Safety Lifecycle Of Safety Instrumented System

Case study: Diesel storage tank

Nabil Boudjoghra [(1)*], Fares Innal [(2)]
[(1)] LRPCSI Laboratory of Skikda, Department of Process Engineering, University of 20 Août 1955, Skikda, Algeria
[(2)] Institute of Applied Science and Techniques (ISTA), University of 20 Août 1955, Skikda, Algeria
[*] nabil.boudjoghra@univ-skikda.dz

Abstract: In this article, we explored the safety lifecycle of the Safety Instrumented System (SIS). First, we introduced the SIS, its Safety Instrumented Function (SIF), its Safety Integrity Level (SIL) and its Safety Lifecycle. Then, we illustrated the safety lifecycle stages of an SIS belonging to a boil-over risk safety system of diesel storage tank using engineering techniques and methods: HAZOP, LOPA, FTA, and SIF test scheduling, which interact with each other's data.

Keywords: Safety Instrumented System, SIS safety lifecycle, Boilover, HAZOP, LOPA, SIF proof testing

1. INTRODUCTION

Numerous risks that could endanger individuals, the environment, and company property are recognized to exist in the processing industry, particularly in the oil, gas, and chemical industries. This is because they use high-pressure procedures, combustible chemicals, and heavy machinery—all of which can quickly result in hazardous or even deadly accident. Consequently, it is essential for companies in these sectors to identify possible risks on the premises. These companies also need to design and implement adequate safeguards against these risks.

These safeguards, also known as Layers Of Protection (LOP), are independent layers that serve either to prevent an initiating event from becoming an accident or to mitigate the consequences of an accident once it occurs (Fig.1).

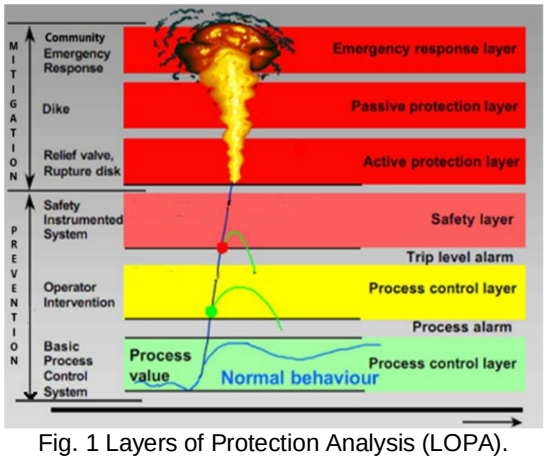

Fig. 1 Layers of Protection Analysis (LOPA).

The safety instrumented system (SIS) is the third layer of protection after the Basic Process Control System (BPCS) and the operator intervention, it serves to prevent the occurrence of the accident by controlling the process parameters (pressure, temperature, level, flow, etc.) when they are outside its normal ranges.

The SIS consists of three elements (Fig.2): sensors, logic solvers and final elements, the combination of which makes it possible to detect dangerous conditions and control them, ensuring a safe state.

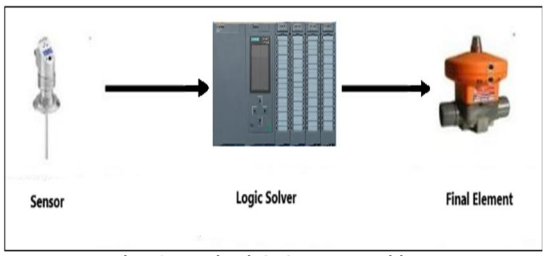

Fig. 2 Typical SIS composition.

IEC 61508 [1] is the most well-known international standard aimed at quantifying the safety probabilistic performance of Electrical/Electronic/Programmable Electronic (E/E/PE) control systems, including SIS, and introducing the concept of safety life cycle. The main objective of this standard is to minimize failures in all E/E/PE safety-related E/E/PE systems. This standard represents the cornerstone of a set of standards for specific fields, including the IEC615011 [2] standard designated for the

the industrial process field where it provides requirements for the specification, design, operation and maintenance of SIS.

Safety Integrity Level (SIL) is a measure of the level of risk reduction offered by a Safety Instrumented Function (SIF) that is carried out by a SIS in a given process. Stated differently, SIL is a measure of the performance of the SIF in terms of probability of failure on demand (PFD). The table below [1] shows the associated average Probability of Failure on Demand (PFDavg) and average Risk Reduction Factors (RRFavg) for each SIL.

