

IDENTIFYING REQUIRED SAFETY INSTRUMENTED FUNCTIONS FOR LIFE SAFETY SYSTEMS IN THE HIGH- TECH AND SEMICONDUCTOR MANUFACTURING INDUSTRIES

Michael D. Scott, P.E.
Principal Safety System Specialist
AE Solutions
P.O. Box 26566
Greenville, SC 29616

Ken O'Malley, P.E.
Principal Control System Specialist
AE Solutions
P.O. Box 26566
Greenville, SC 29616

KEYWORDS

ANSI / ISA S84.01, Safety Instrumented Systems, Safety Instrumented Functions, Safety Integrity Levels, Life Safety Systems

ABSTRACT

This paper will discuss the issues, decisions, and challenges encountered when attempting to initially apply the concepts of the Safety Lifecycle per ANSI / ISA S84.01 to the design of a Life Safety System at a state of the art fiber optic manufacturing facility. More specifically, the methodology / procedures utilized for identification of Safety Instrumented Functions (SIF) and subsequent Safety Integrity Level (SIL) determination will be discussed in detail. In addition, industry specific issues associated with the design of Life Safety Systems and the use of mitigation versus prevention techniques (typically encountered in the process industry) will also be discussed.

INTRODUCTION

Standard design practices for the high-tech industry involve the inclusion of a Life Safety System. A Life Safety System is typically designed to protect personnel by isolating sources of specialty chemicals through the shutdown of equipment and / or machines. Many of these chemicals pose a flammable, corrosive and /or toxic hazard to personnel and / or the environment. A Life Safety System is typically comprised of some combination of toxic and / or combustible gas analyzers, other means to detect loss of containment of specialty chemicals, shutoff valves, Fire Detection system interface(s), HVAC interface(s), Basic Process Control System (BPCS) interface(s), emergency stop(s), as well as, personnel

warning / alarm initiating devices. Thus, a Life Safety System contains systems designed to prevent hazards, as well as, systems designed to mitigate the consequences after the hazard has occurred.

To effectively reduce a facility's risk a methodology / procedure was developed following the concepts of the Safety Lifecycle as outlined in ANSI / ISA S84.01. This procedure provided a means for the project team to analyze a hazard, quantify the associated risk, assign a Safety Integrity Level, and ultimately establish the design requirements for the Life Safety System. This paper will expand upon the methodology / procedures developed for a client to identify a Safety Instrumented Function, perform risk ranking, analyze layers of protection and if necessary assign a Safety Integrity Level.

PROJECT HISTORY

The fiber optic manufacturing facility had under taken an initiative to increase production through the design and construction of a new manufacturing line. The project design basis was to "copy" the design of a previous production line in an attempt to get product to market at the lowest cost. Design efforts were initiated and the project proceeded through conceptual process design and a Process Hazards Analysis.

In parallel with the project design efforts, the client's EH&S and Engineering staff began evaluating the company's existing design basis for Life Safety Systems and their compliance with the latest industry codes and standards. The process itself is a combination of discrete manufacturing utilizing individually operated machines and a continuous chemical process utilizing the concepts of bulk storage and distribution of a variety of toxic / flammable gases and liquids. The entire facility is maintained in a clean room environment with strict environmental requirements associated with scrubbing of exhaust air. With operators present at machines and a chemical distribution system piped throughout the facility a large gas detection system was typically installed. This blend of machine discrete manufacturing, chemical processing, and gas detection / annunciation left the team with a multitude of codes and standards to review with respect to the design of a Life Safety System.

During this code review process the team concluded that the design of the Life Safety System itself would be implemented by piecing together key requirements from a variety of codes and standards (i.e. SEMI, NFPA, IEC, etc). However, the requirement to design the overall system architecture based upon an established Safety Integrity Level as defined within ANSI / ISA S84.01 was determined to be the best overall design approach for the company. Based upon this decision, it was determined that site-specific engineering standards needed to be upgraded to ensure compliance, minimize risk and maximize production. The team presented two options to management. Option one was to proceed with the existing design and recognize that the Life Safety System would probably not be in compliance and would require additional funding for re-work shortly after construction was completed. The second option was to aggressively develop a new company standard while also applying these new requirements to the new manufacturing line project, in an attempt to limit future wholesale re-work of the Life Safety System. Management decided to proceed with option two.

