Second Annual Symposium, Mary Kay O'Connor Process Safety Center
"Beyond Regulatory Compliance: Making Safety Second Nature"
Reed Arena, Texas A&M University, College Station, Texas
October 30-31, 2001

Evaluating Safety Instrumented System Needs Using Process Hazard Analysis Data

Fred Leverenz Jr.
and Kelli M. McEldowney
Battelle - Integrated Risk Management
505 King Avenue, 11-10-114
Columbus OH 432012693

Phone: (614)424-7485
Email: mceldowneyk@battelle.org

ABSTRACT

Determining Safety Instrumented Systems (SIS) needs is the first step of a long process of complying and maintaining compliance with national and international standards. How a company goes about determining SIS needs can have a significant impact, not only on process safety, but also on process economics. Much of the process analysis used to evaluate the need for SIS, based on Safety Integrity Levels (SIL), is already included in process hazards analyses. Using existing analyses will allow you to minimize "re-analysis" and help focus SIS and recommended actions on plant economics.

Hazard analysis data can help determine if existing equipment and instrumentation are adequate to ensure a safe shutdown of the plant. In instances where the existing safeguards are not sufficient, companies can look to good engineering practices, such as ISA S84.01, and determine if an SIS is necessary.

In addition to identifying the need for SIS, companies can use Importance Measures, used to relatively rank equipment based on their influence to the overall risk, to help prioritize SIS selection. By prioritizing SIS selection, the minimum number of SIS can be identified while still addressing all the hazards of the process. This paper present processes and results from using process hazards analysis for SIL determination and action item/maintenance prioritization.

Evaluating Safety Instrumented System Needs Using Process Hazard Analysis Data

Fred Leverenz Jr. - Battelle Memorial Institute, Integrated Risk Management
Kelli M. McEldowney - Battelle Memorial Institute, Integrated Risk Management

Abstract

Determining the need for Safety Instrumented Systems (SISs) is the first step in complying and maintaining compliance with national and international standards. How a company goes about determining the need for SISs can have a significant impact, not only on process safety, but also on process economics. Much of the analysis used to evaluate the need for SISs based on Safety Integrity Levels (SILs) is already included in Process Hazards Analyses (PHAs). Using existing PHAs will allow you to minimize "re-analysis" and help focus the need for SISs and recommended risk reduction actions on plant economics.

Process Hazard Analysis data can help determine if existing equipment and instrumentation are adequate to ensure the safe shutdown of a plant. In instances where existing safeguards are not sufficient, companies can look to good engineering practices, such as ISA S84.01 to determine if an SIS is necessary.

Importance Measures can be used to relatively rank equipment based on their influence to the overall risk. Companies can also use Importance Measures to help prioritize SIS selection. By prioritizing SIS selection, you can identify the minimum number of SISs while still addressing all the hazards of a process. This paper focuses on how you can determine when and where an SIS is required. It discusses target SILs and how you can use PHAs both to determine SILs and to prioritize action items and maintenance.

Introduction

In order to increase safety and minimize risk for process industries, the Instrument Society of America[1] (ISA) and the International Electrotechnical Commission[2] (IEC) have developed standards addressing Safety Instrumented Systems. A Safety Instrumented System (SIS) is a "system composed of sensors, logic solvers, and final control elements for the purpose of taking the process to a safe state when predetermined conditions are violated."[1] Examples of SISs include emergency shutdown systems (ESD, ESS), safety shutdown systems (SSD), and safety interlocks. The need for an SIS is determined by a target Safety Integrity Level (SIL). An SIL is defined by the probability that a SIS will fail on demand. Both ISA and IEC agree with the definition for SILs 1, 2, and 3. However, IEC includes an additional level, SIL 4 that ISA does not. The higher the SIL is, the more reliable or effective it must be. Table 1 lists the definitions of each SIL.