Table 1 SIL according to PFDavg and RRF

SIL	PFD	RRF
SIL4	0.001% - 0.01%	100.000 - 10.000
SIL3	0.01% - 0.1%	10.000 - 1.000
SIL2	0.1% - 1%	1.000 - 100
SIL1	1% - 10%	100 - 10

Therefore, a higher SIL level corresponds to a higher level of safety, and a lower probability that a system will not operate. Processing plants usually only require SIL 1 and SIL 2. Since they necessitate a significant level of duplication, SIL 3 and SIL 4 are extremely uncommon and typically not cost-effective to implement.

Determining the SIL of a SIF requires calculating the overall PFD of the SIF. This SIL calculation process involves combining the failure rate data for each individual component of the SIF (i.e., sensors, logic solvers, and final elements). It also factors in considerations like test frequency, redundancy, and voting modalities.

The failure rate data for each component can be sourced from equipment manufacturers or generic databases. Even with access to this data, the overall SIL calculation remains a complex undertaking.

To understand how the SIL calculation fits into the broader context, we need to first comprehend the overarching Safety Lifecycle.

2. SAFETY INSTRUMENTED SYSTEM SAFETY LIFECYCLE

The IEC standards define a concept known as the "safety lifecycle". This is a cyclical process where all potential hazards are identified and thoroughly analyzed to determine which of these hazards require a SIS to be put in place for prevention [3].

The IEC 61511-1 presents the SIS safety life cycle as follow (Fig.3) [2]:

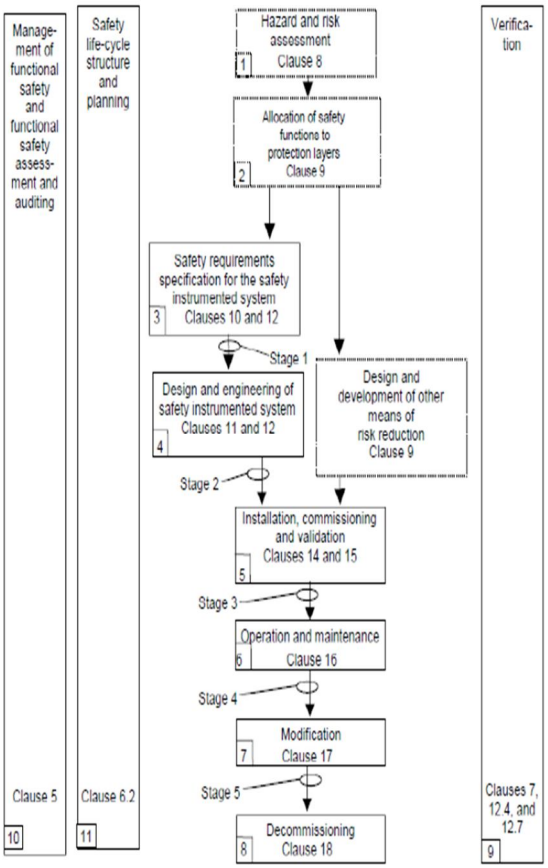

Fig. 3 SIS safety life cycle phases.

The SIS Safety Lifecycle can be outlined in a few steps to show where the SIL calculations fit in [3]:

1. First, identify the hazard and its frequency.

2. Determine if this frequency is acceptable (without SIS). If so, no SIS is needed, otherwise:

3. Determine the required SIL level of SIS by calculating the required PFD of each SIF. Determine the SIF's minimum PFD. This is the hazard's frequency (without SIS) divided by the acceptable frequency. When the minimum PFD is known, the SIF's required SIL level can be obtained from the Table 1.

4. Design an SIS so that each SIF has a PFD corresponding to the required SIL level.

The SIF's RRF can then be compared to the minimum required RRF (remember RRF = 1/PFD.). If greater than the minimum required RRF, the SIF is sufficient. Otherwise, the SIF must optimize.

The SIS Safety Lifecycle management based on different techniques and disciplines whitch interacts with each other (Fig.4), you can think of HAZOP (Hazard and operability studies) reports, LOPA (Layers of Protection Analysis) study reports, SIF design verification reports, SIF test procedures, and so on.

The entire SIS safety lifecycle is a loop, meaning that once additions or modifications are made to the original design, the previous study documents become obsolete and need to be revisited.

