MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Cybersecurity Consideration in Process Hazard Analysis

Addie Cormier, Christopher Ng
Siemens Energy, Inc.
Process Safety Consulting
Houston, TX 77027
Email: info.ogconsulting.energy@siemens.com

Abstract

Traditional process hazard analysis (PHA), such as Hazard and Operability (HAZOP) studies, typically includes a systematic assessment of initiating events and consequences affecting process facilities. Relationships among initiating events, safeguards, and consequences are evaluated in depth, but such evaluation is generally based on unintentional causes such as human error or some unexpected failure of equipment, instrumentation, controls, or safeguards. As the process industry evolves toward greater reliance on and integration with information technology, it is critical to also consider malicious and intentional disruption of process operations by parties who exploit the enhanced capabilities and integration of modern communication with process controls and operations.

This paper discusses the significance of considering cybersecurity threats during a PHA/HAZOP. A step-by-step and systematic technique is presented to show how a PHA team could assess the vulnerability of a system or facility to potential cyber threats, analyze adequacy of safeguards, and develop necessary countermeasures to resist cyberattacks. A typical refinery or chemical plant can have thousands of signals that are connected to a Distributed Control System (DCS) to ensure safe and smooth process operation. This arrangement could inadvertently present multiple pathways for malicious parties to intervene by manipulating signals or disrupting communications, potentially leading to severe process hazards and consequences such as a fire, explosion and fatality. Not only does incorporating cybersecurity in a PHA/HAZOP help identify the vulnerability of your system or facility, it could also be used to prioritize limited resources to ensure critical vulnerabilities are mitigated in a timely and efficient manner. The application of this technique will be demonstrated using case examples.

Introduction

Process hazard analysis (PHA) is an essential element of process safety management and widely adopted to evaluate systematically the hazards associated with process plant design and operation and to minimize the risks associated with such hazards. Traditional methods such as Hazard and

Operability (HAZOP) and What-If/ Checklists have been successfully applied by using a team based approach to evaluate potential design flaws or deviations from safe design and operational practices as well as to identify initiating events, assess potential consequences of such events, and implement acceptable safeguards or barriers to prevent or mitigate the consequences. Relationships among initiating events, safeguards, and consequences are evaluated in depth, but generally based on unintentional causes such as human error or some unexpected failure of equipment, instrumentation, controls, or safeguards.

As the process industry evolves toward greater reliance on and integration with information technology, it is critical to also consider malicious and intentional disruption of process operations by parties who might exploit the enhanced capabilities and integration of modern communication with process controls and operations.

Attacks using cyber technology on process facilities have been well-publicized, such as the socalled Stuxnet computer worm that might have infected industrial control systems in several countries, impacting plant operations and damaging plant equipment. Another cyberattack using so-called spear-phishing techniques has apparently occurred at a German steel mill, impacting both control and safety instrumented systems and resulting in physical damage to a furnace system. Common types of cyberattacks together with further details on the examples cited above are provided below.

Total costs to companies which are victims of cyberattacks are easily in the billions of dollars per year and are likely under-reported as companies seek to avoid negative publicity and loss of clients or business as well as many companies may not have resources to detect and recover from such attacks, let alone to prevent future attacks.1 Therefore, the impacts of cyberattacks have often been realized but not fully quantified.

A systematic method to integrate cybersecurity analysis as part of a PHA/HAZOP is presented in this paper.

Types of Attack

Cyberattack vulnerability could be traced to the exploitation of various complex network loop holes thus allowing malicious software to penetrate inadequate firewalls or be introduced into a computer network by means of a USB thumb drive. A list of some of the common cyberattack methods is highlighted below.2

- Malware: Code with malicious intent that typically steals data or destroys something on the computer.
- Phishing: Phishing emails include a link that directs the user to a dummy site that will steal a user's information. In some cases, all a user has to do is click on the link.
- Man in the Middle (MITM): Gains access through a non-encrypted wireless access point. They would then have access to all of the control information being transferred between both DCS and equipment.
- Malvertising: Compromise your computer with malicious code that is downloaded to your system when you click on an affected ad.
- Rogue Software: Malware that masquerades as legitimate and necessary security software that will keep your system safe.

- Drive-By Downloads: Through malware on a legitimate website, a program is downloaded to a user's system. It doesn't require any type of action by the user to download.

