UNDERSTANDING SAFETY INTEGRITY LEVELS (SIL)

Why SIL is important and how SIL compliance benefits you.

By Byron McLendon, P.E. 6/13/2013

SCOTT SAFETY

Scott Safety Article

Understanding Safety Integrity Levels (SIL)

Defining Safety and Risk

Safety is an important consideration in process design. Safety integrity level (or SIL) is often used to describe process safety requirements. However, there are often misconceptions or misunderstandings surrounding SIL. While the general subject, functional safety and SIL, can be highly technical, the general ideas can be distilled down to a few readily understandable concepts. In this paper, we will discuss what SIL is, why it is important, what certification means, and the implications and benefits of that certification to the end user.

The Oxford dictionary definition of safety is "the condition of being protected from or unlikely to cause danger, risk, or injury" or stated another way, "freedom from unacceptable risk". Risk can be thought of both as the product of frequency of occurrence and the consequence of the hazard (risk = occurrence x consequence). Occurrence is the probability (or likelihood) that an event is realized and consequence is a measure of the severity of that event. Consequences can be framed in either relative, monetary, or injury terms. This quantification enables different risks to be compared on an objective basis and is a metric for judging the efficacy of risk reduction measures.

When it comes to risk management, there are three often competing considerations: financial, moral and legal. Financial considerations include the desire to minimize cost, maximize availability (minimize down time) and the avoidance/minimization of property damage should an event occur. Moral considerations include an organization's obligation to minimize harm to people and the environment. Legal considerations include the imposition of hazard analysis and corresponding risk reduction measures mandated by governmental agencies. Given these considerations, the question arises: how much risk reduction is enough?

ALARP and What Is Reasonable?

A widely adopted framework for answering this question is the U.K.'s Health and Safety Executive's principle known as "as low as reasonably practicable" or ALARP. The ALARP principal is flexible in that it set goals for organizations rather than being prescriptive. The concept is simple: divide the continuum of risk into three levels and base your risk reduction response on the level that applies to the scenario. The lowest level is the region where the risk is broadly recognized as acceptable or negligible. In this region, operators are not required to undertake any additional risk reduction measures. However, there is an onus on the operator to ensure that the risk is indeed "broadly recognized" as acceptable. The highest level is the intolerable risk level. Above this level risks cannot be justified on any grounds and additional risk reduction measures are mandatory. In between these two levels lies the ALARP region, where risk reduction is pursued as low as reasonably practicable.

What is meant by "reasonably practicable"? In this context, reasonably practicable means that the risk reduction measure is implemented unless it can be shown that there is a gross disproportion

between cost or effort needed to implement the safety measure and the risk reduction achieved. Note that the framework is weighted towards the implementation of the safety measure. This differs from a traditional cost-benefit analysis in that a slightly unfavorable outcome would not meet the "grossly disproportionate" standard and the risk reduction measure would have to be implemented even though it might not be financially justified. This is usually accomplished by using a weighting factor in the cost benefit analysis equation and the weighting factor increases as risk increases. While there is some judgment involved in the in performing the analysis, generally accepted guidelines have been established by governmental agencies and,in some cases, industry groups and individual companies. In order to perform this analysis, it is necessary to quantify the level of risk reduction.

The Layers of Protection

Risk management can take many forms, from the basic process control system, to the emergency response plan in case of an incident. These risk reduction measures are often referred to as layers of protection. Recall that the risk equation has two components: likelihood and consequence. Risk reduction can be accomplished by addressing either of these components. For example, consequence can be mitigated through passive measures such as a containment dike. On the other hand, likelihood can be reduced by introducing devices into the process design such as relief valves or burst disks, which serve to reduce the likelihood of a catastrophic incident. Once the basic process has been designed, including these devices to address risk reduction, there is a residual risk level associated with the design. What happens if the residual risk is still unacceptable, or in other words, is not as low as reasonably practicable? In this case, an independent safety system must be implemented.