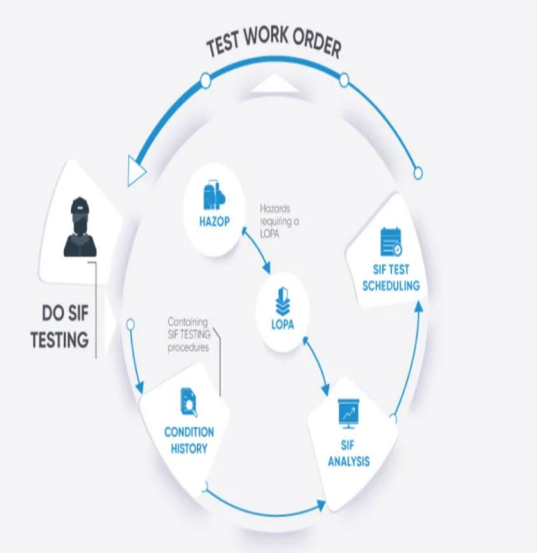

Fig. 4 Interaction between HAZOP, LOPA, SIF analyses and SIF testing for SIS safety life cycle management.

3. CASE STUDY

In this study, the facility in question is a diesel storage tank (Fig.5), located at condensate topping unit (Skikda refinery RA2K-Algeria).

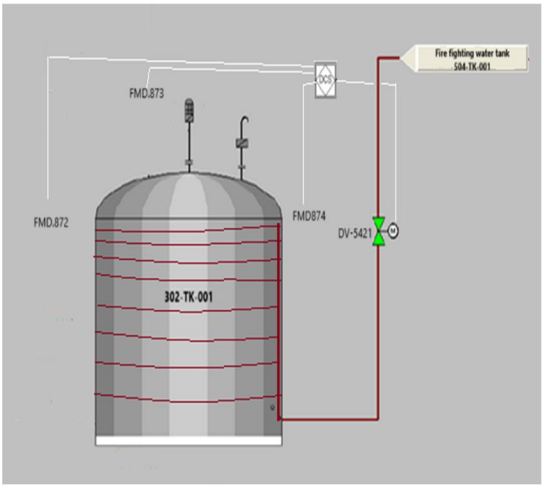

Fig. 5 302-TK-001 diesel storage tank.

The technical data of this tank and the diesel characteristics are presented in Tables 2 and Table 3 [4].

Table 2 The tank technical data

Item number	302-TK-001
Operating fluid	Diesel
Capacity	2316 m^3
Nominal height	12000 mm
Design temperature	65 C°
Design pressure	3500 Pa

Table 3 Diesel characteristics

Flash Point	>50 °C
Auto Inflammation Temp	≥ 250 °C
Lower Explosive Limit LEL	0,5 %
Upper Explosive Limit UEL	5 %
Boiling temp	150 – 380 °C
Kinematic viscosity	1,5 mm2/s à 40 °C
Solubility (in water)	4 à 5 mg/l
Density	820-860 kg/m3 à 15°C
Labeling	
Risk phrase	H225, H304, H315, H336, H361f, H373, H411

Hazard identification

The HAZOP analysis method allows to identify different potential accident scenarios resulting from process parameter deviations [5, 6, 7]. For our study we have chosen a possible deviation that can lead to catastrophic accidents (high temperature inside the diesel storage tank "Table 4").

Table 4 HAZOP analysis versus “high temperature in diesel storage tank” deviation

Deviation	Causes	Consequences	Protection barriers	Recommandations
High Temperaure	- Fire in or near the tank	- Dilation and weakening of the tank walls - Pool fire - **Boilover**	- Deluge system - Foam Spreading System - Emergency response system	- Verification of the safety barriers reliability

Our study is limited to one hazard whitch is "Boilover".

A. Boilover description

Phenomenon that may be encountered in the event of a fire in tanks of relatively viscous hydrocarbons (heavy fuel oil, diesel, domestic fuel oil) when water is present at the bottom of the tank.

In a fire situation, the hydrocarbon is gradually consumed and a heat wave forms in the rest of the tank. When the heat wave comes into contact with the layer of water at the bottom of the tank, it vaporizes instantly, forming a piston effect that violently projects the hydrocarbon upwards. A fireball forms, and flaming hydrocarbon spreads all around the tank. This phenomenon gives rise to thermal effects (see Fig. 6). Depending on the nature of the hydrocarbon involved, this phenomenon can be more or less violent (case of the RTE-Skikda accident in 2005) [8].