While it would be unreasonable to expect a typical PHA team to address in detail the vulnerability of a process plant to such cyberattack methods, the team should at a minimum check that such an assessment has been completed (outside of the PHA) and resulting findings adequately resolved. The PHA team could also check that a cybersecurity program has been implemented at the site, consistent with current industry best practices, such as the ISA/IEC 62443 series and particularly ISA/IEC 62443-3-2 standard (Security Risk Assessment and System Design) 3 which is pending ballot/ release.
Such assessment would include an extensive mapping of the control system network architecture, detailing how control and communication functions are implemented between the DCS and field devices such process sensors and actuators for control valves. In addition, communication links between the control system and the network or workstation operating system environment as well as with the business enterprise software and the outside world (through the internet) are mapped as well and then partitioned into zones with conduits allowing for communication between zones based on the type and criticality of function, access control, etc. Target security risk levels are assigned for each zone, and appropriate safeguards implemented to ensure target levels are met.

1. Case Study Malware Attack: The Stuxnet Virus Centrifuge Breach
   The Stuxnet was introduced by the infection of a computer and propagated to all other connected machines running Microsoft Windows. Stuxnet was a malicious worm virus.

   The virus apparently compromised the target systems at the Iranian Natanz nuclear plant and took control of the centrifuges, misleading operations by overriding the process variables and giving false feedback to the outside controllers (alarm and automatic safety shutdown system) and thus reportedly caused the impacted centrifuges to spin outside their safety operating limits and to fail eventually.

   Later, a separate operating company confirmed a potential Stuxnet virus breach on its machines, indicating the virus might have inadvertently spread beyond its intended target (Natanz plant) possibly due to a programming error and thus allowing the worm to spread from an engineer's infected computer to the internet. 4

2. Case Study Spear-Phishing Attack: Steel Mill Furnace Breach
   Germany's Federal Office for Information Security (or BSI), indicated the attackers gained access to a steel mill through its business network and then worked their way into the production network, gaining access to the control systems for plant equipment. 5 This type of attack is known as "Jumping" where the intrusion is in one area of the company's network but then jump to another. The breach was in the business network but leaped to the production network. The attack reportedly resulted in loss of shutdown control on one of the blast furnaces and physical damage to equipment.

As experts, in the cyber world, race to keep up with the evolving nature of the attacks, hackers are constantly deploying new ways to infiltrate and cause harm or damage. Beyond implementing robust information technology (IT) practices to detect and ward off malicious

software as well as recover from such attacks, it is also important to raise organizational awareness, identify vulnerabilities, and develop effective countermeasures by using all other available tools.

The PHA process lends itself well as an effective tool to support such efforts. By systematically evaluating the hazards associated with each section of the facility, the PHA team should already have a well-documented understanding of the type of consequences for various initiating events and the effectiveness of available safeguards. Historically, PHA's have been focused on preventing and mitigating consequences categorized usually in terms of safety, asset damage/business interruption, environment, and reputation. Cyberattacks have the potential to inflict any of such consequences, and traditional PHA's could be leveraged to help minimize them.

A traditional PHA team is comprised of representatives from different areas such as operations, engineering (different disciplines), and management who collectively review and discuss what could go wrong at a process plant and how to prevent the associated consequences. Equipped with the right mix of skillset among the PHA team members, the team should be able to recognize what types of initiating events are relevant to the undesirable consequences to be prevented and what safeguards would be considered effective. Using a typical nodal approach, the PHA team would evaluate each section of the plant systematically in this context and develop recommendations for improvement as needed.

Taking a step further, the PHA team could include an assessment of cybersecurity threats and vulnerabilities, their potential consequences, and safeguards under consideration. With qualified Instrumentation and Control (I&C) and Information Technology (IT) subject matter experts participating in the PHA's, weak points in the control and communication systems that might be exploited by hackers to gain access and cause harm could be identified and eliminated. A couple of general approaches are presented below.

General Approach

There are two general methods to perform a PHA integrated cybersecurity assessment.

- The first method is used to assess the basic process control system (BPCS) vulnerabilities as an independent node, such as by means of a Control Systems Hazard and Operability Study (CHAZOP) which could be extended to cover cybersecurity vulnerability.

