International Journal of Emerging Engineering Research and Technology
Volume 2, Issue 4, July 2014, PP 374-382
ISSN 2349-4395 (Print) & ISSN 2349-4409 (Online)

An Approach towards Safety Using Safety Instrumented Systems: A Case Study

Vivek Kadam[1], Sharad Jadhav[2], Mahesh Parihar[3]

[1] Department of Instrumentation Engg, R.A.I.T, Navi Mumbai, India

Abstract: *In industrial globalization "safety" is emerging as most noticing and valued factor. The main intention of this design of safety systems is to avoid unexpected accidents and to achieve reduction in dangerous environment according to health and property risk. The different safety functions considered to increase the relative safety of the plant are combinable and all together named as safety instrumented system. These systems works in response to its inputs, when pre-included the safety functions fails which includes operator faults, system hardware failures and environmental changes. This paper is focused on these systems. This paper will introduce you different concepts related to safety analysis like safety life cycle model, ALARP principle, LOPA concept, probability of failure on demand (pfd) and mean time to failure (MTTF) along with small review of safety standards iec61508 and IEC 61511. After a preliminary introduction of the SIL (safety integrity level) concept in accordance with iec61508 / iec61511, a case study concerning the evaluation of both the mean time to failure (MTTF) and the probability of failure on demand (pfd) to select an appropriate SIL for a basic process safety control system for a tank is considered.*

Keywords: *Safety instrumented system, Safety Integrity Level, IEC 61508/IEC61511, As low as reasonably Practicable (ALARP).*

1. Introduction

In the edge of emerging technologies in each and every discipline of the worldwide engineering environment, the complexity of system is increased in huge manner so to handle this growing challenge, all engineers and research technicians have to involve in process engineering and to be aware of the complexities of designing and operating safety-related systems [13]. The reason is industrial hazards and safety. This is because industries run many different continuous and batch processes involving different raw materials, processing waste, bi-products and final products with desired requirement. While operating these process plants, different hazards can be encountered such as fire, explosion, toxic release and environmental damage. These considered as four principle hazards.

Safety Instrumented Systems (SIS) always plays a major role to provide a protective layer functionality in many industrial engineering process and automated systems. It's not false to say SIS is the method to apply a safety function for a process in order to observe and maintain the safety level of any instrument/equipment under its control in response to hazardous change in process cycle or routine, as suggested by the IEC61508 and IEC61511 standards. These standards help to identify the mandatory safety functions, direct to establish their applicable SIL and demand to implement them on a SIS to achieve the desired safety level for the process [5]. These are the objectives behind the standards. SIL represents static range of the Integral safety of an SIS at the time of process demand. It is considered as basic building block of acceptable SIS design and includes the Factors like Device integrity, Diagnostics, Systematic and common cause failures, Testing, Operation and Maintenance etc [14]. SILs can be defined in terms of the probability of failure on demand (PFD) and risk reduction factor (RRF) and can be determined by PHA process like Layer of Protection analysis or different qualitative and quantitative SIL determination methods.

2. Safety Standards and Life Cycle Model

2.1 Safety Standards:

The process industries have been now acknowledging the importance of the safety-critical and safety-related digital systems in engineering mainstream over the last few years. A "standard" is a document, design and developed by respective authority that provides rules, guidelines for functional activities for their desired outcome. These standards can helps to define terms accordingly to avoid misunderstanding among the users. The "International Electro technical Commission" (IEC) is the organisation who develops and sets international standards in technological engineering fields. In 1997 the IEC published standard IEC61508, "Functional safety of electrical/electronic/programmable electronic safety-related systems". These standards have significant practical importance in the design and operation of the E/E/PE safety systems in technical systems and hazardous installations. In further few years IEC introduced the next standards as IEC61511 "Functional Safety: Safety Instrumented Systems for the Process Industry Sector" and as mentioned these modified standards gives minimum acceptable requirement criteria for design and installation of safety instrumented systems (SIS) for the process industries [18] [19] [20].

