

ISA-TR84.00.05-2009

**Guidance on the Identification of Safety
Instrumented Functions (SIF)
in Burner Management Systems (BMS)**

Approved 10 December 2009



Documents
Document Sharing Hub

ISA-TR84.00.05-2009, Guidance on the Identification of Safety Instrumented Functions (SIF) in Burner Management Systems (BMS)

ISBN: 978-1-936007-41-7

Copyright © 2009 by ISA. All rights reserved. Printed in the United States of America. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without the prior written permission of the Publisher.

ISA
67 Alexander Drive
P.O. Box 12277
Research Triangle Park, North Carolina 27709

Preface

This preface is included for information purposes and is not part of ISA-TR84.00.05-2009.

This technical report has been prepared as part of the service of ISA, the International Society of Automation. To be of real value, this document should not be static but should be subject to periodic review. Toward this end, the Society welcomes all comments and criticisms and asks that they be addressed to the Secretary, Standards and Practices Board; ISA, 67 Alexander Drive; P.O. Box 12277; Research Triangle Park, NC 277099; Telephone (919) 549-8411; Fax (919) 549-8288; E-mail: standards@isa.org.

This ISA Standards and Practices Department is aware of the growing need for attention to the metric system of units in general, and the International System of Units (SI) in particular, in the preparation of instrumentation standards, recommended practices, and technical reports. The Department is further aware of the benefits to users of ISA standards documents of incorporating suitable references to the SI (and the metric system) in their business and professional dealings with other countries. Toward this end, the Department will endeavor to introduce SI and acceptable metric units in all new and revised standards documents to the greatest extent possible. The Metric Practice Guide, which has been published by the Institute of Electrical and Electronics Engineers (IEEE) as ANSI/IEEE Std. 268-1992, and future revisions, will be the reference guide for definitions, symbols, abbreviations, and conversion factors.

It is the policy of ISA to encourage and welcome the participation of all concerned individuals and interests in the development of ISA standards. Participation in the ISA standards-making process by an individual in no way constitutes endorsement by the employer of that individual, of ISA, or of any of the standards, recommended practices, and technical reports that ISA develops.

CAUTION — ISA DOES NOT TAKE ANY POSITION WITH RESPECT TO THE EXISTENCE OR VALIDITY OF ANY PATENT RIGHTS ASSERTED IN CONNECTION WITH THIS DOCUMENT, AND ISA DISCLAIMS LIABILITY FOR THE INFRINGEMENT OF ANY PATENT RESULTING FROM THE USE OF THIS DOCUMENT. USERS ARE ADVISED THAT DETERMINATION OF THE VALIDITY OF ANY PATENT RIGHTS, AND THE RISK OF INFRINGEMENT OF SUCH RIGHTS, IS ENTIRELY THEIR OWN RESPONSIBILITY.

PURSUANT TO ISA'S PATENT POLICY, ONE OR MORE PATENT HOLDERS OR PATENT APPLICANTS MAY HAVE DISCLOSED PATENTS THAT COULD BE INFRINGED BY USE OF THIS DOCUMENT AND EXECUTED A LETTER OF ASSURANCE COMMITTING TO THE GRANTING OF A LICENSE ON A WORLDWIDE, NON-DISCRIMINATORY BASIS, WITH A FAIR AND REASONABLE ROYALTY RATE AND FAIR AND REASONABLE TERMS AND CONDITIONS. FOR MORE INFORMATION ON SUCH DISCLOSURES AND LETTERS OF ASSURANCE, CONTACT ISA OR VISIT WWW.ISA.ORG/STANDARDSPATENTS.

OTHER PATENTS OR PATENT CLAIMS MAY EXIST FOR WHICH A DISCLOSURE OR LETTER OF ASSURANCE HAS NOT BEEN RECEIVED. ISA IS NOT RESPONSIBLE FOR IDENTIFYING PATENTS OR PATENT APPLICATIONS FOR WHICH A LICENSE MAY BE REQUIRED, FOR CONDUCTING INQUIRIES INTO THE LEGAL VALIDITY OR SCOPE OF PATENTS, OR DETERMINING WHETHER ANY LICENSING TERMS OR CONDITIONS PROVIDED IN CONNECTION WITH SUBMISSION OF A LETTER OF ASSURANCE, IF ANY, OR IN ANY LICENSING AGREEMENTS ARE REASONABLE OR NON-DISCRIMINATORY.

ISA REQUESTS THAT ANYONE REVIEWING THIS DOCUMENT WHO IS AWARE OF ANY PATENTS THAT MAY IMPACT IMPLEMENTATION OF THE DOCUMENT NOTIFY THE ISA STANDARDS AND PRACTICES DEPARTMENT OF THE PATENT AND ITS OWNER.

ADDITIONALLY, THE USE OF THIS DOCUMENT MAY INVOLVE HAZARDOUS MATERIALS, OPERATIONS OR EQUIPMENT. THE DOCUMENT CANNOT ANTICIPATE ALL POSSIBLE APPLICATIONS OR ADDRESS ALL POSSIBLE SAFETY ISSUES ASSOCIATED WITH USE IN HAZARDOUS CONDITIONS. THE USER OF THIS DOCUMENT MUST EXERCISE SOUND PROFESSIONAL JUDGMENT CONCERNING ITS USE AND APPLICABILITY UNDER THE USER'S PARTICULAR CIRCUMSTANCES. THE USER MUST ALSO CONSIDER THE APPLICABILITY OF ANY GOVERNMENTAL REGULATORY LIMITATIONS AND ESTABLISHED SAFETY AND HEALTH PRACTICES BEFORE IMPLEMENTING THIS DOCUMENT.

THE USER OF THIS DOCUMENT SHOULD BE AWARE THAT THIS DOCUMENT MAY BE IMPACTED BY ELECTRONIC SECURITY ISSUES. THE COMMITTEE HAS NOT YET ADDRESSED THE POTENTIAL ISSUES IN THIS VERSION.

The following served as voting members of ISA84 and approved this technical report:

NAME	COMPANY
W. Johnson, Chair	E I du Pont
V. Maggioli, Managing Director	Feltronics Corp
R. Adamski	RA Safety Consulting LLC
T. Ando	Yokogawa Electric Co
R. Avali	Westinghouse Electric Corp
L. Beckman	Safeplex Systems Inc
J. Campbell	ConocoPhillips
I. Chen	Aramco
M. Coppler	Ametek Inc
M. Corbo	ExxonMobil
K. Dejmek	Baker Engineering & Risk Consultants
P. Early	Langdon Coffman Services
K. Gandhi	KBR
J. Gilman	JFG Technology Transfer LLC
W. Goble	Exida
P. Gruhn	ICS Triplex
B. Hampshire	BP
J. Harris	UOP A Honeywell Company
J. Jamison	EnCana Corporation Ltd
R. Johnson	Dow Process Automation
K. Klein	Celanese Corp
T. Layer	Emerson Process Management
E. Marszal	Kenexis Consulting Corp
N. McLeod	ARKEMA
R. Peterson	Lyondell Chemical Company
G. Ramachandran	Shell Global Solutions US
M. Scott	AE Solutions
D. Snizek	Lockheed Martin Federal Services
C. Sossman	CLS Tech-Reg Consultants
R. Strube	Strube Industries
A. Summers	SIS-TECH Solutions LP
L. Suttinger	Savannah River Nuclear Solutions
R. Taubert	Consultant
H. Thomas	Air Products & Chemicals Inc
T. Walczak	Conversions Inc
M. Weber	System Safety Inc
A. Woltman	Shell Global Solutions
P. Wright	BHP Engineering & Construction Inc
D. Zetterberg	Chevron Energy Technology Company

The following served as members of the ISA Standards and Practices board and approved this technical report:

NAME	COMPANY
J. Tatera, VP	Tatera & Associates Inc.
D. Dunn, VP Elect	Aramco Services Co
P. Brett	Honeywell, Inc
M. Coppler	Ametek, Inc
E. Cosman	The Dow Chemical Co
B. Dumortier	Schneider Electric
R. Dunn	DuPont Engineering
J. Gilsinn	NIST/MEL
E. Icahan	ACES Inc
J. Jamison	EnCana Corporation Ltd
D. Kaufman	Honeywell International Inc
K. Lindner	Endress+Hauser Process Solutions AG
V. Maggioli	Feltronics Corp
T. McAviney	Jacobs Engineering
A. McCauley	Chagrin Valley Controls Inc.
G. McFarland	Emerson Process Mgmt Power & Water Sol
R. Reimer	Rockwell Automation
N. Sands	DuPont
H. Sasajima	Yamatake Corp
T. Schnaare	Rosemount Inc
I. Verhappen	Industrial Automation Networks Inc.
R. Webb	ICS Secure LLC
W. Weidman	Consultant
J. Weiss	Applied Control Solutions LLC
M. Widmeyer	Kahler Engineering Inc.
M. Wilkins	Yokogawa IA Global Marketing (USMK)
M. Zielinski	Emerson Process Management

This page intentionally left blank.

Copyright 2009 ISA

CONTENTS

1	Foreword	9
2	Introduction.....	10
3	Scope	10
4	References	11
5	Abbreviations and Acronyms.....	12
6	Safety Lifecycle and Protection Concepts.....	13
7	Example of a Hazard and Risk Analysis Applied to a Single Burner Boiler	32
8	Example of a Hazard and Risk Analysis Applied to a Multi-Burner Process Heater	37
9	Example of a Hazard and Risk Analysis Applied to a Thermal Oxidizer.....	43
10	Example of a Hazard and Risk Analysis Applied to an Oil Heater Treater	47
11	Example of a Hazard and Risk Analysis Applied to a Glycol Reboiler.....	53
12	Example Hazard and Risk Analysis and Verification	59

Copyright International Society of Automation

This page intentionally left blank.

1 Foreword

As a technical report, ISA-TR84.00.05 is provided for information purposes only and is not part of ANSI/ISA-84.00.01-2004 (ref. 4.1)

ISA-TR84.00.05 is intended for reference in applications where it has been determined that ANSI/ISA-84.00.01-2004 applies.

NOTE Throughout this technical report, the term "ANSI/ISA-84.00.01-2004" is used to refer to ANSI/ISA-84.00.01-2004 Parts 1-3 (IEC 61511 Modified).

ANSI/ISA-84.00.01-2004 provides minimum requirements for designing and managing safety instrumented systems (SISs) based on functional and integrity requirements established during a hazard and risk analysis. The specific methods used to conduct the hazard and risk analysis are outside the scope of this technical report. Additional guidance is provided in ANSI/ISA-84.00.01-2004 Part 3 (ref. 4.1) and in *Guidelines for Hazard Evaluation Procedures* (ref. 4.2).

The ISA84 committee determined that it was appropriate to provide supplemental information on the application of hazard and risk analysis to Burner Management Systems (BMS). The purpose of ISA-TR84.00.05 is to provide users of ANSI/ISA-84.00.01-2004 with guidance on how to identify safety functions within the BMS. Safety functions classified as Safety Instrumented Functions (SIFs) should be designed and managed according to ANSI/ISA-84.00.01-2004, as well as other applicable practices. The presented work processes and illustrations are not intended to replace, but instead to supplement, the requirements of good engineering practices applicable to BMS, such as NFPA 85, NFPA 86, API 556, ASME CSD-1, and API RP 14C (see Clause 4).

In jurisdictions where the governing authorities (e.g., national, federal, state, province, county, city) have established process safety design, process safety management, or other requirements, these take precedence over the guidance provided in this technical report.

NOTE The example BMS architectures 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 where 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.

The users of ISA-TR84.00.05 will include:

- Manufacturers of BMSs who are applying the requirements of ANSI/ISA-84.00.01-2004, in addition to other applicable good engineering practices.
- Hazard and Risk Analysis teams identifying and classifying the SIFs within a BMS.
- SIS designers who want an understanding of the safety requirements of BMS.

2 Introduction

In the process industries, many types of instrumented systems are used to maintain a process within normal operating limits. When a process exceeds these limits, protective functions are used to reduce the risk of identified hazardous events associated with safety, environmental, and business consequences. Protective functions are often allocated to instrumented systems, which are designed and managed to achieve or maintain a safe state when a process reaches a prescribed condition.

ANSI/ISA-84.00.01-2004 applies to safety instrumented systems (SISs), which are instrumented systems implemented to prevent an event that results in major consequences and unacceptable lasting effects, usually involving significant harm to humans, substantial damage to the environment, and/or loss of community trust with possible loss of franchise to operate. As companies apply ANSI/ISA-84.00.01-2004 to the design of their process equipment, many want to consistently apply an identification and classification process across a facility.

Fired equipment is found throughout the process industries in many applications, including various types of heaters and boilers. The hazards associated with burner operation are managed by an instrumented system commonly referred to as the burner management system (BMS). The BMS provides interlocks and permissives to prevent misoperation of equipment and to safely handle faults caused by equipment failure. These events potentially result in uncontrolled fires, explosions, or implosions and in the unintended release of the materials being heated. This technical report refers to these functions as BMS functions.

This technical report shows examples of BMS functions required by good engineering practices applicable to BMS, such as NFPA 85 (ref. 4.4), NFPA 86 (ref. 4.5), API 556 (ref. 4.6), ASME CSD-1 (ref. 4.7), and API RP 14C (ref. 4.8). This technical report demonstrates how the work processes of Clauses 8 and 9 of ANSI/ISA-84.00.01-2004 can be applied to establish the functional and integrity requirements of the functions within the BMS. BMS functions should be implemented according to applicable good engineering practices, such as those previously referenced. ISA-TR84.00.05 illustrates how an identification and classification work process can be used to identify SIFs within the BMS.

3 Scope

- 3.1 ISA-TR84.00.05 is strictly informative and does not contain any mandatory requirements.
- 3.2 ISA-TR84.00.05 is intended to be used by those with an understanding of the basic requirements of ANSI/ISA-84.00.01-2004 and other good engineering practices applicable to BMS (references 4.4 to 4.8).
- 3.3 ISA-TR84.00.05 is intended to be used in conjunction with other good engineering practices. This technical report is not intended to stand alone or be a replacement for BMS-specific practices.
- 3.4 This technical report is intended to:
 - a) Identify and classify SIFs within typical BMSs for typical operating modes of fired equipment (e.g., pre-firing, light-off, shutdown, and normal operation);
 - b) Provide examples of typical safety assessments for the following equipment with BMSs: boilers (single burner), fired process heaters (multi-burner), thermal oxidizers, oil heater treaters and glycol reboilers.

4 References

- 4.1 ANSI/ISA-84.00.01-2004 (IEC 61511 Mod), *Functional Safety: Safety Instrumented Systems for the Process Industry Sector*, Parts 1, 2 & 3, ISA, 2004. www.isa.org/standards.
- 4.2 CCPS/AICHE, *Guidelines for Hazard Evaluation Procedures*, Second Edition with Worked Examples, 1992.
- 4.3 ISA-TR84.00.02-2002, *Safety Instrumented Systems (SIS) – Safety Integrity Level (SIL) Evaluation Techniques*, ISA, www.isa.org/standards.
- 4.4 NFPA 85, *Boiler and Combustion Systems Hazards Code*, National Fire Protection Association, 2003.
- 4.5 NFPA 86, *Standards for Ovens and Furnaces*, National Fire Protection Association, 2004.
- 4.6 API RP 556, *Instrumentation, Control and Protective Systems for Fired Heaters and Steam Generators*, 1997.
- 4.7 ASME CSD-1, *Controls and Safety Devices for Automatically Fired Boilers*, American Society of Mechanical Engineers, 2006.
- 4.8 API RP 14C. *Recommended Practice for Analysis, Design, Installation, and Testing of Basic Surface Safety Systems for Offshore Production Platforms*, 2001.

5 Abbreviations and Acronyms

1oo2 – One out of Two Voting
2oo2 - Two out of Two Voting
2oo3 – Two out of Three Voting
AIChE – American Institute of Chemical Engineers
ANSI – American National Standards Institute
API – American Petroleum Institute
API RP– American Petroleum Institute Recommended Practice
BMS – Burner Management System
BPCS – Basic Process Control System
CCPS – Center for Chemical Process Safety
E/E/P E – Electrical/Electronic/Programmable Electronic
HAZOP – Hazards and Operability Study
IEC – International Electrotechnical Commission
IPF – Instrumented Protective Function
IPL – Independent Protection Layer
ISA – International Society of Automation
LEL – Lower Explosion Limit
LOPA – Layers of Protection Analysis
MTTF – Mean Time to Failure
MTTFD - Mean Time to Failure Dangerous
MTTFS – Mean Time To Fail Safe
MTTR – Mean Time to Repair or Restore
NFPA – National Fire Protection Association
OSHA – U.S Occupational Safety and Health Agency
P&ID – Piping and Instrumentation Diagram
PE – Programmable Electronic
PES – Programmable Electronic System
PFD_{avg} – Probability of Failure on Demand Average
PHA – Process Hazards Analysis
PLC – Programmable Logic Controller
SIF – Safety Instrumented Functions
SIL – Safety Integrity Level
SIS – Safety Instrumented Systems

Copyright International Society of Automation

6 Safety Lifecycle and Protection Concepts

6.1 The Safety Lifecycle

6.1.1 Overview

Safety consequences can result from the misoperation of fired equipment during start-up, normal operation, maintenance, and shutdown. A BMS is implemented to prevent misoperation and to safely handle faults caused by equipment failure. Misoperation can be caused by equipment failure or improper firing and can potentially result in uncontrolled fires, explosions, or implosions and in the unintended release of the materials being heated. Consequently, the hazard and risk analysis for the fired equipment often focuses on events that lead to hydrocarbon fuels being introduced into the equipment under abnormal operating conditions.

The ANSI/ISA-84.00.01-2004 Safety Lifecycle addresses SISs used to prevent unacceptable hazardous events, generally involving harm to people and/or damage to the environment. The lifecycle is supported by a management system that focuses on reducing the potential for SIS failure through effective SIS design and management. The Safety Lifecycle includes steps for:

- Identifying the hazardous events resulting in unacceptable consequences
- Identifying the safety functions that prevent hazardous events
- Establishing the performance criteria (e.g., the risk reduction) for these safety functions
- Allocating safety functions to systems designed and managed to achieve the performance criteria
- Documenting the functional and integrity requirements in a design specification
- Verifying that the design and management practices are sufficient to meet the performance requirements
- Documenting and implementing operation and maintenance procedures to support performance requirements
- Managing changes to the process equipment and its safety systems to ensure safe operation

Many types of fired equipment are subject to application-specific good engineering practices. The hazard and risk analysis described in ANSI/ISA-84.00.01-2004 can be used to classify these already identified BMS functions. The BMS design should meet the intent of any applicable good engineering practice, regardless of the perceived risk. This technical report demonstrates how ANSI/ISA-84.00.01-2004 complements other good engineering practices, allowing the owner/operator to define the requirements for each instrumented system consistent with methods used for other process equipment. ANSI/ISA-84.00.01-2004 work processes can also be used to determine whether planned BMS design and management practices are sufficient to provide the required risk reduction for identified hazardous events.

This technical report addresses various aspects of the Safety Lifecycle and its application to BMS. While this technical report provides examples of hazardous events, it does not illustrate all of the hazardous events possible with the referenced equipment. Hazardous event identification can be accomplished through a variety of methods ranging from checklists based on prior design and experience to formal, structured techniques, such as Hazard and Operability Studies (HAZOP) and What If?/checklists. The choice of method is not specific to BMS. More information on the hazard identification can be found in *Guidelines for Hazard Evaluation Procedures* (Reference 4.2).

6.1.2 Safety Instrumented Functions

An SIS may implement one or more SIFs to address unacceptable hazardous events associated with process equipment operation. The starting point for this technical report is a description of the measurements and actions taken by various BMS functions required by applicable practices. The reader is cautioned that identification of an individual SIF within an SIS may seem simple, but many errors are common, such as:

- Not including all of the process measurements that can detect the hazardous condition
- Including actions that are not required to achieve or maintain a safe state
- Including measurements that do not detect the hazardous condition

The risk analysis is further complicated when multiple initiating causes can result in a hazardous event, but not all initiating causes are detected by the same process measurement. In this case, multiple SIF may be defined, each of which provide risk reduction against a set or subset of the initiating events that can cause the hazard. When selecting the risk reduction and the associated SIL for these SIF, the aggregation effect of the multiple SIFs protecting against the same hazardous event should be considered. In many cases, the lack of independence between the SIFs necessitates the consideration of the functions as a single function with diverse process measurements.

6.1.3 Safety Integrity Level

When a BMS function is classified as an SIS, the risk reduction allocated to the BMS function is related to its SIL. The required risk reduction can be defined using qualitative, semi-quantitative or quantitative risk analysis techniques. All techniques rely on process hazards analysis to identify hazardous events. The primary difference between the techniques is the different degrees of rigor employed to estimate the event likelihood (or frequency) and consequence severity.

Various hazard and risk analysis techniques are discussed in *Guidelines for Hazard Evaluation Procedures* (ref. 4.2). While all techniques follow the same general steps, there is much variability in the detail and degree of resolution between different owner/operators that apply ANSI/ISA-84.00.01-2004. This report does not endorse a specific methodology for performing risk analysis. The CCPS concept book *Layers of Protection Analysis: A Simplified Risk Assessment* discusses a semi-quantitative risk analysis technique, which uses order-of-magnitude bands to assess the event likelihood.

The risk analysis process can be summarized as:

- 1) Identify the hazardous event (e.g., the event that the SIF under consideration is preventing).
- 2) Estimate consequence severity of the hazardous event.
- 3) Estimate likelihood (or frequency) of the hazardous event, considering all credible initiating causes.
- 4) Assess the process risk of the hazardous event as a function of its consequence severity and likelihood (or frequency).
- 5) Compare process risk to the risk criteria to determine the risk reduction requirements.
- 6) Identify safety functions required to achieve the risk reduction requirements.
- 7) Assign an SIL to the SIF that meets the risk reduction requirements.

ANSI/ISA-84.00.01-2004 defines four discrete levels of SIL. Each SIL is an order of magnitude range of values associated with the probability that the SIS will perform its required function under all stated conditions within a specified time period. The risk reduction factor is defined in Table 6.1 as $1/PFD_{avg}$.

Table 6.1 – SIL Categories

Safety Integrity Level (SIL)	Average Probability of Failure on Demand (PFD_{avg})	Risk Reduction Factor
4	10^{-4} to 10^{-5}	10,000 to 100,000
3	10^{-3} to 10^{-4}	1,000 to 10,000
2	10^{-2} to 10^{-3}	100 to 1,000
1	10^{-1} to 10^{-2}	10 to 100

Step 1. Identify Hazardous Event

Identifying the hazardous event is a critical step in the risk analysis process. Errors in this step may result in an SIF design basis that does not adequately address the process risk. Hazardous events should be identified using a process hazards analysis as discussed previously. This technical report provides examples of the application of the risk analysis process to identified hazardous events. The reader is cautioned that these examples are not comprehensive and should not be considered a substitute for performing an analysis on similar fired equipment.

Step 2. Estimate Consequence severity

The consequence severity is typically estimated qualitatively. While consequence models employing explosion, fire, and population density calculations are possible, they are rarely used for BMS assessments. While risk analysis techniques are often focused on an evaluation of safety impacts, many owner/operators consider environmental and business impacts.

Step 3. Estimate Likelihood (or frequency)

Likelihood (or frequency) is estimated qualitatively, semi-quantitatively, or quantitatively. Many owner/operators use order-of-magnitude estimates for the event likelihood, e.g., once per year, once in 10 years, etc. The likelihood should be assessed without considering the presence of any protection layers, e.g., instrumented systems and pressure relief devices. This yields the unmitigated likelihood of the hazardous event.

Step 4. Assess Process Risk

The process risk is a function of the estimated consequence severity (step 2) and unmitigated likelihood (Step 3) of the identified hazardous event.

Step 5. Compare Process Risk Against Risk Criteria

Many owner/operators represent their risk criteria as a risk matrix where event likelihood and consequence severity are the two axes. The required risk reduction is provided as a function of the event likelihood and consequence severity. The process risk is used to determine the required risk reduction for the specific consequence-likelihood pair.

Some owner/operators use quantitative risk metrics, such as the individual risk of fatality or the risk to the maximum-exposed individual (or societal risk criteria). In these cases, a numerical estimation of the frequency of the hazardous event is compared to the risk criteria relevant for the specified consequence severity.

When the process risk exceeds the risk criteria, safety functions are identified that reduce the process risk to the risk criteria.

Step 6. Identify safety functions required to achieve the risk reduction requirements.

Safety functions are implemented to achieve or maintain a safe state in response to a specified hazardous event. The safety functions are allocated risk reduction as required to reduce the residual risk below the risk criteria. Finally, the safety functions are allocated to protection layers that are designed and managed to achieve the required functionality and risk reduction.

Step 7. Assign an SIL to the SIF that achieves the risk reduction requirements.

Those safety functions allocated to the SIS layer are SIFs. The risk reduction allocated to an SIF is related to its SIL as shown in Table 6.1.

6.2 Safety Integrity Level Verification

The Safety Lifecycle, as defined in ANSI/ISA-84.00.01-2004, requires the verification of the SIL of each SIF using quantitative analysis of the average probability of failure on demand. This calculation should consider the failure characteristics of each SIF device, the SIF architecture, and the SIF proof test interval. These calculations can be performed using the techniques described in ISA-TR84.00.02, *Safety Instrumented Systems (SIS) Safety Integrity Level (SIL) Evaluation Techniques*. Examples of the evaluation of a BMS function are presented in clause 12 of this technical report.

6.3 Operating Modes, Undesirable Events and SIF

The various operating modes of the fired equipment should be considered during the analysis. Each operating mode may require specific protective layers. The operating modes, undesirable events and safety functions discussed in this section are based on a review of the existing BMS good engineering practices. Again, the reader is cautioned that these examples should not be considered a substitute for an analysis of a specific piece of fired equipment. There may be situations or complexities that pose process hazards with unacceptable consequences that are not discussed in this technical report, e.g., fuel rich conditions due to use of staged LoNox burners or flue gas recirculation. It is the responsibility of the owner/operator to identify hazardous events pertaining to fired equipment operation.

NOTE This section covers a variety of fired equipment including boilers, process heaters, thermal oxidizers, and ovens. The undesirable events and SIFs covered below may not be applicable to all types of fired equipment. End users need to identify which are applicable to their specific applications and corporate/local requirements.

6.3.1 Pre-firing cycle

The pre-firing cycle prepares the fired equipment for the introduction of fuel and light-off of the burners. The pre-firing cycle includes prevention of fuel entering the firing chamber and purging of the chamber to remove any residual hydrocarbon that may be present.

6.3.1.1 Excess Combustibles in the Firing Chamber

Misoperation of the fired equipment can result in an excessive amount of unburned fuel being introduced to the firing chamber. If this fuel mixes with air in a flammable proportion and finds a source of ignition, it may ignite. Ignition of a flammable mixture in the firing chamber may result in a fire that may propagate into an explosion (deflagration) that could damage equipment and injure personnel in the area of the explosion.

6.3.1.1.1 Fuel Valves Improperly Aligned (Permissive)

To ensure a sufficiently fuel-free environment in the firing chamber, it is necessary to verify that the valves are lined up such that fuel is not being introduced to the firing chamber. If the fuel valves were improperly aligned, fuel is introduced into the firing chamber during the purge period, making the purge ineffective. A successful purge requires that the valves remain in the closed position during the purge and an adequate purge rate be sustained for a specified period of time.

The hazardous condition is detected by monitoring position switches on the fuel valves. If the valves are determined to be in the wrong position, the startup sequence is stopped and fuel introduction is prevented. While this functionality is considered good engineering practice, it is rarely considered an SIF. Failure of the fuel valves to reach the closed position when required should be detected and annunciated, because a valve failure could allow a hazardous condition to continue to exist after shutdown or during later re-start activities.

6.3.1.1.2 Accumulation of Flammable Materials and Failure to Purge (Permissive)

Prior to ignition, any accumulation of unburned hydrocarbons needs to be removed to ensure that introduction of an ignition source(s) will not cause an undesired fire or explosion of the accumulated fuel. To prevent this consequence, the heater firebox is purged by operating the air fans for a pre-determined period of time.

The air flow measurement device varies from application to application, but is typically some combination of one or more of the following: (1) differential pressure measurement across the fan, (2) pressure measurement at the outlet of the fan, (3) flow measurement device (such as a pitot tube), or (4) fan motor running indication using motor contacts / speed probes and pressure indication. Each of these measurement types has benefits and limitations, and decisions regarding the measurement type should consider the specific application under consideration. In general, more direct measurement, such as actual flow rate, is superior to indirect means of measurement, such as motor running contacts, as there are a number of failure modes that may result in the indirect measurement giving a false positive indication of flow. For instance, if a fan shaft decoupled from its motor, the motor running contact indicates that the motor is running, but air is not actually flowing. Alternatively, motor amps could be used to indicate that the fan motor is running and has a load. The benefits and limitations of the various measurement devices are considered during the SIL verification, where the probability of failure on demand is calculated. Inferior measurements will result in higher probabilities of failure on demand and thus lower achieved SIL levels.

The timer functionality will either be supplied by a time delay relay or in the programming of a programmable electronic system. The appropriate timer settings for purging are established in the BMS practices (refer to clause 4 for a listing).

Measuring a proper purge is straightforward in a forced, induced, or balanced draft heater. Ensuring a proper purge in a natural draft heater is less direct, but still important. There are a number of methods that are commonly used in the process industries.

- 1) Use an external purge medium, such as steam, plant air, or instrument air, for a predefined period of time. If this method is chosen, either the flow of the medium is measured and used as an input to the permissive function, or the medium is confirmed to be flowing by inspection (audible and/or visual evidence) and only the timer is used in the automatic function.
- 2) Allowing the natural draft occurring through the heater to purge the firebox. If this method is chosen, some feedback, via limit switches, can be used to confirm the existence of flow in combination with the purge timer.

NOTE If no positive automatic means is used to ensure the firebox has been purged prior to light off, some consideration for manual testing of the concentration of combustibles in the firebox, via combustible gas detectors, should be considered.

The risk posed by failure to purge a heater firebox is significant and has resulted in a number of fired equipment accidents. While not always classified as an SIF, depending on hazards associated with burner light-off, this functionality is often considered safety-related and is reviewed for risk reduction requirements.

6.3.1.2 Proceeding to the Light-Off cycle when the permissives are not satisfied

6.3.1.2.1 Flame Detector Indicating Premature Presence of Flame (Permissive)

To ensure a fuel-free firing chamber prior to introduction of fuel gas and ignition, all sources of fuel must be stopped. If a flame were present at the burner prior to a planned light-off sequence, it would indicate that fuel is being introduced to the heater and is being burned at the burner tip. While this scenario is not likely to occur, if it did, it would result in an ineffective purge that might result in accumulated unburned fuel in the firing chamber prior to light-off. This fuel might then be ignited, causing a fire or explosion.

In this case, the flame detectors at the burners detect the hazardous condition. If a flame is detected, the startup sequence is stopped and introduction of fuel and ignition is prevented.

While this functionality is considered good engineering practice, it is rarely classified as an SIF as it is considered sufficiently unlikely. Premature presence of a flame either indicates failure of the flame detector in a dangerous state or that fuel is being introduced to the heater and combustion is occurring without the knowledge or direction of operations staff. This could also indicate the presence of an oil pool fire or leaking fuel valves that fail to fully extinguish the burner flames. It is very unlikely that after a successful shutdown that fuel could be re-introduced to the heater and ignite at the burner without the direct involvement of operations staff. As a result, this functionality is typically treated as a diagnostic of the proper operation of the flame detectors rather than an indication that a hazardous condition exists.

6.3.1.2.2 Low Fuel Gas Pressure (Permissive)

After purging, but before light-off, a heater's fuel systems typically at the header upstream of the control valve are checked to ensure that they are prepared for introduction of fuel into the purged heater. This preparation includes verification that the fuel gas pressure is sufficiently high to support combustion. If fuel gas pressure were not high enough to support combustion it is possible that fuel gas could be introduced to the firebox that would not be ignited at the burner. This fuel gas could then subsequently accumulate in the firebox, find a source of ignition and cause an undesired fire or explosion.

Measuring the pressure of fuel gas in the main header detects the hazardous condition. If a hazardous condition is detected, the startup sequence is stopped and introduction of more fuel and ignition is prevented.

While this functionality is considered good engineering practice, it is rarely classified as an SIF. While there are safety consequences that might result from low pressure conditions in the fuel gas header prior to light-off, detection of the hazards posed by this scenario are more directly detected by the "Igniter Flame Not Proven" and "Main Flame Not Proven" as described in clauses 6.3.2.1.1 and 6.3.2.1.2. As a result, these pre-light off functions are typically considered an operational convenience than an SIF.

6.3.1.2.3 High Fuel Gas Pressure (Permissive)

After purging, but before light-off, a heater's fuel systems are typically checked to ensure that they are prepared for introduction of fuel into the purged heater. This preparation includes verification that the fuel gas pressure is sufficiently low so that the velocity of the fuel gas leaving the burner tips is not so high that it will prevent ignition from occurring. If fuel gas pressure were too high to allow combustion it is

possible that fuel gas could be introduced to the firebox that would not be ignited at the burner. This fuel gas could then subsequently accumulate in the firebox, find a source of ignition and cause an undesired fire or explosion.

Measuring the pressure of fuel gas in the main header detects the hazardous condition. If a hazardous condition is detected, the startup sequence is stopped and introduction of more fuel and ignition is prevented.

While this functionality is considered good engineering practice, it is rarely classified as an SIF. While there are safety consequences that might result from high pressure conditions in the fuel gas header prior to light-off, detection of the hazards posed by this scenario are more directly detected by the "Igniter Flame Not Proven" and "Main Flame Not Proven" as described in clauses 6.3.2.1.1 and 6.3.2.1.2. As a result, these functions are typically considered to be more of an operational convenience than an SIF. However, each situation must be analyzed individually. For example, there could be a situation where light-off is a manual operation. In this situation, the operator may be exposed to a flash fire.

6.3.1.2.4 Valves Not in Minimum Firing Position (Permissive)

To successfully light the heater, the fuel and air valves should be in their proper firing positions (sometimes referred to as minimum firing positions). If the valves are not in a position where they will generate a fuel/air mixture appropriate for combustion, ignition might not occur upon introduction of fuel. The un-ignited fuel gas could then subsequently accumulate in the firebox, find a source of ignition and cause an undesired fire or explosion.

In this case, the limit switches at the valves detect the hazardous condition. In some heater configurations, special-purpose valves are used that have specified positions with associated limit switches for minimum firing. In other applications minimum firing is set by use of a pressure regulator that bypasses the fuel control valve. In this case, the minimum firing is proven by ensuring the fuel control valve is confirmed closed and all fuel is entering the system through the bypass regulator. If the valves are not proven to be in the correct position, the startup sequence is stopped and introduction of fuel and ignition is prevented.

While this functionality is considered good engineering practice, it is rarely classified as an SIF. While there are safety consequences that might result from valve misalignment in the fuel/air system prior to light-off, detection of the hazards posed by this scenario are more directly detected by the "Igniter Flame Not Proven" and "Main Flame Not Proven" as described in clauses 6.3.2.1.1 and 6.3.2.1.2. As a result, these functions are typically considered to be more of an operational convenience than an SIF.

6.3.1.2.5 Burner Header Fuel Gas Does Not Hold Pressure (Permissive)

Prior to lighting a multiple burner fired heater, all of the block valves for the main gas at the individual burners must be closed. If one or more of the individual block valves are left in the open position, then when fuel gas is allowed into the main gas header, gas will be allowed to flow out into one or more burners whose pilots are not lit. The un-ignited fuel gas could then subsequently accumulate in the firebox, find a source of ignition and cause an undesired fire or explosion.

In this case, a hazardous condition is detected by a pressure measurement in the main gas header after the pressure control valve but before the split to the individual burners. Prior to lighting, the main fuel gas header will have its pressure increased to a normal operational level either by temporarily opening the main fuel gas block valves or by introducing nitrogen from a separate source. If all of the individual block valves are closed then the pressure in the header will increase above the permissive point and the start-up process is allowed to proceed. If the pressure set point is not achieved after a suitable period of time, the startup sequence is stopped and the valves introducing gas into the header (i.e., either the main fuel gas shutoff valves or the nitrogen addition valve) are closed. It is important to note that if this permissive is successful when nitrogen is used to pressure the header, then time should be allowed during the

lighting process to allow the nitrogen that is contained in the header to be purged out, allowing the fuel gas to arrive at the burner.

This functionality is considered good engineering practice and is especially beneficial in multiple burner fired equipment. This permissive will reveal failures that could result in a significant safety consequence. As a result, this function is typically analyzed for risk reduction requirements

6.3.1.2.6 Steam Drum Level Not Established or Failure of Drum Level Measurement (permissive)

To ensure safe operation of the steam drum after the boiler is fired, the level of the steam drum shall be measured and the level of water in the steam drum should be established at the desired range before light-off of the burners. Higher level may result in water carryover to downstream equipment, such as a steam turbine, possibly causing damage. Lower level may result in dry boiler tubes which reach their temperature design limit leading to tube rupture and injury of personnel.

To proceed with burner light-off, appropriate steam drum level should be proven.

6.3.2 Light-off Cycle

The objective of the light-off cycle is to safely introduce fuel to the burner and ignite it. After ignition is attempted, existence of a stable flame is proven prior to moving to the normal operation mode. If a proven stable flame is not achieved in this phase, the light-off sequence will be stopped and the fired equipment will return to the pre-firing sequence.

6.3.2.1 Excess Combustibles in the Firing Chamber

Misoperation of the fired equipment can result in an excessive amount of unburned fuel being introduced to the firing chamber. If this fuel mixes with air in a flammable proportion and finds a source of ignition it may ignite. Ignition of a flammable mixture in the firing chamber will result in a fire that may propagate into an explosion (deflagration) that could damage equipment and injure personnel in the area of the explosion.

6.3.2.1.1 Igniter Flame Not Proven Within a Specified Time (Trip)

If igniter flame ignition does not occur, continued introduction of fuel gas into the firing chamber could result in accumulation of a flammable mixture. Failure to ignite could occur for a number of reasons, including: ignition transformer failure, ignition valve failure, plugged pilot nozzle, pilot gas contamination, improper fuel air ratio, etc. The accumulated mixture can result in a fire or explosion if a source of ignition in the firing chamber or vent stack is encountered.

In this case, detection of igniter flame is performed using a flame detector at the burner in combination with a time delay device. The timer functionality will either be supplied by a time delay relay or in the programming of a programmable electronic system. If no flame is detected within a set time period, the valve supplying fuel gas to the igniter is closed.

The risk posed by failure of the time delay device could be significant if the fuel fails to ignite.

While not always identified as an SIF, this functionality is typically deemed safety-related and should be reviewed for risk reduction requirements.

6.3.2.1.2 Main Flame Not Proven Within a Specified Time (Trip)

If main flame ignition does not occur then continued introduction of fuel gas into the firing chamber could result in accumulation of a flammable mixture, since the fuel is not being consumed. This accumulated mixture can result in a fire or explosion if a source of ignition in the firing chamber or vent stack is encountered.

In this case, detection of main flame is performed using a flame detector at the burner in combination with a time delay device. The timer functionality will either be supplied by a time delay relay or in the programming of a programmable electronic system. If no flame is detected within a set time period, the valve supplying fuel gas to the main burner is closed.

The risk posed by failure of the time delay device could be significant if the fuel fails to ignite.

While not always identified as an SIF, this functionality is typically deemed safety-related and should be reviewed for risk reduction requirements.

6.3.3 Normal Operation

The normal operation phase of fired equipment occurs when a stable proven flame is used for process heating purpose. In this phase conditions that ensure stable operation of the flame are monitored to detect any deviations that might compromise the flame. If these conditions are detected various degrees of action may be taken to bring the process to a safe state.

6.3.3.1 Excess Combustibles in the Firing Chamber

Misoperation of the fired equipment can result in an excessive amount of unburned fuel being introduced to the firing chamber. If this fuel mixes with air in a flammable proportion and finds a source of ignition it may ignite. Ignition of a flammable mixture in the firing chamber will result in a fire that may propagate into an explosion (deflagration) that could damage equipment and injure any personnel in the area of the explosion.

6.3.3.1.1 High Fuel Gas Pressure (Trip)

High fuel gas pressure can result in loss of flame and introduction of fuel gas into the firing chamber without a flame available to ensure that ignition will occur at the burner. High fuel gas pressure typically occurs as the result of failure of pressure control. This failure results in an uncontrolled high pressure at the burner. If the pressure is sufficiently high, the rate of flow through the burner will be so great that the flame will be lifted off the burner and extinguished. After the flame is extinguished, a high rate of unburned fuel gas will continue into the firebox unless the fuel gas flow is stopped.

In this case, the hazardous condition can be detected either by the high fuel gas pressure that precedes the actual loss of flame or by the flame detector detecting that the flame has been extinguished. If both of these measurements are available to detect the hazardous condition, the measurements can be voted 1oo2, since either sensor can detect the hazardous condition. Detection of this condition will result in a Master Fuel Trip or Individual Burner Valve Trip depending upon system configuration.

The risk posed by high fuel gas pressure leading to complete loss of flame and/or incomplete combustion leading to secondary ignition can be significant. Continuous pilots may not be considered a layer of protection in all applications. It is possible that there could be a fuel rich (or air starved) condition that would not permit complete combustion resulting in a hazard, if air is re-introduced or the fuel rich mixture reaches an oxygen source (near top of stack).

6.3.3.1.2 Low Fuel Gas Pressure (Trip)

Low fuel gas pressure can result in loss of flame and subsequent re-introduction of fuel gas into the firing chamber without a flame available to ensure that ignition will occur at the burner. Low fuel gas pressure typically occurs as the result of loss of fuel gas supply from the external source of fuel or failure of the fuel gas control system. This failure will result in a fuel pressure at the burner tip that is not sufficient to support combustion. This may result in loss of flame with continued addition of fuel gas.

In this case, the hazardous condition can be detected either by the low fuel gas pressure that precedes the actual loss of flame, or by a flame detector detecting that the flame has been extinguished. If both of