Foreword

The work to develop this edition of ISA-TR84.00.07 began in 2014 and was completed in 2018. At the same time, the functional safety standard ANSI/ISA 84.00.01-2004 was undergoing updates in parallel with IEC 61511. The ISA84 Fire and Gas Working Group maintained awareness of committee activities associated with modifying the governing standards. The scope of updates to the 2nd Edition of this technical report was limited by the ISA84 committee, and it was not in the working group's charter to align this edition of the technical report with the subsequent issuance of ISA's functional safety standard.

This technical report describes how the underlying principles of the functional safety standards can be applied to fire and gas systems. Those same underlying principles that were used to develop the guidance in the technical report remain consistent in the new issuance of IEC 61511-2016 and ANSI/ISA-61511-2018 (replacing ANSI/ISA-84.00.01-2004). Because of the timing associated with approval and publication, this technical report retains the references to ANSI/ISA-84.00.01-2004. At the time of publication, the working group provides this acknowledgment that the recent publication of ANSI/ISA-61511-2018 retains the same scope, application and underlying principles associated with fire and gas systems.

ISA-TR84.00.07-2018 is intended for use in evaluating the effectiveness of fire and gas systems (FGSs) in process industry applications. It addresses the implementation of FGSs to reduce the risk of hazardous releases involving safety impact.

NOTE Users can choose to apply the concepts in this technical report to environmental and/or operational loss scenarios.

ISA-TR84.00.07-2018 is provided for information purposes only and is not part of ANSI/ISA-84.00.01-2004 (IEC 61511 Modified) (reference 2.1).

ANSI/ISA-84.00.01-2004 and IEC 61511 (reference 2.9) are performance-based standards that provide the minimum requirements for designing and managing a safety instrumented system (SIS). As part of the safety lifecycle, the functional and integrity requirements are established for safety functions that reduce the risk of hazardous events identified using a hazard and risk analysis. Guidance is provided in Part 3 of either ANSI/ISA-84.00.01-2004 or IEC 61511 on the various methods used to evaluate risk and allocate risk reduction to identified safety functions. An underlying assumption in all of the methods is that the identified safety functions are capable of achieving the allocated risk reduction in the operating environment.

The scope of ANSI/ISA-84.00.01-2004 covers electrical / electronic / programmable electronic systems for use in safety applications. Accordingly, the ISA84 committee develops standards and technical reports to provide guidelines for the implementation of automated (or instrumented) systems in safety applications. The purpose of ISA-TR84.00.07-2018 is to provide guidance on how to evaluate the effectiveness of identified FGS functions in a manner that is consistent with the underlying principles of ANSI/ISA-84.00.01-2004. FGS functions that are identified as safety controls, alarms, or interlocks should be implemented according to the applicable requirements of ANSI/ISA-84.91.01-2012 (reference 2.10) and ANSI/ISA-84.00.01-2004, based on the degree of risk reduction being claimed for the FGS function, in addition to relevant application specific practices. For example, FGS functions should be implemented per applicable requirements in the following standards, based on the risk reduction needed:

- General fire and gas system safeguards with no specific risk reduction claimed should be implemented per application-specific standards from local jurisdiction having authority.
- FGS functions with claimed FGS risk reduction factor (RRF) less than or equal to 10 should be implemented per applicable requirements of ANSI/ISA-84.91.01-2012, *Safety Controls, Alarms and Interlocks in the Process Industries.*
- FGS function with claimed FGS risk reduction factor (RRF) in excess of 10 should be implemented per the applicable requirements of ANSI/ISA-84.91.01-2012 and ANSI/ISA-

84.00.01-2004 (based on IEC 61511 compliance, which includes consideration for IEC 61508 compliance and/or end-user prior use approval of sensor, logic solver and final element sub-systems).

Prescriptive approaches for the design of some/all components of an FGS are provided in recognized and generally accepted good engineering practices (reference 2.2 and 2.3) for certain applications. In complex hazard scenarios, especially those involving high-risk exposure (e.g., offshore oil and gas installations), and in situations where no other prescriptive guidance is available, supplementing these practices with performance-based analysis can result in an improved design with more effective coverage and lower probability of FGS failure. It is ultimately the user's decision on when to apply performance-based approaches. Nothing in this technical report suggests the prescriptive practices are invalid or that they should not be followed as required by local jurisdictional authorities. The concepts underlying a performance-based approach are suitable to the analysis and design of FGSs in process industries, and these principles can be used effectively in conjunction with other good engineering practices.

THE EXAMPLE RISK ANALYSIS METHODS AND RISK CRITERIA CONTAINED IN THIS TECHNICAL REPORT HAVE BEEN PROVIDED SOLELY AS EXPLANATORY MATERIAL AND SHOULD NOT BE INTERPRETED AS RECOMMENDATIONS.

ALSO, THE EXAMPLE FGS ARCHITECTURES, DETECTOR COVERAGES, AND MITIGATION EFFECTIVENESS REPRESENT POSSIBLE SYSTEM CONFIGURATIONS AND SHOULD NOT BE INTERPRETED AS RECOMMENDATIONS. THE CONFIGURATIONS USED IN ACTUAL APPLICATIONS ARE SPECIFIC TO THE OPERATING ENVIRONMENT AND PROCESS CONDITIONS IN WHICH THEY ARE USED. AS SUCH, NO GENERAL RECOMMENDATIONS CAN BE PROVIDED THAT ARE APPLICABLE IN ALL SITUATIONS.

