# Safe instruments

## Safe instruments for a safer process

Robert Martinez, Frank Fengler

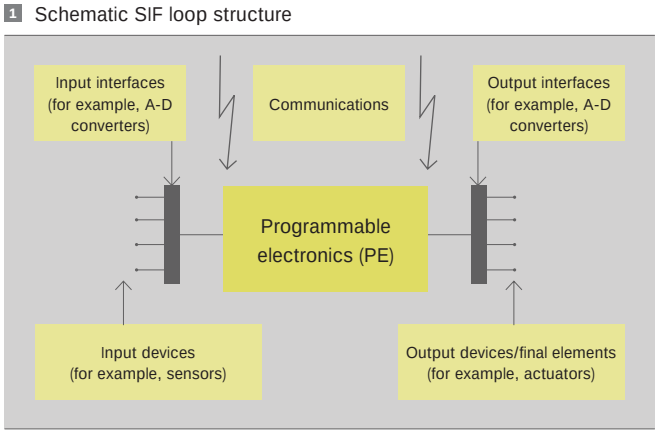
The safety of a plant, its employees and its surroundings depends on the ability of the plant to shut down or shift to a safe state should an abnormality occur. A false trigger can lead to a costly shutdown and unnecessary loss of production, whereas a failure to trigger can possibly have more far-reaching consequences. The reliability and safety of a plant is therefore dependent on the integrity of its sensors.

Instruments are classified by their Safety Integrity level (SIL). The SIL of a device determines the applications it is suitable for. In this article, ABB Review discusses failure rates, how they are quantified and how ABB goes about assuring its instruments fulfill the integrity levels that are expected of them.

For process industry system builders and operators, a hazard is the result of a misbehaving process. The safety instrumented function (SIF) must act to bring the process to a safe state. As the name implies, a SIF consists of a chain of instruments to detect this hazardous condition, manipulate the input data in a programmable device (the CPU) and then send a command to the output instruments. These output devices are also known as “actuators” because they act to bring the process under safe control or to shut it down completely. A schematic of a SIF loop is shown in 1.

The main challenge for process safety engineers is to identify all the possible hazards related to that process and then to quantify the impact each of these would have on the plant surroundings. When this “risk level” is known, the process safety engineer can choose SIF instruments with a matching Safety Integrity Level (SIL). The SIL level of the entire chain of instruments is always that of the lowest SIL component ie, “the weakest link in the chain”.

1 Schematic SIF loop structure




The IEC 61511 standard provides process engineers strict guidance for this task, but also puts responsibility on management, process operators and people in other project lifecycle phases to ensure that the process is adequately protected. This lifecycle approach is so successful that it has become the preferred model for other draft international standards for machinery, nuclear and even for security.

The classification of safety instruments by SIL level is itself an enormous achievement for industry. Born in the aftermath of the tragic chemical plant accident at Seveso, Italy in 1976, this international standard allows engineers to focus on the process hazards, confident that their safety instruments

will perform at the required level. This separation of functions is more than just a practical convenience; it carries legal obligations for both the system builder or operator and the safety instrument supplier.

To make this regime work in practice, safety instrument suppliers today must follow the rules in the ”sister” IEC standard #61508 “Functional safety of electrical/electronic/programmable electronic safety-related systems” and achieve the desired SIL certification for their products.

### “Sister” standards for safety

ABB is in the interesting position of being both an instrument supplier (eg, safety pressure transmitters) and a system builder (eg, safety and automation for oil and gas projects). Thorough knowledge of the application of the IEC safety standards is crucial in maintaining the company’s position as a safety leader.

The IEC standards for these two different levels of supply are surprisingly similar and can be mutually understood by a simple change of terms:

- For safety instrument engineers the hazard comes from within the component itself in the form of device failure.
- The process engineer performs a hazard analysis whereas the instrument engineer performs an FMEA (Failure Mode and Effect Analysis).
- For safety instrument engineers it is the impact of a dangerous event on the safe output of the device which must be assessed.

