Improvements in the performance of an SIS by bypass reduction on the safety functions

Sklab Ramdane[(1)], Zennir Youcef[(2)], Bendib Riad[(3)]
[(1)] Université 20 Août 1955, LGCES Laboratory, Skikda, Algeria
[(2,3)]Université 20 Août 1955, Automatic Laboratory of Skikda, Skikda, Algeria
r.sklab@univ-skikda.dz ; y.zennir@univ-skikda.dz; r.bendib@univ-skikda.dz

Abstract: In order to maintain the integrity of its installation, the BIR EL MSANA (BMS) oil company has equipped itself with a safety instrumented system (SIS), complying with IEC 61508 and IEC 61511 standards. Whereas some constitutive functions of this system are disabled and not available, this means that the installations remains unprotected for a significant period of time, hence the obligation to look for adequate and permanent solutions. Through this work, we clarify the causes that led to this deactivation, proposing effective solutions for each case, this will allow reactivating them and ensuring a safe and sustainable exploitation.

Keywords: safety instrumented system, safety instrumented function, spurious activation, disabled

1. INTRODUCTION

.The technology of oil and gas production and processing is associated with considerable hazards. The mixture of petroleum and impurities is delivered from the reservoir through the wellheads and the gathering infrastructure to the processing facilities, where oil and gas are separated and prepared for further transportation to storage depots, refineries, and export to the end users. These processes are carried out on hazardous industrial facilities, where the occurrence of an incident may lead to significant economic losses, harm to personnel, environmental damage and other negative socio-political consequences. Proper design of processes and industrial instrumentation contributes significantly to the safety of operations on such hazardous facilities [6]. The international standard IEC 61511 [1] introduces the safety instrumented system as a protection layer or “barriers” aimed at reducing the risk, to which the hazardous facility is exposed .Spurious activation of the SIS is one of the most issue, which may lead to unwanted partial or full process shutdown. The spurious activation may be due to false process demands or SIS element failures. A false process demand is a demand that is erroneously treated as a real process demand, for example, a stray ray of sunlight that is mistakenly read as a fire by a flame detector. In the oil and gas industry, it is important to reduce the number of spurious activations to avoid unnecessary production loss [7], through this study we will deal with false triggering alarms related to crude oil storage system .In the aim of improving the safety instrumented system, by bypass reduction of the disabled safety functions due to their spurious activation, we propose in this paper an integration frame between the hazard and operability study (HAZOP) and safety integrity level (SIL), such that all the hazard related to the disabled safety functions is reviewed with the HAZOP study, and using Risk matrix and FTA the required safety level is also reviewed based on probability of failure under demand and the design of the corresponding disabled safety instrumented functions is reconsidered.

2. SAFETY INSTRUMENTED SYSTEMS (SIS)

System composed of sensors, logic solvers, and final control elements for the purpose of taking the process to a safe state when predetermined conditions are violated (see Figure 1). Other terms commonly used include Emergency Shutdown System (ESD, ESS), Safety Shutdown System (SSD), and Safety Interlock System. [3] .A SIS may perform several safety instrumented functions (SIF) and is sometimes referred to as a safety barrier or a protection layer [4]. Related SIFs may be combined into more comprehensive protection systems, like fire and gas detection systems and emergency shutdown systems.

2.1 Safety instrumented function

A safety instrumented function (SIF) is used to describe the safety functions implemented by instrumented technology. The SIS is the physical system implementing one or more SIFs. The SIF may be considered as a barrier function, while the SIS may be considered as a barrier system. The SIF usually performs the following actions or sub functions, detect process demands, decide what to do and act in order to bring the process back to a safe state. [8;15]

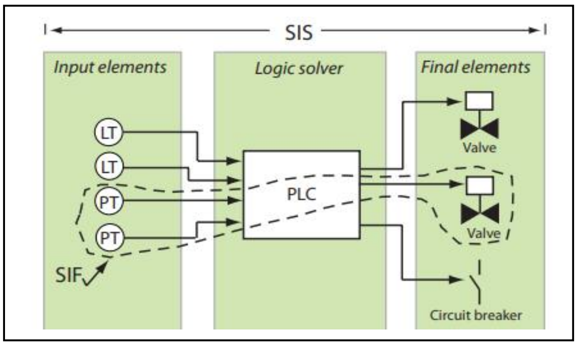

Fig. 1. Main parts of a safety instrumented system. [5]

2.2 Safety integrity level (SIL):

Discrete level(one out of four)for specifying the safety integrity requirements of the safety instrumented functions to be allocated to the safety instrumented systems. Safety integrity level 4 has the highest level of safety integrity, safety integrity level1 has the lowest [1].

Table. I. Safety integrity level.

	Probability of Failure on Demand (PFD)	Availability Required	Mean Time Between Failures (MTBF)
4	1.0E-5 ~ 1.0E-4	99.99% ~ 99.999%	10,000 ~ 100,000
3	1.0E-4 ~ 1.0E-3	99.90% ~ 99.99%	1,000 ~ 10,000
2	1.0E-3 ~ 1.0E-2	99.00 ~ 99.90%	100 ~ 1,000
1	1.0E-2 ~ 1.0E-1	90.00% ~ 99.00%	10 ~ 100

3. FAULT TREE ANALYSIS (FTA):

Quantitative risk assessment will be done in this paper by modelling the safety-instrumented functions using Fault Tree Analysis (FTA). Fault Tree Analysis was developed in the 1960 by Bell Laboratories in the United States. The military, the space program, and the nuclear industry have used FTA extensively. It is a highly adaptable logic diagram based technique that can be readily applied to the processes of the refining, petrochemical, chemical, oil and gas production, pipeline, pulp and paper, utility, nuclear, manufacturing and pharmaceutical industries. FTA was chosen, because it is a very structured, systematic, and rigorous technique that lends itself well to quantification. Is the best way to priorities the multitude of Potential hazards of loss production by determining numerically how much each cause contributed to the loss (safety of production) [5].

4. HAZARD AND OPERABILITY STUDY (HAZOP):

A HAZARD study is a highly disciplined procedure that identifies how a process may deviate from its design intent .it is defined as the application of a formal, systematic critical examination of the process and the engineering intentions of new or existing facilities to assess the malfunctioning potential of individual components of an equipment, and the consequential effects on the facility as a whole [9].but to reduce the chance that something is missed it must be done in a systematic way. The first step of HAZOP study is to identify system entities (elements) and their attributes by examining a description of the system under study. The description of the system may be of the physical or logical design, in the chemical industry for example, the system description may be a piping and instrumentation (P&I) diagram. For computer software it might be a data flow diagram, a state transition diagram, and so on. The next step, which is the core of the studies, is applying a number of predetermined ‘guide words' to an attribute of a system element to investigate possible deviations, and determining the possible causes and consequences of the deviations. A guideword is a word or phrase which expresses and defines a specific type of deviation. HAZOP study is a creative work, it is usually carried out by a team so that the members can stimulate each other and build upon each other's ideas [10]. In this paper the following documentation is used to review the HAZOP study for the crude oil storage system:

- Piping and instrumentation diagrams (P&ID) for installation.
- Philosophy or process description documentation.
- Existing operating and maintenance procedures.
- Cause and effect diagrams (C&E).
- Factory layout plans.

5. MAIN CONCEPTS OF SPURIOUS ACTIVATION:

Spurious activation is known under several different names in the literature, for example, spurious operation (SO), spurious trip, spurious stop, nuisance trip. There are three main types of spurious activation: (1) spurious activation of individual SIS elements,(2) spurious activation of a SIS (i.e., of a SIF), and (3) spurious shutdown of the process.

- **Spurious operation:** A SO is an activation of a SIS element without the presence of a specified process demand. Examples, a false signal about high level from a level transmitter due to an internal failure of the transmitter, or fail-safe-close safety valve due to leakage in the hydraulic circuit, a high level alarm from a level transmitter without the liquid level having exceeded the upper limit, due to failure to distinguish the foam from the real level of the liquid in the separator.
- **Spurious trip:** A spurious trip is activation of one or more SIS elements such that the SIS performs a SIF without the presence of a specified process demand. Examples, two flame detectors in a 2oo3 configuration give false signal about fire, causing the final elements of the SIF to be activated, or one out of two shutdown valves in a 1oo2 configuration of final elements closes prematurely due to an internal failure.
- **Spurious shutdown:** A spurious shutdown is a partial or full process shutdown without the presence of a specified process demand.

6. DESCRIPTION OF THE OIL STORAGE AND EXPEDITION SYSTEM:

- ***Storage system:***

The objective of this system is to store crude oil meeting the export specifications after treatment, it consists of three floating roof tanks 14-T-0-0101 / 02/03, each tank has a capacity of 3092 cubic meters, these tanks are used as follows

- The first tank: reception of crude oil responding to specifications (filling).
- The second: waiting (Settling).
- The third: crude oil shipment to haoudh el hamra. (Export).

The crude oil storage tanks are equipped with three level transmitters for each tank ,to monitor the level inside, two transmitters are Micropolitain M FMR245 radar type, which are directly connected to the instrumented safety system (SIS), represented by the Safety Manager, and the third transmitter is connected with the DCS represented by the Experion PKS system. The two transmitters connected to the safety instrumented system, one has a very high level alarm and the other a very low level alarm, these transmitters generate emergency stop actions as follows:

- The very high level (LHH) of liquid will stop the filling operation of the related tank and send the production to off spec tank.
- The very low level of liquid (LLL), will trigger the emergency stop of the oil shipping operation.

- ***Expedition system:***

The expedition system consists of three booster pumps 15-P-0-0101 / 02/03, and three expedition pumps 15-P-0-0201 / 02/03, the role of booster pumps is to ensure sufficient NPSH for expedition pumps.

- ***Issue (Spurious trip):***

The level transmitters related to crude oil tank give some time disturbing echoes, this generates false alarms and leads to unwanted spurious activation and production loss, which is not desirable, for that all SIFs connected to these transmitters are disabled and bypassed by operators most of while, this means that the installations remains unprotected for a significant period of time.

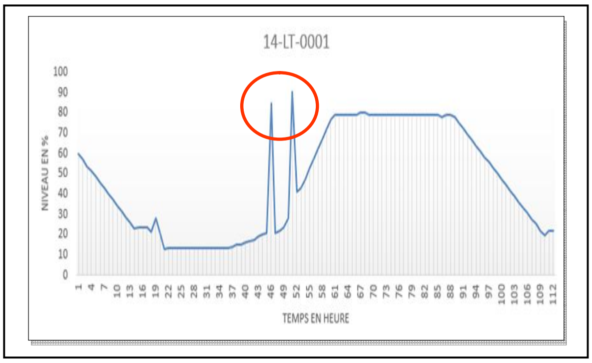

Fig.2. False alarm very high level of 14-LT-0001.

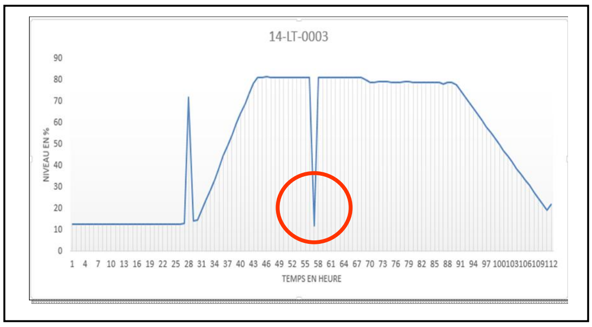

Fig.3. False alarm very low level of 14-LT-0003.

Table. II. Identification of the disabled interlocks and SIFs

Interlock	Réservoir	SIF	Description	Conséquences	SIF
I-1402	14-T-0-0101	14-LAHH-0001	High high level.	-Closing of valve 14-ESV-0001. - Shutdown of transfer pumps: 12-P-0-0201 and 15-P-0-0202.	Disabled
I-1405		14-LALL-0003	Low low level.	-Closing of valve 14-ESV-0002. -Stooping booster pumps: 15-P-0-0101 / 102/103 -Stopping of shipping pumps: 15-P-0-0201 / 0202/0203	Disabled
I-1403	14-T-0-0102	14-LAHH-0005	High high level	-Closing of valve 14-ESV-0003. - Shutdown of transfer pumps: 12-P-0-0201 and 15-P-0-0202.	Disabled
I-1406		14-LALL-0003	Low low level.	-Closing of valve 14-ESV-0004. -Stooping booster pumps: 15-P-0-0101 / 102/103 -Stopping of shipping pumps: 15-P-0-0201 / 0202/0203	Disabled
I-1404	14-T-0-0103	14-LAHH-0013	High high level.	-Closing of valve 14-ESV-0005. - Shutdown of transfer pumps: 12-P-0-0201 and 15-P-0-0202.	Disabled
I-1407		14-LALL-0008	Low low level.	-Closing of valve 14-ESV-0006. -Stooping booster pumps: 15-P-0-0101 / 102/103 -Stopping of shipping pumps: 15-P-0-0201 / 0202/0203	Disabled

