Integrating Cybersecurity Risk Assessments Into the Process Safety Management Work Process

Harold W Thomas
Exida LLC
64 North Main Street
Sellersville, PA 18960
thomashw@exida.com

John Day
Air Products & Chemicals, Inc.
7201 Hamilton Blvd
Allentown, PA 18195
dayjd@airproducts.com

Copyright © exida.com LLC 2015

Prepared for Presentation at
American Institute of Chemical Engineers
2015 Spring Meeting
11th Global Congress on Process Safety
Austin, Texas
April 27-30, 2015

UNPUBLISHED

AIChe shall not be responsible for statements or opinions contained in papers or printed in its publications
Integrating Cybersecurity Risk Assessments
Into the Process Safety Management Work Process

Harold W Thomas
Exida LLC
64 North Main Street
Sellersville, PA 18960
thomashw@exida.com

John Day
Air Products & Chemicals, Inc.
7201 Hamilton Blvd
Allentown, PA 18195
DAYJD@airproducts.com

Keywords: Cybersecurity, Process Safety Lifecycle, Risk Assessment, Vulnerability Assessment

Abstract

Cybersecurity is rapidly becoming something that process safety can no longer ignore. It is part of the Chemical Facility Anti-Terrorism Standards (CFATS)[8]. In addition, the President’s Executive Order 13636[6] – “Improving Critical Infrastructure Cybersecurity,” has drawn attention to the need for addressing cybersecurity in our plants as it has been demonstrated that in our new world, they are now a source of potential process safety incident. IEC 61508[2], “Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES)” now has a requirement to address cybersecurity in safety instrumented systems and ANSI/ISA 84.00.01[3], “Functional Safety: Safety Instrumented Systems for the Process Industry Sector” is looking to include this requirement in the next revision. Currently the industry is playing catch up as there tends to be a gap in understanding between information technologists, traditionally responsible for cybersecurity, and the process automation and process safety engineers responsible for keeping our plants safe with help from automated controls and safety instrumented systems. As a result, guidance is being developed, but much of it continues to be a work in progress.

ANSI/ISA-62443-2-1[4], “Establishing an industrial automation and control system security program,” requires a high level risk assessment, a detailed level risk assessment and a cybersecurity vulnerability assessment to be performed. This paper explains the purpose of these risk assessments and where they fit into the process safety management lifecycle. As the entire cybersecurity lifecycle is described, the National Institute of Standards & Technology (NIST) Framework[7] for Improving Critical Infrastructure Cybersecurity is used to better understand the analysis, design/implement, and operate/maintain phases of the lifecycle. As companies have relatively recently begun to understand the need to address the issue of potential cyber-attacks on the process control and protection system, few have a fully implemented work process. Guidance
is provided for existing plants to begin the process and how to fully implement the lifecycle as well as how to approach new projects.

1 Introduction

With the advent of cyber incidents that have specifically targeted control and protection systems, it has become clear that the discipline of process safety needs to consider cybersecurity. Compounding the issue is the gap in understanding between information technologists traditionally responsible for cybersecurity and the process automation and process safety engineers whose control and safety systems are at risk. The need to integrate and reduce this knowledge gap is clear. This paper explains how integration between these disciplines can be accomplished.

Management of Functional safety and Cyber for ICS encompasses many aspects, however this can be illustrated in figure 1 below. Beginning with a new grass roots facility or green field site, each of the major phases are shown and how the process safety work process works in conjunction with cybersecurity, showing the relative interaction of the two lifecycles.

Figure 1: Safety/Cybersecurity Integration

Although this paper will touch upon the full lifecycle, a more in depth focus will be placed on the high level risk assessment, detailed risk assessment and vulnerability assessments. For companies with operating facilities that have previously not considered process safety related cybersecurity, guidance is provided as to how to begin the process of implementing the full lifecycle as a sustainable activity.
Safety and Cyber have similar and co-dependent thought processes throughout the lifecycle. There are specific roles and responsibilities required from Manufactures, Certifying bodies and Owner Operators. Within the roles and responsibilities, specific standards are utilized to manage the lifecycle of products, systems, applications and approaches. Policies, procedures, current industry equipment and software capabilities, level of rigor and useful life attributes all combine to form the basis for cybersecurity management that provides sustainability. This forms a management of functional cybersecurity that is akin to the management of functional safety. The end user is responsible to ensure that the residual risk is commensurate with the level of risk that the business is willing to tolerate.

ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod)[3], Clause 5, Management of functional Safety and Functional Safety Assessment, coupled with Clause 6.2, Safety Life-cycle Structure and Planning are the governing standards for owner operators with respect to safety instrumented systems. A similar approach to industrial control system (ICS) cybersecurity must be taken.

