Fire and gas protection systems as part of safety instrumented systems and risk management

Garth Watkins, Director Europe, Middle East, Africa
Detector Electronics Corporation
Presented at HazardEx International Conference 2008

Process-systems operators today face increasing demands for lower costs and higher safety standards in an increasingly regulated environment. In addition, companies desire to provide a working environment that is as safe as possible. As a result, plant owners strive to improve operation and safety of their assets and extend the lifecycle to maintain profitability.

Safety Instrumented Systems (SIS) are an important part of this process, and fire and gas protection systems form an integral part of risk management.

This paper provides operators and designers of process plants an overview of the current approaches to risk reduction and the methodology required to comply with new standards for instrumented systems such as IEC 61508. (Functional safety of electrical/electronic/programmable electronic safety-related systems)

Meeting Stricter Demands

The safety industry persistently examines how to identify and mitigate hazards. Their examination intensifies after a catastrophic event. The investigation following a failure usually identifies a hazard that initiated the event – a hazard that might have been previously thought to be inoffensive or unlikely.

The UK's Buncefield Oil Depot is an installation that operated safely for years. A probe failure led to a large-scale fuel spill and resulted in a vapour cloud explosion. The six-month investigation resulted in a report: "Safety and Environmental Standards for Fuel Storage Sites." The industry now must conform to these new standards.

As demands on safety systems have increased, standards requirements have tightened. Old and new hazards must be detected and identified in fresh ways; operators cannot assume that an existing facility will continue to operate safely.

Once hazards are identified, they must be addressed. Best practices must be re-examined and adopted.

Another force in setting stricter demands is the required increase in up time and lifecycle to improve profitability. Downtime, especially unplanned, can eliminate profit.

With an imperative to keep plants running, companies are using higher quality equipment and performing careful lifecycle costing analyses. Upfront investment can mean less maintenance and a longer lifecycle.

Managing Risk

For a company to meet its obligations – reviewing hazards and operations to identify risks and eliminate or mitigate their effects – it must systematically analyze protective requirements of the operating plant.

This analysis enables layers of protection (figure 1) to be assigned to the plant and process. Layers reduce the risk by ensuring that potential consequences to the business are minimised and that plant and equipment meet operational and legal requirements.

- Process and component design – The design must be mechanically sound. Operating procedures and maintenance cycles must be suited to the demands placed on the process.
- Process controls – Sufficient and appropriate measurements must be taken to ensure that the process is operating within predetermined safety limits.
- Safety Instrumented System (SIS) – This must reduce

Detector Electronics Corporation
T: 952.941.5665 or 800.765.3473
F: 952.829.8750
www.det-tronics.com

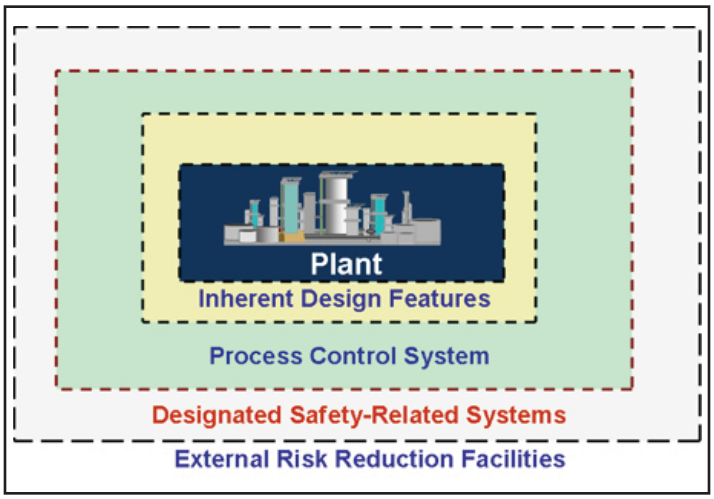

Figure 1. Layers of protection.

residual risk of failure to the agreed level – known as the Safety Integrity Level (SIL).

Reviewing SIS Requirements

A company will determine their tolerable risk levels (Figure 2). The engineers will assess the inherent risk in the operation of a process and assign risk reduction criteria to meet the tolerable risk by the assignment of SILs.

An SIS detects an unsafe or hazardous condition and returns the process to a safe condition. For example, when the detector senses a predetermined gas concentration, the SIS is configured to take some action, such as isolation or venting a vessel.

The SIS designer needs to select hardware (field devices and logic solver) that will meet the required target SIL's for each SIF, and create the cause and effect logic that will drive the process to the required safe state.

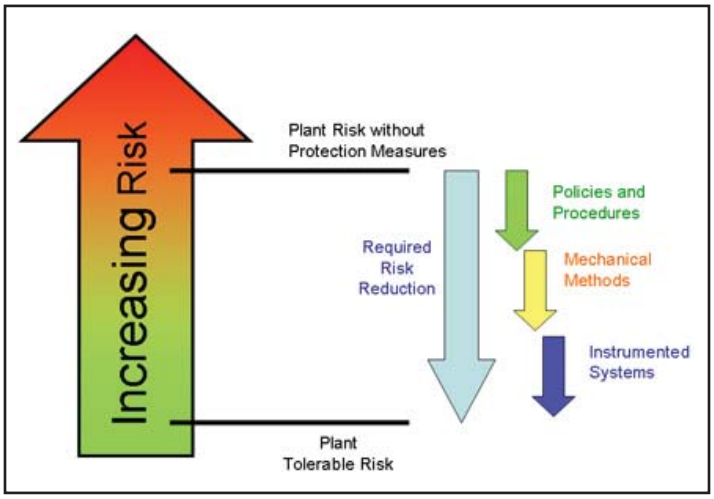

Figure 2. Tolerable risk levels.

Some detectors are self testing. However, many devices have undisclosed failures. For instance, the common catalytic flammable gas detector employs a technique that slowly destroys the sensor over time. The decay is not self revealing, and eventually the sensor stops working. The only way to know is to apply gas and measure the output.

A flame detector's ability to operate depends on clean optics. The detector used in a SIS should be self checking to ensure it can perform to specification.

In addition, because it interprets inputs from detectors and initiates outputs to bring the process into a safe condition, the logic controller must give an adequate level of integrity. Using the IEC 61511/61508 methodology, the user can determine the accrued SIL. Each safety loop is assessed from sensor through controller to output device and a measurement made of its SIL.

Assessing Fire and Gas Needs

The design of a fire and gas safety system starts with assessing the hazard. Designers ask questions such as what is the fuel and at what level should it be detected? In considering these questions, the plant is broken into zones to mitigate the hazardous event and prevent escalation.

In selecting detectors for a SIS, their performance is not the only criteria for selection. Rejecting false alarms is critical. Simple performance data is also deceptive and should be tested by third parties where performance is part of the certification.

Although many gas detectors do not fail to danger, they can experience undisclosed failures. For example, if the optics of an IR gas detector are fouled, the detector should be able diagnose the condition and raise and alarm to the operator.

Be aware that not all SIS logic controllers certified for energize to tripsystems as required by fire codes. Third-party certification needs careful review to ensure the equipment is suitable for the application i.e. fire alarm systems.

Certification is a major issue. Many AHJ require compliance with specific country-specific codes. Also, certification bodies perform impact analysis to control product changes and ensure they are made in such a way as to continue compliance.

Detector Electronics Corporation
T: 952.941.5665 or 800.765.3473
F: 952.829.8750
www.det-tronics.com

DET-TRONICS®
A UTC Fire & Security Company

Assuring SIL Certification

There are differences between products third-party certified "SIL-capable" and manufacturer "SIL suitable" claims.

SIL presented without third-party verification is based on mechanical failure assessment from a Failure Modes, Effects and Diagnostic Analysis (FMEDA). This assessment does not include the software, which in most devices forms a large part of it capabilities. This places the onus on the engineer to show that the device is suitable for the target SIF.

Certified products also have FMEDAs plus an assessment of the firmware with fault injection testing to verify the performance of the device to the claimed SIL. Third-party certification provides the engineer proof that the device has been truly put through its paces to ensure suitability for the target SIF with minimal extra work for the engineer. This safety data is published in the safety manual that should accompany the product.

Detector Electronics Corporation
T: 952.941.5665 or 800.765.3473
F: 952.829.8750
www.det-tronics.com

DET-TRONICS®
A UTC Fire & Security Company