The company immediately set forth in developing a procedure / methodology for SIL selection as their previous work processes did not output this information. A procedure was developed with the goals of

compliance with applicable regulations, consideration of the practices of industrial peers, conformance with the recommendations of applicable standards, and consistency with current facility risk ranking schemes used in previously conducted Process Hazard Analysis (PHA) studies.

GUIDELINE FOR THE SELECTION OF SAFETY INTEGRITY LEVELS

The team considered several different SIL selection methodologies. These included the following:

- Risk Matrix
- Layer of Protection Analysis
- Fault Tree
- Risk Graph

The Risk Graph methodology as contained in IEC 61508 Part 7 was ultimately selected as the “best” for the client as it could be easily integrated with the existing PHA procedures, provided a speedy means to evaluate a large number of Safety Instrumented Functions, and included a means to consider several key parameters (severity, likelihood, occupancy, avoidance).

SIL SELECTION PROCEDURE

The SIL Selection process was performed using the risk graph technique in a systematic team approach. Because the PHA had already been completed, a dedicated SIL selection study was conducted utilizing the results of the PHA as a screening tool. Selection of SIL was a team exercise that included individuals from the original PHA team along with new experienced personnel. The process utilized is represented by the flowchart shown in Figure 1. The following is a detailed explanation of the SIL selection process.

