NEXCOM
Committed to Customer Success

White Paper

ISA 140 Building Zero Compromise OT Network Security

OT network security is critical in the Era of Industry 4.0

As Industry 4.0 and digital transformation becoming an essential part of smart manufacturing, building a reliable network between devices grows into the first step towards a secure future of OT. For the purposes of collecting and analyzing all data generated during the manufacturing processes, literally every single device, unit, or fixture, has to be equipped with sensor(s) and connected to internal network. However, staying online, unfortunately, not only means convenience, but also may usher in different types of cybersecurity risks and uncertainties. Even if there is only one device infected in an OT network, potential impacts, or costly downtime to production, would be inevitable. Not to mention the damage and losses to business thereafter.

For plant managers, productivity is the highest KPI they care for and little attention is given to OT security. Usually no dedicated IT staff is assigned to safeguard information security in manufacturing facilities. In the context of harsh environments with a great variety of new and legacy devices interconnected, it poses high risks for OT security. Even if cybersecurity measures have been implemented, the maintenance itself is still a tough task.

The following are some common practices for OT security.

- **Network Segregation** categorizes all the connected devices in the factory so that the communications among zones could be under proper management or simply disconnected when needed. To achieve that, it is recommended to segment the OT network, setting up security units as checkpoints as well as policies of communication at each node of these segments.

- **Real-Time Monitoring** is synonymous to network visualization. Other than attacks from the outside, internal weaknesses pose more threats to OT networks. Malicious threats, like malware or spyware, in any unguarded segment may exist or spread unnoticed. To improve the visibility of the networks, an effective approach is implementing a number of "probes", or micro detectors, into the intranet. Through real-time analysis, it is easier to spot potential threats and react in time to prevent security breaches.

- **Key Assets Protection** is yet another crucial step easily neglected. Connected devices at any manufacturing site are of various sizes, types and purposes, and therefore differ in their importance. Every single of them can fall vulnerable under cyberattacks, and the consequent damage to productivity may vary. It is highly recommended to provide multiple levels of protection over devices in accordance with their relative importance to the entire system. For instance, an entire SMT production line and a monitoring sensor for factory environment are totally incomparable in terms of importance.

The above cases illustrate how OT security differs from conventional IT security in many perspectives. Unlike the high-performance IT security units, which are usually huge in size but scarce in number, what better fits OT security contexts is a rather large number of lightweight units. Between and within network segregations, in front of key assets, or even in any cabinets or boxes at the manufacturing

ISA 140 proves successful against external and internal cyberattacks during field tests

site, security units deployed should ensure a universal coverage of intranet. However, a proper and effective management over the OT security system may become a challenge for security professionals.

To make a cost-effective decision in cybersecurity solution choices, striking a balance between deployment, operation and management is critical. The Out-of-Band (OOB) remote management functions and bypass mechanism make ISA 140 a winner in cost effectiveness, for either operation or management. OOB supports remote power on, shut down, and reboot of devices while the bypass mechanism keeps accessibility of network connections, making the days of OT professionals a lot easier. Its compact size along with a total of six 1GbE RJ45 ports offers another edge for OT administrator, ensuring its capability to create a high number of connections to devices with no compromise on protection.

EPS (Event Per Second) is a long-standing standard in the field of cybersecurity. Widely adopted by suppliers as a performance index, EPS also serves as a solid reference for anyone who seeks a smart purchase.

A EPS test (Figure 1) was conducted at NEXCOM's Huaya plant, as a field application showcasing the availability and performance of ISA 140, with eSAF (TMRTEK cybersecurity package) installed. Huaya Plant is not just a production site, but also a demo center for smart manufacturing, embodying NEXCOM's vision for Industry 4.0. Junction boxes come into use as a means to integrate or amplify communication signals in this application ISA 140, especially for network wiring at a vast manufacturing site like Huaya. As junction boxes typically need to be placed in cramped spaces or beyond easy reach, the compact size of ISA 140 has made a huge difference for it can be put easily into a junction box and fit seamlessly into any corner.

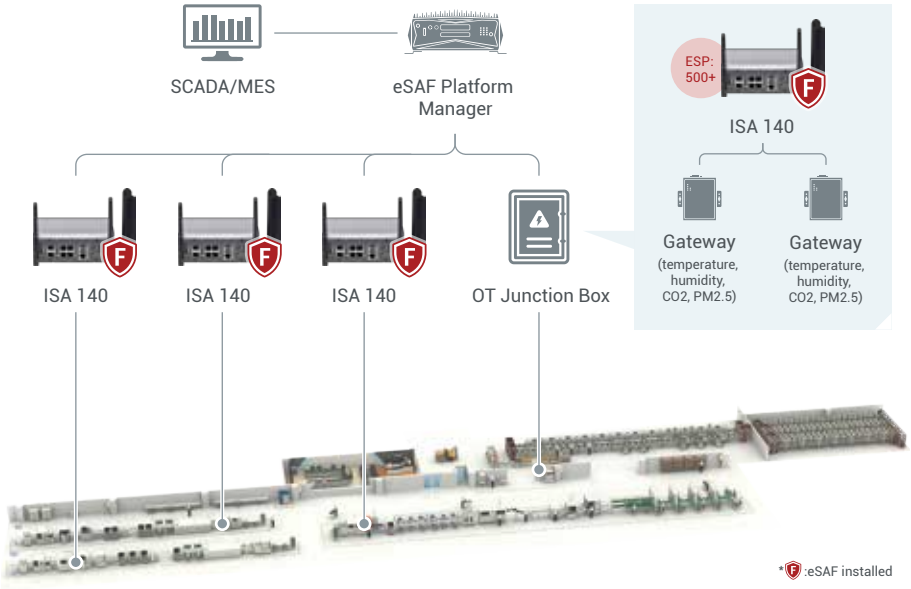

Figure 1. ISA 140 field deployment at Huaya Plant

ISA 140 saves a lot of efforts and time to upgrade and maintain network security

Figure 2. ISA 140 in OT junction box

Figure 2 is an integration demo based on our suggested framework. Through ISA 140 and eSAF, all connected devices, including sensors, fixtures, gateways, and servers, are allocated into subnetworks. Communications between devices are under management and monitoring with events reported and presented to the war room. ISA 140 averaged over 500 EPS, accompanied by eSAF, based on NEXCOM lab tests at Huaya Plant. ISA 140 protects the production from cyber threats, external and internal, and its network segregation effectively stops damage from spread.

Conclusion

ISA 140 is a compact industrial firewall solution in ruggedized design. A competent dual-core Intel Atom® processor with six 1GbE RJ45 ports ensures safe connectivity for processing multiple devices. The Wi-Fi/LTE ready appliance offers extensive network coverage as well as high reliability. OOB functions make remote management even more convenient, and wide temperature design ensures stable operation even under harsh environments.

ISA 140 is the best choice for your IIoT protection. The test result proves ISA 140 makes zero compromise in performance while maintaining high intensity in event reporting. This helps to minimize the number of units to be deployed, and therefore the total cost in operation and maintenance. Its compact & DIN rail design creates convenience for fitting ISA 140 into existing network architecture. Following a basic principle of creating segregated network, it saves a great amount of efforts to upgrade OT security. Administrators will only need to implement a proper amount of nodes as security checkpoints, and deploy one ISA 140 unit along with necessary security software at each of the nodes.

A customized security software (eSAF as current example) monitors and manages all packets going through ISA 140, blocking all potentially harmful packets, reporting suspicious behaviors, and preventing unauthorized accesses. The synergy of hardware and software guarantees that all network will be within control should any cybersecurity event occur.

Founded in 1992, NEXCOM integrates its capabilities and operates eight global businesses, which are Industrial Mesh, Intelligent Platform @ Smart City, Intelligent Video Security, Mobile Computing Solutions, Medical and Healthcare Informatics, Network and Communication Solutions, Smart Manufacturing, and Open Robotics and Machinery. This strategic deployment enables NEXCOM to offer time-to-market, time-to-solution products and services without compromising cost.

www.nexcom.com

NEXCOM is a Titanium member of the Intel® Partner Alliance, as a top tier of the Alliance. Intel and more than 500 global IoT partners of the Intel® Partner Alliance provide scalable, interoperable Intel® -based technologies and solutions that accelerate deployment of intelligent devices and end-to-end analytics. Close collaboration with Intel and each other enables Alliance members to innovate with the latest technologies, helping developers deliver firstin-market solutions.

Learn more at: https://www.intel.com/content/www/us/en/partner-alliance/overview.html

Intel and Atom are registered trademarks of Intel Corporation in the United States and other countries.