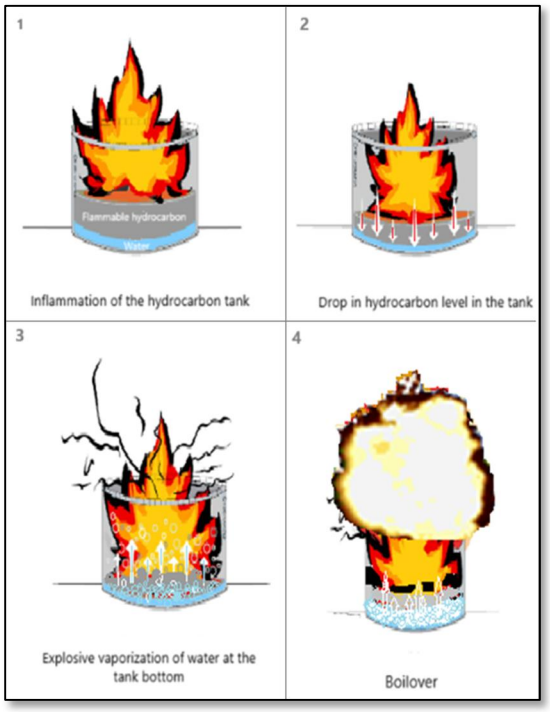

Fig. 6 The boilover mechanism.

Current research highlights two types of Boilover: The Boilover "Classic" and Boilover "thin layer". The two phenomena are quite similar in their sequence. The difference originates from the scope of the distillation range of the cut. The effects are much lower in the case of boil-over in thin layer [9].

Boilover occurrence frequency estimation

Using the LOPA method allows us to determine quantitative values regarding the frequency of accidents through the quantification of the frequencies of initiating events and the probabilities of failure on demand (PFD) of each layer of protection. It is based on data developed in the qualitative risk analysis (HAZOP study) [1, 10, 11].

$$f^c = f^{IE} \times \prod_i PFD_{avg}^i \quad (1)$$

- f^c: accident occurrence frequency.
- f^{IE}: initiating event occurrence frequency.
- PFD_{avg}^i : average probability of failure on demand of barrier i.

Table 5 Boilover initiating events

Initiating event	Description	Frequency
Fire on the tank roof	A fire is generated by off-specification diesel vapors coming into contact with an ignition source (e.g., lightning)	10^{-1}
Fire near the tank	A fire near the tank (e.g., pool fires, etc.)	10^{-1}
Presence of water in the tank	A layer of water at the tank bottom due to both the failure of the upstream process and the failure of the tank drainage system	10^{-1}

Table 6 Boilover security barriers

Security barrier	Description	PFD
Deluge system	Is an automatic tank cooling system (according to IEC61508 it is considered a low demand operating SIS whitch consist of three flames detectors (FMD-782, FMD783, FMD783), logic solver (DCS) and valve (DV-21))	10^{-1}
Foam Spreading System	is an automatic system for spreading foam on the tank roof in order to extinguish a possible roof fire (according to IEC61508, it is considered as a low demand SIS)	10^{-2}
Emergency response system	Is an organizational system for managing the intervention team and resources (it is modeled as an emergency response plan)	10^{-1}

It should be noted that the minimum combination generating a boilover initiating event is either a fire on the tank roof and the presence of water in the tank, or a fire near the tank and the presence of water in the tank. Therefore, the occurrence frequency of initiating events is calculated according to the following two rules [12]:

- The probability of occurrence of event E, if it can result from i OR j (independent) is the sum of the probabilities of occurrence of A and B reduced by their product; which can be formulated as follows:

$$P(e_i \cup e_j) = P(e_i) + P(e_j) - P(e_i) \times P(e_j) \quad (2)$$

- The probability of occurrence of event E, if it can result from i AND j (independent) is the product of the probabilities of occurrence of A and B; which can be formulated as follows:

$$P(e_i \cap e_j) = P(e_i) \times P(e_j) \quad (3)$$

$f^{IE} = (10^{-1} + 10^{-1} - 10^{-1} \times 10^{-1}) \times 10^{-1} = 1.9 \times 10^{-2}$/year

$f^{C} = 1.9 \times 10^{-2} \times 10^{-1} \times 10^{-2} \times 10^{-1} = 1.9 \times 10^{-5}$/year

Boilover occurrence frequency assessement

The hazard assessment is a process of comparing the results of the hazard estimation with the hazard criteria to determine whether the hasard is acceptable, tolerable or unacceptable [13]. In our study, the Boilover hazard is assessed according to RA2K criteria where its frequency is judged unacceptable. According to RA2K criteria, the boilover maximum tolerable frequency is: $f^{T} = 10^{-6}$/ year.

