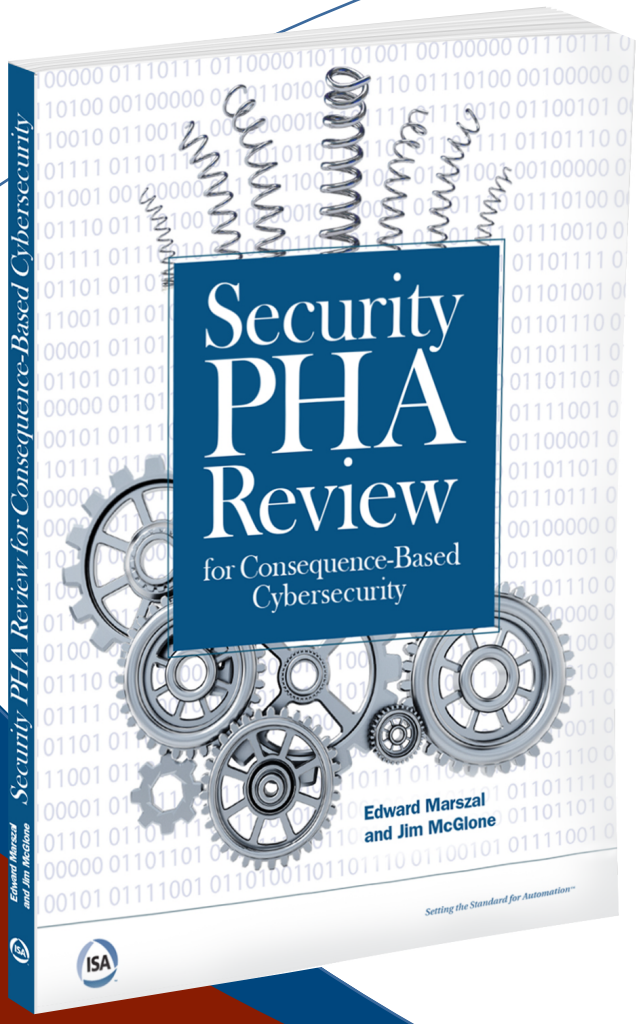
ISA

Standards
Certification
Education & Training
Publishing
Conferences & Exhibits



eBook available!

Table of Contents

View Excerpt

Buy the Book

Setting the Standard for Automation™

Security PHA Review for Consequence-Based Cybersecurity

By Edward M. Marszal and Jim McGlone

Notice

The information presented in this publication is for the general education of the reader. Because neither the author nor the publisher has any control over the use of the information by the reader, both the author and the publisher disclaim any and all liability of any kind arising out of such use. The reader is expected to exercise sound professional judgment in using any of the information presented in a particular application.

Additionally, neither the author nor the publisher has investigated or considered the effect of any patents on the ability of the reader to use any of the information in a particular application. The reader is responsible for reviewing any possible patents that may affect any particular use of the information presented.

Any references to commercial products in the work are cited as examples only. Neither the author nor the publisher endorses any referenced commercial product. Any trademarks or tradenames referenced belong to the respective owner of the mark or name. Neither the author nor the publisher makes any representation regarding the availability of any referenced commercial product at any time. The manufacturer's instructions on the use of any commercial product must be followed at all times, even if in conflict with the information in this publication.

Printed in the United States of America.
Version: 1.0

ISBN-13: 978-1-64331-000-8 (Paperback)
ISBN-13: 978-1-64331-002-2 (EPUB)
ISBN-13: 978-1-64331-001-5 (MOBI)

ISA
67 T. W. Alexander Drive
P.O. Box 12277
Research Triangle Park, NC 27709

Library of Congress Cataloging-in-Publication Data in process

Copyrighted Material

Contents

About the Authors

Edward M. Marszal

Edward M. Marszal, Professional Engineer (PE) and ISA84 Safety Instrumented Systems Expert, is the president and chief executive officer of Kenexis. Kenexis is an engineering consultancy dedicated to assisting process industry customers with assessing the risks that are posed by their plant operations and then reducing those risks to a tolerable level by the specification of instrumented safeguards, such as safety instrumented systems (SISs), fire and gas systems (FGSs), critical alarm systems, and cybersecurity. Marszal is a longtime practitioner and pioneer of the techniques and tools associated with technical safety and the performance-based design and implementation of instrumented safeguards.

Marszal started his career after receiving a BA in chemical engineering, with an emphasis on process controls and artificial intelligence, from The Ohio State University. After graduating, Marszal took a position with UOP in Des Plaines, Illinois where he worked as an instrumentation and control field advisor, performing functional safety assessments of control systems and safety instrumented systems at customer sites worldwide. At UOP, he designed and managed the development of custom control systems and SIS projects.

After leaving UOP, Marszal joined Environmental Resources Management (ERM) in their business risk solutions consulting group. In this position, he specialized in financial risk analysis and process safety management. He performed and managed risk assessment projects that involved quantitative risk analysis, including preparation

of Environmental Protection Agency (EPA) Risk Management Plans with off-site consequence analysis for over 100 facilities. Companies used his recommendations from these projects to ensure regulatory compliance, justify risk reduction expenditures, and optimize insurance coverage.

Marszal then co-founded and joined exida. At exida, Marszal was responsible for helping users and vendors of industrial automation systems develop safety critical and high-availability solutions. Marszal performed numerous SIS safety life-cycle projects that included process hazard analysis (PHA) facilitation, Layer of Protection Analysis (LOPA) facilitation, safety integrity level selection, safety requirements specification development, start-up acceptance testing assistance (validation), and function test plan development.

After leaving exida, Marszal joined Kevin Mitchell in the founding of Kenexis, where he is still employed today. Kenexis was founded to assist process industry users implement instrumented safeguards.

Marszal has been active in professional societies, an active instructor, and a prolific author throughout his entire career. Marszal joined the ISA84 committee for the development of standards and technical reports in 1994 and has been an active participant since then. Marszal has been involved in all aspects of the committee's work but has been instrumental in leading several technical report efforts, including ISA84 Working Group 7 that issued technical guidance on performance-based determination of fire and gas detection requirements.

Marszal is the author of record for ISA's EC52 Advanced Safety Integrity Level (SIL) Selection training course, which he presents several times per year in combination with ISA's EC54 Advanced Design and SIL Verification course. He is also the author of the award-winning ISA textbook *Systematic Safety Integrity Level Selection with Layer of Protection Analysis*, which is the accompaniment to the EC52 training class. Additionally, Marszal is the co-developer and frequent presenter of ISA EC56P Fire and Gas System Engineering: Performance-Based Methods for Process Facilities. In addition to providing ISA training, Marszal also presents a large amount of Kenexis' training offerings, which cover a range of instrumented safeguard topics.

James McGlone

James McGlone is the chief marketing officer of Kenexis. McGlone has more than 30 years of experience in the development and deployment of many of the embedded

control systems used in industrial automation, building automation, Internet of Things (IoT), and cybersecurity.

McGlone started his career in the US Navy as an electronics technician and nuclear reactor operator on fast attack submarines. McGlone was on the pre-commissioning crew of two submarines during construction and shakedown, eventually taking the boats to sea as operational platforms. While in the Navy, McGlone acquired computers and began programming in various languages including BASIC, COBOL, and FORTRAN. After 9 years of maintaining and operating nuclear power plants in submarines, McGlone decided to pursue a civilian career as a technical specialist for a Rockwell Automation (Allen-Bradley) distributor in Akron, Ohio where he solved challenging applications for drives and motion control systems and learned to program programmable logic controllers (PLCs).

After 5 years as a technical specialist, McGlone's interest in computers grew and he realized that the computer was likely to replace the large operator panels that were being built with hardware such as switches and pilot lights. McGlone ended up with ICOM in Milwaukee, Wisconsin promoting, selling, and supporting industrial software on DOS and Windows 3.0 era machines. ICOM was acquired by Rockwell Automation and McGlone pursued a variety of positions promoting and driving the development of industrial software to solve industrial automation problems worldwide.

After 15 years, McGlone left to become the vice president of Tridium, a Honeywell subsidiary in Richmond, Virginia where he ran sales and operations. Tridium supplied technology that other vendors deployed under their own brands. This technology included nondeterministic embedded programmable controllers, which were similar to deterministic PLCs but most of the inputs and outputs were remote over network connections throughout buildings. This technology intrigued McGlone, who pursued other vendors to deploy it in new and unique ways, including what is commonly referred to as the Internet of Things (IoT) today.

After Tridium, McGlone moved back into the industrial software business only to discover that his passion had shifted, and he needed to solve problems on another scale. McGlone moved on to bring high-speed inline encryption technology from government applications into the industrial marketplace when he was introduced to Kenexis.

At Kenexis, McGlone promotes and deploys the disciplines necessary to build and operate process systems safely with secure industrial control systems.