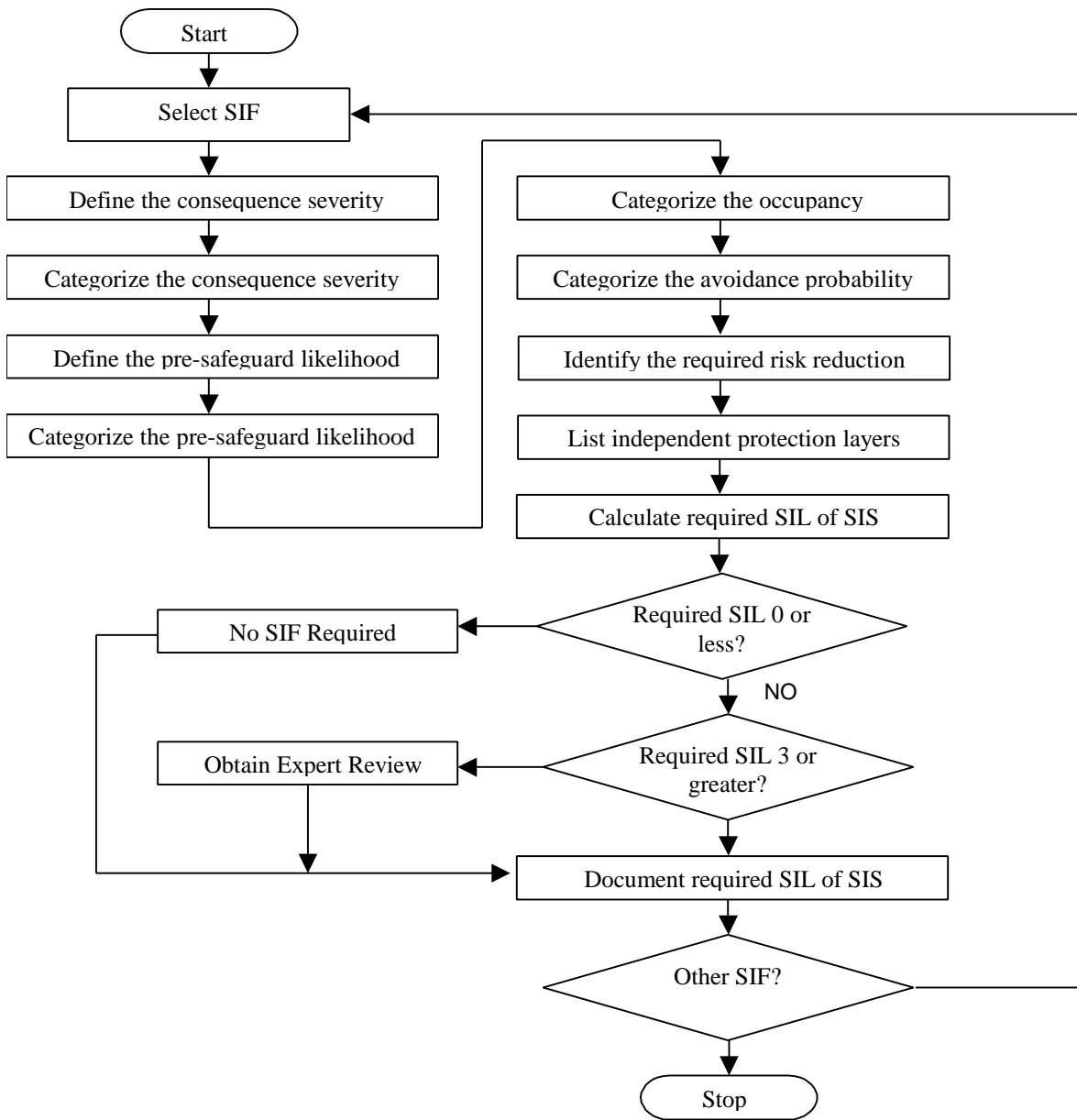


FIGURE 1 SIL SELECTION PROCESS FLOW

The study began with a list of Safety Instrumented Functions that were to be analyzed. These Safety Instrumented Functions were identified through reviewing the recommendations and safeguards noted in the Process Hazard Analysis reports.

For each Safety Instrumented Function that was identified, the consequence severity of the accident being prevented was defined. The consequence severity was then categorized using the information provided in Figure 2. The consequence definition and selected category were then documented in a SIL selection worksheet.

Category	Description
C ₁	No injury or occupational illness, First Aid
C ₂	Injury or occupational illness that are recordable but not lost time
C ₃	Injury or occupational illness that are lost time
C ₄	Death or severe occupational illness

FIGURE 2 CONSEQUENCE SEVERITY CATEGORIZATION

After the consequence was addressed, the pre-safeguard likelihood of the accident was defined. The pre-safeguard likelihood was categorized using information provided in Figure 3. The pre-safeguard likelihood definition and selected category were then documented in the SIL selection worksheet. Note the pre-safeguard likelihood category required for SIL selection should only reflect the likelihood of the causes. For example, one should analyze the severity of a vessel rupture for an exothermic reaction without considering the benefits of a relief valve. This allows the required effectiveness of the safeguards, including the Safety Instrumented Function, to be analyzed.

Category	Description
W ₁	Not expected to occur during the facility lifetime
W ₂	Expected to occur several times during the facility lifetime
W ₃	Expected to occur once a year
W ₄	Expected to occur frequently (like once a month)

FIGURE 3 LIKELIHOOD CATEGORIZATION

Next, the occupancy in the hazardous zone was analyzed. The frequency of, and exposure time in, the hazardous zone was categorized using Figure 4. The occupancy parameter was then documented in a SIL Selection Worksheet.

Category	Description
F ₁	Rare to more often exposure in the hazardous zone
F ₂	Frequency to permanent exposure in the hazardous zone

FIGURE 4 OCCUPANCY CATEGORIZATION

The probability of avoiding the hazardous event was then analyzed. The probability of avoiding the hazardous event was categorized using Figure 5. The probability of avoidance parameter was then documented in a SIL Selection Worksheet.

