Journal of Mechanics Engineering and Automation 5 (2015) 472-480
doi: 10.17265/2159-5275/2015.08.008

The Design Improvement of High Integrity Protection System

Jin Hyung Park
System MK Team, Yokogawa Electric Korea, Seoul 150-866, South Korea

Abstract: HIPS (High Integrity Protection System) is a really important system to protect the fractionation column from overpressure and to protect any atmospheric pollution from flare stack, scrubber and VCU (vapor combustion unit), etc. KOSHA (Korea Occupational Safety & Health Agency) made criteria about HIPS inspection in 2007 to enforce HIPS inspection. HIPS is the first system which KOSHA and KGS (Korea Gas Safety Corp.) officially required to attach SIL verification report in the Process Safety Report. KOSHA and KGS uniformly require SIL3 for HIPS and require to configure the safety instrumented function to meet SIL3 requirement. The flare system with SIL3 application should have the interlocks to shut off the heat source in case of high pressure from tower, the cooling system failure and the power failure. KOSHA and KGS admit that the flare load is 0 where SIL 3 is applied to the flare system. So it is beneficial to plant because the equipment investment cost can be saved if SIL3 is applied to the flare system. By this reason, so many plants in Korea applied SIL3 to the flare system, scrubber system and VCU, etc. For SIL3 application, the redundant shutdown valve with PST (partial stroke test) should be installed with 1 out of 2 voting and the positioner for PST function should have HART communication function. There were problems caused by HART communication devices, so the system design should be cautiously done considering the operation availability and safety at the same time.

Key words: HIPS, SIL, SIS, HFT.

1. Introduction

HIPS (High Integrity Protection System) is one of most important systems in refinery and petrochemical plants to protect overpressure or liquid carryover of column or tower and any atmospheric pollution from flare stack, scrubber and VCU (vapor combustion unit), etc. The failure of pressure control of column or tower can result in severe consequences, so the roll of HIPS is very important for the plant safety. HIPS is the first system which KOSHA (Korea Occupational Safety & Health Agency) and KGS (Korea Gas Safety Corporation) officially required to attach SIL verification report in the Process Safety Report. KOSHA and KGS uniformly required SIL3 for HIPS and require to configure the safety instrumented function to meet SIL3 requirement. There are several applications to meet SIL3 in HIPS. In this paper, the HIPS design to meet the operation availability and safety at the same time will be introduced.

Corresponding author: Jin Hyung Park, CFSE, research fields: LOPA methodology, turret safety system in FPSO on 15 m wave height. E-mail: jinhyung.park@kr.yokogawa.com.

2. What Is HIPS?

HIPS is a SIS (Safety Instrumented System) that is designed to provide overpressure and over-temperature protection that is at least equivalent in reliability to a mechanical relief device. HIPS has traditionally been used for rapid depressurization of Hydrocrackers and Acetylene Hydrogenators in runaway conditions, to simultaneously reduce pressure and remove heat, where a safety valve is ineffective. More recently, HIPS has been employed to remove the heating supply to fractionation columns to avoid activation of the pressure relief device and causing a release to atmosphere or a flare system. In this use, it is a secondary overpressure protective system for the purpose of optimizing the design of the flare header system and connected pressure devices [1]. In Korea, HIPS is used to reduce the flare load of flare stack, scrubber, VCU

