SIL ratings for fire & gas system hardware –
An introduction to ISA TR84.00.07

Paul Gruhn, PE, ICS Triplex | Rockwell Automation, Houston, TX

There are many devices (sensors, logic solvers and final elements) used in safety instrumented systems that are independently certified for use in certain safety integrity levels (SIL). There is considerable debate however whether fire & 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 & gas systems, focusing on the SIL rating or performance of the actual fire & 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 & gas systems, b) how typical voting of fire & 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 & gas systems.

So why the fuss?

Current fire detection and alarm standards such as EN 54\textsuperscript{1} and NFPA 72\textsuperscript{2} are prescriptive and focus on commercial applications (e.g., hotels). Current gas system standards such as ISA 12.13.01\textsuperscript{3} and 92.0.01\textsuperscript{4} are titled as performance based, but the term is used differently than in IEC standards such as 61508\textsuperscript{5} and 61511\textsuperscript{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 & gas systems from a performance (SIL) rather than a prescriptive point of view that was focused on industrial applications. The committee formed a new task team 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 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., 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.
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 61511.

<table>
<thead>
<tr>
<th>Safety integrity level (SIL)</th>
<th>Target average probability of failure on demand</th>
<th>Target risk reduction</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>≥10⁻⁵ to &lt;10⁻⁴</td>
<td>&gt;10,000 to ≤100,000</td>
</tr>
<tr>
<td>3</td>
<td>≥10⁻⁴ to &lt;10⁻³</td>
<td>&gt;1000 to ≤10,000</td>
</tr>
<tr>
<td>2</td>
<td>≥10⁻³ to &lt;10⁻²</td>
<td>&gt;100 to ≤1000</td>
</tr>
<tr>
<td>1</td>
<td>≥10⁻² to &lt;10⁻¹</td>
<td>&gt;10 to ≤100</td>
</tr>
</tbody>
</table>

Table 1: Performance Requirements for Safety Integrity Levels

EN 50402⁵ and IEC draft 60079-29⁶ on gas detection and safety integrity levels have recently been released. These documents focus on the effectiveness of the fire & gas system hardware alone and use the term SIL as used in IEC 61508 and 61511. However, IEC 61511 focuses on
safety instrumented systems which are prevention layers, although the concepts presented in the standard can be applied to all safety layers. Figure 4 in IEC 61511 clearly indicates the standard can be applied for mitigation safety layers.

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 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.

However, fire & 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 actually 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 100. This concept can be better understood with the event tree shown in Figure 2.

---

**Figure 2: Factors Effecting Fire and Gas System Performance**

- **Leak/Fire Detection Coverage:** The probability of the device actually being able to see 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 actually 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). \( \frac{1}{0.19} = 5 \). 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 naturally wish to do, is no guarantee of an effective fire & gas system.

Detector coverage

Fire & gas applications are capable of taking action 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 sensor failure. Typically, two or more sensors in a zone must 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 actually responding to a hazardous event. It is actually less likely for two or more detectors in a zone to be in the effected 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 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).

Conclusions

Concepts that apply to prevention safety layers such as safety instrumented systems do not necessarily apply to mitigation safety layers such as fire & gas systems. Unlike safety instrumented system hardware, claiming any integrity level for fire & 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 & 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 & 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. Work is proceeding within the ISA 84 committee on ways to account for detector coverage, mitigation effectiveness and other factors, thus allowing a quantitative, performance based approach to fire and gas system design. Once the detector coverage and mitigation effectiveness limitations are better understood and addressed, then focusing on the SIL rating of the hardware will be more meaningful.

Acknowledgements

The author does not claim to be the original developer of this work and gratefully acknowledges the ongoing efforts within the ISA 84 committee and fire & gas task team (TR84.00.07), information presented by end users such as Shell, BP and Chevron, and analysis work done by Kenexis. The intent of publishing this paper is to inform industry of the work being done, stimulate discussion, and recruit others to be involved in the continuing effort.

References

1. EN 54: Fire detection and fire alarm systems.
4. ISA 92.0.01: Performance Requirements for Toxic Gas Detection Instruments: Hydrogen Sulfide.
7. EN 50402: 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.

Author Bio: Paul Gruhn, PE, is the Training Manager at ICS Triplex | Rockwell Automation in Houston, Texas. Paul is an ISA Fellow, a member of the ISA 84 standard committee and its fire & gas task team, the developer and instructor of ISA courses on safety systems, and co-author of the ISA textbook on the subject. He has a B.S. degree in Mechanical Engineering from Illinois Institute of Technology, is a licensed Professional Engineer (PE) in Texas, and an ISA 84 Expert.