Originally appeared in:
July 2016, pgs 55-58.
Used with permission.

HYDROCARBON PROCESSING®

HP | Process Control and Instrumentation

T. AYRAL, Honeywell Industrial Cyber Security, Woodland Hills, California; and **J. O'DONNELL,** Honeywell Industrial Cyber Security, Houston, Texas

Minimize industrial cyber security risk in plants in 12 steps

Most companies and plants have taken steps to implement some degree of industrial cyber security control. However, new industrial cyber security threats and vulnerabilities appear on a daily basis and can quickly undermine the effectiveness of established cyber security countermeasures. Companies cannot predict when or how a facility might be attacked, but they can assess the risk of different threat scenarios. By implementing the 12 steps described in this article, plant managers can take a proactive approach to staying ahead in this dynamic and perilous environment.

An industrial process control system (PCS) typically includes routers, switches, controllers and Windows-based servers and workstations, all communicating on the process control network (PCN). It is critical to monitor the PCN and all attached devices for cyber security threats and vulnerabilities. A single device that is compromised on a PCN can be used as a jump point to access, modify or shut down multiple nodes. If PCS security is compromised, plant processes and production can be affected, with possibly disastrous consequences.

In this article, differentiators between industrial cyber security and general information technology (IT) cyber security are described. Consequences of an attack in a production facility are compared to those from a general IT attack. A well-documented industrial cyber security attack (Stuxnet) is described, proving that "a successful industrial cyber security attack has already occurred."

Well-established industrial cyber security risk management methodologies have been defined by standards, including ISA99/IEC 62443 and ISO 27005, and the steps described in this article are in accordance with them. A proposed cyber security risk management software solution used by plant engineers to monitor industrial cyber security threats, vulnerabilities and risks is described. Additionally, an explanation is provided about how the solution calculates metrics.

Differentiating between industrial and general IT cyber security. Industrial cyber security protects against cyber attacks that assault industrial control systems, which monitor and control production and processing plants by ultimately controlling the positions and percentage open of valves; the amperage of heaters and transformers; the revolutions per minute (rpm) and speed of pumps; centrifuges and motors; and temperatures of reactors, among others. The consequences of an industrial cyber security attack might involve loss of production, destruction of production plants and facilities, death and injury of employees, explosions and the release of poisonous gases or smoke causing injury and death to non-employees or civilians, environmental impact, government fines, damage to corporate reputation and loss of confidence by investors and customers.

General IT cyber security protects against cyber attacks that compromise IT systems, where the consequences might involve the loss of intellectual property (designs, formulas, etc.), databases (credit card numbers, personal data, medical records, etc.) or loss of operation (shutdown of a website resulting in loss of sales orders and client service).

Consequences of industrial cyber attacks. A recent study[1] described that the mean number of days to resolve cyber attacks is 46, with an average cost of $21,155/day, or a total cost of $973,130 over the 46-day remediation period. This cost is estimated primarily for general IT cyber attacks. The consequences resulting from general IT cyber attacks and industrial cyber attacks on industrial control systems and production sites may result in dollar consequences hundreds or thousands of times higher than the consequences of a general attack. For this reason, these types of attacks, as documented above, should be differentiated.

Two examples of recent process incidents—not caused by cyber attacks, but providing typical costs of these types of industrial incidents that could be the result of industrial cyber attacks in production facilities—are described:

- A 2012 fire in a San Francisco, California-area refinery. The associated costs of this refinery fire included crude unit repairs, state and city fines, payments to affected community members and local government agencies exceeding $12 MM, and a loss of crude processing in excess of 100 Mbpd for over six months. Using a conservative refinery processing margin for lost

production, and summing these other costs, yields a conservative total incident cost estimate in excess of $100 MM.

- A gas company explosion in California.[2] The California regulator fined this gas company $1.6 B for a 2010 explosion that killed eight people.

Stuxnet: Proof that industrial cyber attacks are possible. The 2010 Stuxnet industrial cyber attack has been well-documented, and it proved that malware can override industrial control systems and fool plant operators into believing the process is operating normally, when in reality it is operating far outside of acceptable limits. Stuxnet propagated itself until it found the designated target, a PLC control system. The malware was introduced by USB flash drives. Stuxnet fooled plant operators by overriding the actual process variables to show "normal values" in the control system displays. It appears that no alarms or automatic safety shutdown systems and events occurred, so the operators were unaware that the centrifuge process was tearing apart.

Steps to reduce attack risk. For the nodes, endpoints, workstations, computers and servers on the industrial process control network, the following 12 steps should be performed to minimize the risk of an industrial cyber security attack:

1. Complete all control system software backups as recommended, according to schedules provided by manufacturers.
2. Install and properly configure firewalls.
3. Apply all industrial control system critical software patches as soon as possible, and use mitigating controls to protect systems between maintenance and patch cycles.
4. Update anti-malware/anti-virus (AV) software and virus definitions (DAT files).
5. Install application whitelisting technology that permits the execution of only good or known files. This is accomplished by creating a list of approved files and allowing only them to execute.
6. Install an automatic method to track and inventory assets or nodes on the control system network, including infrastructure devices, personal computers and servers.
7. Install a method to automatically detect "dark devices" or "rogue devices" (i.e., control system assets or nodes that communicate on the network but are not monitored for cyber risk). These may include removable media brought onto the site, such as USB drives and CD/DVDs, as well as laptops and smart phones.
8. Train company employees about industrial control system security, including the importance of password controls and awareness of social engineering attacks. The percentage of policy violations and security incidents detected should be automatically tracked.
9. Automatically monitor the plant's and PCN's status on important industrial cyber security metrics and show how its security posture is improving.
10. Monitor the percentage of control system hardware, nodes and endpoints free of detected malware and viruses.
11. Automatically estimate the overall vulnerability in the control system hardware, nodes and endpoints, and know whether the number is decreasing.
12. Have an automatic method that points to the source of a cyber threat. This may include connections between the corporate IT network and the industrial process control network.[3]

Plant process control engineers can quickly and easily track their cyber security risk profile on a daily basis, so no head count increase is required.

