SIL ratings and certification for fire & gas system hardware; Is industry barking up the wrong tree?

Paul Gruhn, P.E., CFSE
Global Functional Safety Consultant
aeSolutions, Houston, TX

KEYWORDS

FGS, F&G, Fire and gas systems, SIL, Safety integrity level, ISA 61511, certification

ABSTRACT

There are many devices (sensors, logic solvers and final elements) used in safety instrumented systems that are independently certified for use in safety applications to different safety integrity levels (SIL). There is considerable debate however whether fire and gas system hardware should have SIL ratings at all. Vendors are naturally interested in promoting independently certified hardware in order to differentiate their products. Considering the differences between safety instrumented systems and fire and gas systems, focusing on the SIL rating or performance of the actual fire and gas hardware alone is considered by some to be a misleading and questionable practice. This paper reviews a) the differences between safety instrumented systems and fire and gas systems, b) how typical voting of fire and gas sensors not only reduces nuisance trips (which is desirable) but also reduces the likelihood of the system actually responding to a true demand (which is not desirable), and c) why concepts and standards that apply to safety instrumented systems (e.g., SIL ratings) may not be appropriate for fire and gas systems.

SO WHY THE FUSS?

Current fire detection and alarm standards such as EN 54 [1] and NFPA 72 [2] are prescriptive and focus on commercial applications (e.g., hotels). Current gas system standards such as ISA 12.13.01 [3] and 92.0.01 [4] are titled as 'performance' based, but the term is used differently than in IEC standards such as 61508 [5] and 61511 [6]. Performance in the case of ISA gas system standards refers to drop tests, vibration, accuracy, repeatability, response to temperature and humidity, etc. The ISA gas system standards are focused for industrial applications (e.g., refineries).

End users on the ISA 84 committee (covering safety instrumented systems in the process industry) felt there was a need to address fire and gas systems from a performance (SIL) rather than a prescriptive point of view that was focused on industrial applications. The committee formed a working group around 2005 to address the issue.

DIFFERENCES BETWEEN PREVENTION AND MITIGATION LAYERS

The "onion diagram" of Figure 1 is an example of various safety layers in a process facility. The layers are intended to reduce the overall level of risk. Risk is the combination of the frequency and severity of an event. If the process control system were perfect, meaning it never failed and could prevent any and all hazardous events, there would be no need for any other layers. Unfortunately, control systems are not perfect. The layers are not solid (i.e., not 100% effective in preventing hazardous scenarios from propagating further). The layers are more like Swiss cheese with holes that appear and disappear, grow and shrink, and move. Hence the need for defense-in-depth, or multiple diverse safety layers.

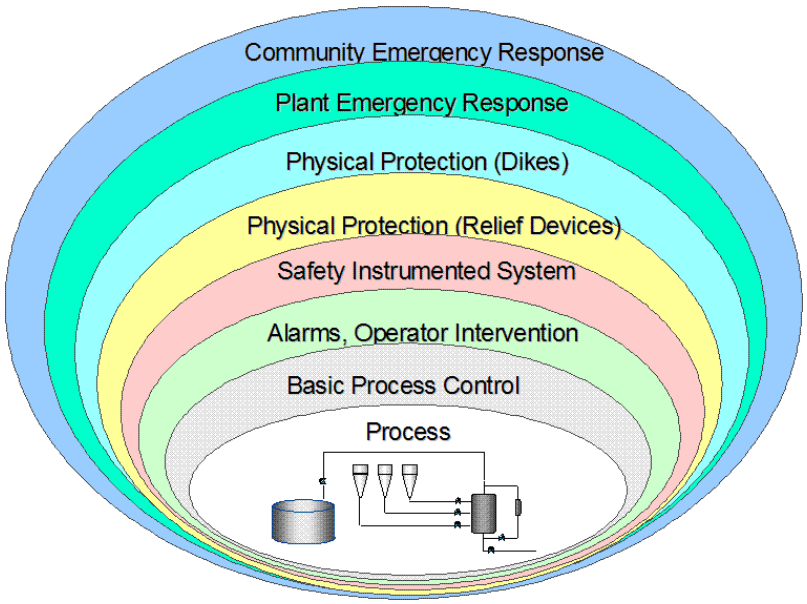

Figure 1: The Onion Diagram

The inner layers are referred to as prevention layers. They are intended to lower the *probability* of an event. The goal is to keep the material in the pipe. Safety integrity levels have historically been assigned to the safety instrumented system layer, often with other prevention layers also being allotted a certain amount of performance.

The outer layers are referred to as mitigation layers. They are intended to lower the *consequences* of an event that has already happened. The material is now outside the pipe and downtime, environmental and other potential safety losses may result. Safety integrity levels have historically *not* been assigned to mitigation layers (as the overall goal is to keep the material in the pipe and prevent any losses), but nothing precludes the practice.

Table 1 shows the performance requirements for the different safety integrity levels according to IEC/ISA 61511.

DEMAND MODE OF OPERATION		
Safety integrity level (SIL)	**Target average probability of failure on demand**	**Target risk reduction**
4	$\geq 10^{-5}$ to $< 10^{-4}$	>10,000 to ≤100,000
3	$\geq 10^{-4}$ to $< 10^{-3}$	>1000 to ≤10,000
2	$\geq 10^{-3}$ to $< 10^{-2}$	>100 to ≤1000
1	$\geq 10^{-2}$ to $< 10^{-1}$	>10 to ≤100

Table 1: Performance Requirements for Safety Integrity Levels

The assumption with prevention layers is that a) they will always be able to see the hazardous condition, and that b) if they respond correctly their action will prevent the hazardous event from occurring. In other words, using a SIL 2 rated sensor, a SIL 2 rated logic solver, and a SIL 2 rated final element should result in a SIL 2 rated function that should provide at least a Risk Reduction Factor of at least 100 (see Table 1) assuming all the other requirements in the standard are met. If a properly functioning sensor is unable to see the hazardous condition it was designed to detect, and if a properly functioning final element doesn't eliminate the hazard, then the system simply wasn't designed properly to begin with.

However, fire and gas systems, which are mitigation layers, are different. Sensors may be working properly, but they simply may never see the gas release or fire. For example, sensors may be placed improperly, there may not be enough sensors, wind may dilute the gas before it can be detected, obstructions may divert the release or hide a fire, a release or fire may be too small to be detected, etc. The system may respond properly, but there is no guarantee that the consequences of the hazardous event will be eliminated or mitigated. For example, the deluge may not put out a large fire, the blow down may not be fast enough to prevent reaching a critical accumulation of gas, etc. In other words, using a SIL 2 rated sensor, a SIL 2 rated logic solver, and a SIL 2 rated final element may *not* result in a SIL 2 rated fire & gas function that may *not* provide a Risk Reduction Factor of at least 100. This concept can be better understood with the event tree shown in Figure 2.

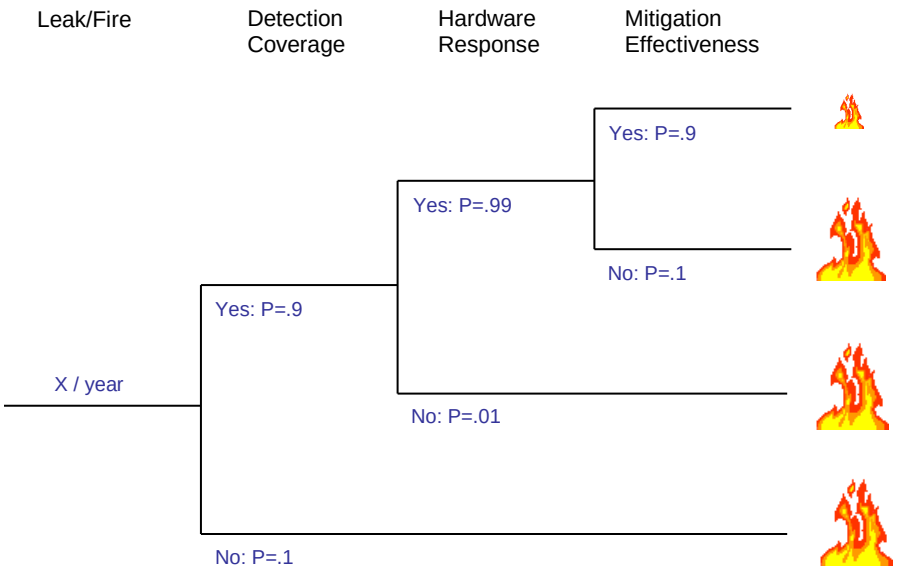

Figure 2: Factors Effecting Fire and Gas System Performance

Detector Coverage: The probability of the device seeing the hazardous condition

Hardware Response: The probability of the hardware responding properly to the demand. 1-PFD (Probability of Failure on Demand)

Mitigation effectiveness: The probability that the overall system response prevents or mitigates the hazardous event

Detection coverage is typically less than 90% (as described below). Mitigation effectiveness is also considered by many to be less than 90%. 90% x 90% = 81%. One minus the Safety Availability is the Probability of Failure on Demand (PFD). 100% - 81% = 19%. The reciprocal of PFD is the Risk Reduction Factor (RRF). 1/.19 = 5. This is below SIL 1 performance (a Risk Reduction Factor between 10 and 100, as shown in Table 1). Therefore, debating on the level of performance of the fire & gas system hardware alone may prove to be of little worth. In this example – which is realistic – the *overall* system will *never* meet SIL 1 performance no matter *what* hardware is used. Focusing on the hardware alone, as some may naturally wish to do, is no guarantee of an effective fire & gas system.

DETECTOR COVERAGE

Fire and gas applications can activate based on only one sensor going into alarm. However, most systems implement some form of voting of multiple sensors in a zone to reduce the likelihood of system activation due to a single faulty sensor or false indication. Two or more sensors in a zone are typically required to go into alarm before automatic action is taken. While this reduces the

probability of nuisance trips due to a single sensor failure, evidence shows it also *reduces* the probability of responding to a hazardous event. It is *less* likely for two or more detectors in a zone to be in the affected area, assuming the layout of detectors has not been changed with the implementation of voting.

Confidential end user studies have been undertaken to estimate detector coverage. In one example, an end user asked an expert consultant for his recommendation on the number and placement of fire detectors on an offshore platform. The consultant recommended nine sensors. This information was input into a detailed three-dimensional computer model of the platform capable of estimating detector coverage. At floor level, the detector coverage for a single sensor (1 out of N) was 82%, dual sensor (2 out of N) was 68%, and three or more sensors (>2 out of N) was 49%. Numbers at three meters above floor level were considerably lower for multiple sensor configurations. The computer program suggested using only five detectors rather than nine. Numbers for detector coverage based on the computer selected locations at floor level were 98% for a single sensor (1 out of N), 90% for dual sensor (2 out of N), and 62% for three or more sensors (>2 out of N). One should always keep in mind that computer models are not reality; they are estimates of reality based on assumptions that may not always be correct.

An often referred to HSE (United Kingdom Health & Safety Executive) report [7] sites automated gas detection coverage in the range of 76%.

One way to possibly improve on this situation would be to not require multiple sensors to see the *same* level of gas (e.g., 50% LEL (Lower Explosive Limit)), but rather take action if one sensor were to see the high level (e.g., 50% LEL) and any other sensor were to see a *lower* level (e.g., 25% LEL). Use of multiple sensing methods (e.g., point detectors, line of sight detectors, ultrasonic detectors) will most likely result in higher detector coverage factors.

ESTIMATING DETECTION COVERAGE AND MITIGATION EFFECTIVENESS

Just as there are different methods of analyzing safety instrumented system performance (e.g., Reliability Block Diagrams, Fault Trees, Markov Models) there are different methods of estimating detection coverage. There are many variables to consider, such as the size of the area to be monitored; is the space enclosed, partially enclosed, or non-enclosed; number of detectors; density of gas; wind speed; number of leak sources in the space, etc. Simple and complex models currently used by members within the fire and gas task team show that detector coverage can vary greatly. Detection coverage is very high for single sensors and a catastrophic release. Detection coverage is very low for multiple sensors detecting medium or small releases. Estimating mitigation effectiveness may best be done by reviewing historical company records and/or expert opinion (e.g., the PHA team). There are several software packages that can perform such modeling and recommend detector number and location.

As with detector coverage, mitigation effectiveness will also vary depending upon many different factors. The ISA technical report [8] covers both in more detail.

CERTIFICATION OF DEVICES IS NOT A SILVER BULLET

Certification of devices used in safety instrumented system applications has been occurring for more than 20 years. Logic solvers were the first devices to get certified, and field devices followed many years later. Certification of devices is an excellent way for a user to have assurance that a product is well designed and satisfies the intent of the safety standards. However, certification of devices is no guarantee a device will actually *work* in an application. The right device and technology must still be selected based on the unique application requirements. When it comes to fire and gas systems, if the detector is unable to actually see the release due to inadequate location, it doesn't matter what level it may be certified to, it still will not work. As covered earlier in this paper, and as covered in the ISA fire and gas technical report, the primary factors affecting fire and gas system performance are detector coverage and mitigation effectiveness.

IMPLICATIONS OF SIL RATINGS FOR FIRE AND GAS APPLICATIONS

Some have set SIL targets for fire and gas layers in an attempt to lower the SIL target for the preventative SIF. Think about the implication of doing this; it's akin to saying, "It's OK to have fires, we'll simply put them out." Designers can readily determine where to detect abnormal pressure, temperature, level and flow, but it is not possible to determine exactly where gas leaks will come from, as most occur due to corrosion and inadvertent operation of valves. Gas detection monitors an *area* and getting multiple detectors to detect the same release is *not* an easy matter.

CONCLUSIONS

Concepts that apply to prevention safety layers such as safety instrumented systems do not necessarily apply to mitigation safety layers such as fire and gas systems. Unlike safety instrumented system hardware, claiming any integrity level for fire and gas hardware alone may be misleading. That information alone does not allow one to determine whether the overall system will meet the desired level of risk reduction.

A chain is only as strong as its weakest link. Focusing on the performance of the fire and gas hardware alone and not accounting for the detector coverage and mitigation effectiveness is just as misleading as focusing only on the logic solver in a safety instrumented system. The impact of field devices (sensors and final elements) typically has a dominating impact on safety instrumented system performance. Similarly, detector coverage and mitigation effectiveness have a dominating impact on fire and gas system performance and may prevent most systems from ever meeting SIL 1 performance levels.

However, it *is* possible to apply performance-based concepts to fire and gas systems. It *is* possible to assign risk reduction targets for fire and gas systems and apply quantitative techniques in system verification. An ISA 84 committee working group spent more than five years working on a technical report [8] covering ways to account for detector coverage,

mitigation effectiveness and other factors, thus allowing a quantitative, performance-based approach to fire and gas system design. This report was first released in 2010, and a second edition in 2018.

REFERENCES

1. EN 54: Fire detection and fire alarm systems. (This is a family of more than two dozen standards, with the most recent editions updated since 2010.)

2. NFPA 72: National Fire Alarm and Signaling Code. 2019

3. ISA-TR12.13.01-1999 (R2013) - Flammability Characteristics of Combustible Gases and Vapors. 2013

4. ISA 92.0.01: Performance Requirements for Toxic Gas Detection Instruments: Hydrogen Sulfide. 2015

5. IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems. 2010

6. IEC/ISA 61511: Functional Safety: Safety Instrumented Systems for the Process Industry Sector. 2018

7. Offshore hydrocarbon releases statistics and analysis, 2002, UK Health & Safety Executive Report HSR 2002 02, Feb 2003.

8. ISA Technical Report 84.00.07, Guidance on the Evaluation of Fire, Combustible Gas and Toxic Gas System Effectiveness. 2018