Securing the Industrial Internet of Things

The very benefits that make the IIoT so compelling, makes it equally capable of damaging infrastructure operations and processes through bad actors.

Andre Froneman, Business Unit Manager and Industrial Cyber Security Adviser at Axiz

Beginning with the Industrial Revolution in the mid-1700s, the manufacturing industry has undergone several revolutions. However, in today’s age of skyrocketing technological advancements, times are changing at a far more rapid pace, as we see the automation era being replaced by the Fourth Industrial Revolution (4IR).

The 4IR has been driven by several factors. Digital transformation, evolving business models, increased pressures around costs and time to market, have all ushered in this new age, and given rise to the Industrial Internet of Things (IIoT), which facilitates unprecedented levels of real-time connectivity, visibility and control across operations.

However, alongside the plethora of benefits, is one major downfall. A dramatic increase in cybersecurity risk. Although the IIoT aims to streamline manufacturing processes, it also endangers the Industrial Control Systems (ICS) as they are vulnerable to exploits that can be found freely on the internet. The vulnerabilities range from basic issues like systems without passwords or with hard-coded passwords to configuration issues, software bugs and hardware vulnerabilities.

“Once a threat actor has the ability to run software on a host that has access to a controller, the chances of a successful attack are extremely high,” says Andre Froneman, business unit manager and industrial cyber security adviser at Axiz.

Traditional security is not enough

According to Froneman, traditional security is not enough to protect against proliferating cyber threats to both operational technology (OT) and IT systems. Industrial control systems (ICS) on OT networks have totally varying operational requirements that affect the entity’s ability to adapt and respond to evolving cyber security threats.

“This opens up the organisation to new avenues for attackers. ICS cyber security strategies must be designed with asset and operational requirements in mind to protect critical processes without negatively impacting efficiency, productivity and safety. In addition, effective ICS cyber security requires a combination of tools, processes and skills.”

Froneman says to remember, that when ICS systems were designed, it was with manageability and control with maximum reliability in mind.

“Essentially, they were never designed to be attached to the internet. In this way, these systems now face all the expected challenges associated with vulnerabilities and exploits, but with the additional burden of these systems operating in dispersed geographical environments that can be physically difficult to reach or that can never be taken offline.”

Overcoming the 2019 cyber threat
Ronald Ravel 1 Apr 2019

Moreover, all of the equipment that runs these systems is monitored and controlled by Industrial controllers (PLC, RTU, and HMI) as well as sensors. They are connected to management systems such as Distributed Control Systems (DCS) and Supervisory Control and Data Acquisition (SCADA) systems SCADA or Distributed Control Systems (DCS), and form an ICS solution that enables efficient collection, monitoring and analysis of data and automation of production and industrial processes.

He says consider critical infrastructure facilities, such as electricity, oil, gas, water, waste, and suchlike, that are key to keeping nations up and running.

“One can’t simply switch off these facilities, and it doesn’t take much imagination to think about what could happen if control of these systems fell into the wrong hands. Take, for example, the air traffic control at an airport such as OR Tambo, the ramifications should hackers be able to control this, defy thought.”

The wide adoption of these systems is due to their benefits - they are dependable, as well as rugged and stable, allowing critical infrastructure facilities to use them for decades at a time. However, the benefits that make them so compelling, make them equally capable of damaging infrastructure operations and processes through malfeasance.

Froneman explains that these systems commonly employ propriety operating systems that have not been subjected to any form of security hardening. In addition, default passwords and baseline configurations make it child’s play for attackers to compromise them. Similarly, the software they use can’t be updated or patched often, due to the limitations of their geographical locations, as well as worries about downtime.

The software run is more often than not, legacy software that lacks the appropriate user and system authentication, data authenticity verification, as well as data integrity checking features. Legacy SCADA controllers are also unable to encrypt communications, and this can enable cyber crooks to employ sniffing software to find out username and passwords.

These, and other flaws give hackers the ability to inject commands and manipulate parameters to modify, delete, or copy the information on controlled access systems.

“Should a threat actor alter commands sent to the controllers, changing the controller logical sequence or alter the sensors readings, attackers can change the industrial processes themselves,” he explains.

What can industrial organisations do to protect their data and systems?

Froneman says ICS security needs to be built in layers to prevent attacks from both external and internal sources. “There is no one-size-fits-all approach when it comes to securing ICS/ SCADA infrastructures. A segmented, multi-layer defence-in-depth strategy must be designed for their specific and highly tailored needs.”

He says that a good number of attacks suffered by ICS networks happened via IT attack vectors, including spear phishing via email and ransomware on endpoints.

“Using a solution such as Check Point Threat Prevention that has features including sandboxing, as well as network and endpoint security, can prevent and eliminate this type of attack before it hits the ICS system. These technologies are also effective when used in OT networks. SCADA vendors release vulnerability advisories for their ICS devices on an ongoing basis, and although OT environments are not quick to install and upgrade their machines, leaving systems unpatched, and creating a vulnerability window. Having this type of solution on the OT network closes that window.”

Froneman says another way of securing ICS systems, is by segmenting IT and OT, and applying the principle of least privilege access.

“Boundary protection has been cited as number one for several years in a row by US ICS-CERT, and this type of protection should ensure the availability, integrity and confidentiality of this data, and maintain physical network separation between the real time components of the industrial network.”

Deploying a remote access solution

Here, he says deploying a remote access solution into the network, for example client-to-site VPN that supports strong multi-factor authentication, as supplied by Check Point.

“To prevent tampering with legacy data that is communicated in open text without encryption on these systems, secure site-to-site VPN tunnels between boundaries interconnects should be created. In addition, security gateways should be installed at all interconnects, guaranteeing that only relevant and legitimate traffic is able to enter or leave the network. All communication, protocols, methods, queries and responses and payloads should be validated using a firewall, application control, IPS and antivirus.

Going back to a layered approach, achieving an appropriate level of protection for critical networks, means that security needs to stem from a variety of separate technologies and practices to an effective business process. Although no system is ever 100% secure, implementing security tools, such as those designed by Check Point that are specifically designed for industrial networks can vastly better networks security.

Find the appropriate skills

However, it is no good having the top security solutions in place, with no-one to manage them.

“One of the biggest constraints that hampers IIoT security, is a lack of skills,” says Froneman. “The skills shortage in SA has been well documented for years, and nowhere is this more true, or crucial, than in cyber security.”

Many industrial organisations simply don’t have, and can’t find the appropriate skills to help them secure these crucial operations. “That’s where having a partner such as Axiz, who uses best-of-breed tools, and has the years of knowledge and expertise to successfully implement and manage them, comes in.”