Your Factory Could Be the Next Target for a Cyber Attack. Will You Be Prepared?

Erik Halthen, Product Development Manager

You are the head of a leading manufacturer in charge of North American operations working through a normal day when suddenly you get a report from one of your largest factories that shows a list of product defects. The trend appears to have started some time ago and keeps climbing, but the factory manager can’t seem to locate the source of the defect. Everything in the factory seems to be running as intended. Do we take the equipment offline to run more detailed diagnostics, or do we continue and hope the trend ceases and product output reverts to normal? Finally, you reach the decision, the equipment will come offline for nonroutine maintenance. After hours of diagnostics, there seems to be a breakthrough. Although everything looks normal on the surface, there is a strange anomaly with the PLC software. With further diagnostics, it becomes evident that the factory was hacked! But why was this not discovered earlier? The hackers must have been very clever and kept the malicious code hidden so that the operators would think everything was normal. After weeks of progressively increasing defects and having to take equipment offline, the factory is back up and running, but were we successful in quarantining all the effected equipment? Fortunately, we require all factory floor devices, including the drives and servos, to have a hardware root-of-trust so that we can confidently push a software update to all potentially affected machines globally. Maybe this update will save our plant in Japan from having the same issues.

With the cyber attack surface changing, there is increased security risk and a greater need for security solutions at the edge. It is imperative that factories adopt a resilient posture against cyber attacks, meaning the ability to detect and recover when an attack takes place. The question is no longer if I will get hacked, but when will I get hacked. Building a connected factory requires smart edge devices to be able to recover from attacks. This requires security to be implemented at the lowest level: the hardware itself. Being able to trust the lowest levels of a device’s boot and issue software updates enables a factory to recover quickly and resume normal operations.

What Is Changing the Security Risk?

The need for edge computing means more devices are being connected that interact with the real-world based on the data they receive. These smart devices are critical to enabling the outcomes of today’s digital era. As computing power becomes more pervasive, so does the need for security to address the increased cyber risk. It is only a matter of time before the next smart coffee machine makes the news for being held ransom by a cyber attack. Even though the ransom will be negligible, the incentive to attack a coffee machine exists because there is a low barrier to facilitate a successful attack, which makes performing the attack worthwhile. Consider the effort one might put toward holding an entire factory ransom. The potential reward increases significantly, as does the incentive for the attacker. Only relying on firewalls for critical infrastructure is no longer effective with the converged IT and OT networks. The assumption should be made that someone has already gained access to the factory network. For this reason, device integrity and robust authentication protocols must be in place for all connected devices.

Network connected devices need to be able to authenticate with other devices on the network, establish shared keys, perform signatures on data, and validate data being received. There are standard ways for doing this, but the factory presents constraints that can make adapting security challenging for some use cases. For instance, the sensitivity to time in motion control applications can create latency tolerances that make traditional means of doing device-to-device authentication prohibitive. Using standard public key infrastructure, devices will challenge each other to establish authenticity and exchange a shared session key using means such as TLS. This method has already been adopted to many factory applications; however, this method is prohibitive in high speed motion-control applications as many devices need to interoperate together on a specific time scale. When latency requirements are measured in microseconds, the appropriate message authentication scheme must be selected to achieve the desired level of security and speed. The flow of data from the controller to all devices on the control loop need to be received congruently. One method to effectively enable this flow of data is to have all devices use the same shared session key. This requires a unique network configuration that allows devices to
authenticate with a security manager that will provide the same session key to all devices on a designated security group. These keys will be exchanged using standard TLS and revert to alternative protocols during time critical operation.

Extending Identity and Integrity to the Edge of the Network

The ADI Chronous™ portfolio of Industrial Ethernet connectivity solutions enables secure communication at the edge of the control loop. Our devices exist at the communication endpoints and are capable of securing network communications at each node point within the system while minimizing trade-offs in power, performance, and latency. These scalable Ethernet solutions provide the means to extend security in highly time sensitive applications to meet the changing security risks, such as:

- Securing the edge of the factory control network to establish a resilient and trusted architecture.
- Allowing for secure connectivity of robots, drives, and production machines within an integrated OT/IT TSN network.
- Providing means for authentication and encryption (as required) in a highly time critical environment.

Analog Devices’ security solutions for ADI Chronous Industrial Ethernet enables the rapid adoption of the connected factory. Leveraging ADI’s secure development processes, our Industrial Ethernet solutions ensure the security design enables the system application while allowing for risk to be managed throughout the product lifecycle. ADI’s Industrial Ethernet solutions provide security features such as key generation/management, secure boot, secure update, and secure memory access. Integrating security in devices at the edge of the industrial control loop will provide trust in data necessary to scale solutions capable of making real-time decisions on the factory floor.

Accelerate the path to Industry 4.0 by assuring:

- Machine/worker safety
- Reliable operation
- Product quality

With the next cyber attack happening today, how will you address the changing cyber risk? Will the attacker target the device’s software or will it be a network attack inserting bad data? Regardless, your devices will need to provide the ability to communicate securely and recover from the next attack. This requires security to be implemented at the lowest level: the hardware itself. Being able to trust the lowest levels of a device’s boot and issue software updates, enables a factory to recover and resume normal operations.

About the Author

Erik Halthen joined ADI through the acquisition of Sypris Electronics in 2016 and brings extensive background in cyber security solutions. As part of ADI’s cyber security center of excellence, Erik has taken on the role of security systems manager for industrial solutions. Leveraging his experience as a cyber security program manager in the defense industry, Erik is focused on developing leading security solutions to meet key market demands in Industrial IoT. He can be reached at erik.halthen@analog.com.

Engage with the ADI technology experts in our online support community. Ask your tough design questions, browse FAQs, or join a conversation.