- ***Identification of the disabled interlocks and SIF:***

The three storage tanks are equipped with a security system consisting of several interlocks and safety instrumented functions, which are as follows:

TABLE.3. Application of the HAZOP method for crude oil storage system related to level.

parameter	Deviation	Causes	Consequences	Prevention et Protection	Recommendations
Level	High level	- Penetration of rainwater through the floating roof - Sudden increase of filling flow. - The valves of the filling lines are not waterproof when they are in close position. - Failure of the level indicator or false indication. - Operation error (Sending crude oil to an already filled tank).	- Overflow and flood the floating roof of the tank. - Overflow of the product and possibility of a fire. - Possibility of explosion if the flooded crude contains gas. - Surrounding environment pollution.	- Switching system between the three tanks. - Level indication 14-LI-0002. - Level indication 14-LI-0001. - Alarm DCS 14-LAH-0002. - Alarm high high (Trip) 14-LAHH-0001. - Presence of fire and gas detectors.	- Periodic verification of measuring instruments, indicators and alarms. - Addition of a local indication at the foot of the tank. - Remove the bypass of the high-level LAHH interlock.
	Low level	- Failure of the level indicator or false indication. - Important leak from the drain valve. - Important leak in the filling line (pipe, vanne, pump…). -Important leak in the expedition line. - Sudden increase in crude oil extraction by booster pumps and shipping pumps.	- Disturbance of the expedition operation. - Booster pumps and shipping pumps work with great cavitation. - Degradation of booster pumps and shipments pumps. - Implosion of the storage tank.	- Level indication 14-LI-0002. - Level indication 14-LI-0003. - Alarm DCS 14-LAL-0002. - Alarm low low level (Trip) 14-LALL-0003.	- Periodic verification of measuring instruments, indicators and alarms. - Addition of a local indication at the foot of the tank - Remove the bypass of the high-level LAHH interlock.

An overview of disabled instrumented safety function as shown by DCS screen for 14-T-0-0101 tank is shown in Fig. 4.

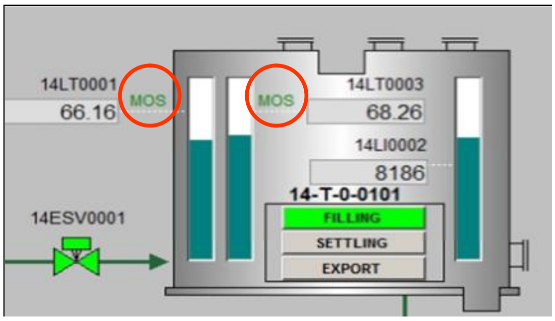

Fig.4. An overview of disabled instrument safety function.

7. APPLICATION OF THE HAZOP METHOD:

The HAZOP method is applied taking into account the divergences of the level tank, and considering the causes , the consequences for each diversion and the existing correction actions, the table below summarizes the application of HAZOP for a single tank, which is then generalized to the remaining tank [12-14].

The major recommendation after the application of the HAZOP method is to remove the bypass of the safety instrumented functions that is why a SIL study is required to propose the best solution.

8. SIL STUDY REVIEW FOR CRUDE OIL STORAGE AND EXPEDITION SYSTEM (FOR DISABLED SIFS):

The classification of SIL using risk matrix (example I-1402) are illustrated in the following table:

TABLE.4. Classification of SIL using risk matrix.

