Design of Functional safety for process automation by considering the justification of cost – benefit using ALARP evaluation method

Teerawat Thepmanee, Pornpatchara Khamkoon

Faculty of Engineering, King Mongkut's Institute of Technology Ladkrabang
Ladkrabang, Bangkok, 10520, Thailand

teerawat.th@kmitl.ac.th, pornpatchara.k@gmail.com

Abstract

This paper addresses the design of functional safety for process automation in accord with IEC 61508/ 61511 standard. Functional safety design of a tail gas treating unit has been conducted in this study. The average probability failure on demand was calculated using fault analysis and then used as the criterion for the safety instrumented function design in order to conform the required safety integrity level (SIL). The result reveals that the architecture of safety instrumented function, the test interval, and the test method made a significant impact on improving the average probability of failure on demand (PFD_{avg}) of the process. In addition, the cost-benefit evaluation was justified from asset & production loss consequence using As Low As Reasonably Practicable (ALARP) method in order to determine justification for the additional investment of the high SIL against the given additional risk reduction.

Keywords: Functional safety, IEC 61508, IEC 61511, SIS, SIF, SIL, ALARP.

1. Introduction

In industrial automation processes, risks and hazards is very likely to occur due to the production process and the chemicals used. The consequences of this may cause injury, loss of production and environmental damages etc. Safety Instrumented System (SIS) is provided to reduce from a process hazard. In the other word, it is used to detect a specific hazard and bring the process to safe state. For decades, many researchers have focused on the various designs and developments of Safety Instrumented System

in accordance with IEC 61508/61511 standards [1,2]. Laihu Fang [3] presented the procedure to evaluate the Safety Integrity Level (SIL), also the methods and techniques that such as Layer of Protection Analysis (LOPA), Fault Tree Analysis (FTA), Risk matrix and Risk graph. T.Thepmanee [4] designed a safety instrumented function of the two-phase gas - liquid separator using graphs risk and calculated average probability failure on demand via a simplified equation. The significant parameters that affect the calculation such as period of testing, the architecture and test methods were focused. However, the selected process was not complicated and the cost analysis of safety instrumented function design was not yet performed. Later on, cost-benefit analyses of the safety function for functional testing was then studied [5]. GE Jolliffe [6] discussed on the ALARP (As Low As Reasonably Practicable) assessment for the costs of Safety Instrumented Function design and installation. The high cost by considering the relationship between the costs of investing in the benefits to be received, including compilation of case studies related to the introduction of ALARP. This paper addresses design of safety functions for process automation. After evaluating the safety function is the safety integrity level for the property loss is high. Will be done considering the cost of capital relative to the benefits by ALARP that the highest SIL is resulted from asset & production loss consequence, to determine the additional investment of the high SIL of safety instrumented function against the given additional risk reduction gained is justified or not.

2. Functional Safety Design

2.1 Safety Integrity Level (SIL)

Safety instrumented system is used to prevent or mitigate hazardous situation to tolerable levels. The safety integrity of safety instrumented system is identified as the Safety Integrity Level (SIL). The higher SIL means the better the safety performance of SIS.

IEC 61508 standard has categorized four overall safety integrity level for continuous mode system, referred to as the average probability of failure on demand (PFDavg), shown in Table 1.

Table 1 Safety integrity level.

Safety Integrity Level (SIL)	Average probability of failure on demand (PFDavg)
4	$< 10^{-5}$ to $< 10^{-4}$
3	$< 10^{-4}$ to $< 10^{-3}$
2	$< 10^{-3}$ to $< 10^{-2}$
1	$< 10^{-2}$ to $< 10^{-1}$

2.2 Probability of a Failure on Demand (PFD)

PFD can be calculated by knowing failure rate and test interval. The approximation probability of a failure on demand (PFD) is given by following equation [1-4].

$$PFD = \lambda_D T_i \quad (1)$$

Where

λ_D = Failure rate (failures per hours)

T_i = Test interval (hours)