THE USER OF THIS TECHNICAL REPORT IS CAUTIONED TO CLEARLY UNDERSTAND THE ASSUMPTIONS AND DATA ASSOCIATED WITH THE METHODOLOGIES IN THIS DOCUMENT BEFORE ATTEMPTING TO UTILIZE THE METHODS PRESENTED HEREIN.

Users of ISA-TR84.00.07-2018 will include:

- Vendors, end-users, and consultants who are applying the performance-based concepts to FGS functions, in addition to other applicable good engineering practices.
- Hazard and risk analysis teams that are allocating risk reduction to FGS functions.
- FGS designers who want to understand the impact of detector coverage and mitigation effectiveness on the integrity of FGS functions.
- Any additional entities who wish to gain further insight into performance based FGS design concepts.

Introduction

The ISA84 standards committee formed a working group to study the analysis and design processes that are commonly used in the process industry for fire and gas systems (FGSs) and to provide guidance on how these processes can be adapted to incorporate performance-based concepts.

FGSs, as they are considered in this report, are a subset of industrial automation and control systems that are employed in the process industries for the purpose of detecting loss of containment of hazardous materials from the process and initiating a response to mitigate the release impact. Loss of containment can be a small leak or a catastrophic release. It can be detected by measuring the presence of the released materials (e.g., gas concentration) or inferred from the effects of the release (e.g., thermal radiation from a fire).

Detection methods considered in this technical report can include detection of combustible gas, toxic gas, smoke, flame, acoustic emission, or rapid heat rise in areas adjacent to the process itself and in critical areas, such as occupied buildings or buildings with unrated electrical equipment. Detector coverage and associated detection capability vary substantially depending on the hazard scenario and the characteristics of the detector.

Actions taken by the FGS can be manually or automatically initiated and can affect a wide variety of systems, such as sheltering in place or evacuation in response to audible and visual alarm indications; water deluge; fire suppressant initiation; manipulation of heating, ventilation, and air conditioning (HVAC) system equipment; process isolation; or process depressurization. Similar to detection capability, the effectiveness of these mitigative actions is highly scenario dependent.

Use of performance-based design is not widely adopted for FGSs within the process industries. However, ANSI/ISA-84.00.01-2004 or IEC 61511 can be employed as a design basis for mitigative fire and gas safety functions by considering the following definitions from ANSI/ISA-84.00.01-2004 or IEC 61511:

mitigation
action that reduces the consequence(s) of a hazardous event

NOTE 1 Examples include emergency depressurization on detection of a confirmed fire or gas leak.

prevention
action that reduces the likelihood of occurrence of a hazardous event

protection layer
any independent mechanism that reduces risk by control, prevention, or mitigation

NOTE 1 It can be a process engineering mechanism such as the size of vessels containing hazardous chemicals, a mechanical mechanism such as a relief valve, a SIS, or an administrative procedure such as an emergency plan against an imminent hazard. These responses may be automated or initiated by human actions.

[SOURCE: IEC 61511-1:2016, Definition 3.2.61, modified – reference to Figure 9 removed from Note 1]

safety function
function to be implemented by one or more protection layers, which is intended to achieve or maintain a safe state for the process, with respect to a specific hazardous event

NOTE 1 The safe state of the process for each identified safety function is defined such that a stable state has been achieved and the specified hazardous event has been avoided or sufficiently mitigated.

[SOURCE: IEC 61511-1:2016, Definition 3.2.69, added Note 1, derived from 10.3.1.d]

safety instrumented function (SIF)
safety function to be implemented by a safety instrumented system (SIS)

NOTE 1 A SIF is designed to achieve a required SIL, which is determined in relationship with the other protection layers participating in the reduction of the same risk.

There are two broadly different philosophical approaches used in the process industries for establishing design requirements to ensure the availability and effectiveness of FGSs: prescriptive and performance-based. The choice of design method is an owner/operator decision. FGSs have traditionally been designed and implemented according to various good engineering practices, such as NFPA 72 (reference 2.2) and EN 54 (reference 2.3). These prescriptive practices do not require evaluation of the risk reduction capability of the FGS as measured by its safety integrity and probability of failure on demand (PFD), nor do they consider quantitative measures for detector coverage.

A performance-based approach consistent with the ANSI/ISA-84.00.01-2004 or IEC 61511 is attractive because it builds on the strength of the existing standard. However, without guidance, a performance-based approach has historically been challenging to apply to FGS design due to several factors.

Traditional hazard and risk analysis techniques are suited for hazards related to process deviations from normal operation. These process hazards have known initiating causes and consequences, allowing the safety function to be specifically designed to detect the event and to respond by achieving or maintaining a safe state of the process. FGSs are typically implemented to reduce the risk of general loss of containment, such as leaks from equipment seals, flanges, and piping, and are often not associated with a specific hazardous scenario. These hazards can be difficult to define and analyze and often require the use of advanced risk analysis techniques, such as gas dispersion, fire, and explosion modeling.

