Session Number: 3

SIL-Rated Fire (& Gas) Safety Functions Fact or Fiction?

Raymond Wright PhD
Senior Consultant, FSE Global Australia Pty Ltd

Abstract

SIL-rated process safety functions are now commonplace, and as an extension of this many users are specifying SIL-rated fire (and gas) safety functions. Perhaps this is without an adequate understanding that there are significant differences in the design and implementation of fire (and gas) safety functions – differences that can make it difficult to achieve even SIL 1 safety performance.

This paper will discuss these differences and their impact on achieving safety performance; then it will explore the impact of recommendations made in ISA TR84.00.07-2010: “Guidance on the Evaluation of Fire, Combustible Gas and Toxic Gas System Effectiveness”; and finally, offer a method to manage fire and gas risk without the need for SIL-rated fire and gas safety functions.

Introduction

IEC 61511 acceptance and adoption varies around the world, but in the UK the Health and Safety Executive (HSE) regards it as close to law. The HSE's IEC 61511 committee member Simon Brown explained: "IEC 61511 is becoming well accepted as the standard of good practice for safety instruments systems in the process sector. It's certainly not a legal requirement in itself, but the requirement to implement good practice is a legal requirement."

The acceptance of IEC 61511 has meant that SIL-rated process safety functions are now commonplace and, as an extension of this, many users are specifying SIL-rated fire (and gas) safety functions.

The aim of the paper is to demonstrate that there are significant differences in the design and implementation of fire (and gas) safety functions; and that these differences can make it difficult to achieve even SIL 1 safety performance.

This paper takes a ‘high-level’ look at the issues related to SIL-rated Fire (and Gas) safety functions. This means that the focus will be on practical concepts and common sense rather than an academic treatment of the subject.

Background

The following concepts are needed to understand Safety Instrumented Functions (SIF), Safety Integrity Level (SIL), and how a SIL rating can be achieved.

Definitions

Where the following definitions have been taken from the IEC 61511 standard, a corresponding reference is provided

Term	Definition
Safety Instrumented System (SIS)	**3.2.72** Instrumented system used to implement one or more safety instrumented functions. An SIS is composed of any combination of sensor (s), logic solver (s), and final elements(s)
Safety Instrumented Function (SIF)	**3.2.71** Safety function with a specified safety integrity level which is necessary to achieve functional safety and which can be either a safety instrumented protection function or a safety instrumented control function
Safety Integrity Level (SIL)	**3.2.74** Discrete level (one out of four) for specifying the safety integrity requirements of the safety instrumented functions to be allocated to the safety instrumented systems. Safety Integrity Level 4 has the highest level of safety integrity; safety integrity level 1 has the lowest

Table 1: Terms and Definitions

SIL Chart

The relationship between a particular SIL and a range of PFDavg values for the demand mode of operation is given in Table 3 of the IEC 61511 standard. The values in the table have been adapted to form the following chart

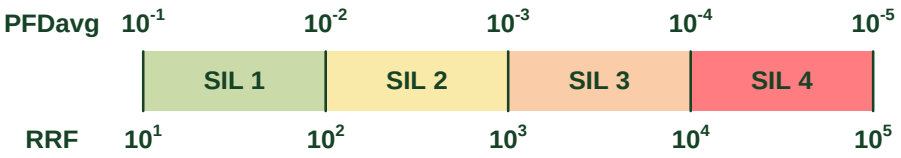


Figure 1: Safety Integrity Level Chart

Where:

PFDavg is the average probability of failure on demand. PFDavg ~ λ_{DU} x TI/2

λ_{DU} is the dangerous undetected failure rate

TI is the proof test interval

RRF Is the Risk Reduction Factor = 1 / PFDavg

Achieving a SIL Rating

In order to evaluate the performance of a Safety Instrumented Function, it is split into three subsystems – Sensor, Logic Solver, and Final Element, as represented in the following diagram.

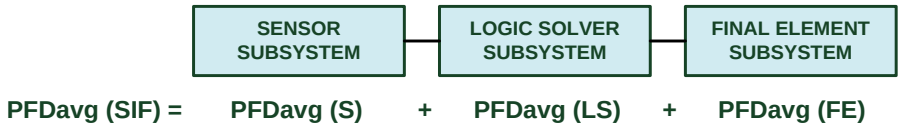


Figure 2: Subsystems of a Safety Instrumented Function

The SIL rating belongs to the SIF, not to each subsystem, and not to individual devices used in the SIF. Devices may be approved for use in applications requiring a particular SIL, but it is incorrect to say that a device is a SIL 2 or SIL 3 device.

For a SIF to achieve a particular SIL, each subsystem needs to satisfy two criteria:

1. PFDavg Requirement

To achieve the required PFDavg each subsystem must achieve at least the level of performance required (PFDavg) within the relevant SIL range, with the PFDavg of the SIF also within the relevant SIL range.

2. Architectural Constraints

Architectural Constraints uses the concepts of Hardware Fault Tolerance (HFT) and Safe Failure Fraction (SFF) to determine if each SIF subsystem has achieved the desired Safety Integrity Level.

Where a Hardware Fault Tolerance of X means the SIF subsystem can survive X dangerous failures; and

Where the Safe Failure Fraction equals the ratio of safe failures (safe plus dangerous detected failures) to total failures (SFF = (λSU+ λSD+ λDD) / λTotal).

Architectural constraint tables can be found in IEC 61508 (Tables 2 and 3), and IEC 61511 (Tables 5 and 6).

While complying with architectural constraints is necessary to achieve a SIL rating and must be considered, it will not be dealt with in this paper. It will be sufficient to explore the PFDavg requirements related to a SIL rating.

Safety Functions as Layers of Protection

Risk Scenario

The risk scenarios identified in a process hazard analysis (PHA) will include a potential incident, its cause and consequence, and the safeguards in place to reduce risk.

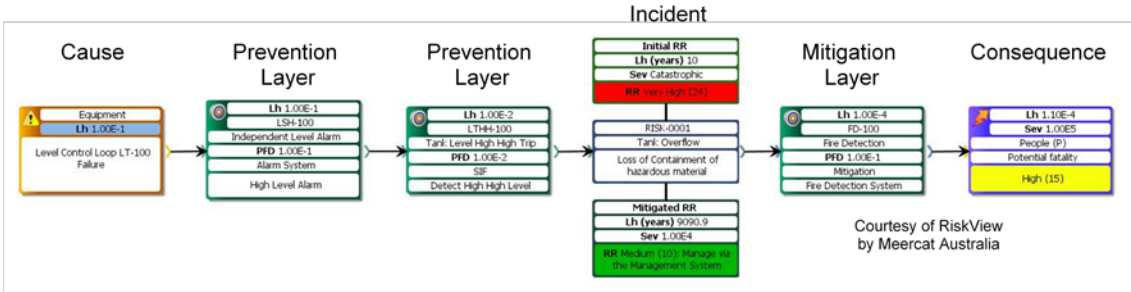


Figure 3: Risk Scenario Bow Tie

If the risk is high compared to the tolerable risk, it is common to put these risk scenarios through further analysis, often in the form of a Layer of Protection Analysis (LOPA), where the existing safeguards are examined to determine their effectiveness in either preventing the incident, or mitigating its consequences.

Layers of Protection

If a safeguard is independent, specific, reliable and auditable it may be considered as an independent layer of protection with an estimated risk reduction factor.

Each risk scenario identified will have a number of layers of protection implemented to reduce the risk of the scenario to a tolerable level. Figure 4 shows the typical layers of protection at a process facility.

Figure 4: Layers of Protection

The layers from process design to physical relief devices are known as prevention layers, and act to reduce the frequency of a potential incident, usually a loss of containment.

The layers from Passive physical protection to community emergency response are known as mitigation layers, and act to mitigate the consequences if the incident occurs.

Safety Functions as Prevention Layers

Process safety functions are generally implemented to prevent a specific hazardous event, usually a loss of containment. The function has sensors and final elements that interface directly with the process in a way that detects a deviation from normal operation and takes action to achieve a safe process state. By design, as long as the sensor is functioning correctly it will always see the process condition it is measuring; and as long as the final element is functioning correctly it will act to prevent the incident from occurring.

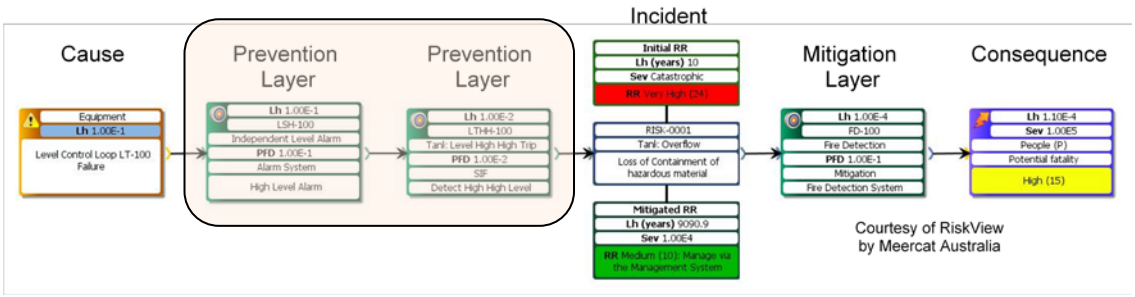


Figure 5: Prevention Layers of Protection

Safety Functions as Mitigation Layers

A fire (or gas) safety function is implemented to mitigate the effect of a loss of containment. These may be small leaks from seals or flanges, or pinholes in pipes; or they may be catastrophic as in pipe or vessel ruptures.

In contrast to a process safety sensor, a fire (or gas) detector generally does not have a direct interface to what it is trying to detect. For example, a flame detector may be functioning properly, but may not detect a flame because of issues such as location or equipment obstruction; or a gas detector may be functioning properly but the gas may not reach the detector because of issues such as location or wind direction.

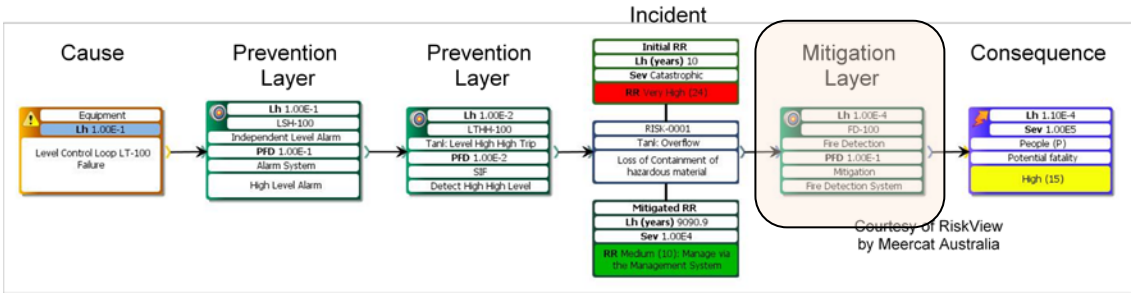


Figure 6: Mitigation Layers of Protection

The other major difference with fire (and gas) functions is the response to detecting fire or gas. The response to detecting a fire may be to initiate a foam release or deluge; or the response to detecting gas may be to isolate potential sources to limit the release; but these actions are by no means certain to completely eliminate the consequence.

In this situation, having the hardware of the fire (and gas) safety functions working correctly at a particular performance level is not enough. It doesn't matter how good the hardware performance is if the fire or the gas leak is not detected, or if the mitigation action is not effective.

So this raises two issues that need to be addressed:

- Detector coverage
- Mitigation effectiveness

This is not a sudden revelation. The problem has been known for years, but has been masked by prescriptive standards that largely address the requirements for building protection. Only after the widespread acceptance of performance based safety standards, especially IEC 61508, did these issues start to get the attention they deserve, and there is a lot of effort on both sides of the Atlantic to provide guides for dealing with these issues.

As an example, the ISA84 committee has formed a separate working group to develop guidance, in the form of a Technical Report on the Evaluation of Fire, Combustible Gas and Toxic Gas System Effectiveness (ISA TR84.00.07-2010). This Technical Report has been published but is still a work in progress as it currently only deals with detector coverage, and not mitigation effectiveness.

ISA-TR84.00.07-2010 Technical Report

[Guidance on the Evaluation of Fire, Combustible Gas and Toxic Gas System Effectiveness]

The report recognises that detector coverage and mitigation effectiveness are key factors in determining the performance of fire (and gas) safety functions, but only addresses detector coverage. Achieving mitigation effectiveness is currently under study.

The report lists three difficulties in applying a performance based approach to fire (and gas) functions, and these can be summarized as follows:

- FGS are generally implemented to reduce the risk from losing containment, such as leaks from equipment seals, flanges, and piping. These hazards may be difficult to define and analyze without using advanced risk analysis techniques, such as gas dispersion modeling or fire modeling associated with a given scenario
- Mitigation rather than prevention - typical hazards and risk analysis assumes that the identified safety function eliminates the consequence; FGS typically reduce the magnitude and severity of the consequence instead of eliminating it.
- Inadequate detector coverage and mitigation effectiveness

The report goes on to say ...

"As a result of these factors, it is difficult to develop a sound technical justification for allocating risk reduction to FGS functions in a simplified risk assessment process, such as layer of protection analysis (LOPA). The identification of FGS functions and allocation of risk reduction to them requires detailed release scenario development and residual risk considerations that are beyond simplified risk assessment tools. Further, FGS performance verification requires evaluation of the detector coverage and mitigation effectiveness, as well as hardware and software design."

At face value, it is difficult to argue with sentiment expressed; but the requirement for detailed release scenario development may be falling into the trap of believing that modeling solves the problems; and that more estimates and assumptions cobbled together in an algorithm provides something useful in determining, even improving, the performance of fire (and gas) safety functions.

It begs the question – does it really solve the problem of achieving a SIL rating for fire (and gas) safety functions?

So our path has to take us to explore detector coverage and mitigation effectiveness, the effect of modeling to improve these, and to see what effect this has on safety performance.

Detector Coverage

It is common to divide the area to be covered by fire a gas functions into zones, identify the most likely places for leaks and fires to occur, and place detectors in such a way to optimize the probability of detection.

In terms of operation, one detector is capable of initiating the appropriate action, and it is common to use 1ooM voting for areas where unwanted automatic mitigation actions are unlikely to cause significant losses.

However, to reduce spurious mitigation actions due to the failure of a single sensor, 1ooM voting is more widely used for alarms, and 2oo2 or 2ooM voting is used for initiating mitigation action where the anticipated loss from a spurious mitigation action is unacceptable.

If a voting scheme is used, then estimates of the detector coverage factor need to be based on more than one detector detecting a fire or gas release.

Voting for Fire

A typical voting scheme for flame detectors is 1ooM for alarm, and 2ooM for mitigation action.

Adopting a particular voting scheme requires careful consideration. Flame detectors can be positioned to overlap within their 'cone of vision' to provide a 2ooM voting. However, if the fire is in a given location, this overlap is location and elevation dependent, which means that coverage of an area by two detectors is generally smaller than the coverage from single detectors.

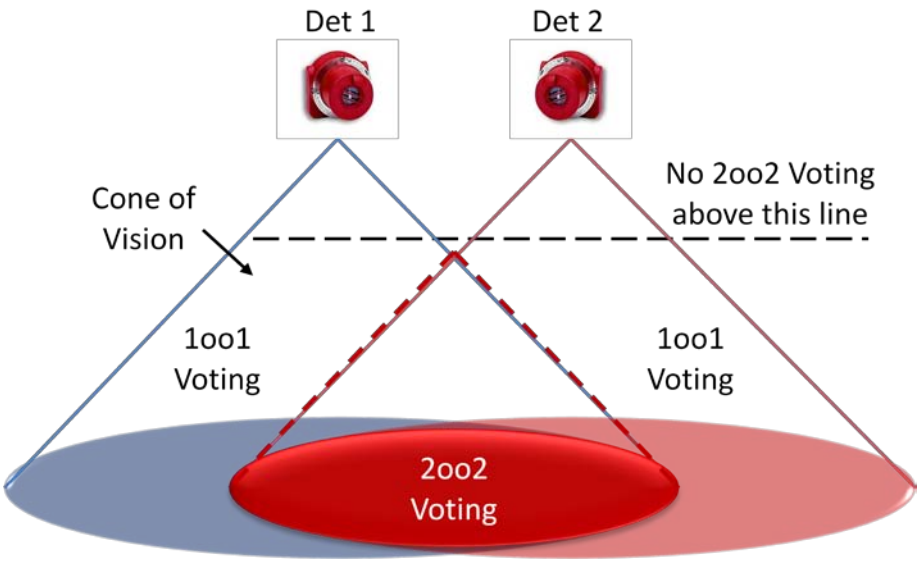


Figure 7: Flame Detector Cone of Vision

In many instances a 2ooM voting mechanism is applied to flame detectors within a zone (where M is the number of detectors in the zone), but this also needs careful consideration. Even with modeling results providing coverage factors for two or more detectors, unless all detectors are covering identical areas, then 2ooM may not be appropriate, and consideration should be given to voting specific pairs or subgroups of detectors that address specific fire risk scenarios.

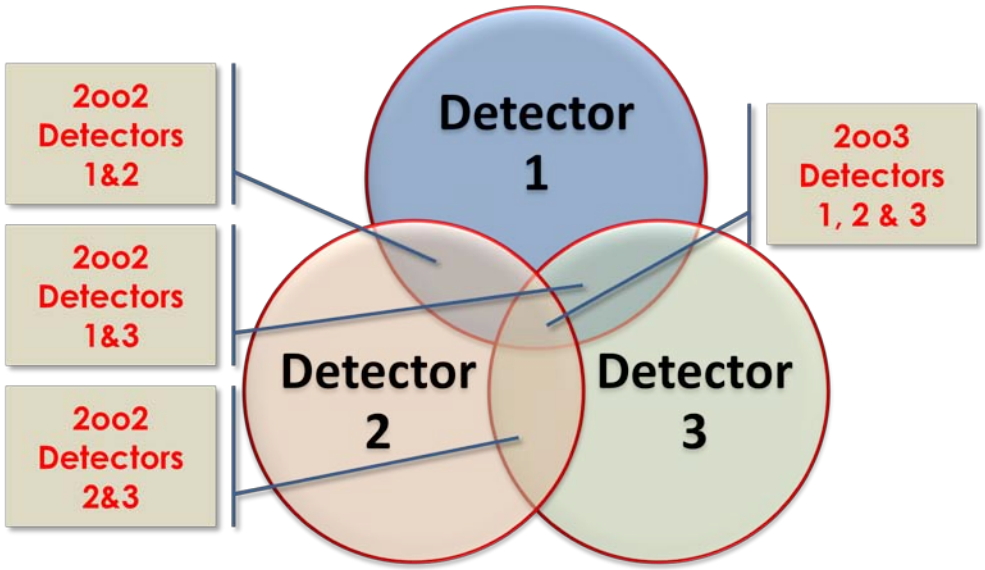


Figure 8: Voting Flame Detectors

Voting for Gas

Point gas detectors are often set to alarm at one LEL value (typically 20% to 25%LEL) and initiate mitigation action at a higher LEL value (typically 50% to 60%LEL). However, if the anticipated loss from a spurious mitigation action is unacceptable, voting between gas detectors is used to reduce the frequency of spurious mitigation actions.

Gas may leak from one location but would need to disperse to be detected by more than one detector. Dispersion relies on such factors as the physical properties of the gas, the volume of gas released, wind speed and wind direction, and physical obstacles. So, depending on the volume of the release, effective 2ooM voting may require both detectors to be in close proximity. Therefore, preventing small releases from becoming large releases may require more detectors at closer proximity.

Open path gas detectors have gained relatively rapid acceptance, primarily because of their promise to cover a much larger area with fewer detectors. It is reported by one vendor that a client decided to replace 438 older point catalytic gas detectors with IR point gas detectors; but after an analysis by the vendor, the point detectors were replaced with just 48 open path detectors in a grid arrangement – lowering capital and ownership costs.

A typical voting scheme for point gas detectors is 1ooM >20%LEL* for alarm, and 2ooM >60%LEL* for mitigation action.

Some organisations are more conservative in their approach, where 1ooM >20%LEL* provides an alarm, and mitigation action is initiated when at least one detector is >60%LEL* and another is >20%LEL*.

A typical voting scheme for open path gas detectors is 1ooM >20%LELm* provides an alarm, and mitigation action is initiated when at least one detector is >60%LELm* and another is >20%LELm*.

(* Note that the 20%LEL/LELm and 60%LEL/LELm values will vary from company to company.)

Once a voting scheme has been decided and adopted, manually optimizing detector positions and numbers to achieve the highest detector coverage factor becomes a rather tedious exercise, and one much better suited to computer simulation modeling.

Modeling

Achieving a very high detector coverage value is not easy. More recently, efforts to define the optimal number and placement of detection devices has resulted in 3-D modeling to provide the coverage factor from single detectors, and the coverage factor from two or more detectors (for voting purposes).

Modeling results show that the coverage factor achieved by single detectors is higher than the coverage factor achieved by two or more detectors, but as discussed previously, voting schemes will provide a lower number of spurious mitigation actions.

So what factors does a detector coverage model need to take into account?

Flame

The factors taken into account by a detector coverage model for fire detection using flame detectors will typically include:

- Location where the fire is most likely to occur
- Physical area – enclosed, partially enclosed, or open
- Expected radiant heat output (RHO) from a fire at the location (fire grade mapping)
- Cone of vision for the particular detector
- Location, orientation, distance and elevation of each detector
- The number and type of detectors used in the model
- The physical environment may include equipment and piping that obstruct vision of flame detectors
- Voting Scheme - one detector for alarm, 2ooM for initiating action.

Gas

The factors taken into account by a detector coverage model for gas detection using point or open path gas detectors will typically include:

- Location where the leak is most likely to occur
- Physical area – enclosed, partially enclosed, or open
- Expected size of release
- Physical properties of the gas
- Pressure behind the release
- Location, orientation, distance and elevation of each detector
- The number and type of detectors
- The physical environment may include equipment and piping that may influence the path of escaping gas
- Average wind speed
- Average wind direction
- Voting Scheme - one detector for alarm, 2ooM for initiating action.

The results of the 3-D modeling is usually provided in the form of a 2-D detector coverage map overlaid on a plot plan of facility, and gives different colours and coverage factors for single detector coverage and 2ooM detector coverage.

Figure 9: Flame Detector Mapping (courtesy Micropack Detection)

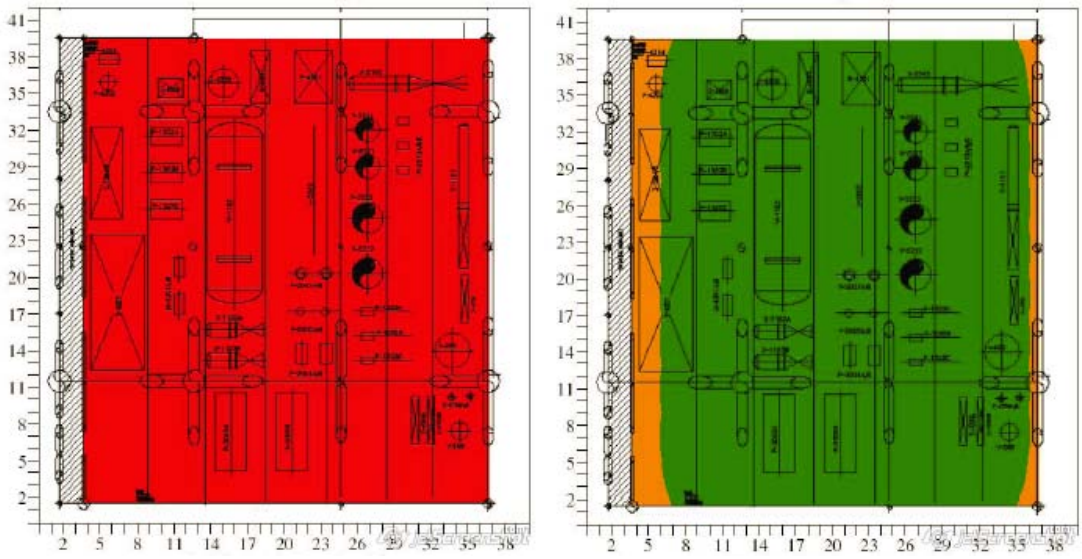


Figure 10: Open Path Gas Detector Mapping (courtesy Micropack Detection)

It must be kept in mind that modeling results are only true for a very specific set of circumstances – it needs all estimates and assumptions made to be true, for the model results to be true.

Models are static, they do not dynamically monitor changes in estimated or assumed parameters and update accordingly; and even if they were dynamic, the installed detection and mitigation system can't move with the changes.

A vision for the future might be of fire (or gas) detectors embedded in "snitches", or dynamically positioned FGS robots moving to the commands of a real-time model.

In the meantime, it would pay to remember that a model is not reality any more than a map is the territory it represents, and the validity of a model should come from knowing what percentage of the time all of the estimates and assumptions used in the model are true at the same time.

So what's the bottom line here? Optimising the number of detectors, and detector placement through modeling techniques can improve the detector coverage factor; but is it really going to help achieve the goal of implementing a SIL-rated fire (or gas) function?

It's time to look at the effect of detector coverage on achieving a SIL rating.

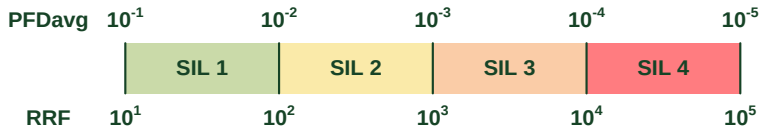
The Effect of Detector Coverage on Performance

The effect of detector coverage on the performance of fire (and gas) functions is significant. Table 8 shows that even if the hardware of a function can meet the performance requirements to achieve a specific SIL, when the detector coverage is factored in, the performance decreases dramatically.

	Detector Coverage	Sensor Subsystem	Logic Solver Subsystem	Final Element Subsystem	Mitigation Effectiveness	PFD	Risk Reduction	Safety Availability
SIL 3	1.00	1.00E-04	1.00E-04	1.00E-04	1.00	3.00E-04	3333.3	99.97%
	0.99	1.00E-04	1.00E-04	1.00E-04	1.00	1.03E-02	97.1	98.97%
	0.95	1.00E-04	1.00E-04	1.00E-04	1.00	5.03E-02	19.9	94.97%
	0.90	1.00E-04	1.00E-04	1.00E-04	1.00	1.00E-01	10,0	89.97%
	0.89	1.00E-04	1.00E-04	1.00E-04	1.00	1.10E-01	9.1	88.97%
SIL 2	1.00	1.00E-03	1.00E-03	1.00E-03	1.00	3.00E-03	333.3	99.70%
	0.99	1.00E-03	1.00E-03	1.00E-03	1.00	1.30E-02	76.9	98.70%
	0.95	1.00E-03	1.00E-03	1.00E-03	1.00	5.30E-02	18.9	94.70%
	0.90	1.00E-03	1.00E-03	1.00E-03	1.00	1.03E-01	9.7	89.70%
	0.89	1.00E-03	1.00E-03	1.00E-03	1.00	1.13E-01	8.8	88.70%
SIL 1	1.00	1.00E-02	1.00E-02	1.00E-02	1.00	3.00E-02	33.3	97.00%
	0.99	1.00E-02	1.00E-02	1.00E-02	1.00	4.00E-02	25.0	96.00%
	0.95	1.00E-02	1.00E-02	1.00E-02	1.00	8.00E-02	12.5	92.00%
	0.90	1.00E-02	1.00E-02	1.00E-02	1.00	1.30E-01	7.7	87.00%
	0.89	1.00E-02	1.00E-02	1.00E-02	1.00	1.40E-01	7.1	86.00%

Table 2: Effect of Imperfect Detection

If we look at this table we can see the effect of imperfect detection on the performance of the function.



The table above only considers changes in detector coverage, and assumes that mitigation is perfect. The results show that even if the hardware of a fire or gas function is designed to perform at the top end of PFDavg range for SIL 3 (1.00E-04), anything less than 100% detector coverage reduces the performance to SIL 1; and a detector coverage factor of less than 90% reduces the performance to below SIL 1.

The Health and Safety Executive (UK) issued a report in February 2003 of an analysis of 9+ years of data relating to offshore hydrocarbon releases (HSR 2002 002). "There were 2471 detection modes connected with the total 2312 reported releases, more than one mode being effective on some releases. Gas detectors detected 41.6% of all releases (75.9% of gas releases), and the remaining releases were mainly detected by means other than equipment designed for the purpose" – sound, sight and smell.

The Effect of Mitigation Effectiveness on Performance

We have seen that detecting a fire or a gas release is not necessarily straightforward, and even a very high detector coverage does not necessarily help to achieve a SIL rating for the fire (or gas) function, even when mitigation effectiveness was considered to be perfect.

So let's assume that the fire (or gas) is detected and explore the effect of imperfect mitigation. The probability that activation of the final element subsystem of our SIF will completely mitigate the consequence is called mitigation effectiveness, and is given as a percentage.

The mitigation effectiveness depends on multiple factors including:

- The characteristics of the physical area – enclosed, partially enclosed, or open.
- The fire suppression system must be designed to control the specific fire hazard completely.
- The isolation of gas leaks must fast enough and tight enough to stop the fuel / air supply.
- The mitigation systems must survive the effects of an incident.

Estimating mitigation effectiveness is a challenge, as is evidenced by the number of major incidents where the systems implemented for mitigation have failed to eliminate the consequence because the severity of the consequence was higher than assumed in mitigation system design.

Estimating the mitigation effectiveness for a specific application such as fire detection in an enclosed space, or gas detection in a duct, is generally easier because the dynamics of a contained environment are better understood; but mitigation in open areas is far more difficult.

While there are industry and standards groups working on ways to better estimate mitigation effectiveness, at this point the best estimation of mitigation effectiveness is likely to come from specific historical plant data, or local expert opinion.

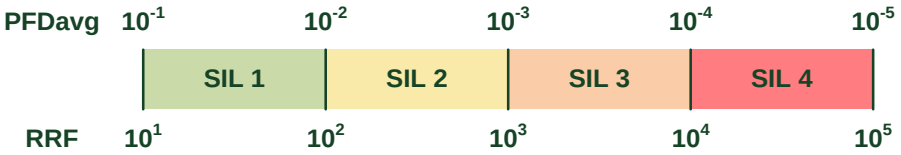
As with detector coverage, achieving higher mitigation effectiveness does not necessarily guarantee a SIF will achieve a SIL rating.

So what effect does imperfect mitigation have on the performance of fire (and gas) safety functions?

	Detector Coverage	Sensor Subsystem	Logic Solver Subsystem	Final Element Subsystem	Mitigation Effectiveness	PFD	Risk Reduction	Safety Availability
SIL 2	99%	1.00E-03	1.00E-03	1.00E-03	100%	1.30E-02	76.9	98.70%
	99%	1.00E-03	1.00E-03	1.00E-03	99%	2.30E-02	43.5	97.70%
	99%	1.00E-03	1.00E-03	1.00E-03	95%	6.30E-02	15.9	93.70%
	99%	1.00E-03	1.00E-03	1.00E-03	90%	1.13E-01	8.8	88.70%
SIL 2	95%	1.00E-03	1.00E-03	1.00E-03	100%	5.30E-02	18.9	94.70%
	95%	1.00E-03	1.00E-03	1.00E-03	99%	6.30E-02	15.9	93.70%
	95%	1.00E-03	1.00E-03	1.00E-03	95%	1.03E-01	9.7	89.70%
	95%	1.00E-03	1.00E-03	1.00E-03	90%	1.53E-01	6.5	84.70%
SIL 2	90%	1.00E-03	1.00E-03	1.00E-03	100%	1.03E-01	9.7	89.70%
	90%	1.00E-03	1.00E-03	1.00E-03	99%	1.13E-01	8.8	88.70%
	90%	1.00E-03	1.00E-03	1.00E-03	95%	1.53E-01	6.5	84.70%
	90%	1.00E-03	1.00E-03	1.00E-03	90%	2.03E-01	4.9	79.70%
	90%	1.00E-03	1.00E-03	1.00E-03	89%	2.13E-01	4.7	78.70%

Table 3: Effect of Mitigation Effectiveness

If we look at this table we can see the effect of imperfect mitigation on the performance of the function.



The table above looks at an example of a SIL 2 requirement where each group of numbers represents system hardware with PFDavg values at the high end of SIL 2, and a fixed detector coverage factor. The only variable in each group is the mitigation effectiveness.

The first group of figures assumes a detector coverage factor of 99% and, as the mitigation effectiveness drops below 90%, the performance of the function drops below SIL 1.

The second group of figures assumes a detector coverage factor of 95% and as the mitigation effectiveness drops below 95% the performance of the function drops below SIL 1.

The third group of figures assumes a detector coverage factor of 90% and even if the mitigation effectiveness is 100% the performance of the function drops below SIL 1.

Performance Verification

This paper has so far discussed the factors that need to be considered if a SIL rating for a fire (or gas) function is going to be achieved; and we have seen that the two dominant factors are detector coverage and mitigation effectiveness. But in terms of achieving a SIL rating this paper has only looked at performance in terms of PFDavg, and, as pointed out in an earlier section has not explored the effect of the requirement to address the architectural constraints of the functions in terms of Hardware Fault Tolerance (HFT) and Safe Failure Fraction (SSF). This will bring another set of challenges to the design of SIL-rated fire (or gas) functions on both the sensor and final element design, especially if the requirement is for a SIL 2 function.

Even if we assume that we are able to achieve a SIL rating for a fire (or gas) safety function, we have to look beyond the design phase and into the testing and verification of the function. How is the detector coverage factor verified? How is the mitigation effectiveness going to be verified? There is currently no guidance on an adequate means of providing this verification. You can't rely on modeling, because the tests of effectiveness for both detection and mitigation are to test the modeling results used to design the function.

Other issues arise when dealing with detection only functions. These functions require operator intervention to decide a course of action and initiate an appropriate mitigation action, and thereby substitute the reliability of the operator intervention for the logic solver. In essence, these look like an alarm and operator response, but carry the additional burden of less than perfect detector coverage, and less than perfect mitigation effectiveness when evaluating and verifying performance.

It is clear that achieving exceptionally high levels of detector coverage and mitigation effectiveness is necessary for a fire (or gas) function to achieve even a SIL 1 rating. It is equally clear that achieving, verifying and maintaining the required high values is practical only in very specific circumstances. Essentially, this means that aiming for SIL rated fire (or gas) functions may not be a practical goal at this point in time.

It does not mean that optimizing detector coverage or mitigation effectiveness is wasted effort, but it does mean that perhaps we need to look at our risk scenarios differently if we are to achieve a tolerable level of risk without relying on a specific performance level from fire (or gas) safety functions.

What can be done if further risk reduction is required to achieve our tolerable risk, but we are not able to guarantee the performance level of fire (or gas) safety functions?

First we need to look at where we are defining our tolerable risk.

Achieving a Tolerable Risk Level

Each risk scenario has an associated level of risk, and this is compared to the tolerable risk level set by an organisation. Tolerable risk can be expressed in different ways, but it is common to express it as a Target Risk Frequency for a given incident (e.g. loss of containment); or as a Target Risk Frequency for a given consequence severity (e.g. fatality, fire, explosion, toxic cloud) - the higher the severity, the lower the Target Risk Frequency.

Defining Tolerable Risk		
Incident	**Physical Effects of the Incident**	**Consequences of the Physical Effects**
A spill, vapour cloud, explosion, toxic cloud, etc.	Radiant heat output, blast overpressure, toxic concentration, etc.	Injury/fatality, environmental impact, financial loss, etc.

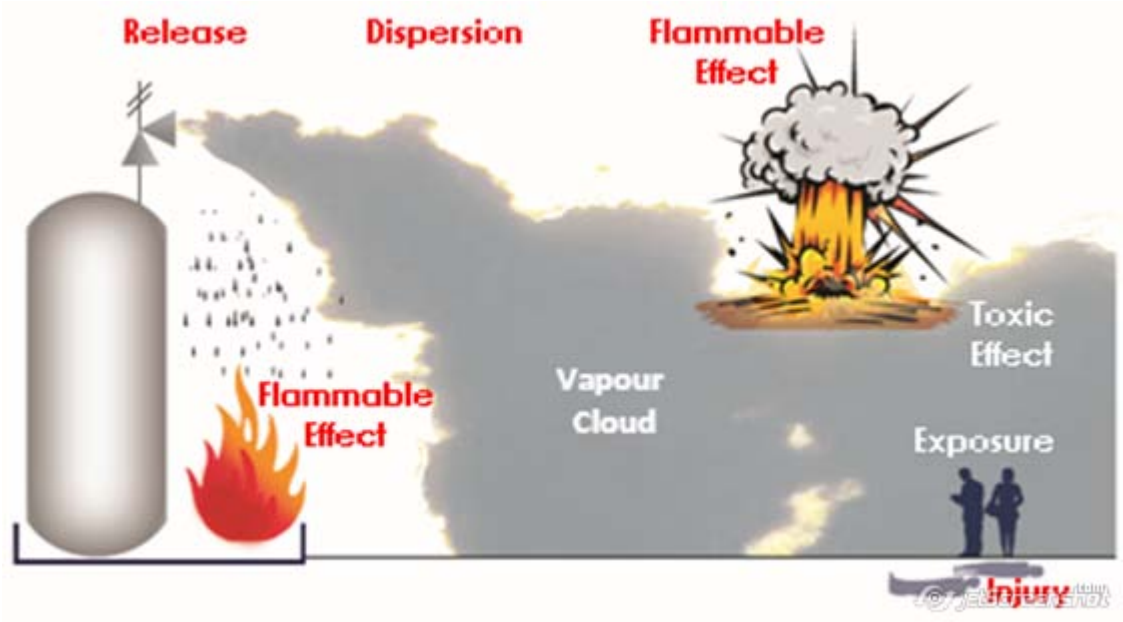


Figure 11: Consequence of Interest

Some organisations specify their tolerable risk as a target risk frequency for the severity of a particular incident, generally a loss of containment (a spill, a flammable vapour cloud, a toxic cloud, etc.); for example, a target risk frequency of 1.00E-06 years for a loss of containment of a defined volume of material. Implicit in this method is the assumption that a release of a certain size is likely to have consequences in terms of safety, environmental impact, and asset loss.

A few organisations specify their tolerable risk as a target risk frequency based on the physical effects of the incident (radiant heat output, blast overpressure, toxic concentration, etc.); for example, a target risk frequency of 1.00E-06 years for a single fatality. Implicit in this method is that the physical effects of a release are likely to have consequences in terms of safety, environmental impact, and asset loss.

Other organisations specify their tolerable risk as a target risk frequency for the severity of a specific consequence (fatality, specific environmental impact, specific financial loss, etc.); for example, a target risk frequency of 1.00E-06 years for a single fatality.

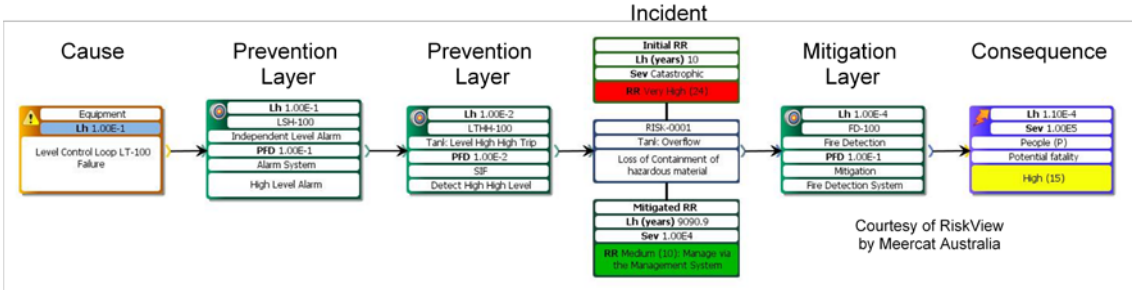


Figure 12: Risk Scenario Bow Tie

If an organisation defines its tolerable risk frequency in terms of consequence then prevention and mitigation layers of protection are available to reduce risk to the tolerable level. In certain risk scenarios a fire (or gas) safety function may be assigned a required risk reduction factor, and this can give rise to a requirement for a SIL-rated fire (or gas) function.

However, if an organisation defines its tolerable risk frequency in terms of the incident (e.g. loss of containment), then only prevention layers of protection are available to reduce risk to the tolerable level. Mitigation layers of protection, though still valuable, are not required to achieve the tolerable risk, and the need to specify SIL-rated mitigation layers such as fire (or gas) functions is eliminated.

Organisations currently defining tolerable risk in terms of a target risk frequency for a given consequence can move that target risk frequency from the consequence to the incident and use prevention layers to achieve it.

Mitigation layers will always have value, and this discussion should not be construed as suggesting that mitigation layers are not required. However, prevention (keeping the hazardous material in the pipe) is always better than mitigation (controlling the situation when the hazardous material has leaked out of the pipe). As a bonus, prevention layers of protection are generally easier to implement and validate.

Conclusions

Fire (and Gas) safety functions are different to process safety functions because the safety performance of fire (and gas) functions does not rely on the hardware alone. The fire (or gas leak) is detected indirectly, and the result of the action taken by the fire or gas function is to reduce rather than eliminate the consequence. Both detector coverage and mitigation effectiveness are dominant factors in achieving safety performance.

Modeling detector coverage can provide higher detector coverage values, but there is a need to consider all of the assumptions made in obtaining the results – if any of these assumptions is not true, the results are no longer valid. So, despite efforts to improve the detector coverage factors, anything less than perfect detector coverage results in dramatically reduced safety performance, making it difficult to achieve even the lowest SIL.

Very little has been done to study or improve mitigation effectiveness as a factor in improving the safety performance of fire (and gas) functions. Mitigation systems are still being built to prescriptive standards that do not require an estimation of effectiveness. This is changing, but a useful guide is not yet on the horizon.

Verifying the performance of fire (or gas) safety functions needs to be thought through very carefully.

This does not mean that mitigation protection layers have no value, they certainly do; but what it does mean is that trying to force the concept of a SIL performance rating onto fire (or gas) safety functions is not meaningful at this point in time. However, SIL-approved fire (and gas) hardware may still be of value in terms of improving hardware reliability.

In situations where further risk reduction is required to achieve a tolerable risk level, and this is pushing the need for the performance requirements of a fire (or gas) safety function towards a SIL rating; instead of specifying a SIL-rated fire (or gas) function, move the target risk to the incident (loss of containment) and concentrate on improving or adding prevention layers.

Acknowledgements

Much of the content in this paper is a distillation of current discussions found in industry forums and standards committees – discussions trying to find a common sense approach to risk management, and stemming the misplaced enthusiasm for SIL-rated fire (and gas) safety functions until better guidance is available. Special thanks to Meercat Australia for the use of RiskView to model a risk scenario, and to Micropack Detection for the use of the images of the results of detector coverage modeling.

Useful References

Reference		Description
1	**IEC 61508**	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems
2	**IEC 61511** **ISA 84.00.01-2004**	Functional safety—Safety instrumented systems for the process industry sector
3	**ISA TR84.00.07-2010**	Guidance on the Evaluation of Fire, Combustible Gas and Toxic Gas System Effectiveness
4	**NFPA 72**	National Fire Alarm Code, National Fire Protection Association, 2007.
5	**EN 54: 1997**	Fire Detection and Fire Alarm Systems.
6	**BS 5839 part 1**	Fire Detection and Fire Alarm Systems for Buildings
7	**BS EN 50402:2005** **+ A1:2008**	Electrical apparatus for the detection and measurement of combustible or toxic gases or vapours or of oxygen. Requirements on the functional safety of fixed gas detection systems
8	**IEC 60079-29-2**	Gas detectors - Selection, installation, use and maintenance of detectors for flammable gases and oxygen
9	**IEC 60079-29-3**	Gas detectors - Guidance on functional safety of fixed gas detection systems
10	**HSE Report**	HSR 2002 02 Feb 2003: Offshore Hydrocarbon Releases Statistics and Analysis

Table 4: References

Definitions

Where the following definitions have been taken from the IEC 61511 standard, a corresponding reference is provided

Term	Definition
Safety Instrumented System (SIS)	**3.2.72** Instrumented system used to implement one or more safety instrumented functions. An SIS is composed of any combination of sensor (s), logic solver (s), and final elements(s)
Safety Instrumented Function (SIF)	**3.2.71** Safety function with a specified safety integrity level which is necessary to achieve functional safety and which can be either a safety instrumented protection function or a safety instrumented control function
Safety Integrity Level (SIL)	**3.2.74** Discrete level (one out of four) for specifying the safety integrity requirements of the safety instrumented functions to be allocated to the safety instrumented systems. Safety Integrity Level 4 has the highest level of safety integrity; safety integrity level 1 has the lowest
Hardware Fault Tolerance (HFT)	**11.4.1 Note 1** Hardware fault tolerance is the ability of a component or subsystem to continue to be able to undertake the required safety instrumented function in the presence of one or more dangerous faults in hardware. A hardware fault tolerance of 1 means that there are, for example, two devices and the architecture is such that the dangerous failure of one of the two components or subsystems does not prevent the safety action from occurring. In other words - a Hardware Fault Tolerance of X means the SIF subsystem can survive X dangerous failures.
Safe Failure Fraction (SFF)	**3.2.65.1** Fraction of the overall random hardware failure rate of a device that results in either a safe failure or a detected dangerous failure. In other words - the Safe Failure Fraction equals the ratio of safe failures (safe plus dangerous detected failures) to total failures (SFF = $(\lambda_{SU} + \lambda_{SD} + \lambda_{DD}) / \lambda_{Total}$)
FGS Effectiveness	**TR84.00.07-2010 §4** The ability of the FGS to perform its intended safety actions in a demand condition. It is dependent on a number of factors associated with design, installation, site-specific operating conditions, and maintenance. FGS effectiveness is the product of detector coverage, FGS safety availability, and mitigation effectiveness.
Detector Geographic Coverage	**TR84.00.07-2010 §4** The fraction of the geometric area (at a given elevation of analysis) of a defined monitored process area that, if a release were to occur in a given geographic location, would be detected by the release detection equipment considering the defined voting arrangement.

Term	Definition
Detector (Scenario) Coverage	**TR84.00.07-2010 §4** The fraction of the release scenarios that would occur as a result of the loss of containment from items of equipment of a defined and monitored process area that can be detected by release detection equipment considering the frequency and magnitude of the release scenarios and the defined voting arrangement.
FGS Safety Availability	**TR84.00.07-2010 §4** The availability of the fire and gas function designed to automatically mitigate the consequences of hazards. FGS Availability is equal to one minus the probability of failure on demand (PFDavg) for the FGS function.
Mitigation Effectiveness	**TR84.00.07-2010 §4** The probability that the results of activating the final element(s) will mitigate the consequence of a defined hazard as expected (e.g., prevents a small fire or gas accumulation from escalating to a large fire or accumulation). The FGS must be activated in a sufficiently timely fashion to reduce the event severity. An FGS function may be ineffective such that the outcome of the event is not significantly different than if no detection/activation occurred.
1ooN Voting Arrangement	**TR84.00.07-2010 §4** Implementation of 1ooN (where N > 1) voting in an FGS is such that upon activation of any single detector in a monitored area with multiple detectors, the logic solver commands specified safety action(s) to occur.
MooN Voting Arrangement	**TR84.00.07-2010 §4** Implementation of MooN (where N > 1) voting in an FGS is such that only upon activation of any M or more detectors in a monitored area, the logic solver commands specified safety action(s) to occur.

Table 5: Terms and Definitions