OT Cybersecurity:
You Cannot Secure What You Cannot See

PAS
Ensuring **OT** Integrity

Introduction

Industrie 4.0, the Industrial Internet of Things (IIoT), and the Digital Plant are all timely conversation topics focusing on the disruptive role of big data and analytics in industrial operations. These concepts are not revolutionary; but simply the next evolutionary step in process automation that was started in the 1970s with the introduction of the first distributed operational technology (OT)/industrial control system (ICS). This is when sensor data and analytics first took hold. As a new era dawns, the challenges remain the same: profitability, safety, and security. How can enterprises best use the abundance of available operational data in today's connected environment to ensure these outcomes?

With smarter plants comes a difficult challenge that has repercussions from the boardroom to manufacturing operations: ICS cybersecurity. This challenge has born a new wave of innovative technologies. While industry has embraced these new technologies, which primarily take an IT-based approach to secure the perimeter of the control network, it has invested insufficiently in securing the systems directly responsible for plant processes and safety. In a growing threat landscape, insufficient control system security is no longer tenable.

In this paper, we'll discuss industry best practices for hardening OT/ICS cybersecurity, focusing on the first and most crucial step: inventory management.

> *"In a growing threat landscape, insufficient control system security is* ***no longer tenable.***"

You Cannot Secure What You Cannot See

When it comes to OT/ICS cybersecurity, nearly every company with which PAS engages is in the same starting position – discovering and tracking the cyber assets they have. While many companies have insight into their non-proprietary, IT-based cyber assets, they lack similar visibility into the proprietary cyber assets that are directly responsible for running processes and enforcing safe operations. Were these systems compromised, worst case scenarios become reality.

The cybersecurity "iceberg." Many cyber asset inventory solutions simply do not have all the right information to support OT/ICS cybersecurity efforts. Most inventories are missing critical data, providing only IT-based system information or limited detail from control system workstations. In the end, this is not enough as it is a partial list of all the cyber assets that exist in a proprietary control network (PCN).

To illustrate, PAS was asked to perform a detailed site inventory at a major oil and gas plant in support of an internal vulnerability assessment. The inventory included information about the Microsoft Windows®-based workstations, switches, and routers, but these only comprised 20 percent of the total cyber assets. Getting information about these systems is relatively straightforward. They are IP addressable, a network ping identifies the devices, and standard protocols,

such as WMI and SNMP, retrieve detailed configuration information. Were there a need, an agent could gather the required configuration data as well.

But what about the remaining 80 percent of cyber assets? The proprietary, heterogeneous control systems store information on I/O cards, firmware installed, software installed, and control strategies – all of which provide a complete picture of these valuable assets. Think about how many Windows machines are in a PCN, and then think about how many I/O cards exist within a distributed control system (DCS). It is easy to understand why an inventory for this class of systems comprises the majority of all the cyber assets.

Unlike open IT-based systems, there are no standard protocols or agent options for gathering proprietary system inventory data automatically. Most companies concede grudgingly that they have limited visibility into these cyber assets, yet a cyber attack or inadvertent engineering change to these assets can have the most severe impact within any layer of the plant.

The OT/ICS Cybersecurity Iceberg: How Do You Secure Cyber Assets You Cannot See?

It is relatively easy to gather detailed configuration information for non-proprietary systems, such as Windows machines and routers, but far more difficult for heterogeneous, proprietary control systems, such as DCSs and PLCs. With critical cyber assets hidden from plain site, companies face increased risk from cyber attacks or engineering mistakes. Inventorying both types of systems enables detection of unauthorized changes, facilitates compliance efforts, and reduces risk.

State of Cybersecurity

How do companies gather information on their proprietary cyber assets? Most continue to focus primarily on the non-proprietary systems, prioritizing perimeter-based security measures, such as network segmentation, firewalls, or malware detection, as these are essential in any defense in depth strategy.

Those gathering inventory on the missing 80 percent do so primarily through manual efforts. This effort involves dispatching a team of engineers on an infrequent basis to gather data on critical control systems. However, this tends to result in an incomplete inventory of proprietary cyber assets. Without an automated inventory process, data errors and staleness are typical, and detailed data, such as control strategies, is wholly missing. Microsoft Excel® spreadsheets and Access™ databases are the most prevalent means of housing inventory data, but these are ineffective tools for functions such as security policy monitoring and alerting as well as workflow-driven change management. Ultimately, Excel is not the best repository for asset data that drives automation within OT/ICS cybersecurity.