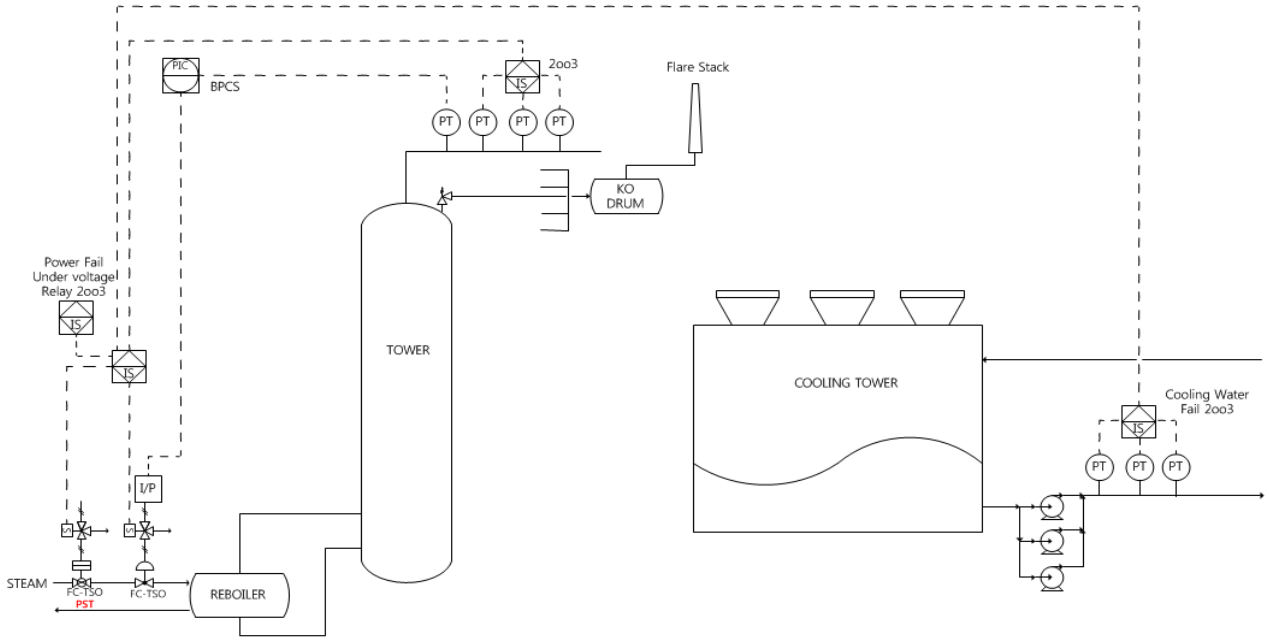


Fig. 1 The typical P&ID in relation with HIPS in Korea.

(vacuum combustion unit), etc. Fig. 1 shows the typical P&ID in relation with HIPS.

3. The Merits of HIPS

The below describe the merits of HIPS.

- The reduction of flare load

If SIF of HIPS meets SIL3, the flare load in the SIF will be calculated at 0 by KOSHA criteria in Korea. The capacity of flare stack, scrubber, VCU, etc. can be reduced by HIPS.

- The protection from overpressure

The tower and reactor can be protected from overpressure.

- The protection of environment

The air pollution will be prevented by the reduction of flare load.

4. HIPS in the Technical Materials of KOSHA

The inspection criteria in KOSHA technical materials about HIPS are described as below [2].

- Review and complementary item checklist

(BPCS stands for Basic Process Control System and SIS stands for Safety Instrumented System.)

The prerequisite for SIL3:

	Yes	No	Remark
2. The appropriateness of SIS application			
- Is the flare load reduction appropriate when SIS is applied to process? * Single SIF check			
- Can all items be processed at the same time when SIS is applied to process? * Global SIF check			
3. The appropriateness of SIS design			
- Which items are added for the reduction of flare load and are those items appropriate for the improvement of reliability when SIS is applied to process? • Sensor, Logic Solver, Final element			
- Which items are added to process the control of all items at the same time and are those items appropriate for the improvement of reliability when SIS is applied to process? • Power supply, the separate SIS panel from BPCS			

	Yes	No	Remark
1. The separation between BPCS and SIS			
- Are BPCS and SIS separated? * Hardware separation (separate panel) * Software separation (separate program access)			
- Are the field instruments (sensor or transmitter) separated? * The sensor for SIS and the sensor for BPCS should be separated. The cables for them should be separated.			
- Are the instrument piping from the sensor in the field separated?			
2. The bypass installation of SIS			
- Is there a master bypass? • The master bypass to bypass all SIS should not be installed in the control room.			
- Is there a bypass procedure for each item? • There should be the clear bypass procedure in case of 1 step bypass when 2 step bypass is impossible.			

(1) Sensor: 2 out of 3 voting;

(2) Logic solver: separate PLC from DCS;

PLC should have a self diagnostic function.

(3) Final element: the valve should be redundant (at least two).

The full stroke test or the partial stroke test should be done and the partial stroke test device should be installed in case of new equipment.

There should be the test procedure for the full stroke test.

5. Why SIL3 for HIPS?

Why is SIL3 required for HIPS as target SIL? We can analyze the target SIL of HIPS by the Risk Matrix methodology as Fig. 2. For health and safety and economics, 4-20 years of demand rate was assumed based on the overpressure of tower and for environment, and for environment, 0.5-4 years of demand rate was assumed based on the fact that there is one or two power failures by lightning on the petrochemical complexes in Korea [3].

Nowadays, several license companies start to apply the highest SIL for flare load 0, so SIL4 is required for HIPS for approval of flare load 0.

6. Why 1 out of 2 Redundancy of PST Valves for SIL3?

Fig. 3 is the example of SDV (shutdown valve) and Fig. 3 shows that this shutdown valve can meet SIL3 only by PVST (Partial Valve Stroke Test) [4].

Consequences			Demand Rate (time between demands)				
Health and Safety	Economics (Loss in €)	Environmental effect	Negligible Demand	> 20 years	4 - 20 years	0.5 - 4 years	0 - 0.5 years
Slight Injury or Health Effect	Slight < 10 k	Slight	-	-	a 1	a 2	a 2
Minor Injury or Health Effect	Minor 10 k - 100 k	Minor	-	a 1	a 2	1	2
Major Injury or Health Effect	Medium 100 k - 1 M	Local	-	a 2	1	2	3
1 – 3 Fatalities	Major 1 M - 10 M	Major	-	1	2	3	4 (x)
Multiple Fatalities	Extensive > 10 M	Massive		2	3	4 (x)	x

Fig. 2 Risk Matrix analyzed for HIPS.

