HAZOP과 안전성 수준(SIL) 평가의 동시 수행에 관한 연구

류정현, 윤난희, 김종훈*, 조원희**
ABS Consulting, 대우건설*, 삼성엔지니어링**

A Study on Combination of HAZOP and SIL Determination

Jueng Hyun Ryu, Nan Hee Yoon, Jong Hun Kim*, Won Hee Cho**
ABS Consulting, Daewoo E&C*, Samsung Engineering**

Abstract

HAZOP study is rigorous, multidiscipline method to check P&ID's using guide words and parameters to identify the possible causes and effects of potential hazards, and to identify design efficient features to mitigate potentially hazardous conditions by analyzing all possible deviation from the design intent. SIL determination is the activity for reviewing whether specific SIS protection layer is needed to achieve the required SIL (Safety Integrity Level) or not. By appropriate HAZOP discussion and proper recording considering SIL process, the combination concept of HAZOP and SIL determination study shall give 1) minimizing the over or under SIL level, 2) maintaining the consistency, and 3) getting more discussion time within given schedule.
Keyword: HAZOP (Hazard and Operability), SIS (Safety Instrumented System), SIL (Safety Integrity Level), SIF (Safety Instrumented Function), IPL (Independent Protection Layer)

1. Introduction

The goal of process plant design is to accomplish the chemical transformation through reaction or physical alteration or separation of material for the design capacity, quality of product at inherently safe process. Various inherent safe design approach, process hazard analysis (PHA), and risk assessment are conducted to prevent and/or mitigate the risk through overall facility lifecycle from basic engineering stage to decommissioning stage.

HAZOP (Hazard and Operability) Study is one of the most commonly used hazard identification tool to identify hazard and operability problem that may be faced during the various facility operation mode (normal operation, startup, shutdown, part operation, maintenance, etc.).

SIL determination study is conducted to allocate of safety functions to specific protection layer during SIS conceptual phase and to allocate the proper Safety Integrity Level (SIL) to safety instrument function (SIF) of safety instrumented system (SIS).

The study team member of HAZOP and SIL Review is similar, but, in case, the HAZOP and SIL Review are requested to conduct at separated timing. During the detail engineering phase, it is hard to arrange the engineers from licensor, owner, operating company, and detail engineering company to make presence on HAZOP session and SIL determination study session both. By this reason, I studied the HAZOP and SIL review study to propose an effective way to combine HAZOP and SIL determination study effectively for detail engineering stage.

2. Overview of HAZOP methodology

In process industry, HAZOP Study is conducted for identification of significant hazards on P&ID using process safety information (e.g. Process Flow Diagram, Heat and Material Balance, Plot Plan, Chemistry, interlock description) that need to be mitigated by additional safeguards or by modification to basic design to reduce the residual risk to acceptable level. The HAZOP methodology has originated in 1960's by ICI (Imperial Chemical Industries) which was a British chemical company.

HAZOP studies are a rigorous, multidiscipline check of P&ID's using guide words and parameters to identify the possible causes and effects of potential hazards, and to identify design efficient features to mitigate potentially hazardous conditions by analyzing all possible deviation from the design intent.

HAZOP study will be carried out in the various design phase of the facility project. HAZOP team may reveal the potential hazards and operational difficulties at each design stage.

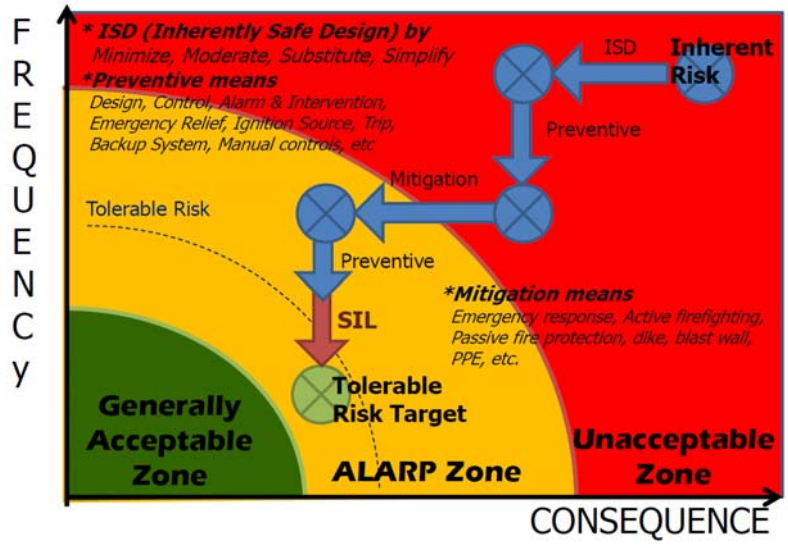
3. Overview of SIL Determination Methodology

For process industry sector the SIL Determination is conducted to determine the Safety Integrity Levels for each safety function in accordance with IEC 61511-3 (Guidance for the determination of the required safety integrity levels).

IEC-61511-3 Section 3.5 states that;

"Risk is a measure of the frequency and consequence of a specified hazardous event occurring. This can be evaluated for different situations (process risk, tolerable risk, residual risk). The tolerable risk involves consideration of societal and political factors. Safety integrity is a measure of the likelihood that the SIF and other protection layers will achieve the specified safety functions. Once tolerable risk has been set, and the necessary risk reduction estimated, the integrity requirements for the SIS can be allocated."

Figure1. Risk Reduction vs. Safety Integrity Level based on LOPA Concept



IEC 61511-3 provides a number of required SIL determination methods. In process industry, the selection of methods is generally depending on the Plant Owner's Engineering Standard. Nowadays many Plant Owner, safety engineer, and EPC Contractor prefer the LOPA method, while some favor the Safety layer matrix method. When Risk Graph method is used for the SIL Determination, protection layers which may effective to prevent the hazardous event are identified to allocate the proper SIL level in safety instrumented system.

Table1. SIL Determination method in accordance with IEC 61511-3

Method	Key Elements
Semi-Quantitative method	Numerical Process Safety Target per year, Hazard and Risk Assessment, Frequency of occurrence. Reliability of existing safety systems using Fault Tree Analysis or Markov Modeling
Safety Layer Matrix method	Process Safety Target (Risk Matrix), Safety Layer Matrix, Hazardous event likelihood and severity rating, existing PL (Protection layers) be applied.
Calibrated Risk Graph method	Numerical value to risk graph parameter which is more suited to the process industry. * Note: Generally not recommended because it can lead to an over-estimation of the effectiveness of the SIS
Risk Graph method	Risk Graph described in DIN V 19250 and VDI/VDE 2180 which has been accepted by the TÜV and German regulating authorities for process industry and the machinery sector.
Layer of Protection Analysis (LOPA)	LOPA described in "Guidelines for Safe Automation of the Chemical Processes, AIChE, CCPS". Risk Tolerable Criteria, Initiating Cause, Independent Protection Layer (IPL), Condition Modifier.

3. Comparison HAZOP methodology and SIL Overview of SIL Determination Methodology

To make an approach of combine HAZOP and SIL determination study at same session at detail engineering phase, the similarity and difference of HAZOP and SIL method are reviewed.

3.1 Study Timing

HAZOP study is carried out in the various design phase of the facility project. At detail engineering phase, the full line-by-line HAZOP is started after issuing of IFD (Issue for design) P&ID.

In accordance with ANSI/ISA-84.00.01, "Hazard & Risk Analysis" and "Allocation of Safety layers" shall be conducted before finalizing the process control & protection philosophy, then preliminary P&ID shall be developed. This means SIL determination study is recommended to be conducted during early stage of process development (e.g. Front-End Engineering Design Phase or Basic Engineering Design Phase), but, in many process facility project, assignment of SIL level on SIF is responsibility of Detail Engineering Company. Generally SIL determination study is requested to conduct after detailed HAZOP study. IEC 61511-3 briefly mentions that performance of hazard identification is part of SIL level determination process.

There is no restriction or requirement whether the HAZOP and SIL study can be combined or be conducted separately.

3.2 Study Team Composition

HAZOP team and SIL Determination team is composed with similar key member, but the qualification of SIL Facilitator is different from HAZOP Team Leader. There is no required certification for HAZOP leader. Generally, the key requirement for HAZOP leader is sufficient process hazard analysis knowledge, minimum 10 year, with a number of HAZOP leading experiences. For SIL facilitator, it is strongly recommend having a certificate of functional safety engineering from TÜV, or equivalent. SIL facilitator also shall have plenty process hazard knowledge.

When qualified SIL facilitator has a sufficient HAZOP experience, it is not a problem to execute using combined of HAZOP and SIL review with study team member.

3.3 Documentation for Study at detail engineering phase

Table2. Process Safety Information for HAZOP and SIL Determination

	HAZOP Study	SIL Determination Study
Key Document	P&ID (Piping and Instrumentation Diagram) HAZOP Node List	SIS interlock description or equivalent SIF List
Secondary Document, but not limited	Shutdown and Control Narratives Distributed Control System (DCS) Cause and Effect Diagram, or equivalent SIS interlock description or equivalent Process Flow Diagram (PFD) Heat and Material Balance Material Safety Datasheets (MSDS)	Shutdown and Control Narratives P&ID (Piping and Instrument Diagram) Process Flow Diagram (PFD) Heat and Material Balance Material Safety Datasheets (MSDS)

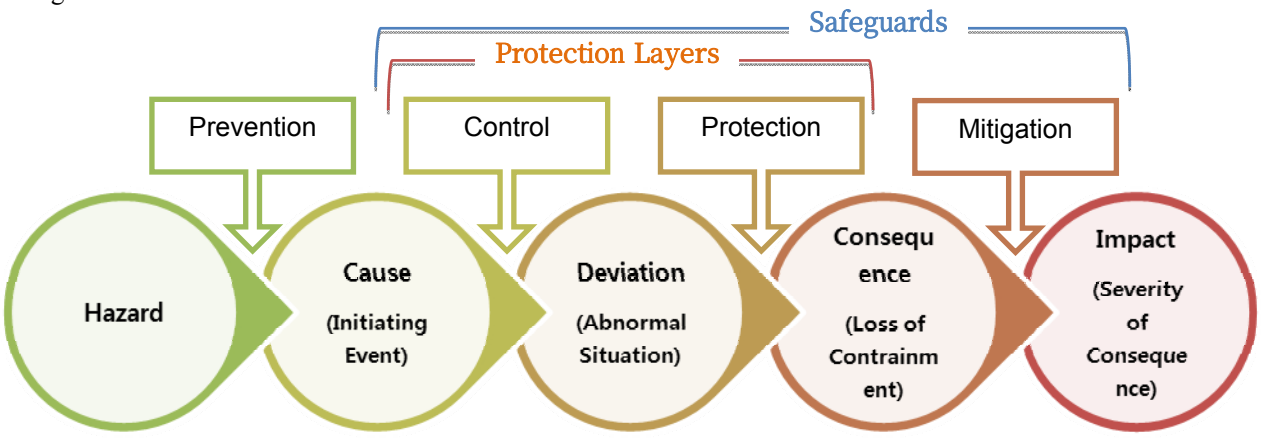
There is no difference of documentation preparation for HAZOP study and SIL determination except SIF List and HAZOP Node list. This means SIL determination study and HAZOP study can be conducted at the same study session.

3.4 Study Worksheet

HAZOP is structured logical exercise by combining guide words and process & operating parameters in order to identify potentially hazardous situations in terms of causes, effects, and safeguards, then results are recorded accordingly. The general procedure of SIL Determination study is performing hazard identification, identifying existing independent protection layer and identifying the need for additional SIS protection layer and assigned required SIL level, then records the study results.

In HAZOP study any of control *(e.g. BPCS, manual control, backup system)*, protection *(e.g. alarm, operator intervention, DCS interlock, SIS, emergency relief system)*, mitigation *(e.g. emergency response, active firefighting, passive fireproofing, dike, drainage system, blast wall, blast building, PPE)* measures shall be reviewed and recorded in HAZOP worksheet. On the contrary, SIL determination ONLY focuses on IPL (independent protection layer) within several protection layers which can give a credit on SIL level.

Figure 2. Structure of an Incident/ Accident



To be an IPL, the protection layer shall meet IPL restriction requirements. Layer of Protection Analysis, CCPS of AIChE, says that IPL is "a device, system, or action that is capable of preventing a scenario from proceeding to the undesired consequence regardless of the initiating event or the action of any other protection layer associated with the scenario. Independent means the performance of the protection layer is not affected by the initiating event and is not affected by failures of other protection layers. The effectiveness and independence of an IPL should be auditable."

Table3. Example HAZOP Worksheet

Node: 31. Mixed Butanol from Butanol Refining Column to Mixed Butanol Drum Drawings / References: 130162-PID-2120-0032; 130162-PID-2120-0037 Design Intent: The bottom of the Mixed Butanol Drum is pumped to the Butanol Isomer Column by the Butanol Isomer Column Feed Pump.							
Deviation	Cause	Consequence	Safeguard	Risk Ranking			Recomm.
Deviation	Cause	Consequence	Safeguard	S	L	RR	
No/Less Flow	FV-2001 malfunction	Increase in level in D-2001. This may lead to potential over filling and high pressure due to blocked condition and damage and spillage. Potential pool fire and personal injury.	1. LAH-2002A/B/C on D-2001 2. LAHH-2002 A/B/C with interlock SIS-10A to stop LPG flow to D-2001. 3. PSV-2001 and sized for liquid overfill. (IPL)	S4 E1	2	4 1 2	-

Table4. Example LOPA Worksheets for SIL Determination

Function: Initiator: SIS-10A (Overfilling Protection of Feed Surge Drum D-2001 on very high level) Initiator(s): LSHH-2002 A/B/C (2oo3) Primary F.E(s): UV-2001 (1oo1) Secondary F.E(s): Noe										
Initiating Cause	Consequence Description	Consequence Category	RTC	IE Likelihood	IPLs	CM	Comments for IPL, CM	IEL	LR	Req. SIL
FV-2001 malfunction	Increase in level in D-2001. This may lead to potential over filling and high pressure due to blocked condition and damage and spillage. Potential fire and personal injury.	Safety 4	1E-5	0.1	PSV-2001 (0.01)	0.5	PSV-63001 sized for liquid overfill. Occupancy 0.5 assumed.	5E-4	2E-2	SIL 1

RTC: Risk Tolerable Criteria, IE: Initiating Event, CM: Conditional Modifier, IEL: Intermediate Event Likelihood, LR: LOPA Ratio

Key discussions during SIL determination study are 1) identifying all potential "initiating causes", 2) assume "consequence", and 3) finding proper "Independent Protection Layers".
The many of these discussions are already discussed during HAZOP session.

Table5. Evaluation of LOPA clause compare to HAZOP clause

LOPA Clause	Utilizing the HAZOP Clause	Remark
Function	Part of "Safeguard"	SIF List
Initiator/ Final Elements	N/A	SIF List
Initiating Cause	Extracte from "Cause"	
Consequence Description	"Consequence"	
Consequence Category	Copy from "Severity of Risk Ranking"	
Risk Tolerable Criteria (RTC)	N/A	As per SIL Procedure
Initiating Event (IE) Likelihood	N/A	As per SIL Procedure
IPL (Independent Protection Layer)	Selected among "Safeguard"	
Conditional Modifier (CM) for ignition, occupancy, fatality	N/A	As per SIL Procedure
Comments for IPL, CM	N/A	Application notes
IEL (Intermediate Event Likelihood)	N/A	Mathematical formula
LOPA Ratio	N/A	Mathematical formula
Required SIL	N/A	As per SIL Procedure

4. Recommendation for combining the HAZOP and SIL Study

4.1 The combined HAZOP and SIL Procedure

The combined HAZOP and SIL procedure shall be fully compliance with selected SIL determination procedure and risk criteria. When **LOPA** is used for combined HAZOP/ SIL study, RTC (Risk Tolerable Criteria) for each severity level shall be developed and included in the procedure. When **Safety Layer Matrix** is used for combined HAZOP/SIL study, study team shall have understanding that likelihood in HAZOP is differ from hazardous likelihood of event of SIL Study. In HAZOP, likelihood is decided considering all existing safeguard. In the contrary, hazardous event likelihood is the likelihood that the hazardous event occurs without any of the IPLs in service. By this reason, generally likelihood in HAZOP report cannot directly utilized for SIL hazard event likelihood. When **Risk Graph method** is proposed, risk reduction concept by applying IPL may be considered in SIL procedure to minimize an over or under design of SIS.

4.2 Qualified safety leader

Qualified safety leader (or chairman or facilitator) MUST be selected for combined HAZOP and SIL determination study. Unqualified lead shall destroy the safety study.
Proposed qualification conditions for the safety leader are;

- Sufficient process hazard analysis knowledge, minimum 10 year, with a number of HAZOP leading experiences.
- Quite a number of SIL session and SIL facilitating experience
- Trained for functional safety and/or IEC 61508/ 61511 and/or ANSI/ISA S84.01
- Recommend having a certification for functional safety engineering from TÜV or equivalent.

4.3 Safety brain storming during HAZOP discussion

For easier and effective utilizing HAZOP discussion, following shall be considered during HAZOP recording.

- **Consequence**: Credible Consequence outcomes (e.g. pool fire, explosion, toxic gas release) with its severity impact (e.g. injury, fatality) shall be discussed and recorded in "Consequence part" during HAZOP. *[Example: Increase in level in D-2001. This may lead to potential over filling and high pressure due to blocked condition and damage and spillage. Potential pool fire and personal injury.]*
- **Safeguard**: Safeguard can be classified into general safeguard and IPLs which can reduce the magnitude of required SIL level. The Safeguard which can be IPL is recommended to have indicator. (e.g. [I] or [IPL]) *[Example: PSV-2001 and sized for liquid overfill. (IPL)]*
  When SIS is part of HAZOP safeguard, the identification number (e.g. SIS-10A) with initiator tag (e.g. LAHH-2002 A/B/C) shall be recorded in worksheets.

[Example: LAHH-2002 A/B/C with interlock SIS-10A to stop LPG flow to D-2001.]

- Severity: Credible Severity level for category (e.g. personnel safety, environment) shall be decided for directly usage during SIL. *[Example: Safety 4, Environment 1]*

4.4 Timing for SIL discussion

Timing for SIL Classification discussion shall be decided by HAZOP/SIL team's preference.

Option1: Many Company wants to start the SIL discussion immediately after completion of HAZOP session.

Option2: While other Company prefers to assign the SIL level on SIF when specific SIF is identified in HAZOP safeguards. When this approach is selected by HAZOP/SIL team, it is recommended that SIL assignment shall be started after finishing the relevant HAZOP node.

4.5 Tips for SIL Discussion

The safety leader shall prepare SIF List which includes the SIS interlock number, SIS function description, SIS initiator(s), and the SIS Final elements(s). Using the SIF list, the safety leader shall check the SIF whether all SIFs are reviewed or not.

- **Copy & Paste from HAZOP into SIL Review**: All HAZOP causes having SIS Interlock as safeguard shall be listed as "Initiating Cause" in SIL Review part. The search function of software package is very helpful to find out these HAZOP causes (e.g. FV-2001 malfunction, LV-2201 fail-closed).

  Then, copy all relevant Consequence, Severity and its category, marked IPLs from that HAZOP cause into SIL Part.

- **IPLs**: The study team shall carefully review the IPLs and give a credit as per defined rule set. During SIL process, the team may find the new IPL which is not mentioned during HAZOP discussion. This new IPL should be added into HAZOP part.

5. Conclusion

By appropriate HAZOP discussion and proper recording considering SIL process, the combination of HAZOP and SIL determination study gives several benefits to the study team.

- ✓ Quality: By reviewing of all HAZOP causes, over or under estimation of SIL Level for SIF can be minimized.
- ✓ Consistency: By conducting the study by same study team at the same period, discussion of the process hazard and risk analysis shall have consistency between HAZOP and SIL.
- ✓ Schedule: By directly referring of HAZOP discussion for Initiating Cause, Consequence, IPLs, discussion time for SIL determination can be considerably reduced. By this, all parties including Company, Licensor, and engineering company shall have more time for detailed process hazard discussion within given schedule.

References

1. IEC 61508 Functional Safety of Electrical/ Electronic/ Programmable Electronic Safety-Related System (E/E/PE), 2003, IEC
2. IEC 61511 Functional safety – Safety Instrumented System for the Process Industry Sector, 2003, IEC
3. ANSI/ISA-S84.01 Application of Safety Instrumented Systems for the Process Industries, 1996, ISA
4. Safety Instrumented Systems: Design, Analysis, and Justification, 2nd Edition, ISA
5. Layer of Protection Analysis – Simplified Process Risk Analysis, 2001, CCPS of AIChE
6. Victor H. Edwards, P.E., Aker Solutions, Designing SAFER Process Plant, Journal of Chemical Engineering, 44-48 page, April, 2011
7. Practical SIL Target SIL Target Selection – Risk Analysis per the IEC 61511 Safety Lifecycle, 2012, Exida.com LLC