SIL classification for I-1402			
The consequences related to personnel health and safety			
S-value	S4	S-justification	Risk of injury and burns to personnel in the event of a fire or explosion
p-value	P2	P-justification	Possibility of escape in certain circumstances.
F-value	F2	F-justification	Occasional place.
S-reduction	-1	MOD-S-value	
D-value	D2	D-justification	to the existing of protection layers
SIL risk :	SIL : 2		

TABLE.5. Classification of SIL using risk matrix (Economic Risk).

Economic Risk:			
L-value	L5	L-justification	Stopping the process unit for a long time due to process disturbance. Débordement et Perte des quantités importante de brut
D-Eco-value	D2	D-Eco-justification	Overflow and loss of large quantities of crude oil
SIL economic:		SIL : 3	

TABLE.6. Classification of SIL using risk matrix (Environment Risk).

Environment Risk:			
E-value:	E1	E-justification	Effect on the local environment within the fence boundary, negligible financial consequence
D-env. Value :	D2	D-env. Justification	Considering the existing of protection layers
SIL environnement			SIL : A1

SIL classification: The overall SIL classification (the maximum SIL for the three consequences) = 3.

8.1. Calculation of PFDavg for interlock I 1402:

In this part, the PFD is used to calculate the corresponding SIL level for each instrumented safety function related to the storage tank level, this SIL is called the calculated SIL. The results are compared with those deduced from the risk matrix.

The recommendations and modifications for each SIF are recorded based on two cases:

Case 1: If the required SIL is small or equal to the calculated SIL therefore no modification necessary since the existing SIS provides more security than required.

Case 2: If the required SIL is greater than the calculated SIL then a change is needed for the SIF.

In our case the values of the PFD used for the different components of SIF's, are illustrated in the table below.

Table.7. PFD values for different SIF components [11].

Initiator		**Logic solver**	
Type	PFD	Type	PFD
Level transmitter	Simple 2.5411 E-2	Safety Manager	2.126 E-5
	Voting 2oo2 1.1711 E-4		
	Voting 2oo3 6.0662 E-5		

Final element		
Electro valve	Valve	contactor
4.7 E-7	On-off valve 1.344 E-4	1.3 E-4

The FTA methods with PFD value are illustrated in the following figures :

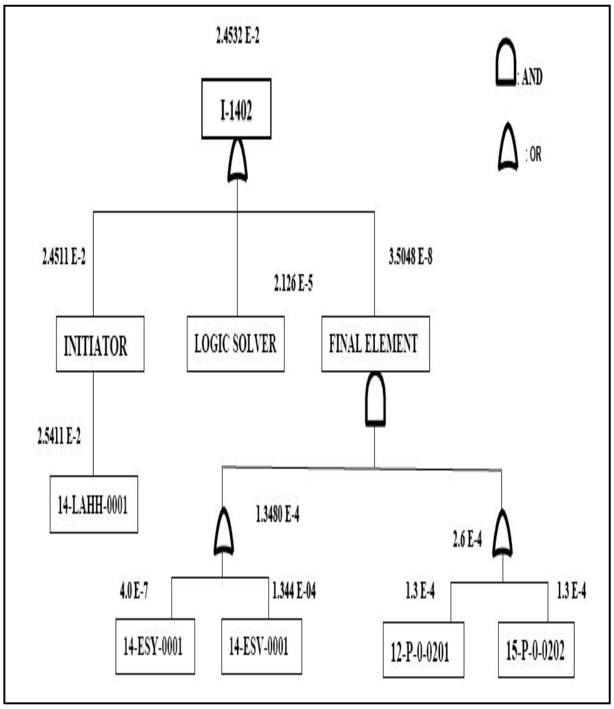

Fig.5. FTA methods with PFD value of different SIF components .

Overview on the FTA method which was applied to tank 14-T-0-0101, interlocks I-1402:

The average PFD for this SIF (I-1402) is 2.4532 E-02 which correspond to a SIL value =2, however and as it is described in the above section the target SIL equal to 3, then new design modification on the SIF component is required. The results are summarized in the table below for all mentioned interlocks.

TABLE .8. Summarized results of SIL Target and SIL cal for all disabled SIFs before modification.