IEC 61508 Failure Rates

Application	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}
Full Stroke, Clean Service	0 FIT	634 FIT	0 FIT	582 FIT
Tight Shut-Off, Clean Service	0 FIT	0 FIT	0 FIT	1229 FIT
Open on Trip, Clean Service	0 FIT	765 FIT	0 FIT	447 FIT
Full Stroke with PVST, Clean Service	0 FIT	634 FIT	273 FIT	309 FIT
Tight Shut-Off with PVST, Clean Service	0 FIT	0 FIT	271 FIT	958 FIT
Open on Trip with PVST, Clean Service	0 FIT	765 FIT	287 FIT	160 FIT
Full Stroke, Severe Service	0 FIT	1265 FIT	0 FIT	985 FIT
Tight Shut-Off, Severe Service	0 FIT	0 FIT	0 FIT	2264 FIT
Open on Trip, Severe Service	0 FIT	1515 FIT	0 FIT	731 FIT
Full Stroke with PVST, Severe Service	0 FIT	1265 FIT	477 FIT	508 FIT
Tight Shut-Off with PVST, Severe Service	0 FIT	0 FIT	476 FIT	1788 FIT
Open on Trip with PVST, Severe Service	0 FIT	1515 FIT	507 FIT	224 FIT

Fig. 3 Exida certificate for a SDV.

Based on IEC61508 SFF (Safe Failure Fraction) formula, SFF of PVST can be calculated as below.

- Full stroke with PVST, clean service

$$SFF = (\lambda S + \lambda Dd) / (\lambda S + \lambda Dd + \lambda Du)$$
$$= (\lambda Sd + \lambda Su + \lambda Dd) / (\lambda Sd + \lambda Su + \lambda Dd + \lambda Du)$$
$$= (0 + 634 + 273) / (0 + 634 + 273 + 309)$$
$$= 75\% \quad \text{-> SIL2 with HFT0}$$

Considering that the HFT (hardware fault tolerance) of one valve is 0 and SFF is 75%, SIL2 is determined by Table 2 of IEC61508-2 [5].

Table 2 — Hardware safety integrity: architectural constraints on type A safety-related subsystems

Safe failure fraction	Hardware fault tolerance		
	0	1	2
< 60 %	SIL1	SIL2	SIL3
60 % - < 90 %	SIL2	SIL3	SIL4
90 % - < 99 %	SIL3	SIL4	SIL4
> 99 %	SIL3	SIL4	SIL4

For SIL3, HFT1 (1 out of 2 voting) is needed.

Table 2 — Hardware safety integrity: architectural constraints on type A safety-related subsystems

Safe failure fraction	Hardware fault tolerance		
	0	1	2
< 60 %	SIL1	SIL2	SIL3
60 % - < 90 %	SIL2	SIL3	SIL4
90 % - < 99 %	SIL3	SIL4	SIL4
> 99 %	SIL3	SIL4	SIL4

7. Recommendations for Better Solution

7.1 Independent 1 out of 2 SDV

Based on IEC61511-2:2003, the independent 1 out of 2 SDVs are highly recommended to meet SIL3 as Fig. 4.

Fig. 5 typical architecture comprising one SDV and one control valve can meet only SIL2.

The reason why the shared control valve between BPCS and SIS is SIL0 is described in IEC61511-2 as below [6].

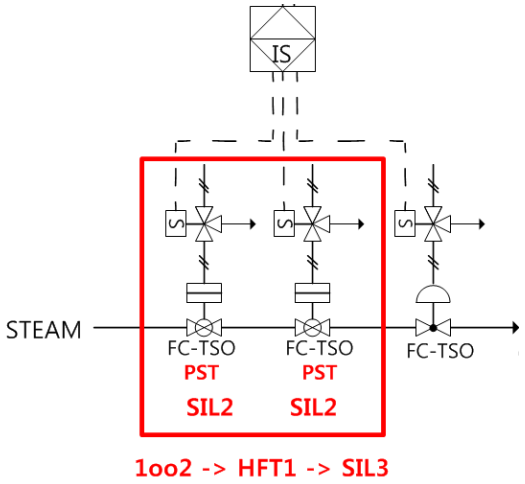


Fig. 4 Independant 1 out of 2 SDV.

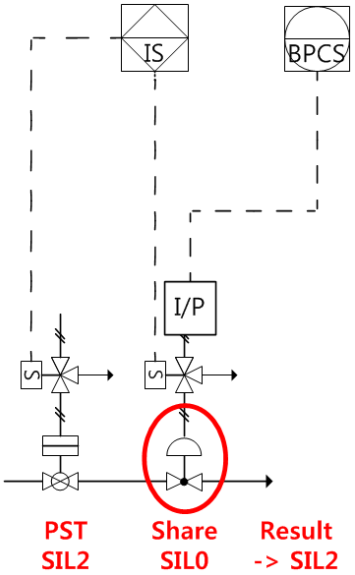


Fig. 5 1 out of 2 valves sharing control valve.