In addition to many years of industrial control system design and programming experience, McGlone has served as the ISA Safety & Security Division Director and is a past president of central Ohio's Control System Cyber Security Association International. McGlone is a graduate of the University of New York. McGlone holds an MBA and a BS in physics and computer systems, several Microsoft certifications, and a Global Industrial Cyber Security Professional (GICSP) certificate.

1 Introduction

Process industry plants are hazardous. Managing the risk associated with these hazards and ensuring that the risk is below a tolerable level is a difficult and resource-intensive activity. As technology evolves, process plants employ new equipment and techniques to reduce costs and improve productivity. And as the new equipment and techniques are employed, new and different hazard scenarios are developed that must be considered during design and addressed with appropriate safeguarding if the hazards are significant enough.

Over the course of the past few decades, the process industries have almost entirely shifted from control systems that were either electronic or pneumatic to programmable electronic systems (PESs). PESs include distributed control systems (DCSs) and programmable logic controllers (PLCs). These systems are computer based, which allowed great leaps in function over their analog counterparts. The advantage of using computer-based systems is that more complex calculations could be performed quickly, improving process control and optimization. Additionally, information about the process operation could be stored and communicated throughout the organization, facilitating a wide variety of operational, management, and maintenance activities.

At the time of writing, most process industry plants have not performed much cybersecurity work on their industrial control systems (ICSs) beyond relying on their information technology (IT) departments to carry out some basic perimeter guarding. Even so, physical damage to controlled processes from known cybersecurity events remains limited. It is true that the number of cyberattacks is increasing and that some have created substantial loss for organizations by disrupting service or business, but the

actual physical damage is minimal so far. In a few cases where damage was possible, operator awareness of system behavior prevented physical damage. Considering the frequency of attacks, this fact is surprising to those who do not fully understand how process plants are designed and safeguarded. Why have we not seen more impact from cyberattacks on ICSs? The answer lies in the way process engineers have designed their plants to be safeguarded against failures that can cause significant safety consequences, and this is true whether the failure occurs organically through random hardware failures or deliberately through cyberattack. The safeguards employed by these process engineers are common, inexpensive, and very often inherently safe against cyberattack because most of these devices were invented long before the advent of the computer.

While the advantages of this computational power and open communication are obvious, unfortunately, they also introduce new potential hazard scenarios that never existed in the analog-only days. The new hazard scenarios generated from inherent failure modes in the new equipment were appropriately addressed by existing process hazard analysis (PHA) methods. Other new hazard scenarios are not adequately addressed by existing PHA techniques—at least not without extending those methods to address the new threats. These new threats are not adequately addressed by existing PHA methods because instead of being random equipment failures, they are the deliberate acts of people.

Even though these new threats are not appropriately assessed with existing PHA methods, there is no reason to abandon what we know about process risk assessment. This book presents methods, which are already being adopted in industry, to extend tried and true methodologies for PHA to address the problem of deliberate cyberattack. By doing so, none of the existing PHA effort is wasted, and effort is not needlessly duplicated. Instead, a traditional PHA is used with a focus on cyberattack scenarios that would prevent safeguards from operating properly. These key scenarios will generate recommendations to implement safeguards that are inherently safe against cyberattack, or they will determine the appropriate level of cyber safeguarding, as defined by a security level (SL).

An SL represents the amount of mitigation of cyberattack risk necessary in an ICS. Unlike safety integrity levels (SILs) of safety instrumented functions (SIFs), which are quantitative measures of probability of failure on demand, SLs are qualitative measures and techniques that are employed on ICSs and networks to prevent unauthorized use and access. To select the SL, organizations should consider the potential consequences of threat vectors that could cause loss-of-containment accidents in process plants by manipulating process control equipment that causes events and prevents existing safeguards from properly operating. Implementing cybersecurity safeguards and selecting an

appropriate SL must involve the consideration of relevant laws, regulations, and national and international standards. Around the world, legislative and regulatory bodies are preparing requirements for process industry plants to safeguard their critical infrastructure against malicious attack, such as the Chemical Facility Anti-Terrorism Standards (CFATS) from the US Department of Homeland Security. Subsequently, industry groups have prepared more detailed guidelines to support practitioners in their area of expertise to meet the broad requirements of these regulations. On September 11, 2001, the International Society of Automation (ISA) had its initial planning meeting to form an ISA Standards Panel (SP) on cybersecurity for ICSs. In October 2002, the ISA99 committee held its first face-to-face meeting. Shortly thereafter, ISA99 released its first in a series of standards that defined the terminology, concepts, models, processes and procedures, and technical requirements for cybersecurity. To promote the standards internationally, ISA99 partnered with the International Electrotechnical Commission (IEC). The standards are now published both by ISA and IEC as the ISA/IEC 62443 Series, *Security for Industrial Automation and Control Systems*.

The ISA/IEC 62443 Series uses the concept of a *security-level life cycle* as a tool for managing the implementation of cybersecurity. An integral part of the security life cycle is the selection of a metric for defining the relative degree of rigor with which cyber safeguards will be applied as a function of the amount of risk associated with the operation of a process plant. Specifically, the risk is associated with a section of the plant controlled by a grouping of industrial control equipment referred to in the standard as a *zone*. The ISA/IEC 62443 Series requires the selection of an SL for each ICS zone (and its associated conduits). Because the ISA/IEC 62443 Series is the basis for many operating companies' processes and procedures for ensuring safe and secure plant operation, it is often considered a recognized and generally accepted good engineering practice (RAGAGEP). The RAGEGEP is used for ensuring the mechanical integrity of process equipment as required by the Occupational Safety and Health Administration (OSHA) through the process safety management (PSM) Regulation (29 CFR 1910.119, *Process Safety Management of Highly Hazardous Chemicals—Compliance Guidelines and Enforcement Procedures*).

Brief History of Cyberattacks on ICSs

For years, industry pundits have warned about the massive physical damage and loss of life that could occur as the result of cyberattacks. In the United States, government agencies have even prepared case studies demonstrating that cyberattacks can cause physical damage to process plants. The most famous of these cases was the "Aurora" test staged by the US Department of Homeland Security, the results of which were widely reported by international news outlets like CNN.

2

Overview of the ISA/IEC 62443 Series

The ISA/IEC 62443 Series is a collection of standards and supporting technical reports. These documents are interrelated in that they set requirements for security for industrial automation and control systems but vary in their focus and scope. This chapter provides an overview of the requirements process safety practitioners must follow when performing the SL assignment during SPR studies. As such, the level of discussion will be kept at a general overview. Readers who desire a more comprehensive discussion of the standard should refer to the standards themselves and to the series of training courses provided by ISA.

Structure of the ISA/IEC 62443 Series

The ISA/IEC 62443 Series, *Security for Industrial Automation and Control Systems*, is a collection of standards that provides cybersecurity requirements for industrial automation control systems (IACSs). Because the topic is so broad, a single document discussing all facets of analysis, design, operation, and maintenance was not practical. Instead, multiple documents were created that were geared toward either a specific stakeholder in the cybersecurity process or a specific discipline in the design, maintenance, and operation processes. Figure 2-1 presents an overview of the documents that make up the ISA/IEC 62443 Series and how they are related.

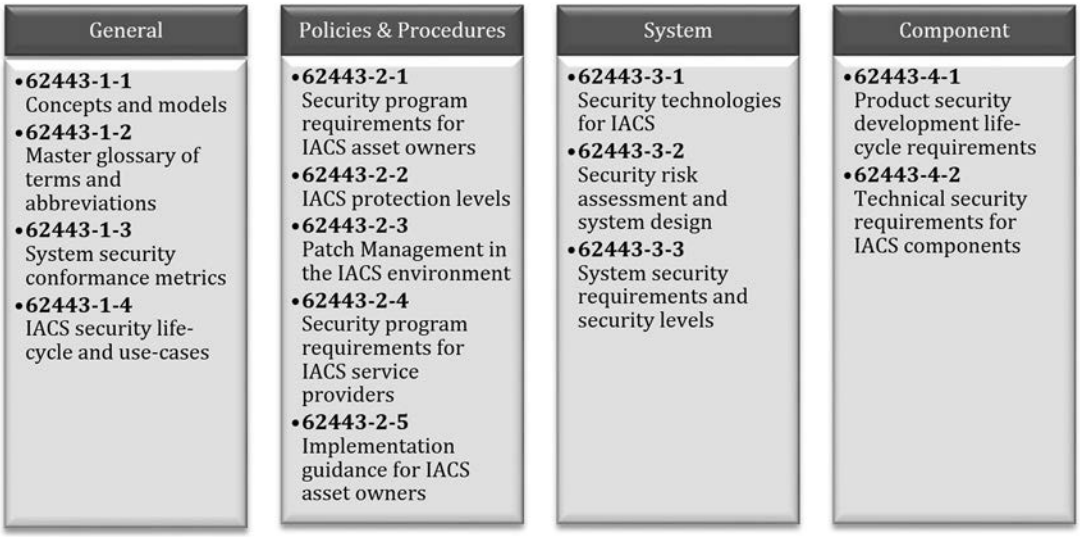


Figure 2-1. Collection of ISA/IEC 62443 Series documents.