Table 1: Safety Integrity Levels.[1,2]

Safety Integrity Level (SIL)	Probability of Failure on Demand Average Range	Effectiveness
1	10^{-1} to 10^{-2}	90% - 99%
2	10^{-2} to 10^{-3}	99% - 99.9%
3	10^{-3} to 10^{-4}	99.9% - 99.99%
4*	10^{-4} to 10^{-5}	99.99% - 99.999%
*Included in IEC standard only		

SAFETY LIFE CYCLE

There are many phases of an SIS, from the design, implementation, and testing through decommissioning, known as the safety life cycle. ISA defines the following steps as the safety life cycle.[1]

1. Conceptual design of process.
2. Identification of process hazards and risks via a hazard analysis and risk assessment.
3. Identification of non-SIS layers of protection.
4. Evaluation for the need of additional protection like an SIS.
5. Determination of target SIL, if an SIS is required.
6. Development of safety requirement specifications.
7. Development of SIS conceptual designs to meet safety requirements.
8. Development of detailed SIS design.
9. Installation of SIS.
10. Commissioning and Pre-startup testing.
11. Development of operation and maintenance procedures.
12. Pre-startup safety review.
13. Operation and maintenance of SIS.
14. Modification of SIS.
15. Decommissioning.

Steps 1 through 5, from the conceptual design of a process through the determination of the target SIL, are outside of the scope of the ISA[1] standard. However, information and examples for determining SILs for SISs is included in the standard. The remaining steps, steps 6 through 15, are covered in both of the ISA and IEC standards. This paper focuses on how to determine when and where an SIS is required and how to determine its target SIL.

USING PROCESS HAZARD ANALYSIS DATA TO IDENTIFY SIS NEEDS

Hazard analysis data can help you determine if existing equipment and instrumentation are adequate to ensure a safe shutdown of a plant. In instances where existing safeguards are not sufficient, companies can determine if an SIS is needed.

During a process hazard analysis, such as a Hazard and Operability (HAZOP) study, all of the elements in a potential incident are recorded, including the initiating event, consequences, and safeguards. All of these elements are needed to determine the target SIL for a scenario. Figure 1 shows the anatomy of an incident, which is helpful when developing a scenario.

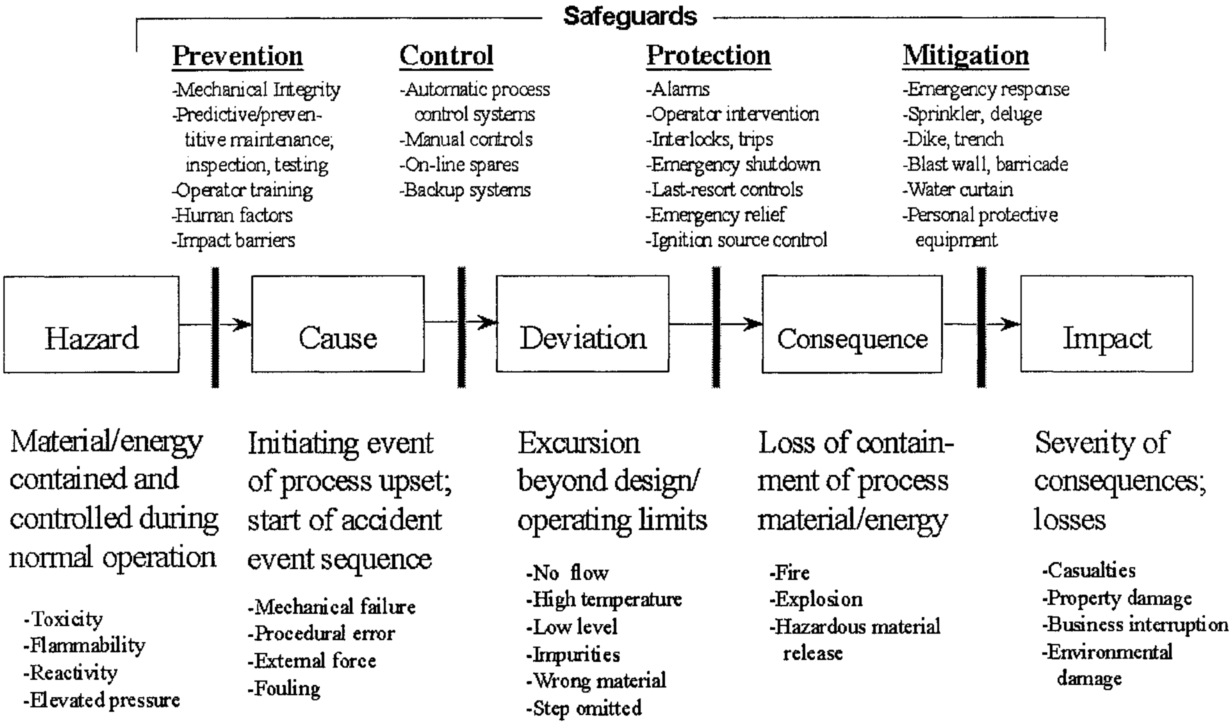


Figure 1: Anatomy of an Incident.

The anatomy of an incident begins with an initiating event that leads to a process deviation and, due to the hazards of the process, a consequence with impacts to workers, environment, business, etc. Several types of safeguards are used to reduce the likelihood that the initiating event will occur (prevention), to maintain the process within the normal operating limits after the initiating event occurs (control), to avoid the consequences after a deviation occurs (protection), and to reduce the severity of the consequences if other safeguards fail (mitigation).

During a HAZOP, all of the elements of an incident are recorded. Table 2 shows how the anatomy of an incident is represented as a HAZOP scenario.

Table 2: HAZOP scenario.

Cause	Frequency Score	Consequence	Health & Safety Impact Score	Safeguard Type	Safeguards	Effectiveness Score
Cooling Water System Failure	-0.5	Runaway reaction, reactor vessel explosion with no warning, possible serious injuries to fatalities, major plant damage	6	Protection (non-IS)	Operator starts backup cooling system in response to loss of flow alarm	-1
				Control (IS)	High temperature quench system	-2
				Protection (non-IS)	Rupture Disk	-2
				Total non-IS PFD Score: (-1) + (-2) = -3 **Total IS PFD Score:** -2		

Once the scenario has been developed using the HAZOP methodology, scores can be assigned to the likelihood of the cause, the severity of the impacts, and the effectiveness of the safeguards in order to determine the level of risk for the scenario. Risk is defined as the product of the frequency, impacts, and safeguards' effectiveness, as seen in Equation 1.

$$\boxed{Risk = Frequency \times Severity \times Safeguard\ Effectiveness}$$

Equation 1: Definition of Risk.

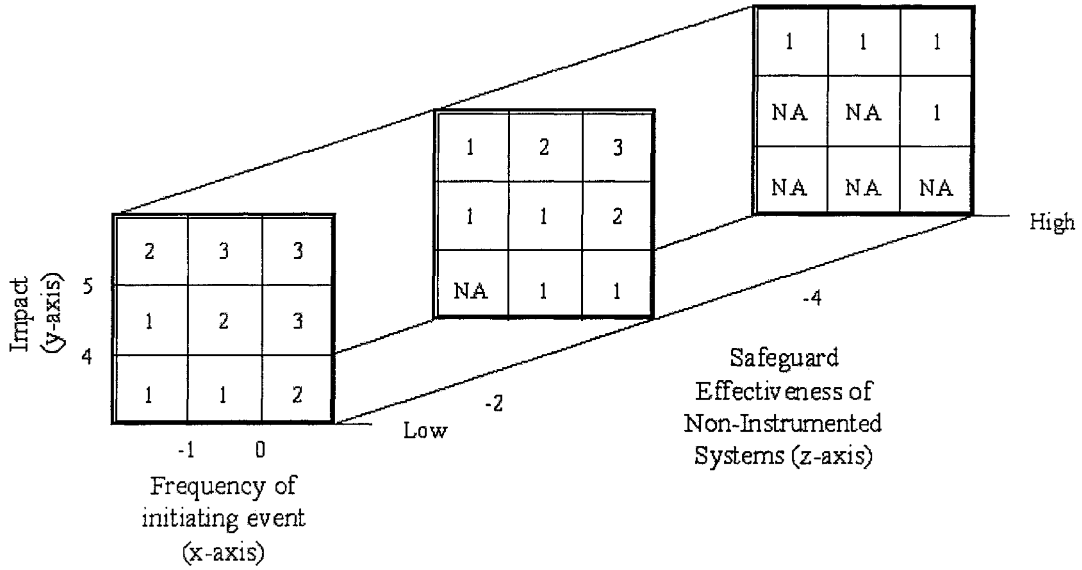
Using an order-of-magnitude approach, this scenario suggests that the cooling water system fails $10^{-0.5}$ times per year or approximately once every three years. Likewise, the severity of the consequences can also be determined using an order-of-magnitude approach. However, it is important to be careful when comparing different types of consequences (i.e., business cost, environmental, worker health and safety) when using this approach. When assigning the business cost associated with a scenario, the order-of-magnitude approach is straightforward (i.e., 10^1 = \$10, 10^2 = \$100, 10^3 = \$1,000). Unfortunately, it is not as easy to use this approach when talking about worker health and safety or the environment. In this case, you may want to use a scale, for worker health and safety, where 1 represents a minor injury, 2 represents injuries requiring medical treatment, 3 represents severe injury, 4 represents permanent health effects, etc. In this example, the worker health and safety impact score of 6 might represent multiple fatalities due to the unexpected explosion of the reactor. The same order-of-magnitude approach can be applied to the safeguards' effectiveness. For example, a safeguard effectiveness score of -1 equates to 10^{-1} or fails 10% when needed (90% effective), -2 equates to 10^{-2} or fails 1% when needed (99% effective), -3 equates to 10^{-3} or fails 0.1% when needed (99.9% effective), and -4 equates to 10^{-4} or fails 0.01% when needed (99.99% effective).

When using an order-of-magnitude approach, the risk for this scenario can be calculated based on the sum of the frequency score, impact score, and safeguard effectiveness score. For this scenario, the risk score is 0.5, as seen in Equation 2.

$$\boxed{Risk = 10^{0.5} \times 10^{6} \times 10^{-5} = 10^{0.5} \quad or \quad Risk\ score = 0.5 + 6 + (-5) = 0.5}$$

Equation 2: Scenario Risk.

After a scenario has been developed, the need for additional protection, such as an SIS, needs to be determined. Using the matrix approach, as suggested by ISA[1], the SIL for the scenario can be determined. The matrix, seen in Figure 2, can be used to determine the target SIL for a scenario. To use this matrix, the same information that is recorded during a HAZOP is required, which is the frequency of the initiating event, the severity of the impacts, and the effectiveness of the non-instrumented system safeguards.


Impact (y-axis)
5
4
-1
0
Frequency of initiating event (x-axis)
Low
-2
-4
High
Safeguard Effectiveness of Non-Instrumented Systems (z-axis)

2	3	3
1	2	3
1	1	2

1	2	3
1	1	2
NA	1	1

1	1	1
NA	NA	1
NA	NA	NA

Figure 2: Safety Integrity Level (SIL) Matrix. (NA indicates that an SIS is not applicable for the scenario)

This matrix has been modified to incorporate the order-of-magnitude approach that was used when developing the HAZOP scenario in Table 2. ISA uses a high, medium, low ranking to determine which cell in the matrix should be used. By replacing the high, medium, low ranking with similar scores that are used in the development of the HAZOP scenario, a straightforward approach can be taken to determine the appropriate SIL for the scenario.

Referring to the HAZOP scenario from Table 2, the target SIL would be 2. A SIL 2 was determined because the effectiveness of the non-instrumented systems (i.e., loss of flow alarm initiating operator to start the backup cooling system [-1] and rupture disk [-2]) is –3. Using the z-axis, -3 indicates the use of the middle matrix. Next, the frequency of the cooling water failure is -0.5; using the x-axis, indicates the middle column should be used. Finally, by using the y-axis, the severity of the worker health and safety impact of 6 indicates the use of the top row. Therefore, the second matrix, middle column, top row indicates a SIL 2 for the scenario.

Based on the definition of SIL 2, from Table 1, this scenario requires an SIS with a probability of failure on demand of 10^{-2} to 10^{-3} or an effectiveness score of -2 to -3. Since this scenario has an instrumented system safeguard (i.e., high temperature quench system) with an effectiveness score of -3, no additional safeguards are required; however, it is required to make the quench system a safety instrumented system. By making the quench system an SIS, the requirement of the ISA standard should be followed for the amount of testing that is necessary to maintain an SIS status for this piece of equipment. By doing this, the SIS requirements for this scenario will be met.

This process is repeated for each scenario in the HAZOP. When all of the scenarios have been evaluated, the result will be a long list of scenarios and the target SILs, for each SIS required. One way to visualize these results is seen in Table 3. This table lists all of the scenarios in the HAZOP study along with the SIL requirements. Also listed are the instrumented systems already recorded as safeguards for each scenario with its effectiveness.

Table 3: Scenario SIL Requirements.

Scenario	Required SIL	Instrumented System Safeguards				
		IS 1	IS 2	IS 3	IS 4	...
		10^{-1}	10^{-3}	10^{-2}	10^{-2}	
Scenario 1	2			X	X	
Scenario 2	Not Required					
Scenario 3	1	X	X			
Scenario 4	3		X	X		
Scenario 5	2	X				
...	...					

This table allows you to determine which instrumented systems should be made into safety instrumented systems in order to meet the requirements of the ISA standard for each scenario. For example, IS 1 and IS 2 fulfill the requirements for Scenario 3. However, IS 2 also fulfills the requirements of Scenario 4; therefore, it would be most effective to make IS 2 a safety instrumented system because it will fulfill the requirements of two scenarios instead of making both IS 2 (to meet the requirements of Scenario 4) and IS 1 (to meet the requirements of Scenario 3) into safety instrumented systems. However, this approach could be very time consuming due to the large number of scenarios that are generated during a HAZOP study and might not allow a company to choose the pieces of equipment to make into safety instrumented systems most effectively.

Importance Measures

In order to help prioritize the selection of safety instrumented systems, Importance Measures can be used to identify which pieces of equipment can reduce the overall risk most effectively. Importance Measures were developed as a way to add understanding to the results from risk and reliability analyses. While Importance Measures are based on numerical calculations, they are for the purpose of relative ranking; hence the numerical values associated with the results have no direct meaning. There are many Importance Measures, some of which are just different ways of representing the results. Two that are useful in understanding how to control and reduce risk are the Risk Achievement Worth and Risk Reduction Worth measures.[3]

Risk Achievement Worth (RAW) is an Importance Measure that provides the decision-maker with information on how to most effectively keep the risk from increasing by indicating which causes and safeguards should receive the most attention to prevent degradation in its effectiveness from the current level.[3] Mathematically, RAW for a piece of equipment is defined in Equation 3.

$$\boxed{RAW = \frac{\textit{Risk of the system as is}}{\textit{Risk of the system if the piece of equipment is made perfect}}}$$

Equation 3: Risk Achievement Worth.

For pieces of equipment with a high RAW, companies should maintain the equipment's current effectiveness by increasing the amount of testing and maintenance that is performed on the piece of equipment. If these pieces of equipment are allowed to degrade from their current level of effectiveness, they have the potential to increase the overall risk the most.

Risk Reduction Worth (RRW) is an Importance Measure that provides the decision-maker with information on how to reduce the overall risk most effectively by giving insight as to which causes should be made less likely and which safeguards should be made more reliable in order to reduce risk. The relative rankings provided by the RRW analysis should be considered as approximate in that there may be little difference in items close to each other on the list. However, there is a greater assurance in the impact of taking action with respect to items that are widely separated on the list.[3] Mathematically, RRW for a piece of equipment is defined in Equation 4.

$$\boxed{RRW = \frac{\textit{Risk of the system if the piece of equipment fails}}{\textit{Risk of the system as is}}}$$

Equation 4: Risk Reduction Worth.

For pieces of equipment with a high RRW, companies should increase the reliability of the piece of equipment or increase its effectiveness as a safeguard to reduce the overall risk most effectively.

SIS Prioritization

By combining the approach of looking at all scenarios and identifying the least number of instrumented systems that should be converted into safety instrumented systems with the results from the Importance Measure analysis, the minimum number of SISs can be identified while still addressing all the hazards of the process and reducing the overall risk most effectively.

For example, if IS 4 is high on the RAW list compared to IS 3, it would be more effective to make IS 4 a safety instrumented system than it would be to make IS 3 an SIS because they both fulfill the same number of scenarios in Table 3 but IS 4 has the potential to increase the overall risk more than IS 3 if it degrades from its current level of effectiveness. By making it a safety instrumented system, which requires a certain degree of routine maintenance, IS 4 is less likely to degrade from its current state and, therefore, is less likely to increase the overall risk.

Likewise, if IS 4 is high on the RRW list compared to IS 3, it would be more effective to make IS 4 a safety instrumented system than it would be to make IS 3 a SIS. Again, they both fulfill the same number of scenarios in Table 3, but if IS 4 is made more reliable it has the potential to decrease the overall risk more than IS 3. By making it a safety instrumented system, safety reviews of the equipment and, if necessary, modifications to the equipment will be made; therefore, IS 4 is likely to be made more reliable and have the potential to decrease the overall risk of the process.

In addition to using Importance Measures to help prioritize SIS selection, it is also helpful to determine the level of risk that is acceptable for a scenario that would not require an SIS. That is, a company should decide if the risk of a scenario is equal to or less than a certain value for which an SIS is not required and, therefore, the process of determining the target SIL and evaluating the need for an SIS for that scenario is avoided.

Conclusions

Determining the need for an SIS is a long, tedious process of complying and maintaining compliance with national and international standards. There are many ways in which a company can determine SIS needs. There are also many things to consider when you determine the need for an SIS, including the safety of the process as well as process economics. Since most of the information used to evaluate SIS needs is already included in process hazards analyses, using existing analyses will allow you to minimize "re-analysis" of the process and help focus the need for SISs and recommended actions on plant economics.

By looking at each PHA scenario independently, you will identify more SISs than are actually needed to minimize the process risk. In order identify the most important SISs and to reduce the total number of SISs needed, you can use Importance Measures to prioritize their selection. By prioritizing SIS selection, you can identify the minimum number of SISs while still addressing all the hazards. Thus, the overall cost to the plant is reduced.

Acronyms

ANSI	American National Standards Institute
HAZOP	Hazard and Operability
IEC	International Electrotechnical Commission
IS	Instrumented System
ISA	International Society of Measurement and Control
RAW	Risk Achievement Worth
RRW	Risk Reduction Worth
SIL	Safety Integrity Level

SIS Safety Instrumented System

[1] ANSI/ISA Standard S84.01-1996, *Application of Safety Instrumented Systems to the Process Industries*, International Society for Measurement and Control, Research Triangle Park, NC, (1996).

[2] CEI/IED 61508 Parts 1-7: 1998, *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems*, International Electrotechnical Commission, Geneva, Switzerland.

[3] G. Bradley Chadwell and Fred L. Leverenz, Jr., "Importance Measures for Prioritization of Mechanical Integrity and Risk Reduction Activities," 1999, 33rd Annual Loss Prevention Symposium, Houston, Texas, March 15, 1999.