Addressing the OT/ICS Cybersecurity Problem

It is fair to say that many organizations want to address the OT/ICS cybersecurity problem, but besides modest automation improvement goals for their Excel spreadsheets, what options are available? Let's examine the options in this section.

Proprietary tools

Control system vendors offer inventory tools for their systems. These are reasonable solutions if plants have systems from a single vendor. Such plants though are unicorns. Leveraging an inventory tool from a single control system vendor means creating information silos and unnecessary complexity as vendors only support their own systems.

Managed services

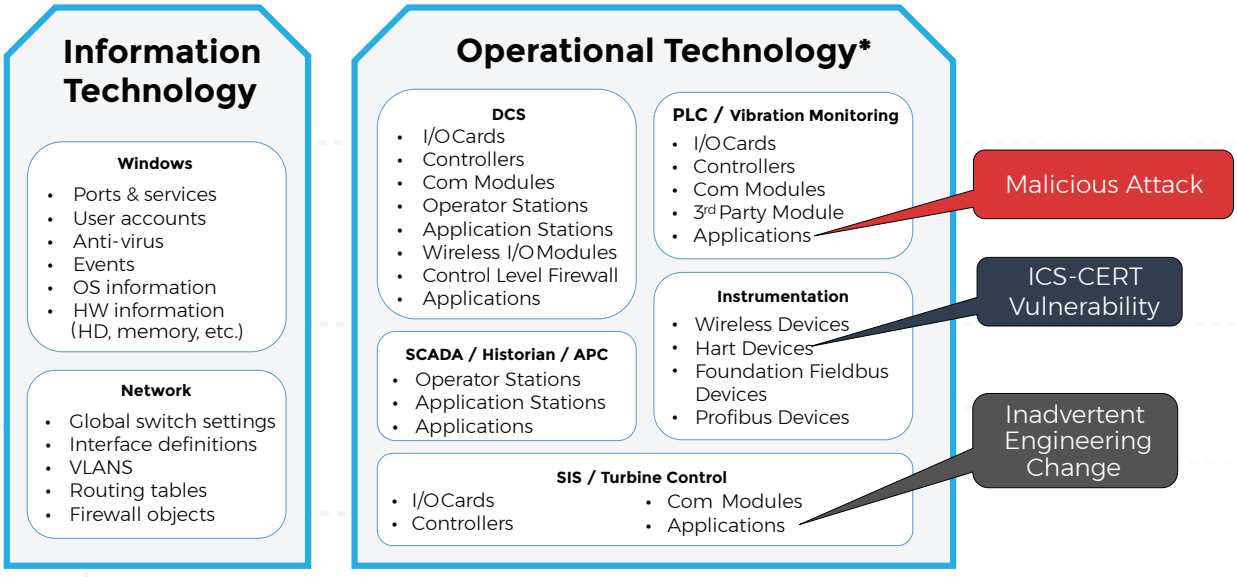
Control system vendors as well as service providers offer a managed service to relieve the internal burden on process control engineers. Periodic inventories by plant engineers are not frequent enough to capture ongoing change that occurs in plants, and important data, such as control strategies, is not collected from the variety of control systems. Retrieving and contextualizing those control strategies requires a deeper understanding of each vendor's control system, and no single control system vendor has that ability today. In the end, such an approach provides periodic inventory snapshots of cyber assets and lacks important data that describes process control, logic, and shutdown interlocks.

IT-based solutions

Many OT/ICS cybersecurity solutions take an IT approach to the process control network. These solutions are adept at gathering detailed inventory and configuration data for Windows workstations, routers, switches, firewalls, anti-virus software, and more. As described earlier, they do not address the proprietary control system inventory data and are unable to gather control strategies and contextualize them for both engineering productivity and cybersecurity purposes. Having non-proprietary configuration data is important, but it only covers 20 percent of the cyber assets in a plant.

Inventory in Depth

Comprehensive, evergreen operational technology (OT) inventory management requires not just manufacturer, model, and version number, but also understands the control strategies for the systems responsible for running processes or providing safety in plants (as shown in Figure 1 on next page). A solution must approach inventory management from an automated OT perspective and provide an option to gather IT-based inventory data. The following section details the critical aspects of that solution.



