Functional safety in process industry

Manju Kurien
Department of Instrumentation,
Vivekanand Education Society's Polytechnic
Sindhi Society,Chembur, Mumbai, India.

Saroj Desai
Department of Instrumentation,
Vivekanand Education Society's Polytechnic
Sindhi Society,Chembur, Mumbai, India.

Lata Upadhye
Department of Instrumentation,
Vivekanand Education Society's Polytechnic
Sindhi Society,Chembur, Mumbai, India.

Abstract- In this paper, a brief idea of the objective and importance of Functional Safety in industry is given including the reliability and the formula for risk. Functional Safety Standards in process system is briefly mentioned. The notion of functional safety can be defined as the trustworthiness of a computing system which allows reliance to be justifiably placed on the service it delivers. The detailed description of SIS, SIF, Safety life cycle and SIL is given next including SIL verification methods. Performance for systems based on SIL level is analyzed. An overview of methods to determine the SIL is given briefly. The methods include ALARP, risk matrix and LOPA.

Keywords – Functional safety, SIS,SIF,SIL,PFD,safety life cycle

I. INTRODUCTION

Functional Safety is the part of the overall safety of a system or piece of equipment that depends on the system or equipment operating correctly in response to its inputs, including the safe management of likely operator errors, hardware failures and environmental changes. The objective of Functional Safety is freedom from unacceptable risk of physical injury or damage to the health of people either directly or indirectly (through damage to property or to the environment).

Functional safety has a two-fold objective: guaranteeing that systems work and that they work safely. Therefore, functional safety can be seen as a method for developing a system that attains the proprieties of reliability, availability, maintainability and safety. In addition, the application of an overall safety lifecycle guarantees that these proprieties are maintained from conception to decommissioning. Functional safety is based on three major axes: people, procedures and methods. The results of a recent study by the HSE (Health, Safety and Environment) on the causes of accidents, shown in Figure below, support this strategy that people, procedures and methods are capital for the reduction of faults and accidents.

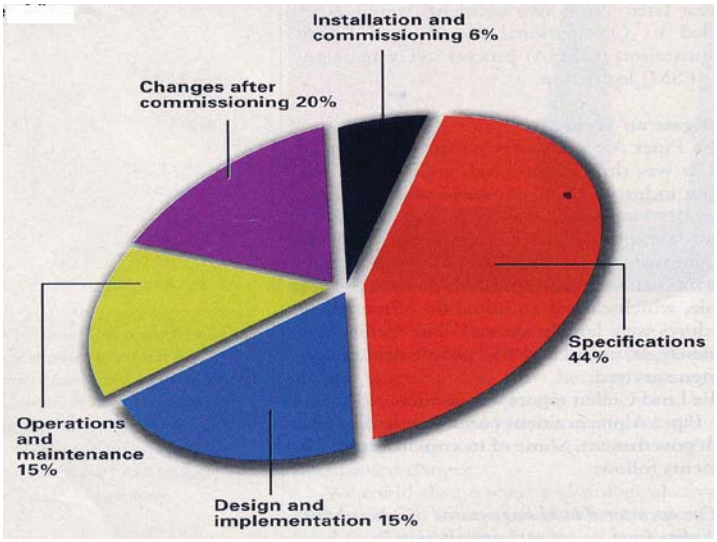

Figure1. Diagram for Causes of control and safety system failure

The distribution of statistics from the diagram is: Operation and Maintenance 15%, Changes after commissioning 20%, Requirement specification 44%, Design and implementation 15% Installation and Commissioning 6%.

II. INDUSTRIAL FUNCTIONAL SAFETY

Nothing is more important than safety to the process control industries where high temperature, pressure, flammable and toxic materials are just some of the issues faced on a daily basis. Industrial safety in pre-digital eras centered mainly on safe work practices, hazardous materials control, and the protective "armoring "of personnel and equipment. Today, safety penetrates far deeper into more complex manufacturing infrastructures, extending its protective influence all the way to a company's bottom line. Contemporary safety systems reduce risk with operational advancements that frequently improve reliability, productivity and profitability as well.

