www.pipelinepub.com
Volume 21, Issue 2

Securing OT/ICS: A Call to Action

By: Christina Hoefer

In the last year, U.S. critical infrastructure has been under constant attack and regularly in the headlines. These attacks include a breach on American Water, one of the largest water and wastewater companies in the U.S., which shut down customer portals and billing temporarily; the Change Healthcare data breach, which compromised protected health information of approximately 100 million individuals; and the recent China-linked hack of several U.S. telecommunication firms, which intercepted surveillance data destined for law enforcement.

While attacks on critical infrastructure make great headlines, most hackers infiltrate systems through IT and connected Internet of Things (IoT) devices before spreading laterally across networks. Devices are increasingly connected — from IT systems to IoT and operational technology (OT) cyber-physical systems — and can be used as entry points for cybercriminals.

Research shows that as of June 2024, IoT devices with vulnerabilities increased by 136 percent since 2023. This problem will only persist with expectations that connected IoT devices will expand to over 25 billion by 2030. As digital systems become more integrated, attack surfaces only grow, leading to new security challenges, vulnerabilities, and risks. These trends in OT and IoT vulnerabilities tell us one simple truth: Immediate action is crucial to secure all devices. No sector or device can afford to be left unprotected.

How to Take Action to Secure IoT, OT, and ICS

OT and ICS security is no longer just a concern for industrial sectors like energy and manufacturing but across all critical infrastructure sub-industries — healthcare, communications, waste, transportation, and more. Consider devices such as robots on assembly lines, IP cameras monitoring the physical security of nuclear power plants, wireless access points and routers in offices, medical devices in hospitals, and even the security of remote sites such as wind turbines or ship vessels. All these devices, when connected to enterprise networks without protections or directly to the internet, can open new security backdoors and vulnerabilities for our most critical systems.

Despite increased awareness around the need to secure OT and ICS systems, many devices and systems remain vulnerable to internet exposure, which can lead to a range of cyber-attacks, including ransomware attacks. There are four essential steps that these industries, including critical services providers and telecommunications organizations, can take to maintain operational efficiency *and* secure all devices and endpoints on their networks.

1. Conduct an Inventory Assessment to Uncover Hidden Devices and Unknown Risks

First, organizations must do an asset inventory to gain comprehensive visibility across *all* connected devices to understand the dependencies, compliance status and governance, locations, and

vulnerabilities or security gaps that may lead to security and operational risks. Organizations can't manage risk if it's hidden and in the dark. Think about the types of devices connected to the network and the unique challenges they bring:

OT Devices and ICS: These are often legacy systems that are not designed to connect to the internet and may not have or support the latest patches and software updates. However, OT systems are becoming increasingly connected, like IT systems, and smarter with analytics functions that are valuable for business operations, but security practices have not kept pace with this evolution.

IoT Devices: These include modern equipment (i.e., voice-over-IP devices, IP cameras, badge scanners, smart buildings, and datacenters, etc.) often manufactured quickly and relatively inexpensively and not with security in mind. Paired with default credentials and access configurations that are rarely changed they can leave the network exposed.

Today, many organizations also have many more remote management services enabled post-pandemic, which increases internet exposure and can potentially open the door to new security risks. Recent research finds that threat actors are heavily targeting VPNs and other perimeter devices, exploiting new vulnerabilities for initial access, with 20 percent of new exploited vulnerabilities targeting virtual private networks (VPNs) or network infrastructure appliances between January 1 and July 31, 2024.

2. Limit Connectivity to What is Essential for Business Processes and Implement a Robust Monitoring Infrastructure

For OT/ICS, connectivity offers operational and productivity advantages, but it also introduces significant risks. Opportunistic attackers are increasingly abusing this exposure, often driven by trends like current events, new hacking guides, or the discovery of vulnerabilities. To address these risks, organizations must limit connectivity to what is essential for business processes. Reducing risk across the network also requires implementing a robust monitoring infrastructure. This allows for the tracking of asset configurations and behavior, not only for security and compliance purposes but also to streamline operational diagnostics. With effective monitoring in place, organizations can detect issues early and mitigate potential consequences before significant damage occurs. As organizations deal with IT/OT convergence, this process can benefit both IT and OT teams to ensure that systems are running securely and smoothly as required for business operations to minimize any potential downtime that can be costly.

3. Take a Risk Based-Approach, Focusing on Most at Risk Areas and Critical Exploitable Vulnerabilities First

Resource limitations are a growing challenge in securing OT and IoT devices. For most organizations that operate critical infrastructure, there is not enough security staff or talent with specialized skill sets and knowledge to investigate new cyber risks and effectively manage the amount of data coming from security tools. This is why organizations need to take a risk-based approach by focusing on most at-risk areas and exploitable vulnerabilities first, allocating resources strategically, and leveraging consolidated security platforms that have automation capabilities to provide real-time insights and correlated alerts.

4. Improve Security Hygiene of OT and ICS

While this starts with increased visibility and monitoring, organizations also need to take immediate action to improve security hygiene. Among the immediate steps organizations can take to secure OT/ICS are:

- Upgrade, replace, or isolate OT and IoT devices that use legacy operating systems with known critical vulnerabilities.
- Change default credentials and disable unused services.
- Deploy automated compliance verification and enforcement tools to prevent non-compliant devices from connecting to the network or to limit their access.
- Strengthen network security measures, such as segmentation, to isolate commonly exposed devices like IP cameras and close high-risk open ports.

OT/ICS Security Global Progress

Across the world, we are seeing countries take steps like reducing the number exposed devices with internet connectivity and critical vulnerabilities to protect critical infrastructure.

North America: From June 2017 to January 2024, the US and Canada significantly reduced the number of exposed devices by 47 percent and 45 percent, respectively. Whereas Spain (82 percent), Italy (58 percent), France (26 percent), Germany (13 percent), and Russia (10 percent) saw an increase in the number of exposed devices.

This progress in the U.S. and Canada is likely the result of significant investment in cybersecurity and technological advancements in the last decade. Many organizations are following the NIST Cyber Security Framework as they embark on their cybersecurity journey. In addition, North America has enacted numerous regulations that require critical infrastructure organizations to invest in security to maintain compliance. This includes, for example, the North American Electric Reliability Corporation (NERC)'s Critical Infrastructure Protection (CIP) standard that applies to bulk electric power systems and is being extended with requirements for Internal Network Security Monitoring (INSM). These standards and frameworks require maintaining an asset inventory, protecting the security perimeter and systems, monitoring and detecting suspicious network activities and communications, and managing incident responses.

Europe: Countries like Spain (82 percent), Italy (58 percent), and France (26 percent) saw increases in exposed devices over the same period, highlighting a slower adoption of comprehensive security measures. The NIS2 Directive, i.e., the second version of the European Union's Network and Information Security Directive, provides additional legal measures to boost the overall level of cybersecurity in the EU by setting a standard for organizations in essential and important sectors, such as energy, healthcare, transport, finance, but also digital infrastructure, to strengthen cyber resilience and incident handling and take a risk-based approach to mitigate cyber threats effectively. It requires 24-hour incident reporting and a level of corporate accountability with management boards.

Despite progress in some regions, there remain nearly 110,000 internet-facing OT/ICS devices worldwide as of January 2024. The evolving compliance landscape emphasizes proactive risk monitoring and remediation, but more work remains to secure critical systems globally.

The Path Forward to Secure the Future of Critical Infrastructure

It's evident that securing managed and unmanaged OT and IoT devices is a global issue. It's not a matter of if, but when, device vulnerabilities will be exploited to attack critical infrastructure. Organizations across the world need to take proactive measures to safeguard critical infrastructure before it's too late. By prioritizing these measures, critical infrastructure operators can not only protect their systems from emerging threats but also build a resilient foundation that ensures operational continuity and public trust in an increasingly connected world.