The National Institute for Standards and Technology (NIST) [7] has developed a framework that is the best practice developed for end users to date to aid in the development of the cybersecurity management systems.

The framework developed by NIST can be used to assist users as they develop the analysis, design/implement, and operate/maintain management policies, standards and procedures for the various phases of the lifecycle. It does not provide guidance on how to accomplish the tasks, rather it is an outline of the things that need to be considered coupled with some level of performance criteria. It is divided into five functions; Identify (I), Detect (D), Protect (P), Respond (R), and Recover (R). Functions then have categories that describe specific aspects of the lifecycle that are relevant to the function. Each category has subcategories that describe numerous activities and performance criteria that are related to the category and function. Finally, the framework provides industry references for each subcategory where more detailed information can be found that an end user might find useful when developing their management systems.

2 Assessment (PHA) Phase

2.1 Cybersecurity Assessment Phase Overview

Figure 2 shows the work process flow of an integrated lifecycle. As part of any new project involving process industry hazards, a scope must be formulated. This is just as true for how to address cybersecurity. One of the requirements in ISA/IEC 62443-3-2[5] is to perform a high level cybersecurity risk assessment. Its purpose is to help define what scope needs to be included. Section 2.2 will discuss the high level risk assessment in more depth.

As part of developing the scope, it is essential that zone and conduit drawings be prepared. To cybersecurity, these are like P&IDs to the process world, and form the basis of what is reviewed during a detailed cybersecurity risk assessment.
The traditional process hazard review, including HAZOP, LOPA or other applicable methodologies should be performed prior to the detailed level cybersecurity risk review as required by ISA/IEC 62443-3-2[5]. This sequence allows the traditional review to identify and analyze the major hazards that need to be considered when conducting the detailed level cybersecurity risk assessment. The high level risk assessment will be discussed in more depth in Section 2.3.

Any major risks identified may need a more rigorous evaluation. This can involve traditional consequence analysis techniques and in the future, there will be a push to understand how to apply more quantitative likelihood analysis techniques, keeping in mind that cybersecurity countermeasures degrade via different mechanisms versus the random and systematic mechanisms that have been addressed by safety instrumented systems and functions. Irrespective, a means to ensure the corporate risk criteria is met is required that addresses both likelihood and consequence. If the risk criteria is not met, then additional measures need to be considered until the risk criteria is met. Once the criteria is determined to be achievable, a cybersecurity requirements specification (CSRS) is documented in a similar manner to the safety...
requirements specification (SRS) for safety instrumented system (SIS) and functions (SIF) so detailed design can begin.

2.2 High Level Cyber Risk Assessment

2.2.1 Purpose

According to ANSI/ISA-62443-2-1 [4] the purpose of a high level cyber risk assessment is to help establish scope. For cybersecurity, a determination of the criticality and consideration of how to respond to various assets being compromised is quite useful.

2.2.2 Procedure

To accomplish, a list of all the types of cyber assets that will be used needs to be developed. Typical cyber assets include but are not limited to:

- Business servers
- Historian
- Personal computers
- Engineering work station
- Operator Consoles for Human Machine Interface (HMI)
- Distributed Control System
- Programmable Logic Controller
- Safety Instrumented System Controller
- Smart field instruments
- Printers
- Etc.

Once the list is complete, the next step is to determine two things; what is the criticality if the device were compromised, and second, if compromised, what type of responses are appropriate. What level of response is required depends upon how much risk may exist if the asset is compromised. Typical responses that can be considered include:

- Keep operating and fix when convenient
- Isolate the asset from other assets & quarantine until threat has been removed
- Shutdown the process

Should something like a Historian server be compromised, it would be more appropriate to isolate while the rest of the process continues to operate. However, should it be determined a SIS is compromised, it would be difficult to justify not shutting down the process. A more interesting question comes about should the basic process control system (BPCS) be compromised. If the SIS is still functional, a case can be made to try and fix on line if it can be determined that the threat is not fatal. This last example raises an important point when selecting a control system at the beginning of a project. As the degree of integration between control systems and safety systems increases, there is less latitude as to the potential responses. In addition, as the level of integration increases, common failure resulting from a cyber-attack can lead to a situation where
it is not possible to satisfy corporate risk criteria. Understanding these issues as soon as possible is the best way to minimize the cost and potential schedule impact to a project. When making the determination of what system and level of integration to use, it is advised to reference the 7 core attributes as described in the CCPS Safe & Reliable Instrumented Protection to help make an appropriate decision based on the relative level of risk inherently posed by the process.