2.2 Life Cycle model:

The base of IEC61508 is the safety life-cycle model, which specifies the pre-structured and accountable planning of safety related systems from first conceptual step to eventual decommissioning of the plant at end. From the beginning to end of the SIS, IEC uses the safety life cycle as Frame work in order to fulfil the criteria relating to analysis, specification, design, installation, operation, maintenance, modification (if suggested) and de-commissioning of safety instrumented system [13]. Sometimes it may disadvantageous that performing all of the steps in the life cycle, like all other tasks designed will increase overall costs and result in lower productivity. So the life cycle model is summarized in three simple steps shown in figure 1 [17].

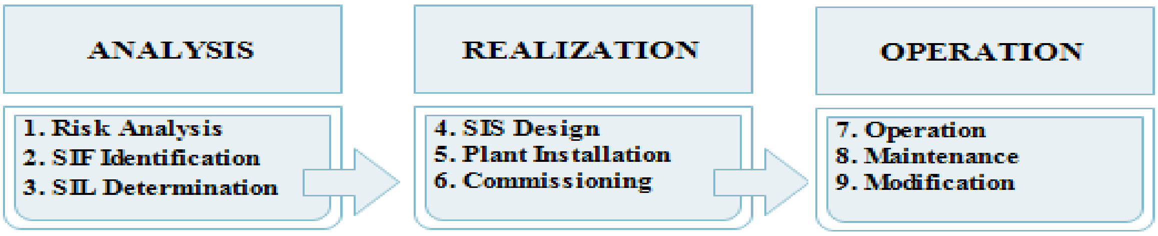


Figure 1. *Simplified Block Diagram of Safety Life Cycle*

2.3 Simplified Steps in Developing Safety System:

1. Formulate the conceptual design of the process and define the overall scope.
2. Identify process hazards and risks via a hazard analysis and risk assessment.
3. Identity non-SIS layers of protection.
4. Determine the need for additional protection i.e. SIS. Where a SIS is identified as being required?
5. Determine the target SIL.
6. Develop safety requirement specification (SRS).
7. Develop SIS conceptual designs to meet SRS.
8. Develop detailed SIS design.
9. Install the SIS in the system.
10. Perform Commissioning and pre-start-up testing.
11. Develop operation and maintenance procedures.
12. Conduct pre-start-up safety review.

13. Carry out operation and maintenance of SIS.
14. Record results and re-assess any modification due to non compliance of expected result.
15. Carry out de-commissioning procedures at the end of the life of the SIS [13].

3. Safety Analysis

3.1 ALARP Concept:

ALARP means “As Low as Reasonably Practicable” for risk. The ALARP principle simply says that the residual risk shall be at its minimum practicable level. Hazard evaluation is based on application of this well known ALARP principle that distinguishes given areas of risks. [15] [16].

- Unacceptable region (Intolerable risk).
- Region of undesirable risk.
- Broadly acceptable region (tolerable risk).
- Region of negligible risk.

3.2 Layers of Protection and its Analysis:

LOPA provides different layers to achieve the minimum risk in hazardous scenarios and comparing it with risk reduction criteria to decide if existing safety layers are precise or some additional layers are needed. LOPA extends the concept of process hazards analysis (PHA). Process design engineers use a no. of protection layers, to maintain safety against catastrophic failures & hazardous accidents. These layers are nothing but consist of devices, systems or preventive actions that are capable of preventing mal operation. Ideally such protection layers should be independent from one another so that if anyone fails then next one will perform its function regardless of the previous one, when they satisfies the criterion they called as Independent protection layers. LOPA includes the safety layers that are IPLs and SIS is one of them. LOPA helps to decide risk reduction up to an acceptable level and which protection layers should be applicable [12] [15]. Figure 2 is general representation if safety layers often referred to as “onion diagram”. [17].

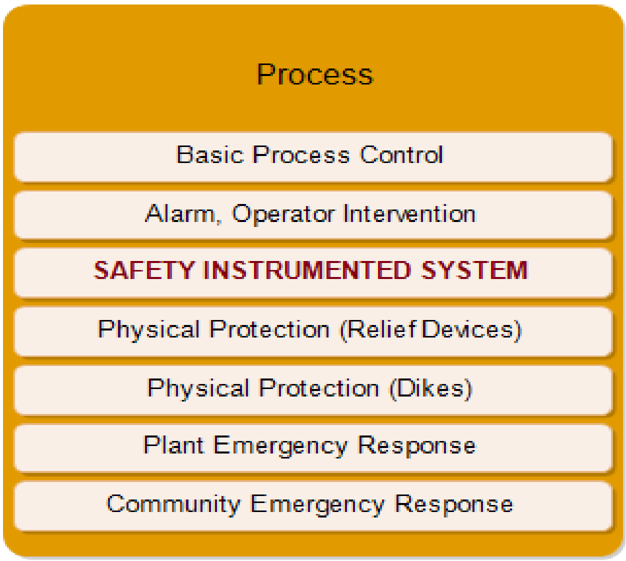

Process
Basic Process Control
Alarm, Operator Intervention
SAFETY INSTRUMENTED SYSTEM
Physical Protection (Relief Devices)
Physical Protection (Dikes)
Plant Emergency Response
Community Emergency Response

Figure 2. *Safety Protection Layers.*

3.3 Probabilistic Safety Assessment (PSA)

Probabilistic Safety Assessment (PSA) is a well defined technique specially used to measure the risk in nuclear power plants or safety engineering systems. The assessment helps to determine probability of undesired scenarios or accidents that can occur and consequences of the respective. Nuclear power plant may have huge complex system model, in which all safety functional systems, consisting thousand no. of components, are managed depending on their reliability and are logically linked together to determine possibility of accidents or overall likelihood of the accidents e.g. core melt failure. In nuclear related applications, three levels of PSAs have evolved. Level 1 addresses the plant failures assessment which tends to the determination of core damage frequency. Level 2 describes about the radiation preventive backup system and phenomenological responses, in accordance with Level 1 results, to the determination of containment release frequencies. And the off-site consequences considering with the results of Level 2 analysis, to estimates of public injuries mentioned in level 3.

4. Safety Instrumented Systems

SIS is a system which combines safety certified sensors, logic solvers and actuators together for the purpose of bringing a process into a safe state when normal pre-determined set points are exceeded or safe working conditions are violated [3] [12]. Safety instrumented system designed to respond to the abnormal conditions occurs in a plant, which may be hazardous to operator, plant or environment and if no preventive action is taken could eventually gives rise to system failures and accidental events. They must generate the correct output to prevent or mitigate the hazardous event. Each SIS can implement one or more Safety Instrumented Functions (SIF), each function has a particular Safety Integrity Level (SIL). The safety function is performed by bringing the process in a pre-determined way into a stable and safe state [13].

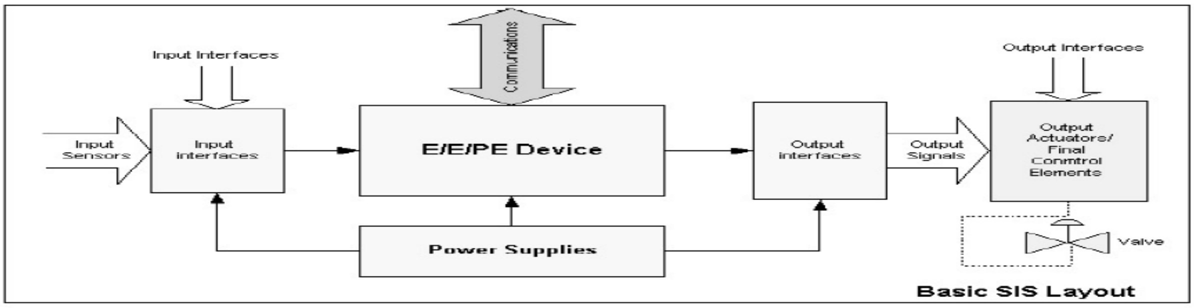


Figure 3. *Safety Instrumented System*

Every element in the control loop is belongs to SIS, and when doing an analysis of the SIS each element should be considered. This could include electrical wiring, process piping, power supplies, software (if required) etc. The function of SIS is to monitor the process for potentially dangerous conditions (process demands), and to take action when needed to protect process.

5. Safety Integrity Level

SIL certification comes from set of standards IEC61508. The Safety Integrity Level (SIL) is “a statistics of the system integrity based on probability of failure of SIS when a process requires its efficient performance”. SIL levels used to define in form of the risk reduction factor (RRF). The inverse of the RRF is the probability of failure on demand (PFD) [14]. IEC61508 defines SIL levels 1 through 4 and shows the acceptable risk level in increasing manner means SIL 1 is for lowest and SIL 4 is for highest. SIL 1 to SIL 3 are very often used in machinery, SIL 4 is mostly used in nuclear power devices and plants, petrochemical and chemical industry. For further simplification of the SIL rating, we could say that SIL 1 is required where there is occasionally danger for human personal, SIL 2 where this harm has lasting effect, SIL 3 where this harm can have fatal consequences and SIL 4 where can be harmed or killed higher number of people [9]. The table 1 shows the safety integrity levels and equivalent PFD and RRF values for process risk availability. According to this levels, the failure categorization placed by the designer and the customer with respect to recommendations of relevant standards [5] [17].

Table 1. *SIL Level and Equivalent values of PFD and RRF*

SIL LEVEL	PFD VALUE	RRF= 1/PFD	AVAILABILITY=1-PFD
4	0.0001-0.00001	10,000-1,00,000	99.99-99.999%
3	0.001-0.0001	1,000-10,000	99.9-99.99%
2	0.01-0.001	100-1,000	99-99.9%
1	0.1-0.01	10-100	90.99%

5.1 Probability to Fail on Demand (PFD)

PFD is a measure of how likely the installed system or device will be operating and ready to perform the function for the purpose it is designed.

- Protective circuit probability to fail on demand (PFD) = (Failure rate * Time interval) / 2

5.2 M.T.T.F. (Mean Time to Failure)

It is the mean time to the first failure under specified experimental conditions. It is calculated by dividing the total number of device hours by the number of failures [17].

Table 2. *Formulae for Calculation*

No. of I/P sensor Logic	PFD avg formulae for dangerous, undetected failures.	M.T.T.F. spurious formulae
1oo1	$((\lambda\ du) * (TI / 2))$	$1 / (\lambda\ s$
1oo2	$((\lambda\ du)^2 * (TI)^2) /3$	$1 / (2 * (\lambda\ s)$
2oo2	$((\lambda\ du) * TI$	$1 / (2 * ((\lambda\ s)^2 * MTTR)$
2oo3	$((\lambda\ du)^2 * (TI)^2$	$1 / (6* ((\lambda\ s)^2 * MTTR)$
TI= Time Interval, (λ du = Dangerous undetected failure rate. (λ s = safe failure rate. MTTR= Mean time to repair, 1oo1= 1 out of 1, 1oo2= 1 out of 2 likewise...		

5.3 Safety Integrity Level Selection

In the safety systems risk cannot be completely eliminated but it can be minimized to a tolerable level. Hence by decreasing the frequency of abnormal incidents and system failures, SIS manages to maintain safety level as per the ALARP principle. A SIS can provide a quantitative measure of risk reduction and recognized by its safety integrity level. SIL selection should be carried out by considering menace of system and effectiveness of all applicable process protection safety layers without neglecting relevant laws, regulations and standards specially IEC61508 and IEC61511 [11]. Many different methods for selecting an SIL can be used. Some methods explicitly use quantitative risk decision criteria. Others use qualitative tools, such as risk graphs, consequence tables, and risk matrices, that tend to obscure the risk criteria on which they are based. No method is more accurate or better than another. The standards IEC 61508, ANSI/ISA S84.01 offer three methods of determining SIL requirements [5] as 1.Qualitative methods 2.Semi-quantitative methods 3.quantitative methods.

6. CASE STUDY OF BASIC PROCESS CONTROL SYSTEM

A basic sample process is considered to determine the safety integrity level (SIL) for possible safety system. In which Flammable materials A and B are automatically and continuously fed in a fixed ratio to a reactor vessel by the basic process control system (BPCS). The set point of primary flow controller 1 is set by the vessel level controller in order to maintain a fixed level in the vessel. The flow controller for feed A adjusts the set point of the flow controller for feed B in order to maintain the fixed ratio. Figure 4 shows the basic process control for a vessel [17].

