Chapter 4 of:

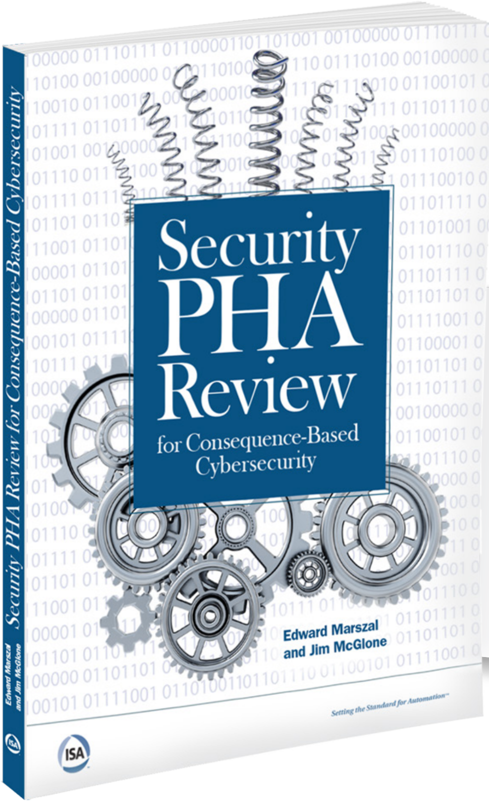
Security PHA Review

for Consequence-Based Cybersecurity

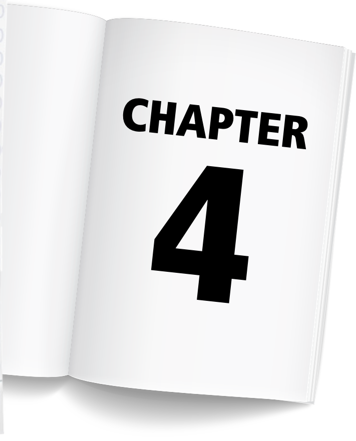
Edward Marszal and Jim McGlone

Security PHA Review

for Consequence-Based Cybersecurity


Security PHA Review for Consequence-Based Cybersecurity
Security PHA Review for Consequence-Based Cybersecurity
Edward Marszal and Jim McGlone
Edward Marszal and Jim McGlone
Setting the Standard for Automation™
ISA

By Edward Marszal and Jim McGlone



Book Table of Contents

Buy the Complete Book

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

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)

- Failure modes and effects analysis (FMEA)
- Event tree analysis
- Fault tree analysis

While six methods are listed, only four of these techniques are methods for identifying hazard scenarios, which is the purpose of a PHA activity. The last two techniques—*event tree analysis* and *fault tree analysis*—are used to thoroughly develop and understand a known hazard scenario.

Checklist is a very simple and common technique. Out of all PHA techniques, it requires the lowest level of effort. A checklist is usually applied to process equipment that poses a relatively low level of risk. Such risks are well understood because any company that develops these checklists has many locations with similar pieces of equipment or processes. For example, a pipeline company might have dozens or hundreds of pumping stations along a pipeline, each of which are nearly identical. In this case, a checklist is prepared in which all known hazard scenarios are listed. An operations/engineering team then reviews it to ensure all items are appropriately addressed in the design of each facility.

A *what-if* study is generally employed as an extension of a checklist study. In a what-if study, the study facilitator provides a brainstorming prompt by asking a question such as, "What if a truck that is delivering LPG to the plant begins to drive away before the loading hose is disconnected?" After the prompt is given, the study assesses the credibility of the scenario, consequences, safeguards, and risk tolerability, as with any other PHA technique. The what-if process has the advantage of being simple and easily documented, but it requires an experienced facilitator who essentially knows, through his or her experience, what accident scenarios are possible for a given set of process equipment. Typically, what-if studies are used in combination with checklists for common pieces of process equipment that pose a low level of risk.

An FMEA is a much more comprehensive and systematic technique than the two described above. When performing an FMEA, the brainstorming prompts are specific modes of equipment failure. First, a list of the equipment contained in the process under study is prepared. Then, a list of failure modes is developed for each piece of equipment. For instance, if a pump is used in a process, its failure modes might be:

1. Fails to start
2. Fails during operation

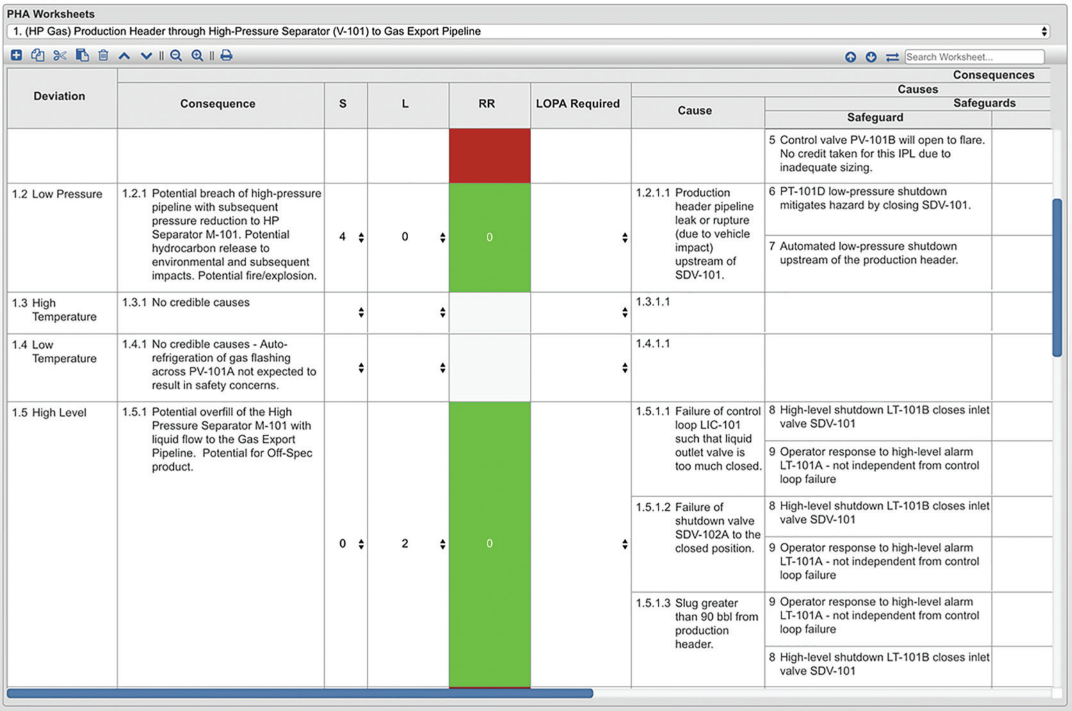
3. Fails to stop when commanded
4. Mechanical seals or gaskets leak

Each of these failure modes is essentially a credible cause to explore. Thus, for each failure mode, the resulting consequence (i.e., the *effect*) is defined and ranked; the safeguards that will prevent the effect are listed; and the overall risk is identified and compared against the tolerable risk criteria. An FMEA is a great tool for thoroughly analyzing highly mechanical systems. However, the use of FMEA in the wet process industries has been somewhat limited. The reason is that an FMEA inherently only regards equipment failures as causes. In the process industries, there are important causes related to human interaction with processes, chemicals that are not compatible, and external events—all of which are not adequately addressed by FMEA.

A HAZOP is the most commonly used PHA technique in the wet process industries because it addresses virtually any hazard scenario and has a systematic approach This is combined with the technique's systematic approach to identifying hazards. While this method is the most time-consuming, it is also the most thorough, making it the optimal choice in high-risk industries and for processes where in which the hazards are not yet well known or well understood. To perform a HAZOP, the team first considers a list of parameters that are important to the facility under study. In the wet process industries, this might be pressure, temperature, or level. For each parameter, a design intent or normal operating condition is defined. Then, a set of guide words is applied, defining departures from the design intent that result in deviations such as higher temperature, lower pressure, and reverse flow. For each deviation, the study team decides whether the deviation is credible, and if so, if it poses a hazard. For credible deviations, the consequences, causes, safeguards, and risk tolerability are all explored to ascertain if the scenario is acceptable. If the risk is deemed unacceptable for the design, the team provides recommendations.

Hazards and Operability Studies

PHAs are performed using a variety of techniques that have been developed over the past 50 years or so. The most common and comprehensive technique is the hazard and operability study, or HAZOP. Because HAZOP is so common, this section provides an in-depth description of the technique and its resulting documentation. In a HAZOP, a facility is broken down into *nodes* of similar operating conditions and walked through a set of deviations, such as high pressure, low temperature, and reverse flow, in a workshop setting with a multidisciplinary team (e.g., operations, safety, and engineering personnel). An example HAZOP worksheet is shown in Figure 4-1.


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

	Consequences						
						Causes	
							Safeguards
Deviation	Consequence	S	L	RR	LOPA Required	Cause	Safeguard
				🟥			5 Control valve PV-101B will open to flare. No credit taken for this IPL due to inadequate sizing.
1.2 Low Pressure	1.2.1 Potential breach of high-pressure pipeline with subsequent pressure reduction to HP Separator M-101. Potential hydrocarbon release to environmental and subsequent impacts. Potential fire/explosion.	4	0	🟩 0		1.2.1.1 Production header pipeline leak or rupture (due to vehicle impact) upstream of SDV-101.	6 PT-101D low-pressure shutdown mitigates hazard by closing SDV-101. 7 Automated low-pressure shutdown upstream of the production header.
1.3 High Temperature	1.3.1 No credible causes					1.3.1.1	
1.4 Low Temperature	1.4.1 No credible causes - Auto-refrigeration of gas flashing across PV-101A not expected to result in safety concerns.					1.4.1.1	
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	🟩 0		1.5.1.1 Failure of control loop LIC-101 such that liquid outlet valve is too much closed.	8 High-level shutdown LT-101B closes inlet valve SDV-101 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.	8 High-level shutdown LT-101B closes inlet valve SDV-101 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.	9 Operator response to high-level alarm LT-101A - not independent from control loop failure 8 High-level shutdown LT-101B closes inlet valve SDV-101

Figure 4-1. Sample HAZOP worksheet.

When a HAZOP is performed, the engineering team examines virtually every possible deviation from the design intent of the plant and ensures there are appropriate safeguards to protect against these situations. If the team determines that the degree of safeguarding is inadequate, it makes recommendations to add new protection layers, modify the process to make it inherently safer, or improve existing safeguards.

While this process systematically and thoroughly assesses potential hazard scenarios, it does not ensure that a plant is inherently safe against cyberattack. Safeguards are examined to evaluate if they are appropriate; however, the study often does not consider whether the safeguards could have been disabled by means of malicious attack. The authors propose that this additional step, referred to as a SPR, become a part of the PHA. As shown in Figure 4-1, for every deviation the HAZOP team encounters, a CAUSE(S) for that deviation is identified, and all SAFEGUARDS that prevent the cause from propagating into a loss-of-containment accident are also listed. From a cybersecurity perspective, the HAZOP scenario can define an attack vector by deliberately generating the CAUSE while simultaneously disabling all the SAFEGUARDS through external control of the industrial control system (ICS) equipment. Based on the authors' analysis and the paucity of cyberattack examples that have caused physical damage, this cyber-exposed position is rarely present in well-designed process facilities and can virtually always be designed out. If a situation does not exist in which CAUSE initiation and SAFEGUARD disabling can occur as the result of an ICS attack, then the plant is *inherently safe* against cyberattack.

Process Safety Information

The HAZOP process begins with assembling documents that define the plant equipment and processing conditions. This information is collectively referred to as process safety information (PSI). PSI includes the following:

- Piping and instrumentation diagrams (P&IDs)
- Process flow diagrams (PFDs)
- Process block flow diagrams
- Material and energy balance (including stream compositions, temperatures, pressures, flow rates, etc.)
- Equipment specification sheets
- Instrumentation specification sheets
- Relief system design basis documentation
- Cause-and-effect diagrams

The information available for a HAZOP should include, at minimum, the P&IDs. If the P&IDs are not available, it is unlikely that the PHA study will be of any value. The other documentation does not necessarily have to be available to all study participants throughout the meeting. It is common to have a single set of some of these documents for the team to review on demand. It is also common to obtain documentation as required over the course of the study. Once the HAZOP facilitator accumulates all the required PSI, node definition and project setup begin.

Node Definition

The HAZOP then evaluates deviations from the design intent. The list of deviations from the design intent is quite significant. It is common to have 4 deviations and 8 process parameters (for a total of 32 combinations). While it is possible to apply this set of deviations to each individual piece of equipment and pipe segment, it would result in a tedious and repetitive study with an interminable duration. Instead, HAZOP facilitators group equipment with similar operating conditions into nodes. The following factors are considered when deciding which pieces of equipment to group together:

- Temperature
- Pressure composition
- Phase (e.g., liquid or vapor)
- Equipment design conditions

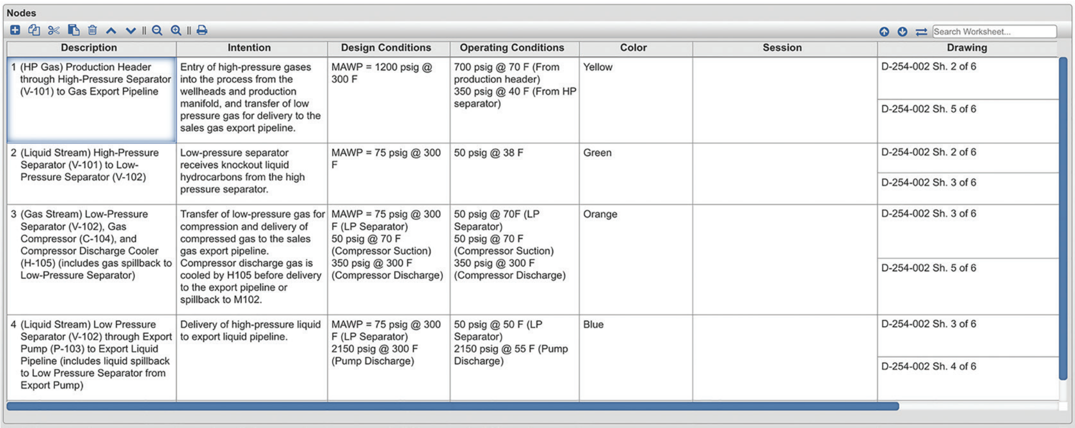
Once the equipment for a node is grouped together, the intention, design conditions, and operating conditions of the node are documented (as shown in Figure 4-2).

Finally, the P&IDs (paper or digital) are marked, using highlighters or the electronic equivalent, to provide a visual indication of the extent of the nodes. An example of marking nodes on drawings is shown in Figure 4-3.

HAZOP Team

Once the facilitator has defined and marked the nodes, the actual study can proceed. The HAZOP is a team-based workshop for structured brainstorming, with "team" being the most critical part. A HAZOP is not intended to be a one-person desktop activity. Rather, it includes multiple members with diverse backgrounds in different disciplines. Only with this depth and breadth of knowledge, training, and experience can reasonable results be achieved. There is no fixed formula for how the HAZOP team should be selected, but the following staff should be considered:

- Facilitator (i.e., leader or chairman)
- Scribe (i.e., technical support engineer)



Description	Intention	Design Conditions	Operating Conditions	Color	Session	Drawing
1 (HP Gas) Production Header through High-Pressure Separator (V-101) to Gas Export Pipeline	Entry of high-pressure gases into the process from the wellheads and production manifold, and transfer of low pressure gas for delivery to the sales gas export pipeline.	MAWP = 1200 psig @ 300 F	700 psig @ 70 F (From production header) 350 psig @ 40 F (From HP separator)	Yellow		D-254-002 Sh. 2 of 6 D-254-002 Sh. 5 of 6
2 (Liquid Stream) High-Pressure Separator (V-101) to Low-Pressure Separator (V-102)	Low-pressure separator receives knockout liquid hydrocarbons from the high pressure separator.	MAWP = 75 psig @ 300 F	50 psig @ 38 F	Green		D-254-002 Sh. 2 of 6 D-254-002 Sh. 3 of 6
3 (Gas Stream) Low-Pressure Separator (V-102), Gas Compressor (C-104), and Compressor Discharge Cooler (H-105) (includes gas spillback to Low-Pressure Separator)	Transfer of low-pressure gas for compression and delivery of compressed gas to the sales gas export pipeline. Compressor discharge gas is cooled by H105 before delivery to the export pipeline or spillback to M102.	MAWP = 75 psig @ 300 F (LP Separator) 50 psig @ 70 F (Compressor Suction) 350 psig @ 300 F (Compressor Discharge)	50 psig @ 70F (LP Separator) 50 psig @ 70 F (Compressor Suction) 350 psig @ 300 F (Compressor Discharge)	Orange		D-254-002 Sh. 3 of 6 D-254-002 Sh. 5 of 6
4 (Liquid Stream) Low Pressure Separator (V-102) through Export Pump (P-103) to Export Liquid Pipeline (includes liquid spillback to Low Pressure Separator from Export Pump)	Delivery of high-pressure liquid to export liquid pipeline.	MAWP = 75 psig @ 300 F (LP Separator) 2150 psig @ 300 F (Pump Discharge)	50 psig @ 50 F (LP Separator) 2150 psig @ 55 F (Pump Discharge)	Blue		D-254-002 Sh. 3 of 6 D-254-002 Sh. 4 of 6

Figure 4-2. Sample HAZOP node definition worksheet.

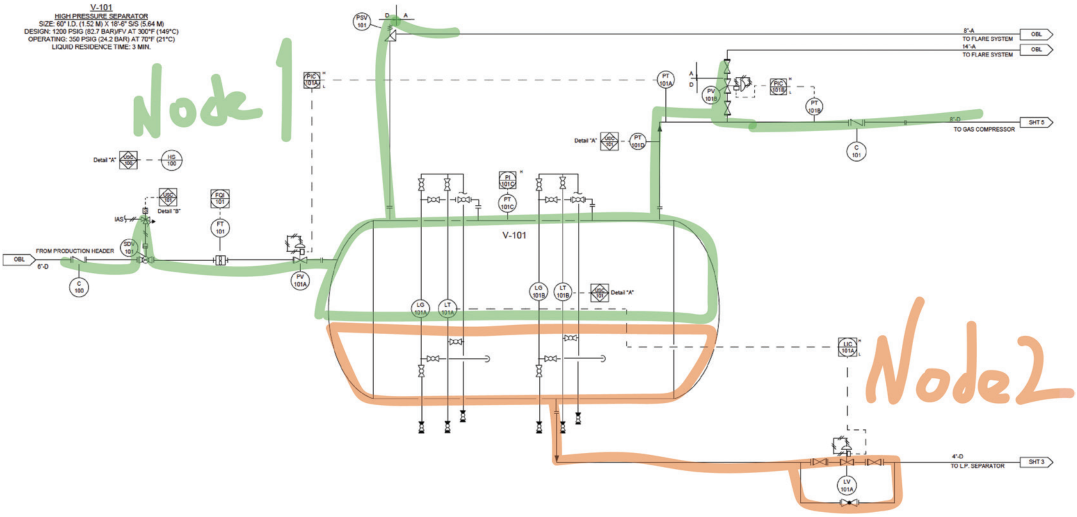


Figure 4-3. Sample HAZOP node mark-up.

- Operations
- Operations management
- Process engineering
- Maintenance (e.g., rotating equipment)
- Process safety management
- Instrumentation and controls engineering
- Specialty equipment engineering (e.g., fired heaters)

While representatives from these disciplines can provide value, they are not required to attend an entire meeting, or in some cases, to attend at all. In the United States, in accordance with the OSHA PSM rule, the only persons absolutely required to attend a PHA meeting are the facilitator and a representative from operations.

Deviation Development

Once the team is collected for the workshop, they will analyze each deviation for every node and document the results of the discussion. The deviations that are applicable will vary from industry to industry and even from process to process. Each deviation is built from a process parameter that is important to the equipment in the scope of the study. Guide words are used to indicate how a parameter can diverge from the design intent. The following is a list of parameters that are commonly used in the process industries (other industries will use other parameters, such as torque, force, and speed in the machine industries):

- Pressure
- Temperature
- Level
- Flow
- Composition
- Viscosity

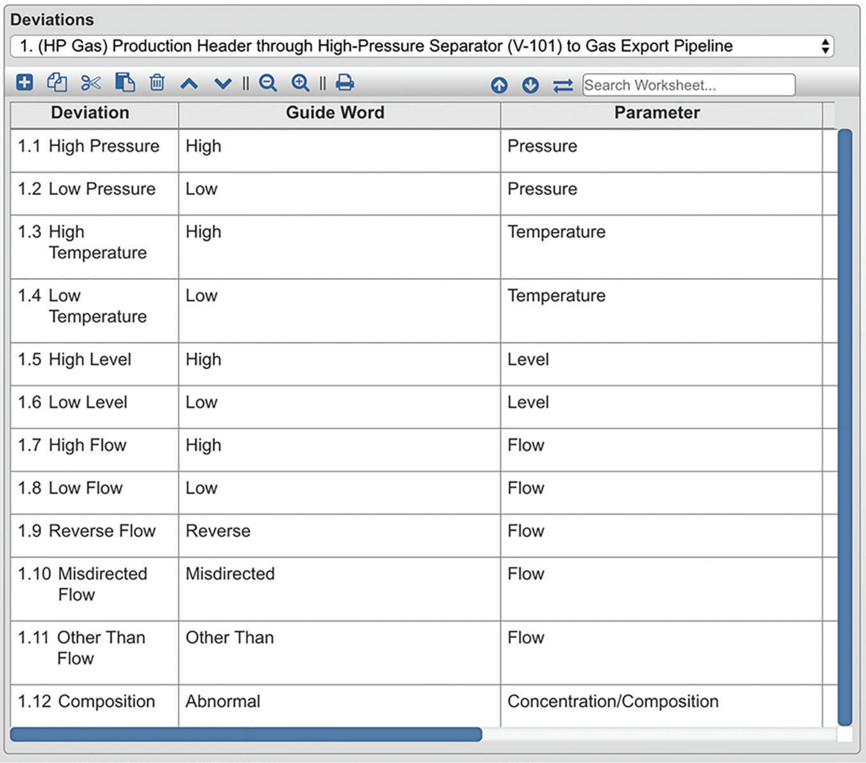
Guide words are then applied to these parameters to create deviations from the design intent. As with parameters, the guide words are a function of the industry and type of analysis being performed. Some common guide words from the process industries include:

- High (more)
- Low (less)
- Reverse
- Misdirected
- Other than
- Abnormal

Once the deviations are built from the parameter and guide-word combinations, they are listed in the HAZOP documentation tool and addressed for each individual node. A typical deviation list is shown in Figure 4-4.

Building the Scenario

In the workshop setting, the HAZOP facilitator leads the team through the analysis of all node deviations. The facilitator begins by explaining the node and then moving to the first deviation, for instance, high pressure. The team considers whether development of the deviation (e.g., high pressure) beyond the design constraints of the node is possible. If it is not, the team documents "no credible causes" and moves on the next deviation. If it is possible, then the team continues the analysis. Next, for each credible scenario, a consequence is identified and described, such as "high pressure will



Deviations

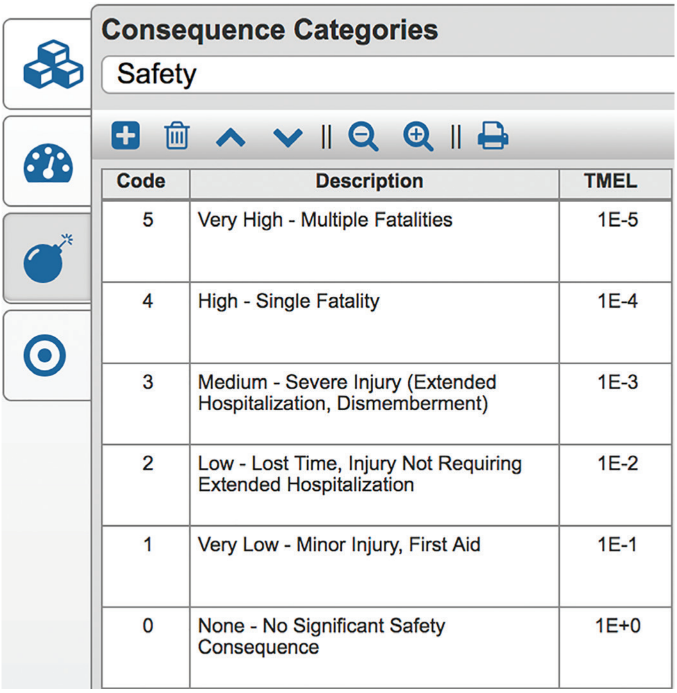
1. (HP Gas) Production Header through High-Pressure Separator (V-101) to Gas Export Pipeline

Deviation	Guide Word	Parameter
1.1 High Pressure	High	Pressure
1.2 Low Pressure	Low	Pressure
1.3 High Temperature	High	Temperature
1.4 Low Temperature	Low	Temperature
1.5 High Level	High	Level
1.6 Low Level	Low	Level
1.7 High Flow	High	Flow
1.8 Low Flow	Low	Flow
1.9 Reverse Flow	Reverse	Flow
1.10 Misdirected Flow	Misdirected	Flow
1.11 Other Than Flow	Other Than	Flow
1.12 Composition	Abnormal	Concentration/Composition

Figure 4-4. Sample HAZOP deviation list.

exceed maximum allowable working pressure with the potential for rupturing a vessel, releasing flammable material, and causing potential fire or explosion, which could result in a single fatality of a member of the exposed personnel.” The consequence is then assigned a category based on its severity. It is important to remember that this assessment is made assuming all safeguards will fail to operate. A typical table for ranking consequence severities is shown in Figure 4-5.

Next, the causes of the deviation (high pressure in this case) are determined and documented. For example, the cause of high pressure might be excessive upstream pressure feeding into this process section or an external fire near the process equipment. After the causes are documented, each cause is analyzed to identify what safeguards are present that might prevent the cause from propagating into the unwanted accident or loss-of-containment scenario. Some safeguards that might prevent the overpressure of process equipment include pressure relief valves, SISs that isolate or stop pressure sources, and operator intervention based on alarms. All applicable safeguards are listed. This assessment is done on a cause-by-cause basis because safeguards that are applicable to one cause might not apply to a different cause. Once the causes and safeguards are all documented, the team evaluates the likelihood that the



Consequence Categories

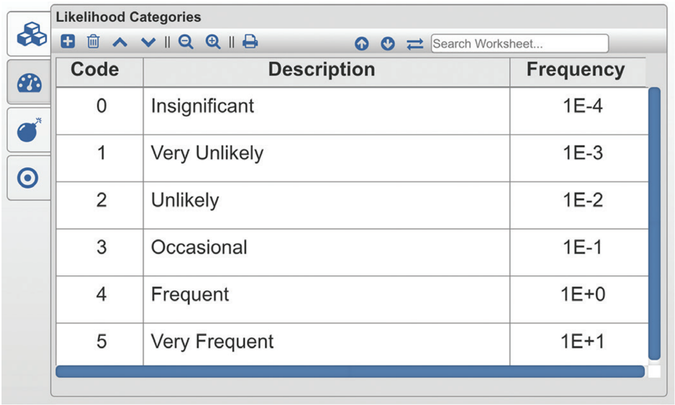
Safety

Code	Description	TMEL
5	Very High - Multiple Fatalities	1E-5
4	High - Single Fatality	1E-4
3	Medium - Severe Injury (Extended Hospitalization, Dismemberment)	1E-3
2	Low - Lost Time, Injury Not Requiring Extended Hospitalization	1E-2
1	Very Low - Minor Injury, First Aid	1E-1
0	None - No Significant Safety Consequence	1E+0

Figure 4-5. Sample HAZOP consequence ranking table.

event and its associated consequence will occur, considering all safeguards that are available. This assessment is usually done using a likelihood table similar to the one shown in Figure 4-6.

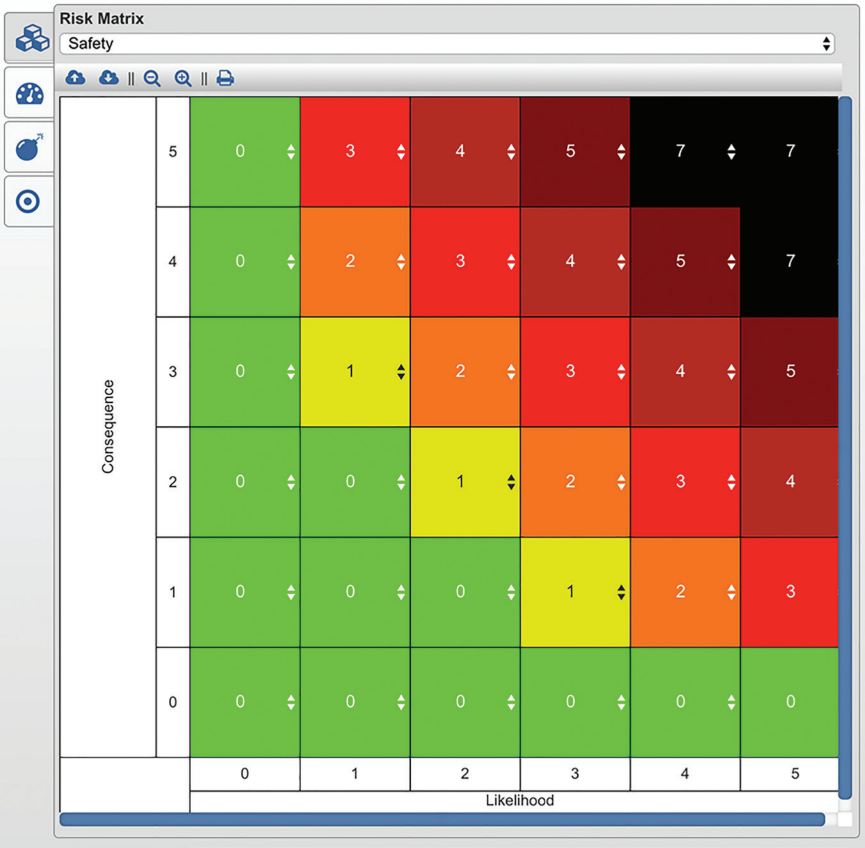
After the scenario's consequence and likelihood are defined, the overall risk posed by the scenario can be determined as it is a function of the combination of consequence and likelihood. Most operating companies use a risk matrix (such as the



Likelihood Categories

Code	Description	Frequency
0	Insignificant	1E-4
1	Very Unlikely	1E-3
2	Unlikely	1E-2
3	Occasional	1E-1
4	Frequent	1E+0
5	Very Frequent	1E+1

Figure 4-6. Sample HAZOP likelihood ranking table.



Risk Matrix

Safety

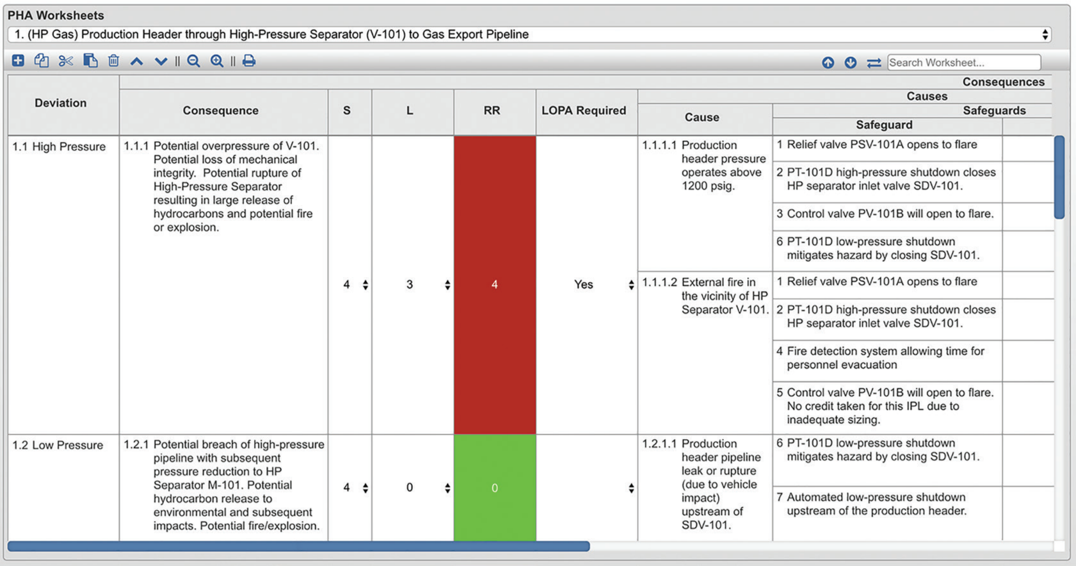
Consequence	5	0	3	4	5	7	7
	4	0	2	3	4	5	7
	3	0	1	2	3	4	5
	2	0	0	1	2	3	4
	1	0	0	0	1	2	3
	0	0	0	0	0	0	0
		0	1	2	3	4	5
		Likelihood					

Figure 4-7. Sample HAZOP risk matrix.

one shown in Figure 4-7) to represent risk tolerability of the various consequence and likelihood pairs.

Each intersection in this matrix represents a statement about the tolerability of a given cause/likelihood pair. For the example criteria shown in Figure 4-7, if the consequence severity was a category 4 and the likelihood was a category 1, then the table shows an orange risk–level 2. In the example criteria, only green risk–level 0 is tolerable. As a result, the HAZOP shows the risk associated with this scenario is not tolerable according to the operating company's guidelines. Therefore, the HAZOP team must make recommendations that, if implemented, will result in a tolerable level of risk being achieved.

The result of the analysis would be a completed worksheet row as shown in Figure 4-8. After the analysis for a deviation is complete, the next deviation is considered. Once all deviations are analyzed, the next node is considered. And finally, after all nodes are assessed, the study is complete.


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

						Consequences Causes	Safeguards
Deviation	Consequence	S	L	RR	LOPA Required	Cause	Safeguard
1.1 High Pressure	1.1.1 Potential overpressure of V-101. Potential loss of mechanical integrity. Potential rupture of High-Pressure Separator resulting in large release of hydrocarbons and potential fire or explosion.	4	3	4	Yes	1.1.1.1 Production header pressure operates above 1200 psig.	1 Relief valve PSV-101A opens to flare
							2 PT-101D high-pressure shutdown closes HP separator inlet valve SDV-101.
							3 Control valve PV-101B will open to flare.
							6 PT-101D low-pressure shutdown mitigates hazard by closing SDV-101.
						1.1.1.2 External fire in the vicinity of HP Separator V-101.	1 Relief valve PSV-101A opens to flare
							2 PT-101D high-pressure shutdown closes HP separator inlet valve SDV-101.
							4 Fire detection system allowing time for personnel evacuation
							5 Control valve PV-101B will open to flare. No credit taken for this IPL due to inadequate sizing.
1.2 Low Pressure	1.2.1 Potential breach of high-pressure pipeline with subsequent pressure reduction to HP Separator M-101. Potential hydrocarbon release to environmental and subsequent impacts. Potential fire/explosion.	4	0	0		1.2.1.1 Production header pipeline leak or rupture (due to vehicle impact) upstream of SDV-101.	6 PT-101D low-pressure shutdown mitigates hazard by closing SDV-101.
							7 Automated low-pressure shutdown upstream of the production header.

Figure 4-8. Sample HAZOP report row for high-pressure deviation.

Summary

Understanding and analyzing the risks of the industrial process controlled by an ICS is a critical part of a well-designed cybersecurity program. Analysis of the computer-based control equipment alone will not provide a sufficient understanding of the hazards because the scenarios in which accidents occur can only be understood by analyzing the process, not the potential ICS failure modes. Understanding the hazards of industrial processes requires a thorough and systematic analysis of all potential hazard scenarios with attendant ranking of risks.

Industrial process hazards can be identified and assessed using myriad methods, but the most common ones include checklist, what if, FMEA, and HAZOP. The HAZOP method is the most flexible workhorse; it provides the most detail and is especially useful for situations in which the risk is high or the process and its hazards are not well understood. A HAZOP considers deviations from the design intent that can occur in industrial processes, such as higher pressure or reverse flow. If the HAZOP team determines the deviation is possible, they analyze the scenario. The team identifies and ranks the consequence severity, identifies the initiating causes for the scenario and the safeguards that are present, and then evaluates the overall risk. The overall risk is compared against the risk criteria tolerability and if the scenario's risk is deemed unacceptable, the team proposes recommendations to reduce it.

PHA, in a formal and documented program, has been successfully applied in the process industries for over 40 years. The methods are well established and effective, and engineers, plant managers, and regulators alike respect the recommendations. A logical extension of the current framework is to examine existing work for necessary insights in developing cybersecurity programs. While the process industries have a head start, all industries will benefit from this type of analysis, not only to improve their cybersecurity position but also to better understand and control their hazards in general.

Exercises

4.1 What is the technique for applying safeguards to hazardous industrial processes using "best practice" rules based on past experience without specific analysis of the hazards present?

A. Performance-based

B. Prescriptive

C. Quantitative risk analysis

D. Hazard and operability study (HAZOP)

4.2 Under what circumstances would a checklist-style process hazard analysis (PHA) be an appropriate choice for assessing the hazards associated with an industrial process?

A. Common equipment with low risk

B. Novel equipment with low risk

C. Common equipment with high risk

D. Novel equipment with high risk

4.3 What is the most common form of PHA used in the process industries?

A. Failure modes and effects analysis (FMEA)

B. Desktop safety review (DSR)

C. Checklist

D. HAZOP

4.4 A HAZOP considers deviations from the design intent of the equipment under study. What level of detail is usually applied to the study?

A. Deviations are analyzed for each piece of equipment and pipe segment.

B. Deviations are analyzed for each piece of equipment, but pipe segments are associated with pieces of equipment and are not analyzed separately.

C. Deviations are analyzed for nodes, which are collections of equipment and pipe segments with similar process conditions and hazards.

D. Deviations are analyzed once for each process plant.

4.5 Which of the following categories of personnel are *required* to attend a PHA meeting?

A. Process safety management

B. Instrumentation and control engineering

C. Information technology

D. Operations

4.6 What is the most important document to include in a set of process safety information (PSI)?

A. Safety instrumented system (SIS) network diagram

B. Cause-and-effect diagram

C. Instrumentation specifications

D. Piping and instrumentation diagrams (P&IDs)

4.7 What is the prompt for brainstorming in a HAZOP, such as high pressure or misdirected flow, called?

A. Deviation

B. Process parameter

C. Guide word

D. Checklist question

4.8 What assumptions about safeguards should be made when selecting an appropriate consequence and consequence severity category for a HAZOP scenario?

A. Assume all safeguards fail or are not effective.

B. Assume that only adequately maintained safeguards will operate.

C. Assume that only safeguards that are inherently safe against cyberattack will operate.

D. Assume that all safeguards will operate.

4.9 What approach is typically used during a HAZOP to define the amount of risk that an organization is willing to tolerate?

A. Target maximum event likelihood tables

B. Risk matrices

C. Cost-to-benefit ratio limits

D. Risk decision arrays

4.10 If the risk for a HAZOP scenario is unacceptably high, what is the most appropriate response for the HAZOP team?

A. Engineer a solution for the problem.

B. Cause operation of the plant to stop.

C. Provide recommendations for safeguards or redesign to reduce risk to a tolerable level.

D. Abandon the plant design because its risk is too high.

Bibliography

29 CFR 1910.119. *Process Safety Management of Highly Hazardous Chemicals—Compliance Guidelines and Enforcement Procedures*. OSHA (Occupational Safety and Health Administration). US Federal Register, February 24, 1992.

Center for Chemical Process Safety (CCPS). *Guidelines for Hazard Evaluation Procedures.* New York: CCPS, 1998.

Kenexis. *Open PHA User Manual Version 1.0.* Columbus, OH: Kenexis Consulting Corporation, 2017.

Marszal, Edward M., and Eric W. Scharpf. *Safety Integrity Level Selection with Layer of Protection Analysis*. Research Triangle Park, NC: ISA (International Society of Automation), 2002.

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.

Contents