Implementation of a safety system must be evaluated in the context of ALARP. In order to do so, risk reduction must be quantified and here is where safety integrity levels (SIL) come into play. Simply stated, SIL is a quantification of the level of risk reduction or more precisely, SIL is the quantification of reduction in the likelihood of a hazardous outcome given the presence of the safety system. The safety system's purpose is to provide one or more functions that take the process to a safe state. For each function, the quantification of risk reduction is assigned a SIL rating. It is important to note that the SIL rating is applied to the safety function, not the individual devices of the system that execute that function. Devices that execute a safety function are typically referred to as "SIL suitable" or "SIL compatible". SIL ratings provide a quantification of the reduced likelihood of a hazardous event from occurring.

The Standard of Functional Safety and SIL

The most widely adopted functional safety standard is the International Electrotechnical Commission's IEC 61508. This seven-part exhaustive standard is the umbrella standard for many industry specific standards including process, railways, nuclear, and machine safety. The standard codifies

the entire safety life cycle from concept to decommissioning. The standard outlines the requirements for SIL certification of safety functions and establishes benchmarks for risk reduction quantification. The standard divides SIL ratings into four levels, one through four, each representing an order of magnitude reduction in risk (likelihood). For example, a given process has a residual likelihood of a catastrophic event of 1 in 200. A SIL 1 safety function would reduce that likelihood to 1 in 2000; a SIL 2 function would reduce that further to 1 in 20,000. A SIL rating represents a quantification of risk reduction for a safety function in terms of order of magnitude. Note that this risk reduction is over and above the basic process control system and passive measures to reduce risk.

The Levels of Compliance and the Nature of Failure

In order to evaluate individual devices for suitability for inclusion in a safety system, it is necessary to delve into the nuances of compliance claimed by manufactures. While the IEC standard is very specific in terms of the requirements, there are various degrees to which a manufacturer can claim compliance to the standard, each affecting the risk calculation and ultimately the cost of ownership. In order to understand these nuances, it is necessary to understand this spectrum of compliance. ---

The IEC standard allows self-certification up to a level of SIL 2. This means that a manufacturer can claim compliance based upon their internal review. Another level of compliance can be an analysis and third party review of random failures. This type of review is most common for existing equipment, that has been designed and used in the field for some time. Yet a more rigorous measure of compliance would be a third party review by a notified body, which not only looks at failure likelihood but is expanded in scope to review the processes a manufacturer uses for the design of safety related equipment. To understand the differences in rigor afforded by these differing approaches, it is necessary to understand the nature of a failure or fault.

IEC 61508-4 divides failures into two categories: random and systematic. Random failures are defined as “failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware.” [4] This is a common approach to claiming SIL suitability for a particular device, especially if it has already been designed and in operation. A manufacturer performs a reliability analysis on the hardware, calculates the requisite safety parameters and claims compliance based upon the results of the analysis. An additional level rigor may be instituted by the manufacturer by having these calculations reviewed by a third party. This review may be internal by a different functional group like quality assurance, or external by a consultant. Clearly, the confidence in both these approaches relies on the capability and reputation of the manufacturer and third party reviewer. Both of these approaches, self-certification and third party review of random hardware failures ignores the second category of failure: systematic.

IEC 61508-4 defines systematic failure as “related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors.” [4] Systematic failures can be thought of as

design flaws in the hardware or errors in firmware (i.e., "bugs") that would lead to an unsafe state. It is generally recognized that systematic failures cannot be quantified, but must instead be evaluated qualitatively. Why does the standard delineate between these two types of failures and why is the consideration of systematic failures important?

Systematic Failure and the Value of Third-Party Review

A frequently cited study by the Health & Safety Executive, "Out of Control – Why control systems go wrong and how to prevent failure," ascribes 59% of failures to specification, design, and implementation. Simply put, a majority of failure causes are, in IEC terms, systematic and inherent in the device before the end user deploys it. Systematic failures are products of the process which governs the design of the device (both hardware and software). A hardware assessment alone cannot possibly account for these types of failures. Only a rigorous design process with checks and balances focused on safety can account for minimizing the occurrence of systematic failures. Third party review by a reputable notified body can assure the end user that both random hardware and systematic failures are addressed by both the design and the process used to reach that design.