Boilover occurrence frequency reduction

Our approach reduces boilover risk via a Deluge-type SIS, with risk reduction dependent on its safety performance (PFDavg/SIL).

A. Determination of required SIL of SIS

The pre-established LOPA method allows us to determine quantitatively the required SIL by following these steps [14, 15]:

a) Calculation of accident frequency without the contribution of SIS ($f^{c}_{w/\,SIS}$).

$$f^{c}_{w/\,SIS} = \frac{f^{C}}{PFD_{SIS}} = 1.9 \times \frac{10^{-5}}{10^{-1}} = 1.9 \times 10^{-4}$$

b) The required PFD of SIS is determined by dividing the tolerable frequency by the frequency of accidents without SIS:

$$\frac{f^{T}}{f^{c}_{w/\,SIS}} = \frac{10^{-6}}{1.9 \times 10^{-4}} = 5.2 \times 10^{-3}$$

c) The required SIL of SIS is determined through the required PFD of SIS by referring to Table 1, it corresponds to an SIL2.

B. Calculation of the real SIL of SIS

In our case, the PFD of the studied SIS (works in low demand mode) is calculated by the Fault Tree Analysis (FTA) [15, 16, 17], using GRIF (Graphic Interactive for Reliability Forecasting) software (Fig.7) [18]. The reliability parameters of each SIS component are presented in Table 7.

Table 7. The reliability parameters of SIS component

Component	λ_DD (failures /h)	λ_DU (failures /h)	DC (%)	T_1 (h)	MTTR (h)	β (%)
Detectors (2oo3)	6.0×10^{-8}	4.0×10^{-8}	60 %	8,760	8	5 %
Logic Unit (1oo1)	4.5×10^{-8}	5.0×10^{-9}	90 %	8,760	8	0 %
Valve (1oo1)	3.5×10^{-6}	3.5×10^{-6}	50 %	8,760	8	0 %

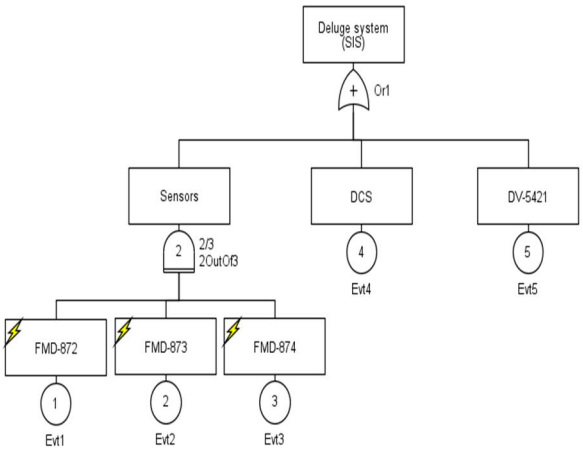

Fig. 7 Fault tree of SIS.

a) The real PFDavg of SIS is: PFDavg = 1.54E−2.

b) The real SIL of SIS is determined through the real PFDavg of SIS by referring to Table 1, it corresponds to an SIL1.

c) This value is greater than the target values (real SIL < required SIL).

d) The PFDavg can be reduced, among other things, by adding valve redundancy (1oo2 voting) with β = 5%, resulting in a new PFDavg of 1.09E−3. This value correspond to SIL2. Since the new real SIL equals the required SIL, the optimized SIS can ensure the necessary frequency reduction.

4. CONCLUSION

The main goal of safety instrumented systems is to make hazardous processes safe. Regretfully, failures can never be completely avoided and risks cannot be completely removed from the equation. That is why it is important to always consider possible disasters and implement reliable safeguards in place, so that, the occurrence frequency of these disasters is at a tolerable level.