A. Achieving functional safety-

Neither safety nor Functional Safety can be determined without considering the system as a whole and the environment with which it interacts. Functional Safety is inherently end-to-end in scope. This means that though Functional Safety standards focus on Electrical, Electronic and Programmable Systems (E/E/PS), in practice Functional Safety methods have to extend to the non-E/E/PS parts of the system that the E/E/PS actuates, controls or monitors. Functional Safety is achieved when every specified safety function is carried out and the level of performance required of each safety function is met. This is normally achieved through the following steps:

1. Identifying what the required safety functions are. This means the hazards and safety functions have to be known.
2. Assessment of the risk-reduction required by the safety function. This will involve a Safety Integrity Level (SIL)
3. Ensuring the safety functions performs as per the recognized Functional Safety standard. In Europe, that Standard is IEC EN 61508, or one of the industry specific standards derived from IEC EN 61508, or ISO 13849.

B. Functional Safety Standards in process system -

Any claim of Functional Safety for a component, subsystem or system should be independently certified to one of the recognized Functional Safety standards. A certified product can then be claimed to be Functionally Safe to a particular Safety Integrity Level or a Performance Level in a specific range of applications; the certificate is provided to the customers with a test report describing the scope and limits of performance.

The principles underpinning Functional Safety were developed in the military, nuclear and aerospace industries, and then taken up by rail transport, process and control industries developing sector specific standards. Functional Safety standards are applied across all industry sectors dealing with safety critical requirements. Thousands of products and processes meet the standards based on IEC EN 61508: from bathroom showers, automotive safety products, medical devices, sensors, actuators, diving equipment, Process Controllers and their integration to ships, aircraft and major plant.
IEC 61511 is the most important standard as it is written specifically for the Process Industries.
IEC 61511-1, Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements, based on EN 61508
IEC 61511-2, Functional safety – Safety instrumented systems for the process industry sector – Part 2: Guidelines for the application of IEC 61511-1, based on EN 61508
IEC 61511-3, Functional safety – Safety instrumented systems for the process industry sector – Part 3: Guidance for the determination of the required safety integrity levels, based on EN 61508

C.Understanding Risk-

All safety standards exist to reduce risk. The goal of eliminating risk and bringing about a state of absolute safety is not attainable. More realistically, risk can be categorized as being negligible, tolerable or unacceptable. The foundation for any modern safety system has to reduce risk to an acceptable or tolerable level. In this context, safety can be defined as freedom from unacceptable risk.
The formula for risk is:
RISK = HAZARD FREQUENCY x HAZARD CONSEQUENCE
Risk can be minimized initially by inherently safe process design, by the Basic Process Control System (BPCS), and finally by a safety shutdown system.

III. LAYERED PROTECTION

Much evaluation work, including a hazard and risk assessment, has to be performed by the customer to identify the overall risk reduction requirements and to allocate these to independent protection layers (IPL). No single safety measure can eliminate risk and protect a plant and its personnel against harm or mitigate the spread of harm if a hazardous incident occurs. For this reason, safety exists in protective layers: a sequence of mechanical devices, process controls, shutdown systems and external response measures which prevent or mitigate a hazardous event. If one protection layer fails, successive layers will be available to take the process to a safe state. If one of the protection layers is a safety instrumented function (SIF), the risk reduction allocated to it determines its safety integrity level (SIL). As the number of protection layers and their reliabilities increase, the safety of the process increases.
The Figure below shows the succession of safety layers in order of their activation.