With the potential consequences and ease of propagation information documented, each asset should be assigned to a zone and the level of protection recommended to prevent propagation across zones should be established. Using industry recognized and generally accepted good practice as documented in the ANSI/ISA 62443 series of standards should be the starting point. Finally, formal zone and conduit drawings should be developed which can be considered required process safety information input to the detailed cyber risk assessment.

2.2.3 Procedure Summary

- List cyber assets
- Document potential consequences if asset compromised
- Risk rank assets based on potential consequences
- Document ease of propagation with open communication
- Recommend zone location for each asset
- Recommend conduit safeguards for communication between each zone
- Document zone and conduit drawing for use in detailed cyber risk assessment

2.3 Detailed Cyber Risk Assessment

2.3.1 Purpose

A detailed cyber risk assessment is intended to rigorously evaluate the instrument and control system IACS and ensure the proposed design and procedures are capable of satisfying the corporate risk criteria. This paper is recommending a methodology similar to a HAZOP, however, the methodology evaluates cyber nodes that represent the cyber assets that are part of the zone and conduit drawings. Although the concern is with the control and safety systems, the entire plant network including all internet and wireless access points, including 3rd party connections, networks, and devices need to be included as these can be pathways to compromise the IACS.

2.3.2 Methodology Differences

It needs to be understood that the typical process hazard analysis (PHA) has a much greater degree of granularity than a Cyber PHA. In a PHA, individual control loops are considered as potential cause of a hazard whereas in a Cyber PHA, the entire basic process control system would be considered all at once. Non cyber causes are more predictable as the common mode failure of an entire controller would result in all outputs failing the same way, whereas a cyber-attack is insidious as it can cause different outputs to fail so as to result in the worst case consequence.
The final difference is that the PHA will consider safeguards that may or are not vulnerable to cyber-attack, whereas a Cyber PHA generally has no practical means to consider safeguards that are not vulnerable to cyber-attack during the hazard identification portion of the Cyber PHA due to the different levels of granularity of what is being reviewed. For instance, if a control failure resulted in high pressure, a relief valve might be listed as a safeguard in a HAZOP. In a Cyber PHA it is not practical to consider this as it does not look at individual loops, but all of the loops, alarms, interlocks contained in a single BPCS. Once the major hazards have been identified, it would be reasonable to consider some safeguards that are not vulnerable to cyber attack on an exception basis.

2.3.3 Leveraging the PHA

After the traditional PHA has been performed, a further step is to consider whether initiating causes and safeguards are potentially vulnerable to cyber-attack. Those that are not vulnerable do not need to be considered in the cyber risk assessment. For those that are vulnerable, the ultimate consequence should be noted. These consequences can be ranked into appropriate categories to be considered in the detailed cyber risk assessment.

The exercise to determine these consequences of concern can be performed by reviewing the HAZOP or by going through the exercise with the layer of protection analyses (LOPA) if performed. If an adequate level of LOPA has been performed, it is somewhat more efficient to use these as they typically cover the hazards. It is not necessary to evaluate every hazard in a detailed cyber risk assessment as once the BPCS and the SIS are protected against major hazards, they would also be protected against the lesser hazards. Table 1 shows a more detailed procedure to leverage the PHA in this manner.

Table 1: Procedure for Leveraging the PHA

<table>
<thead>
<tr>
<th>Major Procedural Step</th>
<th>Detailed Step</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perform traditional PHA</td>
<td>1. Use company HAZOP / LOPA procedures</td>
<td></td>
</tr>
<tr>
<td>Excerpt high risk Initiating Events</td>
<td>2. Filter worksheet data to only include high risk consequence severities</td>
<td>There is no credit for any safeguards at this point</td>
</tr>
<tr>
<td></td>
<td>3. Export the following data fields:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Initiating event (IE)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Consequence</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Severity</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Safeguards</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• PHA Recommendations</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Comments</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. Sort the report by descending Consequence Severties</td>
<td></td>
</tr>
<tr>
<td>Discard those initiating</td>
<td>5. Review each initiating event.</td>
<td></td>
</tr>
<tr>
<td>Major Procedural Step</td>
<td>Detailed Step</td>
<td>Comments</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------</td>
<td>----------</td>
</tr>
</tbody>
</table>
| events not susceptible to cyber influence | a. If it can be caused by a cyber-attack indicate “yes”  
b. If it is not vulnerable to cyber-attack, indicate “no”  
6. Filter the report to only show those cause consequence pairs that are susceptible to cyber-attack. | |
| Identify safeguards not susceptible to cyber influence | 7. Review the safeguards for remaining initiating events as to susceptibility to cyber-attack  
a. If it can be manipulated by a cyber-attack indicate “yes”  
b. If it is not vulnerable to cyber-attack, indicate “no”  
8. Filter the report to only show those safeguards that are not susceptible to cyber-attack | |
| Perform revised risk ranking | 9. Update likelihood of event in the column of the PHA Data Export template.  
10. Update risk ranking in the column of the PHA Data Export template.  
11. Sort revised worksheet by risk in descending order. | - Only take credit for safeguards not susceptible to cyber-attack  
- Risk ranking is based on likelihood of cyber threat being perpetrated and failure of the safeguards not susceptible to cyber-attack for the specific risk receptor category. |
| Provide sorted worksheet to cyber risk assessment team | | - The risk ranked worksheet is to be used by the cyber risk assessment team to:  
  o Improve estimate of actual consequences and severity.  
  o Achieve improved granularity of risk when credit for cyber safeguards is assessed. |
2.3.4 Risk Assessment Procedure

