Whitepaper

A Solution for 360-Degree Industrial Internet Security

ABB, Microsoft, and NXP provide ingredients for an end-to-end co-engineered solution for the Industrial Internet of Things that helps reduce risk, time to market, and cost.

Contents

Executive summary

The landscape

The Internet of Things (IoT), which includes the IIoT, is where the physical world meets the universe of data, connecting industrial sensors and actuators to cloud platforms so information can be captured, analyzed, and transformed into business value. The emergence of real-time edge processing and cloud analytics applications offer Industry 4.0 new opportunities as well as challenges with complexity in both implementation and security.

Inadequate security in these industrial implementations heightens risk to organizations, and value and opportunity are on the line when solutions do not function as expected. More concerning, compromised IoT devices can be points of entry for unauthorized access and potential security breaches.

Still, the expertise to correctly and completely implement the system-level security can be challenging. Building a solution from scratch is a complex undertaking that can yield unproven results, runaway timelines, and high costs. Therefore, IoT systems should follow a set of security best practices which call for integrated security in depth, with roles in data-protection played by the end customer, silicon and device providers, solution operators and integrators, and cloud operators (see Figure 1).

This whitepaper is intended to describe how ABB, Microsoft and NXP have been partnering to deliver an approach to improve security in information technology (IT) and operational technology (OT) environments.

This paper introduces a 360-degree approach to security in IoT, from edge to cloud. This topic is especially relevant for Operational Technology (OT) business leaders who must guarantee secure operations of their IoT devices, systems, and cloud solutions. The paper describes how ABB, Microsoft and NXP guide business leaders in addressing IoT security. Our roles at ABB, Microsoft and NXP each provide elements of an overall integrated solution for secure cloud-based IoT connectivity and continuous monitoring (see Figure 1). This ecosystem-based approach helps ensure a continuous, comprehensive, end-to-end security approach. Because the providers bring decades of experience, projects are predictably successful, thereby decreasing risk of vulnerable products and solutions considerably.

The three companies' roles in providing a cybersecurity solution include the following:

ABB is a manufacturer of digital-enabled products and IoT connectivity solutions that incorporate its own edge hardware. ABB works with a variety of partners to deploy secure solutions, including NXP and Microsoft, and act as an end-to-end integrator for IoT solutions and connectivity from its ABB Ability™ cloud, which is powered by Microsoft Azure.

Microsoft Azure builds security, visibility, and control into every stage of IoT deployment, using the NXP silicon architecture for secure operation from IoT devices to the cloud. Microsoft's purpose-built Azure IoT security capabilities extend to Azure Sphere, Azure Sentinel, the Azure RTOS, Azure Defender for IoT, Azure Security Services and beyond to protect IoT infrastructure and information wherever it resides.

NXP contributes significantly to the expansion of secure IoT ecosystems with a comprehensive and secure product portfolio including application processors, microcontrollers, NFC devices, smart labels, secure elements, authentication devices, and related services.