Interlock	Sil Target (risk matrix)	SIL cal (using FTA)	Recommandations
I-1402 ; I-1403 ; I-1405 ; I-1406	3	2	Use sensors voting

The FTA method applied to tank 14-T-0-0101, interlocks I-1402 is illustrated by the following figure:

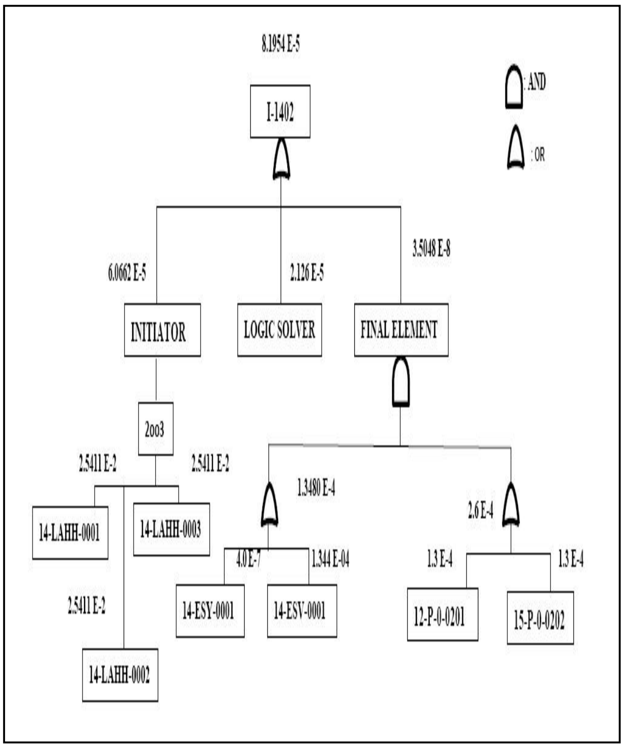

Fig.6. FTA method applied to tank 14-T-0-0101, interlocks I-1402.

8.3. Design modification on the disabled SIFs component (ex: I-1402 using 2oo3 voting):

After the calculation of SIL by several Voting architecture for disabled SIFs, below the results summary:

TABLE .9. Results of SIL Target and SIL cal for all disabled SIFs with several voting architecture

Interlock	SIL Target	PFD 1oo1 voting	SIL cal 1oo1 voting
I-1402	3	2.4532 E-2	SIL 2
I-1405	3	2.5432 E-2	SIL 2
I-1403	3	2.4532 E-2	SIL 2
I-1406	3	2.5432 E-2	SIL 2
I-1404	3	2.4532 E-2	SIL 2
I-1407	3	2.5432 E-2	SIL 2

TABLE .10. Results of SIL Target and SIL cal for all disabled SIFs with several voting architecture

PFD 2oo2 voting	SIL cal 2oo2 voting	PFD 2oo3 voting	SIL cal 2oo3 voting
1.3840 E-4	SIL 3	8.1954 E-5	SIL 3
1.3837 E-4	SIL 3	2.7326 E-5	SIL 3
1.3840 E-4	SIL 3	8.1954 E-5	SIL 3
1.3837 E-4	SIL 3	2.7326 E-5	SIL 3
1.3840 E-4	SIL 3	8.1954 E-5	SIL 3
1.3837 E-4	SIL 3	2.7326 E-5	SIL 3

The following figure shows the overview of the voting 2oo3 implementation on safety manager SIS controller.

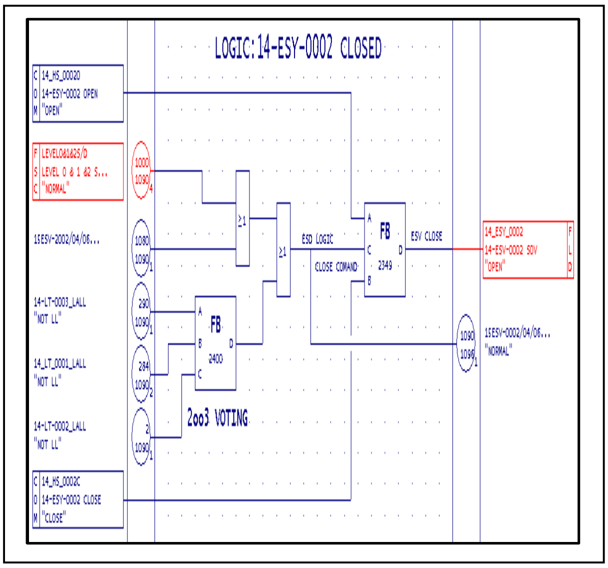

Fig. 7. An overview of the voting 2oo3 implementation on safety manager SIS controller.