The benefits of the latter approach to the end user are enormous. They are assured of a certain availability and hardware reliability, reducing cost of ownership. They are also assured that the design process used to create the device is focused on minimizing the most common causes of systematic failures.

Conclusion

In this paper, we have discussed the concept of safety integrity levels and how it applies to the end user. We have looked at the different approaches to claiming certification and the possible shortcomings with some methods. Every process owner should ask of their suppliers the basis for their claim of SIL compliance. Is the claim based on an internal calculation of random hardware failures, a third party review of hardware failures, or a third party review of both hardware & processes used to created the design, assuring compliance to the most stringent interpretation of function safety? As discussed herein, various interpretations of compliance to SIL can have a profound impact on the bottom line. Is there any reason not to choose someone adhering to the highest standard of functional safety?

For more information about best practices in gas detection or to learn more about Scott Safety's SIL 2 compliant Meridian Universal Gas Detector, please call **800-247-7257** or email us at **scottsafetymeridian@tycoint.com**. We also invite you to visit **UniversalByScott.com**.

References and Recommended Reading

[1] Safety Integrity Level Selection, Marsal & Scharpf, ©2002, ISA, ISBN 1-55617-777-1, Research Triangle Park, NC, USA

[2] Against the Gods – The Remarkable Story of Risk, Peter L Bernstein, ©1996, John Wiley & Sons Inc., ISBN 0-471-12104-5 -8-

[3] The Black Swan – The Impact of the Highly Improbable, Nassim Nicholas Taleb, © 2007, Random House Inc., ISBN 978-1-4000-6351-2

[4] IEC 61504 Functional safety of electrical/electronic/programmable electronic safety-related systems, ©2010 IEC Geneva, Switzerland.

[5] Functional Safety – An IEC SIL3 Compliant Development Process, Medoff & Faller, ©2010, Exida LLC, ISBN 978-0-9727234-8-0, Sellersville, PA, USA.

[6] Out of Control – Why control systems go wrong and how to prevent failure, 2 Crown Copyright, Health & Safety Executive, U.K.

AMERICAS

Global Headquarters
Service, Manufacturing, Offices
4320 Goldmine Rd.
P.O. Box 569
Monroe, NC 28111
US
800.247.7257
scottmarketing.scotths.us@tycoint.com

Houston
Service, Sales, Offices
1455 E Sam Houston Pkwy Ste. 190
Pasadena, TX 77503
US
800.247.7257
scottmarketing.scotths.us@tycoint.com

LATIN AMERICA

Querétaro
Service, Sales, Offices
Parque Industrial Tecnológico Innovación
Querétaro
Km 2.2, Carretera Estatal 431
El Colorado-Galindo, Bodega 4
Municipio El Marqués
Querétaro, CP 76246
442.256.3700
ScottMexico@tycoint.com

EMEA

UAE
Service, Sales, Offices
Corodex Industries – Ground Floor
Musaffah– ICAD – 1
(Industrial City Of Abu Dhabi)
Near Emirates Steel FactoryExit at Gate 5

United Kingdom
EMEA Headquarters
Manufacturing, Sales, Offices
Pimbo Road, West Pimbo
Skelmersdale, Lancashire WN8 9RA
England
+44 (0)695 711711
scott.sales.uk@tycoint.com

ANZ/APAC

Australia
ANZ Headquarters
Manufacturing, Sales, Offices
137 McCredie Road
Guildford NSW 2161
Australia
131 772 (+61 2 8718 2191)
scott.sales.ANZ@tycoint.com

CHINA

China
China Headquarters
Manufacturing, Sales, Offices
Building 1, Lane 995, Jinhai Rd.
Shanghai 201206
China
+86 21 61633377 Ext. 1502
lspcomms@tycoint.com

SCOTT SAFETY