Enabling Continuous Vulnerability Management for Industrial Control Systems

By Sid Snitkin

Keywords
Industrial Cybersecurity, Maturity Model, PAS Cyber Integrity, ICS Vulnerability, Vulnerability Management, Operational Technology (OT)

Summary
Industrial companies have made significant investments in cybersecurity technologies to protect their plants and industrial control systems (ICS). But many companies are unable to keep up with the never-ending stream of new vulnerability alerts from suppliers and groups like ICS-CERT. This leaves many plants at risk of serious cyber incidents, jeopardizing safety and operational reliability.

Industrial companies need to recognize and address this serious risk. Managers need to make sure that plants have programs in place to help ensure that vulnerabilities are continuously managed. Operations and compliance managers also need continuous visibility into vulnerability management efforts across all facilities to help ensure timely and appropriate cyber risk mitigation.

ARC Advisory Group recently discussed continuous ICS vulnerability management with PAS executives. Vulnerability management of the ICS in complex, multi-vendor industrial facilities is a key focus of the company’s Cyber Integrity solution.

A recent ARC briefing with PAS executives showed that they clearly understand the challenges of vulnerability management in industrial facilities. This understanding is reflected in the design of their industrial cybersecurity management solution, Cyber Integrity.

1 For more capabilities, see PAS Solution Designed to Provide a Foundation for Effective Cybersecurity Management, June 9, 2016.
**Vulnerability Management in ARC’s Industrial Cybersecurity Maturity Model**

ARC developed its Industrial Cybersecurity Maturity Model to help managers understand their ICS cybersecurity challenges without having to become cybersecurity experts. The model is also an effective tool for communicating the importance of continuous vulnerability management.

ARC’s Industrial Cybersecurity Maturity Model breaks cybersecurity into a set of steps that can progressively reduce cyber risks. Each step adds an additional layer of security to the foundation provided by all previous steps. Defense-in-depth is achieved by addressing specific, easily understandable security issues. These include maintaining accurate inventory of and securing individual devices, defending plants from external attacks, containing malware in control system environments, and monitoring systems for and addressing known vendor-identified vulnerabilities rapidly and in real time. Each step has an associated set of actions and technologies that can be used to accomplish its goals.

The ARC model also shows the human resources and tools required to utilize and sustain cybersecurity technology investments effectively. Technology investments that exceed an organization’s resource capabilities are wasteful, as security benefits quickly erode without constant maintenance.
Vulnerability Management Is the Foundation of Good Security

Ensuring that devices are free of known vulnerabilities, a focus of the first step in ARC’s model, is at the very heart of effective cybersecurity. Most malware attacks exploit known vulnerabilities - eliminating them is the only real defense. Companies can’t rely solely upon firewalls and anti-malware software to block cyber-attacks. Hackers, who are becoming increasingly more sophisticated, can use “morphing” and “cloaking” techniques to overcome perimeter defenses to penetrate the ICS.

Vulnerability management includes a thorough inventory of all cyber assets, a comparison of findings with known weaknesses, and a complete system hardening/patching effort. Establishing a reliable, automated process for ongoing vulnerability management is also essential. New vulnerabilities appear daily and plant managers need to be sure that the associated risks are being continuously evaluated and addressed.

Systems in industrial facilities need a more extensive continuous vulnerability management program than conventional IT systems. Industrial programs need to deal with software, firmware, and hardware vulnerabilities across a broad range of ICS cyber assets. This includes conventional servers and PCs, networking equipment, level 1 controllers (PLCs, DCS, etc.), I/O systems, etc. Industrial programs also need to support mixed-vendor, mixed vintage ICS environments, and provide visibility across multiple systems and facilities.

Continuous Vulnerability Management Requires an Automated Cybersecurity Management Solution

Even with a good vulnerability management process, most companies struggle to keep up with the myriad ICS alerts and advisories issued each month. Evaluating the relevance of each alert and deciding which and how to mitigate is incredibly time consuming. Tracking the many steps involved in procuring patches or upgrades from suppliers, testing them, and scheduling implementations within scheduled shutdowns or turnarounds adds to the burden. Without effective tools to manage these activities automatically, companies can quickly lose control of their security, leaving managers with a false sense of security regarding their organization’s real cyber risks.

Most companies are already constrained when it comes to investments in cybersecurity technology and available resources. Limited staffs are often
overwhelmed with too much technology and compliance reporting requirements, leaving only limited time to manage vulnerabilities. By automating vulnerability remediation workflows, existing staffs can more effectively manage and properly address key threats. This workflow automation can also provide real-time visibility into the plant’s security status, enabling managers to make better decisions regarding resources and the need for operational downtime.

An appropriate industrial cybersecurity management solution can help staff organize and manage the mundane, time-consuming aspects of vulnerability management. Key elements typically include:

- **Asset Inventory** – Establishing and maintaining an accurate, detailed inventory of all cyber assets in a facility including details regarding device configurations, versions of all installed software and firmware, etc.

- **Monitoring and Evaluation of New Security Threats** – Provides a means to automatically acquire vulnerability alerts from suppliers, US-CERT, and cybersecurity researchers and enable quick reviews of their relevance and risks relative to the facility’s installed software, hardware, and firmware.

- **Risk Mitigation Planning and Implementation Management** – Provides a way for users to document the best course of action for relevant vulnerabilities. This includes options like remediation and/or mitigation via compensatory controls and managing the many work steps involved in implementation. For example, a remediation decision may require several steps (acquire patch from vendor, verify patch on test system, implement patch in on-line system, and so on). The capability to schedule each step and monitor progress would also be helpful here. In this case, the goal of automation is to facilitate proper workflow, rather than perform implementation tasks like automatic patching, which is generally not acceptable in industrial facilities.

- **Security Status and Compliance Reporting** – Support management visibility needs through dashboards and reports that provide the information required to make operational decisions and monitor compliance.
PAS Cyber Integrity Provides Continuous Industrial Vulnerability Management

The PAS Cyber Integrity solution was designed specifically for OT cybersecurity management. The solution was built on more than two decades of expertise in the power and process industry. Significantly, PAS has a long history of automation vendor platform independence. The product supports continuous vulnerability management for a broad range of level 0, 1, and 2 cyber assets.

Asset Inventory Support

According to the company, building asset inventories for proprietary control system components automatically is a key feature of PAS Cyber Integrity. It is designed to automate discovery, collection, and management of information. This includes detailed configuration data for industrial control system elements like DCSs, PLCs, safety systems, and I/O cards for all major control systems, regardless of vendor. It also gathers configuration data for the IT-based systems – all in one data repository. The Cyber Integrity solution can collect this information from devices that are connected through TCP/IP, serial, and other methods.

Automated Vulnerability Monitoring and Evaluation

Cyber Integrity automates the monitoring and evaluation of ICS vulnerability alerts through a combination of an in-depth asset inventory and the National Vulnerability Database (NVD) from US-CERT. The product quickly identifies specific ICS assets with identified vulnerabilities.

The solution displays all vulnerabilities across the entire environment and enables users to filter for quick identification of vulnerabilities by plant, unit, area/zone, or individual asset. Results include the NVD Common Vulnerability Scoring System (CVSS) risk rating for each vulnerability.

Remediation and Mitigation Workflows

PAS Cyber Integrity provides a flexible platform for managing vulnerability remediation and mitigation workflows. This includes documentation, inventory-matching, and reporting on existing vulnerabilities. To help pro-
tect production safety, reliability and availability, rather than pushing patch implementation automatically, Cyber Integrity provides highly customizable patch management workflows. These are designed to document and ensure that all proper steps are followed during the various stages of the patching process, including appropriate patch evaluation, testing, implementation, and verification.

Vulnerability Dashboards and Trend Views
With customizable vulnerability management dashboards, the PAS Cyber Integrity solution provides asset owners, plant staff, ICS and IT cybersecurity professionals, and the executive leadership team visibility into the data they need to make informed decisions about vulnerability remediation and cyber risk management. Vulnerability trend views display trends over time. Drill down capabilities provide additional details on vulnerabilities and trends as needed.

Conclusion
Effective vulnerability management, a key element in ARC’s ICS Cybersecurity Maturity Model, helps provide the foundation for a successful cybersecurity program. Establishing a reliable, continuous vulnerability management process is essential and should be done at the very outset. Given that most companies already have a serious cybersecurity resource gap, implementing an appropriate industrial cybersecurity management solution, like PAS Cyber Integrity, must also be a priority.

For further information or to provide feedback on this article, please contact your account manager or the author at ssnitkin@arcweb.com. ARC Views are published and copyrighted by ARC Advisory Group. The information is proprietary to ARC and no part of it may be reproduced without prior permission from ARC.

Cyber Integrity is a trademark of PAS, Inc. All other trademarks mentioned are the property of their respective owners.