Performance-Based Gas Detection System Design for Hydrocarbon Storage Tank Systems

Srinivasan N. Ganesan, M.S., P.E.
MENA Region Manager, Kenexis DMCC, Dubai, UAE
Edward M. Marszal, PE, ISA 84 Expert

ABSTRACT

The design of hydrocarbon gas detection systems using risk analysis methods is drawing a lot of attention because industry experts have come to a consensus that design codes used in traditional gas detection system design work are not sufficient for open-door process areas having serious hazards, such as fire, flammable gas and toxic gas. The ISA Technical Report TR 84.00.07 provides guidelines for the design of fire and gas systems in unenclosed process areas in accordance with the principles given in IEC 61511 standards. This paper presents an overview of the design of gas detection systems using risk assessment methods that are described in the ISA technical report. These methods are statistical in nature and are used to assign and verify targets for the performance metrics (detector coverage and safety availability) of gas detection systems. This paper also provides an overview of the performance based safety life cycle of gas detection systems from conceptual design stage to operations and maintenance.

1. INTRODUCTION

Risk assessment techniques are being increasingly used in the design of engineered safeguards, such as Fire and Gas Detection and Suppression Systems (FGS), Safety Instrumented Systems (SIS) and Alarm Systems. The principles of risk assessment used in the design of SIS can also be used in the design of Gas Detection Systems. A Gas Detection System is a type of instrumented safeguard intended to reduce risks posed by process plants, such as safety risk, environmental risk, and asset risk (commercial/business) to tolerable levels. However, gas detection systems systems are only capable of mitigating the consequence of a loss of containment, whereas safety instrumented systems are capable of preventing the consequence from occurring altogether.

All automated safety systems such as FGS, SIS, and High Integrity Pressure Protection Systems (HIPPS) need a “basis of safety” for the selection and design of its functional elements (sensor, logic solver and final control elements). In the design of Gas Detection Systems, it is important to select detectors of the appropriate technology and care must be taken to position the right number of detectors at the correct location for the system to respond on demand. In addition, the basis of safety specifies the mechanical integrity requirements for the equipment with respect to the type and frequency of preventive maintenance tasks required. In short, the basis of safety is at the core of decisions that are made with reference to selection and maintenance of instruments.

The two options for choosing basis of safety are – prescriptive and performance-based. Prescriptive basis of safety (such as NFPA 72 and EN 54 for fire alarming equipment) specifies the type of equipment, its location for installation and also addresses the requirements to maintain them. Not only do the prescriptive standards for FGS design provide a very comprehensive set of

rules for designing equipment, but they are also so well established for the design of fire alarm systems that they are often employed, at least, for the signaling portion of gas detection systems. These standards have evolved to be very effective for the fire alarms in occupied buildings, such as office buildings, hospitals, and schools, but often fall short for gas detection and even for fire detection in open process areas.

Prescriptive standards provide detailed requirements for basis many gas and fire system applications. However, they do not provide detailed requirements for gas detection in open-door areas, such as chemical process units and hydrocarbon storage tank farms. Some of the gas detection system elements (sensor, logic solver, final control element) typically found in chemical process facilities are not adequately covered by these prescriptive standards. In addition, they do not provide an optimal solution to deal with the hazards associated with process facilities, such as oil refineries and petrochemical plants. Specifically, they are not geared towards hazards such as, combustible hydrocarbon gases and toxic gases. As a matter of fact, toxic gases are completely unaddressed by these prescriptive standards, and combustible gases only slightly.

It is worthwhile to point out that the institutions that developed these prescriptive standards are cognizant of their shortcomings and therefore allow the use of performance-based basis of safety in areas where the users of the standards believe that the prescriptive guidance is ineffective. Performance-based standards use risk assessment techniques for decisions involving selection, design, and maintenance of gas detection systems. The intent of the performance-based approach is not to replace the prescriptive method, but to supplement it where prescriptive methods are ineffective.

Industry practitioners recognized the need for more guidance for performance-based design for gas detection systems and came to a consensus that this guidance has to come from a standards organization like the International Society of Automation (ISA). ISA Standards Panel 84 created a special working group called “working group 7” specifically to address performance-based design of fire and gas systems. The ISA Technical Report TR 84.00.07 that came out of the working group 7 provides guidelines for fire and gas systems in accordance with the principles provided in IEC 61511 standards. The Technical Report TR84.00.07 has generated considerable interest among oil & gas operating companies and EPC companies and it jumpstarted the application of risk assessment techniques to design fire and gas detection and suppression systems.

The basis of the IEC 61511 standard is to specify targets for performance metrics for each safety instrumented function that is protecting the plant from process-related risks. The target is selected based on the risk associated with the hazard that the safety instrumented function is intended to prevent. Gas detection systems pose challenges when trying to use risk analysis techniques that are compliant with ISA84/IEC 61511 standards for safety instrumented systems. The hazards associated with gas detection systems (especially as applied in the chemical process industries) are general in nature and it is difficult to characterize them in the context of layer of protection analysis (LOPA). Initiating events caused by leaks due to corrosion, erosion, and other physicochemical forces are not included in LOPA. Although the concept of probability of failure on demand is applicable to gas detection system functions, component equipment failures are not the only consideration and usually not even the most important. The inability of an gas detection system function to detect a gas leak because of lack of coverage can also lead to failure on demand. Recent data from the UK

North Sea area indicate that more than 30% of major gas releases were not detected by automated systems.