"11. SIS design and engineering

11.2.4 IEC61511-1, Clause 11, has a number of design requirements for a SIS. On concern is independence between the SIS and the BPCS.

(b) Final element

Where a single valve is used by both the BPCS and SIS, the requirements of IEC 61511-1 will normally only be satisfied if the valve diagnostics can reduce the dangerous failure rate sufficiently and SIS is capable of placing the process in a safe state within the required time.

In practice, this is difficult to achieve even for SIL1 applications."

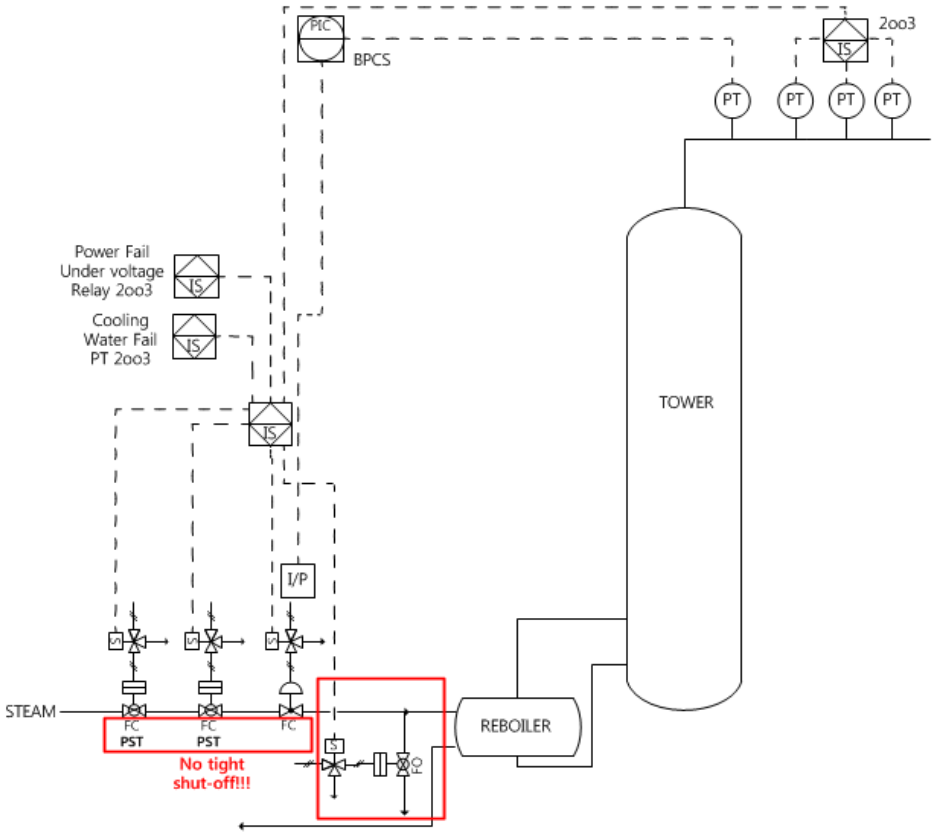


Fig. 6 P&ID with steam bleed line.

7.2 Steam Bleed Line

The installation of steam bleed line can remove the latent heat in reboiler. The P&ID with steam bleed line is as Fig. 6.

The recommended P&ID focused on the steam line to reboiler is as Fig. 7.

The merit of steam bleed line is as below.

• The latent heat can be reduced by removing the remaining steam in the pipe.

• Tight shut-off function of valve function is not necessary. It is very hard to meet SIL3 with tight shut-off function in case of 1 out of 2.

The below example of SDV certificate shows that the SFF with tight shut-off function can meet only SIL1 even with PVST function [4].

The best failure rate among the above 3 cases is tight shut-off with PVST, clean service. The SFF of SDV for tight shut-off with PVST, clean service is calculated as below [5].

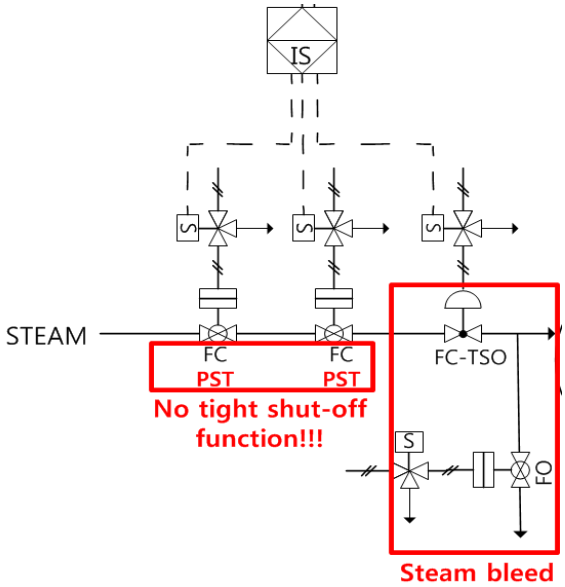


Fig. 7 The recommended P&ID with steam bleed line.

$$SFF = (\lambda S + \lambda Dd) / (\lambda S + \lambda Dd + \lambda Du)$$
$$= (\lambda Sd + \lambda Su + \lambda Dd) / (\lambda Sd + \lambda Su + \lambda Dd + \lambda Du)$$
$$= (0 + 0 + 271) / (0 + 0 + 271 + 958)$$
$$= 22\% \quad \text{-> SIL1 with HFT0}$$

IEC 61508 Failure Rates

Application	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}
Full Stroke, Clean Service	0 FIT	634 FIT	0 FIT	582 FIT
Tight Shut-Off, Clean Service	0 FIT	0 FIT	0 FIT	1229 FIT
Open on Trip, Clean Service	0 FIT	765 FIT	0 FIT	447 FIT
Full Stroke with PVST, Clean Service	0 FIT	634 FIT	273 FIT	309 FIT
Tight Shut-Off with PVST, Clean Service	0 FIT	0 FIT	271 FIT	958 FIT
Open on Trip with PVST, Clean Service	0 FIT	765 FIT	287 FIT	160 FIT
Full Stroke, Severe Service	0 FIT	1265 FIT	0 FIT	985 FIT
Tight Shut-Off, Severe Service	0 FIT	0 FIT	0 FIT	2264 FIT
Open on Trip, Severe Service	0 FIT	1515 FIT	0 FIT	731 FIT
Full Stroke with PVST, Severe Service	0 FIT	1265 FIT	477 FIT	508 FIT
Tight Shut-Off with PVST, Severe Service	0 FIT	0 FIT	476 FIT	1788 FIT
Open on Trip with PVST, Severe Service	0 FIT	1515 FIT	507 FIT	224 FIT

Table 2 — Hardware safety integrity: architectural constraints on type A safety-related subsystems

Safe failure fraction	Hardware fault tolerance		
	0	1	2
< 60 %	SIL1	SIL2	SIL3
60 % - < 90 %	SIL2	SIL3	SIL4
90 % - < 99 %	SIL3	SIL4	SIL4
> 99 %	SIL3	SIL4	SIL4

7.3 2 Out of 2 SOV for Availability

The 2 out of 2 SOV increase the operational availability. The 2 out of 2 SOV are configured as Fig. 8.

The prerequisite of 2 out of 2 SOV is that each SOV should meet SIL3. The below SOV certificate shows that one SOV can meet SIL3 [7].

TÜV

Certificate

Manufacturer: ASCO Controls BV
Industrielaan 21
3925 BD Scherpenzeel
Niederlande

Product Type: 3/2 Way Valves
...327 ...

Intended Use: Automatic Solenoid Valve with safety function

Test results:

- probability of failure of the safety function on demand PFD < 4 x 10^{-4} at a confidence interval of 95%
- The Safe Failure Fraction (SFF) according to Table A1, IEC61508-2 is greater or equal to 0.99.

The merits of 2 out of 2 SOV are as below.

- The partial stroke test is only for shutdown valve. SOV is easy to be stuck without full stroke test.
- There were several shutdown accidents by the dirt in the instrument air in Korea. The operational availability can be higher by 2 out of 2 SOVs.

7.4 Redundant HART Communication

The redundant HART communication increases the operational availability. Fig. 9 is the typical configuration of HART communication.

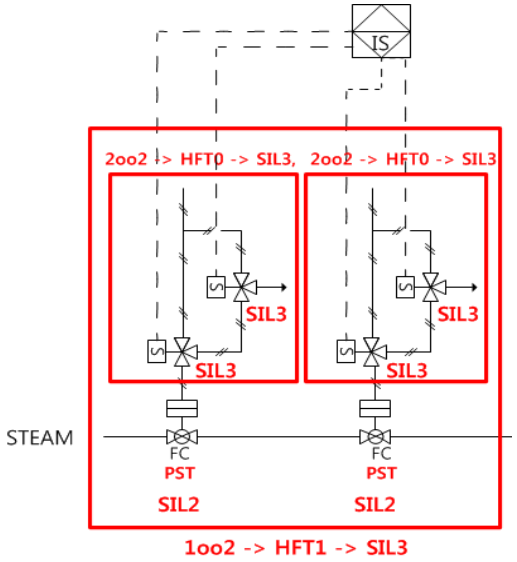
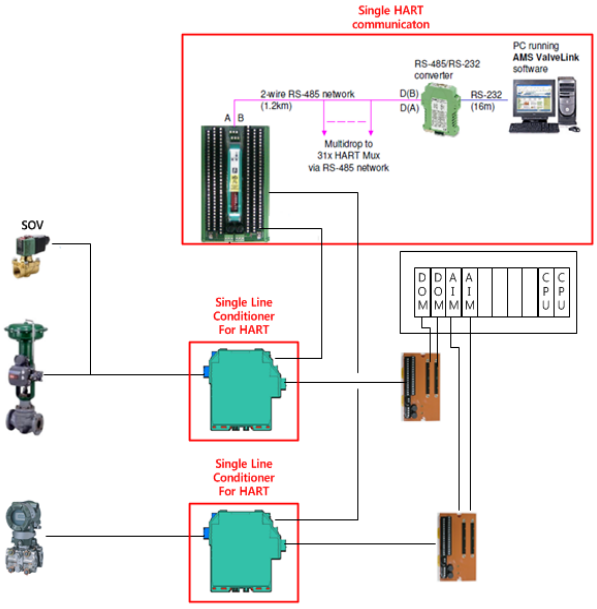