This method controls the cyber risk through process controls network (PCN). For example, instrumentation or process measurements which are attached to the Distributed Control System (DCS) may be vulnerable to an attack, such as the MITM type of attack as reportedly deployed with the Stuxnet virus. For critical applications, emergency shutdown systems involving dedicated sensors, logic solver, final control elements, and communication pathways which are independent of the BPCS might be warranted such as those typically implemented as part of a Safety Instrumented Function (SIF) or automated Emergency Shutdown (ESD) system.

- The second method, based on an integrated cyber process hazard analysis, could also be used to assess the process system cyber vulnerabilities by integrating with a typical PHA and is applied to control the cyber risk by implementing non-hackable countermeasures.

The second method, integrated cyber process hazard analysis, will be described further in this paper. Adding cybersecurity analysis to a typical PHA requires a step by step systematic technique in the review of the cyberattack impacts and countermeasures. This approach could also be used as a "stand alone" or backup to the first method. If the BPCS is compromised, applications that have been reviewed using integrated cyber process hazard analysis method could lessen the overall risk impact.

This method considers the initiating event and safeguards to determine if they can be hacked and if the consequence is ranked significant. If so, the Process Hazard Team could specify instrumentation plus other mechanisms required to mitigate similar gaps using devices that could not be hacked. Device and instrumentation such as pressure safety valve (PSV), level gauges, pressure and temperature indicators that are not integrated into the DCS system and Operations External Monitoring could provide useful back-ups in the event of cyberattacks.

Table 1 shows an application of integrated cyber process hazard analysis. The initiating event is related to a pressure control valve located at the inlet of a pressure vessel and which could fail wide-open. Such failure would have been evaluated in a traditional PHA as possibly caused by mechanical or electrical malfunction. However, one could also observe that the operation of this control valve could also be vulnerable to cyberattack.

The Risk Ranking (RR) before safeguard consideration is an overall 6 based on severity level of 3 and likelihood level of 2. Based on the risk matrix used for this example, a scenario with an RR of 6 can continue to operate only if safeguards are in place to prevent personnel injury.

One might be tempted to take credit for a local pressure indicator/ gauge as a safeguard (SG). While this indicator is not vulnerable to cyberattack, it would require timely and reliable human intervention to be considered effective. The PHA team concluded that such instrumentation even together with human intervention would not be considered an acceptable safeguard as the indicator is not continuously monitored. Similarly, a pressure transmitter and its associated high-pressure alarm PAH-002, even if independent of the process control loop for the PCV-001 and continuously monitored, would also not be reliable as the pressure signal could be vulnerable to manipulation during a cyberattack.

A recommendation was then developed to install an adequately sized PSV to be routed to a safe location. Note that this PSV would not be vulnerable to cyberattack as its opening behavior is dependent on the vessel operating pressure as well as on the closing force exerted by the spring of the PSV.

Table 1: Example of Cyber Integrated

More Flow						Cyber Vulnerable?		Recommendations
Initiating Event (I.E)	Consequence	Risk			Safeguards (SG)	I.E.	SG	
		S	L	RR				
Pressure Control Valve (PCV-001) at inlet of Vessel V-101 fails wide-open due to mechanical/ electrical malfunction or possibly due to cyberattack creating an erroneous signal to force the valve open.	Potential overpressure of Vessel V-101 due to high upstream pressure source, resulting in release/ spill and loss of downstream feed.	3	2	6	Pressure Indicator (P-001) with Operator Intervention	Y	N	Team concurred that P-001 or PAH-002 would not be considered an acceptable safeguard. Therefore, the Team recommends installing an adequately sized PSV to be routed to a safe location.
					PAH-002 (High Pressure Alarm) with Operator Intervention	Y	Y	

While defending against all forms of cyber intrusion into the plant control system and operation is the ultimate goal, the integrated cyber PHA is also well-positioned to help plant personnel identify critical cyber vulnerabilities that could potentially expose the company to the most severe consequences with associated risk that might fail to meet the company's acceptance criteria and thus prioritize the allocation of scarce resources to enhance protection.

