SEPIO

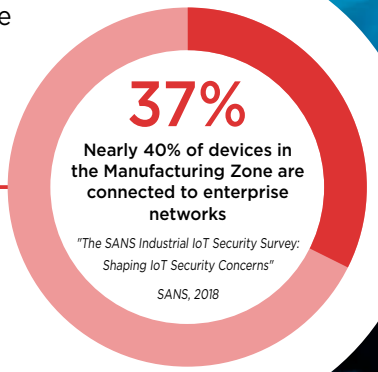
SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

CLOSING THE OT VISIBILITY GAP

Operational technology (OT) is the hardware and software responsible for physical processes, devices, and infrastructure. OT is a core component of critical infrastructure and, in turn, states' national security. The 21st century has seen dramatic technological advancements, known as the Fourth Industrial Revolution (Industry 4.0). Industry 4.0 centers on the development of cyber physical systems (CPS), the umbrella term of engineered systems that orchestrate sensing, computation, control, networking and analytics to interact with the physical world. In short, CPS automate the monitoring and control of OT through IT infrastructure. While CPS have brought significant advantages to industry, visibility challenges make managing such systems a difficult task and, with that, comes a host of potential cybersecurity riskss.

BACKGROUND

Cyber physical systems are comprised of different digital tools that all share the common trait of connectivity. Through connectivity, CPS automate industrial processes, thus allowing for better allocation of resources and increased productivity. Industrial Control Systems (ICS), which include Supervisory Control and Data Acquisition (SCADA) systems and Distributed Control System (DCS), have been around for decades – long before Industry 4.0 came into fruition. However, the development of CPS over the last few years saw the silo that ICS once operated in begin to erode with the introduction of the Industrial Internet of Things (IIoT). ICS are now connected to the "outside" world thanks to the convergence of IT and OT. A survey conducted by the SANS institute found that nearly 40% of devices in the Manufacturing Zone (Purdue levels 0, 1, 2, and 3) are connected to enterprise networks.



By leveraging connectivity, CPS have helped enterprises boost performance by enhancing efficiency and reducing downtime, thereby improving material use and enriching customer experience, among other positive domino effects. Ultimately, the advantages of Industry 4.0 have lowered costs and increased returns on investments, demonstrating significant value across the entire enterprise.

However, as OT becomes more connected and reliant on technology, it is now more vulnerable than ever; a serious risk considering that physical processes rely on the continuous operability of OT. The need for robust cybersecurity is imperative. Yet, visibility challenges remain a fundamental obstacle to effective cybersecurity as blind spots allow vulnerabilities to go unaccounted for and security policies to lack comprehensive enforcement.

SEPIO

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

IMPORTANCE OF VISIBILITY

Asset visibility is the foundation of asset management; and asset management is a paramount component of cybersecurity. Countless devices get connected to OT networks and, maintaining reliability relies on competent asset management. Asset management, which is dependent on continuous visibility, provides insights into assets operating within the OT environment to assist decision making and ensure that security measures get appropriately applied. However, the use of legacy technology means OT was not built with cybersecurity in mind and, thus, many visibility tools are not applicable to this domain; agent-based solutions and network scanning are incompatible with OT devices. As such, a study found that nearly 90% of enterprises have extremely limited to no visibility into their OT environment.

The importance of asset visibility for OT security extends beyond the OT environment; the adoption of IIoT technologies means OT is exposed to the entire threat landscape. Hence, complete visibility and management of assets on the IT environment is just as critical. Nevertheless, visibility into the IT domain is also limited, with reports that 75% of enterprises are experiencing widening visibility gaps into both end-user devices and IoTs.

86%

Nearly 90% of enterprises have extremely limited to no visibility into their OT environment

2021 ICS CYBERSECURITY YEAR IN REVIEW

DRAGOS, 2021

THE NEED FOR PHYSICAL LAYER VISIBILITY

Asset Management

Asset management tools identify devices and provide an accurate and detailed asset inventory. However, enterprises suffer from a lack of Physical Layer visibility as existing security tools fail to cover this domain, thereby leaving the hardware level neglected. As such, the asset inventory is incomplete and, in turn, inaccurate. With extensive OT and IT supply chains, coupled with device heterogeneity, knowing the true identity of an asset is imperative and this requires Physical Layer visibility. Such data tells security teams more about a device than its network data, it provides them with electrical and physical specifications – simply knowing something exists is not enough. However, when a device is passive, enterprises even struggle with that; Physical Layer visibility detects the presence of devices that do not emit traffic and would otherwise go unnoticed. Moreover, Physical Layer information provides necessary insights into IIoTs as these non-802.1x compliant devices currently get authenticated by their MAC address, which can easily get spoofed. Complete asset visibility allows enterprises to understand each device's associated risk posture and handle them accordingly.

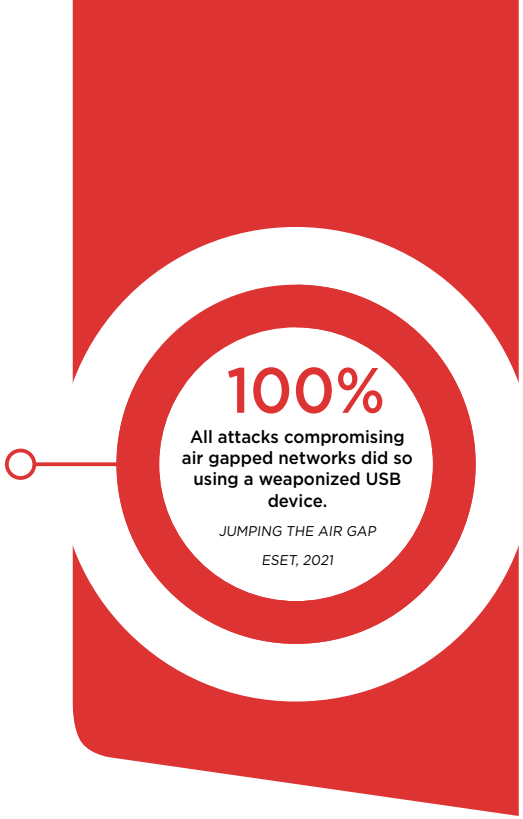
Access Management

Asset visibility and asset management lay the groundwork for access management and policy enforcement. Effective cybersecurity depends on the enterprise's ability to control user and device access to critical resources. The interconnectedness of IT/OT environments means access management and policy enforcement are more necessary than ever; maintaining OT reliability means heavily controlling access to such resources. Pre-defined policies determine, under what circumstances, an entity can access a resource; in other words, security policies address "who, what, where, when, how, or why". Access management tools enforce these pre-defined policies by assessing a device and comparing it with the policy's requirements. Naturally, this is where the importance of an accurate asset inventory comes into play. A flawed asset inventory, due to the Physical Layer blind spot, undermines policy enforcement and access management – a significant risk as all it takes is the exploitation of a single weak spot to jeopardize the entire enterprise.

Rogue Device Mitigation

Attackers know enterprises suffer from a Physical Layer blind spot and exploit this weakness using rogue devices. These hardware attack tools intentionally deceive existing security solutions by hiding their presence or spoofing their identity by using the same VID/PID/Class ID parameters as legitimate devices, thereby raising no alarms. In turn, access controls, such as network segmentation and Zero Trust – which are often relied on as robust defense mechanisms against the cybersecurity risks associated with Industry 4.0 – are futile in preventing these perilous devices from penetrating and moving laterally across the network. This is a significant risk to OT as Industry 4.0 has expanded the attack surface considerably. An interconnected environment that lacks effective access controls means any asset can act as an entry point, in which the first point of compromise gets used as a gateway to more sought-after resources; hardware-based attackers simply need to attach a rogue device to the most accessible endpoint or network switch.

For enterprises that continue to maintain an air-gap, OT is still not immune to hardware-based attacks. A recent study by ESET found that 100% of attacks compromising air-gapped networks did so using a weaponized USB device; and with a 30% increase in USB usage in production facilities in 2021, the risk is considerable. The value of rogue USB devices has not gone unnoticed by bad actors, with 37% of threats specifically designed for removeable media in 2021, nearly double than the previous year.



HAC-1 SOLUTION

OT is highly vulnerable thanks its convergence with IT and the development of IIoT. To improve the security posture of cyberphysical systems and maintain their continuous operability, enterprises need to get to the root cause of the problem: visibility. Sepio's Hardware Access Control (HAC-1) solution provides a panacea to the gap in device visibility by offering protection on the Physical Layer.

By going deeper than any other security solution, HAC-1 uses Physical Layer information to calculate a digital fingerprint of all IT, OT, IoT and IIoT assets – managed or unmanaged – no device goes undetected. HAC-1 accurately identifies devices and their associated risk posture based on multiple Physical Layer parameters and a unique machine learning algorithm to provide visibility like never before – traffic monitoring can only tell you so much. HAC-1's ultimate visibility means unmanaged switches, passive taps and out-bound devices no longer fly under the radar. The solution continuously monitors all hardware assets to account for any anomalies, issuing an alert when there are any chances to a device's risk posture.

HAC-1's Hardware Access Control feature allows the system administrator to define granular hardware access policies for the system to enforce dependent on a device's role or characteristics and its associated risk score, creating a Zero Trust Hardware Access approach. HAC-1 verifies and continuously validates the identity of all hardware assets to enhance policy enforcement. The solution integrates with other access control platforms through specific APIs to provide comprehensive access management.

Physical Layer visibility, augmented by the internal threat intelligence database, enables the immediate detection of rogue devices. Spoofed peripherals get identified for what they truly are – not what they claim to be – and hidden network implants are instantly visible. When a rogue device gets detected, or a device breaches the pre-set rules, HAC-1 automatically blocks the unauthorized device through seamless third-party integration. The Rogue Device Mitigation feature of HAC-1 prevents unwanted and malicious assets from gaining access to the network and potentially causing damage to OT.

How It Works

HAC-1 can get deployed as an agentless or cloud-based solution and does not monitor any traffic, making it compatible with OT infrastructure. The solution's low resource requirement allows for smooth and easy deployment, providing ultimate visibility and Physical Layer protection within just 24 hours. No baseline is required, meaning HAC-1 will detect rogue devices that were present prior to implementation. HAC-1 seamlessly integrates with third-party solutions to support a hands-free, low maintenance process that requires minimal human intervention.

System Architecture