9. CONCLUSION:

By carrying out a SIL study on different disabled SIFs (I-1402, I-1405, I-1403, I-1406, I-1404, I-1407,) we deduce that:

- The use of a single level transmitter (1001 voting) does not achieve the SIL required by the risk matrix of each loop.
- The use of a two level transmitters (2oo2 voting) achieve the SIL required by the risk matrix of each loop.
- The use of three level transmitters (2oo3 voting) achieve the SIL required by the risk matrix of each loop.

Based on the results obtained, we recommend using the 2oo3 voting architecture for the following reasons:

- It offers a much lower PFD compared to that of the 2oo2 architecture.
- It offers better availability for the instrumented safety function.
- The on-site existence of transmitters means no investment in the purchase or installation of new transmitters.

References

[1] International Electrotechnical Commission (IEC), “61511 Functional safety – safety instrumented system for the process industry sector”, IEC, Geneva, Switzerland, 2003, p.175.

[2] Mary Ann Lundteigen, “Safety instrumented systems in the oil and gas industry: Concepts and methods for safety and reliability assessments in design and operation”, PhD thesis, January 2008.

[3] ANSI/ISA-s84.01-1996, “Application of safety instrumented systems for the process industries.”, International Society of Automation (ISA) , March 11, 1997.

[4] Marvin Rausand, Mary Ann Lundteigen. “Common cause failures in safety instrumented systems on oil and gas installations: Implementing defense measures through function testing”. Journal of Loss Prevention in the Process Industries, Volume 20, p. 218 – 229

[5] BENDIB Riad, BENTARZI Hamid, ZENNIR Youcef , RACHID Hind. “Design Of an integration Frame HAZOP-SIL for safety Optimization of a Fired Heater” International Conference on Technological Advances in Electrical Engineering (ICTAEE’16.), October 2016, pp.6.

[6] Yury Redutskiy,”optimization of safety instrumented system design and maintenance frequency for oil and gas industry process”, Management and Production Engineering Review, Vol.8, N.1, 2017, pp. 46–59.

[7] Mary Ann Lundteigen , Marvin Rausand, “Spurious activation of safety instrumented systems in the oil and gas industry: Basic concepts and formulas. Reliability Engineering and System Safety”, Vol.93, 2008, pp.1208–1217.

[8] S. Sklet, "Safety barriers: Definitions, classification and performance", Journal of Loss Prevention in the process industries, Volume 19, Issue 5, 2006, pp.494-506.

[9] El-Arkam MECHHOUD ,Manuel RODRIGUEZ, Youcef ZENNIR, "Automated dependability analysis of the HDPE reactor using D-higraphs HAZOP assistant", Algerian Journal of Signal and Systems (AJSS), vol.2, issue 4, 2017, pp 255-265.

[10] Sunwoo Kim John A. Clark John A. McDermid "The Rigorous Generation of Java Mutation Operators Using HAZOP" University of York, Heslington, York YO10 5DD, United Kingdom, 1999, pp 2-3.

[11] BIR EL MSANA field development project," safety integrity level (SIL) verification report" prepared for HYUNDAI engineering Co, Ltd by ABSG Consulting Inc. august 2013.

[12] Jordi.D; Vasilis.F; Juan.A; Josep.A" Hazard and operability analysis a literature review", Journal of Hazardous Materials, vol.173,2010,pp.19–32.

[13] H.G. Lawley, Operability studies and hazard analysis, Chemical Engineering Progress, vol. 70, N° 4, 1974, pp.45–56.

[14] D.P. Nolan, Application of HAZOP and What-if Safety Reviews to the Petroleum, Petrochemical and Chemical Industries, Noyes Publications, New Jersey, 1994.

[15] P. Stavrianidis, K. Bhimavarapu, Safety instrumented functions and safety integrity levels (SIL), ISA Transactions, 37 (1998) 337–351.