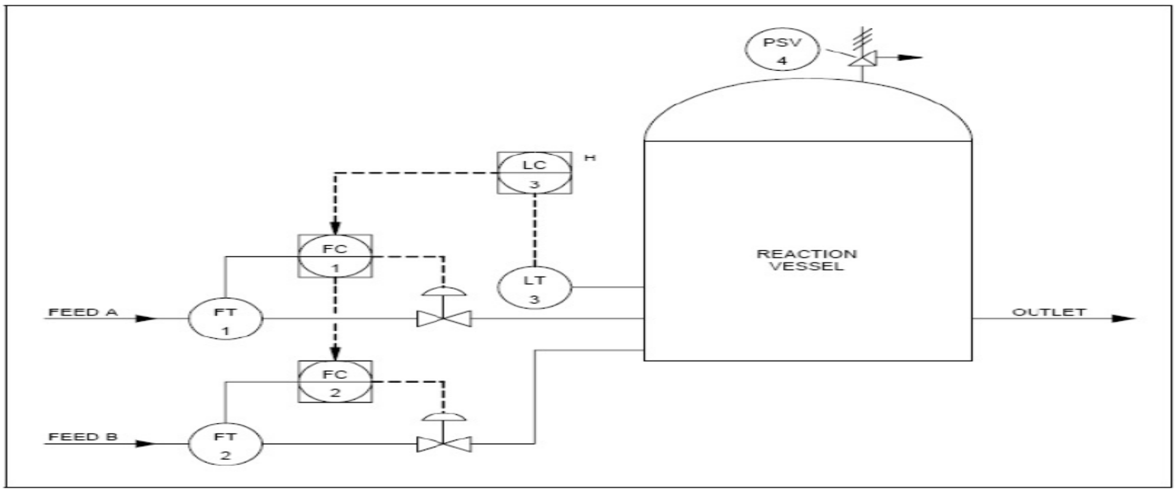


Figure 4. *Basic Process Control System.*

The following hazardous events were identified in a safety review:

Table 3. *Hazards Analysis of Given System*

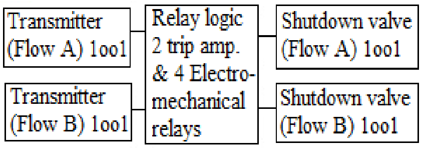
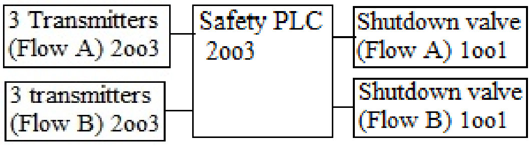
Hazards	**Causes**	**Consequence**	**Likelihood of Analysis**
flammable gas may release to environment	Failure of BPCS	Fire, Explosion, $500k loss	Medium
Vessel Failure	Failure of BPCS and relief valve	$750 k Loss	Low
Note- A nuisance trip costs $10,000		-	-

The following safety instrumentation was recommended after hazard analysis.

- Install a high pressure (HP) shutdown to close off feeds A and B to the vessel.
- Install a high level (HL) shutdown to close off feeds A and B to the vessel.

Based on the above data, and using the SIL determination method" Simplified equations" with reference to table 1, SIL 1 is required for each safety function (pressure and level). The following safety systems were proposed [17].

