



Understanding Safety Integrity Levels

Article By:

Meredith Christman,

Product Marketing Manager, IMI division of PCB Piezotronics

Carrie Termin,

Regulatory Affairs and Product Certification Specialist, PCB Piezotronics



IMI SENSORS
A PCB PIEZOTRONICS DIV.

Understanding Safety Integrity Levels (SIL)

Article by:

Meredith Christman, Product Marketing Manager, IMI division of PCB Piezotronics

Carrie Termin, Regulatory Affairs and Product Certification Specialist, PCB Piezotronics

Electrical, electronic and programmable electronic (E/E/PE) systems have played an integral part in the operation of most commercial and industrial machinery since the Second Industrial Revolution in the early 20th century. While these systems have performed non-safety functions for more than a century, it is only in the last 50 years or so that these same E/E/PE systems have taken on product safety functions as well. Examples of E/E/PE systems performing safety functions are prevalent in everyday life, including in the automotive, transportation, medical and manufacturing industries. Below are some real-world examples:

- Automobile gas tank shut-off sensors to prevent overflow of gas tank.
- Automobile tire sensors to warn of low pressure.
- Furnace sensors that extinguish flames when service door is removed.

But what happens when an E/E/PE system tasked with a safety function fails? Tragically, the scenario often ends with catastrophic consequences. There have been several head-on train crashes in the last twenty years as a result of malfunctioning rail signal systems.

To ensure that an E/E/PE system with safety function responsibilities responds reliably and appropriately when a potentially-hazardous situation arises, the concept of functional safety was developed. Functional safety is the control of hazards associated with the failure and/or malfunction of an E/E/PE system tasked with safety functions in order to reduce the risk for human injury associated with those hazards to an acceptably low level.

International Electrotechnical Commission's Standard 61508

There are a number of industry-specific standards related to functional safety programs, but the most comprehensive, non-industry program is administered by the International Electrotechnical Commission (IEC) via IEC Standard 61508, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems. The standard lays out a safety life cycle that can be divided into two major phases:

- Analysis of unmitigated hazards and their resulting risk levels.
- Implementation of mitigation solutions (ie. Safety Instrumented Systems [SIS] or Safety Instrumented Function [SIF] operating independently of the E/E/PE system) to minimize hazards and resulting risk levels.

The analysis process starts long before a single component goes on to the manufacturing floor, beginning when the equipment is nothing more than a line drawing on paper. Per IEC Standard 61508, the analysis phase of the process (Process Hazard Analysis) can utilize one of three different methodologies - Hazardous event severity matrix (also known as the Qualitative Method), Quantitative Method and Risk Graph. (There are other IEC Standards that reference other acceptable methodologies for determining SIL requirements.)

Regardless of method selected, the goal of the analysis phase is to identify hazards associated with the failure of an E/E/PE system without a SIS/SIF and the resulting risk. (Risk is determined by multiplying hazard frequency by hazard consequence.) The actual risk is then compared to the tolerable/acceptable risk target; if the actual risk exceeds the target, then a risk reduction mechanism must be put in place in the form of an SIS/SIF. The SIS/SIF can typically only lower risk by reducing the hazard frequency; it has little to no effect on the hazard consequence.

The level of mitigation that must be provided by the SIS/SIF to reduce risk to a tolerable/acceptable level is called a Safety Integrity Level (SIL). There are four SILs, each representing an order of magnitude of risk reduction with SIL1 providing the least risk mitigation and SIL4 providing the greatest risk mitigation. The level of needed risk mitigation determines the target SIL of the SIS/SIF.

| Risk Reduction Factors and Applicable SILs | |
|--|------------------------------|
| Risk Reduction Factor | Safety Integrity Level (SIL) |
| 10 to 100 | SIL 1 |
| 100 to 1,000 | SIL 2 |
| 1,000 to 10,000 | SIL 3 |
| 10,000 to 100,000 | SIL 4 |

Once the target SIL of the SIS/SIF is determined, the safety life cycle moves from the analysis phase to the implementation phase. In addition to a specified risk reduction factor, each SIL also specifies two Probability of Failure data points, depending on whether the SIS/SIF will see high demand or low demand. A higher SIL value represents a lower probability of failure.