* Proprietary configurations: Honeywell EB / LVRLOG files and EMDB / ERDB databases; Triconex™ PT2, LT2, and Dbase files, Yokogawa .edf files; and more

Inventory in Depth

A best practice approach to inventory management has five critical elements, which include: automated, configurable data aggregation, proprietary and non-proprietary data collection, data classification, new device discovery, and interdependency mapping.

Automated, configurable data aggregation

Inventory in Depth mandates an architecture that gathers and interprets unique, disparate data sources into a single repository. Automating the data aggregation process offers companies an evergreen inventory depending on the frequency of updates. Since some systems are more integral to processing or safety than others, there is analysis required to determine appropriate frequency of update. Frequencies typically range from once per day to weekly and are configurable down to the asset level.

System access is sometimes an issue as IP connectivity is not always guaranteed. Systems that are islanded or connected serially require evaluation in terms of criticality for incorporation in the inventory process. Import options must include secure FTP in case a direct connection is unavailable and manual data entry or automated import is unavailable.

Proprietary and non-proprietary data

Both proprietary and non-proprietary data must reside in a single repository as it provides a number of advantages. First, it simplifies the process of analysis. Instead of going to two systems or even a third one (e.g., data mart), users can access everything they need from a single pane of glass. Second, when performing other value-added functions, such as patch management and change management, those capabilities are greatly enhanced when they are acting on a larger data set of cyber assets.

Finally, having proprietary and non-proprietary data together gives both cybersecurity and process control engineers the same view into the same data, alerts, policies, change cases, and more. Silos of data tend to create different information sets, which can lead to poor, slow, or uncoordinated decision making – not ideal when working to avoid cyber incidents or needing to act quickly to avoid process upsets.

Asset classification

Risk and cybersecurity practices vary depending on the cyber asset. As an example, a safety instrumented system (SIS) must always function and maintain a desired configuration as this is the last line of defense in an emergency. The incident response protocol for an unauthorized change to an SIS will have prescriptive actions that are more immediate. In contrast, a historian does not directly affect process or safety were it to go down.

To drive the appropriate incident response protocols automatically, a solution must classify assets based on process and safety risk. These classifications will trigger alerts and commensurate workflow-driven responses.

> *According to The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), effective physical and environmental protection requires* ***"a detailed inventory of all hardware and software components utilized in support of operations, including detailed information pertaining to device/model type, serial number, and firmware version."***
>
> *Source: ICS-CERT 2014 Industrial Control Systems Assessments Overview and Analysis*

New device discovery

A best practice approach performs new device discovery to maintain an evergreen inventory. For the non-proprietary portion, or 20 percent of cyber assets that exist in a typical PCN, this is done via a scheduled network ping where responding devices are compared to existing device lists. Standard IT protocols interrogate and gather information about new devices when they are discovered.

For the proprietary assets, the process is quite different. To discover a new cyber asset, the solution must interrogate each proprietary control system's configuration data and look for system references not currently inventoried. Once an asset is recognized, cybersecurity or engineering personnel receive notifications of a new device (as well as missing ones – e.g., system upgrade). A workflow guides them through the process of updating data imports, policies, processes, and other cybersecurity functions.

Interdependency mapping

Finally, systems work with other systems to achieve a process goal. Understanding these interdependencies means capturing the true risk of a cyber asset were it impacted by an unauthorized change. If a PLC goes down, for instance, what other systems rely on it to function? A robust cyber incident response protocol accounts for these interdependencies. Knowing this information is a good engineering practice, but it also allows cybersecurity personnel to better manage risk across the enterprise.

Inventory-Enabled OT/ICS Cybersecurity Scenarios

With a robust inventory of both proprietary and non-proprietary assets, cybersecurity personnel can perform tasks previously unavailable to them. Here are two use cases that illustrate the richness that comprehensive inventory data provides:

Identifying Exposure to Published Vulnerabilities

Scenario: ICS-CERT published a critical vulnerability in early 2015 concerning multiple models and versions of a Honeywell transmitter. This transmitter works with control system vendors besides Honeywell. The advisory describes how the vulnerability could impact operations if unaddressed. Can you identify accurately and quickly where every model and version number of this transmitter exists across your entire enterprise?

Solution: A simple query based on manufacturer, model, and version will immediately identify every control system that has this transmitter. Only an inventory that spans the proprietary control systems will provide complete results. Further, a policy can look for instances in the future when that same transmitter is reintroduced into a control environment (e.g., spares inventory).

Unauthorized Change to a Control Strategy

Scenario: An engineer connects to a Triconex safety system to make a simple change. The engineer mistakenly removes the ability for the operator to recognize the availability of that safety system. How likely are you to detect such a change and drive appropriate remediating action automatically?

Solution: Post inventory data aggregation, changes in configurations are automatically flagged and investigated. If unauthorized, an appropriate incident response protocol will drive the remediating actions

necessary to restore the safety system. Further, the next data import captures evidence that the safety system's configuration was properly fixed.

The vast majority of organizations in power and process industries cannot effectively execute these two use cases. Where these organizations stumble is they do not have an accurate inventory of all their cyber assets that allows them to monitor for certain conditions and drive action when these conditions violate critical security policies.

A Comprehensive OT/ICS Cybersecurity Solution

PAS Cyber Integrity™ is a best-in-class solution that provides inventory management covering all the major cyber assets found in plants today including both proprietary and non-proprietary systems. Cyber Integrity relies on the Integrity software platform that has over 200 man years of investment deciphering and integrating control system configuration data into a single repository. The solution allows for configuration of data aggregation at the asset level, detects new or missing devices, provides a facility for asset classification, enables incident response protocol development and assignment, and captures system interdependencies.

Using Cyber Integrity, industrial facilities gain automated, normalized inventory data across all major OT and IT assets in the control network. The software presents a unique and holistic view of control system assets beyond the reach of traditional IT- or vendor-specific solutions. Cyber Integrity monitors and detects unauthorized changes centrally automating investigation, remediation, and mitigation steps through polices and workflows. It also automates the steps behind a closed-loop patch management process and speeds recovery in the event a lost system.

Cyber Integrity Benefits

- **Reduce compliance efforts by up to 90 percent**
- **Gain inventory visibility into IT and OT cyber assets**
- **Avoid regulatory fines and penalties**
- **Prevent unplanned downtime due to unauthorized changes**
- **Manage across all major control system manufacturers**

Conclusion

In this paper, we've addressed requirements for a comprehensive, evergreen cyber asset inventory as prescribed by ICS-CERT to provide the necessary foundation for effective operational and cyber risk management. A layered defense cybersecurity program remediates cybersecurity breaches before they affect productivity, safety, or company liability.

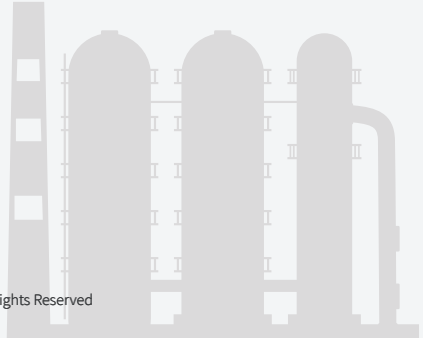
The first step in implementing an effective OT/ICS cybersecurity strategy is establishing and maintaining an automated inventory of all cyber assets. Inventory management comprises a full accounting of both IT and OT assets, including hidden proprietary configuration data, such as control strategies, I/O cards, and installed software. Today, companies largely rely on manual inventory practices to accomplish this task, which typically proves costly, time intensive, and prone to human error.

Additional Resources

To learn more about implementing an OT/ICS Cybersecurity strategy and the PAS methodology for doing so, please visit cyber.pas.com or email info@pas.com.

About PAS

PAS, the OT Integrity company, delivers software solutions that prevent, detect, & remediate cyber threats; reduce process safety risks and optimize profitability; and enable trusted data for decision-making. With operations in over 70 countries, PAS helps many of the world's leading industrial organizations ensure OT Integrity from the sensor to the cloud – including 13 of the top 15 refining, 13 of the top 15 chemical, 4 of the top 5 pulp and paper, 3 of the top 5 mining, and 7 of the top 20 power generation companies. PAS was recently named the #1 Global Provider of Safety Lifecycle Management and #1 Alarm Management Provider by ARC Advisory Group and is named as a Representative Vendor by Gartner for OT Network Monitoring and Visibility and OT Endpoints Security. For more information, visit www.pas.com. Connect with PAS on Twitter @PASGlobal and LinkedIn.



PAS
Ensuring OT Integrity