In preparation for the cyber risk assessment key process safety information needs to be available. This mostly includes what was leveraged from the traditional PHA (Table 1) and the zone and conduit drawings that show:
- Zone location for each cyber assets
- Means of communication protection between zones.

Prior to performing the review, the tool/worksheet being used to conduct the review should be organized to list the zones and assets within each zone. Figure 3 shows a conceptual example taken of a Zone and Conduit drawing using the hierarchy approach from ISA 95.

**Figure 3: Zones & Cyber Nodes**
Excerpted from
CCPS Guidelines for Safe Automation of Chemical Processes \[10\]
(Peer Review Copy)

A HAZOP type approach is recommended to perform the cyber risk assessment. This is a qualitative risk assessment method that identifies potential for cyber-attacks that can cause an incident with the potential to result in harm to human life, the environment, property or loss of operating capability. A summary of the method is included below:
- Select zone
- Select cyber node
- Select threat (smart selections based upon type of cyber-attack)
- Identify & record causes
• Identify & record qualitative cause likelihood (without any credit for counter measures)
• Identify & record consequences (without any credit for counter measures)
• Determine & record qualitative severity of consequences
• Identify & record counter measures applicable to the cyber threat and cause
• Determine & Record qualitative likelihood (with existing counter measures)
• Determine if risk is tolerable per risk criteria. If not make recommendation(s)

Figure 4 shows an example worksheet following review.

**Figure 4: Example Cyber Risk Review Worksheets**
2.3.5 Procedure Summary

In summary, the steps needed to complete the detailed level cyber risk assessment are listed below:

- Determine major hazards vulnerable to cyber-attack from the HAZOP or LOPA
- Document cyber nodes from the zone and conduit drawing
- Perform a Cyber PHA on the zone and conduit drawings
- Make recommendations whenever risk criteria not met

3 Design and Implement Phase

Figure 3 shows the various activities during the design and implement phase. Once the CSRS is provided, an iterative design process between network, IACS, and process safety personnel will take place to ensure that the planned layers of cybersecurity protection including policies, procedures equipment, software capabilities, and level of rigor are appropriate for the cybersecurity performance expectations. Once it has been ascertained that the conceptual design has been validated, detailed design can begin. In parallel with the detailed design, the procedures to test and validate the cyber countermeasures need to be developed.

These test procedures need to support the cyber portion of the factory acceptance test (FAT), the site acceptance test (SAT), pre startup safety review (PSSR) and the initial validation of the
cyber countermeasures. This work parallels and should be conducted as part of the SIS validation during its various stages.

Figure 5: Design & Implement Phase
Prior to start-up, it is a process safety management requirement to perform a Pre Startup Safety Review (PSSR). As part of this PSSR, audit questions to assure the quality assurance of the cyber countermeasures being ready needs to be included as a subset of the overall PSSR.

4 Operate and Maintain Phase

4.1 Purpose

Unlike traditional process safety risks, cybersecurity threats continue to evolve, or new vulnerabilities are discovered, potentially making the countermeasures that have been implemented inadequate to maintain an adequate level of safety relative to the corporate risk criteria. As such, it is the end users responsibility to ensure the continued useful life of the cyber protective system, i.e. its technology currency. Procedures need to be in place to measure performance capability and make improvements should they be determined to be necessary.