In this article, we first discussed the Safety Instrumented System (SIS), its function (SIF), its Safety Integrity Level (SIL) and its safety lifecycle which consists of four stages. Then, we illustrated the safety lifecycle stages of SIS belongs to a boilover risk safety system of diesel storage tank using HAZOP, LOPA, Faulte Tree, and SIF proof testing, whitch interact with each other's data. It identified the risk of "Boilover" and proposed optimizing the reliability of the Deluge system by adding valve redundancy (1oo2 voting), thereby reducing the frequency of accidents to a tolerable level.

References

[1] INTERNATIONAL ELECTROTECHNICAL COMMISSION, "IEC 61508 : Functional safety of electrical/electronic/programmable electronic safety-related systems," IEC Standards Online, Geneva, 2010.

[2] INTERNATIONAL ELECTROTECHNICAL COMMISSION, "IEC 61511: Functional Safety-Safety instrumented systems for the process industry sector," IEC Standards Online, Geneva, 2003.

[3] BLOG "SIL calculation software – An overall introduction to standards and concepts," 16 October '24, from. https://cenosco.com/insights/sil.

[4] DNV GL France SARL, "Oil & Gas Quantitative Safety service," RA2K hazard study, Technical Document No: 1ZUAQSH-4, France, 2019.

[5] F. Crawley, M. Preston, and B.Tyler, "HAZOP: Guide to best practice, Guidelines to best practice for the process and chemical industries", Institution of Chemical Engineers, 2000,128 p.

[6] A. Desroches, A. Leroy, and F. Vallee, "La gestion des risques : principes et pratiques," Paris: Lavoisier, 2007, 295 p.

[7] M. Elamine, H. Mohamed, and M. Rouainia, "Improving Safety and Risk Management in High-Risk Industries: Focus on Safety Instrumented Systems (SIS) in the Oil and Gas Sector," *International Journal of Automation and Safety*, vol. 2, no. 1, pp. 15–18, June 2024.

[8] previnfo.net, "Risque industriel," from. https://www.previnfo.net/sections.php?op=printpage&artid=65&fbclid. Retrieved October 25. 2024.

[9] ARIA – Développement durable, "Boil over d'un bac de pétrole brut à Milford Haven (Royaume-Uni)," August 30. 1983, from. https://www.aria.developpementdurable.gouv.fr/wpcontent/files_mf/FD_6077_MilfordHaven_1983_fr.pdf.

[10] W. G. Bridges, A. M. Dowell, M. Gollin, W. A. Greenfield, J. M. Poulsen, and W. Turetzky, “Layer of protection analysis: simplified process risk assessment,” center for chemical process safety, American Institute for Chemical Engineers, New York, 2001.
[11] A. M. Dowell, “Layer of protection analysis: a New PHA Tool after Hazop, before Fault Tree Analysis,” International Conference and Workshop on Risk Analysis in ProcessSafety, pp. 21-24, October 1997.
[12] P. K. Suetin, A. I. Kostrikin, and Y. I. Manin, “Linear Algebra and Geometry,” CRC Press, 2021.
[13] Guide, ISO, 73: 2009, Risk management—Vocabulary, vol. 551, p. 49, 2009.
[14] N. Boudjoghra, and F. Innal, “Evaluation of Safety Instrumented System in a Natural Gas Facility According to IEC 61508 Standard,” International Journal of Safety and Security Engineering, vol. 13, no. 5, pp. 801-811, 2023. https://doi.org/10.18280/ijsse.130504.
[15] J. Day, H. Thomas, and J. VanOmmeren, “A case study of safety integrity level assessment and verification: Electronics division product line evaluation and analysis,” Process Safety Progress, vol. 27, no. 03, pp. 185-191, 2008.
[16] F. Berrah and F. Innal, “Evaluation of the Performance of a Safety Instrumented System by the ‘Fault Tree’ Method Using GRIF Software,” *International Journal of Automation and Safety*, vol. 2, no. 1, pp. 40–46, June 2024.
[17] S. Bouasla, E. Mechhoud, Y. Zennir, R. Bendib, and M. Rodriguez, “Evaluation of Safety Instrumented System in a Petroleum Plant and Its Impact on the Environment,” *Algerian Journal of Environmental Science and Technology*, vol. 9, no. 1, 2023.
[18] GRIF-Workshop, Graphical interface for reliability forecasting software, 2023, Available at : http://grif-workshop.com.