For PFDavg, it can be derived by integrating the PFD(t) from 0 to the test interval, T_i and dividing by the test interval. The equation is expressed as:

$$PFD_{avg} = \frac{1}{T_i} \int_0^{T_i} \lambda_D T_i dt \quad (2)$$

$$PFD_{avg} = \frac{1}{2} \lambda_D T_i \quad (3)$$

The average probability of failure on demand of a safety function for the SIS is determined by combining the

average probability of failure on demand for all the subsystems (Sensor, Logic Solver and Final Element). This can be expressed by:

$$PFD_{avg} = PFD_{avg(SE)} + PFD_{avg(LS)} + PFD_{avg(FE)} \quad (4)$$

Where

PFD_{avg} = the average probability of failure on demand of safety function (in the test time interval)

$PFD_{avg(SE)}$ = the average probability of failure on demand of sensor subsystem (in the test time interval)

$PFD_{avg(LS)}$ = the average probability of failure on demand of logic solver subsystem (in the test time interval)

$PFD_{avg(FE)}$ = the average probability of failure on demand of final element subsystem (in the test time interval)

2.3 As Low As Reasonably Practicable (ALARP)

ALARP stands for “as low as reasonably practicable” and is the demonstrable process whereby a risk is reduced so low that any further risk reduction would involve time, trouble, difficulty and cost which are grossly disproportionate to the additional risk reduction achieved [7]. This paper applied the ALARP principle to evaluate the design of safety instrumented function by using ROACE equation. The design that meets the justification criteria therefore is ALARP. However, ALARP evaluation is carried out for economic risk only.

The ALARP evaluation process can be done as follows:

1. Design each of the various alternative designs.
2. Establish the required test intervals for each design.
3. Do the ALARP evaluation by using ROACE equation for each improvement and confirm the selection.
4. Finally, establish the target integrity level and the selected design.

Following the ALARP evaluation process, the justified alternative should be selected for implementation and the integrity level of the selected ‘ALARP’ design will become the target safety integrity level.

The justification of the higher design alternative (higher SIL) is based on the Return on Average Capital Employed (ROACE) of the additional benefits and costs of this alternative relative to the lower case (lower SIL). The ROACE is calculated as:

$$ROACE = (Ben - Dep - ATC - ARC - NR) / AI_{TA} \quad (5)$$

Where

$$\begin{aligned} Ben &= \text{Benefits } (\$.y^{-1}) \\ Dep &= \text{Depreciation per year } (\$.y^{-1}) \\ ATC &= \text{Additional test costs } (\$) \\ ARC &= \text{Additional repair costs } (\$) \\ NR &= \text{New risk } (\$) \\ AI_{TA} &= \text{Additional investment this alternative } (\$) \end{aligned}$$

The ROACE is expressed in percentage. Both numerator and denominator may be positive or negative values. If the numerator is negative, the ROACE will be negative unless the denominator is also negative. This design is justified if:

$$ROACE \geq ROACE_{target} \quad (6)$$

Where $ROACE_{target}$ is the specified minimum ROACE to justify an investment (typically taken as 15 % to 20 %).

The parameters in equation (5) can be expressed as following:

Benefits (Ben) are calculated as:

$$Ben = (PFD_{LA} - PFD_{TA}) \cdot IR \quad (7)$$

Where

$$\begin{aligned} PFD_{LA} &= \text{PFD lower alternative} \\ PFD_{TA} &= \text{PFD this alternative} \\ IR &= \text{Initial risk } (\$.y^{-1}) \end{aligned}$$

Initial risk (IR) is the risk without any safety function implemented. It is calculated as:

$$IR = TEC / DI \quad (8)$$

Where

$$\begin{aligned} TEC &= \text{Total Equivalent Consequences } (\$) \\ DI &= \text{Demand Interval (year)} \end{aligned}$$

The total equivalent monetary consequences (TEC) are the sum of the estimated losses calculated from the downtime and repair costs, the monetary equivalent of the personal safety consequences, and the monetary equivalent of the environmental consequences. The demand interval (DI) is the logarithmic average of the lower and upper limit of the selected demand rate category. For instance, if the demand rate category is 10 to 100 years, the logarithmic average is 31.6 years.

The depreciation per year (Dep) is the additional investment of the alternative divided by the depreciation period as specified for the project (10 years). The Dep is calculated as:

$$Dep = AI_{TA} / \text{period} \quad (9)$$

Additional investment of the alternative (AI_{TA}) is calculated as:

$$AI_{TA} = IC_{TA} - IC_{LA} \quad (10)$$

The additional investment of the alternative is the difference between the investment cost of the alternative and lower alternative. The Investment cost of the alternative (IC_{TA}) is the sum of all the investment cost of all components (tags) required to create the alternative design. The Investment cost of the lower alternative (IC_{LA}) is the sum of all the investment costs of all components (tags) required to create the lower alternative design.

The additional test costs (ATC) are the difference between test costs of the alternative (TC_{TA}) and test costs of the lower alternative (TC_{LA}). The ATC is calculated as:

$$ATC = TC_{TA} - TC_{LA} \quad (11)$$

The test costs of the alternative are the sum of all the test costs of all components (tags) required for the alternative design. The test cost of each tag is calculated as the test cost per tag multiply with the test frequency. Test costs include the cost of taking the unit down to facilitate a test that cannot be performed on-line. The test costs of the lower alternative are the sum of all the test costs of all components (assets) required for the lower alternative design. The test cost of each tag is calculated as the test cost per tag multiply with the test frequency.

The additional repair costs (ARC) are the difference between the repair costs of the alternative (RC_{TA}) and the repair costs of the lower alternative (RC_{LA}). The ARC is calculated as:

$$ARC = RC_{TA} - RC_{LA} \quad (12)$$

The repair costs the alternative is the sum of all the repair costs of all components (tags) required for the alternative design. The repair costs lower alternative is the sum of all the repair costs of all components (tags) required for the lower alternative design.

The new risk (NR) is the additional cost due to spurious trips by the alternative design. The higher costs could be attributable to the possibly higher spurious trip rate of the alternative compared to the lower alternative design. The new risk is calculated as the difference between the sum of the yearly costs of safe failures of all safe-failure cluster (SFC) in the function of this alternative design and the lower alternative design. The NR is calculated as:

$$NR = SFC_{TA} - SFC_{LA} \quad (13)$$

First, the sum of the yearly costs due to safe failures of all SFC regarding the lower alternative design is calculated. Then, the sum regarding this alternative is similarly calculated. It was noted that the safe failure cost of this alternative minus the safe failure cost regarding the lower alternative is the new risk (the value could be negative). In case a SFC is safe fault tolerant, the yearly cost of a safe failure is taken as zero.

2.4 Lifecycle cost analysis (LCC)

To justify safety instrumented system expenditure, it is done by completing a lifecycle cost analysis for the various options being considered. The lifecycle costs reflect the total cost of owning the system. By calculating the lifecycle cost, various options can be analyzed in a more quantitative and content manner.

Table 2 describes the predominant costs incurred during the life of a safety system. The list is divided into initial fixed costs, and annual costs. [8]

Table 2 Breakdown of safety system costs.

Cost item	Comments
Initial fixed costs	i.e., the cost for design, purchasing, installation, commissioning, and operating the system
Annual cost (M)	i.e., maintenance and other ongoing costs associated with the system
Present value for annual costs(PV)	The present value of the annual costs based on current interest rates and the predicted life of system. These costs are added to the initial fixed costs to obtain the present value of all costs.

The PV is calculated by solving the given equation:

$$PV = M[1 - (1+R)^{-N}] / R \quad (14)$$

Where

M = the annual cost (\$)

R = the interest rate (%)

N = the number of year (year)

To calculate the total lifecycle costs (LCC) for the life of the system, it can be done by summing the initial fixed costs and the present value for the annual fixed costs.

3. Project Case Study

3.1 Tail Gas Treating Process descriptions

Petrochemical and refinery processes produces harmful chemicals such as sulfur (S) and sulfur dioxide (SO₂) as by products, which can cause potential negative effects on the host community and the environment. Although sulfur dioxide is a colorless, non-flammable, but it can affect the health of people in the host community surrounding the plant. Therefore, sulfur must be recovered more than 95-97% before being released to the atmosphere in order to meet the requirements. Sulfur can be recovered by installing a sulfur recovery unit to convert gaseous hydrogen sulfide (H₂S) into solid sulfur together with installing a tail gas treating unit to increase recovery rates up to 99.9%.

This research was part of the selection process, tail gas treating from Fig.1 in the study and evaluation of safety instrumented function follows. A tail gas treating process starting from the tail gas derived from the sulfur recovery unit. The tail gas is then heated through tail gas heaters E-8671 and E-8676 before sent to a reactor R-8671. Reacted with H₂, the tail gas SO₂, S, COS and CS₂ will be converted to hydrogen sulfide (H₂S) via hydrogenation in the reactor. After this exothermic reaction, which a large amount of energy is released, the high temperature gaseous H₂S is then cooled by forwarded to a reactor effluent cooler E-8672 (heat exchanger) and then to a contact condenser C-8671 in order to separate the gas phase of sulfur removal tail gases and the liquid phase of H₂S/amine liquid mixture. The liquid solution is then forwarded to the amine absorber for H₂S removal before sending them to the incinerator and released to the atmosphere. The sour water is cooled down and sent back into the contact condenser C-8671 again.

Fig. 1 P&ID of the tail gas treating unit (SIF2-A)

3.2 Safety Integrity Level Assessment

Three safety instrumented functions, SIF-A, SIF-B, and SIF-C, for the above tail gas treating unit are evaluated with a target safety integrity level (SIL) as shown in Table 3.

Table 3 Result of SIL Assessment.

SIF No.	Descriptions	SIL target
SIF2-A	Liquid low level protection	2
SIF2-B	High temperature protection	2
SIF2-C	Pump loss suction protection	1

The assessment procedure can be found in [4]. The assessment of the risk of faults that could occur, which will lead to the occurrence of hazards in each event, was firstly performed by considering the demand rate (W), asset & production loss (L), personal safety (C), and the environment (E).

3.3 Design and PFD calculation

After the safety integrity level is assessed, a new system of the safety instrumented function, SIF2-A, is proposed. Regarding section 2.2, the PFD_{avg} for the sensor, the logical solver, and the logical final element of the proposed architecture in various cases are calculated and shown in Table 4 – 6. The test interval T_{i1} and T_{i2} of the final element represent a full test and a partial test respectively.

Table 4 Proposed architecture for sensor

SIF No.	Architecture	Test Interval (T_i)	PFD _{avg} (SE)
SIF2-A1	1oo3	8	0.00363
SIF2-A2	1oo3	4	0.00045
SIF2-A3	1oo3	4	0.00045
SIF2-A4	1oo3	4	0.00045
SIF2-A5	1oo3	4	0.00045
SIF2-A6	1oo3	8	0.00363

Table 5 Proposed architecture for logic solver

SIF No.	Architecture	Test Interval (T_i)	PFD _{avg} (LS)
SIF2-A1	1oo1	4	0.000566
SIF2-A2	1oo1	4	0.000566
SIF2-A3	1oo1	4	0.000566
SIF2-A4	1oo1	4	0.000566
SIF2-A5	1oo1	4	0.000566
SIF2-A6	1oo1	4	0.000566

Table 6 Proposed architecture for logic final element

SIF No.	Architecture	Test Interval (T_i)	PFD _{avg} (FE)
SIF2-A1	1oo1+1oo1	8	0.35720
SIF2-A2	1oo1+1oo1	4	0.18760
SIF2-A3	1oo1+1oo1	4+ $T_{i2}=1$	0.08911
SIF2-A4	1oo2+1oo2	4	0.02346
SIF2-A5	1oo2+1oo2	4+ $T_{i2}=1$	0.00807
SIF2-A6	1oo3+1oo3	4	0.00330

The average probability of failure on demand PFD_{avg} for each element in Table 4 – 6 are summarized and further average in Table 7. It can be obviously seen that the PFD_{avg} (Total) of each of SIF2-A1 to SIF2-A4 is than 0.01, which does not meet the SIL2 requirement. Only SIF2-A5 and SIF2-A6 that can satisfy the safety range of SIL2.

Table 7 Safety Instrumented Function design SIF2-A

SIF No.	PFD _{avg} (SE)	PFD _{avg} (LS)	PFD _{avg} (FE)	PFD _{avg} (Total)
SIF2-A1	0.00363	0.000566	0.35720	0.37940
SIF2-A2	0.00045	0.000566	0.18760	0.18862
SIF2-A3	0.00045	0.000566	0.08911	0.09130
SIF2-A4	0.00045	0.000566	0.02346	0.02448
SIF2-A5	0.00045	0.000566	0.00807	0.00909
SIF2-A6	0.00363	0.000566	0.00330	0.00750

4. Evaluation of the cost – benefit by ALARP

It was found that the costs of the function safety for process automation are costly for design, investment, maintenance and safety instrumentation with a high SIL. Also, it is difficult to install due to the limited space for the shutdown valve. To determine the risk to be reduced compared to the cost and the hassle of having to rise to consider the suitability of installing the evaluation safety integrity level of SIF2-A, it was found the highest SIL as a result of the risk of asset and production loss. Analyzing and evaluating the trade-off between benefits and the additional cost between the safety integrity level 1 (SIL 1) and level 2 (SIL 2) according to section 2.8.1 in Shell's standard [7], it was found that SIL 2 is appropriate to the current process with the average probability of failure on demand (PFD_{avg}) in an acceptable range in ALARP method. Comparing SIF2-A3 (SIL 1) to SIF2-A5 (SIL 2) for the assessment, as shown in Table 3, which are appropriate for the process with different elements in the design, SIF2-A5 has safety valves more than SIF2-A3.

Fig. 2 The life cycle costs and the average probability of failure on demand from cost–benefit evaluation.

Fig. 2 shows the result of the lifecycle (CCL) and PFD_{avg} from cost-benefit evaluation. Table 8 shows the result calculated by Eq. (5) for an alternative design based on the ROACE of the additional benefits and costs of the current alternative concerning the lower one calculated by Eq. (5). It was found that the value of ROACE is 26.69% and greater than the target value ROACE_{target}, 20%. This indicates that the additional cost from SIF2-A3 (with SIL 1) to SIF2-A5 (with SIL 2) in order to reduce more risk.

This study intentionally demonstrates the technique for completing the lifecycle cost analysis. However, because of

a high subjective data, which is not reflecting the actual costs for any particular installations. Thus, the data from individual organization should be used for the assessment in order to reflect an accurate result.

Table 8 ALARP Calculation

The Parameters for calculating the ROACE		ALARP Calculation	
		SIF2-A3	SIF2-A5
Benefit			
Demand interval :DI(year)		3.16E-01	3.16E-01
Consequences			
Economic loss		31622.77	31622.77
Personal Health and Safety		316.23	316.23
Environment impact		3162.28	3162.28
Total Equivalent Consequences :TEC (\$)		35101.28	35101.28
Initial Risk: IR(\$/year)		111080.00	111080.00
Risk Reduction of (PFD _{avg}) SIF2-A3		9.013E-02	N/A
Risk Reduction of (PFD _{avg}) SIF2-A5		N/A	9.090E-03
Total benefits		9001.92	
Investment			
Investment of Lower(\$)	SIF2-A3	52000	N/A
Investment of this(\$)	SIF2-A5	N/A	76000
Additional investment this alternative (AITA)		24000	
Depreciation period(year)		10	
Depreciation per year		2400	
Cost			
Test Cost of	SIF2-A3	900	N/A
Test Cost of	SIF2-A5	N/A	1000
Additional Test Cost :ATC(\$)		100	
Repair Cost of	SIF2-A3	288	N/A
Repair Cost of this	SIF2-A5	N/A	384
Additional Repair Cost :ARC(\$)		96	
New risk			
Spurious trip cost of	SIF2-A3	0	N/A
Spurious trip cost of	SIF2-A5	N/A	0
Additional spurious trip cost		0	
ROACE_{target} (15 to 20 %)		20.00%	
ROACE (%)		26.69%	
Result		Justified	

