# Accelerating Industry 4.0: Extending the Secure Edge in Industrial Control Systems

Erik Halthen
*Analog Devices, Inc.*

## The Perception of Industrial Control Systems Cyber Security

Cyber security in industrial control systems (ICS) is poised to delay the adoption of Industry 4.0. Many business leaders find it hard to understand ICS cyber security challenges as there are many factors contributing to their complexity. Furthermore, the engineers developing solutions for industrial control systems have likely not seen significant cyber security requirements at the device level. Traditional methods for securing industrial control systems have relied on limiting access to networks and devices, and monitoring network traffic through information technology (IT) solutions. A product lead working on devices in a factory will find it easy to dismiss cyber security as an IT problem. However, the traditional methods for securing industrial control systems will no longer be sufficient as Industry 4.0 looms on the horizon. The challenges of ICS cyber security will ultimately delay the adoption of Industry 4.0 if companies do not have a strategy to address device security at the edge. In order to adopt and capitalize on Industry 4.0, cyber security needs to be a critical part of the business plan. Analog Devices recognizes the challenges that Industry 4.0 brings to the market. Although the industrial market has traditionally been slow to change, the adoption of Industry 4.0 has occurred at a record pace that exceeds expectations. With these changes, cyber security is becoming one of the most challenging obstacles to the adoption of Industry 4.0. ICS cyber security standards and guidelines are in place or being established to secure the factory, but they do not provide guidance on how to accelerate Industry 4.0 initiatives. It is our mission to enable our customers to more rapidly adopt Industry 4.0 solutions by extending the secure edge and making it easier to implement security.

## Industry 4.0 Is Changing Industrial Control Systems Cyber Security

There is a reason Industry 4.0 is changing the ICS cyber security problem. The very nature of Industry 4.0 is to increase access and accessibility of control of the devices in the factory. This means increased access to the data to expand transparency, reduce network planning, lower CapEx, reduce OpEx, improve bandwidth, and optimize machine interworking. Increasing access and accessibility of control means that the cyber security risk assessment of the factory system is changing. ICS cyber security solutions need to adapt to address the changing risk, and traditional

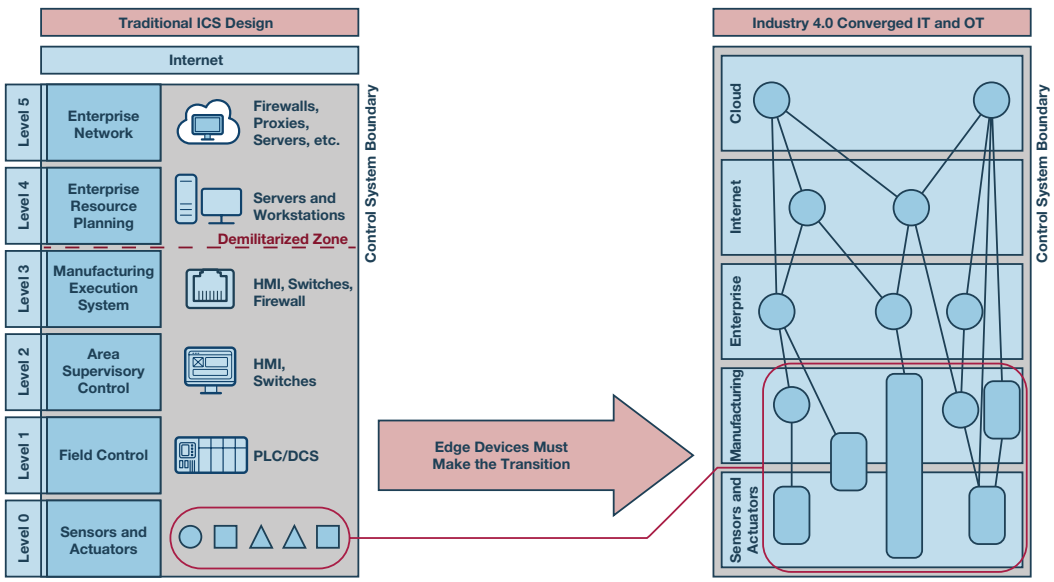


*Figure 1. Edge devices require transition to adopt for Industry 4.0.*

countermeasures applied to the system, such as firewalls and placing a device behind a locked door, are counterintuitive to the goals of Industry 4.0. This means devices will need to be security hardened to enable increased functionality in a secure method. Identity and integrity will be at the core of every device in the field to enable trusted data and secure operation.

There are many different standards in the industrial market that provide guidance on implementing security in industrial control systems. For example, NIST provides security guidance with U.S. governance. IEC 62443 is a security standard in draft form for the international market with governance in Europe. These are two of the most predominant standards, providing useful guidelines for implementing security and assessing one's security posture for industrial control systems; however, they do not provide guidance on how to accelerate the adoption of Industry 4.0. IEC 62443 is currently absent any guidelines for implementing security below the PLC and an ISA99 working group has recently been established to address cyber security at the bottom layers of the factory within the IEC 62443 framework. Today, to meet an acceptable security posture of a system, countermeasures must be applied to devices that do not reach a sufficient level of security. These countermeasures typically rely on methods such as firewalls to limit access and section off or isolate vulnerable devices. In the future, devices will need to reach higher security levels to enable the transition to Industry 4.0.

## Analog Devices: Extending the Industrial Control Systems Cyber Security Edge

Analog Devices is in a unique position to extend the secure edge. Our traditional market space is at the physical edge, where the real world is translated into digital signals and data is born. This gives us the opportunity to establish trust in data by providing identity and integrity much earlier in the signal chain and establish a new definition of the secure edge. Traditionally, the secure edge has originated at gateways, PLCs, or even servers in the industrial control systems security framework.

This view is reminiscent of the traditional IT cyber security view of the factory but it persists throughout the industry. The prospect of driving the secure edge lower in the signal chain is enticing because it enables higher confidence in the decisions that are being made from that data. The earlier identity and integrity can be established in the signal chain, the more trust and confidence can be placed in the data that is driving decisions.

ICS cyber security cannot be addressed by a one size fits all solution and an in-depth defense approach must be adopted and applied based on the risk assessment of the system. Analog Devices has a strategy to extend the depth of ICS cyber security as Ethernet is adopted at the edge. Enabling Industry 4.0 requires the factory to adopt new connectivity methodologies. This means that Ethernet has taken, and will continue to take, a larger role in industrial control systems. Analog Devices' security strategy is to focus on where there is Ethernet connectivity because this significantly changes the impact any one device on the network has on the system. Our current family of industrial Ethernet solutions and TSN solutions has been the focus of our security development. In the near term, the fido5000, RapID® Platform that provides 2-port, multi-protocol connectivity will be enabled with security features that provide key generation/management, secure boot, secure update, and secure memory access to protect against network bound attacks. The product family roadmap includes single-chip solutions that feature a hardware root of trust, secure device lifecycle management, secure communications/mutual authentication, and tamper protection. As the industry continues to adopt sensors with increased intelligence, connectivity will extend lower in the factory driving additional security requirements at the device level. Analog Devices is committed to developing a secure portfolio that enables easier adoption of ICS security solutions and establish trust at the edge to accelerate the adoption of Industry 4.0.

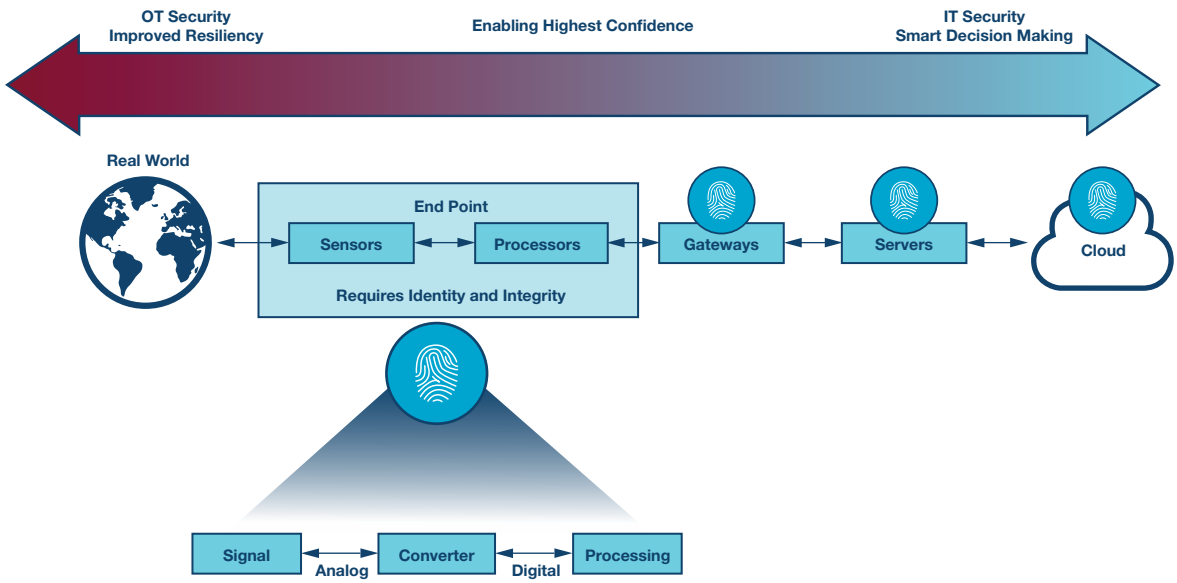


*Figure 2. Enabling the highest confidence in decisions: where physical to digital conversion occurs.*

## About the Author

Erik Halthen, part of ADI's acquisition of Sypris Electronics in 2016, 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*.

## Online Support Community

EngineerZone™
SUPPORT COMMUNITY

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

**Visit *ez.analog.com***

**Analog Devices, Inc.**
**Worldwide Headquarters**

Analog Devices, Inc.
One Technology Way
P.O. Box 9106
Norwood, MA 02062-9106
U.S.A.
Tel: 781.329.4700
(800.262.5643, U.S.A. only)
Fax: 781.461.3113

**Analog Devices, Inc.**
**Europe Headquarters**

Analog Devices GmbH
Otl-Aicher-Str. 60-64
80807 München
Germany
Tel: 49.89.76903.0
Fax: 49.89.76903.157

**Analog Devices, Inc.**
**Japan Headquarters**

Analog Devices, KK
New Pier Takeshiba
South Tower Building
1-16-1 Kaigan, Minato-ku,
Tokyo, 105-6891
Japan
Tel: 813.5402.8200
Fax: 813.5402.1064

**Analog Devices, Inc.**
**Asia Pacific Headquarters**

Analog Devices
5F, Sandhill Plaza
2290 Zuchongzhi Road
Zhangjiang Hi-Tech Park
Pudong New District
Shanghai, China 201203
Tel: 86.21.2320.8000
Fax: 86.21.2320.8222


TA20848-0-12/18

*analog.com*

ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™