An Introduction

Safety Instrumented Systems
Safety Integrity Levels

Background

It was a calm, crisp day the morning of December 11, 2005 in southeast England. Being Sunday morning most citizens were off from their work and enjoying the remaining hour of their sleep, or perhaps beginning their ablutions in preparing to go to their local Church meeting. At 6:01am local time in Hertfordshire, England many lives were changed forever when the first explosion rocked the Buncefield oil storage depot. It was said that at least one of the initial explosions were of "massive proportion" the likes of which England had not seen since World War II.

At the Buncefield depot area significant damage occurred to both commercial and residential property in the area, 20 fuel storage tanks and the majority of the site was engulfed in a massive fire which burned for several days. Forty-three people were injured, 2000 people evacuated from the immediate surrounding area and it is estimated that the cost impact was nearly £1 billion ($1.6 billion). By Grace there were no fatalities.

What happened? The final report of the Major Incident Investigation Board (MIIB) that investigated the Buncefield accident published its final report at the end of 2008. Volume 1 of the report contains the detail, this being over 100 pages in total length. Late in the afternoon of Saturday December 10th, the day before the explosion, a fuel delivery began to arrive at one of the tanks at the Buncefield facility. Unfortunately, the safety systems that were in place to shut off the supply of the fuel to prevent overfilling of the tank failed to operate. As overfilling continued, about 10% of the 300 tons of fuel that had overfilled the tank turned to vapor. The vapor concentration grew and became capable of supporting combustion. The vapor cloud was visible on security film and also witnesses that were nearby the facility reported seeing the vapor cloud. A severe explosion resulted and a massive fire.

Safety Instrumented System

The investigation authorities on the Buncefield accident also indicated that appropriate safety level systems should be employed to prevent this type of accident from occurring again and they referenced IEC 61511 as the standard involved with these types of safety systems.

Actually there are two standards issued in regards to process safety, IEC 61508 and IEC 61511. IEC 61508 preceded 61511 and is targeted primarily to suppliers or manufacturers of equipment. IEC 61508 specifies Safety Integrity Levels (SIL) for systems and devices within Safety Instrumented Systems (SIS) based on the probability of a failure of the device.

To meet a given SIL, the device needs to have less than a specified probability of dangerous failures according to the standard, and also have greater than the specified safe failures. Failure probabilities are calculated by performing a Failure Modes and Effects Analysis (FMEA).

PFD (Probability of Failure on Demand) and RRF (Risk Reduction Factor) for different SILs as defined in IEC61508 are as follows:

SIL	PFD	RRF
1	0.1-0.01	10-100
2	0.01-0.001	100-1000
3	0.001-0.0001	1000-10,000
4	0.0001-0.00001	10,000-100,000

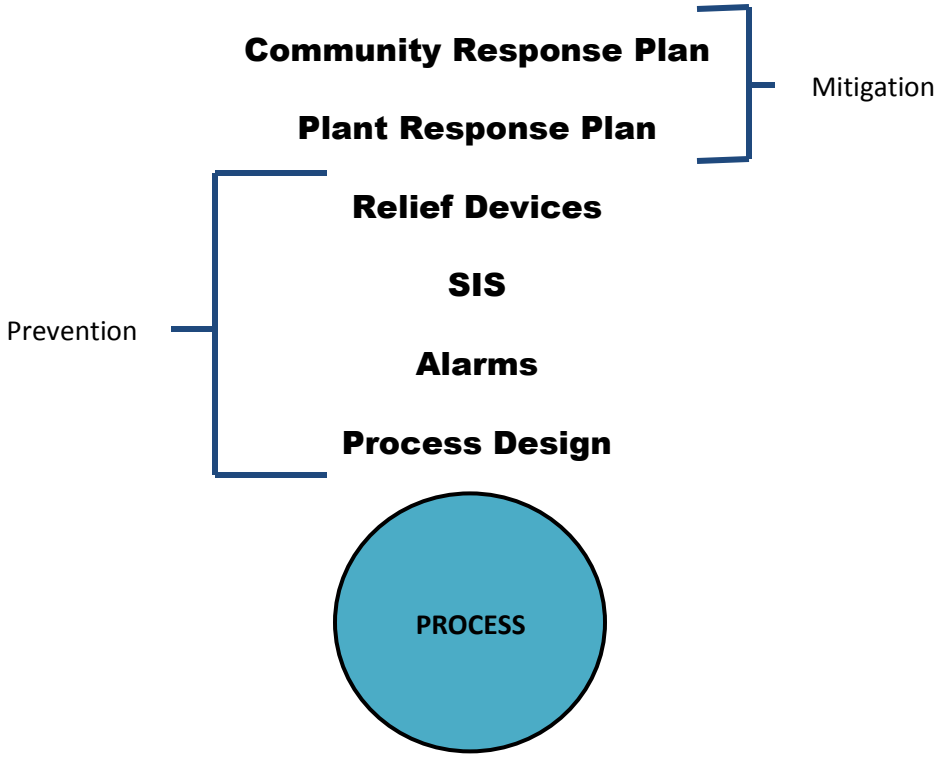
The SIL requirements define what needs to be done to prevent systematic failures from being introduced into the device or system during design. These requirements can be met by establishing a very rigorous development process or by establishing that the device has a sufficient history of operation in order to argue that it has been proven by field use.

Electric and electronic devices can be certified for use in functional safety applications according to IEC 61508, providing application developers the evidence required to demonstrate that the application including the device is also compliant.

IEC 61511 was written and targeted to end users and provides “best practices” recommendations for users to follow when implementing a Safety Instrumented System (SIS). Let’s backup for a few minutes.

Hazards Analysis

The IEC standards prescribe layers of protection be used. They further state that these layers should be independent of each other, meet a certain reliability level, be capable of being checked or audited, and be specific in their design regarding the level of risk they contain. Protection layers are to be designed to either mitigate (reduce the severity) a hazardous occurrence or prevent one. Community and Plant response plans are mitigation layers, while the basic process design, alarm system, automated SIS and relief devices are prevention type layers of protection. All should be utilized.



The specific layers of protection required will emanate from the Hazards Analysis. Such an analysis will include from an engineering study that reviews the process, electrical, mechanical, safety, instrumentation and management aspects of the process for those processes with severe risks. The Hazards Analysis will determine if an SIS is required. The purpose of the SIS, a.k.a. safety shutdown or safety interlock, is always to take the process to what is considered a minimal “safe state”.

A SIS consists of safety instrumented functions of SIF's and there can be multiple SIF's within an SIS. Each SIF can contain sensors, signal processing equipment, logic solvers and actuators. A SIF might be an over-pressure control on a vessel. A pressure sensor detects pressure at a level above its normal set-point. Logic then determines that a vent or relief valve should be open to return the vessel to a safe state and the control value responds to the output from the logic controller and opens and relieves the pressure build-up until the pressure in the vessel is again detected to be within safe set-point levels.

A SIS can have a single or multiple SIF's. An SIL is assigned to indicate the extent to which a process is expected to perform safely. Process measurement and control equipment and a SIS are not assigned a SIL. The equipment are indicated to be "suitable for use" within certain SIL environment.

Safety Integrity Level

The Safety Integrity Level (SIL) is established to indicate the acceptable probability of a failure on demand for the safety system to work. The questions the SIL answer are the extent a process can be expected to perform safely and to fail safely. They are a measure of safety risk for a given process. The SIL indicates what the tolerable failure rate is for the process. The SIL encompasses the entire process rather than just one specific component. This is determined upon completion of a Hazards Analysis. If the analysis determines that safety protection is sufficient, then a SIS is NOT required, otherwise it will be needed.

There are four levels of integrity defined in the standards. Each level represents an order of magnitude of greater risk reduction. The higher the impact a failure can have, the lower the tolerable failure rate will be, and the higher the SIL number will be. For example, SIL 4 has greater risk reduction than SIL 3, which is greater than SIL 2, which is greater than SIL 1.

The effectiveness of an SIS can be described in terms of the probability of it failing to perform its function upon demand to perform. This is called the Probability of Failure on Demand or PFD. The average PFD is used to determine the SIL required. Refer to Table 1 for the relationship between the PFD_{avg}, SIS availability, risk reduction, the SIL and potential consequences.

Table 1: SIL and related parameters

SIL	SIS Availability	PFD avg	Reduction of Risk	Potential Consequence
4	>99.99%	10^{-5} to $<10^{-4}$	100,000 to 10,000	Fatalities in community
3	99.9%	10^{-4} to $<10^{-3}$	10,000 to 1,000	Multiple fatalities
2	99-99.9%	10^{-3} to $<10^{-2}$	1,000 to 100	Major injuries of a single fatality
1	90-99%	10^{-2} to $<10^{-1}$	100 to 10	Minor injuries

Standards

Refer to the following standards for more information:

IEC 61508 (issued in 2000)

IEC 61511 (issued in 2003)

ANSI/ISA 84 (issued in 2004)

Conclusion

The effective operation of a group of processes will impact the quality of the product produced and its availability and profitability. Proper safety hazard analysis and implementation of safety systems using SIS and SIL will help ensure that your plant, processes, your neighbors and perhaps even yourself will be around to benefit from it all.

For critical safe process control of inventory and process vessels, consider instrumentation rated for use in the applicable SIL environment when needed.