The Role of Hardware Security to Meet Industry 4.0 Aspirations

Erik Halthen
Analog Devices, Inc.

Industry 4.0 Aspirations and the Cyber Security Implication

Industry 4.0, which involves the digitization of factories, can mean many different things to organizational leaders in the industrial market sector, and the implications of digitization can have an extensive impact on cyber security as factory devices become smart and connected. For example, this can mean transforming your factory to realize higher levels of autonomy and customization that improve the total cost of operations and bring higher value to customers. It can also mean suppliers of systems and subsystems are making factory devices smarter to enable real-time decisions and autonomous interaction of manufacturing cells within larger, multicelled systems and across enterprise systems. Depending on how you aspire to take advantage of the Industry 4.0 solutions, the strategy for adopting these solutions will depend on where they will be integrated in the value chain and the depth of integration within the factory.

The digitization of the factory is transforming all aspects of the value chain and directly affects both the top line and bottom line of a business. What is most commonly discussed is innovation that unlocks new lines of revenue, such as new products, services, or some combination of the two. Digital production, the use of processing, and analyzing data at the edge are demanding new product innovation, while the collection of the metadata is resulting in new services that optimize control, maintenance, and usage. Both aspects of digital production exist in different parts of the value chain that directly impact revenue performance. On the flip side, cost reduction initiatives are focused on improving supply chain efficiency and optimizing operational performance. These improvements require the adoption of more capable products and services in one's own factory. It is the consumption of new product innovation that is necessary to realize below the line benefits of Industry 4.0. Depending on how one aspires to take advantage of Industry 4.0 solutions, the cyber security strategy will change to ensure the successful adoption and scaling of digital solutions in the factory.

The cyber security strategy will also change depending on how pervasive digital solutions are integrated at the edge of the industrial control loop. Traditional industrial automation architecture is highly disparate and relies on segregating control of field devices from the rest of a plant's information systems, services, and applications to guard against cyber security threats. Additionally, actual field devices are typically point-to-point solutions with limited data exchange and edge processing, which limits the cyber security risk any one device contributes to a system. Disrupting this typical architecture is no easy task and will need to be undertaken in a staged approach. Aggressive adopters of Industry 4.0 solutions will need to determine how deep they want to integrate new technology in the factory and drive a cyber security strategy that enables the realization of these aspirations. The new industrial automation architecture is poised to look significantly different. Where the factory is traditionally segmented into five different levels using the Purdue model or similar, the future factory architecture will likely not equate to the same model. The field device of the future will combine sensing and actuating with manufacturing execution and control. These devices will not only be networked into an integrated connected architecture on the factory, but some of them will be directly connected to the enterprise system, internet, and cloud services, which greatly increases the cyber security risk any one device has to the system. In whatever way the future Industry 4.0 architecture is perceived, achieving the end goal will take a multistaged approach and a cyber security strategy that is linked to the desired depth of integrating digital solutions in the factory.

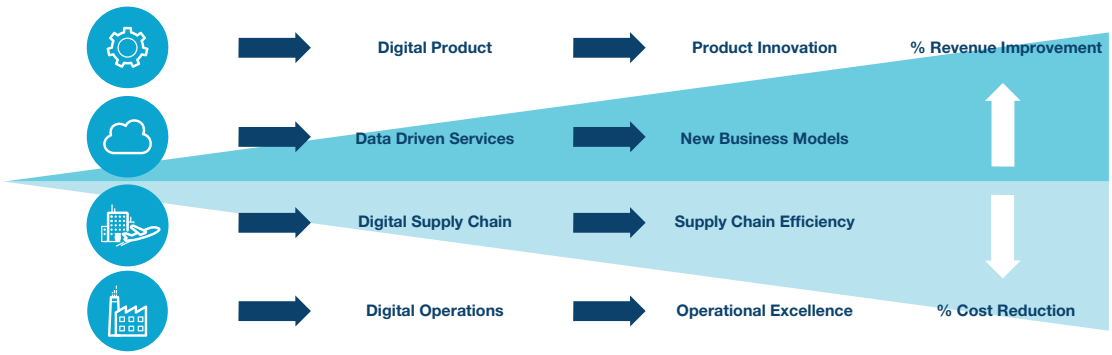

Figure 1. The digitization of the factory is transforming all aspects of the value chain and directly affects both the top line and bottom line of a business.

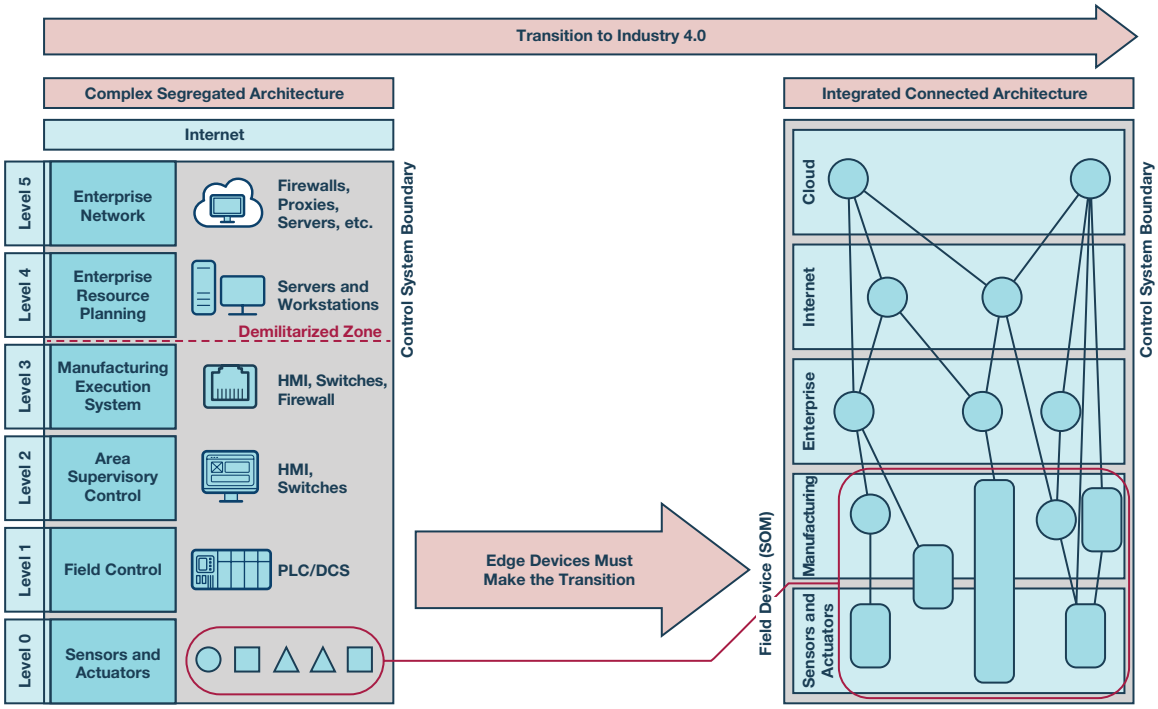

Figure 2. Transition into a fully digitized Industry 4.0 factory.

Three Steps to the Realization of a Cyber Secure Industry 4.0

There are many different perspectives on what Industry 4.0 will look like when its solutions are fully integrated. Some believe the traditional factory design will largely remain intact, while others have the more aggressive view that the new factory will hardly be recognizable by traditional standards. What everyone can agree on is that the factory is changing and it won't happen overnight. There are some obvious reasons for this transition, but the primary reason is the lifespan of devices in the field today. These devices are designed to operate well over 20 years and could remain operational much longer. Efforts may be made to retrofit these devices to enable additional functionality and connectivity, but they will be limited by their hardware designs and the factory system architecture will have to compensate for their inadequacy. From a cyber security perspective, these devices will always be limited and present a cyber risk. A secure device requires a secure architecture and system design approach. Retrofitting a device with security features is a stop gap approach that will always leave cyber security vulnerabilities. Fully transitioning to the digitized factory will require that devices reach high levels of security hardening to be resilient to cyber attacks without impeding their ability to share information in real time and to make decisions. Resiliency—the ability to recover quickly from difficulties—has a huge influence on how cyber security is implemented and the necessary steps to a cyber secure Industry 4.0.

The first major hurdle to overcome is achieving compliance to new cyber security industry standards and best practices. To achieve compliance within a changing factory requires a different approach. The traditional methods of applying information technology (IT) security solutions that isolate, monitor, and configure network traffic will not provide the required resiliency in the Industry 4.0 factory. As devices become connected and share real-time information, hardware security solutions will be required to enable autonomous real-time decisions while maintaining resiliency in the factory. As the approach to cyber security changes, organizations will also need to adapt to address the new challenges. Many organizations are restructuring to build a cyber security competence that is both separately managed from the traditional engineering organization and integrated throughout the organization's project teams. Building an organization that enables the implementation of a cyber security solution strategy to meet industry standards and best practices is the first major step to achieving the Industry 4.0 aspiration.

After organizations gain solid footing with emerging security standards and when they are equipped to manage security requirements across product life cycles and cross-organizational boundaries, they can direct their focus toward increased autonomy within factory cells. Autonomy can only be achieved when devices in the factory become smart enough to make decisions based on the data they receive. The cyber security approach is a system design that builds on-edge devices capable of substantiating trust in data where the data is born. The result is the confidence to make real-time decisions provided through a cyber secure system that is capable of accepting input from the real world, assessing its trustworthiness, and acting autonomously.

The last issue will be building a factory that is not only connected to the cloud, but that operates in synchrony with other factory systems through cloud services. This requires much more widespread adoption of digital solutions and will ultimately be the final hurdle due to the time required to fully transition to the digital factory. Devices today are already connected to the cloud, but in most cases, this is only to receive data. This data is analyzed and decisions are made remotely from the factory floor. A product of these decisions may be to accelerate or delay maintenance or fine tune an automated process. Today, it is rare that these decisions would be executed from the cloud as the field control is local to the factory and segregated from the enterprise system. As more autonomy is adopted on the factory floor, it will be more relevant to monitor and control a factory through cloud services, and to share real-time information across enterprise systems.

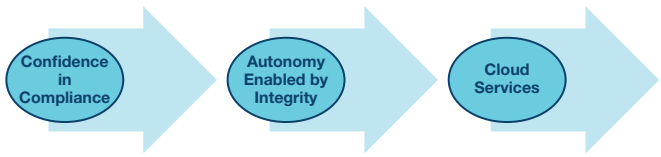

Figure 3. Autonomy adoption on the factory floor.

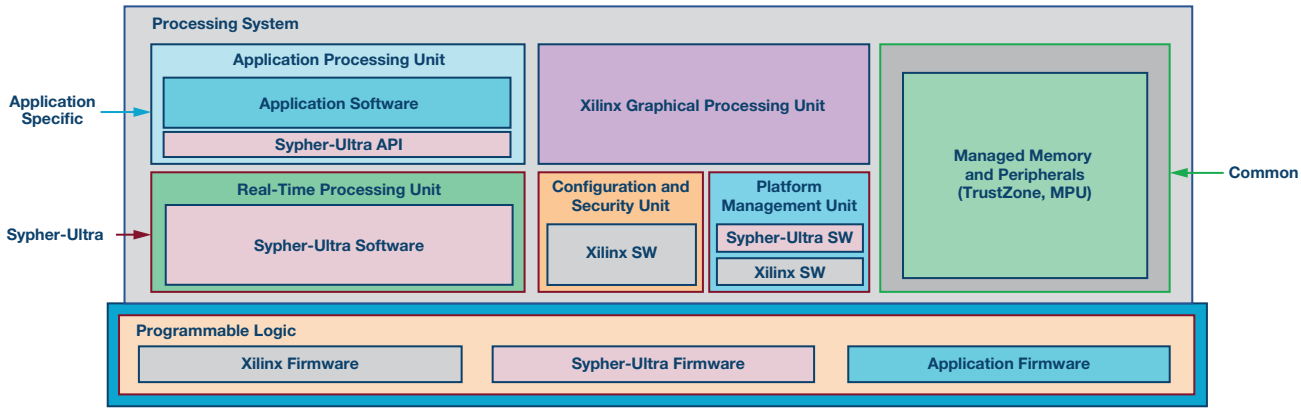

Figure 4. Analog Devices' Sypher-Ultra implementation.

Enabling the Connected Factory with Hardware Security

The need for hardware security is being driven by industry standards that reach higher levels of security to enable connected solutions in the factory. Increasing access and accessibility of control means new risks that traditional IT security solutions are ill-equipped to defend against without combining device level security with a hardware root-of-trust. As devices are connected to a network, these devices become access points to the system at large. The damage that can be caused from any one of these access points extends to the entire network and can make critical infrastructure vulnerable. Traditional security methods that rely on firewalls, malware detection, and anomaly detection need constant updating and configuration, and they are prone to human error. In today's environment, it should be assumed that an adversary is already in the network. To defend against these adversaries, a defense-in-depth and zero-trust approach needs to be adopted. To achieve the highest confidence that connected devices are operating as expected, a hardware root of trust is required in the device. Putting the right hardware hooks in devices today is critical to enabling a transition to tomorrow's digital factory.

Utilizing the Xilinx® Zinq® UltraScale+™ MPSoC (ZUS+) family of FPGAs, Analog Devices has developed Sypher™-Ultra, which provides higher levels of confidence to the integrity of data being generated and processed through its high assurance cryptographic system with multiple layers of security control. It leverages the security foundation of the ZUS+ along with additional Analog Devices developed security features to facilitate end products that meet security requirements such as NIST FIPS 140-2, IEC 62443, or Automotive EVITA HSM. The Sypher-Ultra resides between the embedded ZUS+ capability and the end application to provide design teams with a single-chip solution to enable secure operations. In order to provide high assurance security, the Sypher-Ultra platform utilizes a trusted execution environment (TEE) that provides a foundation for secure data at rest and in motion. Security-related features are executed primarily within the real-time processing unit and the programmable logic to afford design teams the ability to easily add their application within the application processing unit. The design eliminates the need for product teams to master all the complexities of security design and certification, while providing high levels of confidence in secure operations.

Formulating a path to achieve higher device level security is challenging especially considering the time to market constraints to meet the demanding pace of the digital factory. The complexity of implementing security requires unique skill sets and processes. Analog Devices' secure platform provides design teams with a solution to implement security closer to the edge of the industrial control loop. Offloading implementation complexities from product design teams, such as the security design, certification to security standards, and vulnerability analysis, greatly reduces risk and design time. Analog Devices' solution provides easy to use secure APIs on a commonly adopted platform that enables the coexistence of high assurance security and higher level applications on a single FPGA. Analog Devices' Sypher-Ultra product enables secure use of the Xilinx Zynq UltraScale+ MPSoC (ZUS+) family to isolate sensitive cryptographic operations and prevent unauthorized access to sensitive IP, which provides a path to the connected factory through hardware security at the edge.

About the Author

Erik Halthen, part of ADI's acquisition of Sypris Electronics in 2016, possesses an 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

analog.com

ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™