4.2 Operation and Maintain Phase Overview

Figure 4 shows the various activities during the operation and maintain phase, beginning with startup. Following this, the plant is operated to make product. Periodically, cybersecurity countermeasures need to be revalidated. This is the equivalent of inspecting and testing safety instrumented systems and functions. Vulnerability assessment techniques are the backbone of this exercise and should have been developed and documented as part of FAT, SAT and initial validation.

Any time there is a management of change, potential impacts on cybersecurity needs to be considered. Just as the PHA needs to be periodically revalidated, this revalidation needs to account for cybersecurity as part of the lifecycle work process. The cybersecurity vulnerability assessment is a key part of this revalidation. Finally, if a portion of the facility is being decommissioned, it is recommended that the full lifecycle be employed to ensure that the remaining plant and equipment are not adversely impacted.
Figure 6: Operation & Maintain Phase

Startup

Operation

Cyber Security
Countermeasure Maintenance
(Mechanical Integrity Program)
(ANSI/ISATR84.00.09)

Required MOC
due to change?

Yes

Vulnerability
Assessment Report
(ISA/IEC 62443.3.2)

No

Periodic Assessment?

Yes

No

Decommission?

Yes

No
4.3 Vulnerability Assessment

A vulnerability assessment is intended to provide a review of the cybersecurity environment for the control and instrumented safety systems at the facility. It identifies vulnerabilities and then develops recommendations for possible improvements. It is best done in concert with a detailed cyber risk assessment per the lifecycle. During a vulnerability assessment, the following is accomplished:

- Existing facility cybersecurity practices and policies reviewed versus current industry practice, including current industry based alerts;
- Control & instrumented safety system network architecture reviewed and validated versus cybersecurity requirements specification (CSRS);
- Sample configuration data for facility network equipment and control system devices is collected and compared against documented expectations;
- Penetration testing is performed when the plant is offline;
- Findings are documented and compared against CSRS and with current industry best practices;
- Gaps that show corporate risk criteria not being met must be further evaluated in accordance with company policies.

5 Getting Started with an Existing Facility

5.1 Purpose

In today’s world, not that many existing facilities have had the benefit of going through the lifecycle as previously described. In this section, the method to implement the lifecycle will be covered.

5.2 Overview

In order to implement the lifecycle, the starting point is during the operation and maintain phase of the lifecycle. A seven step process has been documented in the course titled, 7 Steps to Industrial Control System (ICS) Security\textsuperscript{[9]}. These steps are as follows:

- Perform Vulnerability Assessment
- Develop & document policies and procedures
- Train personnel & contractors
- Segment the network
- Control access to the system
- Harden system components
- Monitor and maintain system security

Figure 5 shows how these 7 steps ultimately allow a facility to ultimately be fully integrated with the lifecycle described above, achieving a sustainable solution.
The first step is to perform a vulnerability assessment. When performed for a facility that has not implemented the lifecycle yet, it is somewhat different than what was described in section 4.3. When the first item performed is the vulnerability assessment, all it can do is test and assess the system versus recognized and generally accepted good engineering practices (RAGAGEP).

Once the vulnerability assessment has been performed, it provides valuable feedback to the company, helping them to develop appropriate policies, standards, and procedures. With the policies, standards, and procedures in place, training for employees and contractors may begin. In addition, segmentation of the network, access control and hardening of the assets can also begin based upon recommendations that come out of the vulnerability assessment.

There is still the need to perform the cyber risk assessment, which in turn, will most likely fine tune initial recommendations that emanated from the vulnerability assessment. After the recommendations have been fully implemented, the plant needs to monitor and maintain the
system security. At this point, the facility should be fully following the lifecycle as described in sections 2, 3 and 4.

6 Conclusion

As described in this paper, the most effective and efficient means to achieve cybersecurity is to adopt a lifecycle approach, addressing analysis or assessment, design and finally operation and maintenance that is fully integrated with the process safety work process. It is only when the purpose built security countermeasure layers augmented with the performance and lifecycle management (NIST Framework\(^7\)) of functional cybersecurity are followed, does an end user have a comprehensive strategy. As part of this lifecycle, it is important to conduct cyber risk assessments and vulnerability assessments. As the effectiveness of cybersecurity countermeasures may degrade over time due to increasing sophistication of the threat, on-going performance measurements and periodic reassessments are essential to meet the performance level and to judge the effective useful life of any cybersecurity system.

For existing facilities that have not had the benefit of the lifecycle, they can begin implementation via performance of a vulnerability assessment against RAGAGEP and recycle back to the beginning of the lifecycle, performing a cyber-risk assessment and fully integrating the cyber and process safety lifecycle work processes.

7 References


[9] exida.com LLC training course; 7 Steps to Industrial Control System (ICS) Security


Additional references not cited: