Proceedings of the 2nd Faculty of Industrial Technology International Congress
International Conference
Bandung, Indonesia, January 28-30, 2020
ISBN 978-623-7525-37-0

Safety Integrity Level (SIL) Study for HIPPS

Dzulfikar Ali Hafizh[1*], Dani Rusirawan[2], Ahmad Taufik[3], Deddy Nugraha[3]

[1] Under Graduate Student of Mechanical Engineering, Itenas, Bandung – INDONESIA

[2] Dept. of Mechanical Engineering, Itenas Bandung – INDONESIA

[3] Indonesian Society for Reliability (ISR)

[*]Corresponding author e-mail: dzulfikarahafizh@gmail.com

Abstract

A safety analysis is a type of study that examines system-level and related assets to determine loss of containment scenarios, identify risk levels, decide whether a safety instrumented system (SIS) is required, and define the provisions that protect against, or mitigate, loss of containment. Safety analysis is a key component of integrity management. Other components of integrity management include process design, alarm identification and management, protective devices, and community and plant emergency response plans. Together, these actions form a layer of protection around critical systems.

Keywords: safety integrity level, layer of protection, A high-integrity pressure protection system (HIPPS)

1. Introduction

James Reason's Swiss cheese model for process safety illustrates how major accidents and catastrophic system failures actually uncover multiple, smaller failures leading to an actual hazard. In the model, each slice of cheese represents a safety barrier for a particular hazard and that no single barrier is fool proof, each having 'holes.' When the holes align a catastrophic failure occurs, which can result in serious consequences. To protect ourselves from these holes, systems need to be properly managed, inspected and tested to verify their ongoing reliability. The procedure for defining this process needs to be documented and designs reviewed. A safety instrumented function (SIF) study assesses system risk, defines risk mitigation or elimination actions required to return the system to a safe state when conditions such as pressure or temperature reach a threshold level. An SIF detects a specific hazard and brings the process to a safe state. It provides a defined level of risk reduction or safety integrity level (SIL) for a specific hazard by automatic action using instrumentation.

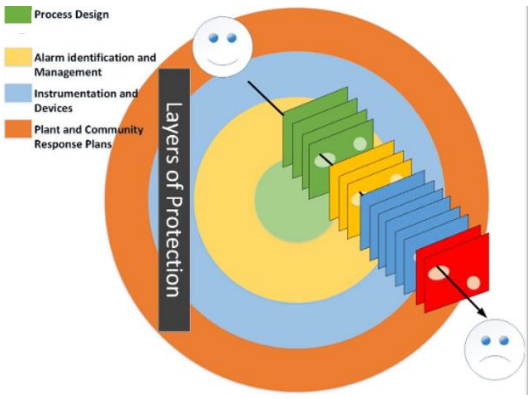

Fig. 2 Swiss Cheese Model

A high-integrity pressure protection system (HIPPS) is a type of safety instrumented system (SIS) designed to prevent over-pressurization of a plant, such as a chemical plant or oil refinery. The HIPPS will shut off the source of the high pressure before the design pressure of the system is exceeded, thus preventing loss of containment through rupture (explosion) of a line or vessel. Therefore, a HIPPS is considered as a barrier between a high-pressure and a low-pressure section of an installation.

HIPPS is a complete functional loop consisting of:

- sensors, (or initiators) that detect the high pressure
- a logic solver, which processes the input from the sensors to an output to the final element
- final elements, that actually perform the corrective action in the field by bringing the process to a safe state. In case of a HIPPS this means shutting off the source of overpressure. The final element consists of a valve, actuator and solenoids.

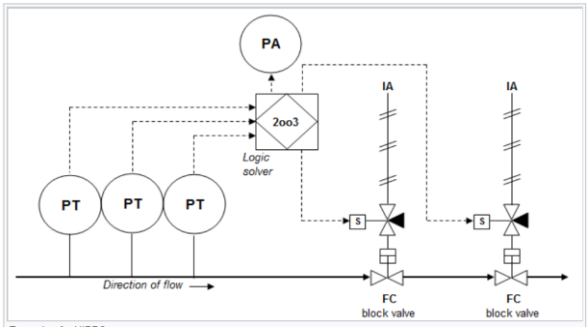

Fig. 3: HIPPS Configuration

The scheme above presents three pressure transmitters (PT) connected to a logic solver. The solver will decide based on 2-out-of-3 (2oo3) voting whether or not to activate the final element. the 1oo2 solenoid panel decides which valve to be closed. The final elements consist here of two block valves that stop flow to the downstream facilities (right) to prevent them from exceeding a maximum pressure. The operator of the plant is warned through a pressure alarm (PA) that the HIPPS was activated. This system has a high degree of redundancy:

- failure of one of the three pressure transmitters will not compromise the HIPPS functionality, as two readings of high pressure are needed for activation.
- failure of one of the two block valves will not compromise the HIPPS functionality, as the other valve will close on activation of the HIPPS.

2. Standards and Design Practices

2.1 IEC 61508 & IEC 61511

The International Electrotechnical Commission (IEC) has introduced the IEC 61508 and the IEC 61511 standards in 1998 and 2003. These are performance based, non-prescriptive, standards which provide a detailed framework and a life-cycle approach for the design, implementation and management of safety systems applicable to a variety of sectors with different levels of risk definition. These standards also apply to HIPPS.

The IEC 61508 mainly focuses on electrical/electronic/programmable safety-related systems. However, it also provides a framework for safety-related systems based on other technologies including mechanical systems. The IEC 61511 is added by the IEC specifically for designers, integrators and users of safety instrumented systems and covers the other parts of the safety loop (sensors and final elements) in more detail.

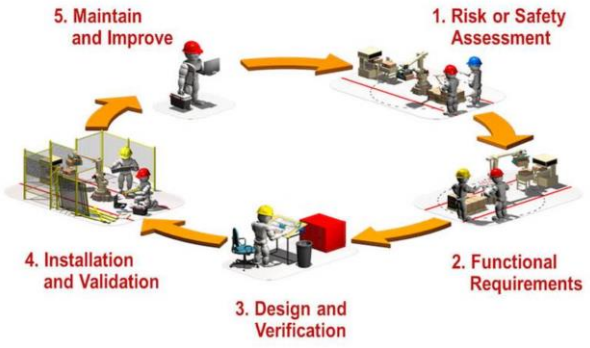

Fig. 4: Safety Life Cycle

The basis for the design of your safety instrumented system is the required Safety Integrity Level (SIL). The SIL is obtained during the risk analysis of a plant or process and represents the required risk reduction. The SIS shall meet the requirements of the applicable SIL which ranges from 1 to 4. The IEC standards define the requirements for each SIL for the lifecycle of the equipment, including design and maintenance. The SIL also defines a required probability of failure on demand (PFD) for the complete loop and architectural constraints for the loop and its different elements.

In laymen terms, SIL basically classifies your plant by its probability to detect dangerous failures that might lead to injuries, fatalities or a catastrophic disaster.

SIL1 your plan could fail to detect danger once in 10 times to 100 times. (0.1% to 0.01% fail on demand)

SIL2 your plan could fail to detect danger once in 100 to 1000 times (0.01% to 0.001% fail on demand)

SIL3 your plan could fail to detect danger once in 100 to 1000 times (0.001% to 0.001% fail on demand)

SIL4 your plan could fail to detect danger once in 100 to 1000 times (0.0001% to 0.00001% fail on demand)

Table 6 Relation Between SIL, PFD, and RRF

Safety Integrity Level	Risk Reduction Factor	Probability of Failure on Demand
SIL 4	100,000 to 10,000	10^{-5} to 10^{-4}
SIL 3	10,000 to 1,000	10^{-4} to 10^{-3}
SIL 2	1,000 to 100	10^{-3} to 10^{-2}
SIL 1	100 to 10	10^{-2} to 10^{-1}

2.2 Layer of Protection Analysis (LOPA)

Layer of Protection Analysis (LOPA) is a risk management technique commonly used in the chemical process industry that can provide a more detailed, semi-quantitative assessment of the risks and layers of protection associated with hazard scenios.

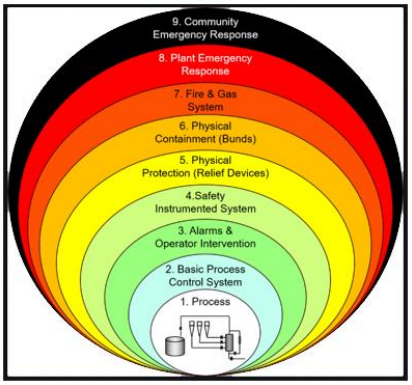

Fig. 5: Layer of Protection Analysis (LOPA)

LOPA combines both qualitative and quantitative elements of hazard evaluation and risk assessment to analyze and judge the adequacy of existing or proposed safeguards against process deviations and accident scenarios. A key to the success of LOPA is its rules for judging if protection layers are truly independent. Because of these rules, LOPA helps the analysts make consistent judgments of if the risk of scenarios are “as low as reasonably practical (ALARP)”.

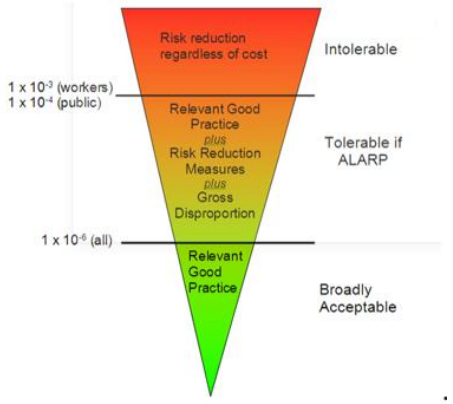

Fig. 6: As Low as Reasonably Practical (ALARP)

3. Methodology

In this model, it is assumed that a control system controls some equipment that has associated high-level safety requirements. These high-level requirements generate two types of more detailed safety requirements that apply to the protection system for the equipment:

- Functional safety requirements that define the safety functions of the system
- Safety integrity requirements that define the reliability and availability of the protection system. These are based on the expected usage of the protection system and are intended to ensure that it will work when it is needed. Systems are classified using a safety integrity level (SIL) from 1 to 4. Each SIL level represents a higher level of reliability; the more critical the system, the higher the SIL required.

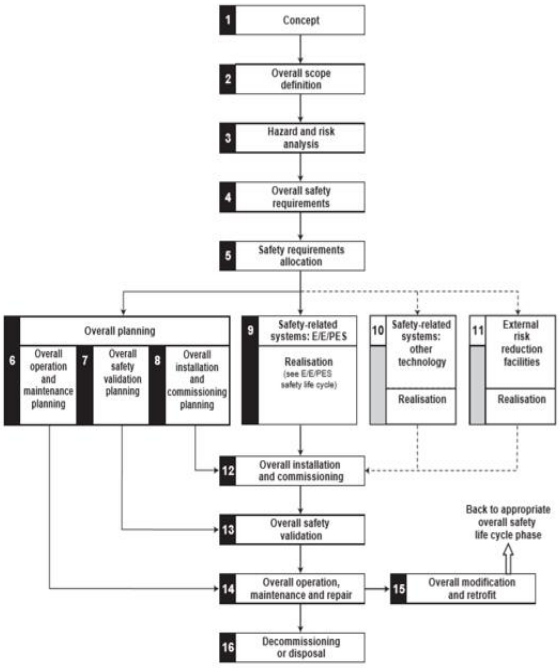

Fig. 7: Safety Life Cycle Based on IEC 61508

The first stages of the IEC 61508 safety life cycle define the scope of the system, assess the potential system hazards and estimate the risks they pose. This is followed by safety requirements specification and the allocation of these safety requirements to different sub-systems. The development activity involves planning and implementation. The safety-critical system itself is designed and implemented, as are related external systems that may provide additional protection. In parallel with this, the safety validation, the installation, and the operation

and maintenance of the system are planned.

4. Verification HIPPS

Overall safety requirement system HIPPS defined SIL 3

SIF configuration refer to figure 2 HIPPS

$PFDavg\ sensor\ (1oo1) = 1.6206x\ 10^{-4}$ (in 1 year)

$PFDavg\ sensor\ (2oo3) = 2.431\ x\ 10^{-5}$ (in 1 year)

$PFDavg\ logic\ solver = 5\ x\ 10^{-4}$ (in 1 year)

$PFDavg\ actuator\ (1oo1) = 9.417x\ 10^{-4}$ (in 1 year)

$PFDavg\ actuator\ (1oo2) = 4.743\ x\ 10^{-5}$ (in 1 year)

$PFDavg\ valve\ (1oo1) = 4.038\ x\ 10^{-8}$ (in 1 year)

$PFDavg\ valve\ (1oo2) = 2.02\ x\ 10^{-9}$ (in 1 year)

$PFDavg\ system = PFDavg\ sensor + PFDavg\ logic + PFDavg\ final\ element$

$= 5.243\ x\ 10^{-4}$ (in 1 year)

This value presented that probability of failure on process will occur once per 5204 years. Therefore, with minimum required system SIL 3 for HIPPS, this configuration meet the requirement that said PFD_{avg} must be in range $10^{-4} – 10^{-3}$. In this study, we can conclude that HIPPS is qualified for SIL 3 as required.

5. Conclusions

This study is aimed to implement safety integrity level on safety instrumented function based on IEC 61508/61511. In this study, we can conclude that:

- HIPPS met the minimum required SIL 3 because it lays within the determined range.
- To maintain HIPPS consistanly on SIL 3, inspection and test or maintenance activity should be conducted every 3 years align with re-certification program set up by Indonesian Oil & Gas Authority (MIGAS).

6. References

Marszal, E.M., & Scharpf, E.W. (2002) *Safety Integrity Level Selection: Systematic Methods Including Layer of Protection Analysis.* New York: ISA–The Instrumentation, Systems, and Automation Society

Gulland, W.G. (2004, Februari) *Methods of Determining Safety Integrity Level (SIL) Requirements - Pros and Cons*. Article posted on *International Symposium on Safety Science and Technology*, Boston: *Elsevier*.

Ingrey, A., Lerévérend.P (2005) *SIL IEC 61508/61511 Edition 2005, Manual Safety Integrity Level*

Willey, J.R. (2014, Desember) *Layer of Protection Analysis*. Artikel dipublikasi dalam *The Proceedings of the Safety-Critical Systems Symposium*, London, Springer-Verlag London Ltd.