Integrating Industrial Control System (ICS) Cybersecurity with Process Safety Management

Why modern process safety programs must incorporate ICS security assessments

John Cusimano, CISSP, GICSP, CFSE
Director of Industrial Cybersecurity
john.cusimano@aesolns.com
aeSolutions

Paul Gruhn, P.E., CFSE
Global Functional Safety Consultant
paul.gruhn@aesolns.com
aeSolutions

Abstract
The majority of process plants today are controlled and operated by automation systems built on Ethernet TCP/IP networks and legacy Microsoft operating systems. These systems are vulnerable to cyber security breaches resulting in potentially significant risks. Standards have been developed on how to assess and mitigate cyber risks to these systems. This paper provides an introductory summary of these topics.

Process safety & industrial cybersecurity are tightly coupled
Figure 1 will be familiar to people involved with process safety, control systems, and safety instrumented systems. It helps explain why process safety and industrial cybersecurity are so tightly coupled.
Figure 1: Layers of Protection

Figure 1 shows the different systems used to protect hazardous processes, including basic process control systems (BPCS), process alarms, safety instrumented systems (SIS), overpressure protection, dikes, and more. Process control systems often consist of either a Distributed Control System (DCS), or Supervisory Control and Data Acquisition (SCADA) system. These systems are responsible for both controlling the process as well as providing alarms to operators. Safety instrumented systems have traditionally been completely separate systems. These are dormant, passive systems designed to detect an abnormal condition (meaning the control system has failed), and bring the process and/or equipment to a safe state (usually shutting things down).

However, modern control systems tend to be integrated with the safety systems, some more tightly than others, and they are often supplied by a single vendor. Some vendors provide control and safety platforms using diverse hardware and software. Some vendors provide them using similar or even the same hardware and software. These are intelligent, microprocessor based systems programmed using computers running Windows operating systems. They are also monitored and operated using computers running Windows operating systems. Control and safety systems often reside on the same process control network. That process control network often has other computers and monitors connected to it and will typically interface with the enterprise network. The enterprise network will often interface with the Internet.

What if a malicious actor or malicious code were able to enter and compromise the control system? This could result in a loss of both control and alarm layers. Values in both layers could be manipulated if they were to reside in the same system. An even worse scenario would be if the malicious code were also to compromise the safety instrumented system. In this scenario an attack could result in the loss of three layers of protection based on a single initiating event or attack. Such attacks have happened.

Unfortunately, traditional hazard and operability studies (HAZOPs) and layer of protection analysis (LOPAs) do not account for the cyber compromise of these layers of protection.

Regulations and standards have been developed

Fortunately there is help available now. Many standards and regulations have been developed over the last decade to address this known issue; our control systems are susceptible to cyber compromise. Agencies such as the North American Electric Reliability Corporation (NERC), the International Society of Automation (ISA), the American Petroleum Institute (API), National Institute of Standards and Technology (NIST), the International Electrotechnical Commission (IEC), and others have developed numerous documents describing the need to protect control systems from cyber attacks, as well as how to do it.

Process safety standards are also now beginning to require cyber vulnerability and risk assessments. The second edition of IEC 61511 (Functional Safety: Safety Instrumented Systems for the Process Industry Sector) is expected to be released in the summer of 2016. One new clause states that a security risk assessment shall be carried out to identify the security vulnerabilities of the SIS. Another clause states
the design of the SIS shall provide the necessary resilience against the identified security risks. That’s as far as the new standard goes, but it does provide further guidance by pointing readers to an ISA 84 technical report and the ISA/IEC 62443-3-2 standard (Security Risk Assessment and System Design) which covers how to perform cyber vulnerability and risk assessments.

ICS cybersecurity vulnerability assessment

So what is an ICS cybersecurity vulnerability assessment? It is an evaluation of a control system’s design. In a brownfield design we need to start with the control system as-built or as-found drawings. An example is shown in Figure 2.

How is that control system constructed? What devices make up the system? How are they networked together? How do those networks communicate with one another? Modern control systems are based on Ethernet networking and Microsoft operating systems. We need to understand how all these pieces go together. Unfortunately, in many facilities it is very difficult to find a drawing that shows the entire system architecture; these systems have often grown and evolved over decades.