Category	Description	Notes
P ₁	Possible under certain conditions	This parameter should account for: Operation of the process (e.g., continuously monitored) Rate of development of the hazardous event Ease of recognition of danger Avoidance of hazard (e.g., possible escape routes) Actual safety experience with similar processes
P ₂	Almost impossible	

FIGURE 5 PROBABILITY OF AVOIDANCE CATEGORIZATION

Once the consequence, pre-safeguard likelihood, occupancy and probability of avoidance were defined, the required risk reduction was determined from Figure 6. The required risk reduction can take place by any combination of safeguards, either instrumented or non-instrumented. The required risk reduction is a value that defines the number of order-of-magnitude decreases in either the consequence severity or likelihood of the unwanted accident (usually the likelihood) that are required.

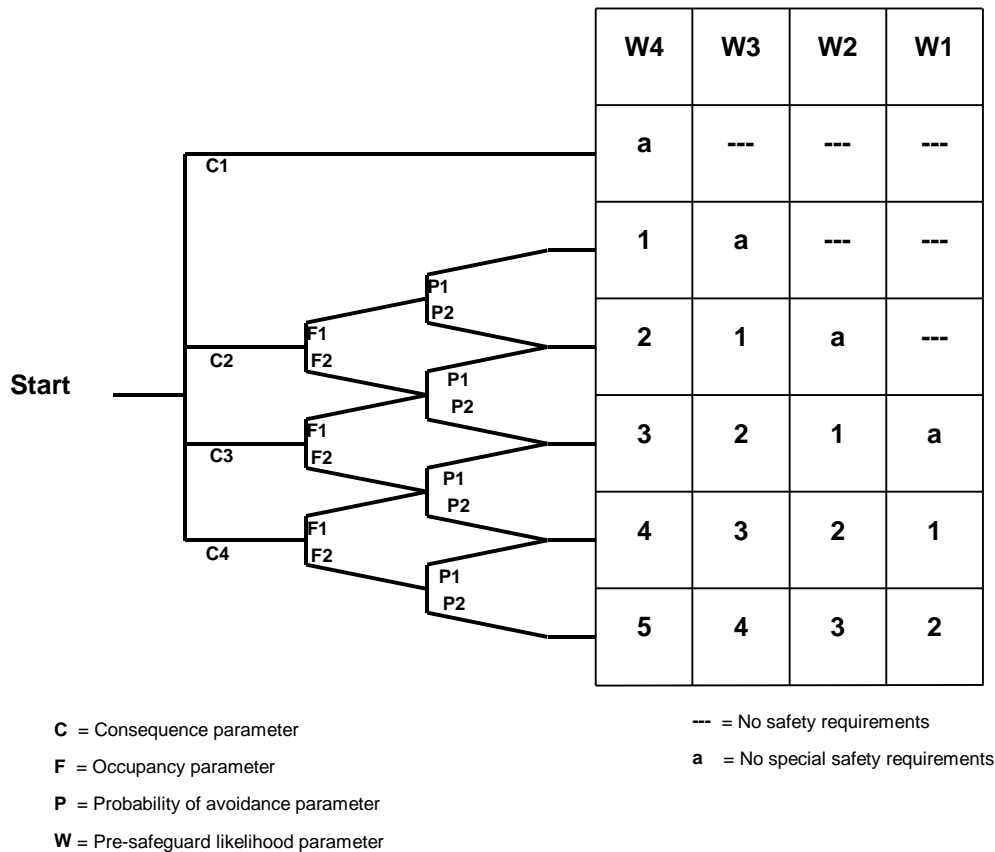


FIGURE 6 RISK GRAPH

The required risk reduction was typically accomplished using a combination of instrumented and non-instrumented safeguards. In order to know what amount of risk reduction was required to be performed by the Safety Instrumented Function, one must know the total amount of risk reduction provided by the other protection layers. This was accomplished by summing the number of independent protection layers that were available to prevent the hazard

An Independent Protection Layer (IPL) was defined as a specific category of safeguard. Independent Protection Layers were evaluated and must meet all of the following criteria to be utilized in the SIL selection process:

Specificity – An independent protection layer must be specifically designed to prevent the consequences of one potentially hazardous event.

