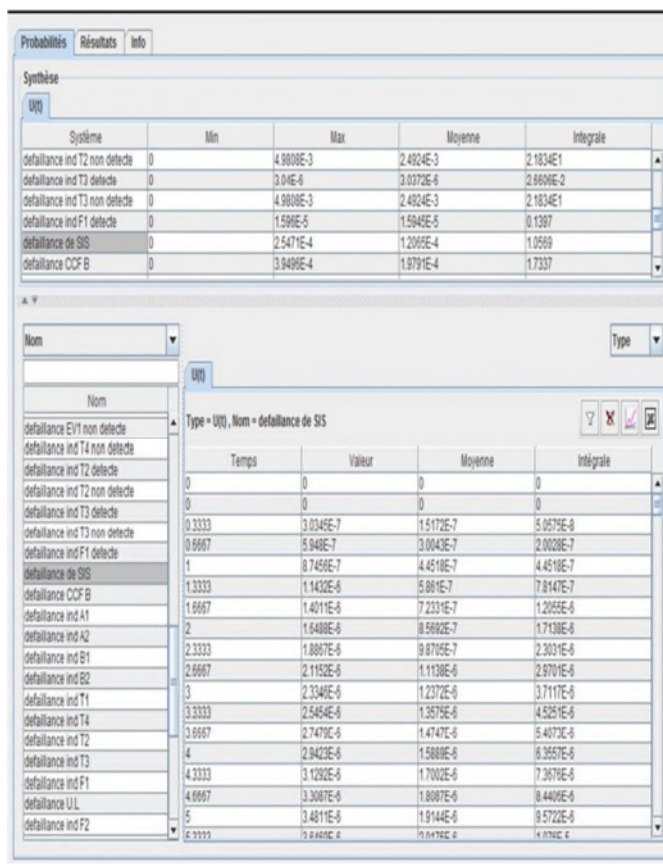


Figure. 11 PFD results

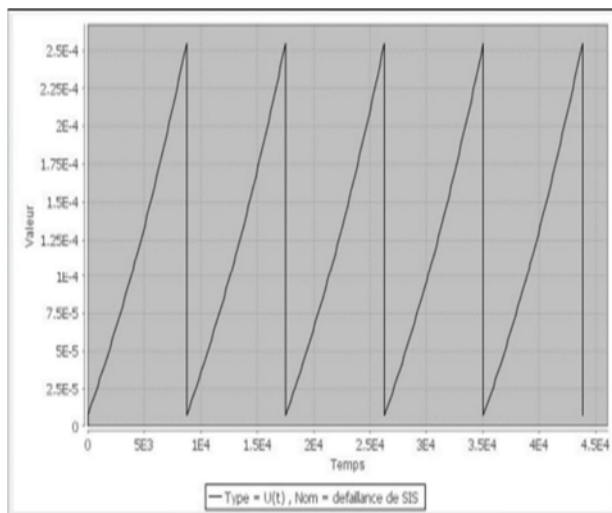


Figure. 12 PFD curve of fire fighting system

5. CONCLUSIONS

Ensuring a certain acceptable level of safety in industrial facilities requires the application of evolving measures to cope with the complexity of the systems involved and the dangerous substances that form the basis of most processes. Safety Instrumented Systems are a key solution in this context, taking various forms and objectives covering both prevention and protection. The use of such systems requires a careful assessment of their ability to ensure proper operation when needed and their ability to avoid causing significant disruptions.

This article is dedicated to measuring the safety integrity of a commonly employed Safety Instrumented System, which is a CO2 fire fighting system. Since such systems typically operate in low demand mode, its PFDavg has been estimated regarding the different parameters required by the IEC 61508 standard. This objective is addressed utilizing Fault Tree Analysis, which provides a flexible framework and is also familiar in the industrial community, assisting ensure the necessary interaction with these significant measures. This case study focuses on describing the various stages of modeling the hazardous behavior of Safety Instrumented Systems (SIS), which can be regarded as a first step toward the advanced incorporation of more dynamic and uncertain aspects.

REFERENCES

- [1] IEC61508, Functional safety of electrical/electronic/programmable electronic (e/e/pe) safety related systems. International Electrotechnical Commission(IEC),1998.
- [2] IEC61511, Functional safety: Safety instrumented systems for the process industry sector. International Electrotechnical Commission (IEC), 2000.
- [3] Innal, F., Contribution to the modeling of Safety Instrumented Systems and the evaluation of their performance: A critical analysis of IEC 61508 standard. (PhD thesis), University of Bordeaux I, France, 2008.
- [4] CHEBILA M. 2015. Modeling and evaluating the performance of safety instrumented systems with the consideration of the associated uncertainties. Ed. Hadj Lakhdar University, Batna.
- [5] Berrah, F., Chebila, M., Innal, F., Got, A. (2023). Cost effective analysis of the design of safety instrumented systems using Manta-Ray Foraging Optimization algorithm. International Journal of Safety and Security Engineering, Vol. 13, No. 6, pp. 975-986. <https://doi.org/10.18280/ijss.130601>
- [6] Innal, F., Dutuit, Y., Chebila, M. (2015). Safety and operational integrity evaluation and design optimization of safety instrumented systems. Reliability Engineering and System Safety, 134: 32-50. <https://doi.org/10.1016/j.res.2014.10.001>
- [7] <https://grif.totalenergies.com/en/about-grif/about-grif>

- [8] Clifton, E. (1999, August). Fault tree analysis-a history. In Proceedings of the 17th International Systems Safety Conference (pp. 1-9).
- [9] Pan, K., Liu, H., Gou, X., Huang, R., Ye, D., Wang, H., ... & Kong, J. (2022). Towards a systematic description of fault tree analysis studies using informetric mapping. *Sustainability*, 14(18), 11430.
- [10] Vesely, W. E., Goldberg, F. F., Roberts, N. H., & Haasl, D. F. (1981). *Fault tree handbook* (p. 0216). Washington, DC: Systems and Reliability Research, Office of Nuclear Regulatory Research, US Nuclear Regulatory Commission.
- [11] <https://www.yumpu.com/fr/document/read/65741118/add-grif-skikda>
- [12] Yazdi, M., Mohammadpour, J., Li, H., Huang, H. Z., Zarei, E., Pirbalouti, R. G., & Adumene, S. (2023). Fault tree analysis improvements: A bibliometric analysis and literature review. *Quality and Reliability Engineering International*, 39(5), 1639-1659.
- [13] Ong, N. A. F. M. N., Sadiq, M. A., Said, M. S. M., Jomaas, G., Tohir, M. Z. M., & Kristensen, J. S. (2022). Fault tree analysis of fires on rooftops with photovoltaic systems. *Journal of Building Engineering*, 46, 103752.
- [14] Qin, G., Li, R., Yang, M., Wang, B., Ni, P., & Wang, Y. (2024). Failure probability estimation of natural gas pipelines due to hydrogen embrittlement using an improved fuzzy fault tree approach. *Journal of Cleaner Production*, 141601.

NOMENCLATURE

CCF	common cause failures
CD	Diagnostic Coverage factor
FE	Final elements
FTA	Fault Tree Analysis
Grif	GRaphical Interface for reliability Forecasting
MTTR	Mean time to restoration
LS	Logic solver
PFD _{avg}	Average probability of failure on demand
PFD _{avg} ^{SIS}	SIS average PFD
PFH _{SIS}	SIS probability of dangerous failure per hour (average)
S	Sensor
T1	Proof tests interval
β	CCF proportion (β factor)
λ_x	X failure rate
λ_{xccf}	X failure rate (CCF)
$\lambda_{x\ ind}$	Independant x failure rate
λ_D	Dangerous failure rate
λ_D^{IND}	Independent dangerous failure rate
λ_D^{CCF}	Dependent dangerous failure rate (CCF)
λ_{DD}	DD failure rate
λ_{DD}^{IND}	Independent DD failure rate
λ_{DD}^{CCF}	Dependent DD failure rate
λ_{DU}	DU failure rate
λ_{DU}^{IND}	Independent DU failure rate
λ_{DU}^{CCF}	Dependent DU failure rate