Table 4. *SIL Determination of Proposed Systems*

	System 1	**System2**
Sensors:	Single Transmitters	Triplicate transmitters voted 2oo3
Logic:	Relay logic	Fault-tolerant safety PLC
Valves:	Single independent shut down valves on each line.	Single independent shut down valves on each line.
Proposed System Diagram:	 Transmitter (Flow A) 1oo1 Transmitter (Flow B) 1oo1 Relay logic 2 trip amp. & 4 Electro-mechanical relays Shutdown valve (Flow A) 1oo1 Shutdown valve (Flow B) 1oo1	 3 Transmitters (Flow A) 2oo3 3 transmitters (Flow B) 2oo3 Safety PLC 2oo3 Shutdown valve (Flow A) 1oo1 Shutdown valve (Flow B) 1oo1
Given Failure Data: (Failures/year) (common for both systems)		
Sensors:	**λ du** = 0.01 (100yrMTTF) &	**λ s** = 0.02 (50 yr MTTF)
Valve and Solenoid:	**λ du** = 0.02 (50 yr MTTF) &	**λ s** = 0.1 (10 yr MTTF)

Trip Amplifier:	**ƛ du** = 0.01(100 yr MTTF) &	**ƛ s** = 0.01 (100 yr MTTF)
Mechanical Relay:	**ƛ du** = 0.002 (500 yr MTTF) &	**ƛ s** = 0.02 (50 yr MTTF)
Addition data: Test Interval (TI)= 6 months		

6.1 PFD avg Calculations:

	PFD avg = (ƛ du * TI/2		**PFD avg = (Failure rate * undetected failure% *common cause% *test interval/2)**		
Sensor:	=0.01 * 0.5/2	= 0.0025	**Sensors:**	= 0.01 * 0.01 * 0.1 *3/2	= 0.000015
Trip amplifier:	= 0.01 * 0.5/2	= 0.0025	**Safety PLC:**	=(from spec or vendor)	= 0.00005
Mechanical Relay:	= 3*0.002 * 0.5/2	= 0.0015	**Solenoid Valve:**	= 2 * 0.02 * 0.5/2	= 0.0100
Solenoid valve:	= 2 * 0.02 * 0.5/2	= 0.0100	**PFD avg (Total) = 0.01**		
PFD avg. (Total) = 0.0165					
System 1			**System2**		
System 1 satisfies the safety requirements as it gives PFD value below 0.1 which comes under SIL 1 (The risk reduction factor [1/PFD] is 60, which is between 10 and 100 required for SIL 1.)			The maximum value for a SIL 1 is 0.1. Therefore, this system 2 also satisfies the safety requirements as its PFD value is 0.01 (The risk reduction factor is 100)		

6.2 MTTF spurious Calculations:

The MTTF spurious calculation should include all components that may cause a shutdown:					
2 transmitters, 2 trip amplifiers, 4 mechanical relays, and 2 valves for system 1			both transmitter arrangements, safety PLC and both valves for system 2		
MTTF spurious = 1/ ((ƛ*s*)			**MTTF spurious = (1 / quantity * failure rate * common cause %)**		
Sensors:	= 1/ (2 * 0.02)	= 25 years	**Sensors:**	= 1/(2 * 0.02* 0.1)	= 250 years
Trip Amplifier:	= 1/ (2 * 0.01)	= 50 years	**Safety PLC:**	= (from vendor)	= 200 years
Mech. Relay:	= 1 /(4 * 0.02)	= 12.5 years	**Solenoid Valve**	=1/ (2 * 0.1)	= 5 years
Solenoid Valve	=1/ (2 * 0.1)	= 3 years	**MTTF spurious (Total) = 5 years**		
MTTF spurious (Total) 3 years					
A nuisance trip may be expected to occur, on average, every 3 years.			A nuisance trip may be expected to occur, on average, every 5 years.		

By analysing the PFD and MTTF calculations for both the systems, we can conclude that the considered BPCS system requires SIL 1 and system 2 is safer than system 1 and offers fewer nuisance trips. Following figure 5 and 6 shows the conceptual block diagram of both the systems.