Fig. 8 The 2 out of 2 SOV configuration.



Glossary
AIM: Analog Input Module without HART function
AOM: Analog Output Module without HART function
DOM: Digital Output Module
CPU: CPU Module

Fig. 9 The typical configuration of HART communication.

The redundant HART communication can be configured as Fig. 10.

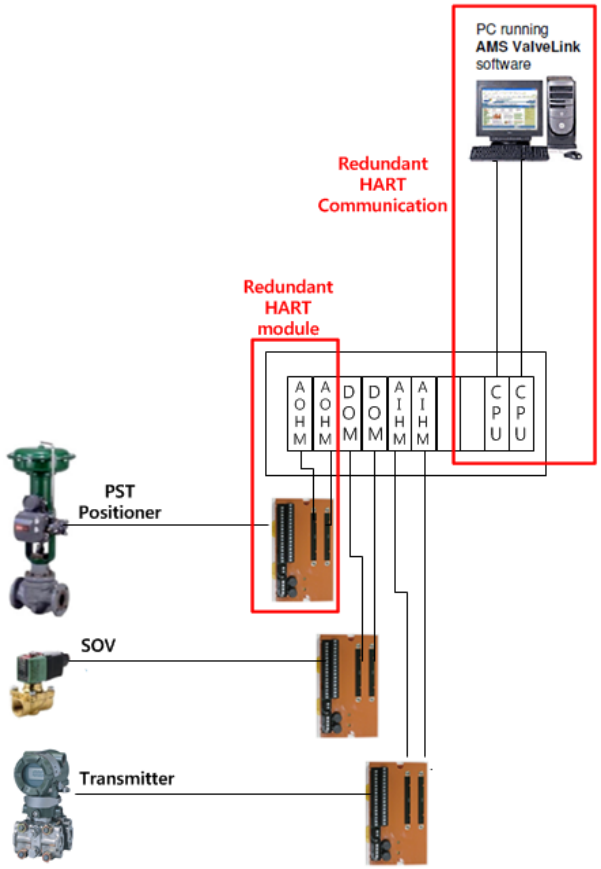
The redundant HART module increase the operational availability compared with the single external HART communication device.

7.5 HMI Integration

The integrated HMI (Human Machine Interface) between BPCS and SIS increase the operational availability of plant. Fig. 11 shows the integrated network between BPCS and SIS.

The merits of the integrated HMI are as below.

SIS alarm and status can be monitored on integrated HMI in case of BPCS controller failure.



Glossary
AIHM: Analog Input Module with HART function
AOHM: Analog Output Module with HART function
DOM: Digital Output Module
CPU: CPU Module

Fig. 10 The configuration of redundant HART communication.

The detailed alarms and status of SIS failure can be clearly monitored on HMI.

The status of SIS controller can be monitored on the integrated HMI as Fig. 12.

IEC 61511-1 recommend the monitoring of SIS status as below [8].

"11.7.4. The SIS status information that is critical to maintaining the SIL shall be available as part of the operator interface. This information may include the results of diagnosis."

7.6 The Integration of Recommendations about SIL3 Application

The integration of all recommendation on P&ID can be drawn as Fig. 13.

7.7 The Integration of Recommendations about SIL4 Application

The integration of all recommendation on P&ID for

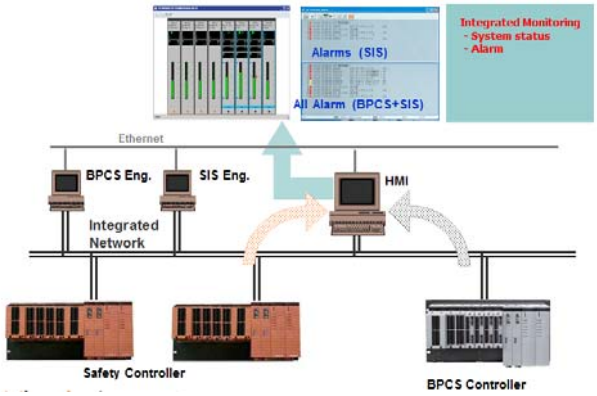


Fig. 11 The integrated HMI between BPCS and SIS.