Most often FGSs do not prevent hazardous consequences from occurring, but rather mitigate the effects of an event that has already occurred. FGSs typically reduce the magnitude and severity of the consequence instead of eliminating it. Typical hazard and risk analysis assumes that the identified safety function eliminates the consequence. Therefore, it is important to understand and evaluate the hazard scenario resulting from FGS operation to ensure that the residual risk is acceptable.

An FGS can provide poor risk reduction due to an inadequate detection rate. An analysis by Health and Safety Executive (HSE) of eight years of hydrocarbon release data (reference 2.4) showed that the effective detection rate was about 60%. The detection of many releases was significantly delayed, leading to higher consequences than expected. Even if very high integrity can be achieved by the hardware design and testing (e.g., low average probability of failure on demand), sufficient reduction in risk will not occur unless the detector coverage is also very high. For FGS functions, detector coverage should be analyzed with the same (if not more) quantitative rigor as the verification of the average probability of failure on demand for the hardware design.

FGS effectiveness is also related to the ability of the mitigation elements (e.g., fire water system, ventilation system, process isolation) to function in a way that reduces hazardous consequences predictably. Mitigation can include

- stopping the process
- diverting the hazardous material
- applying fire water with the appropriate flow and spray characteristics
- activating alarms notifying personnel to shelter in place or evacuate

As in the case of detector coverage, the effectiveness of the mitigative actions is dependent on many situational or scenario-specific factors. As a result of these complexities, initiating an FGS's action might not necessarily mean that the consequence can be fully mitigated.

As a result of these factors, a comprehensive approach to the hazard and risk analysis is indicated, as it is often difficult to develop a sound technical justification for allocating risk reduction to FGS functions using a simplified risk assessment process, such as layer of protection analysis (LOPA)

(reference 2.5 and 2.6). The identification of FGS functions and allocation of performance targets to them requires hazard and risk considerations that are beyond typical LOPA implementation. Furthermore, FGS performance verification should include evaluation of the detector coverage and consider the effectiveness of the mitigative actions and the safety availability of FGS hardware and software design.

This ISA technical report describes the analysis that should be undertaken and the effectiveness criteria that should be specified when an FGS is implemented in a safety application. The report integrates performance-based fire and gas system design techniques into the applicable portions of the safety life cycle described in either ANSI/ISA-84.00.01-2004 or IEC 61511. The report also discusses the development of detector-coverage criteria applicable to each FGS function and includes a series of application examples (Annex D) that illustrate the techniques used to develop and verify the detector coverage and mitigation effectiveness.

1 Scope

This technical report is informative and does not contain any mandatory requirements.

This technical report is intended to be used in conjunction with other good engineering practices applicable to FGS installations. It is not intended to stand alone or be a replacement for application-specific practices.

ISA-TR84.00.07 is a derivative of the ANSI/ISA-84.00.01-2004 (IEC 61511 Mod) standard with application to process industries. This technical report is intended to address detection and mitigation of fire, combustible gas, and toxic gas hazards in process areas. Fire detection and mitigation within nonprocess areas is outside the scope of this document.

This technical report is intended to:

- Be used by those with a thorough understanding of ANSI/ISA-84.00.01-2004.
- Clarify the additional information that should be considered when developing a performance-based FGS design. This includes integrating the design activities into relevant portions of the safety life-cycle model.
- Clarify how to define FGS functions within typical FGS designs where automatic action is taken as a result of detection of a fire or gas event.
- Provide example scenario assessments to demonstrate the application of performance-based concepts to the analysis and design of FGSs.
- Demonstrate that any coverage or effectiveness factor below 90% results in an FGS risk reduction factor of less than 10 of the FGS design.
- Offer a performance-based methodology—for facilities using a prescriptive methodology (e.g., API-14C or API 14G) (reference 2.20 and 2.21) to allocate fire and gas detection. The methodology provides considerations for how to improve fire and gas effectiveness. The performance-based design process described in this TR can provide more effective hazard detection and detector placement in cases where fusible plugs (fire) may be needed.
- Define a methodology that addresses the design and effectiveness of FGS mitigative functions that is consistent with the underlying principles used to design and assess the effectiveness of preventative functions.

2 References

1. ANSI/ISA-84.00.01-2004 (IEC 61511 Mod), *Functional Safety: Safety Instrumented Systems for the Process Industry Sector,* Parts 1, 2 & 3, International Society of Automation, Research Triangle Park, N.C., 2004.

2. NFPA 72, National Fire Alarm Code, National Fire Protection Association, 2016.

3. EN 54-2: 1997 Fire Detection and Fire Alarm Systems Part 2: Control and Indicating Equipment.

4. HSE Offshore Fire and Explosion Strategy – Issue 1; http://www.hse.gov.uk/offshore/strategy/fgdetect.htm.

5. CCPS/AIChE, Layer of Protection Analysis: Simplified Process Risk Assessment, First Edition, New York, 2001.

6. CCPS/AICHE, Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis, First Edition, New York 2015.