

Risk Prevention and Mitigation Where does gas detection fit in?

Dirk Schreier
Functional Safety Consultant
HIMA Australia Pty Ltd
L3, 37 St Georges Terrace
Perth WA 6000
Australia

It is quite common in today's process industry to see the terms fire and gas (F&G). These terms have been used hand in hand for many years and are also combined when referring to applications involving safety-instrumented systems.

This article challenges the thinking behind this concept and demonstrates that although fire systems and gas detection systems both reduce risk, their methods are actually quite different.

It is important to understand what risk means in the context of safety instrumented systems. The AS61508 and AS61511 standards describe risk as essentially a measure of likelihood and consequence. The total risk is the product of these two. This is illustrated in Figure 1.

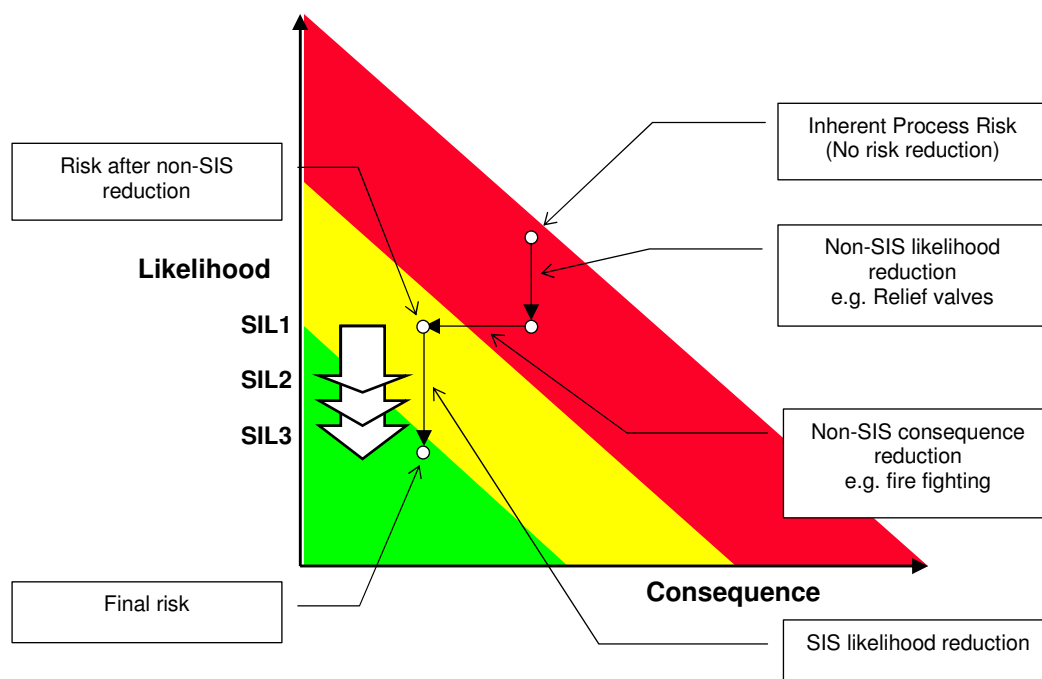


Figure1



Risk can be expressed in several ways depending on the nature of the consequence. In the context of AS61508 and AS61511, the risk considered is associated with physical safety, and thus the consequences are potential fatalities and injuries to employees and the public.

Although these standards are specifically based on safety, their risk assessment methods are often applied to scenarios where the consequences are environmental damage or asset/financial loss.

The first and most effective way to reduce risk is to reduce the likelihood of a hazardous occurrence. With reference to figure 1, safety instrumented systems are generally associated with likelihood reduction. Simplistically, safety integrity levels (SIL) are a measure of the required risk reduction to bring a particular function into the tolerable risk region. Other likelihood reducing methods often employed are process control systems, physical relief devices, operator intervention etc. This is often analyzed by means of a Layer of Protection Analysis (LOPA).

The second way to reduce risk is to reduce the consequence of the hazardous occurrence. With reference to figure 1, consequence-reducing methods may include containment dykes, occupancy reduction, fire systems etc.

Common sense here would say that it is far more desirable to prevent the hazardous event from occurring rather than mitigating its consequence once it has occurred and thus the emphasis is placed on the reduction of likelihood in order to meet the desired SIL target.

Consider a flammable gas leak. Even though this is classified as a loss of containment, a gas detection system is effectively a system that is preventative by nature and reduces risk by decreasing the likelihood of the hazard occurrence. An example of a flammable gas related hazardous occurrence could be a vapour cloud explosion. In case of a toxic gas release, there is no question that the system is performing mitigation.

If we consider the outbreak of a fire, the application of a fire protection system is considered a mitigation method, as the aim is to reduce the consequence by containment of the hazard once it has already occurred.

If we investigate the executive actions of these two functions we can also see distinct differences. Executive actions for the detection of gas are generally similar if not the same as normal emergency shutdown (ESD) functions i.e. the equipment or plant is shutdown to a safe state by 'de-energize to trip' outputs. A loss of power of such a system does not mean a loss of the safety function.

Executive actions for fire systems generally start and activate equipment such as fire pumps, deluge systems, beacons and sirens. These functions are often carried out by 'energize to act', line-monitored I/O cards to enable fault detection such as a wire break.

A loss of power to a fire protective system means loss of the safety function. Fire systems therefore require at least two independent power supplies (NFPA72).

The two risk reduction layers identified are Safety Instrumented Prevention Systems and Safety Instrumented Mitigation Systems. It is common to see safety instrumented systems where the Fire and Gas functions have been combined in logic solvers and I/O cards / racks, only to find that in the logic solver program the gas shutdown functions are always logically grouped with the normal ESD functions. Fire detection functions are generally placed on their own.



This raises the question that “when designing a combined safety system (CSS) that includes ESD and F&G functions, shouldn't we consider logically separating out the fire system functions?”