Engineers in both disciplines must quantify the likelihood of their respective dangerous events. The instrument engineers calculations result in a PFD (Probability of Failure on Demand). The PFD value can be directly mapped to a SIL level according to 2. For example, a SIL2 device must fail less than once out of every 100 demands.

### Understanding failure rates

The simple PFD value is a powerful number; not only does it determine the market for the device by virtue of its SIL certification, but it also determines the complexity and hence price of the instrument as well as the cost to the end-customer to maintain it in the field. The PFD calculation is:

$PFD = \lambda \cdot \tau / 2$

where:

$\lambda$ : number of dangerous, undetected failures per hour

$\tau$ : testing interval in hours

A lower $\lambda$ can be achieved in one of three ways:

- Re-design of critical parts
- Increased detection capability
- Increased hardware redundancy

The FMEA document provides valuable input to the first approach: re-design for greater integrity. For ABB’s 2600T pressure transmitter 2, some of the key points were; CPU and clock integrity, power supply monitoring, analog output stage integrity and software sequences. Analysis also revealed that $\lambda$ could be reduced by using an all-welded design in a critical area of the device.

The second approach to reducing $\lambda$ means adding extra circuitry and software enabling the device to detect a greater number of dangerous internal failures and alarm the system accordingly. This approach increases the Safe Failure Fraction (SFF) of the device, but at the cost of extra hardware and code development. The SFF rating of a device affects the allowable architecture if IEC 61511 or ISA-S84 is being used as the design standard. An SFF rating of 90 percent or greater is needed to use a single transmitter in a SIL2 application, for example, as shown in 3.

2 PFD failure rates

| SIL | PFD |
|---|---|
| 1 | 0.1 < PFD <= 0.01 |
| 2 | 0,01 < PFD <= 0.001 |
| 3 | 0.001 < PFD <= 0.0001 |
| 4 | 0.0001 < PFD <= 0.00001 |

3 Safe failure fraction ratings versus SIL

| SFF | 0 | 1 | 2 |
|---|---|---|---|
| < 60% | – | SIL1 | SIL2 |
| 60–90% | SIL1 | SIL2 | SIL3 |
| 90–99% | SIL2 | SIL3 | SIL4 |
| > 99% | SIL3 | SIL4 | SIL4 |

The third approach involves duplicating critical elements to achieve greater Hardware Fault Tolerance (HFT). In ABB’s SIL pressure transmitter, for example, a differential inductive sensor provides two independent signals proportional to input pressure and a dual architecture processes these signals independently.

In 3, the columns numbered 0,1,2 refer to the number of simultaneous hardware faults which the device can tolerate. Increasing redundancy clearly has a beneficial effect on SIL but at the cost of some duplicated hardware.

The standard has a loophole which allows suppliers to claim a higher HFT if the device is “proven-in-use”. Proven–in-use imposes a significant burden on the supplier who often does not have access to high-quality, long-term historical data showing device failures. Without such data, it is recommended that safety transmitters, for example, have a HFT value of 1.

It is particularly important that software failures be included in this SFF analysis. As software in instrumentation gets more and more complex, field failures due to systemic software errors are increasing. Therefore, any assessment of a device must include the potential software failures and/or have reliable software diagnostics built-in to the device.

### Understanding MTBF

Mean Time Between Failures (MTBF) is defined as the inverse of the Safe Failure Rate. The $\lambda$ data is normally presented in terms of “FITs”, failures-in time. Typical FIT data is expressed in $10^{-9}$, or the number of failures per one billion hours usage.

$MTBF = 1/\lambda$ (for 1oo1 architecture[1)])

There is often a trade-off between SFF and MTBF. For instance, one transmitter on the market has a SFF of 96.7 percent and an $\lambda$ rating of 963, while another has specifications of 70 percent and 490. The first achieves the 90

Footnote

1) 1oo1 is explained later on in the article.

percent SFF criteria for single device usage in SIL 2 applications but has an MTBF that is half of the second device. What the user needs to understand is that safety transmitters are designed to have a very high reliability in terms of their main function but may be less reliable from a pure MTBF perspective. A good rule of thumb for a safety transmitter, therefore, is to specify a minimum of a 100-year MTBF value.

### Proof testing to maintain integrity in operation

The second term in the PFD calculation, $\tau$, represents the hours between mandatory proof-testing of the device when in operation. This is a luxury for device suppliers since frequent testing has a beneficial effect on SIL. Operators, however, must bear the burden of proof-testing every such device as often as several times a year – a part of the lifetime operating cost that will not go unnoticed at purchasing time.

As a general rule, actuators such as solenoid-operated valves represent at least 50 percent of the dangerous undetected failures of the entire SIF loop. The sensor accounts for approximately 30 to 40 percent and the remainder is attributed to the CPU and I/O boards, collectively known as the “logic solver”.

The research and development effort invested to achieve the lower failure rates in ABB SIL instrumentation is worth the effort. The typically high failure rates of actuators is an opportunity for sensor and logic-solver suppliers such as ABB to reduce their product’s PFD values so that the SIL of the entire safety loop can be preserved. Lower PFD values translate into lower costs and simplified engineering for end customers because they will not need to boost SIL by specifying redundant transmitters or by choosing more expensive actuator valves.

Automation vendors have only recently started to exploit fieldbus-based diagnostic capabilities to offer on-line proof-testing. Such a technique eliminates field visits and will maybe one day even be fully automated. The ABB Corporate Research Center in Norway has investigated this technique for the proof-testing of actuators such as valves by executing a partial-stroke only, allowing production to continue uninterrupted. Fieldbus diagnostics carry stroke test data to the logic solver where potentially dangerous failures can be detected. In this way, they decrease the device’s $\lambda$ and allow operators to wait longer between mandatory full shut-downs for valve testing. The research center is also investigating the use of new safety variants of Profibus and Fieldbus Foundation to complete the picture for robust safety asset management.

### Safety Instrument Portfolio

ABB supplies a range of safety pressure transmitters that use a variety of sensing methods. ABB also offers a range of temperature sensors, positioners and a flowmeter all classified to SIL2. The AC800M-HI High Integrity SIL2 Safety Controller and its associated safety I/O round off the company’s safety portfolio. These SIL classifications are awarded after assessment by accredited third-party companies 4, an effort which requires ABB to provide thorough documentary proof of compliance.

The 2600T-Series pressure transmitter 5 has models certified to SIL2. 37 have recently been sold to Statoil in Norway. Other customers of ABB SIL instrumentation include Tractebel Gas Engineering GmbH (TGE), who have particular expertise in the areas of storage, conditioning and shipping of liquefied gases (LNG and LPG) and petrochemical gases.

### A tool for optimizing safety design

The complexity of trade-offs involved in safety instrument design is multiplied when an entire SIF is configured. These can be investigated and visualized in the ABB TRAC tool’s Trip Requirement and Availability Calculator. This was developed by John Hunt and Ian Bradby of ABB Engineering Services in the U.K. TRAC is a PC-based software tool used to assist safety, project and maintenance engineers in determining the optimum design configuration and periodic test intervals for safety instrumented functions. TRAC is used by ABB engineering consultants and has also been licensed for use by end-customers worldwide.

The TRAC tool provides the engineer with a systematic and consistent approach to calculating the required SIL using either Risk Graph or LOPA (Layer of Protection Analysis). TRAC is pre-loaded with both field reliability data and the manufacturer’s reliability data, including data for many of ABB’s safety instruments. All calculations discussed so far in this article are used within TRAC, permitting the user to focus on the design task.

### Finding the optimum configuration

One of the main benefits of TRAC is allowing project engineers to investigate various redundancy schemes. Some standards prescribe the use of redundancy as the cure for system reliability, but do not explain the quantitative analysis this redundancy is based upon. Risk analysis is based on probability theory and can be derived

4 ABB’s 800xA HI safety system is certified to the IEC 61508 and IEC 61511 safety standards


5 ABB’s 2600T pressure transmitter is certified to SIL2

6 Simplified PFD formulae for redundancy

| Architecture | PFD |
|---|---|
| 1001 | $\lambda \cdot \tau / 2$ |
| 1002 | $\lambda^2 \cdot \tau^2 / 3$ |
| 2002 | $\lambda \cdot \tau / 2$ |
| 2003 | $\lambda^2 \cdot \tau^2$ |

from several methods. All methods rely on certain key elements in order to provide objective analysis – failure rates, failure modes, diagnostic coverage and common cause data. The most common architectures used in the process industries are the following:

- *1oo1 One-out-of-One*
  When using a single device, the safety is affected by the dangerous failures, the reliability by the safe failures.
- *1oo2 One-out-of-Two*
  With 1oo2 voting, if either transmitter fails, then the process is tripped. This increases safety (versus 1oo1) at the expense of reliability.
- *2oo2 Two-out-of-Two*
  With 2oo2 voting, both sensors need to fail in order to trip the system. This increases reliability at the expense of safety.
- *2oo3 Two-out-of-Three*
  This architecture is very common in the process industries since you have very good safety and reliability, but at the expense of added cost.

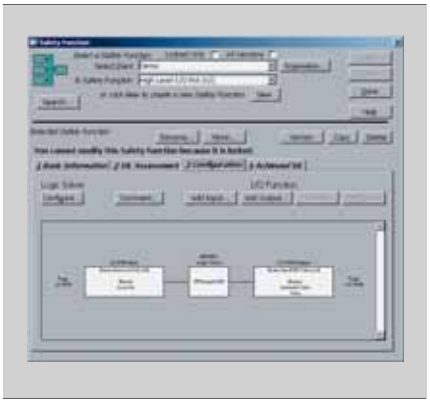
A set of simplified equations has been developed to provide a quick risk analysis based on a few key parameters of the device in question – the safe failure rate, and dangerous undetected failure rate. The analysis typically will assume the same MTTR (mean time to repair) and TI (test interval) values. The equations used are shown in 6.

The good news is that the data required for the calculations shown above is now published by most major vendors and has been included in the TRAC software package. This allows the user to perform what-if analysis, as shown in 7, to assist selection of various vendors and/or architectures.

## Finding the optimum proof test interval

The tool represents one approach to calculating SIF proof-test intervals. By focusing on the relevance of the system and consequence of failure on demand, the tool provides a range of test intervals. In many cases, this is likely to permit an extension to existing intervals. Where an integrity level is not defined, test intervals may be justifiably extended to align with the convenience of a plant shutdown or other inspection criteria such as electrical integrity – or simply just repair on breakdown. TRAC provides multiple solutions for testing inputs and outputs within the bounds of the required maximum and minimum allowable probability of failure on demand. For each span of test intervals, the cost of testing is calculated from known annual testing costs. Results are displayed graphically and a comprehensive report is issued in a fully traceable format 8.

7 TRAC tool for safety function configuration



8 TRAC tool for proof-test interval optimization


Robert Martinez
ABB Corporate Research
Billingtsad, Norway
robert.martinez@no.abb.com

Frank Fengler
ABB Automation Products GmbH
Minden, Germany
frank.fengler@de.abb.com



References

[1] IEC 61508 "Functional safety of programmable electronic safety-related systems"
[2] IEC 61511 "Functional safety – Safety instrumented systems for the process industry sector"
[3] ISA Automation West 2004, "Selection of Safety Transmitters in SIS applications, Michael Cushing", ABB Pressure Products
[4] Safety Solutions and Safe Networks Highlight Hannover Fair, ARC Insights, 28.04.2005



ABB Review Special Report
Automation Systems
March 2007





Publisher's office
ABB Schweiz AG
Corporate Research
ABB Review / REV
CH-5405 Baden-Dättwil
Switzerland





Printers
Vorarlberger Verlagsanstalt GmbH
AT-6850 Dornbirn / Austria

Layout
DAVILLA Werbeagentur GmbH
AT-6900 Bregenz / Austria





ISSN: 1013-3119

www.abb.com/abbreview