We start with an analysis of network communications. We want to understand how these networks are constructed, how they are configured, and how data is moving throughout the system. This is done by recording actual network traffic and plotting it out so we can see the data flows. We can identify what devices are communicating with each other. What devices should be communicating with each other? What devices are communicating with each other that perhaps should not be, or were not expected to be? Are any devices communicating using protocols we did not expect to find? Are there control system devices that are trying to communicate out to the Internet? We plot the communications and look for anomalous behaviors.

A vulnerability assessment would then go on to analyze the actual servers and workstations that make up the system. Most of the operating systems that are controlling the bulk of industrial facilities today...
are legacy Microsoft platforms such as XP and Windows Server 2003. We need to identify vulnerabilities. We also need to look at the control devices themselves, the programmable logic controllers, the safety instrumented systems, the operator interfaces, the variable frequency drives, the analyzers, etc. Most of these devices now have Ethernet ports and are connected to common networks that make up the control system network.

The next step in a vulnerability assessment would be to partition the system into zones and conduits, as shown in Figure 3. We do this so we can better analyze the system and better design protections to limit communications to only that which needs to go into and out of a zone.

A vulnerability assessment should also include a review of policies and procedures and include a gap analysis. How does the system stack up against industry standards and best practices? Finally, the assessment should list the vulnerabilities that have been discovered and the recommended mitigations to close the gaps.

ICS cybersecurity risk assessment

Understanding vulnerability is only one part of the equation. Cyber risk is a combination of threats, vulnerabilities, and consequences. Most organizations want to understand what the true cyber risks are. A method has been developed to do so; it’s called a cyber risk assessment or cyber PHA (process hazards analysis). It’s a very systematic approach similar in many ways to a PHA or HAZOP. The actual process is documented in the IEC 62443-3-2 standard. The method has been applied many times within companies following the process safety management of highly hazardous chemicals regulation (29 CFR 1910.119). The method works quite well because it’s very similar in nature to a HAZOP, a technique that has been used in industry for more than 40 years. An example of a cyber risk assessment study excerpt is shown in Figure 4.

Instead of the traditional ‘causes’, what we are looking for here are ‘threats’. We also consider vulnerabilities and consequences. We use the same risk matrix used in ranking other risks within the organization. Performing such a study helps us prioritize activities and resources, helps designers

Figure 3: Zones and Conduits

©2016 aeSolutions

Cusimano & Gruhn
Integrating ICS Cybersecurity & PSM

April 18, 2016
Page 4
intelligently design and apply countermeasures, and helps document and justify decisions. A cyber risk assessment will document why certain controls were put in place, and sometimes why they were not put in place. This can also be a very effective training and awareness exercise. Like HAZOPs, these studies require a multi-disciplinary team. There needs to be people from IT (information technology), operations, engineering, and automation to work together and study the system. Following the process the team will ultimately develop a risk register and risk profile, so we can have a ranked set of risks, and understand where those risks are in our system. Ultimately, we can then come up with a set of recommendations and a plan to mitigate those risks.

Author bios

John Cusimano is the Director of Industrial Cybersecurity with aeSolutions. John has over 20 years of experience and has performed many control system cybersecurity vulnerability and cyber risk assessments. He is a member of the International Society of Automation (ISA) and is a voting member of the ISA 99 cybersecurity standards committee. As part of that committee, he is the chair of the zones and conduits working group, and co-chair of the product development working group. He is the developer and primary instructor of the ISA courses on cybersecurity. John is a Certified Functional Safety Expert (CFSE), a Certified Information Systems Security Professional (CISSP), and a Global Industrial Cyber Security Professional (GICSP). John has a B.S. in Electrical and Computer Engineering from Clarkson University in New York.

Paul Gruhn is a Global Functional Safety Consultant with aeSolutions. Paul is an International Society of Automation (ISA) Life Fellow, a 25+ year member of the ISA 84 standard committee (on safety instrumented systems), the developer and instructor of ISA courses on safety systems, the author of two ISA textbooks, and the developer of the first commercial safety system software modeling program. Paul has a B.S. degree in Mechanical Engineering from Illinois Institute of Technology, is a licensed Professional Engineer (P.E.) in Texas, and both a Certified Functional Safety Expert (CFSE) and an ISA 84 Safety Instrumented Systems Expert.