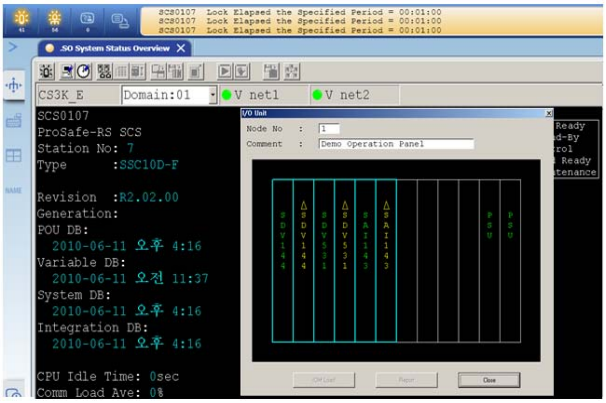


Fig. 12 The status of SIS controller on the integrated HMI.

SIL4 application can be drawn in Fig. 14.

SIL4 application is necessary in case that the existing flare stack load is much lower than the maximum flare load.

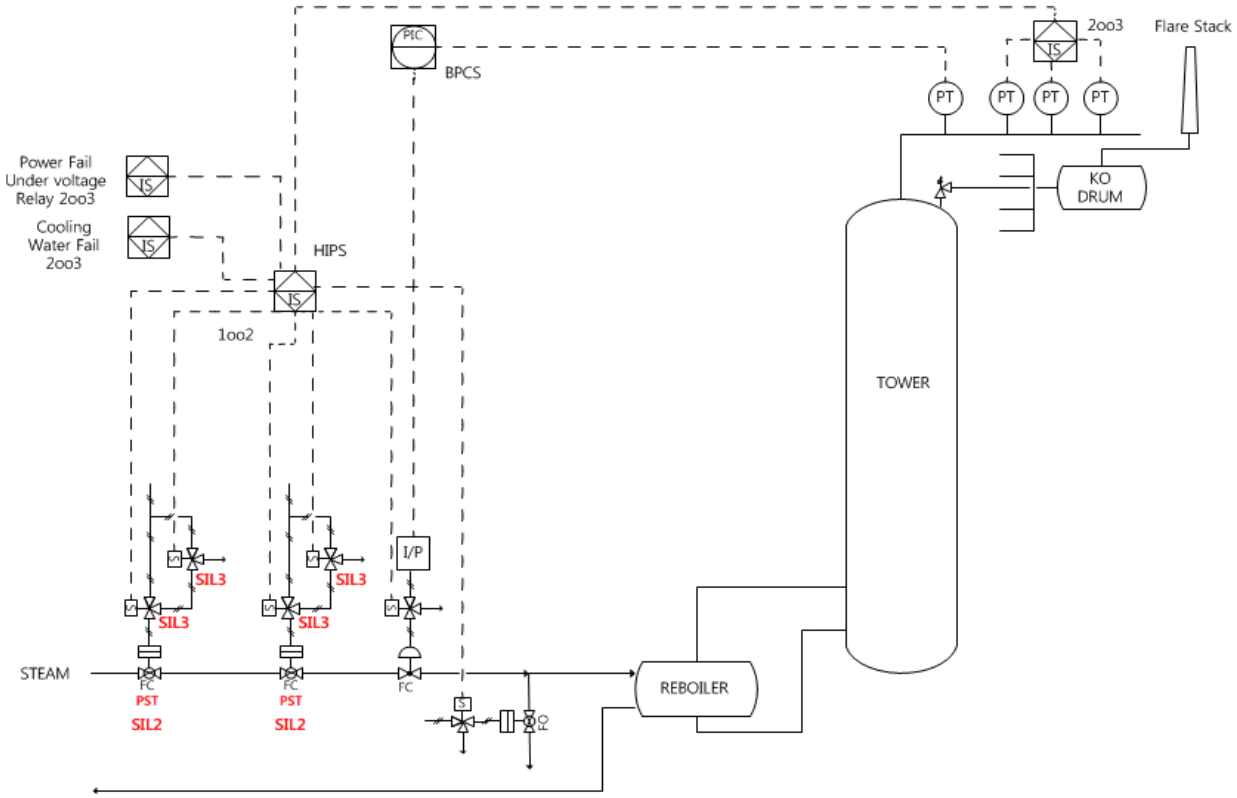


Fig. 13 The integration of all recommendations on P&ID.