The ISA 84 working group 7 determined that a gas detection system can be designed similar to a SIS if detector coverage is considered as an additional performance metric. In addition to assigning targets for safety availability (equivalent to SIL), targets for detector coverage need to be assigned for gas detection systems so that the verification and validation of detector coverage is required in the gas detection system design.

2. FIRE and GAS DESIGN LIFE CYCLE

The safety life cycle defined in the ISA Technical Report TR84.00.07 for fire and gas systems is very similar to the one defined for safety instrumented systems in the IEC61511 standard. Risk scenarios must be identified before fire and gas systems can be selected for a particular application. The hazards and consequences associated with each scenario must be analyzed taking into account the impact on human lives and assets. It is also important to consider the frequency of occurrence of the consequence while making decisions on the fire and gas system. If it is anticipated that the consequence will occur quite frequently, then a more rugged risk mitigation system needs to be considered.

A risk assessment is performed before making a decision on the need for a fire and gas system. If the unmitigated risk is tolerable, there would be no design for a fire and gas system. If the unmitigated risk is not tolerable, recommendations would be made to design a fire and gas system to reduce the overall risk to tolerable levels.

If a decision is made to install a fire and gas system, the initial design is typically done using heuristics (rules of thumb). The ISA Technical Report TR 84.00.07 proposes that the procurement and installation of fire and gas systems should not immediately follow the initial design. Instead, the technical report suggests that the coverage provided by the detector layout in the initial design be calculated and verified to check if it meets its target. In addition to the coverage, the safety availability (equivalent to SIL) for each function should be calculated and verified in a way identical to verifying the SIL of a safety instrumented system in accordance with the IEC 61511 standard. The typical work flow in the safety life cycle of performance-based fire and gas system design is shown in Figure 1.

2.1. Identify Gas Detection System Requirements

The first step in the FGS safety life cycle is identifying the need for a gas detection system. The need for a gas detection system usually stems from risk assessment studies, such as PHA, HAZOP, and “What-if”-checklist. Typically, the study team would come to a qualitative consensus that the unmitigated risk is not tolerable and would recommend the implementation of a gas detection system for mitigating the risk to tolerable levels. Even semi-quantitative risk analysis techniques like layer of protection analysis (LOPA) often recommend the implementation of fire and gas systems. And finally, a lot of jurisdictions around the world mandate the creation of safety cases that include quantitative risk assessment (QRA) studies in plant design as a pre-requisite to issue an operational permit for the facility.

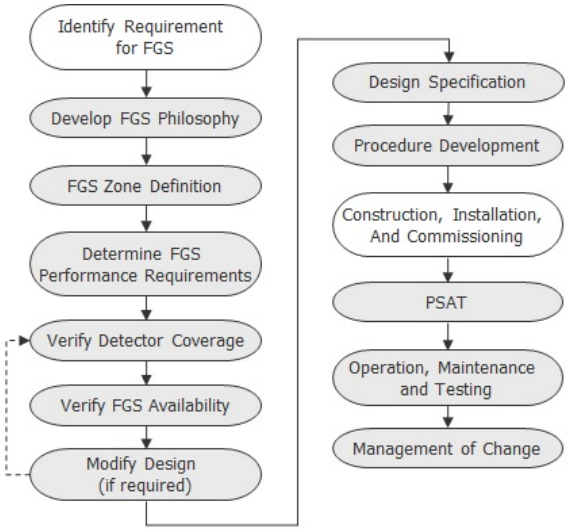


Figure 1. Typical work flow in the safety life cycle of performance-based FGS

If a QRA study has been the basis for an operational license from an authority, the process facility needs to have a gas detection system in place whose performance is in accordance with the assumptions made in the QRA study – otherwise, the basis for the safety case and operational permits are invalid. In addition, industry best practices and corporate HSE policies often require gas detection systems to be implemented in a process facility to mitigate risk. Last but not the least, insurance companies often require a fully functional fire and gas system as a pre-requisite to insure the facility.

2.2. Gas Detection System Philosophy Development

Once the need for a gas detection system has been established, the next step in the safety life cycle is the development of a gas detection system philosophy document (which often incorporates requirements for fire detection as well as gas detection). Efforts should be directed towards the creation of a comprehensive fire and gas philosophy that would be the basis for making decisions involving the design of fire and gas systems. The fire and gas system philosophy would define the tools, techniques, policies, and procedures surrounding fire and gas system design. The document, compliant with the IEC 61511 standard and ISA Technical Report 84.00.07, is developed once, most likely at the corporate level, so the philosophy can be applied to all fire and gas systems within the organization. In other words, it provides a common framework for making decisions involving fire and gas systems throughout the organization.

The intent of the fire and gas philosophy document is to standardize the methods that will be used in identifying the hazards the fire and gas systems intend to protect against. Hazards will be identified based on criteria such as properties of material being processed (flammability, reactivity, toxicity), and process conditions (pressure, temperature). The philosophy document will have the list of requirements for the safety analysis that is going to be performed. In addition to setting up the methods and procedures for designing fire and gas systems, there will be criteria for various design-related tasks, such as zone definition, and zone grading. There will also be criteria for assigning

targets for performance metrics (detector coverage and safety availability) and criteria for choosing the appropriate technology for detectors and voting architecture for detection equipment.

2.3. Gas Detection System Zone Definition and Categorization

The next step in the life cycle is zone definition, which requires a thorough understanding of the process being analyzed. Technical documentation such as process flow diagrams, piping & instrumentation diagrams, cause & effect diagrams, and plot plans would aid in the understanding of the facility being studied. The process starts out by identifying zones within the entire plant area. Zones are small areas that are geographically limited so that specific mitigation actions could be taken depending upon the hazard present within the particular zone.

It is worthwhile to point out why zone definition is critical to the safety life cycle. Different areas in a process plant have different gas release hazards. Some process units such as amine treatment units and sulfur recovery units pose a H_2S toxic gas hazard. Some areas may be prone to pool fires while others may be prone to gas releases or gas jet fires. Therefore, it becomes important to define and segregate the zones from each other.

Finally, the definition of zones will assist plant operations personnel trained in hazard communication to respond effectively to an emergency situation. In a fire or gas release scenario, operations personnel will be forced to shut down process units and bring them to a safe state as a proactive measure to mitigate the consequence. Emergency response action plans in a process facility are developed with a good understanding of the nature and location of the hazards.

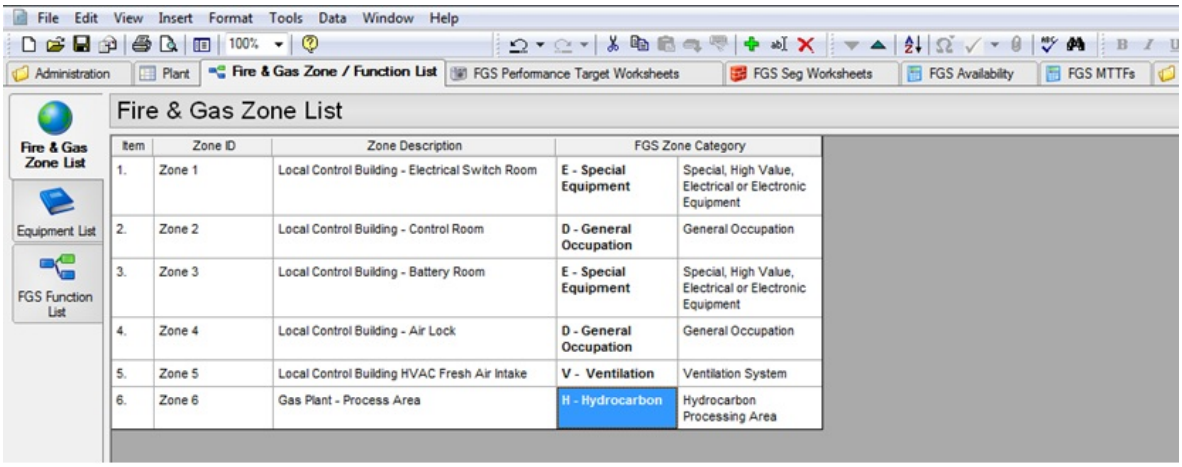
The definition and categorization of zones in a typical process facility are shown in Figure 2. The categorization of zones is necessary to select the appropriate mitigation techniques and actions for each particular zone. The different zone categories such as H, N, G, E, T, and V define different attributes of a process area. The first type of zone is type H which would include hydrocarbon process areas having fire and combustible/toxic gas hazards. The second type of zone is type N which would also include process areas, but with non-hydrocarbon fire hazards. The area with non-hydrocarbon fire hazard is not grouped into type H zone because the detection and suppression equipment for non-hydrocarbon-related fires is different from those of hydrocarbon-related fires.

Zone Categories	Area Definition	Examples
H	Hydrocarbon Possessing Area, General Fire / Flammable Gas, Toxic Gas Hazard	Production Separation, Gas Compression,
N	Non-Hydrocarbon Fire Hazard	Combustible Liquid Storage, Lubrication Oil System
G	General Occupancy, No Hydrocarbon Fire Hazard	Accommodations Area, Control Building
E	Non-Hydrocarbon Special Equipment Protection	Non-classified Electrical Equipment
T	Gas Turbine or Engine Enclosures	Gas Turbine and Turbine Enclosures
V	Combustion Air Intake / Ventilation Air Intakes	Combustion Air blower, HVAC Fresh Air Intake

Figure 2. Definition and categorization of zones

The third type of zone is type G which would include occupancy areas, such as control rooms, maintenance workshops, and administrative offices that are normally occupied by people and no chemical processing occurs inside them. The fourth type of zone is type E which would include non-hydrocarbon special equipment protection areas like instrument control rack rooms that house unrated electrical equipment and pose an explosion hazard if flammable gases were to enter the zone.

The fifth type of zone is type T which includes gas turbine enclosures and engine enclosures for which the fire and gas equipment requirements are very specific and stringent. The sixth and final zone type is type V which includes air intake ducts of occupied buildings in close proximity to a hydrocarbon process area. Type V zone is similar to type E zone from a standpoint of detecting flammable and toxic gases entering occupied buildings through an air intake system.



Item	Zone ID	Zone Description	FGS Zone Category	
1.	Zone 1	Local Control Building - Electrical Switch Room	E - Special Equipment	Special, High Value, Electrical or Electronic Equipment
2.	Zone 2	Local Control Building - Control Room	D - General Occupation	General Occupation
3.	Zone 3	Local Control Building - Battery Room	E - Special Equipment	Special, High Value, Electrical or Electronic Equipment
4.	Zone 4	Local Control Building - Air Lock	D - General Occupation	General Occupation
5.	Zone 5	Local Control Building HVAC Fresh Air Intake	V - Ventilation	Ventilation System
6.	Zone 6	Gas Plant - Process Area	H - Hydrocarbon	Hydrocarbon Processing Area

Figure 3. Typical zone list for a process area

The result of the zone definition task is a zone list that is shown in Figure 3. Each zone will be identified by a specific tag number defining the zone along with a brief description of the zone's location and its contents. The zone list will also show the category (as mentioned above) along with the attributes why that category was chosen for that particular zone. The zone list is entered into a database called the FGS design basis toolkit for managing the zones.

2.4. Setting and Verifying Performance Targets

Once all the zones are identified, targets for detector coverage and FGS safety availability (for FGS functions) in each zone need to be assigned consistent with the corporate philosophy on fire and gas system design. The detector coverage for the initial design will be calculated using quantitative models and will be verified to check if it meets its target. Similarly, the FGS safety availability (equivalent to SIL) for the functionality in each zone will be calculated and verified using conventional SIL verification techniques laid out in the IEC61511 standard.

If it is determined that the performance metrics fail to meet their target, the initial fire and gas system design will be revised by making changes to the number and position of detectors. The

verification calculations are rerun on the revised design and this recursive process continues until the performance metrics meet their target.

Assigning Detector Coverage

For the fire and gas detector coverage, the ISA Technical Report TR 84.00.07 identifies two types of coverage assessment methods – scenario coverage and geographic coverage.

Scenario coverage is defined as the fraction of the release scenarios that would occur as a result of the loss of containment in 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.

Geographic coverage is defined as the fraction of the geometric area (at a given elevation of analysis) of a defined monitored process area which, if a release were to occur in a given geographic location, would be detected by the release detection equipment considering the defined voting arrangement.

Consistent with the above definitions from the ISA Technical Report, there are two common methods for assigning targets for detector coverage – fully quantitative and semi quantitative. In the fully quantitative method, the targets for detector coverage are calculated using rigorous mathematical models that estimate the likelihood of an event and the magnitude of the consequence if that event were to occur. A consequence such as a gas release would be modeled using dispersion modeling techniques to determine the size and location of the gas cloud. In addition, fire and explosion models will be used to determine the impact on human lives and property if the gas cloud were to ignite and explode.

Unlike a safety instrumented system, a gas detection system can only mitigate the consequence but cannot prevent the initiating event from happening. Initiating events (such as a gas release) caused by factors such as welded joint failure, pipe/equipment corrosion, and gasket failure cannot be adequately addressed during a risk analysis study like HAZOP. It is therefore not possible to plan ahead for a consequence of this nature and the frequency of occurrence cannot be calculated based on a familiar matrix of initiating events. Instead, historical failure data of equipment will be used to estimate leak rate. The leak size is assumed to follow a standard statistical distribution and the likelihood of occurrence will be calculated using the estimated leak rate and leak size.

Once the parameters are estimated, a risk integration task is carried out integrating the consequence and likelihood to generate a list of possible scenarios. Each scenario will be associated with a certain risk level and it will be modeled using event trees. The risk posed by each scenario will be modified taking into account various mitigating factors, such as ignition probability, explosion probability, occupancy probability, and mitigation effectiveness. The individual risk associated with hundreds of thousands of scenarios in each zone will be integrated using a risk integration tool (event tree) like the one shown in Figure 4.

The semi quantitative approach is similar with respect to level of analysis effort to LOPA (layer of protection analysis) used in SIS design where tables with orders of magnitude in risk parameters are used to establish performance requirements. The semi quantitative techniques need to be calibrated

in order to ensure accuracy of the results. It is a team-based risk analysis of a fire and gas zone using calibrated risk assessment tables.

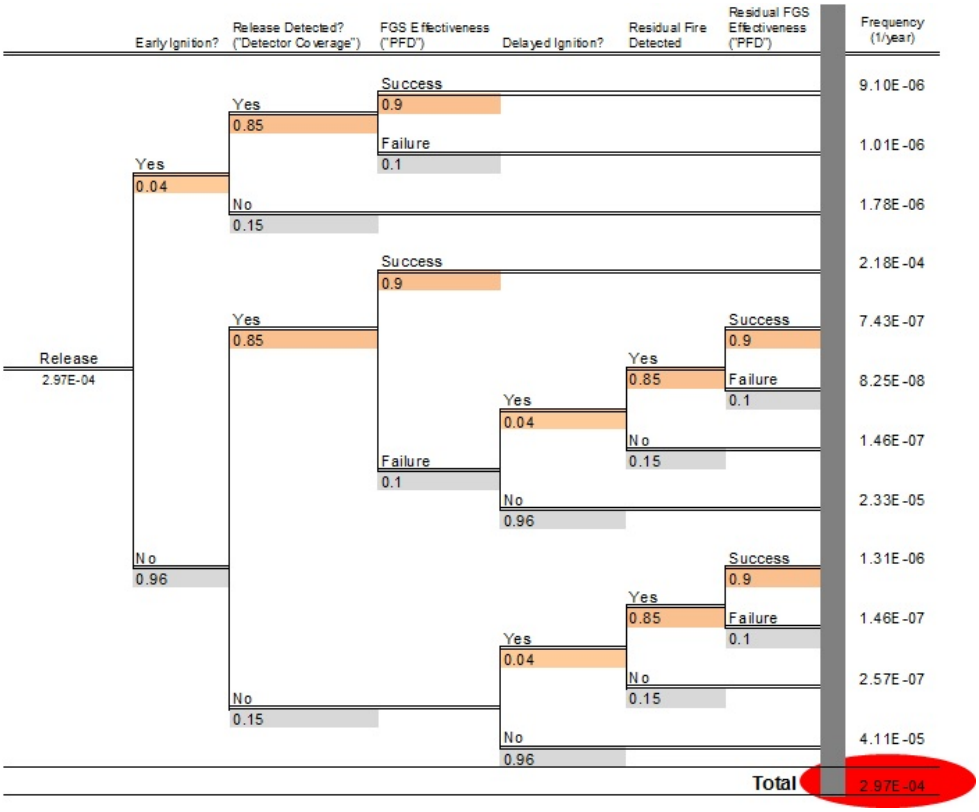


Figure 4. Risk integration using event tree for scenario coverage

The likelihood of an event (based on type of equipment in the zone), magnitude of the consequence (based on process parameters such as temperature, pressure and material composition), and mitigating factors (such as occupancy and ignition sources) are considered in determining the level of risk, utilizing a process similar to a risk graph. Grades are assigned inside each zone using a risk graph or a risk matrix that is developed for this purpose. Figure 5 shows a typical example of the different grades that could be used inside a zone and the associated level of risk along with targets for the performance metrics (detector coverage & safety availability).

Grade	Level of Risk	Detection Coverage	FGS Safety Availability
A	High Risk	0.90	0.95 (High SIL 1 Equivalent)
B	Medium Risk	0.80	0.90 (SIL 1 Equivalent)
C	Low Risk	0.60	0.90 (SIL 1 Equivalent)

Figure 5. Zone grades and associated level of risk

The performance target assigned to each grade in a zone is intended to make the risk tolerable for that particular zone. In the table shown in Figure 5, the risk associated with Grade A is the highest and the risk associated with Grade C is the lowest. Therefore, it is prudent to assign 90%

geographic coverage and 95% safety availability for Grade A and 60% geographic coverage and 90% safety availability for Grade C to reduce risk to tolerable levels.

It is important to note that a detailed and comprehensive calibration of the tables containing the performance targets is essential to the dependability and reliability of the semi-quantitative approach. A fully quantitative risk analysis is performed on typical process zones that have been assigned performance targets and zone grade and the magnitude of risk reduction is determined. The data from this analysis is used to develop an empirical model that is the backbone for this approach. The calibration technique is going to be based on geographic coverage as opposed to scenario coverage because of the strong positive correlation between these two coverage methods. In addition, geographic coverage is significantly easier and less expensive to determine than scenario coverage.

In addition to selecting different grades within a zone, it is also important to define boundaries for the different graded areas within that particular zone. In other words, one can conveniently assume that the hazards do not exist outside the graded areas in any particular zone. As mentioned earlier, the criteria for assigning grades within a zone must be available in the FGS philosophy document. The assignment of the extents of a graded area is done in a very similar fashion to electrical area classification, where potential leak sources are identified and areas within a certain distance of those sources are set off as "graded". While performing a geographic coverage assessment, the calculations are limited only to the graded areas and not to the entire zone.

Figure 6 shows the extent of grading and the geographic coverage for a typical process zone. The geographic coverage shown on the right is a color-coded map where red indicates that no detectors can detect the hazard, yellow means that only one detector can detect the hazard and green indicates that two or more detectors can detect the hazard. The visual map may also be supplemented with tables indicating percentage of the geographic area with no coverage, coverage by one detector and coverage by two or more detectors.

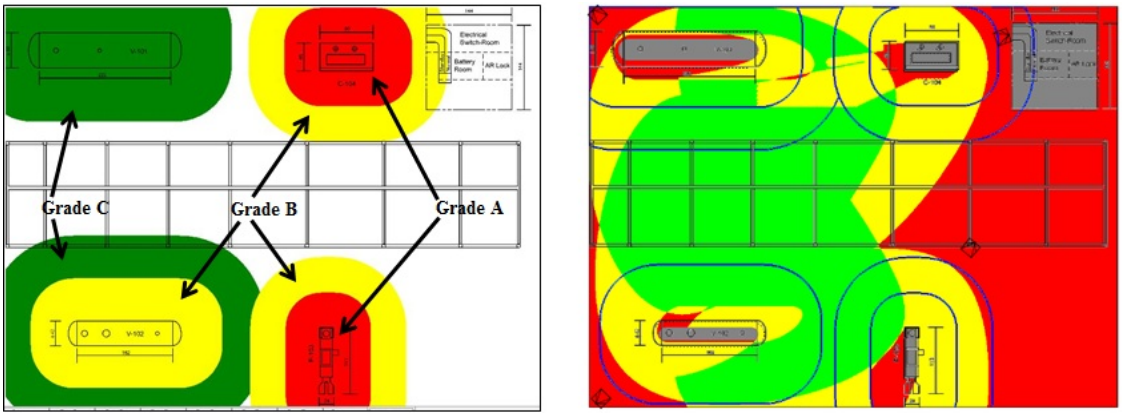


Figure 6. Extent of grading and geographic coverage in a process zone

Verifying Detector Coverage

After assigning the targets for detector coverage, the next step is to verify the fire and gas system detector coverage. The verification is based on factors such as zone definition, performance targets, and approved procedures for performing coverage calculations. The result of this analysis will be a

visual fire and gas map that is a color-coded representation of the areas covered and the extent of coverage of each area.

The performance of the detector plays a major role in a gas detector mapping assessment and it is usually provided by the equipment manufacturer. When performing a gas detector mapping assessment one needs to consider many attributes of the zone in consideration, the first consideration would be the performance of the detector. Subsequently, the size and shape of the gas release needs to be considered relative to the location of the detection equipment. When employing geographic coverage, the analyst sets the size of a "design basis" cloud, usually by determining the minimum gas cloud size that could result in a significant consequence (often, 4, 5 or 10 meters in diameter, depending on the situation). This design basis cloud is the moved around the zone that is under analysis. For each point in the zone, the ability of each individual detector to detect the design basis cloud if it were centered at that point is determined, fully in three dimensions. For scenario coverage, each potential release (considering multiple hole sizes, multiple release orientations and multiple wind directions) is plotted, and then each detector is assessed to determine if it would detect that release. The methods for gas detection coverage analysis are visually described in Figure 7.

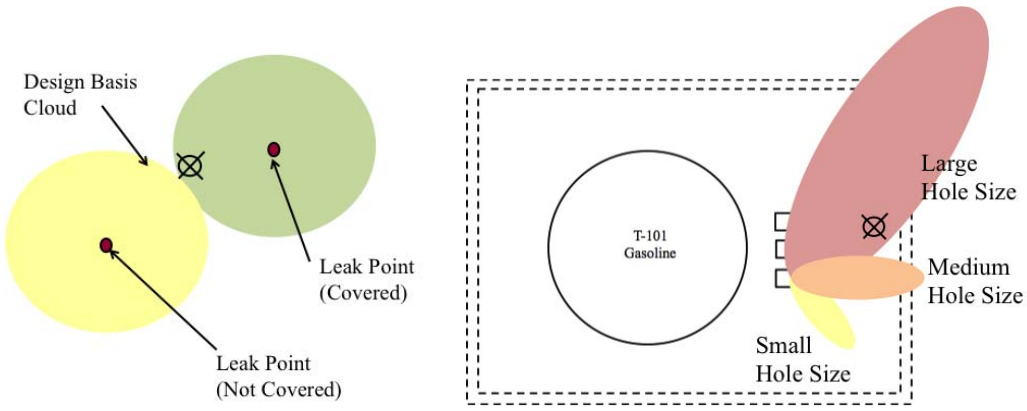


Figure 7. Gas Detection Mapping Technique Illustration

The geographic fire detector coverage for an example gasoline storage area with a few export pumps is shown in Figure 8. In this geographic coverage figure, green indicates coverage by two or more detectors, yellow indicates coverage by a single detector, and red indicates no coverage. It is also important to note that the areas containing equipment and vessel internals are eliminated from the coverage calculations.

Figures 9 and 10 show geographic risk profiles that result from the more rigorous quantitative risk analysis process and associated scenario coverage assessment. The first result (Figure 9) shows the unmitigated risk, or the risk assuming that there is no gas detection system in place.

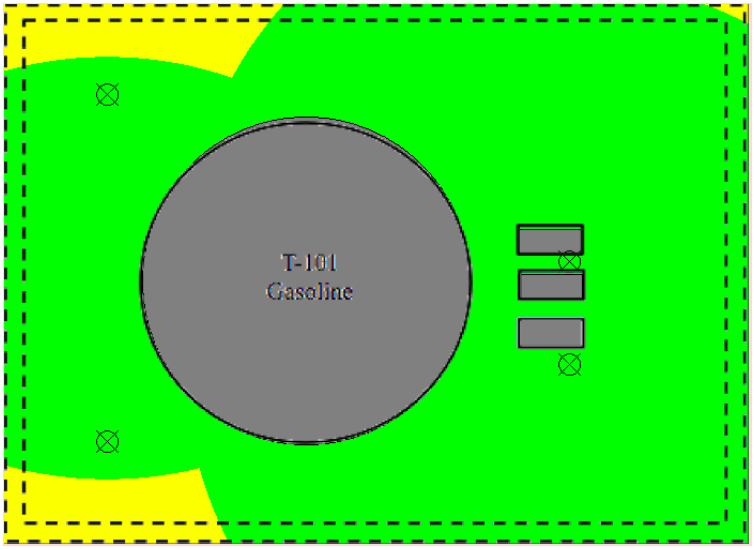


Figure 8. Geographic Coverage of a Typical Gasoline Tank Area

The geographic risk profile in a zone is represented using the visible color spectrum, where a color indicates the frequency of a gas release (or a fire release) existing at that specific location. At any particular location, colors on the right side of the visible color spectrum indicate high likelihood of a gas release or fire and colors on the left side of the visible spectrum indicate low likelihood of a gas release or fire.

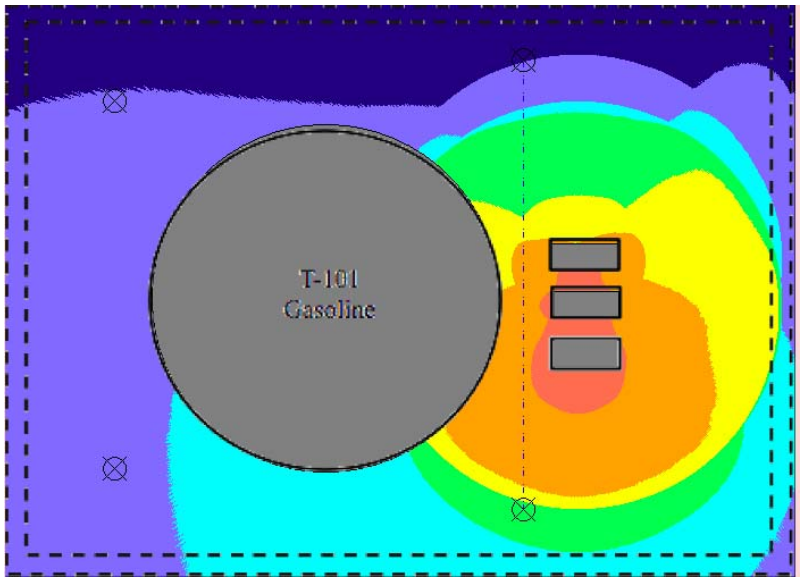


Figure 9. Geographic Risk Profile (Unmitigated by Gas Detection)

Figure 10 presents the mitigated geographic risk profile that includes risk reduction by the gas detection system. In this case, the gas system comprises of two point detectors on the left side of the tank and an open path detector between the tank and the associated transfer pumps. The graph contains colors predominantly on the left side of the visible color spectrum indicating that the risk has been substantially reduced. This figure is drawn, once again, by considering all of the leaks that are possible, but instead of plotting all of the gas clouds, only the gas clouds that are not detected by

the gas detection array are plotted. In addition, a calculation of the fraction of releases that are detected is calculated. This detection fraction is the scenario coverage, which can subsequently be used in the risk integration event tree.

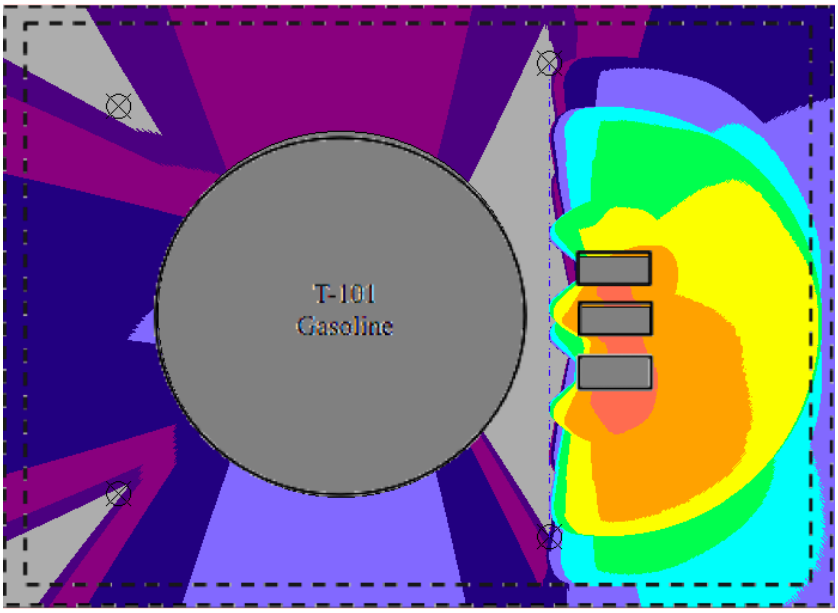


Figure 10. Geographic Risk Profile (Unmitigated by Gas Detection)

FGS Safety Availability

As discussed earlier, performance targets for safety availability need to be assigned and verified along with the detector coverage. The ISA Technical Report TR 84.00.07 specifically defines the metric in terms of safety availability in lieu of safety integrity level (SIL) because it was believed that assigning safety integrity level would be inappropriate for fire and gas systems. The effectiveness of a fire and gas system to respond on demand is primarily a function of the detector coverage rather than the ruggedness of hardware elements. The detector coverage has to be extremely high (99%) in order for the difference between SIL 2 and SIL 3 probability of failure to be of any significance.

During the conceptual design of the fire and gas system, FGS safety functions are defined and targets for safety availability are assigned in accordance with the guidelines given in the FGS philosophy document. The fire and gas detection equipment selected to achieve the performance target must meet both the general and specific requirements specification as applied to the overall system.

The factors that influence the FGS functions ability to achieve the target are component selection, fault tolerance, functional test interval, effect of common cause failures, and the diagnostic coverage of devices in the loop. All these variables are used in the calculations to verify if the specified safety availability target has been achieved. The safety availability verification calculations are identical to the SIL calculations done for safety instrumented systems and are based on the equations contained in the ISA Technical Report TR84.00.02.

The verification calculations are done using a customized tool kit that is developed from the equations given in the ISA Technical Report TR84.00.02. As an option, the verification calculations can also be performed manually using the same equations with the aid of a software application.

2.5. Gas Detection System Safety Requirements Specification

The next step in the gas detection system life cycle is to generate the gas detection system safety requirements specification (SRS) for the system. The safety requirements specification is a comprehensive document that includes detector placement drawings, cause & effect diagrams and general requirements on the attributes of the gas detection system.

After verifying the safety availability of all the functions, the final design needs to be documented in a safety requirements specification (SRS). The SRS defines how the gas detection system will perform and it is essentially the basis for the design and engineering of the FGS equipment. It contains not only the functional specification that defines the design basis but it also contains integrity specifications that define the system in terms of its performance metrics (detector coverage and safety availability). The FGS requirements specification provides the functional specification of the FGS logic solver which could be either take the form of cause and effect diagram or a binary logic diagram. The IEC 61511/ISA 84 standards provide guidelines and a checklist for the items that must be part of the FGS requirements specification.

2.6. Detailed Design & Procedure Development

The next step in the gas detection system design life cycle involves the detailed design and engineering of the system. This step involves a variety of tasks such as loop sheet development, internal wiring diagram preparation, cable schedule drawing development, and PLC (logic solver) programming. Along with the detailed design and engineering, procedures are also developed for the fire and gas system for various phases of the life cycle, such as start-up, operations, maintenance, and de-commissioning. It is quite likely that design shortcomings may be discovered during procedure development and this may trigger the need to revisit the initial steps of the safety life cycle and make changes to include provisions for bypasses and resets without having to take the system offline. If a hardware component in the fire and gas system fails, the failed component must be detected and repaired within the mean-time-to-repair (MTTR) that was assumed during the design phase and system maintenance procedures must clearly address repairs of this nature that have an impact on the facility's tolerable risk level. Finally, the functional testing of the fire and gas system needs to be carried out on a periodic basis and procedures need to be developed for the same.

2.7. Procurement, Construction & Installation

The next step in the fire and gas system life cycle involves the procurement, construction and installation of the equipment that has been engineered. Physical hardware such as, instrumentation cabinets, cables, fire detectors, and gas detectors will be purchased and installed on site. It is recommended that caution be exercised during the installation of field equipment for gas detection systems because the location and orientation of the detection equipment has a profound impact on the system's ability to achieve tolerable risk. The location and orientation of the detectors must be consistent with the values given in the safety requirements specification. Furthermore, the

placement of equipment with respect to the detectors must be consistent with the assumptions made during the design phase. Upon successful completion of the hardware installation, the software is installed into the system and the logic solver is custom programmed for the facility.

2.8. Pre-Startup Acceptance Testing (Validation)

The IEC 61511 standard requires that automated safety systems like gas detection systems be validated before they can be turned over to operations and maintenance. Validation is the task of verifying the installation of gas detection system equipment and software programming to check if the installation is conformance with both the safety requirements specification and the detailed engineering documentation. Validation involves a complete physical test of all safety critical functions starting from the field all the way to the plant control room. The deviations discovered during this step will be documented in a record called “punch list” and the items in the punch list need to be satisfactorily resolved before the system can be handed over to plant personnel.

2.9. Operations, Maintenance & Testing

Once the validation is completed, the system is turned over to operations and maintenance for day-to-day operations, which include simple things such as responding to alarms, responding to failure alarms, and periodic functional testing and preventive maintenance to ensure that performance levels that were specified during design are being achieved round-the-clock throughout the life cycle of the facility. During the normal operation and maintenance phase of the life cycle, periodic function testing and maintenance need to be carried out to ensure that the targets for the performance metrics (detector coverage and safety availability) are still achieved.

2.10. Management of Change (MOC)

During the life cycle of the facility, any changes made to the facility or to that of the fire and gas system need to be considered in the safety life cycle to make sure that the change(s) do not affect the performance of the system. It is not unusual for a facility to go through a wide range of changes such as retrofitting equipment, adding new pumps, building new structure, etc. These changes may increase the number of leak sources, change zone definition and may also change the categorization of the zone discussed earlier. It is also possible that these changes may obstruct the ability of gas detection equipment and may compromise the achieved detector coverage. It is therefore very important to make sure that the facility’s management of change procedures includes step-by-step instructions to review changes that have an impact on the gas detection system. If it is determined that changes will impact the performance of the gas detection system, the appropriate steps in the safety life cycle of the system needs to be revisited and design must be revised.

3. CONCLUSION

Risk assessment methods are being increasingly used in the design of instrumented safeguards, such as SIS, Alarm Systems, HIPPS, etc. Gas detection systems are no exception to this trend. However, gas detection systems are only capable of mitigating the consequence, whereas safety instrumented systems are capable of preventing the consequence from occurring – which greatly complicates their analysis. The hazards associated with fire and gas systems are general in nature and it is difficult to characterize them in the context of layers of protection analysis (LOPA). Initiating events caused by pipe leaks due to corrosion, erosion, and other physicochemical forces are typically not included in LOPA.

The ISA Technical Report TR 84.00.07 provides recommendations for the design of gas detection systems in open-door chemical process areas having serious hazards. The technical report proposes that an FGS be designed similar to a SIS if detector coverage is considered as an additional performance metric. This paper has provided an overview of the risk-assessment methods used in the design of fire and gas systems and has described the methods available to assign and verify targets for the performance metrics. This paper also provides a roadmap of the steps involved the safety life cycle of a gas detection system explaining how each step is interconnected with the other and why it is important to follow a holistic approach to the design of automated systems in a safety critical environment.

REFERENCES

1. ISA TR84.00.07 “The Application of ANSI/ISA 84.00.01 – 2004 Parts 1-3 (IEC 61511 Parts 1-3 Modified) for Safety Instrumented Functions (SIFs) in Fire & Gas Systems” Version A, October 2007.