- Probability of Failure on Demand (PFD): Failure rate range for a low-demand/intermittent-operation SIS/SIF.
- Probability of Failure per Hour (PFH): Failure rate range for a high demand/continuous-operation SIS/SIF.

| SIL and Acceptable Failure Rate Depending on Demand Mode | | |
|--|----------------------------------|---------------------------------|
| Safety Integrity Level (SIL) | Probability of Failure on Demand | Probability of Failure per Hour |
| SIL 1 | 10^{-1} to 10^{-2} | 10^{-5} to 10^{-6} |
| SIL 2 | 10^{-2} to 10^{-3} | 10^{-6} to 10^{-7} |
| SIL 3 | 10^{-3} to 10^{-4} | 10^{-7} to 10^{-8} |
| SIL 4 | 10^{-4} to 10^{-5} | 10^{-8} to 10^{-9} |

To ensure that the Probability of Failure of the overall SIS/SIF falls within the acceptable range of the target SIL:

- Individual components must be selected and their individual Probabilities of Failure considered.
- Proof testing of the SIS/SIF as an entirety must be performed to ensure that everything is working properly and as expected. Proof testing includes wiring and operation of the SIS/SIF as an entire unit.

Typically, the components included in a SIS/SIF are sensors (for measurement of process parameters), logic solvers (for interpretation of process and parameters and execution of response) and final elements (for implementation of logic solver's response). As referenced above, the individual components' Probabilities of Failure must be examined before instituting into a SIS/SIF. Typically, an individual component is considered to be acceptable within a given SIL rating if one of the two following conditions hold true:

- The component's Probability of Failure is equal to or better than the Probability of Failure range of the overall SIS/SIF's target SIL.
- The component's Probability of Failure is worse than the Probability of Failure range of the overall SIS/SIF's target SIL but it is used in conjunction with other components for a redundant system. The overall Probability of Failure for a complete redundant system will be tested out and determined as part of the proof testing.

An individual component's Probability of Failure data can usually be obtained from the component manufacturer. Manufacturers can self-certify a product by performing calculations internally or they may outsource the failure data calculations to an outside agency. The Probability of Failure data may be presented in one or multiple measurement ranges including:

- Failure in Time (FIT): Number of expected failures per one billion hours of operation.
- Mean Time Between Failure (MTBF): Number of failures per one million hours of operation.
- Mean Time to Failure (MTTF): Mean time expected until first failure.
- Probability of Failure on Demand (PFD): Probability of failure to respond to a demand.
- Probability of Failure per Hour (PFH): Probability of failure to respond per one hour of operation.

Keep in mind that the document provided by the manufacturer does NOT qualify the product to be "SIL certified" as certification applies only to an ENTIRE SIS/SIF, not an individual component. At best, the individual component can be labeled as "SIL compliant" or as "being suitable for use in a particular SIL environment."

Using IMI Products in a SIL-Certified SIS/SIF

Depending on the particular SIS/SIF being constructed, many IMI Sensors' products could be included as a sensor component. As general practice, IMI Sensors chooses to self-certify its products' Probability of Failure data. Data can be provided on a "SIL Compliant" Certificate in terms of Mean Time Between Failure (MTBF) or Mean Time to Failure (MTTF). An example of IMI Sensors' certificate is provided as reference on the next page. Probability to Failure data is provided on an as-requested basis. Contact your IMI Sensors' contact to request product failure data.



**SIL Certificate of Conformity
Manufacturer Declaration**

Product: Type: 682A06
Name: Universal Transmitter

Manufactured by: PCB Piezotronics
3425 Walden Avenue
Depew, NY 14228
USA

PCB Piezotronics as a manufacturer declares that the 682A06 device is suitable for use in a safety instrumented system up to a Safety Integrity Level of SIL 2 if the appropriate safety instructions are observed.

This certification is based on reliability calculations conducted by the original component supplier, and strict safety requirements used during the design of the product that are suitable for SIL 2 applications.

The 682A06 Universal Transmitter is considered to be a Type B component with a hardware fault tolerance (HFT) of 0.

Place: Depew, NY

Date: 04/05/16

Signature: Carrie Termin

Name: Carrie Termin

Title: Regulatory Affairs and Product
Certification Specialist

What are divisions of PCB Piezotronics?

PCB Piezotronics, a member of the PCB Group families of companies, has five major divisions, all of which offer targeted sensor technologies. These divisions are supported by an active outside direct sales force of Field Application Engineers, as well as international direct sales offices throughout the world. Individual PCB Piezotronics divisions, locations and their primary product specialties include:

 **PCB PIEZOTRONICS**^{INC.}



Depew, NY, USA - www.pcb.com – Piezoelectric, ICP®, piezoresistive & capacitive pressure, acoustic, force, torque, load, strain, shock & vibration sensors.

 **AEROSPACE & DEFENSE**
A PCB PIEZOTRONICS DIV.



Depew, NY, USA - www.pcb.com/aerospace – Sensors & Instrumentation for aerospace & defense applications, including air and spacecraft testing.

 **AUTOMOTIVE SENSORS**
A PCB PIEZOTRONICS DIV.



Novi, MI, USA - www.pcb.com/auto – Sensors & Instrumentation for automotive testing, including modal analysis; NVH; component durability; powertrain testing; vehicle dynamics; safety and regulatory testing.

 **IMI SENSORS**
A PCB PIEZOTRONICS DIV.



Depew, NY, USA - www.imi-sensors.com – Industrial vibration sensors, bearing fault detectors, mechanical vibration switches, panel meters, cables & accessories for predictive maintenance and equipment protection.

 **LARSON DAVIS**
A PCB PIEZOTRONICS DIV.



Depew, NY & Provo, UT, USA www.larsondavis.com – Precision microphones, sound level meters, noise dosimeters, audiometric calibration systems.

 **PCB PIEZOTRONICS**^{INC.}
MEMS ADVANCED DESIGN CENTER



San Clemente, CA, USA - www.pcb.com – Research & development engineering center for special technologies.

Seattle, WA, USA - www.pcb.com – Process development and fabrication of MEMS sensors.

 **PCB LOAD & TORQUE**
A PCB PIEZOTRONICS DIV.



Farmington Hills, MI, USA - www.pcb.com/LoadAndTorque – Designs and manufactures high quality, precision load cells, wheel force transducers, torque transducers, telemetry systems, and fastener torque-tension test systems.

PCB® Group Companies:

 **TMS DYNAMIC METROLOGY**
A PCB GROUP COMPANY



Cincinnati, OH, USA - www.modalshop.com – Global leader in dynamic calibration offering a complete line of automated calibration systems and recalibration services to support dynamic vibration, pressure and force sensors in applications such as: national standards, commercial labs, government/military research, consultancies, and industrial/plant floor operations.



Rochester, NY, USA - www.sti-tech.com – Mechanical engineering consulting firm specializing infinite element analysis, advance analytical techniques, experimentation, technology development, & design optimization for turbo machinery, industrial machine systems & mechanical structures.

 **IMI SENSORS**
A PCB PIEZOTRONICS DIV.

Corporate Headquarters 3425 Walden Avenue Depew, NY 14043-2495 USA
Toll-free in the USA 800-959-4464 ■ **24-hour SensorLineSM** 716-684-0003 ■ **Fax** 716-684-3823 ■ **Email** imi@pcb.com
AS9100 CERTIFIED ■ ISO 9001 CERTIFIED ■ A2LA ACCREDITED to ISO 17025