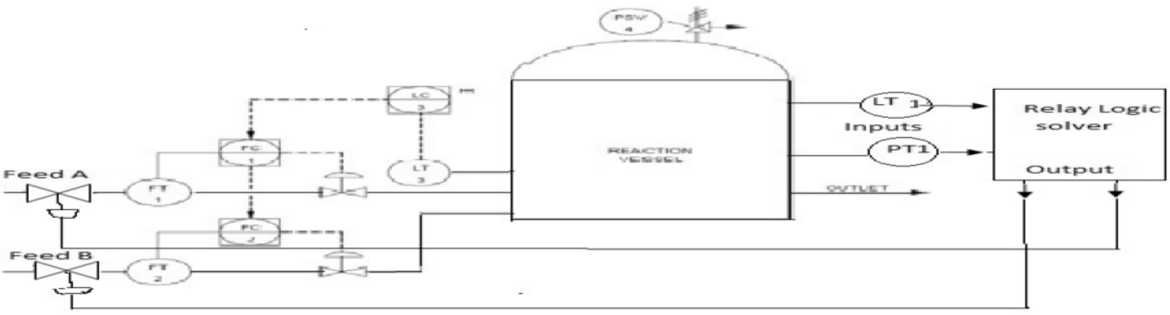


Figure 5. *Proposed SIS 1*

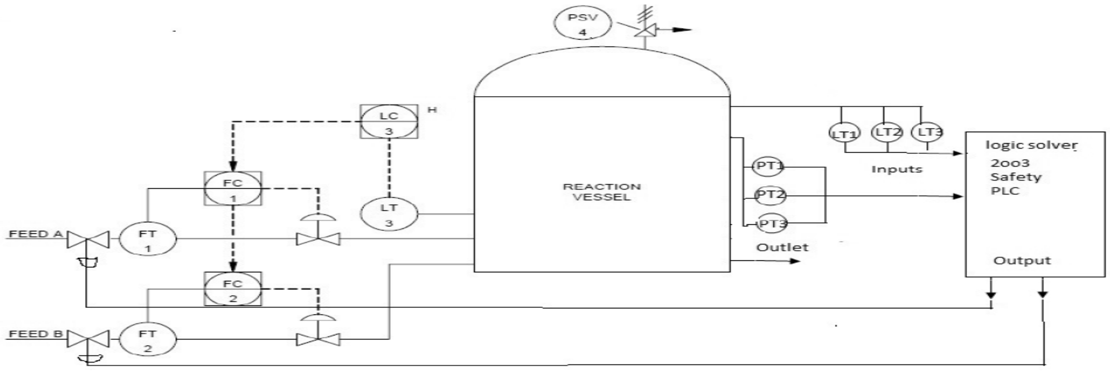


Figure 6. *Proposed SIS 2*

7. CONCLUSION

In industrial systems, like oil and gas, power plants, nuclear, chemical and space applications, it always has a potential of catastrophic failure leading to the accidental scenario endangering to operator life, economic loss due to plant shut down as well as hampering environmental aspects due to release of chemicals. In such accidental scenario, Safety Instrumented system plays very crucial role in ensuring safety to plant operation as well as human/operator life. The Standards have created an international platform for the design and development of safety related components, sub-systems and Safety Instrumented Systems for implementing the safety critical systems.

From the HAZOP analysis of plant, safety functions & its SIL as well as interlocks can be devised. Then identification of safety certified instruments, valves and controllers should be carried out to implement the safety systems as per IEC61508 / IEC61511. The safety life-cycle model is followed to find the SIL level using one of the different methods and then suggested to implement safety instrumented system in safety critical process plant as desired.

REFERENCES

[1] Kazimierz T, Kosmowski, “Functional safety concepts for hazardous systems and new challenges” Journal of Loss Prevention in the process industries 19 (2006) pp 298-305.

[2] Per Hokstad, Kjell Corneliussen, “Loss of safety assessment and the IEC 61508 standard” Reliability Engineering and System Safety 83 (2004) pp.111-120.

[3] M. Catelani, L. Ciani. V., Luongo “A simplified procedure for the analysis of Safety Instrumented Systems in the process industry application” Microelectronics Reliability 51 (2011) pp. 1503-1507.

[4] Jianghong Jina, Shoutang Zhaoa, Bin Hua “Defining the Safety Integrity Level of Public Safety Monitoring System Based on the Optimized Three-dimension Risk Matrix” (ISSSE) Procedia Engineering 43 (2012) pp.119-124.

