Functional Safety and Safety Integrity Levels

BENTLY Nevada

Background:

In 1996, in response to an increasing number of industrial accidents, the Instrument Society of America (ISA) enacted a standard to drive the classification of Safety Instrumented Systems for the process industry within the United States. This standard, ISA S84.01, introduced the concept of Safety Integrity Levels. Subsequently, the International Electrotechnical Commission (IEC) enacted an industry neutral standard, IEC 61508, to help quantify safety in programmable electronic safety-related systems. The combination of these standards has driven industry, most specifically the Hydrocarbon Processing and Oil & Gas industries, to seek instrumentation solutions that will improve the inherent safety of industry processes. As a byproduct, it was discovered that many of the parameters central to Safety Integrity Levels, once optimized, provided added reliability and up time for the concerned processes.

This document will define and describe the key components of safety and reliability for instrumentation systems as well as draw contrasts between safety and reliability. Additionally, this document will briefly describe available methods for determining Safety Integrity levels. Lastly, a brief depiction of the governing standards will be presented.

What are Safety Integrity Levels (SIL)

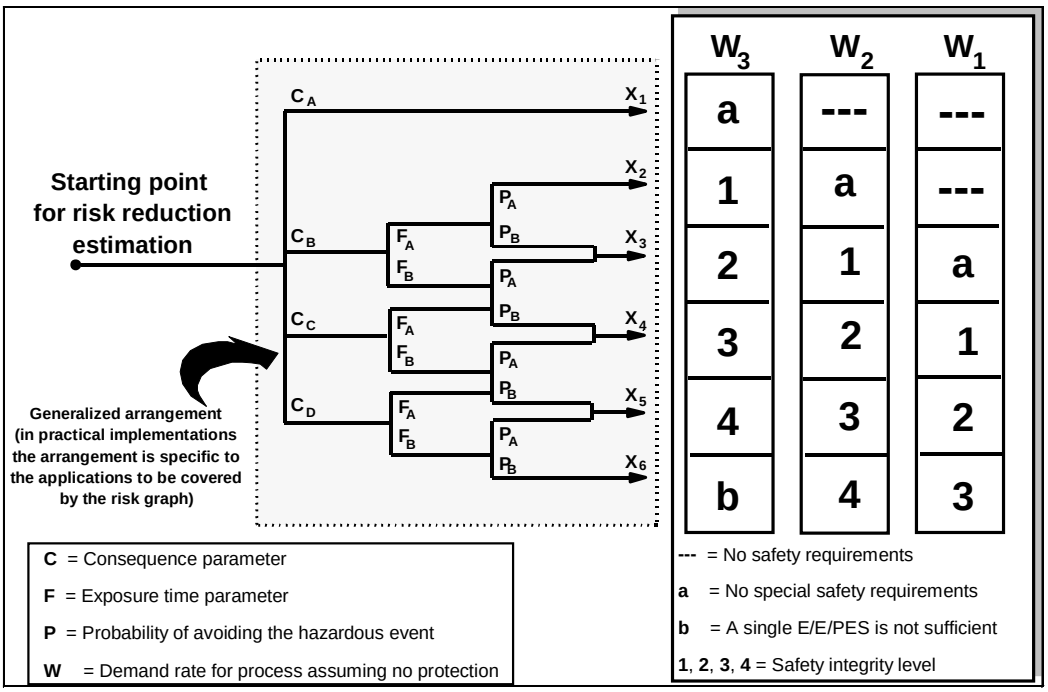
Safety Integrity Levels (SIL) are measures of the safety of a given process. Specifically, to what extent can the end user expect the process in question to perform safely, and in the case of a failure, fail in a safe manner? The specifics of this measurement are outlined in the standards IEC 61508, IEC 61511, JIS C 0508, and ISA SP84.01. It is important to note that no individual product can carry a SIL rating. Individual components of processes, such as instrumentation, can only be certified for use within a given SIL environment.

The need to derive and associate SIL values with processes is driven by Risk Based Safety Analysis (RBSA). RBSA is the task of evaluating a process for safety risks, quantifying them, and subsequently categorizing them as acceptable or unacceptable. Acceptable risks are those that can be morally, monetarily, or otherwise, justified. Conversely, unacceptable risks are those whose consequences are too large or costly. However risks are justified, the goal is to arrive at a safe process.

A typical RBSA might proceed as follows. With a desired level of safety being a starting point, a “risk budget” is established specifying the amount of risk of unsafe failure to be tolerated. The process can then be dissected into its functional components, with each being evaluated for risk. By combining these risk levels, a comparison of actual risk can be made against the risk budget. When actual risk outweighs budgeted risk, optimization is called for.

Processes can be optimized for risk by selecting components rated for use within the desired SIL environment. For example, if the desired SIL value for the process is SIL 3, then by using components rated for use within a SIL environment this goal may be achieved. It is important to note that simply combining process components rated to be used in a given SIL rated environment does not guarantee the process to be rated at the specified SIL. The process SIL must still be determined by an appropriate method. These are Simplified Calculations, Fault Tree Analysis, or Markov Analysis.

An example of a tool used to estimate what SIL rating to target for a given process is that of the Risk Assessment Tree (RAT). See the figure below. By combining the appropriate parameters for a given process path, the RAT can be used to determine what SIL value should be obtained. As the example below illustrates, by optimizing certain process parameters, the SIL value of the process can be affected.



Risk parameter		Classification	Examples
Consequence (C)	C_A	A failure with minor damage that is not very severe but is severe enough to be reported to plant management	A moderate leak from a flange or valve Small scale liquid spill Small scale soil pollution without affecting ground water
	C_B	Failure with significant damage	A cloud of obnoxious vapour travelling beyond the unit following flange gasket blow-out or compressor seal failure
	C_C	Failure with major damage which can be cleaned up quickly without significant lasting consequences	A vapour or aerosol release with or without liquid fallout that causes temporary damage to plants or fauna
	C_D	Failure with major damage which cannot be cleaned up quickly or with lasting consequences	Liquid spill into a river or sea A vapour or aerosol release with or without liquid fallout that causes lasting damage to plants or fauna Solids fallout (dust, catalyst, soot, ash) Liquid release that could affect groundwater

SILs versus Reliability

While the main focus of the SIL ratings is the interpretation of a process' inherent safety, an important byproduct of the statistics used in calculating SIL ratings is the statement of a product's reliability. In order to determine if a product can be used in a given SIL environment, the product must be shown to "BE AVAILABLE" to perform its designated task at some predetermined rate. In other words, how likely is it that the device in question will be up and functioning when needed to perform its assigned task? Considerations taken into account when determining "AVAILABIITY" include Mean Time Between Failure (MTBF), Mean Time To Repair (MTTR), and Probability to Fail on Demand (PFD). These considerations, along with variations based upon system architecture (i.e. 2oo2 versus 2oo3, or TMR installation), determine the reliability of the product. Subsequently, this reliability data, combined with statistical measure-

ments of the likelihood of the product to fail in a safe manner, known as Safe Failure Fraction (SFF), determine the maximum rated SIL environment in which the device(s) can be used.

SIL ratings can be equated to the Probability to Fail on Demand (PFD) of the process in question. The following tables gives relationships based on whether the process is required "Continuously" or "On Demand".

Table 3 – Safety integrity levels: probability of failure on demand

DEMAND MODE OF OPERATION		
Safety Integrity Level (SIL)	**Average Probability of Failure on Demand**	**Risk Reduction**
4	$\geq 10^{-5}$ to $<10^{-4}$	>10,000 to ≤ 100,000
3	$\geq 10^{-4}$ to $<10^{-3}$	>1000 to ≤ 10,000
2	$\geq 10^{-3}$ to $<10^{-2}$	>100 to ≤ 1000
1	$\geq 10^{-2}$ to $<10^{-1}$	>10 to ≤ 100

Table 4 – Safety integrity levels: frequency of dangerous failures per hour

CONTINUOUS MODE OF OPERATION	
Safety Integrity Level (SIL)	**Frequency of Dangerous Failures Per Hour**
4	$\geq 10^{-9}$ to $<10^{-8}$
3	$\geq 10^{-8}$ to $<10^{-7}$
2	$\geq 10^{-7}$ to $<10^{-6}$
1	$\geq 10^{-6}$ to $<10^{-5}$

Determining SIL Values

(Note that the following text is not intended to be a step-by-step "How To" guide. This text is intended to serve as an overview and primer.)

As mentioned previously, there are three recognized techniques for determining the SIL rating for a given process. These are Simplified Calculations, Fault Tree Analysis, and Markov Analysis.

Each of these techniques will deliver a useable SIL value; however, generally speaking the Simplified Calculations method is more conservative and the least complex. Conversely, Markov Analysis is more exact and much more involved. Fault Tree Analysis falls somewhere in the middle.

For each of these techniques, the first step is to determine the PFD for each process component. For a 2oo3 process configuration, this can be done using the following relationship:

$PFD_{ave} = (\text{Failure Rate})^2 * \text{Test Interval}$

Note that Failure rate = 1/MTBF

In the case of the Simplified Calculations method, the next step would be to sum the PFD values for every component in the process. This summed PFD can then be compared to table 3 above for the SIL rating for the process.

In the case of the Fault Tree Analysis method, the next step would be to produce a fault tree diagram. This diagram is a listing of the various process components involved in a hazardous event. The components are linked within the tree via Boolean logic (logical ORing & ANDing relationships). Once this is done, the PFD for each path is determined based upon the logical relationships. Finally, the PFDs are summed to produce the PFD_{ave} for the process. Once

again, the PFD_{ave} can be referenced in table 3 for the proper SIL.

The Markov Analysis is a method where a state diagram is produced for the process. This state diagram will include all possible states, including all "Off Line" states resulting from every failure mode of all process components. With the defined state diagram, the probability of being in any given state, as a function of time, is determined. This determination includes not only MTBF numbers and PFD calculations, but it also includes the Mean Time To Repair (MTTR) numbers. This allows the Markov Analysis to better predict the availability of a process. With the state probability (PFD_{ave}) determined, they can once again be summed and compared to table 3 to determine the process SIL.

As the brief descriptions above point out, the Simplified Calculations method will be the easiest to perform. It will provide the most conservative result, and thus should be used as a first approximation of SIL values.

If having used the Simplified Calculations method, and find that a less conservative result is desired, then employ the Fault Tree Analysis method. This method is considered by many to be the proper mix of simplicity and completeness when performing SIL calculations.

For the subject expert, the Markov Analysis will provide the most precise result. It can be very tedious and complicated to perform. A simple application can encompass upwards of 50 separate equations needing to be solved. It is suggested, that relying upon a Markov Analysis to provide that last little bit of precision necessary to improve a given SIL, is a misguided use of resource. A process that is teetering between two SIL ratings would be better served being redesigned to comfortably achieve the desired SIL rating.

Reliability Numbers: What do they mean?

It seems that every organization has its own special way of characterizing reliability. However, there are a few standards in the world of reliability datum. These are Mean Time Between Failure (MTBF), Mean Time To Repair (MTTR), and Probability to Fail on Demand (PFD). Bently Nevada has chosen to provide all of these pieces of data for the 3500 Monitoring System.

The following is a brief explanation of these terms.

MTBF. This is usually a statistical representation of the likelihood of a component, device, or system to fail. The value is expressed as a period of time (i.e. 14.7 years). This value is almost always calculated from theoretical information (Laboratory Value). Unfortunately, this often leads to some very unrealistic values. Occasionally, MTBF values will have observed data as their basis (Demonstrated Value). For example, MTBF can be based upon failures rates determined as a result of accelerated lifetime testing. Lastly, MTBF can be based upon reported failures (Reported Value). Because of the difficulty in determining Demonstrated Values, and the likelihood that the true operating conditions within any given plant are truly replicated in this determination, as well as the uncertainty associated with Reported Values it is recommended that Laboratory Values be the basis of comparison for MTBF. However, MTBF alone is a poor statement of a device's reliability. It should be used primarily as a component of the PFD calculation.

MTTR. Mean Time To Repair is the average time to repair a system, or component, that has failed. This value is highly dependent upon the circumstances of operation for the system. A monitoring system operating in a remote location without any spare components may have a tremendously larger MTTR than the same system being operated next door to the system's manufacturer. So the ready availability of easily installed spares can significantly improve MTTR.

PFD. The Probability to Fail on Demand is a statistical measurement of how likely it is that a process, system, or device will be operating and ready to serve the function for which it is intended. Among other things, it is influenced by the reliability of the process, system, or device, the interval at which it is tested, as well as how often it is required to function. Below are some representative sample PFD values. They are order of magnitude values relative to one another.

INDEPENDENT PROTECTION LAYER	PFD
Control Loop	$1,0 \times 10^{-1}$
Relief Valve	$1,0 \times 10^{-2}$
Human Performance (Trained, No stress)	$1,0 \times 10^{-2}$
Human Performance (Under stress)	0,5 x 1,0
Operator Response To Alarms	$1,1 \times 10^{-1}$

Many end users have developed calculations to determine the economic benefit to inspections and testing based upon some of the reliability numbers used to determine SIL values. These calculations report the return on investment for common maintenance expenditures such as visual equipment inspections. The premise of these calculations is to reduce the number of maintenance activities performed on systems that:

- Have a high degree of reliability, or
- Those that protect processes where monetary loss from failure would not outweigh the cost of maintenance.

The Cost of Reliability:

There is much confusion in the marketplace on the subject of SIL values. Many have confused the SIL value as a strict indicator of reliability. As described earlier in this text, reliability indicators are a very useful byproduct of SIL value determination, but are not the main focus of the measurement.

A sample calculation would be the Reliability Integrity Level (RIL):

$$RIL = a - \frac{b \bullet c \bullet d}{e}$$

where

RIL_2 = Reliability Integrity Level

a_1 = Maintenance Cost Savings as a percentage[1]

b = Dollar Loss of Process per unit of time

c = MTTR

d = Probability of failure per unit of time

e = Current cost of maintenance activity per unit of time

1

1 The savings as a percentage of total maintenance cost

2 In this sample calculation, a RIL greater than one would indicate that a given process is reliable enough to discontinue the maintenance activity. Of course, many times a process offers benefits that go beyond simple monetary considerations.

Why use a Certified product?

A product certified for use within a given SIL environment offers several benefits to the customer. The most common of these would be the ability to purchase a “Black Box” with respect to SIL requirements. Reliability calculations for such products are already performed and available to the end user. This can significantly cut lead times in the implementation of a SIL rated process. Additionally, the customer can rest assured that associated reliability statistics have been reviewed by a neutral third party.

The most important benefit to using a certified product is that of the associated certification report. Each certified product carries with it a report from the certifying body. This report contains important information ranging from restrictions of use to diagnostics coverage within the certified device to reliability statistics. Additionally, ongoing testing requirements of the device are clearly outlined. A copy of the certification report should accompany any product certified for functional safety.

Governing Specifications:

There exist several specifications dealing with Safety and Reliability. SIL values are specified in both ISA SP84.01 and IEC 61508. IEC 61511 is the specification that is specific to the Process Industry. In the table below, some of the various specifications are cross referenced so as to give an understanding of how they relate to one another.

DIN V 19250			IEC 61508/61511	VDI/VDE 2180
Demand 3	**Demand 2**	**Demand 1**		
1			No Safety Require-ments	No Safety Require-ments
2	1		No Safety Require-ments	No Safety Require-ments
3	2	**1**	No Special Safety Requirements	No Special Safety Requirements
4	3	**2**	SIL 1	Risk Area I (Lower Risk)
5	4	**3**		
6	5	**4**	SIL 2	
7	6	**5**	SIL 3	Risk Area II (Higher Risk)
8	7	**6**		
8	7		SIL 4	Can not be covered by SIS only
8			SIS Not Sufficient	