As shown in Figure 2-1, the ISA/IEC 62443 Series is a collection of 14 documents that are separated into four separate categories.

First, there is the *general* category. It contains four documents that are intended to be of general interest to all stakeholders and disciplines. The first document, *Part 1-1: Terminology, Concepts, and Models*, contains an overview of why cybersecurity must be implemented; a definition of the security-level life cycle, including the requirements for each step of the life cycle; and an overview of the risk-based nature of the standards set. *Part 1-2: Master Glossary of Terms and Abbreviations*, effectively performs the role that its title implies. *Part 1-3: System Security Conformance Metrics*, contains a set of parameters that can be measured to determine the effectiveness of ICS performance, along with typical values. *Part 1-4: IACS Security Life Cycle and Use-Cases*, expands on the original definitions of the life-cycle steps and requirements that were presented in Part 1-1 with more detail.

The second category, *policies & procedures*, has five documents and is intended to be of primary interest to persons who work for companies employing an ICS to control their process operations. This group of documents helps these stakeholders develop internal or corporate policies and procedures for how an operating company will specifically implement cybersecurity. *Part 2-1: Security Program Requirements for IACS Asset Owners*, provides an overview of the content that should be included in corporate guideline documents, along with some options for implementation. *Part 2-2: IACS Protection Levels*, describes the protection level concepts

with related security and maturity levels. *Part 2-3: Patch Management in the IACS Environment*, provides detailed guidance to those who maintain the ICS as to how to perform patch management in an operational environment, highlighting differences between that process and how it is commonly performed in an office environment and why those methods would not be effective for the ICS. *Part 2-4: Security Program Requirements for IACS Providers*, defines normative requirements regarding installation and maintenance. *Part 2-5: Implementation Guidance for IACS Asset Owners*, defines requirements associated with the operation of a security management system.

Third is the *system* category that contains three documents that outline the details of system design that are implied or referred to in other documents. *Part 3-1: Security Technologies for IACS*, provides details on the types of equipment, operational parameters, and procedures that can be used for cybersecurity on an ICS. *Part 3-2: Security Risk Assessment and System Design*, provides information related to performing risk assessments and discusses how the results of the risk assessment process are related to design parameters. *Part 3-3: System Security Requirements and Security Levels*, is the document that defines what the various SLs mean in terms of equipment and the operational requirements needed to achieve the various SLs.

Fourth is the *component* category. It is composed of two documents that are dedicated to defining cybersecurity requirements at the component level, as opposed to the overall system level that is the primary focus of the documents in the other categories. Because these documents discuss the component level, they are primarily of interest to equipment vendors that supply ICS components to end users. *Part 4-1: Product Security Development Life-Cycle Requirements*, sets out requirements for equipment vendors with respect to the procedures that must be used when developing their products. *Part 4-2: Technical Security Requirements for IACS Components*, provides a more detailed set of technical features that should be implemented in components provided by ICS equipment vendors to enhance cybersecurity. Whereas Part 4-1 is really focused on the design process, Part 4-2 is more focused on the attributes of the components.

The ISA/IEC 62443 Series Life Cycle and Requirements

Like many other standards about instrumentation and control systems implemented in process plant applications, the ISA/IEC 62443 Series employs a life-cycle approach to structure the tasks that must be accomplished, the inputs and outputs from those tasks, and the requirements that those tasks must achieve. The ISA/IEC 62443 Series

3 Limitations of Cybersecurity Risk Analysis Methods

This chapter begins with the admonition from some cybersecurity practitioners that when it comes to risk analysis, much of what is proposed does not help. Many of the methods developed to define cybersecurity practices state that the starting point for cybersecurity is a risk analysis that will define the required degree of cyber safeguarding the ICS. Unfortunately, these methods go on to confuse and conflate risk analysis terms and processes, resulting in recommendations to perform tasks that do not adequately identify the correct hazards to safeguard. Much of the confusion comes from using the term *risk assessment* to describe life-cycle steps that include hazard identification, safeguard failure mode assessment, and ICS design verification and validation. The other types of analysis are appropriate when used to determine other risks that occur at different times in the life cycle; this analysis provides appropriate results that can be used to predict equipment failures and other potential issues. To alleviate the confusion surrounding risk assessment, this chapter and the following one will clearly define the precise terminology and specific methods used in risk assessment.

Process industry practitioners who are familiar with the successful and well-established methodologies for process hazard analysis are asking themselves why a new methodology is required to assess the risk of process plants to cyberattack. Some cybersecurity practitioners in government, academia, and industry have developed, or suggested, additional methods to address this issue. The primary problem with these additional methods is that they complicate the problem in process industries that already perform risk analysis designed to identify risk to the process itself. By focusing on the process under control, the other industrial processes, including batch and discrete manufacturing, can also be protected. While focus on the computer-based ICS equipment

should not be ignored, we actually want most of our focus on the actual industrial process controlled by the ICS. Additionally, risk analysis of controlled industrial processes requires an understanding of the industrial process and how it reacts or malfunctions. Analysis of the ICS equipment alone provides little knowledge of the actual risk posed by the industrial process.

This chapter provides an overview of some of the methods that have been proposed to address cybersecurity risk analysis and considers their origins, strengths, and limitations. The chapter goes on to discuss the primary limitations of these existing methods that prevent them from being optimal solutions for the process industries. Finally, the chapter sets the stage for the next, which presents traditional methods for assessing the risks of industrial processes as well as methods for extending these existing processes to achieve cybersecurity requirements.

The ISA/IEC 62443 Series Requirements for Risk Assessment

The ISA/IEC 62443 Series requires that a risk assessment be performed to determine the appropriate level of cybersecurity safeguarding. Unfortunately, the standards use the term loosely and in different situations. As a result, even defining what risk assessment is supposed to mean becomes confusing and varies depending on the situation and context. The ANSI/ISA-62443-2-1 standard defines two kinds of risk assessment that should be performed on an ICS with regard to cybersecurity: high-level and detailed. What the standard refers to as *high-level risk assessment* considers general types of ICS vulnerabilities with regard to cybersecurity and the process consequences that can be expected if those vulnerabilities are present in the system. The detailed risk assessment is similar but instead of general categories of vulnerabilities, specific vulnerabilities that are directly related to the makes, models, and software revisions of the specific ICS components are used.

To clarify the terminology, this chapter presents a simplified workflow for applying cybersecurity. The workflow shown is consistent with traditional PHA techniques and the application of the full range of process safeguards (of which cybersecurity is only one). The terminology and techniques in the workflow are from the ISA/IEC 62443 Series.

Figure 3-1 presents the simplified cybersecurity safeguard application workflow. The first task is the identification of *process* scenarios in which risk is intolerable. In the terminology of the ISA/IEC 62443 Series, this is the *high-level risk analysis.* The most critical word here is *process.* Without understanding the industrial process being controlled, and knowing under what circumstances control can be lost—along with the consequences, causes,

Figure 3-1. Simplified cyber-safeguarding workflow.

and safeguards related to that scenario—the risk simply cannot be known. Traditional risk assessment methods promulgated by the cybersecurity community are simply not capable of performing this task, which is why the SPR method was developed. This initial identification task involves analyzing the process and not the ICS.

Once the scenarios vulnerable to cyberattack are identified, one can determine the extent to which cybesecurity should be used to reduce the risk. In accordance with the ISA/IEC 62443 Series, an SL would be assigned to achieve this. After the SL is defined, a cybersecurity requirements specification can be developed that will enumerate and define the ICS equipment and attributes required to achieve the assigned SL. At this point in the security-level life cycle, a verification task can be undertaken that analyzes the ICS design to ensure that all SL requirements are achieved. At this stage, a technique can be used to assess the effectiveness of the design. In the terminology of the ISA/IEC 62443 Series, this would be considered a *detailed risk assessment*. In the opinion of the authors, use of the term *risk assessment* here is confusing; nevertheless, it is contained in the standard and we must accommodate its use. In fact, at this stage, the project team is performing a design review. By way of analogy, it is not uncommon for a project team designing a pump to consider all the failure modes and effects of their design for a specific application (e.g., their selected metallurgies, wall thicknesses, and gasket and seal materials) to ensure it is appropriate for the specific application. However, no one would ever call this a risk analysis. So, what the cybersecurity community is calling a *detailed risk assessment*, every other engineering discipline would call a *design review.*

4

Process Hazard Analysis Overview

In the process industries, facilities are systematically assessed to identify possible hazard scenarios that could result in significant consequences. For each scenario, the safeguards capable of preventing the accident are evaluated to determine if they are adequate. This exercise is called a PHA, and in the United States, it is required (and revalidated every 5 years) for all facilities that pose a significant hazard according to the Occupational Safety and Health Administration (OSHA), the labor regulator, through the process safety management (PSM) regulation (29 CFR 1910.119). Most jurisdictions around the world have similar requirements.

While PHA methods are routinely used in the wet process industries (e.g., chemical, oil refining and petrochemical) and have been a standard part of the engineering workflow since the 1990s, they systematically assess hazards of industrial equipment not common to other industries. In these industries, safeguards are based on prescriptive (i.e., cookbook) sets of rules that come from years of experience with the same equipment. For instance, consider a boiler. This piece of equipment either heats water or turns water into steam (which is still technically heating water). Boilers have been in use for hundreds of years and as a result, designers have learned what accidents can occur and have applied safeguards to prevent them. This experience is typically codified in an industry group standard, in this case National Fire Protection Association (NFPA) 85, *Boiler and Combustion Systems Hazards Code*. The code is applied to all subsequent projects to prevent past accidents from recurring. The problem with this approach is that it presents the answer (i.e., the safeguard that should be used), but it does not present the question (i.e., what accident scenario the safeguard protects against). An example from NFPA 85 is the requirement for an automatic shutdown to

close fuel gas valves if the fuel gas pressure exceeds an acceptable threshold. Although the standard lists the requirement, it does not explain the scenario the safeguard protects against. In this example, the scenario is that the fuel gas valves fail to the open position, sending a large amount of fuel gas to the burner, which it is not able to consume. This situation can cause the flame to blow out, generating a large gas fuel/air cloud that can subsequently encounter a source of ignition and explode. This information should be of interest to malicious attackers as well as cybersecurity designers because it defines the accident scenario (or attack vector) that can be exploited to cause damage.

There are significant advantages that all industries would glean from incorporating PHA methods. Performing PHA on all industrial equipment has the following benefits:

- The operations/engineering team gains a better understanding of their equipment.
- The complete scenarios (attack vectors) that can cause a plant accident are developed.
- Operations/engineering personnel gain a better understanding of how equipment failures can lead to accidents with potentially significant consequences.
- New hazards that come from applying new and less understood equipment can be identified.
- New hazards that are the result of combining equipment in a new configuration can be identified.
- Scenarios that require advanced safeguarding are identified and developed (whether the safeguarding is traditional or based on cybersecurity).

Because there are so many benefits to performing a systematic PHA, the authors expect this technique to be increasingly adopted by the complete range of process industry customers. If for no other reason, the authors anticipate it will be adopted to develop potential scenarios that may require safeguarding through cybersecurity and to define the required level of integrity of cyber safeguarding.

All formal PHA methods are exercises in structured brainstorming. They are designed to stimulate thinking about a topic by providing a prompt to trigger ideas and a framework in which ideas can be evaluated. The prompts range from checklist questions or equipment lists to process parameters, depending on the selected technique. Brainstorming is expected to identify scenarios that the prompt identifies.

The scenarios are subsequently analyzed. PHA techniques are generally applied using the following steps:

1. Select a prompt to generate potential scenarios.
2. Brainstorm about the prompt to identify any credible scenarios related to it.
3. For each credible scenario that is identified:
    a. Determine the consequence of that scenario assuming that no safeguards operate.
    b. Determine what causes or initiating events can make the scenario occur (e.g., equipment failures, human error, and external events).
    c. For each cause, determine what safeguards are available and to what degree they are effective in mitigating the scenario under consideration.
    d. Consider all available safeguards and determine the likelihood of the accident scenario occurring.
    e. Consider the consequence and likelihood of the scenario in the context of the organization's criteria for determining acceptability of risk, and assess whether the scenario is tolerable as designed or if additional safeguarding is required.
    f. If required, make recommendations regarding redesign or safeguard implementation/modification to reduce the risk to a tolerable level.

Common PHA Methods

Many PHA methods have been defined and used. A few of these methods have been widely adopted in the process industries, and their procedures and techniques have been documented in the literature. The choice of which PHA methodology is appropriate for a specific process in an industry is at the discretion of the owner/operator of the facility, but it must be made in compliance with local law and regulation. In the United States, this is the OSHA PSM regulation. The OSHA PSM regulation lists a set of techniques allowed for PHA, with the note that novel techniques and combinations of techniques can be used if they are appropriate for the situation. The listed techniques include:

- Checklist
- What if?
- Hazard and operability study (HAZOP)

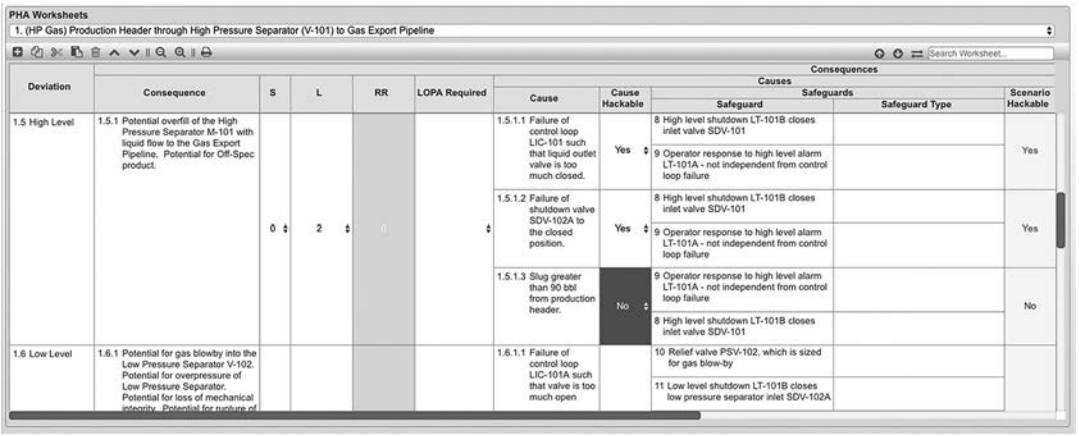
5
The SPR Study Process

A Security PHA Review (SPR) is a comprehensive process that identifies where safeguards that are inherently safe against cyberattack should be deployed. In a SPR, each scenario is reviewed to determine if a pathway that is vulnerable to cyberattack (i.e., a *hackable* pathway) exists. If it does, an inherently safe (i.e., *non-hackable*) safeguard is recommended. Because many non-hackable safeguards use springs as their means of motive force to take the process to a safe state, SPR studies are sometimes referred to as *spring studies*. Essentially, they confirm that there are enough springs in the plant's mechanical design to ensure it is safe against cyberattack.

Figure 5-1 maps out the tasks of a SPR study.

In order for the initiating event or cause of the scenario to be considered cyber-exposed or hackable, the physical cause (discussed in the hazard and operability study or HAZOP) would have to be the result of an industrial control system (ICS) virtual command. So, whereas a "flow control valve going closed" is hackable, the cause of an "operator inadvertently opens a bypass valve" is not—that is, if the bypass valve is hand-cranked and not actuated from the control system. As such, the first step in the SPR is to go through the cause of each deviation scenario to determine if it is hackable.

The next step is to review all safeguards to assess if they are hackable. Any operator action or computer-controlled safety instrumented function (SIF) is generally hackable (assuming the controller is a microprocessor-based system) but many safeguards are not. The SPR then reviews the list of safeguards for each scenario and identifies any that are non-hackable. If the deviation in the HAZOP includes at least


PHA Worksheets

1. (HP Gas) Production Header through High Pressure Separator (V-101) to Gas Export Pipeline

Search Worksheet...

Deviation	Consequence	S	L	RR	LOPA Required	Consequences				
						Causes		Safeguards		
						Cause	Cause Hackable	Safeguard	Safeguard Type	Scenario Hackable
1.5 High Level	1.5.1 Potential overfill of the High Pressure Separator M-101 with liquid flow to the Gas Export Pipeline. Potential for Off-Spec product.	0	2			1.5.1.1 Failure of control loop LIC-101 such that liquid outlet valve is too much closed.	Yes	8 High level shutdown LT-101B closes inlet valve SDV-101		Yes
								9 Operator response to high level alarm LT-101A - not independent from control loop failure		
						1.5.1.2 Failure of shutdown valve SDV-102A to the closed position.	Yes	8 High level shutdown LT-101B closes inlet valve SDV-101		Yes
								9 Operator response to high level alarm LT-101A - not independent from control loop failure		
						1.5.1.3 Slug greater than 90 bbl from production header.	No	9 Operator response to high level alarm LT-101A - not independent from control loop failure		No
								8 High level shutdown LT-101B closes inlet valve SDV-101		
1.6 Low Level	1.6.1 Potential for gas blowby into the Low Pressure Separator V-102. Potential for overpressure of Low Pressure Separator. Potential for loss of mechanical integrity. Potential for rupture of					1.6.1.1 Failure of control loop LIC-101A such that valve is too much open		10 Relief valve PSV-102, which is sized for gas blow-by		
								11 Low level shutdown LT-101B closes low pressure separator inlet SDV-102A		

Figure 5-1. A SPR flowchart.

one non-hackable safeguard, then it cannot be generated through a cyberattack and is therefore non-hackable.

When completing the SPR, if you go through the CAUSE and SAFEGUARDS for a particular deviation and identify that everything is hackable, you must review the consequences to evaluate if they are significant. If they are not, the attack vector can be considered a nuisance best left to traditional cybersecurity. However, if the consequences are significant, then it is incumbent on the analyst to recommend adding a non-hackable safeguard or establishing a security level (SL) based on the organization's tolerable risk criteria (see Appendix C for more information).

The addition of new non-hackable safeguards is not required as frequently as one might think and is not difficult to accomplish. The safeguard designer will always have the option to "mimic" one of the programmable electronic system (PES) SIFs with an analog pathway (i.e., a control loop current monitor relay). For instance, in the case of a high reactor temperature and an SIF opening a depressuring valve, if the SIF control function is in a safety programmable logic controller (PLC), then in theory, it can be hacked. However, the SIF could use an analog signal splitter on the 4–20 mA signal from the temperature transmitter (including a current monitor relay) to interrupt power to the solenoid valve of the pneumatic circuit of the depressuring valve. This method would result in a hack-proof analog secondary pathway for that SIF (shown in Figure 5-2).

By going through the SPR process, plant designers can ensure that any process plant is inherently safe against cyberattack. This type of safety does not rely, in any way, on the cyber defenses employed by the facility, only on the physical design of the plant itself. In a facility designed accordingly, an attacker could be seated at an operator

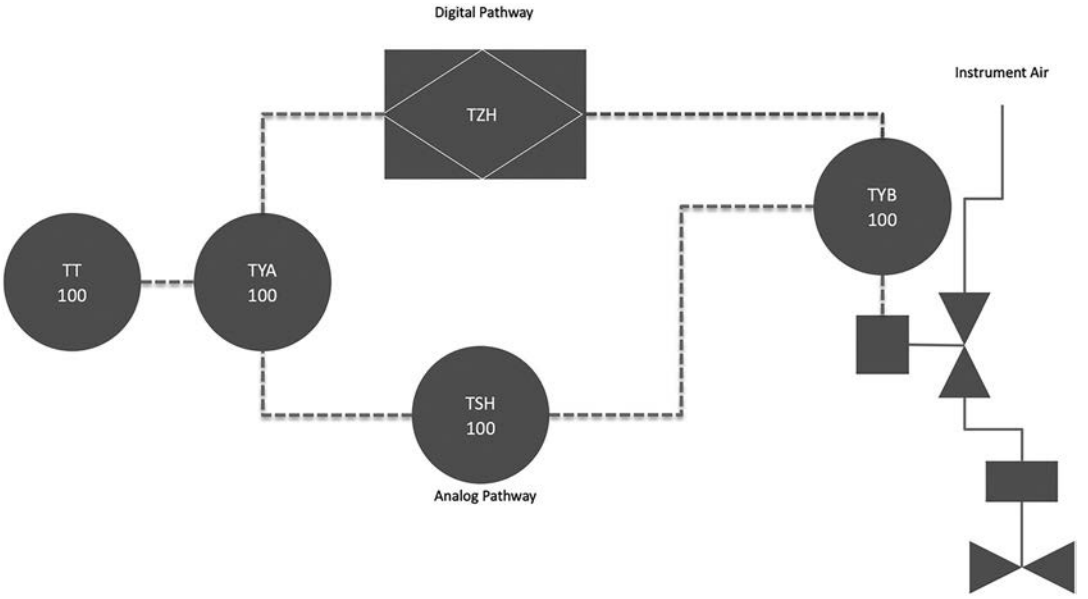


Figure 5-2. An analog "mimic" of a digital SIF.

station with full access to all operator and programming terminals with ample training on the plant and its control systems, and still would not be able to do any physical damage even though they might shut down the process.

Documenting a SPR

A SPR can be documented in a variety of ways depending on the nature and desires of the organization undertaking the study. Additionally, the whole process can be entirely automated and have no impact on the duration of the PHA study with the use of PHA software templates and safeguard and initiating-event-type databases.

The Highlighter Method

The most basic technique, for those aficionados of paper copies, is referred to as the *highlighter method*. It begins with a printed copy of a completed PHA study. Using this copy and the tangible results of the PHA study as the basis for the SPR, the analyst begins with the initial scenario. The first action is to review the cause(s) of this scenario. It should be noted here that while HAZOPs generally have the same workflow, there are often style differences in industry practices. Many HAZOP studies are indexed by cause, and each cause can have multiple consequences. Others, such as the one shown in Figure 5-3, are indexed by consequence, wherein a single consequence can have multiple causes. Either way, the analysis will proceed the same way and yield the same results.

6 Non-Hackable Safeguards

Several safeguards are commonly employed in the process industries that are inherently safe against cyberattack. One of these safeguards, the analog mimic of a digital safety instrumented function (SIF), can be employed to protect a process plant against virtually any conceivable cyberattack. However, the real work of protecting process industry plants lies in making the safeguard selection and installation process thorough and systematic.

The common process industry safeguards that are inherently safe against cyberattack include:

- Pressure relief devices
- Mechanical overspeed trips
- Check valves
- Motor-monitoring devices
- Instrument-loop current monitor relays (analog SIF mimic)

Pressure Relief Devices

Pressure relief devices protect pressure-containing pipes and vessels from bursting or leaking due to the pressure exceeding what the equipment can withstand. These devices come in several forms and diverse technologies, including traditional direct-operated, spring-activated relief valves; pilot-acting relief valves; and rupture disc and rupture pin-style devices.

Direct-Operated Relief Valve

A traditional *direct-acting, spring-activated relief valve* is mounted such that the inlet nozzle is directly connected to the protected process. As the pressure in the process increases beyond the desirable limit (which in some cases can be set with the set-pressure adjusting screw), the force of the pressure in the vessel overcomes the force of the spring holding down the relief valve plug. This safely vents the vessel's contents to a containment or disposal system and prevents damage to the process equipment. Figure 6-1 illustrates the internal structure of this typical relief valve.

Relief valves are ubiquitous in the process industries. In fact, in the United States, the law at the state level requires the use of relief valves for virtually all pressure vessels. The authors believe this simple safeguard could have prevented the damage to the Baku–Tbilisi–Ceyhan (BTC) pipeline's pumping station due to the alleged cyberattack over-pressurizing the discharge (see Chapter 1 for more details).

Rupture Discs

Rupture discs (also called *bursting discs*) are relief devices that operate according to the engineered failure of a metal (or usually metal) disc. Rupture discs are used in lieu

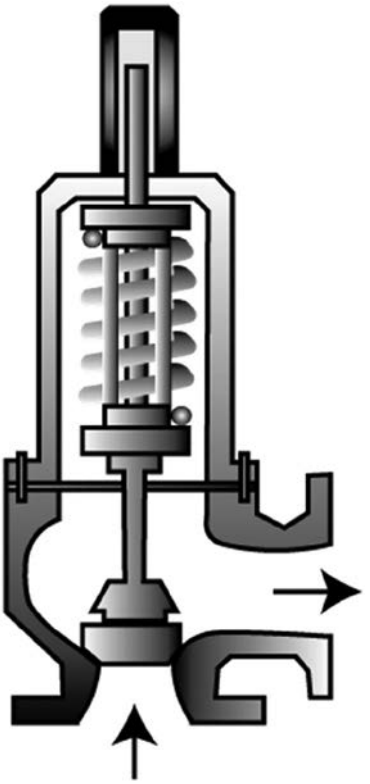


Figure 6-1. Spring-loaded pressure relief valve diagram.

of relief valves when there is no need to immediately re-close a pressure vessel after a pressure relief event. Because rupture discs are significantly less expensive than relief valves, they are the preferred choice if the pressure relief event does not occur frequently.

Rupture discs are placed in a holder as shown in Figure 6-2. The disc is directly exposed to the process fluid and its pressure. When the pressure exceeds the rupture disc's designed pressure point, the rupture disc will tear at the disc etchings, opening them to vent the pressure.

Buckling Pins

Buckling pins (shown in Figure 6-3) are the active parts of a valve system that relieve pressure under high-pressure situations. Buckling pins are like rupture discs in that a mechanical deformation destroys the protective device, which must be replaced prior to restoring the plant to operational mode. However, buckling pins have some distinct advantages over rupture discs. First, they can be replaced without disassembling the process or venting system piping, thereby protecting workers from exposure to process chemicals and decreasing replacement time. Secondly, buckling pins provide more flexibility, causing a valve to either open to relieve pressure or close to prevent further pressure. Finally, buckling pins are fast-activating, giving them an advantage over rupture discs and relief valves in specialty situations such as the venting of deflagrations.

Buckling pins do not operate in isolation; rather, they are part of a valve system. The buckling pin holds the valve element (typically a butterfly-type valve element) in position until the force created by the valve element on the buckling pin exceeds its strength, causing the valve element to move to the open position, venting the protected vessel.

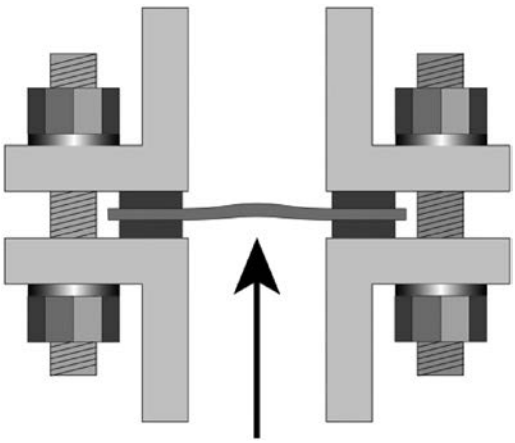


Figure 6-2. Rupture disc diagram.

7
Security PHA Review Examples

In this chapter, the SPR process will be used to assess some common process plant scenarios to provide insight into how the technique is applied and what results are generated. The examples were developed from a wide range of industrial applications throughout the process industries. In each example, a description of the process unit operation will be provided and then a scenario for causing a loss-of-containment accident in that unit operation will be postulated. An example of a typical hazard and operability study (HAZOP) scenario will be discussed, and then the SPR process will be applied.

This chapter is intended to provide a full range of scenarios that might be encountered in the process industries, from scenarios that start out as inherently safe against cyberattack to those in which cyberattack on the original design is feasible and could lead to devastating consequences. In these scenarios, where appropriate, recommendations for changing the process design to be inherently safe against cyberattack are presented along with the method for selecting an appropriate security level (SL) for cybersecurity if the inherently cyberattack-safe recommendation is not implemented.

In the IT and cybersecurity communities, it is common to discuss IT and industrial automation control system (IACS) equipment *vulnerabilities*. This chapter effectively presents the vulnerabilities of the industrial processes themselves. For each vulnerability to cyberattack that is identified, an inherently cyberattack-safe alternate design is proposed or the appropriate level of cyber safeguarding is presented. It is important to note that selecting the appropriate level of cyber safeguarding is based on example

risk criteria (see Appendix C for more details). The criteria used for specific and real applications are expected to vary from the examples in this book.

Vessel Overpressure

Consider a system in which a vessel is used as a knock-out drum in a high-pressure fuel gas service. In this service, the material that is mostly in the vapor phase (fuel gas) with some amount of entrained liquid (natural gas liquid) enters a pressure vessel. In the vessel, the liquids fall out of the bulk fluid with assistance from momentum changes and demister pads. The liquid level in the vessel is controlled by a level control loop that throttles the valve position in the liquid outlet line. Throttling a control valve in the vapor outlet line controls the pressure in the vessel.

A simplified piping and instrumentation diagram (P&ID) of a separator vessel is shown in Figure 7-1.

If the pressure control of the vessel (PIC-101) were to fail (e.g., if the pressure control valve on the vapor outlet of the vessel fails in the closed position), the pressure in the vessel would significantly increase to the supply pressure of the gas entering the vessel. If the vessel pressure were to increase above the maximum allowable working pressure (MAWP), it could potentially rupture the vessel, resulting in a loss of containment of fuel gas and natural gas liquids, which if ignited could result in a fire or explosion.

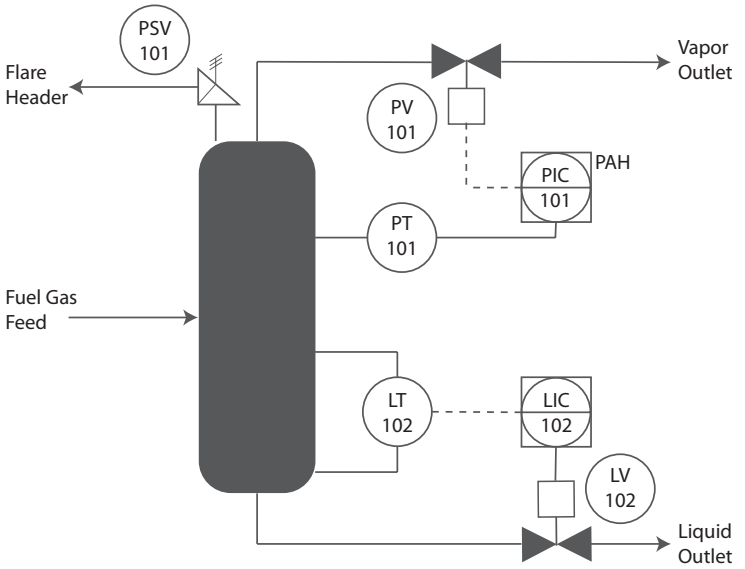
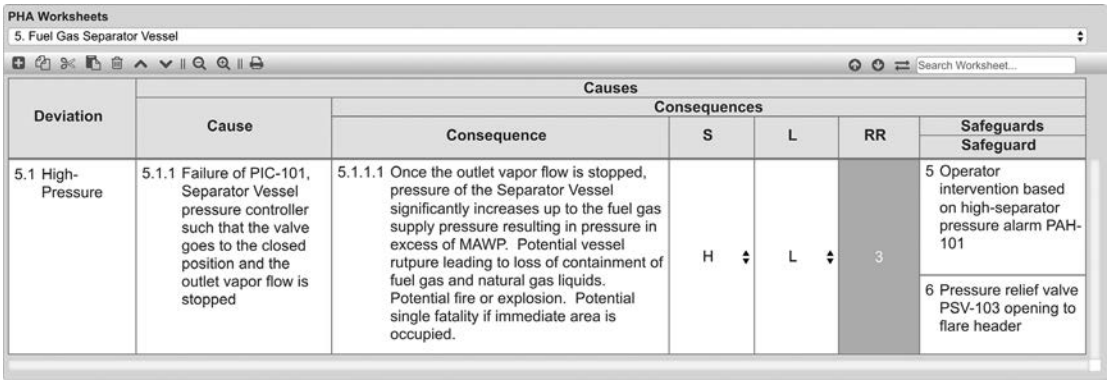


Figure 7-1. Simplified P&ID of a separator vessel.


PHA Worksheets

5. Fuel Gas Separator Vessel

Search Worksheet...

Deviation	Causes					
	Cause	Consequences				Safeguards
		Consequence	S	L	RR	Safeguard
5.1 High-Pressure	5.1.1 Failure of PIC-101, Separator Vessel pressure controller such that the valve goes to the closed position and the outlet vapor flow is stopped	5.1.1.1 Once the outlet vapor flow is stopped, pressure of the Separator Vessel significantly increases up to the fuel gas supply pressure resulting in pressure in excess of MAWP. Potential vessel rutpure leading to loss of containment of fuel gas and natural gas liquids. Potential fire or explosion. Potential single fatality if immediate area is occupied.	H	L	3	5 Operator intervention based on high-separator pressure alarm PAH-101 6 Pressure relief valve PSV-103 opening to flare header

Figure 7-2. Separator vessel high-pressure scenario PHA worksheet.

This scenario was considered during a HAZOP-style PHA. The worksheet for the high-pressure deviation is shown in Figure 7-2.

The SPR begins with an analysis of the initiating event. In this case, the initiating event is the failure of a pressure control loop (PIC-101). Because the control loop is contained in a distributed control system (DCS, based on its P&ID representation), it is computer-based, and if the DCS were remotely taken over by an attacker, the position of the valve could be manipulated to the closed position. As such, the initiating event is determined to be hackable.

Initiating Event	Location	Hackable?
Failure of PIC-101, Separator Vessel pressure controller, such that the valve goes to the closed position and the outlet vapor flow is stopped	DCS	Yes

Next, all safeguards are reviewed to determine if they are hackable. In this case, there are two safeguards. One is an operator intervention action based on an alarm and the other is a pressure relief valve. The operator intervention safeguard is determined to be hackable because the alarm annunciation occurs in the DCS (PAH-101). If an attacker were to take control of the DCS, the operator could be blinded to the loss-of-flow condition if the alarm were disabled and if the human-machine interface (HMI) value were frozen in its last good state. The pressure relief valve, on the other hand, is not hackable. As shown in the P&ID representation, the relief valve is not associated with any computer controller and is a simple mechanical device.

8 Conclusions

Process industry plants contain hazards whose consequences can be very severe if a loss of containment occurs. Because of the high levels of risk present in the process industries, engineers have developed techniques for identifying and addressing process hazards such that a tolerable level of risk exists across the full range of operating plants. As industrial accident statistics for most of the developed world will demonstrate, these efforts have been so successful that a typical worker is safer from accidental death in the workplace than he is at home. This safety record is a result of the systematic techniques that are consistently applied to process operations that allow for hazards to be identified and evaluated. The techniques consider the causes of potential accidents, the safeguards that are available to prevent them, and—if the accidents were to occur—the consequences that would result. These techniques have been in place for almost 50 years at the writing of this book, and their effectiveness is obvious.

Starting in the 1990s, the proliferation of computer systems as a part of ICSs changed the landscape of the process industries and shifted the risk profile. The new pieces of equipment brought failure modes that were not present in previous control systems. Some failure modes were related to random hardware failures of the new equipment. However, the advent of computer systems that employed routable communication protocols introduced the new failure mode of deliberate cyberattack. Existing PHA methods were not designed to assess many computer-based control system failure modes, and the problem of deliberate cyberattack is a specific failure mode of concern that requires updating and modifying current PHA techniques.

In the years following the adoption of computer-based control systems, including those with communication protocols that permit ICS communication with the outside world (either through dedicated phone lines or in many cases through the Internet), there have been many cyberattacks on industrial control equipment. While some of these attacks have been able to stop communication or shut down equipment, very few have resulted in physical damage or the loss of containment of highly hazardous chemicals from process plants. The reason for this surprising fact is that most process plants are safeguarded against virtually all equipment failures and in many cases they use mechanical safeguards that predate computer control systems by hundreds of years. Process plant engineers have made extensive efforts to identify the effects of process plant equipment failures through systematic safety studies and ensure that appropriate safeguards are in place to protect against these scenarios.

In the age of ubiquitous computer control, the game has changed, but most existing systems and equipment can still be leveraged to ensure that process plants are safe. While Internet-connected control systems have resulted in new failure modes related to deliberate malicious attack, the scenarios by which loss-of-containment accidents can occur in process facilities are still largely the same. The difference is that instead of organic and random hardware failures, now we must also consider deliberate failures through cyberattack. Even so, our existing methods for risk analysis, such as hazard and operability studies (HAZOPs), can still be used and leveraged to address these new failure modes.

In this book, we have discussed the SPR method, which extends existing PHA techniques (i.e., HAZOPs) to meet the challenges of an Internet-connected world and malicious cyberattacks. A SPR is an extension of the traditional PHA that specifically considers the ability of PHA scenarios to be generated through cyberattack. The SPR process typically begins with a completed PHA study. Of course, a skilled PHA facilitator educated in SPR can perform the SPR in the background while a PHA study is in progress. In a typical PHA study, accident scenarios are developed and assessed. These accident scenarios begin with an initiating event or cause. Each cause is then reviewed to determine what safeguards are in place that would prevent the cause from progressing into the final loss-of-containment event. The consequences and likelihood of the scenario are then reviewed to determine if the existing safeguards are adequate, and if they are not, recommendations are made to reduce the risk.

The SPR portion of the analysis extends the PHA to address deliberate cyberattack. First, each cause is assessed to determine if it can be generated through a deliberate cyberattack (i.e., if the cause is hackable). If it cannot be generated this way, the entire

Appendix A: Acronyms

ALARP	as low as reasonably practical
ANSI	American National Standards Institute
API	application programming interface
BPCS	basic process control system
BSI	German Federal Office for Information Security
CFATS	Chemical Facility Anti-Terrorism Standards
CHAZOP	control hazard and operability study
CSTR	continuously stirred tank reactor
CVA	cyber vulnerability assessment
cyber HAZOP	cyber hazard and operability study
cyber PHA	cyber process hazard analysis
DC	data confidentiality
DCS	distributed control system
DHCP	Dynamic Host Control Protocol
DMZ	demilitarized zone
DNS	domain name system
DoS	denial-of-service

Appendix B: Definitions

Buckling pin – A mechanical device used to operate a valve that buckles based on excessive force (from pressure) and causes a valve to move to either the fully open or fully closed position.

Deflagration and detonation – Types of explosions. Deflagrations are differentiated from detonations in terms of the speed of the rate of overpressure rising. In a detonation, peak overpressure is achieved almost instantaneously, whereas in a deflagration, the overpressure occurs more slowly (but still in fractions of a second). Due to the nature of a deflagration, it is sometimes possible to relieve the full force of a deflagration from process equipment through quickly activated pressure relief devices.

Frequency – Rate of occurrence.

Foundational requirements (FRs) – Foundational requirements are attributes of the industrial control system (ICS) design related to the system cybersecurity. FRs are defined in ISA 62443-1-1 (99.01.01)-2007, *Security for Industrial Automation and Control Systems – Part 1-1: Terminology, Concepts, and Models*, and then expanded on in ANSI/ISA 62443-3-3 (99.03.03)-2013, *Security for Industrial Automation and Control Systems – Part 3-3: System Security Requirements and Security Levels*.

Hackable – The attribute of being vulnerable to being accessed or broken into and controlled by malevolent actors. Specifically, the component is programmable, and the program can be altered by malevolent actors who can control the device in ways that were not expected or desired by the system owners.

Appendix C: Sample Risk Tolerance Criteria

Process plant owners/operators use risk tolerance criteria to make decisions about the amount of safeguarding required to make a plant safe. According to ANSI/ISA-61511-1-2018, safety is defined as "freedom from risk which is not tolerable" and tolerable risk is defined as the "level of risk which is accepted in a given context based on the current values of society."[1]

Risk tolerance criteria are used for many purposes and can take many forms. In process plants, risk tolerance criteria are used for a wide variety of engineering design tasks, such as:

- PHA
- Safety integrity level (SIL) selection
- Facility siting
- Risk-based inspection
- Reliability-centered maintenance

1 ANSI/ISA-61511-1-2018/IEC 61511-1:2016+AMD1:2017 CSV, *Functional Safety – Safety Instrumented Systems for the Process Industry Sector – Part 1: Framework, Definitions, System, Hardware and Application Programming Requirements* (IEC 61511-1:2016+AMD1:2017 CSV, IDT).

Because risk tolerance criteria have such a diverse base of uses, care must be taken to ensure all criteria (used in all risk-based design tasks) are consistent and consistently applied. As the use of risk analysis in the process industries, both fully quantitative and semi-quantitative, matures in the process industries, the representations of tolerable risk become more standardized. This appendix presents the most common approach to representing tolerable risk. Specifically, this includes a consistent set of fully quantitative criteria based on a tolerable individual risk of fatality, a matrix that represents the tolerability of a given scenario based on its consequence and likelihood category, and a set of target maximum event likelihoods (TMELs) based on the severity of consequence that is being prevented.

While the tolerability of risk can be represented in many ways, they all typically refer to a single metric—the individual risk of fatality. All other representations of tolerable risk, which are subsequently used for risk management tasks such as SL selection, are derived from this single value. Figures that are employed by various organizations for tolerable individual risk vary but commonly fall within a fairly narrow range. Figure C-1 presents data used by some operating companies in the process industries. The individual risk of fatality is typically represented as a range; the beginning of the range (the highest frequency) represents the frequency at which risk is not tolerable under any circumstance, and the end of the range (the lowest frequency) represents the point at which risk is negligible. In the middle, risk should be reduced to be as low as reasonably practical (ALARP).

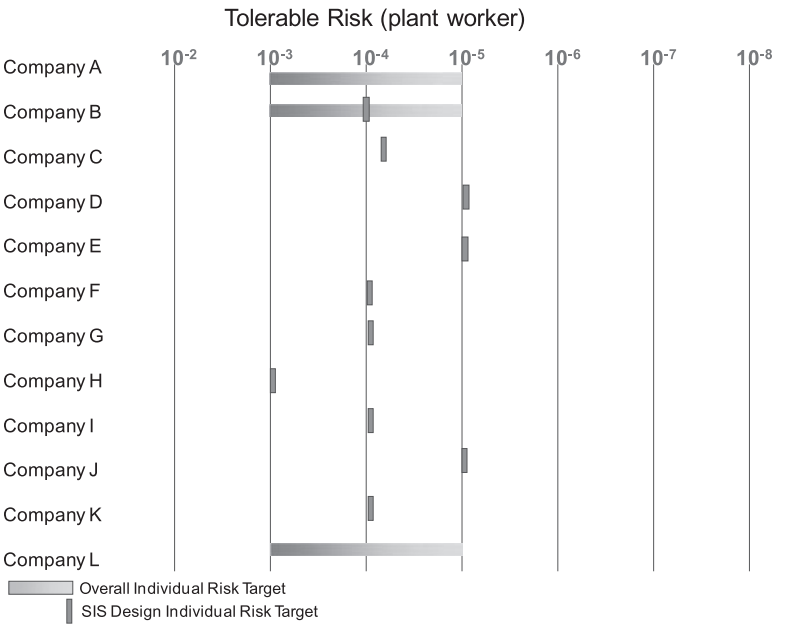


Figure C-1. Operating company risk tolerance criteria.

The two most common approaches used to represent tolerable risk for a single-hazard scenario (which is representative of the task of security level, or SL, selection) are the *risk matrix* and the *consequence table*. The risk matrix provides a two-dimensional representation of risk in terms of consequence and likelihood. Each intersection contains a numeric figure that represents the number of orders of magnitude of risk reduction required to make the risk of a particular hazard tolerable. The consequence table, on the other hand, is only consequence-based. For each category of consequence, the table contains a TMEL that is tolerable for a specific hazard and an appropriate SL. For the purposes of SL selection, the consequence-based approach is the most sensible; because the frequencies of deliberate human activities are impossible to define, it is impossible to assess the likelihood that they will occur. Additionally, the magnitude of the consequence also reflects the potential frequency as the desirability of the target is higher.

At this point, it is important to explain the correlation between the ALARP range of the individual risk of fatality, which represents tolerable risk to an individual, and the single point TMEL, which represents risk that is tolerable for a specific hazard. ALARP ranges are based on correlating risks posed by common hazards against a societal perception of the tolerability of those risks. Figure C-2 plots situations that people are frequently in as well as the risk tolerability for each situation.

While the ALARP range is an excellent tool for representing tolerable risk, it is difficult to directly apply to risk engineering tasks for two reasons. First, ALARP is a range, and engineering requires a single point as a design target. Second, ALARP represents the individual risk of fatality, which considers the sum of all risks to which

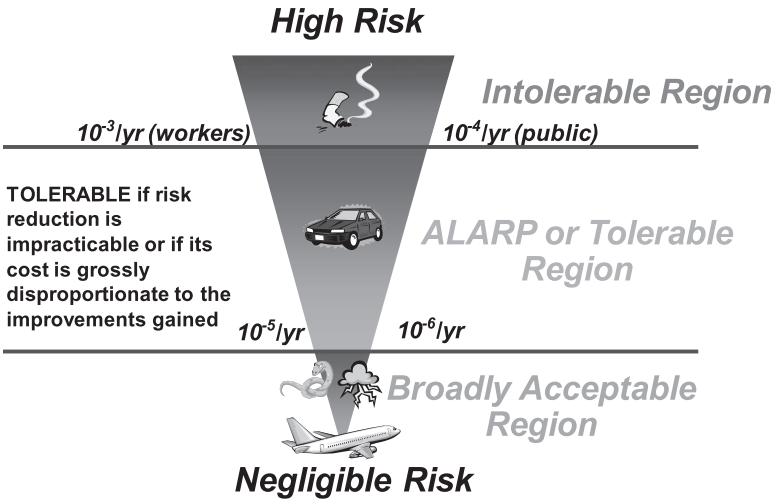


Figure C-2. ALARP conceptual representation.

Appendix D: ISA/IEC 62443 Security Levels

This appendix provides an overview of the ISA/IEC 62443 security levels (SLs) and how an organization would use them as part of its design process. As noted in the Preface, this book is not intended to provide guidance to control system engineers on how to perform cybersecurity design. Instead, this section provides an informal background on how SLs are used in the design process. Appendix D explores the ramifications of assigning a particular SL, which is much like the impact of assigning a security integrity level (SIL) in terms of the difficulty and expense of implementing the design.

Standard Terms

ISA 62443-1-1 defines an SL as a "level corresponding to the required effectiveness of countermeasures and inherent security properties of devices and systems for a zone or conduit based on assessment of risk for the zone or conduit."[1]

1 ISA-62443-1-1 (99.01.01)-2007, *Security for Industrial Automation and Control Systems – Part 1-1: Terminology, Concepts, and Models* (Research Triangle Park, NC: ISA [International Society of Automation]).

From a standards perspective, this definition is carefully chosen to facilitate the writing of requirements and conformance language. From a practical perspective, definitions like these are somewhat difficult to understand. While the ISA/IEC 62443 Series attempts to provide supplemental guidance and rationale material, sometimes these documents are not easy to understand. This appendix discusses how to use SLs in a practical way.

Foundational requirements (FRs) make up a set of seven categories of industrial control system (ICS) design attributes for which certain design practices should be specified to provide an appropriate degree of cybersecurity. As defined in ISA 62443-1-1, the seven FRs include the following:

1. Identification and authentication control (IAC)
2. Use control (UC)
3. System integrity (SI)
4. Data confidentiality (DC)
5. Restricted data flow (RDF)
6. Timely response to events (TRE)
7. Resource availability (RA)

Each FR includes system requirements (SRs) and requirement enhancements (REs), which are the ICS design specification attributes that define countermeasures for each FR. SRs form the basic structure for the system-level design attributes that should be applied to the system or zone. In addition, SRs may have (but are not required to have) REs that enhance the requirement so that it increases the level of security. The resulting set of specifications define the requirements for meeting a particular SL.

How SLs Came to Be in the ISA/IEC 62443 Series

The need to identify different levels of security was one of the cornerstone concepts for the ISA/IEC 62443 Series. The committee realized that not every ICS required the same protection. Some systems could use simple policies, procedures, and practices, while others needed more stringent protection. The committee also realized that there must be a way to distinguish between the security needs of different environments based on risk.

In the initial set of documents for the ISA/IEC 62443 Series, the concept of the SL was defined; however, no specific levels or definitions for the levels were developed. Subsequently, ANSI/ISA 62443-3-3 was developed to define the set of technical

requirements for systems. These requirements were expected to be implemented by the end-user organization. While drafting the standard, an attempt was made to use the existing National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 as the basis for ICS security requirements. However, it became apparent that converting the NIST documents for use within the ISA framework would be challenging because they failed to cover health, safety, and environmental impacts and were too detailed and inflexible in their classification of requirements.

Verifying the Achievement of an SL

After the required SL of a zone or conduit is defined, it is important to determine if the ICS design attributes can achieve the target SL. To do so, the specified technical requirements are assessed to determine if the target SL was achieved.

To assess a system, it is evaluated against the requirements described in ANSI/ISA-62443-3-3. Each SR and RE will be compared against the system design for compliance. Currently, the standard is written with a simple compliance evaluation of whether the SR or RE was achieved. After compliance has been assessed, the achieved SL for the system or zone can be determined as the lowest SL value achieved for any of the FRs. Table D-1 shows how SL verification is performed. In this example, each of the SRs and REs are evaluated independently. After determining the compliance of each attribute, the achieved SL is assigned by reviewing each SL column and determining if all requirements have been met for that particular SL. In this case, the resulting achieved SL for the zone would be SL 2.

Table D-1. Example assessment table for FR 5.

SRs and REs	Compliant	SL 1	SL 2	SL 3	SL 4
SR 5.1 – Network segmentation	Yes	✓	✓	✓	✓
RE (1) Physical network segmentation	Yes		✓	✓	✓
RE (2) Independence from non-control system networks	Yes			✓	✓
RE (3) Logical and physical isolation of critical networks	No				✓
SR 5.2 – Zone boundary protection	Yes	✓	✓	✓	✓
RE (1) Deny by default, allow by exception	Yes		✓	✓	✓
RE (2) Island mode	No			✓	✓
RE (3) Fail close	No			✓	✓
SR 5.3 – General purpose person-to-person communication restrictions	Yes	✓	✓	✓	✓
RE (3) Prohibit all general purpose person-to-person communications	No			✓	✓
SR 5.4 – Application partitioning	Yes	✓	✓	✓	✓

Appendix E: Exercise Solutions

The following are the answers to the exercise questions at the end of each chapter.

Chapter 1: Introduction

1.1. What is the meaning of the acronym SPR?

Answer: C. Security Process Hazard Analysis (PHA) Review

1.2. How many security levels (SLs) have been defined in the ISA/IEC 62443 Series?

Answer: B. 4

1.3. Cyberattacks against process industry facilities have never been able to cause physical damage.

Answer: B. False

Feedback: Several cyberattacks are believed to have caused physical damage. Sparse information exists on many of these attacks, resulting in an unconfirmed nature of the overall causes and consequences. However, at least one attack—Stuxnet—is widely accepted to have resulted in physical damage.

1.4. Process plants can often be made inherently safe against cyberattack through the application of which safeguards?

Index

Note: Page numbers followed by f or t indicate figures or tables.

R

S