Software to monitor security risks. The ability to quickly monitor the metrics associated with these 12 steps and recognize how they are changing with time is crucial to the success of industrial cyber security. A solution has been developed to monitor industrial cyber security risks, vulnerabilities and threats.

Dials and trends are used to show the immediate and varying status of risks. Notifications explain and point to warnings and errors from inputs. Drilldown capability allows plant engineers to determine the exact node, endpoint, server, device or computer causing the alert or warning. Changes in site trend and site risk indicate whether the site's cyber security risk is improving or worsening. Standardized reports can be prepared showing key industrial cyber security metrics (**FIG. 1**).

Plant employees do not need to be industrial cyber security experts to monitor and minimize the plant's risk. Plant process control engineers can quickly and easily track their cyber security risk profile on a daily basis, so no head count increase is required.

When a cyber attack occurs, plant control engineers receive e-mail alerts and can identify and prioritize system security risks. They can drill down to the problem and make quick logical decisions with minimal effort, as well as assess the plant and PCN's cyber security posture on a daily or more frequent basis.

Risk trend. The "risk trend" on the dashboard shows the total cyber security risk across the entire site over time, whether it is increasing or decreasing, and if there are any patterns. This function is extremely important, as cyber security risk is most relevant when viewed in context: a very high risk score of 90 is bad, but if the risk score has been 100 for months, a reduction to 90 is positive. Trends reflect "risk appetite" and "risk tolerance" for that particular site. Risk appetite is the amount and type of risk an organization is willing to accept in pursuit of its business objectives. Risk tolerance is the specific maximum risk an organization is willing to take regarding each relevant risk.

Patches risk. At a regular time interval, for each endpoint/node on the industrial process control network, a list of all secure

patches is prepared. This list is sometimes referred to as a vendor patch capability (VPC) file. The risk management software validates the existing patches on all possible nodes and calculates the patch risk level value between 0% and 100%, based upon a patented algorithm. Some of the factors used in the algorithm include:

- The percentage of nodes missing one or more software patches
- The criticality of those nodes to the operation of the facility and the consequences that would result from an industrial cyber security attack (i.e., a chemical reactor would probably be more critical than a water cooling area)
- The general criticality of those nodes (i.e., a server is more critical than a workstation)
- The location of the controlled area in proximity to other, more critical zones—i.e. adjacent risk.

Adjacent risk refers to risk causes that originate from other devices in the system. Risk adjacency is used to track how risk can impact other devices in an interconnected system, such as a distributed control system (DCS). The risk adjacency algorithms are complex, and there are several patents defining them.

The most important aspects of a cyber security program are identifying security risks, being proactive, embracing a security philosophy and developing a long-term strategy that eliminates (or reduces) potential cyber security threats.

To protect systems and networks, industrial facilities require a comprehensive approach to cyber security that involves ongoing risk assessment, well-defined security policies and an aggressive overall security posture. Vigilance must be maintained, as the consequences of cyber attacks on critical infrastructure are too great to ignore. HP

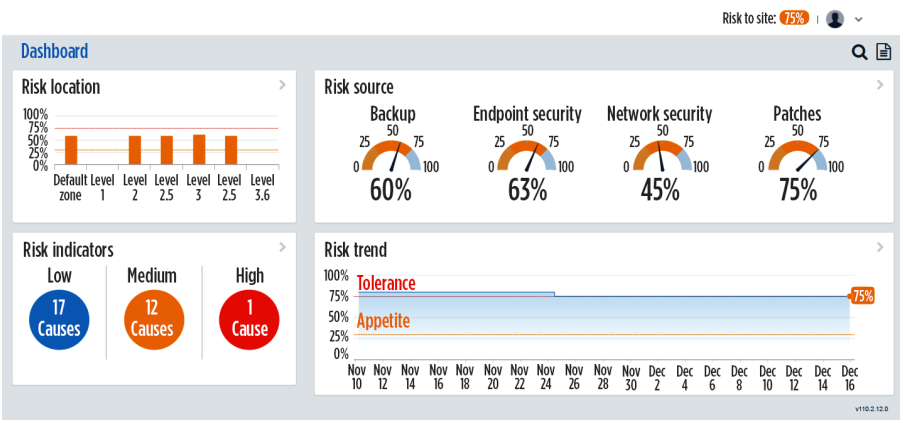

FIG. 1. An example of a software solution that proactively monitors, measures and manages cyber security risk for industrial plants and systems.

LITERATURE CITED

[1] Ponemon Institute, *2015 Cost of Cyber Crime: Global,* Benchmark Study of Global Companies, 6th Ed., October 2015.
[2] Smith, R. and C. Sweet, "Utility's fine for explosion: $1.6 billion," *Wall Street Journal,* April 2015.
[3] McKinnon, J. D., "Cybersecurity measure encourages sharing of data," *Wall Street Journal,* December 2015.

TOM AYRAL is a cyber security account specialist with Honeywell's Industrial Cyber Security division. With over 30 years of experience in the industry, he specializes in developing economic and technological justifications. Mr. Ayral has published over 80 articles and was recently named Engineer of the Year by Control magazine. He earned a BS degree in chemical engineering at Brooklyn Poly (now NYU) and an MBA degree at Pepperdine University in California.

JOE O'DONNELL is director of Honeywell Industrial Cyber Security's business development efforts. He has over 18 years of cyber security experience with Cisco, Nortel, F5 Networks and Juniper Networks, as well as with cyber security startups.