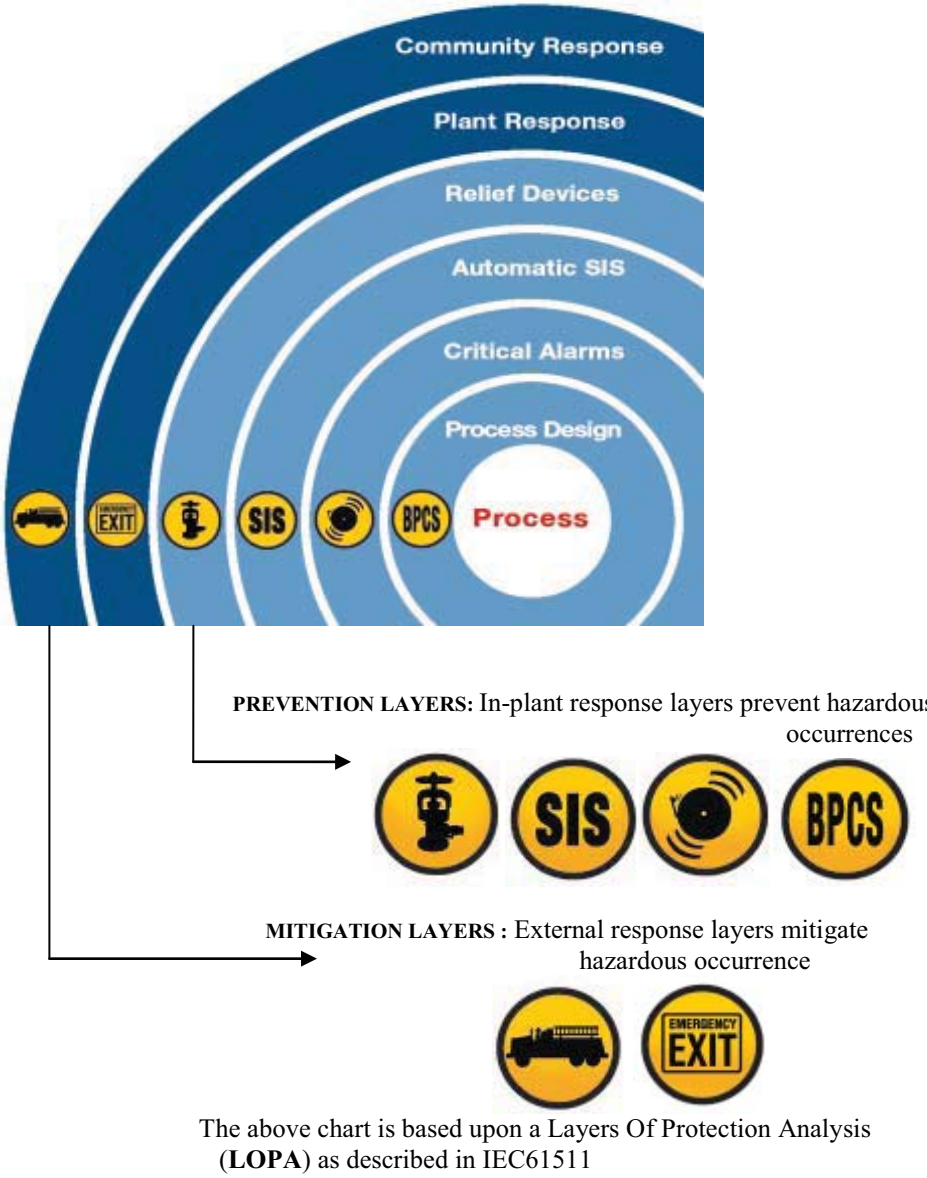

Figure2. Layers of Protection

Safety is provided by layers of protection. These layers start with safe and effective process control, extend to manual and automatic prevention layers, and continue with layers to mitigate the consequences of an event.

The first layer is the Basic Process Control System BPCS. The control system itself provides significant safety through proper design of process control.

The next layer of protection is also provided by the control system and the system operators. Automated shutdown sequences in the process control system combined with operator intervention to shut down the process are the next layer of safety.

The third layer is the Safety Instrumented System SIS. It is a safety system independent of the process control system. It has separate sensors, valves and logic system. No process control is performed in this system. These layers are designed to prevent a safety related event. If a safety related event occurs there are additional layers designed to mitigate the impact of the event.

The fourth layer is an active protection layer. This layer may have valves or rupture disks designed to provide a relief point that prevents a rupture, large spill or other uncontrolled release that can cause an explosion or fire.

The fifth layer is a passive protection layer. It may consist of a dike or other passive barrier that serves to contain a fire or channel the energy of an explosion in a direction that minimizes the spread of damage.

The final layer is plant and emergency response. If a large safety event occurs this layer responds in a way that minimizes ongoing damage, injury or loss of life. It may include evacuation plans, fire fighting, etc.
Overall safety is determined by how these layers work together.
Hazards Analysis: The levels of protective layers required are determined by conducting an analysis of a process's hazards and risks known as a Process Hazards Analysis (PHA). Depending upon the complexity of the process operations and the severity of its inherent risks, such an analysis may range from a simplified screening to a rigorous Hazard and Operability (HAZOP) engineering study, including reviewing process, electrical, mechanical, safety, instrumental and managerial factors. Once risks and hazards have been assessed, it can be determined whether they are below acceptable levels. If the study concludes that existing protection is insufficient, a Safety Instrumented System (SIS) will be required.

IV. THE SAFETY INSTRUMENTED SYSTEM (SIS)

The Safety Instrumented System is an instrumentation and control system that detects out-of-control process conditions, and automatically returns the process to a safe state. SIS provides a protective layer around industrial process systems, between the hazards of the process and the public (the worse the potential hazard, the more layers required for prevention/protection). SIS consists of an engineered set of hardware and software controls which are especially used on critical process systems. SIS is engineered to perform "specific control functions" to failsafe or maintain safe operation of a process when unacceptable or dangerous conditions occur. SIS must be independent from all other control systems that control the same equipment in order to ensure SIS functionality is not compromised.
SIS is composed of the same types of control elements (including sensors, logic solvers, actuators and other control equipment) as a Basic Process Control System (BPCS). However, all of the control elements in an SIS are dedicated solely to the proper functioning of the SIS.

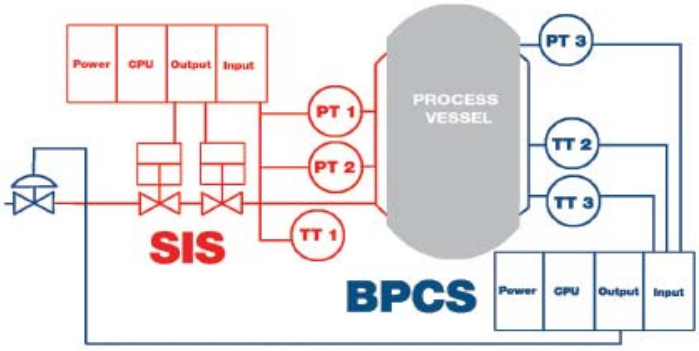

Figure3. Process schematic showing functional separation of SIS (red) and BPCS (blue).

A.SIF: Safety Instrumented Functions-

SIF is the safety functions assigned to instrumentations or the specific control functions performed by SIS.They are implemented as part of an overall risk reduction strategy which is intended to eliminate the impact of the risk event. SIF is designed to minimize process risks to a tolerable level (or ALARP). Each SIF is assigned a Safety Integrity Level (SIL) during SIL analysis which is implemented by a SIS in order to achieve or maintain a safe state. A SIF's sensors, logic solver, and final elements act in concert to detect a hazard and bring the process to a safe state.
An example of a SIF: A process vessel sustains a buildup of pressure which opens a vent valve. The specific safety hazard is overpressure of the vessel. When pressure rises above the normal set points a pressure-sensing instrument detects the increase. Logic (PLC, relay, hard-wired, etc.) then opens a vent valve to return the system to a safe state. In fact, the increased availability and use of this reliability data has allowed the traditional example above to be improved using HIPPS (High Integrity Process Pressure System) to eliminate even the risk of venting to the environment. When HIPPS is implemented, the system controls are so thorough and reliable that there is no need to vent, or use a relief valve.

B.The Safety Life Cycle-

The Safety Life Cycle is a sequential and systematic approach to developing a Safety Instrumented System (SIS). It is an engineering process designed to achieve a risk-based level of safety with performance criteria that allow versatile technologies and optimal design solutions. Safety Life Cycle is designed to minimize risk. A simplified version is shown here.

Figure 4. Safety Life Cycle

V. SAFETY INTEGRITY LEVEL (SIL)

In parallel with the allocation of the overall safety requirements to specific safety functions, a measure of the dependability or integrity or reliability of those safety functions is required. This measure is the safety integrity level or SIL according to IEC/EN 61508. More precisely, the safety integrity of a system can be defined as "the probability (likelihood) of a safety-related system performing the required safety function under all the stated conditions within a stated period of time." SILs are measures of the safety risk of a given process or it is a way to indicate the tolerable failure rate of a particular safety function. It is the standard referring to the level of performance required from SIF. Each SIF is assigned a SIL during SIL analysis. SIL is a measure of safety system performance; it is not a direct measure of process risk.
Since SIL is a measure of the amount of risk reduction provided by a SIF, SIL selection is an exercise in analysing the risk of the hazard and determining how much risk reduction is required to achieve a tolerable level of risk. Therefore, SIL is a unit of measurement for quantifying risk reduction. A SIL is determined based on a number of quantitative factors in combination with qualitative factors such as development process and safety life cycle management

A. Four Levels of Integrity-

It is a well-known fact that technical equipment can pose a safety risk so dangerous that people should not be exposed to the equipment. In such cases, the relevant risks must be reduced to meet the need for safe operation. It must be possible to quantify (and measure) risk reduction in order to satisfy this requirement. This is achieved using

the SIL "unit", in which only whole values are defined within a range from 1 to 4 making overall 4 layers of SIL. Here, safety is stratified into four discrete *levels* of safety.Each level represents an order of magnitude of risk reduction.

SIL 0/none – lowest risk
SIL 1 – 95% of the SIFs
SIL 2 – 5% of SIFs
SIL 3 – < 1% (not likely in refineries, but possible in off- shore platforms or nuclear)
SIL 4 – highest risk (only seen in nuclear industry

SIL verification involves multiple equations to determine the achieved SIL. Some of the components to verify this include:

1) MTTFS (Mean time to failure): the length of time a device or other product is expected to last in operation. MTTF is one of many ways to evaluate the reliability of pieces of hardware or other technology
2) PFD
3) RRF

Generic term describing system performance in terms of safety is safety availability. The compliment of safety availability is referred to as PFD or Probability of Failure on Demand. Or, Safety Availability is the complement of PFD (i.e., 1-PFD). PFD represents the amount of risk reduction that can be provided by a preventive SIF. PFD is also the probability a device will fail to perform its required function when it is called upon to do so. The average PFD (PFDavg- failure rate of all elements within a SIF) is used for SIL evaluation. As per their definition in IEC 61511 (ISA 84.00.01) SIL are order of magnitude bands of average PFD (PFDavg). But these numbers are so small; therefore the reciprocal of PFD is commonly used known as RRF or Risk Reduction Factor.

The ranges for each of the four SIL levels defined in the standard are presented in the table given below. All of these metrics are commonly used in industry.

Table -1 Performance for systems based on SIL level:

Safety integrity Level (SIL)	Probability of Failure on Demand (PFD)	Safety Availability (1-PF)	Risk Reduction Factor (1/PFD)	Qualitative Consequence
4	0.0001-0.00001	99.99-99.999%	10000-100000	Potential for fatalities in the community
3	0.001-0.0001	99.9-99.99%	1000-10000	Potential for multiple on-site fatalities
2	0.01-0.001	99-99.9%	100-1000	Potential for major on-site injuries or a fatality
1	0.1-0.01	90-99%	10-100	Potential for minor on-site injuries

SIL 1 is the lowest level of Safety Integrity that is defined by safety availability by at least 90% up to 99%, providing one order of magnitude of risk reduction. SIL 2 is an order of magnitude safer than SIL 1 in terms of its safety availability with 99% and up to 99.9%. SIL 3 is an order of magnitude on top of SIL 2 in terms of safety availability, and SIL 4 follows accordingly. SIL 4 is rarely seen in the process industries, and is often reserved for application to other non-process related industries that could be covered by international standards for Safety Instrumented System design. If a SIL selection process results in a requirement for SIL 4 the user should proceed with care and obtain the assistance of experts.

The governing standards for Safety Instrumented Systems state that the components of SIS must be tested frequently enough to reduce the PFD and meet the target SIL.A formal process of hazard identification is performed by the project team engineers and other experts at the completion of the engineering design phase of each section of the process, known as a Unit of Operation. This team performs a systematic, rigorous, procedural review of each point of possible hazard, or "node", in the completed engineering design. This review and its resulting documentation is called a HAZOP(hazard and operability) study. SIS will have specified SIL rating. Based on HAZOP study recommendations and the SIL rating of the SIS, the engineering, the BPCS and the SISs designs for each unit operation can be finalized.

B.SIL Determination Methods-

For the purposes of performing SIL selection, companies often represent their risk tolerance in terms of either risk matrices or Tolerable Maximum Event Likelihood (TMEL) Tables.Based on process risk issues there are various methods to determine the required SIL level. Such methods as per the IEC 61508 and 61511 standards are:

1. As Low As Reasonably Practical (ALARP)
2. Risk matrix
3. Layer of Protection Analysis (LOPA)

1. ALARP hinges on 3 overall levels of risk and economics associated with lowering the risk. The 3 levels are defined as “unacceptable”, “tolerable”, and “broadly acceptable”
2. Risk matrix: It is a method categorizing the frequency or likelihood and severity of a risk event using multiple qualitative levels. The risk tolerance is represented here with risk matrix. An example of risk matrix is shown below:

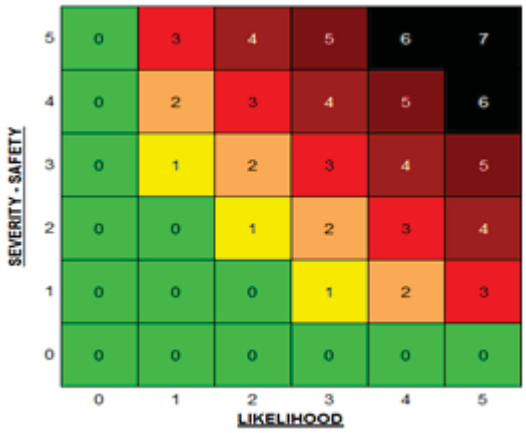

Figure 5. Risk matrix

3. Layer of Protection Analysis (LOPA): In this analysis, there are multiple layers of protection in any process plant. Each layer will have its own associated level of performance or risk reduction. To determine the level of performance of each safety layer, specificity, independence, dependability and auditability are to be considered. The figure below presents a graphical depiction of the concept of layer of protection analysis, where each concentric sphere contains the process risk with it. In order for a process hazard to escape it will need to go through all of the layers.

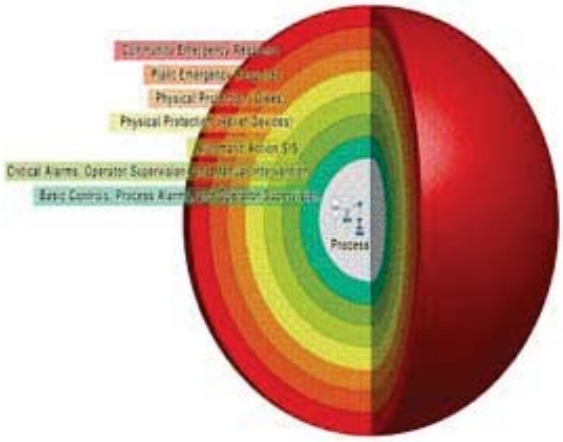

Figure 6. Graphical depiction of the concept of layer of protection analysis

VI. CONCLUSION

In this paper, the importance of functional safety in process industry is analyzed. Safety Instrumented Systems (SIS), Safety Instrumented Function (SIF) and Safety Integrity Level (SIL) are analyzed in detail. The strategies guarantee to protect personnel, equipment and the environment by reducing the likelihood (frequency) or the impact severity of an emergency event in the process industry. Furthermore, better overall safety can be achieved by reducing the risk to a tolerable level. These improvements were possible because of the different methods to analyze SIL. To understand how functional safety is quantified in IEC 61508/61511 through the various aspects of analysis, the following diagram helps:

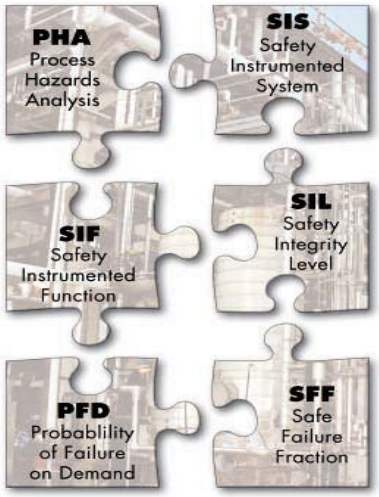

Figure 7. Graphical depiction showing how functional safety is quantified through the various aspects of analysis

REFERENCES

[1] PEPPERL+FUCHS Safety Integrity Level Manual

[2] Mitchell, KJ, Longendelpher, TM, Kuhn, MC, "Safety Instrumented Systems Engineering Handbook", Kenexis, Columbus, OH, USA, 2010..

[3] D. Smith, K. Simpson, "Safety Critical Systems Handbook - A Straightforward Guide to Functional Safety, IEC 61508 (2010 Edition) and Related Standards" (3rd Edition, ISBN 978-0-08-096781-3).

[4] M. Charlwood, S Turner and N. Worsell, UK Health and Safety Executive Research Report 216, "A methodology for the assignment of safety integrity levels (SILs) to safety-related control functions implemented by safety-related electrical, electronic and programmable electronic control systems of machines", 2004. ISBN 0-7176-2832-9

[5] Marszal, Edward, "Safety Integrity Level Selection - Systematic Methods Including Layer of Protection Analysis", The Instrumentation, Systems, and Automation Society, Research Triangle Park, NC, USA, 2002.

[6] F. Redmill, "Understanding the Use, Misuse Of SILs" http://www.csr.ncl.ac.uk/FELIX_Web/3A.SILs