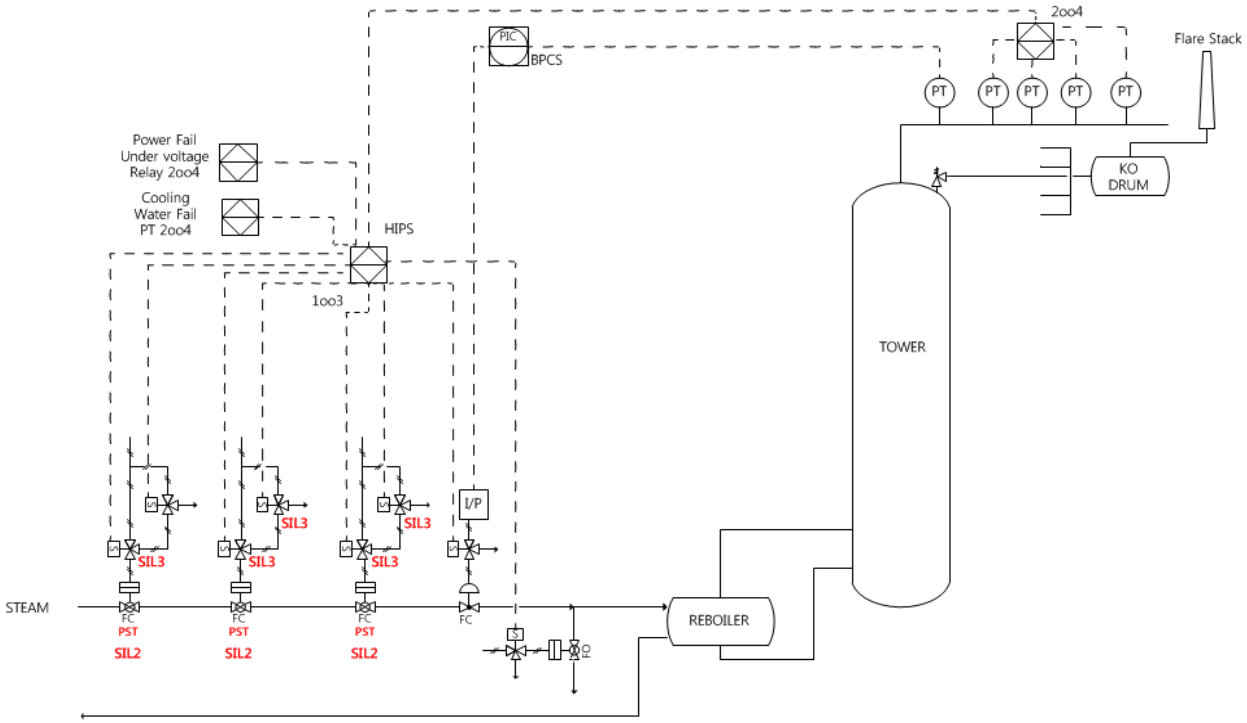


Fig. 14 The integration of all recommendations about SIL4 application on P&ID.

5. Conclusions

In this paper, the problems of the existing HIPS in Korea were analyzed based on the latest IEC61508 and IEC61511 and latest instrument technology. The valve separation between BPCS and SIS, steam bleed line, 2 out of 2 SOV, redundant HART communication, SIS status monitoring on HMI were highly recommended in this paper. There is no system with no failure rate in the world, so nobody can guarantee that the flare load from tower is 0 by HIPS theoretically. But the highest SIL (SIL4) is the best solution with lowest possibility to prevent flare load increase based on the latest technology developed so far. The incidents in relation with overpressure of tower show how much the HIPS application is important. HIPS is really important system to prevent the major incident of plant and the design development of HIPS is still on-going. For several years, the design criteria of HIPS is reinforced continuously so far and the HIPS design should be upgraded in future based on the better discussion about hazard and trials and errors during design.

Acknowledgments

The discussion about HIPS with Korea Gas Safety Corporation for several years was very helpful to write this paper. I would like to thank Korea Gas Safety Corporation.

This paper was presented at the 7th International Conference on Thin-Walled Structures, 19 September - 1 October 2014, Busan, Korea.

References

[1] Melhem, G. A. 2006. “Maximize the Use of Your Existing Flare Structures.” An ioMosaic Corporation Whitepaper.

[2] Korea Occupational Safety & Health Agency. 2007. *Main Review Contents during Inspection.* Technical Materials-Process Safety Report.

[3] Yokogawa Europe B.V. 2013. Details on Functional Safety, Safety Assurance and Consultancy.

[4] Certificate of UNI 090115 C001 from exida, TOD Series Triple Offset Design Valves, Korea Unicom Valve Co., Ltd.

[5] IEC 61508-2, Edition 2.0, 2010-04, Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/ programmable electronic safety-related systems.

[6] BS IEC 61511-2: 2003 Functional safety – Safety instrumented systems for the process industry sector – Part 2: Guidelines for the application of IEC 61511-1.

[7] TUV Certificate of ASCO Controls BV, 3/2 Way Valves.

[8] BS IEC 61511-1: 2003 Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements.