ISA GLOBAL CYBERSECURITY ALLIANCE

Leveraging ISA 62443-3-2 For IACS Risk Assessment and Risk Related Strategies

THE TIME IS NOW

May 2021

www.isa.org/ISAGCA

Leveraging ISA 62443-3-2 For IACS Risk Assessment and Risk Related Strategies

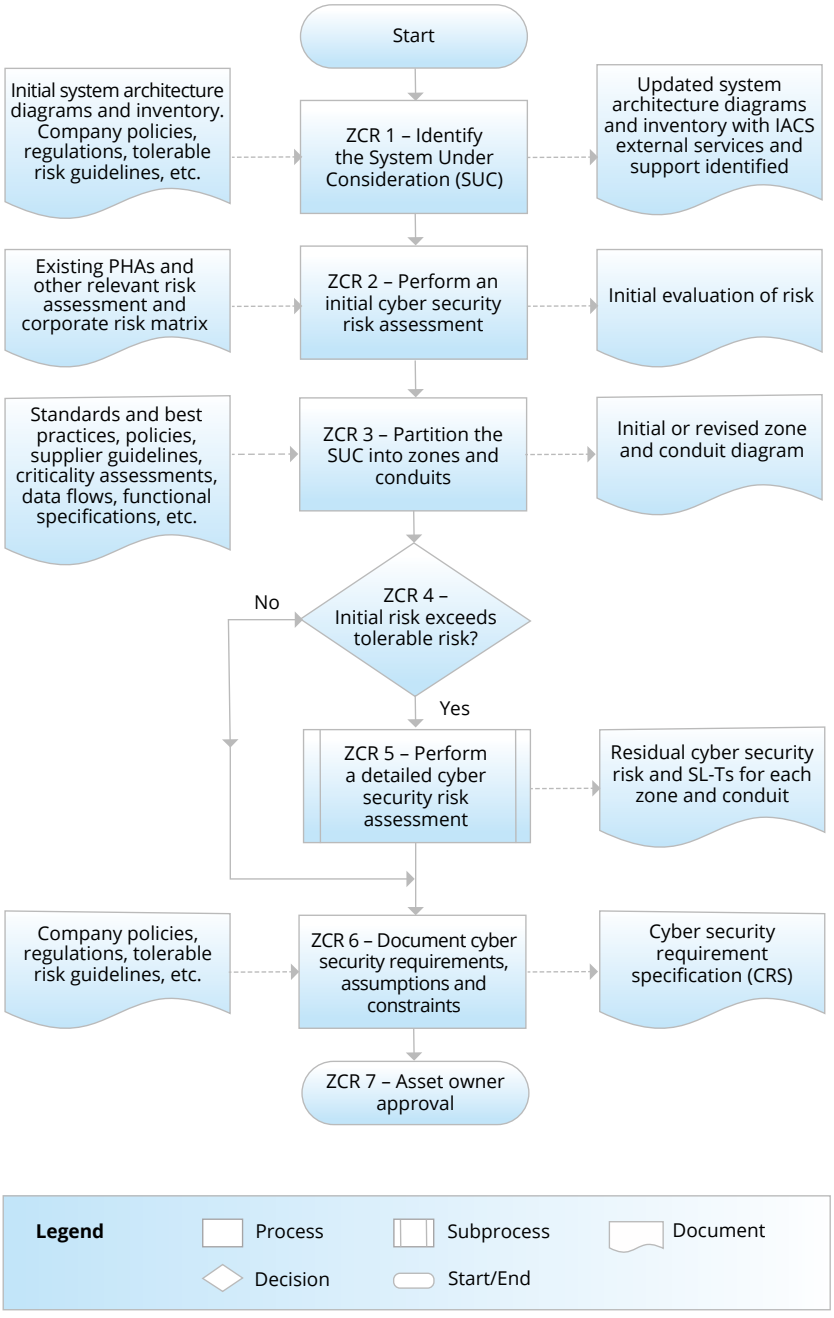

Figure 1: Workflow diagram outlining the primary steps to establish zones and conduits, as well as to assess cyber risk[4]

Executive Summary

This document is intended to provide the reader with an overview of ISA 62443-3-2, "Security Risk Assessment for Design", as well as a summary of some methodologies that can be used to assist execution of the industrial automation control system (IACS) cyber security risk assessment work process requirements detailed in the standard. This risk assessment work process is applicable to many sectors, e.g. industrial process sector, building automation, medical devices, transportation sectors, electrical production, water treatment, etc. Risk management of the IACS starts with a proposed design that is based on company standards and practices and/or recognized and generally acceptable good engineering practice (RAGAGEP). It then requires the understanding of how to identify vulnerabilities, threats, consequences of a successful attack, ranking risks, and then implementing mitigation measures to lower risks to tolerable levels. The standard itself is considered a (RAGAGEP).

The standard can be summarized in two figures, both workflow diagrams. Figure 1 illustrates the overall work process, while figure 2 illustrates the detailed level risk assessment sub process shown in figure 1.

The major steps include:

- Identification of the System under Consideration (SuC)
- Perform an Initial Cyber Risk Assessment
- Partition the SuC into Zones and Conduits
- Perform a Detailed Level Cyber Risk Assessment
- Document Updated Cyber Security Requirements for Detailed Design

Each zone and conduit requirement (ZCR) number shown in figures 1 and 2 represents a specific requirement within the standard. The boxes in the left column of each figure represent inputs that are required for the different steps. The boxes in the right column represent outputs that are created in each step. The purpose of the cyber security risk assessment work process as a whole is to evaluate the consequences and associated likelihoods of risk scenarios due to security being compromised in order to prioritize which risks require mitigation as well as what cyber security measures are necessary to reduce the risk to tolerable levels established by the authority having jurisdiction, typically the operating company, referred to as the asset owner in the 62443 series of standards.

Risk is considered to be a measure of human injury, environmental damage, and economic loss, loss of intellectual property or loss of privacy in terms of both the incident likelihood and the magnitude of the loss or injury. A simplified version of this relationship expresses risk as the product of the likelihood and the consequences (i.e., risk = consequence x likelihood) of an incident. With respect to safety, health and environmental risk, consequences are measured in the same manner, irrespective of whether they are due to a cyber-attack or are identified via traditional risk assessments that in the past have not considered cyber security. Likelihood, however, can be thought of as a combination of vulnerabilities and the likelihood that a threat agent or source has the requisite skills, resources, and motivation to exploit the potential vulnerabilities or that vulnerabilities are unknowingly exploited by non-malicious human error.

During the initial cyber security risk assessment, likelihood is often expressed as a conditional

Table of Contents

probability equal to one, while detailed cyber security risk assessments must consider likelihood as an estimated frequency or probability. Cyber risk assessments should address uncertainty (at least qualitatively if not quantitatively) since not considering uncertainties can produce misleading and potentially dangerous decisions. Should a detailed level cyber security risk assessment be required, its work process is shown in figure 2 below.

The ISA/IEC 62443-3-2 standard, entitled "Security Risk Assessment for System Design" was released in February 2020 and may be purchased either from the ISA, or the International Electrotechnical Commission (IEC). The benefits of using a risk-based standards approach include:

- Reducing the likelihood of a successful cyberattack
- The use of a common set of requirements among stakeholders
- Security throughout the lifecycle, and a
- Reduction in overall lifecycle cost.

Like most performance-based standards, it provides general requirements and is not prescriptive, meaning it defines what to do, but not how to do it. The standard defines general requirements and links those requirements to examples of common best practices. For instance, it describes how to rank risk. Most corporations have a risk matrix that helps them establish their level of risk tolerance. Cyber risk assessments should be performed according to that basis and cyber risk, like any other corporate risk, should be ranked using that scale.

To support the "How" to execute the risk assessment requirements of the standard, this paper includes a summary of various methodologies for the performance of both vulnerability and risk assessments. More detail on these methodologies can be found in the source references. In addition, some guidance for application of the standard is provided to contrast green field projects versus brown field facilities.

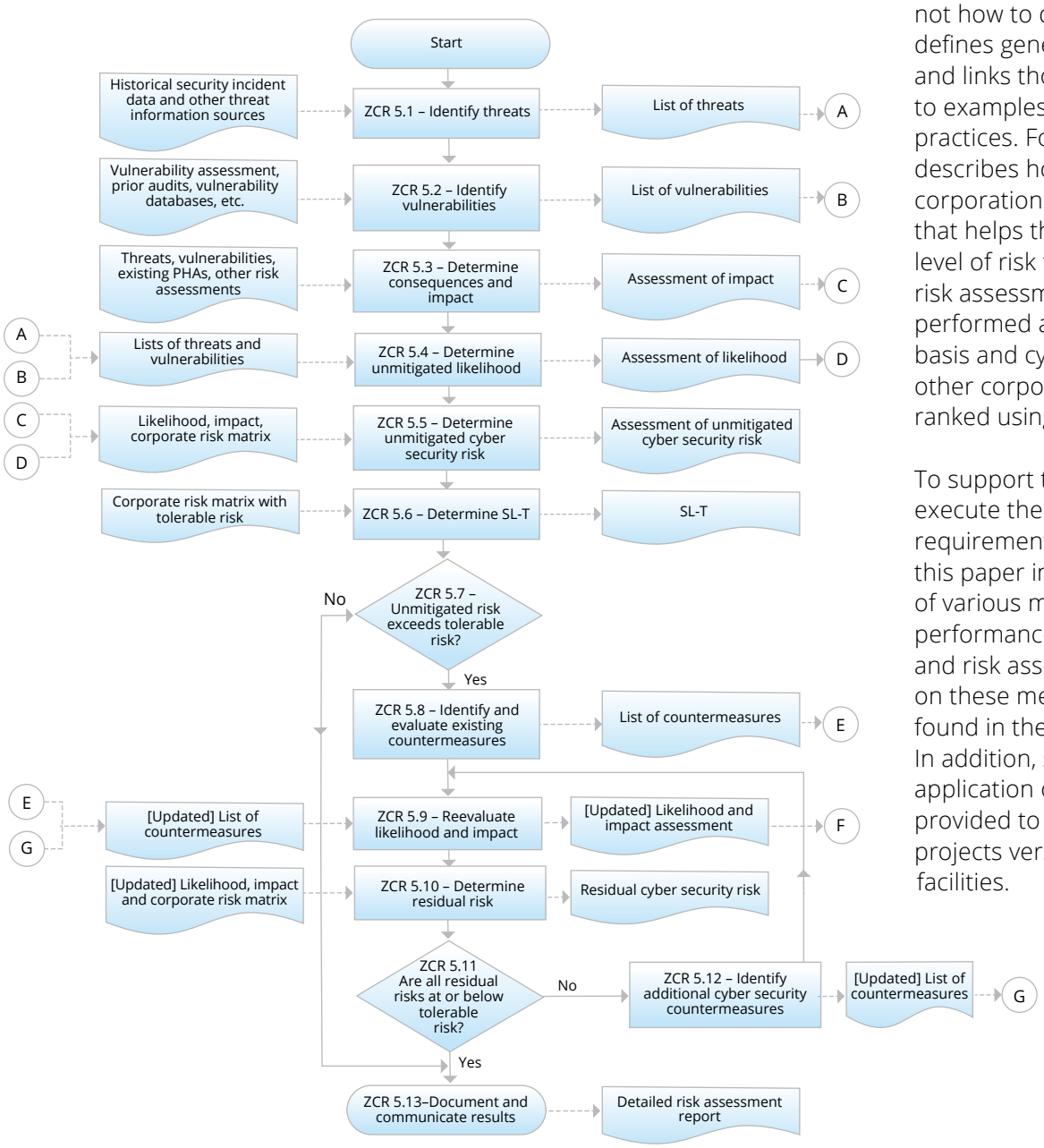

Figure 2: Detailed cyber security risk assessment workflow per zone and conduit[4]

Introduction

Scope

The ISA 62443-3-2 scope establishes requirements for:

- Defining the SuC for an industrial automation and control system (IACS) and its associated networks
- Partitioning the SuC into zones and conduits
- Assessing the risk for each zone and conduit and establishing the technical measure security level targets (SL-T) for each zone and conduit
- Documenting the security requirements needed to design, implement, operate and maintain effective technical security measures

Purpose

ISA 62443-3-2 was developed because it was determined that IT standards and practices were not sufficient to ensure the safety, integrity, reliability, and security of an IACS. This is due to many reasons, e.g. performance requirements, availability requirements, change management, the time between maintenance windows, expected equipment lifetimes and most importantly, the stark difference between information risk and risks that involve loss of life or health, damage to the environment, loss of product integrity, extended business interruption due to equipment damage. Simply stated, the consequences of a successful cyberattack on an IACS are fundamentally different than the impact on information systems where the primary consequences of a successful cyberattack on IT systems is financial and privacy loss due to information disclosure.

The standard provides requirements to establish a work process for cyber security risk assessment that can be integrated with an existing risk assessment program and represents RAGAGEP. The benefits of using this standard include reducing the likelihood of a successful cyberattack, the use of a common set of requirements among stakeholders, security throughout the lifecycle, and a reduction in overall lifecycle cost.

Importance of Conducting Cybersecurity Risk Assessments

Within any industry that utilizes industrial control and safety systems, risk due to safety, environmental and / or business interruption generally transcends the risks associated with just information. This helps explain the difference between information technology and operational technology, both of whom rely on the same types or hardware and software to perform their respective functions. Risk management programs and work processes are generally already in existence in companies that use industrial control and safety systems, however, in the past, these work processes did not consider cyber security as a potential contribution to these risks.

There are several trends that have stressed the need to make cybersecurity an essential property of IACS, along with safety, integrity, and reliability. First, over the last two decades, IACS technologies have migrated from vendor-proprietary to commercial off-the-shelf technologies such as Microsoft Windows™ and TCP/IP networking. Second, the value of data residing in the IACS for business purposes external to the IACS has significantly increased the interconnectivity of IACS internally within the organization as well as externally to the organization. In addition, the means, resources, skills, and motivation of threat agents have significantly increased. With the advent of cyber-attacks on control and safety systems, there is now recognition that cyber security must be addressed not only versus recognized and generally accepted good engineering practice (RAGAGEP), but also assessed versus a company's risk tolerance criteria following implementation of RAGAGEP.

Risk Assessment Work Process

Risk is considered to be a measure of human injury, environmental damage, and economic loss, loss of intellectual property or loss of privacy in terms of both the incident likelihood and the magnitude of the loss or injury. A simplified version of this relationship expresses risk as the product of the likelihood and the consequences (i.e., risk = consequence x likelihood) of an incident. With respect to safety, health and environmental risk, unmitigated consequences are measured in the same manner, irrespective of whether they are due to a cyber-attack or are identified via traditional risk assessments that in the past have not considered cyber security.

Likelihood, however, can be thought of as a combination of vulnerabilities and the likelihood that a threat agent or source has the requisite skills, resources, and motivation to exploit the potential vulnerabilities or that vulnerabilities are unknowingly exploited by non-malicious human error.

Identify System under Consideration (SuC)

Prior to the initial cyber security risk assessment, the SuC perimeter and access points should be identified and documented. It is important to recognize that when defining the SuC, the equipment ranging from field sensors and final elements all the way through to the overlapping interface with information technology (IT) within the demilitarized zone (DMZ) should be considered. In the event that the industrial internet of things (IIOT) or the cloud are used to perform functions within the OT levels, they would necessarily be included as well. This concept is illustrated in figure 3.

Initial Cyber Security Risk Assessment

An initial cyber security risk assessment can be thought of as a screening exercise that helps to determine if more work is needed and to help define and prioritize zones and conduits. During the initial cyber security risk assessment, a simplifying assumption is made that the likelihood has a conditional probability equal to one. Conducting an initial risk assessment requires knowledge of the consequences should the equipment be compromised. If the initial assessment determines the system does not exceed the tolerable risk, the detailed risk assessment may be skipped, and the cyber security requirements may be documented. This is not a likely outcome unless the consequences were deemed to be relatively inconsequential, e.g. even safety systems would not be needed.

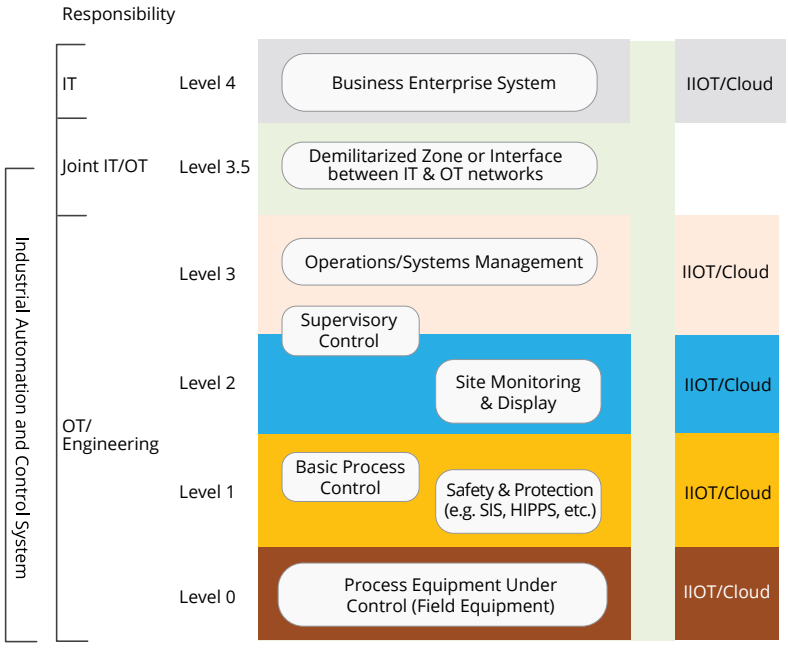

Figure 3: Excerpted from working draft of TR84.00.09 3rd edition currently under development

Detailed Level Risk Assessment

A detailed level cyber security risk assessment is intended to identify both the consequences and the likelihood of cyber-attack scenarios that are identified during the work process. This requires knowledge of the (proposed) design, policies and procedures to support the technical measures included in the design as well as of its system architecture. The detailed cyber risk assessment may be performed quantitatively or qualitatively, however, it is easier to consider uncertainties when the analysis is quantitative. Not considering uncertainties can produce misleading and potentially dangerous decisions.

Zones and Conduits

Prior to performing the detailed level cyber security risk assessment, zones and conduit drawings need to be developed. These can be developed on a prescriptive basis in a subjective manner using the segmentation and separation requirements documented in ANSI/ISA-62443-3-2 or they can additionally use the results from the initial cyber risk assessment to enhance the decisions made.

Vulnerability and Threats

If a system had no vulnerabilities, it could be considered inherently secure. The reality is that all systems are more or less vulnerable to threats. Together, actual threats and vulnerabilities result in the likelihood of successful exploitation of a vulnerability.

Vulnerabilities

Vulnerabilities can be thought of as flaws or weaknesses in a system's design, implementation, operation or management providing an environment capable of being exploited in a manner that can compromise the system's integrity or security, in turn causing harm. Various

types of vulnerability assessments can be used to identify, quantify, and prioritize (or rank) the vulnerabilities identified in a system.

Threats

Threat sources or agents can be categorized as follows:

- Nation states
- Disgruntled employee or contractor
- Non-malicious employee or contractor human error
- Criminal
- Determined adversary (activist, political, religious)

It is generally assumed that nation states have the most resources and sophistication, however, the dynamic nature of technology is such that differences in capabilities can decrease over time. Each of the threat sources will typically have different motivations for their actions, although some may overlap at times. Their motivations will also have an impact on target attractiveness. A criminal for instance wants to make money, so that will have an impact on the types of consequences that are likely or not. A foreign government may want to steal information, simply establish a presence on the system allowing them to engage in future mischief, or to incur physical harm such as was done with Stuxnet or to the Ukraine power grid. A terrorist will typically want to do physical harm. An important aspect of threat agents is the sub categorization into:

- Insiders
- Outsiders
- Insiders working in collusion with outsiders

The common thought process by IT professionals and network specialists that a robust perimeter to the outside world is sufficient is a flawed assumption. This was shown by the introduction of the Stuxnet virus by an insider working in collusion or unknowingly with an outsider. A disgruntled employee still having access to the system can cause harm from the inside (i.e. below the firewall to the outside) as well.

Consequences

Whenever industrial control systems are utilized, failure to adequately control can result in consequences such as fatalities or impact on health, environmental impacts, and financial impacts due to equipment damage or business interruption. Some of these if severe enough can result in the loss of privilege to operate. Table 1 below provides an example of a consequence severity scale. Actual consequence severity tables such as this are the responsibility of the authority having jurisdiction, typically the operating company as part of a risk matrix that they develop.

When consequences are assessed, they are based on no safeguards or countermeasures being present as this allows the determination of what's known as the unmitigated risk.

	Operational			Financial			HSE		
Category	Outage at one site	Outage at multiple sites	National infrastructure and services	Cost (Million USD)	Legal	Public confidence	People onsite	People offsite	Environment
A (High)	>7 days	>1 day	Impacts multiple sectors or disrupts community services in a major way	>500	Felony criminal offense	Loss of brand image	Fatality	Fatality or major community incident	Citation by regional agency or long-term significant damage over large area
B (Medium)	<2 days	>1 hour	Potential to impact sector at a level beyond the company	>5	Misdemeanor criminal offense	Loss of customer confidence	Loss of work day or major injury	Complaints or local community impact	Citation by local agency
C (Low)	<1 day	<1 hour	Little to no impact to sectors beyond the individual company. Little to no impact on community.	<5	None	None	First aid or recordable injury	No complaints	Small, contained release below reportable limits

Table 1: Example of consequence or severity scale[4]

Tolerable Risk

Risk is based on the hazards a system may be exposed to, the likelihood of those threats arising coupled with the inherent vulnerabilities in the SuC, and the consequences if the SuC were to be compromised. Each organization that owns and operates a control system has its own tolerance for risk. Table 2 provides an example of a risk matrix that can be used to determine if an identified scenario is tolerable. Using the consequence severity from table 1, the unmitigated risk can be determined. If the unmitigated risk is tolerable, then there is no need for further action. By looking at the risk matrix in table 2, the security level target (SL-T) can be determined by the necessary risk reduction to lower the likelihood to a block that represents tolerable risk. This example assumes a nominal order of magnitude improvement in risk reduction for each increase in security level capability. Other risk matrices may be based on more qualitative measures.

Once countermeasures that conform to ANSI/ISA-3-3 are identified that are specific to the threat/vulnerability scenario, the security level capability (SL-C) can be estimated by determining if they are part of the scope. This allows an estimate of likelihood. Table 3 provides an example of a likelihood scale. This one is based on the concept of quantitative risk reduction. Other risk matrices have been created that are more subjective in approach.

		Severity		
		A	B	C
Likelihood	5	High	High	Med-high
	4	High	Med-high	Medium
	3	Med-high	Medium	Med-low
	2	Medium	Med-low	Low
	1	Med-low	Low	Low

Table 2: Example of 3 x 5 risk matrix[4]

With the estimated likelihood, the mitigated risk may be determined. If there is a gap where the SL-C is less than the SL-T, then recommendation(s) should be made to close the gap. Should the SL-C equal or be greater than the SL-T, then it is presumed that no further action is necessary.

Likelihood scale	Guideword	Likelihood description	Frequency-based guidance
1	Certain	Almost certain	$>10^{-1}$ per year (High demand)
2	Likely	Likely to occur	10^{-1} to 10^{-3} per year (Low demand)
3	Possible	Quite possible or not unusual to occur	10^{-3} to 10^{-4} per year
4	Unlikely	Conceivably possible, but very unlikely to occur	10^{-4} to 10^{-5} per year
5	Remote	So unlikely that it can be assumed it will not occur	$<10^{-5}$ per year

Table 3: Example of likelihood scale[4]

Cyber Security Requirements Specification / Mitigation Plan

The Cybersecurity Requirements Specification (CRS) provides a documented basis for detailed design as well as future management of change throughout the system's life within the facility. A good design basis that clearly establishes the zone and conduits, the technical measures needed to establish a SL-C as well as the organizational measures necessary to support the technical measures reduces the potential for cost overruns due to the need for future rework/scope changes during detailed design and beyond. It also supports an effective management of change program. It should be noted that if the organizational measures are not sufficient to support and sustain the technical measures, the technical measure will not be effective and the risk may be greater than what is tolerable.

Green Field Application

As part of a capital project, performance of initial design work assists determination of project cost. Initial development of the cyber security requirements specification (CRS) should begin

to document best estimates of requirements. Following completion of the detailed cyber risk assessment and identification of required countermeasures, finalization of the CRS reflecting the design basis, allows commencement of detailed design work.

The CRS can be a separate document or additional information included as part of requirement specifications, such as the safety requirements specification (SRS) required by other standards that address Safety Instrumented Systems (SIS)[4][8]. The CRS should consolidate all of the cyber security requirements. Any conflicting requirements that may exist between the CRS and SRS need to be resolved in a manner that is commensurate to the company's ultimate risk criteria. It is not one or the other.

Brown Field / Revalidation Applications

It is quite possible that some existing brown field sites were built prior to the recognized need for cyber security risk assessments involving the IACS. In these cases, the essential information needed to conduct a risk assessment needs to be made available and created to the extent it does not exist. As the information is made available, the applicable vulnerability assessments and then the risk assessments need to be conducted using the work process described earlier. This should culminate in a CRS as well.

Once the risk assessment has been performed and a CRS is documented, whether as a result of a capital project or performed on an existing brown field facility, after some period of operation, the hazard review/risk assessment is supposed to be revalidated at a defined interval. With operating experience, the previous risk assessment assumptions can be evaluated versus real performance and to correct and / or update as applicable if non-tolerable risk is determined.

The following activities can assist this risk revalidation assessment:

- Review cybersecurity incidents since last revalidation
- Review cybersecurity related management of changes since last revalidation
- Review current vulnerability assessment and update as applicable
- Review detailed level cybersecurity risk assessment and update as applicable
- Review of key performance indicators that result from audit program
- Address all recommendations resulting from revalidation

Persons knowledgeable in the processes, operations and design under review with at least one person knowledgeable and competent in the assessment methodologies used in the workshops should participate. The membership of the assessment team should include at least one senior competent person not involved in the operation and maintenance.

Risk assessment and CRS documentation should be updated on an ongoing basis as part of the MOC program. Following the risk assessment revalidation, the risk assessment and CRS documentation needs to be updated once again to support a defensible design and operations basis as well as to provide a solid foundation to support future management of change.

Methodologies

To be effective, standards often need to be supported by methodologies that allow implementation of the standard. For example, in functional safety standards such as ISA/IEC 61511 "Functional Safety – Safety Instrumented Systems for the Process Industry Sector" require the performance of a hazard review whereby safety instrumented function and system requirements can be determined. Methodologies not covered in that standard that practitioners use to help in this activity include examples like hazard and operability studies (HAZOP), failure modes and effects analysis (FMEA), and fault tree analysis (FTA).

Likewise, in the field of industrial security, ISA/IEC 62443-3-2 is a standard that needs methodologies separate from the standard to enable its implementation. An overview of various methodologies have been included to support both security vulnerability and cyber security risk assessments where Industrial control systems are being used. Some of these methodologies seem to include both aspects of vulnerability assessment as well as risk assessment and have been referred to as hybrid assessments.

Vulnerability Assessments

In order for a threat to be realized, it is necessary to

exploit one or more vulnerabilities in one or more assets. Understanding what vulnerabilities exist is thus an important input to the performance of a detailed cybersecurity risk analysis. These vulnerabilities help in the identification of threat scenarios during the risk assessment workshop. Vulnerability assessment is best performed prior to convening the risk assessment team to perform their assessment as the composition of the personnel performing those assessments is often quite different than those in the actual risk assessment workshop. Documented below are a number of different types of vulnerability assessments that may be performed.

Device vulnerabilities (hardware, software)

There are two different aspects to device vulnerabilities. The first is to perform a security level capability assessment versus the requirements in ANSI/ISA 62443-4-2. The assessment identifies gaps in device technical capabilities relative to the security level target of the zone where these devices are intended to be deployed by the asset owner. Understanding the capabilities of the equipment help to perform system level assessments based on ANSI/ISA 62443-3-3. Figure 4 provides an excerpt of an example worksheet.

The second type of device vulnerability assessment is the on-going discovery of software flaws that can be exploited. There are numerous sources of information and tools regarding known and common vulnerabilities in IACS, such as the industrial control system computer emergency response team (ICS-CERT) database or CVE databases, which can be used to look up and document existing vulnerabilities for the proposed asset inventory.

Gaps in technical capabilities

Zone and conduit documentation is one of the requirements prior to performing a detailed cyber security risk assessment. One of the outputs from the initial risk assessment can be the assignment of SL-T for both devices and zones. Once a zone has been assigned a SL-T, a vulnerability assessment can be performed to measure the applicable requirements in ANSI/ISA 62443-3-3 versus the technical measures that either exist or are proposed in a design scope. This activity would provide the SL-C for each zone. Figure 5 provides an excerpt of an example worksheet.

Req ID	Pass / Fail	Reference Name	Requirement Description	SL-1	SL-2	SL-3	SL-4	Assessment Notes
FR 1 – Identification and authentication control								
CR 1.1		Human user identification and authentication	Components shall provide the capability to identify and authenticate all human users according to ISA-62443-3-3 SR 1.1 on all interfaces capable of human user access. This capability shall enforce such identification and authentication on all interfaces that provide human user access to the component to support segregation of duties and least privilege in accordance with applicable security policies and procedures. This capability may be provided locally by the component or by integration into a system level identification and authentication system.	Y	Y	Y	Y	
CR 1.1 (1)		Human user identification and authentication	Unique identification and authentica-tion. Components shall provide the capability to uniquely identify and authenticate all human users.		Y	Y	Y	
CR 1.1 (2)		Human user identification and authentication	Multifactor authentication for untrusted interface. Components shall provide the capability to employ multifactor authentication for all human user access to the component.			Y	Y	

Figure 4: Example Device SL-C Assessment

Req ID	Pass / Fail	Reference Name	Requirement Description	SL-1	SL-2	SL-3	SL-4	Assessment Notes
FR 1 – Identification and authentication control								
SR 1.1		Human user identification and authentication	The control system shall provide the capability to identify and authenticate all human users. This capability shall enforce such identification and authentication on all interfaces which provide human user access to the control system to support segregation of duties and least privilege in accordance with applicable security policies and procedures.	Y	Y	Y	Y	
SR 1.1 (1)		Human user identification and authentication	Unique identification and authentication. The control system shall provide the capability to uniquely identify and authenticate all human users.		Y	Y	Y	
CR 1.1 (2)		Human user identification and authentication	Multifactor authentication for untrusted networks. The control system shall provide the capability to employ multifactor authentication for human user access to the control system via an untrusted network.			Y	Y	
CR 1.1 (3)		Human user identification and authentication	Multifactor authentication for all networks. The control system shall provide the capability to employ multifactor authentication for all human user access to the control system.				Y	

Figure 5: Example Zone SL-C Assessment Worksheet

Gaps in procedural capabilities

Technical measures are not effective if the organizational procedures necessary to sustain them are not adequate from either an implementation or an ongoing performance perspective. Once the organizational measures required by the technical measures are known, those organizational measures in place or included within the scope can be compared to ISA 62443-2-1 to determine any gaps. As part of this vulnerability assessment, the maturity level of those procedural measures should also be determined. The general vulnerability assessment procedure is as follows:

1. Document applicable technical measures applicable to all zones
2. Document applicable technical measures applicable as a function of specific zones
3. Document organizational measures (i.e. ANSI/ISA 62443-2-1) and procedures necessary to support specific technical measures. Should those procedures include requirements from ANSI/ISA 62443-2-4, then they must also be considered
4. Assess each organizational measure and procedure for its maturity level
5. Document the results

IACS Network Vulnerability Assessments

As part of the development of architecture drawings, it is generally accepted good practice to conduct an architecture drawing review. During this review meeting, vulnerabilities due to potential segmentation issues are documented. At a minimum, the segmentation requirements within ANSI/ISA 62443-3-2 should be used to determine adherence.

System integration vulnerabilities

System integration vulnerabilities require an integrated system to be in place. This vulnerability assessment type is really a form of testing, analogous to proof testing of safety systems and functions. Integration testing for vulnerabilities may occur as part of factory acceptance testing, site acceptance testing, initial validation or periodic revalidation. These types of tests include but are not limited to:

- Basic Fuzz Testing
- Advanced Fuzz Testing

Req ID	Pass / Fail	Reference Name	Requirement Description	Assessment Notes / Evidence
Element – Security Policies and Procedures				
4.3.2.6.1		Develop security Policies	The organization shall develop high-level cyber security policies for the IACS environment which are approved by management.	
4.3.2.6.2		Develop security procedures	The organization shall develop and approve cyber security procedures, based on the cyber security policies, and provide guidance in how to meet the policies.	
4.3.2.6.3		Maintain consistency between risk management systems	Cyber security policies and procedures that deal with IACS risks should be consistent with or extensions of policies created by other risk management systems.	

Figure 6: Example Organization Capability Worksheet

- Comprehensive Fuzz Testing
- Storm Testing
- Security Requirements Testing
- Known Vulnerability Scan
- Threat Mitigation Testing (Requires the creation of a threat model)
- Binary Scan for Vulnerabilities
- Penetration Testing

It should be noted that most of these tests should not be performed during operating production. Following startup, revalidation testing is normally reserved for periods when the plant is down for maintenance, e.g. a turnaround. Whilst vulnerabilities identified by this test information are not available for cyber security risk assessment during the design phase of a capital project, this testing information is quite valuable input for brown field site initial reviews as well as periodic risk assessment revalidations.

Hybrid Assessments

Site Vulnerability Assessments

Site vulnerability assessments (SVA) are generally performed as part of a regulatory requirement (e.g. 6 CFR part 27: Chemical Facility Anti-Terrorism Standards (CFATS). They are intended to prioritize sites based upon potential risk due to the type and quantity of chemicals on site and to assist in the development of a security plan. When one exists, it will contain information that might be considered an initial cybersecurity risk assessment and should be useful input when conducting the detailed cyber security risk assessment.

Consequence-driven Cyber-informed Engineering (CCE) Methodology

The CCE methodology is a consequence-driven methodology developed at Idaho National Laboratory. It was developed to focus on securing the nation's critical infrastructure systems, which includes industrial control systems. It starts with the assumption that if a critical system is targeted it can and will be sabotaged, i.e. likelihood equal to one.

It is a four-step process consisting of

1. Consequence prioritization,
2. System of systems analysis (similar to partitioning the system into zones and conduits),
3. Consequence-based targeting, and
4. Mitigations and protections.

When one exists, the CCE will contain information that could be considered an initial cybersecurity risk assessment as it does not consider likelihood in its framework. It should provide useful input when conducting the detailed cyber security risk assessment as it does go beyond (e.g. mapping the industrial control system kill chain) what is generally intended to be included in an initial cyber security risk assessment.

Cyber Security Risk Assessments

Asset Focused Cyber Risk Assessments

One asset based cyber risk assessment methodology was described in a paper by Paul Baybutt, *An Asset-Based Approach for Industrial Cyber Security Vulnerability Analysis* [18].

The methodology considers how cyber assets can be exploited by threat agents to do harm. The following provides an overview of this methodology:

1. Preparation and organization
2. Target Analysis (Likelihood that identified critical assets will be attacked)
3. Threat Analysis (Identification of threat agents and purpose/type of threat)
4. Identification of vulnerabilities
5. Identification of consequences
6. Estimation of risks
7. Identification of recommendations
8. Documentation and reporting
9. Follow-up

Although the title of the paper uses the term vulnerability, it is really risk based and can be considered a detailed cyber security risk assessment methodology.

Another asset based methodology is shown in TR84.00.09 2nd Edition [9] based on the paper by Harold Thomas and John Day, *Integrating Cybersecurity Risk Assessments into the Process Safety Management Work Process* [16].

A summary of the procedural steps is included below:

- List cyber assets.
- Identify worst case potential consequences as a function of process/utility area.
- Document potential consequences if asset is compromised.
- Document ease of propagation with open communication.
- Select target security level for each asset category as a function of process/utility area.
- Verify risk criteria are adequate for cyber risk management.

This methodology is an example of an initial cyber risk assessment. Figure 7 provides an example worksheet for the performing and documenting this methodology.

Cyber PHA Methods

Cyber process hazard analyses follow a systematic, safety-oriented methodology to conduct a cyber security risk assessment of an industrial control or safety system. The methodology integrates multiple engineering disciplines, including process safety, industrial automation, industrial IT, and cyber security. It leverages established process safety management methodologies and uses that information to perform a Cyber PHA, using HAZOP like worksheets. It delivers a risk ranked mitigation plan that typically includes both cyber and non-cyber safeguards and countermeasures. It also provides a methodology for meeting the security requirements called out for in the ISA/IEC 61511 standard.

TR84.00.09 2nd edition provides a documented example of a Cyber PHA methodology. A summary of the method is included below:

1. Select a zone
2. Select cyber node, e.g., a cyber asset.
3. Identify and record a cyber threat.
4. Identify and record causes.
5. Identify and record qualitative cause likelihood (without any credit for countermeasures).
6. Identify and record unmitigated consequences (without any credit for countermeasures, e.g. monitoring and detection).
7. Determine and record qualitative severity of unmitigated consequences.
8. Identify and record countermeasures applicable to the cyber threat and cause.
9. Document the security level requirement for the threat vector.
10. Determine and record qualitative likelihood (with existing countermeasures). Note that when countermeasure(s) work, the attack may be prevented or mitigated, i.e. results in consequences that are less severe than the unmitigated consequences.
11. Determine if risk is tolerable per risk criteria. If not make recommendation(s).

Process / utility area	Cyber asset type	Consequence to process / utility area if compromised	Criticality	Security level	Ease of propagation	Recommended response if compromised

Figure 7: Example Asset Based Initial Cyber Risk Assessment Worksheet

The Cyber PHA methodology documented in TR84.00.09 2nd edition is considered a detailed cyber security risk assessment methodology. Ed Marzsel and Jim McGlone wrote a book for ISA titled, *Security PHA Review for Consequence-Based Cybersecurity* [17]. The methodology they documented is a form of Cyber PHA. Its procedure is documented in Figure 8

Although this is a form of Cyber PHA, it does not address likelihood. It does provide a means to assign SL-T in a rigorous manner and should be considered something of a hybrid, i.e. more than an initial risk assessment, but less than a detailed cybersecurity risk assessment. Tweaking the methodology to include likelihood by a user should not be that difficult.

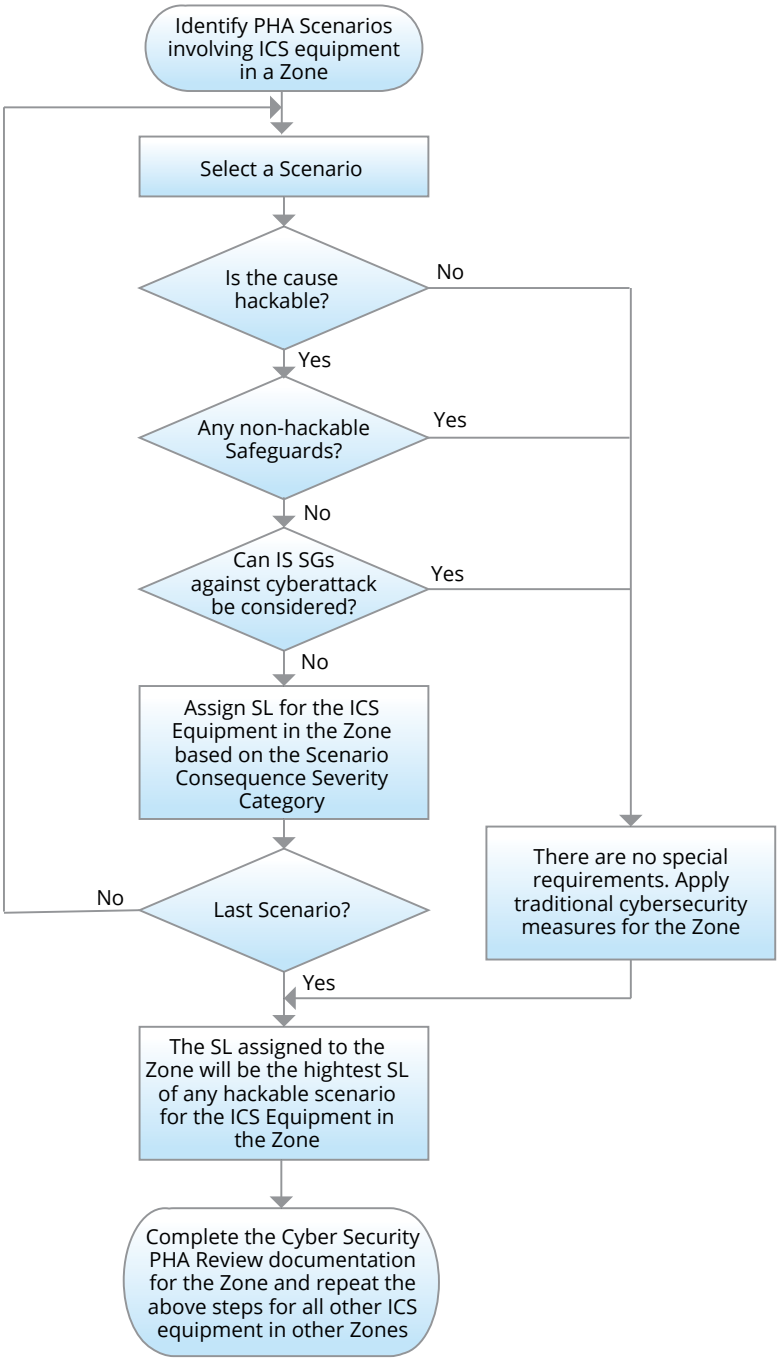

Figure 8: Security PHA Review Procedure

Cyber Kill Chain

Methodologies based on the cyber kill chain look at the chain of events that have to occur for a successful attack. Table 4 illustrates the kill chain progression of activities or phases an attacker would have to take for a targeted malware attack as developed by Lockheed Martin.

By understanding every point in the chain of events of a cyber-attack, an analyst can help focus the efforts on breaking that chain and mitigating the damages. When designing an IACS cybersecurity monitoring program, and in evaluating the combined effectiveness of the countermeasures and associated monitoring activities in deferring a successful attack, it is important to understand where the countermeasures are effective in the attack sequence. ISA TR84.00.09 second edition provides examples of countermeasures as a function of kill chain phase applicability. Use of the kill chain in conjunction with sneak path analysis can be complementary.

A method that is based on the kill chain concept is MITRE ATT&CK® for ICS. It stands for MITRE Adversarial Tactics, Techniques, and Common Knowledge for Industrial Control Systems (ATT&CK). The MITRE ATT&CK® for ICS framework is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's attack lifecycle and the platforms they are known to target. The MITRE ATT&CK® for ICS matrix contains a set of techniques used by adversaries to accomplish a specific objective. Those objectives are categorized as tactics, which are an expansion of the kill chain phases, in the MITRE ATT&CK® for ICS Matrix. The objectives are presented linearly from the point of reconnaissance to the final goal of "impact". The following adversary tactics are categorized as:

1. **Initial Access:** trying to get into your ICS environment, i.e., spear phishing
2. **Execution:** trying the run malicious code, manipulate system functions, parameters, and

Kill Chain Phase [15]	Description
Reconnaissance	Research performed to identify and select target
Weaponization	Means of coupling a Trojan and an exploit designed to accomplish attacker's objective
Delivery	Transmission of the weapon into the targeted system
Exploitation	Attacker's code triggered
Installation	Allows attacker to maintain a presence within the system, e.g., remote access Trojan or backdoor
Command and control	Allows attacker access to the programming / configuration keyboard
Actions on objectives	Attacker can now achieve their objective

Table 4: Cyber Kill Chain Phases

data in an unauthorized way, i.e., running a remote access tool
3. **Persistence:** trying to maintain their foothold, i.e., changing configurations
4. **Privilege Escalation:** trying to gain higher-level permissions, i.e., leveraging a vulnerability to elevate access
5. **Evasion:** trying to avoid being detected, i.e., using trusted processes to hide malware
6. **Discovery:** trying to figure out your environment, i.e., exploring what they can control
7. **Lateral Movement:** moving through your environment, i.e., using legitimate credentials to pivot through multiple systems
8. **Collection:** gathering data of interest to the adversary goal, i.e., accessing data in cloud storage
9. **Command and Control:** communicating with compromised systems to control them, i.e., mimicking normal web traffic to communicate with a victim network
10. **Inhibit Response Function:** trying to prevent your safety, protection, quality assurance, and operator intervention functions from responding to a failure, hazard, or unsafe state.
11. **Impair Process Control:** trying to manipulate, disable, or damage physical control processes.
12. **Impact:** manipulate, interrupt, or destroy systems and data, i.e., encrypting data with ransomware

Within each tactic of the MITRE ATT&CK® for ICS matrix there are adversary techniques, which describe the actual activity carried out by the adversary. Some techniques have sub-techniques that explain how an adversary carries out a specific technique in greater detail.

Sneak Path Analysis

A sneak path methodology was described in a paper by Paul Baybutt, Sneak Path Security Analysis for Industrial Cyber Security [20]. The methodology is used to identify flaws in systems that may result in serious consequences should an attack be successful. The following provides an overview of this methodology:

1. Collection of needed information
2. Development of system topology diagram (e.g. simplified architecture diagram)
3. Identification of sources
4. Identification of targets
5. Identification of paths
6. Identification of events and impacts
7. Identification of barriers
8. Estimation of risks
9. Development of recommendations

Once a path and potential event(s) (i.e. consequences) have been identified, barriers (i.e. countermeasures) are identified that would prevent the attack from continuing via that path. The severity should the attack be successful and the likelihood of being successful are qualitatively documented. The sneak path security analysis is considered a detailed cyber security risk assessment methodology.

Cyber Attack Tree / Event Tree

Cyber-attack trees use Boolean logic through the use of gates in the same manner that fault trees are created. The top gate would be the expression of a successful attack. The gates leading up to the top gate would model demand by threat agents exploiting vulnerabilities AND the failure of countermeasures to prevent or mitigate the demands.

Event trees start with a threat agent with a goal in mind and explores attack success paths, attack mitigated paths and attack prevented paths. ISA TR84.00.09 second edition provides

examples of various cyber event trees of different threat agents with different intended outcomes.

Cyber-attack and event trees are considered a form of an advanced detailed level methodology. They are generally much narrower in their scope and are sometimes used to gain more insight following other techniques such as cyber PHA or kill chain methods.

Bibliography

Regulations

1. 6 CFR part 27: Chemical Facility Anti-Terrorism Standards (CFATS) Risk-Based Performance Standard (RBPS) 8, Cyber.

Published Standards and Technical Reports

2. ANSI/ISA-62443-2-1 (99.02.01)-2009, *Security for Industrial Automation and Control Systems Part 2-1: Establishing an Industrial Automation and Control Systems Security Program.*
3. ANSI/ISA-62443-2-4, *Security for Industrial Automation and Control Systems Part 2-4: Requirements for IACS Solution Providers.*
4. ANSI/ISA-62443-3-2, *Security for industrial automation and control systems Part 3-2: Security risk assessment for system design.*
5. ANSI/ISA 62443-3-3, *Security for industrial automation and control systems Part 3-3: System Security Requirements and Security Levels.*
6. ANSI/ISA-62443-4-2, *Security for Industrial Automation and Control Systems Part 4-2: Technical Security Requirements for IACS Components.*
7. IEC 61508, *Functional safety of electrical/electronic/programmable electronic safety-related systems.*
8. ANSI/ISA 61511, *Functional safety – Safety instrumented systems for the process industry sector.*
9. ISA TR 84.00.09-2017, *Cybersecurity Related to the Functional Safety Lifecycle, 2nd Edition* (3rd edition is work in progress draft).

References

10. NIST Special Publication 800-30, *Guide for Conducting Risk Assessments*, June 2008 version 1.0.
11. NIST Special Publication 800-39, *Managing Information Security Risk – Organization, Mission, and Information System View,* March 2011.
12. Department of Homeland Security, Chemical Security Assessment Tool (CSAT)
13. API 780, *Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries.*
14. API 1164, *Pipeline SCADA Security, 2nd edition,* June 2009.
15. Hutchins, E.M; Cloppert, M. J.; and Rohan, A. M.; *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, Lockheed Martin Corporation.
16. Thomas H. W & Day J.; *Integrating Cyber security Risk Assessments into the Process Safety Management Work Process,* 11th Global Congress on Process Safety, April 2015.
17. Marszal E. M. & McGlone J; *Security PHA Review for Consequence-Based Cybersecurity*, July 30, 2019.
18. Baybutt P.; *An Asset-Based Approach for Industrial Cyber Security Vulnerability Analysis, Process Safety Progress*, p. 220, December 2003, Vol. 22, No. 4.
19. Baybutt P.; *Scenario Based Approach for Industrial Cyber Security Vulnerability Analysis,* p. 220, June 2004.
20. Baybutt P.; *Sneak Path Security Analysis for Industrial Cyber Security,* Intech, p. 56, September 2004, Vol. 51, Issue 9.
21. CCPS, *Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites,* 2003.
22. Cusimano, J. & Rostick, P; *If it isn't secure, it isn't safe,* 14th Global Congress on Process Safety, April 2018.
23. Canadian Communications Security Establishment, TRA-1, *Harmonized Threat and Risk Assessment Methodology,* October 2007.
24. Idaho National Laboratory, INL/EXT-16-39212, *Consequence-driven Cyber-informed Engineering (CCE),* October 18, 2016.

,