Table 9 Life Cycle Costs Calculation

Safety system costs	SIF2-A3	SIF2-A4	SIF2-A5	SIF2-A6
Investment / Initial Fixed Cost				
Sensor	12,000	12,000	12,000	12,000
Logi Solver	16,000	16,000	16,000	16,000
Final Element	24,000	48,000	48,000	72,000
Total	52,000	76,000	76,000	100,000
Annual Cost				
Test cost per year	900	255	1,000	435
Repair cost per year	288	384	884	480
Spurious trip cost	-	-	-	-
Total	1,188	639	1,884	915
Present value for annual costs				
Number of years (N) 20				
Interest rate % (R) 6				
PV	13,626	7,329	21,609	10,495
Total Life Cycle Cost	\$ 65,626	\$ 83,329	\$ 97,609	\$ 110,495

5. Conclusion

Risk assessment of the proposed tail gas treating process show the crucial three functions for the safety instrumented function by evaluating the safety integrity level using the risk graph method. Designs for each function were then proposed before analyzing the probability failure on demand of each function for the safety instrumented functions SIF2-A. The results showed that both the design of device and the test method have an effect on the probability failure on demand. Also, the result from assessment of the benefits-costs by evaluating ALARP with ROACE and comparing the designs SIF2-A3 and SIF2-A5 with the safety integrity level of SIL 1 and SIL 2, respectively, showed the value of ROACE obtained from the analysis is 26.69% and greater than the target value of 20%. Thus, to reduce the risk from SIF2-A3 (SIL 1) to SIF2-A5 (SIL 2), the additional cost has to be provided.

References

- (1) IEC-61508 : “Functional safety of electrical / electronic / programmable electronic safety-related systems”, International Electrotechnical Commission, 2000
- (2) IEC-61511 : “Functional safety - Safety instrumented systems for the process industry sector”, Inter-national Electrotechnical Commission, 2003
- (3) Laihua Fang, Zongzhi Wu, Lijun Wei and Ji Liu. “Design and Development of Safety Instrumented System” Proceedings of IEEE International Conference on Automation and Logistics, Qingdao, China, September 2008.
- (4) Teerawat Thepmanee and Pornpatchara Khamkoon “SIL Assessment and implementation case study: A safety instrumented function for overpressure protection in a two – phase gas – liquid separator”, ICIC Express Letters Part B: Applications Volume 5, Number 1, February 2014, pp. 45 – 50.
- (5) Amornsak Potiteerabuit, Teerawat Thepmanee “Probabilistic assessments of Safety Instrumented Function by considering the justification of cost-benefit using ALARP evaluation method”, The 3rd International Conference on Industrial Application Engineering 2015, Kitakyushu, Japan, March 28-31, 2015.
- (6) G.E. Jolliffe. “Consideration of ALARP for Complex Safety Related Systems”, 3rd IET International Conference on Safety System, Birmingham, England, October 2008.
- (7) Shell GSI : “Classification and Implementation of Instrumented Protective Functions”, DEP 32.80.10.10 – Gen (Shell Standard), 2010.
- (8) Paul Gruhn and Harry L. Cheddie, “Safety Instrumented Systems: Design, Analysis and Justification”, 2nd edition, ISA, 2006.