[5] Mohamed Sallak, Christophe Simon, and Jean-Francois Aubry “A Fuzzy Probabilistic Approach for Determining Safety Integrity Level” IEEE TRANSACTIONS ON FUZZY SYSTEMS, VOL. 16, NO. 1, pp 239-248 FEBRUARY 2008.

[6] Bert Knegtering a, Hans Pasman b, “The safety barometer How safe is my plant today? Is instantaneously measuring safety level utopia or realizable?” Journal of Loss Prevention in the Process Industries 26 (2013) pp.821-829.

[7] Robert W. Johnson “Beyond-compliance uses of HAZOP/LOPA studies” Journal of Loss Prevention in the Process Industries 23 (2010) pp. 727-733.

[8] Catelani .M. Ciani. L. Luongo V. “Safety analysis in oil and gas industry in compliance with standards IEC 61508 and IEC61511: Methods and applications,” Instrumentation and Measurement Technology Conference (I2MTC), 2013. IEEE International, vol., no., pp.686, 690, 6-9 May 2013.

[9] Radek Stohl, Karel stibor, "Safety through common industrial protocol Carpathian Control Conference (ICCC), 2013 14th International 2013.

[10] Jianfeng Huang, Guohua Chen, Duomin Li, "The SIS improvement in hydrogen furnace based on SIL, Quality, Reliability, Risk, Maintenance, and Safety Engineering" (ICQR2MSE),2012 International Conference on, vol., no., pp.1443,1447, 15-18 June 2012.

[11] Laihua Fang Zongzhi Wu Lijun Wei Ji Liu, "Design and development of safety instrumented system" Automation and Logistics, 2008.ICAL 2008. IEEE International Conference on ,vol., no., pp. 2685, 2690, 1-3 Sept.2008

[12] Kapasi.C.P. Jose.V.J., Sharma M., Warke. N. "Safety instrumented system and alarm system for heater" Recent Advancements in Electrical, Electronics and Control Engineering (ICONRAEeCE), 2011 International Conference on, vol.,no.,pp.512,516,15-17 Dec.2011.

[13] Steve Gillespie, "safety Instrumented System".

[14] Safety instrumented systems (SIS), safety integrity levels (SILs), IEC61508 and Honeywell field instruments. By Honeywell.

[15] Timms, C.R. "Achieving Alarp with Safety Instrumented Systems System Safety, 2006. The 1st Institution of Engineering and Technology International Conference 2006 IET.

[16] Vintr, M.; Vintr, Z., "Safety management for electromechanical systems of railway vehicles," Reliability and Maintainability Symposium, 2008. RAMS 2008. Annual, vol., no., pp.155, 160, 28-31 Jan. 2008.

[17] Paul Gruhn, Harry Cheddie, "SAFETY INSTRUMENTED SYSTEMS: Design, Analysis, an Justification" 2nd Edition ISA publications.

[18] IEC61508, Electric / Electronic / Programmable Electronic safety related systems, parts 17. Technical report, International Electro-technical Commission, May 2010.

[19] IEC 61511, Functional safety: safety instrumented systems for the process industry sector, parts 13. Geneva: International Electro-technical Commission; 2003.

[20] ANSI/ISA Standard S84.01-1996, Application of Safety Instrumented Systems to the Process Industries, International Society for Measurement and Control, Research Triangle Park, NC, (1996).

AUTHOR'S BIOGRAPHY

Vivek Kadam received the Bachelors of Instrumentation & control from the University of Pune, India in 2011. Now he is a P.G. student (Instrumentation Engg.) at the Mumbai University, India and Lecturer at Ramrao Adik Institute of Technology, Nerul, Navi Mumbai. His research interest includes sensors transducers and process instrumentation, area.

Sharad Jadhav has received Bachelors and masters degree from university of Pune in 2000 & 2007 respectively. Currently he is working as assistant professor and head of Department in Instrumentation Engg. Department at Ramrao Adik Institute of Technology, Nerul, Navi Mumbai. His research area includes process control and fractional order control.

Mahesh Parihar has acquired Masters degree in Electronics & Instrumentation engineering from College of Engineering Pune, India in 2007 & has 9 years industrial work experience in instrumentation systems. His research areas include design of instrumentation systems for different process Engg applications.