Independence – The operation of the protection layer must be completely independent from all other protection layers, no common equipment can be shared with other protection layers.

Dependability – The device must be able to dependably prevent the consequence from occurring. Both systematic and random faults need to be considered in its design. The probability of failure of an independent protection layer must be demonstrated to be less than 10%.

Auditability – The device should be proof tested and maintained. These audits of operation are necessary to ensure that the specified level of risk reduction is being achieved.

Some common Independent Layers of Protection utilized on the project included:

Coaxial Piping Systems

- Relief Valves
- Check Valves
- Operator Response ***

*** Note Operator Response was only considered as an Independent Protection Layer if all of the following criteria were met.

1. Ample indications that a process upset requiring manual intervention exist.
2. The operator has been trained on the proper response to the specific upset condition under consideration.
3. An operator is always stationed at the location where the process upset will be annunciated, and can take action from that station.
4. The operator has adequate time to consider the process condition and the proper response action prior to the accident occurring (>2 minutes).
5. The operator is not under a great deal of stress due to an emergency in progress when the process upset indications occur.

Once the Independent Protection Layers were identified, the total number of protection layers represents the amount of risk reduction that was provided by non-Safety Instrumented System means. The difference between the risk reduction provided by the Independent Protection Layers and the required risk reduction that was determined from Figure 6 is the risk reduction contribution that must be provided by the Safety Instrumented Function. The SIL that is assigned to a Safety Instrumented Function protecting against a specific hazard is then the difference between the required risk reduction determined from the pre-safeguard risk ranking and the number of independent protection layers.

$SIL = \text{Required Risk Reduction} - \text{Number of IPL}$

If the SIL calculated using the equation above is either zero or negative, then a Safety Instrumented Function was not required for risk reduction purposes. If the calculated SIL was greater than 2, then it was felt that an expert should review the scenario.

In addition to degrees of required risk reduction, Figure 5 also shows a required risk reduction category of “a” that is less than SIL 1, but still significant enough to warrant special consideration. When SIL “a” is selected, the following considerations should be made in the design of the Safety Instrumented Function.

1. In general, SIL 1 qualitative design practices are followed, but quantitative analysis of the probability of failure on demand of the Safety Instrumented Function is not required.
2. The same logic solver that is used for other Safety Critical Functions is used.
3. Simplex field devices are used (i.e., no redundancy or advanced diagnostics are required).
4. The Safety Instrumented Function will be periodically function tested on an interval determined by the judgment of the design team.

Once the required SIL was calculated, the results were documented in a SIL selection worksheet.

CONCLUSION

The above procedure to determine the Safety Integrity Level for a given Safety Instrumented Function was utilized on the new manufacturing line project with great success. The team found the process easy to implement and a very efficient way to quickly analyze a large quantity of Safety Instrumented Functions. The resultant Safety Integrity Levels was then used to establish the design requirements for the Life Safety System. A new system architecture was ultimately selected for the Life Safety System that met the required Safety Integrity Levels while maximizing system availability. This procedure forms the basis of the company's new Life Safety System design standards and practices.

REFERENCES

1. ANSI/ISA S84.01-1996, Application of Safety Instrumented Systems for the Process Industries
2. IEC 61508, Functional safety of electrical/electronic/programmable safety-related systems
3. IEC d61511, Functional safety: Safety Instrumented Systems for the process industry sector
4. SEMI S2-0200, Environmental, Health, and Safety Guideline for Semiconductor Manufacturing Equipment
5. SEMI S10-1296, Safety Guideline for Risk Assessment
6. SEMI S14-0200, Safety Guidelines for Risk Assessment and Mitigation for Semiconductor Manufacturing Equipment
7. Marszal, Edward, "Guideline for the Selection of Safety Integrity Levels", 11/11/01