Safeguards

Performing an integrated cyber PHA requires one to control threats, vulnerabilities, and consequences. In order for a typical cyberattack to propagate from initiation to completion, it would typically require that both the initiating event and the safeguard(s) both be hackable. By making at least one of these two be non-hackable, the risk would substantially be reduced. By making both be non-hackable, the risk would be eliminated. For example, can a USB port be used to compromise the system? Then the first order of controls is to deactivate the ports. This would eliminate a conduit whereby the virus could intentionally or inadvertently be introduced into the system. Table 2 is an example of a Cyber Vulnerability Matrix that can be used during an integrated cyber PHA to assess system cyber weaknesses.

Table 2: Cyber Vulnerability Matrix

	Case 1	Case 2	Case 3	Case 4
Initiating Event Hackable?	N	Y	N	Y
Available Safeguards Hackable?	N	N	Y	Y
Likelihood of Consequence	N/A	Unlikely	Unlikely	Likely
Require Non-hackable Safeguard?	N	N	Decide based on risk tolerance	Likely

Note: N=No and Y=Yes

By understanding the different types of cyber threats that a process could be exposed to, one could then fully comprehend the in-place risks and develop effective mitigations to reduce or eliminate the risk. Staff training on cybersecurity awareness is essential to the understanding of cyber threats and safeguarding against them. Integrated cyber PHA could be used to enhance both awareness and readiness of plant personnel against cyber threats.

Table 3 contains examples of safeguards that would be resistant to cyberattack for different scenarios. To the extent that one could rely on devices that operate independently of the control system, common mode failure could be avoided. For example, a spring-operated PSV would relieve excess system pressure without relying on a signal from the DCS.

In terms of designing safeguards, there is a well-established concept called "defense-in-depth" which includes multiple independent layers of protection to protect against process hazards. In the context of cyberattacks, such layers might include but not limited to company policies and operating procedures, personnel training, network compartmentation, access restriction, physical barriers, installing software patches for operating systems, running up-to-date antivirus software, and continuous system monitoring to detect and contain intrusion.

With regards to SIS, IEC 61511 (Functional Safety: Safety Instrumented Systems for the Process Industry Sector) 6 has implemented a new clause, requiring that a security risk assessment shall be carried out to identify the security vulnerabilities of the SIS. The PHA team could also check if this is being implemented for installed SIS.

Table 3: Examples of Cyber Secure

Scenario	Cyber Secure Instrumentation	Cautionary Remarks
Overpressure due to blocked outlet	Pressure Safety Valve (PSV)	Ensure appropriate design and sizing of PSV
BPCS failure	1. Safety Instrument System 2. Analog Back-up	Ensure SIS is independent of the BPCS.
Rotating equipment failure	Mechanical Overspeed Control/ Trip	Routine maintenance
Reverse Flow due to Pump or Compressor Failure	Non-return Check Valve	Routine maintenance
Critical (Shutdown) Valves	Back-up Hand Valve	Routine maintenance
Area H2S Monitor Failure	Back-up Personal Monitors	Routine maintenance
Level Alarm or Transmitter Failure	Level Gauge on Tank or Vessel	Routine maintenance and Operator rounds

Conclusion

Ultimately, the integrated cyber PHA results could help determine what countermeasures would be needed to lessen the cyberattack risks. In additional, the PHA along with a Layer of Protection Analysis (LOPA) could help with prioritizing resources for implementing required countermeasures. If the risk for a particular cyberattack is not considered significant, then it could be protected by using standard safeguards. However if a scenario has signification

consequences or risks and all safeguards could be compromised, the application would likely need at least one cyberattack resistant safeguard. Since the timing or type of a cyberattack cannot be fully predicted, the integrated cyber PHA could serve as a useful tool to reduce the overall risk profile of a process plant against such attacks.

References

1. Fernandez, I. (2013) “Cybersecurity for Industrial Automation & Control Environments, Protection and Prevention Strategies in the Face of Growing Threats”
2. Sullivan, M. "8 Types of Cyber Attacks Your Business Needs to Avoid”, quickbooks.intuit.com
3. ISA/IEC 62443-3-2 standard (Security Risk Assessment and System Design)
4. Kushner, D. (2013) “The Real Story of Stuxnet”, spectrum.ieee.org
5. Zetter, K. (2015) “A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever”, www.wired.com
6. IEC 61511 (Functional Safety: Safety Instrumented Systems for the Process Industry Sector)