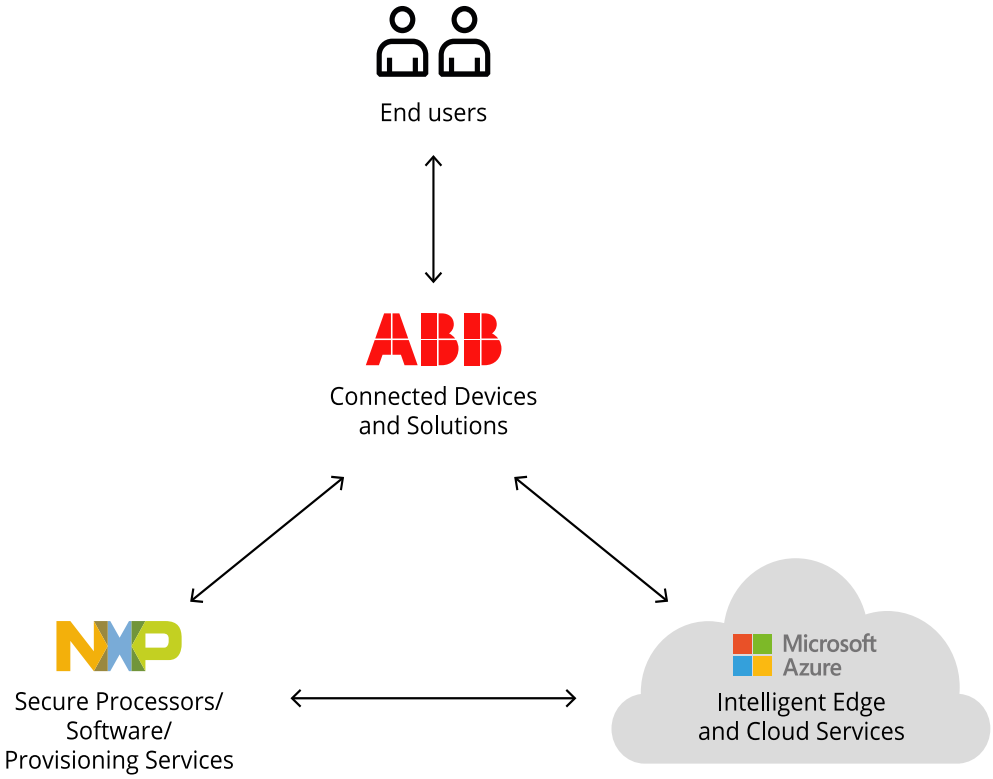

Figure 1: Expertise from ABB, Microsoft, and NXP to create best-in-class IoT security solutions

Introduction

Threats and vulnerabilities in IoT security

The ongoing digital transformation in IoT settings is only accelerating, as Industry 4.0 and IoT drive manufacturing and other industrial processes toward greater optimization while creating new value chains. Decision-makers cite security as their greatest concern related to deploying IoT technologies[1]. However, many organizations are unaware of the full range of security concerns and some lack the expertise to address them.

[1] Base: 262 global decision-makers of IoT planning and deployments. Source: A commissioned study conducted by Forrester Consulting on behalf of Microsoft, June 2019.

Compounding this difficulty is a lack of comprehensive IoT expertise within most organizations. Instead, there are typically separate IT and OT domain experts operating without overarching management to coordinate them. And although the merger of IT with OT components unleashes vast benefits for data collection and analysis, new cyber-risks emerge. Indeed, attacks on industrial automation systems and critical infrastructure are on the rise in terms of severity, sophistication, and frequency - exposing organizations to business risks including safety and environmental incidents, revenue loss from production downtime, and theft of sensitive intellectual property such as proprietary formulas, designs, and manufacturing processes.

Security challenges and implications

Introducing risk as IoT expands

As a result of its expansion, the IoT enables the collection of vast amounts of data and rapid, precise analysis of physical parameters in the industrial realm; this process generates greater knowledge, allows predictions, and can create immense value for customers. But as IT and OT converge, a familiar threat profile emerges: inadequate patching, malware, ransomware, botnet attacks, and more, all of which can lead to extensive financial losses.

The reliance on remote connectivity in modern architectures, which include devices such as smart sensors and actuators, results in an increased exposure to risks. Particularly in the context of endpoints in industrial settings, cybersecurity measures may not be implemented or adhered to the same way as in conventional IT settings. IoT networks must therefore be secured from a variety of attacks, compared to conventional network endpoints:

Local attacks are based on physical access to a device, often as a means of gaining knowledge that can be used to mount automated **remote attacks**, which can be more scalable because they don't require local access.

Logical attacks exploit weaknesses in software, using wired or wireless access. These attacks on devices or internet services may be automated and mounted by amateurs on a large scale.

Physical attacks hack devices based on physical characteristics during device operation to break a critical piece of security, such as inferring the contents of restricted memory or a cryptographic key.

Manufacturing attacks aim to steal the firmware and credentials of devices, allowing a manufacturer to counterfeit genuine devices.

STRIDE—or spoofing, tampering, repudiation, information disclosure, Denial of Service (Dos), and escalation of privilege—attacks all attempt to access, capture, modify, or destroy cloud-based data with the goal of manipulating or harming an IoT solution or system.

Landscape and best practices

The need for security in every connected device is largely underestimated. Without adequate security implementation in the device, cybercriminals and attacks of all types can more easily proliferate. Underpinning the exposure that this mindset enables is the challenge of integrating the diverse elements of the IoT environment to create a consistent and strategic security posture across them as new deployments skyrocket.

Effectively mitigating business risks requires addressing threats to devices, applications, services, connections, and data holistically, from end nodes to edge devices and to the cloud. Highly secure network-connected devices require adherence to some specific best practices and properties to remain protected throughout their development and operation: hardware-based root of trust, small trusted computing base, defense in depth, compartmentalization, certificate-based authentication, security renewal, and failure reporting.

For industrial focused solutions, cybersecurity compliance with governmental and industrial regulations and standards, such as IEC 62443, can protect deployments for their entire lifecycle. As a result, IEC 62443 has gained global support as a way to improve the safety, availability, integrity, authenticity, and confidentiality of IoT systems. IoT devices that conform to such standards can be trusted to protect data and minimize risk, because they use industry-recognized mechanisms to address and mitigate current and future security vulnerabilities. For instance, ABB's Security Assurance Center performs IEC 62443 EDSA Communication Robustness Testing on applicable ABB products. And NXP's EdgeLock SE050 is a tamper-resistant, Common Criteria Evaluation Assurance Level 6+ (CC EAL 6+) certified product that helps secure IoT devices and meets the stringent requirements of IEC 62443 standards, while eliminating much of the complexity of the security implementation. NXP EdgeLock SE050 allows the OEM to strengthen the IoT device even more against logical and physical attacks, and the advanced cryptographic features further help enable the device to be future-proof.

The cost of gaps in IoT security

Data breaches and financial losses

These increasingly sophisticated threats put organizations at risk of potentially catastrophic losses to business continuity. Compromised IoT assets can interfere with the operation of sensor networks, industrial equipment, and other infrastructure, potentially causing massive financial losses and reputational damage. A major pharmaceutical company lost more than US $1 billion due to production downtime and cleanup costs from the NotPetya attack[1], which also caused losses of hundreds of millions of dollars for a major food manufacturer, a global shipping and logistics firm, and a global manufacturer of construction materials[2].

A global aluminum manufacturer lost US $60-70 million from a ransomware attack that crippled production operations[3].

Damage to global business value

Consulting company Accenture estimates the global business value at risk from cybercrime over the next five years at US$5.2 trillion[4]. Put another way, the amount of potential loss from cybercrime over the next five years is approximately twice the size of the entire annual economy of the United Kingdom. Manufacturers across all industries have become significant targets, while intruders have broadened their malicious behavior from corporate IT to industrial OT control systems. As more devices are connected, large scale attacks, such as botnet attacks, are a growing concern.

[1] https://www.bloomberg.com/news/features/2019-12-03/merck-cyberattack-s-1-3-billion-question-was-it-an-act-of-war

[2] https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[3] https://www.securityweek.com/norsk-hydro-receives-first-insurance-payout-following-cyberattack

[4] Ponemon Institute and Accenture Security. "The cost of cybercrime: Ninth annual cost of cybercrime study, unlocking the value of improved cybersecurity protection." https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

Securing IoT platforms and infrastructures

Solutions throughout the lifecycle

Cybersecurity is critical at all stages of an IoT device lifecycle. Security starts before the product design in the conception phase, accompanying product development, product certification and qualification, and manufacturing processes. It plays an essential part in end-customer or operator onboarding, too, and is a key driver during operation of the device and its associated services.

Due to the high complexity of IoT systems and the rich feature set customers expect from modern devices, it is nearly impossible for any solution developer or operator to start from a blank sheet. Instead, they often integrate off-the-shelf hardware components, software libraries, and services. For this reason, among others, the IoT industry must introduce mature ecosystem solutions to manage the entire lifecycle of the product, starting with secure design and continuing throughout implementation, onboarding, operating, updating, and end-of-life phases (see Figure 2).

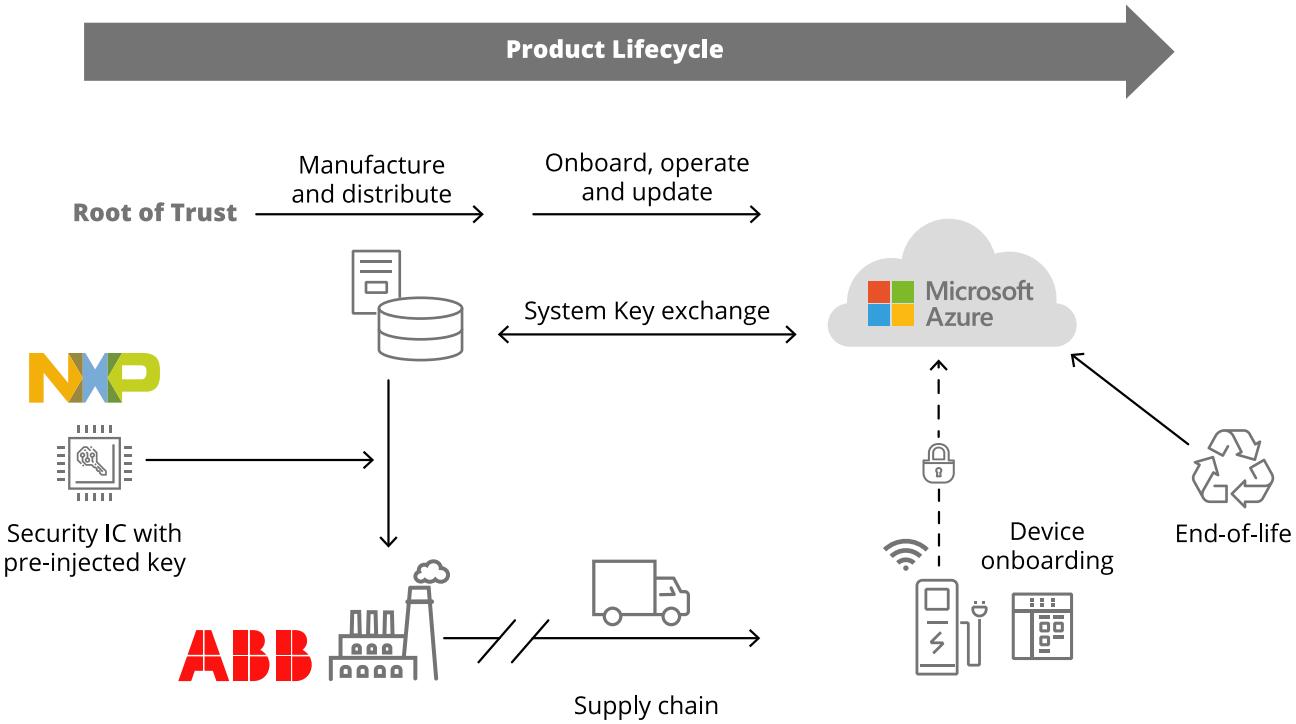

Figure 2: An example of IIoT device security across the value chain and entire device lifecycle

A secure supply chain

Hardware such as processors, microcontrollers, or secure elements (SEs) usually integrate blocks for common functionality that come from global intellectual property (IP) vendors, and many silicon providers have their integrated circuits (ICs) manufactured in highly specialized fabs. But trust in the silicon provider doesn't necessarily extend to its suppliers. That holds true for software and cloud services, where solutions depend on third-party libraries, frameworks, and other building blocks, as well as contractors or subsidiaries. Even the simplest of today's IoT solutions make up highly complex systems comprised of a hierarchy of components, all of which must be vetted and authorized to ensure tight security. Following a 360-degree approach to cybersecurity means controlling this "system-of-systems" from design to manufacturing, operation, and beyond.

Development, manufacturing, and provisioning

Unsecured manufacturing can leave ICs and devices vulnerable to malware injection, counterfeiting, key capture, overproduction, and the creation of security backdoors in the supply chain. Chips and components—as well as the manufacturing machines themselves—must be protected against tampering and attacks, both local and remote in a highly secure process.

Operate and update

Here, the device is protected by its intended security and privacy features, which must perform in scenarios where the device is left unattended or stolen. While in operation, the device must also accept functional or security enhancements, meaning the update mechanism must be protected against attackers, too.

Onboarding and offboarding

In the onboarding phase, the device comes in contact with the network for the first time. Security features must protect against remote attacks and ensure that attacks against specific operational devices are not extensible to others. During offboarding, care needs to be taken to securely wipe customer or other sensitive data from the device while still allowing re-use and a subsequent onboarding.

End of life

Even after the device has been damaged, decommissioned, or destroyed, its security functionality still must be able to fend off a scalable attack by unauthorized parties. Protections must continue to prevent entry into the ecosystem and the extraction of keys, sensitive data, and other secrets of the device.

Business solutions from the device-to-cloud ecosystem

This overarching commitment to cybersecurity can only be enabled when silicon solution providers, cloud service providers, and solution operators act in harmony. Enabling security across an IoT infrastructure requires a unified end-to-end approach, enabled by multi-provider solutions from a trusted device-to-cloud ecosystem. IoT solutions that rely on Microsoft Azure and use solution components provided by ABB and NXP provide secure connectivity from the silicon outward to the device, through the network edge, and to the cloud.

Solutions built on security

An end-to-end security emphasis

ABB, Microsoft, and NXP each maintain robust and independent services and standards for security, that are described in the following.

Microsoft Azure: Foundation for IoT infrastructure

Microsoft Azure – a full end-to-end platform – reaches out into IoT environments at the device, edge, and cloud levels enabling holistic security:

- At the device level, Azure Sphere provides a hardware and software device platform for creating secured, internet-connected devices based on Azure-certified microcontrollers from partners, including NXP. For resource-constrained devices, Azure RTOS, an embedded development suite including a small but powerful operating system, provides reliable and ultra-fast performance. For more resourceful devices, Windows for IoT is the foundation for an intelligent edge with world class developer tools, enterprise grade long term support, and a global partner ecosystem. Finally, built explicitly to connect to any device, the Azure IoT environment enables ecosystem members to design and build devices according to their specific needs and their responses to individual risks.
- Azure IoT Edge enables edge gateways placed between endpoints and the rest of the IoT infrastructure, providing an additional layer of in-depth security without extra effort from IT organizations. Those benefits are broadly useful to all types of endpoint devices, particularly those that may not be manufactured to high security standards.
- The Azure cloud, hardened from the ground up, is built for security and scale, enabling ease of use while also helping ensure protection against threats. Customers can reinforce this protection with Azure Defender for IoT, a practical, agentless solution for securing brownfield IoT/OT environments. Rapidly deployed—typically less than one day per site—the solution auto-discovers all your IoT/OT assets and continuously monitors industrial networks for anomalous or unauthorized behavior, with zero impact on OT performance or reliability. It analyzes specialized IoT/OT protocols (IEC 61850, Ethernet /IP, etc.) and secures diverse equipment such as PLCs, HMIs, and historians from all major OT automation vendors (including legacy Windows systems like XP that can't easily be upgraded). The solution can be deployed fully on premises or in Azure-connected environments, where it integrates via Azure IoT Hub.
- Azure Defender for IoT is deeply integrated with Azure Sentinel and supports third-party SIEM platforms (Splunk, IBM QRadar, ServiceNow, etc.) to provide a birds-eye view of security across both IT and OT networks. Sentinel leverages machine learning, automation, and large-scale intelligence from decades of Microsoft security experience to accelerate threat detection and response in your SOC.
- For device builders, Microsoft also offers an additional layer of security via lightweight endpoint detection and response (EDR) agents for embedding security into new IoT/OT devices.

ABB: Edge intelligence and secure device-to-cloud integration

As the edge-to-cloud integrator and solution provider, ABB delivers secure IoT solutions from connected devices, systems, and factories to the ABB Ability™ platform, which provides a set of common software technologies and services at the device, edge and cloud levels. ABB's solutions enable the rapid creation, extension, deployment, and operation of secure industrial, cloud-based applications. Both draw on ABB's deep domain expertise to protect the cloud, manage the vulnerable network edge, and generate value in the physical world.

The ABB Ability™ digital solutions that run on Microsoft Azure cloud support connectivity and delivery of web services. This ecosystem solution provides results across a range of use cases, such as factory and building automation, energy management solutions, and secure transmission of encrypted by managing continuous security, monitoring operational conditions, and prompting predictive maintenance to keep systems running at optimal conditions.

Security is handled in two different ways - within ABB and in the cloud. Microsoft is responsible for the cybersecurity of the cloud (Azure).

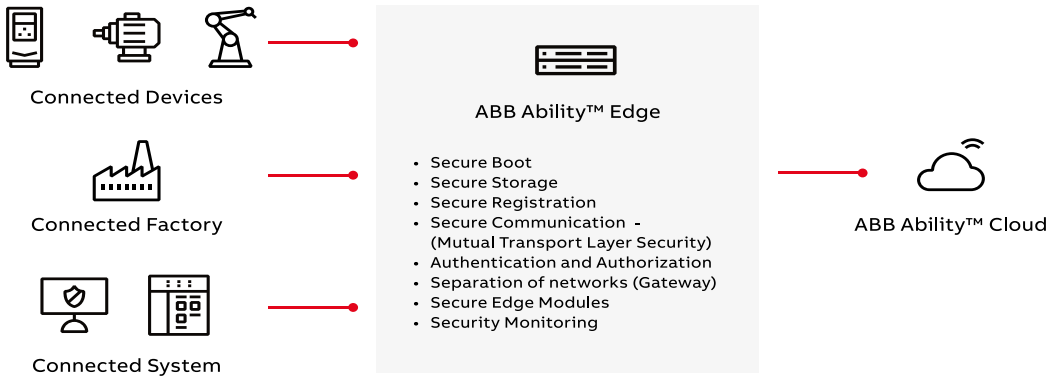

Figure 3: ABB's approach to cybersecurity

As a crucial element of cybersecurity, ABB understands that data ownership is a concern of many customers. So, the use of the customer's data is based on the following three core principles, as defined in ABB's Data Manifesto:

- Customer data remains theirs
- Customers know what happens with their data
- ABB will not disclose customer data without their consent.

NXP: Security solutions for IoT devices

NXP's comprehensive portfolio of processors, microcontrollers and signature software is built on a foundation of scalability, energy efficiency, security, machine learning and connectivity. The broad portfolio provides a foundation to achieve effective security levels at the edge, while facilitating their deployment in complex, multiparty IoT ecosystems. It is uniquely positioned to provide end-to-end security solutions, including discrete secure elements, integrated security on its processors and microcontrollers, and flexible security provisioning and cloud on-boarding services. With the breadth of solutions and wide customer base that spans multiple industries, NXP is highly focused on IoT security. Furthermore, products that are in the NXP EdgeLock™ Assurance program follow proven security-by-design processes and have undergone validation assessments to meet industry standards to ensure they meet a wide range of security challenges.

NXP and Microsoft have worked together to introduce a number of solutions built on NXP's portfolio of application processors, microcontrollers, and secure element devices that integrate with Microsoft Window 10 IoT Core, Azure RTOS and IoT services, with connectivity to Azure IoT Hub and IoT Central. The EdgeLock SE050 is a discrete secure element that can be attached to industrial devices to protect the credentials of the device. When used in combination with the EdgeLock 2GO service, it can simplify the provisioning of the device and automate the onboarding process to Microsoft Azure IoT Hub or IoT Central.

Keeping an edge device secure long after initial deployment is a challenge that requires nonstop trusted management services. NXP and Microsoft partnered to bring this capability to its customers with Microsoft Azure Sphere chip-to-cloud.

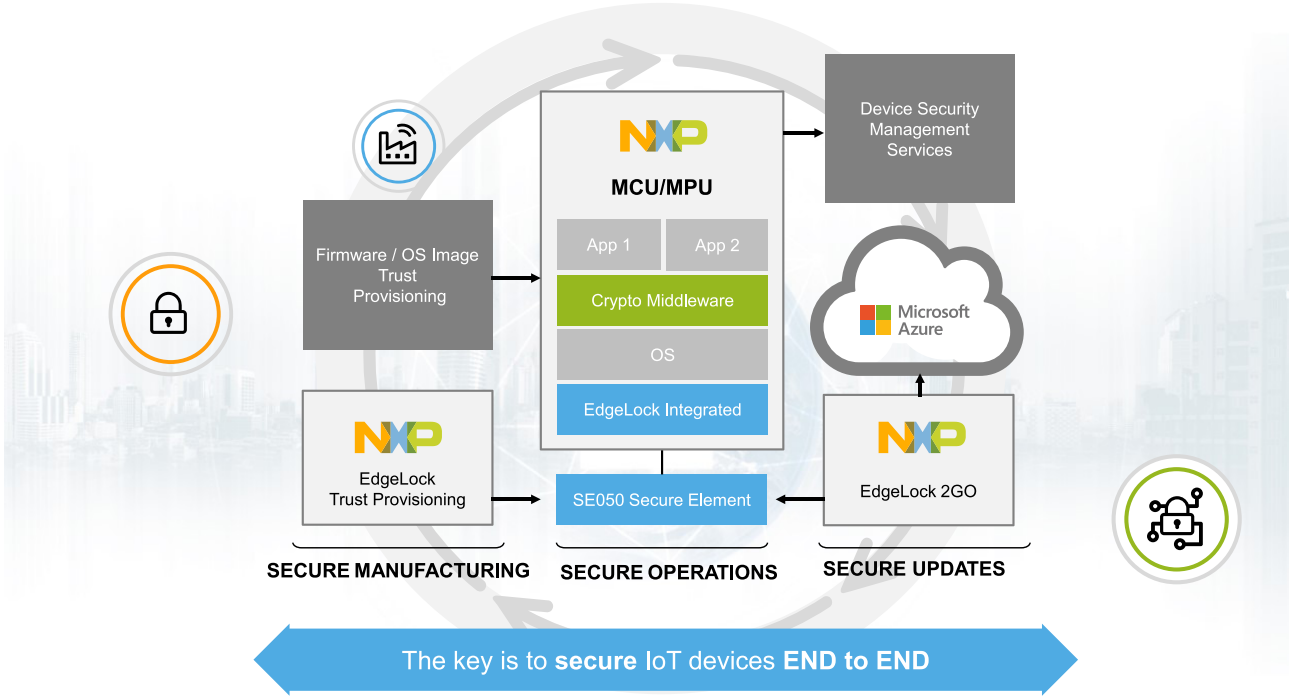

Figure 4: NXP: End-to-End security over IoT device lifecycle

Our continuous commitment to built-in security

Cybersecurity cannot be defined by products or technologies, and it is never complete. It is a total commitment to dynamic improvement across the IoT platform and multiple digital solutions, technologies, and products designed to anticipate threats and deliver the best available protection. Organizations must value cybersecurity proactively and continuously, rather than just in response to a breach or other event. And with global adoption of privacy measures driven by legislation and regulations, privacy must be a first-order consideration when designing the architecture of a solution; it cannot be treated as an afterthought.

Cybersecurity and privacy are built into solutions based on ABB, Microsoft, and NXP technologies from the earliest steps of their development. This approach makes security an inherent part of the solution at every level, from the device silicon to the edge to the cloud (see Figure 5).

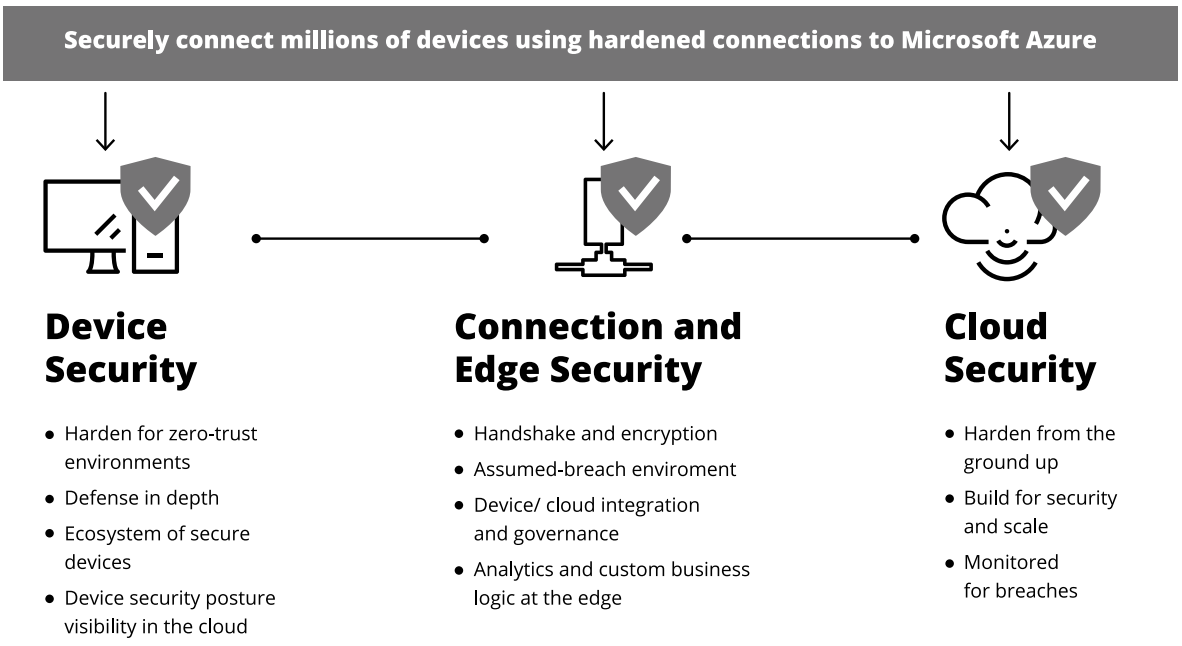

Figure 5: Security measures across the device-edge-cloud continuum

Security by design

Because reliability, availability, and safety are important to the products, services, and systems that ABB offers, cybersecurity is a core principle—indeed, it's endorsed by the company's executive board as part of ABB's license to operate. ABB provides secure, end-to-end digital solutions for all lifecycles through its ABB Ability™ offering which is based on the Microsoft Azure cloud computing service.

Similarly, at the earliest stage of silicon design during the manufacturing process, NXP injects credentials such as secure keys to build a root of trust. This ensures confidentiality and integrity of its firmware and assets throughout the value chain. The partnership between NXP and Microsoft allows solution providers to easily leverage products from NXP, as well as the associated provisioning and update services, to assemble and provision IoT devices securely and onboard them into the cloud in a trusted manner.

Our joint security approach

Security is the foundation for solutions developed by ABB, Microsoft, and NXP; it is woven deeply into the DNA of all three companies. This approach reinforces that security cannot be bolted onto an existing product but rather needs to be considered during the design and development, with security experts involved from the beginning and throughout its lifecycle.

ABB, Microsoft, and NXP each offer robust, wide-ranging security functionality to their customers. They securely store keys, manage device identities while respecting privacy settings, and enable confidential communication and provide a comprehensive, flexible range of encryption capabilities. All ABB Ability™ digital solutions adhere to ISO 27018, Platform "Industrie 4.0", and the Industrial Internet Consortium's standards, as well as the European Union's General Data Protection Regulation (GDPR) and California's Consumer Privacy Act. As ABB's cloud partner, Microsoft Azure also complies with the GDPR, as well as privacy regulations instituted by Japan, Argentina, and Canada.

To this end, in 2019, ABB and Microsoft were founders of the Operational Technology Cyber Security Alliance (OTCSA), an international consortium of OT operators and their vendor communities to "build and support an understanding of OT cybersecurity challenges and solutions from the board room to the factory floor." Areas of cybersecurity focus for the OTCSA include industrial control system equipment, software, and networks; IT equipment and networks used with OT systems; building management and control systems; medical equipment; and more.

Creating opportunities for tailored solutions

The prioritization of security by these three companies ensures that their solutions not only meet, but go beyond the unique security requirements while empowering customers to make informed decisions. With that comes an understanding that not every business will need protection at the same level. Depending on a business' needs and the level of risk it faces, this partnership allows for the application of expertise and appropriate technologies among the companies' scalable offerings to right-fit security solutions.

ABB, Microsoft, and NXP's solutions account for the customer's individual security requirements and offer tailored options with expertise and ingenuity in a unique 360-degree approach.

Our commitment to businesses

ABB, Microsoft, and NXP jointly promise to provide digital solutions that are enduring leaders in generating business insights with unsurpassed cybersecurity risk mitigation and privacy protection. The Azure ecosystem will remain in the forefront of empowering businesses through the IoT-based digital transformation of industries around the world.

Implications for decision-makers

Every organization has unique parameters for a given IoT implementation, tuning the balance between cost, complexity, performance, and protection. As a solution integrator, ABB has long experience assessing the needs of specific security implementations, sizing protection measures against requirements, and providing just the level of security needed, no more and no less. Not exclusively but in certain areas, ABB has been relying on NXP technology.

NXP's portfolio supports these solutions by providing security integrated at the right level, including hardware functionality, software enablement, and provisioning services. And the Microsoft Azure ecosystem is built to foster interoperations among solution elements from multiple providers, a co-development that's enabled by direct collaboration between Microsoft and ecosystem members, as well as through adherence to standards and best practices.

The powerful capabilities between the three companies and their shared commitment to securing the IoT—at scale for the businesses that use their technologies—help ensure that solutions are cost-effective while meeting requirements for data protection throughout a product's development and operation (see Figure 6). Further, it removes the risk for businesses introduced by developing their own technical architecture by offering ready-made, reliable, and customizable solutions reinforced by decades of expertise.

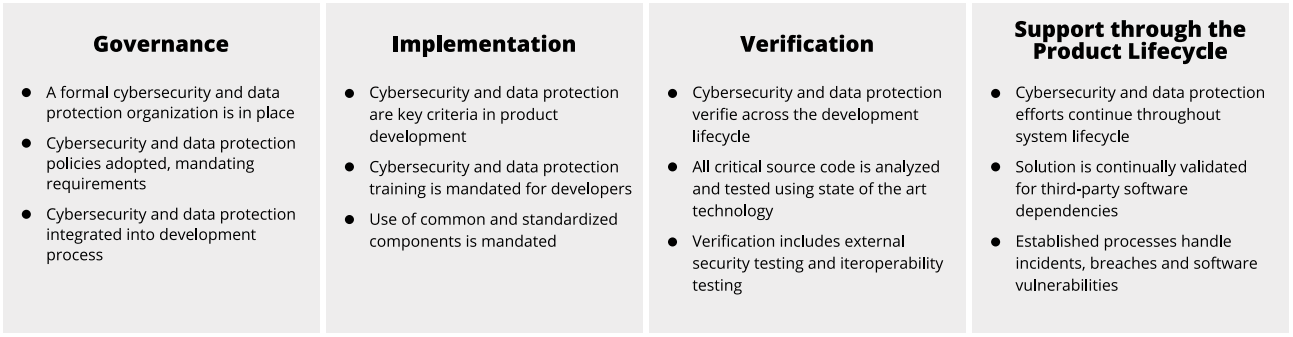

Figure 6: A security-first mindset enables IoT security solutions that span a product's entire lifecycle

What we offer customers

ABB, NXP, and Microsoft each provide a broad portfolio of scalable security solutions that offer a foundation to achieve the right security level at IoT end nodes and edge nodes, while facilitating their deployment in complex, multiparty IoT ecosystems. Each of these companies and their partners' solutions cover end to end security deployment, from manufacturing, to operations and over-the-air updates. At the manufacturing side, ABB, NXP and its partners allow IoT device manufacturers to establish trust of their devices, by injecting device identities via trusted processes and to create a root of trust. At the chip level, NXP offers multiple scalable security architectures, from discrete devices to integrated security on our chips. On the device update side, ABB, Microsoft, NXP and their partners offer cloud-based services for device zero-touch onboarding, to OS and firmware update and maintenance over time.

To make cybersecurity functions even easier to deploy, NXP and Microsoft are taking a step further, and investigating in a complete solution hardware, operating systems and cloud service, that addresses challenges of secure manufacturing, operations and device update.

ABB is using the Secure Boot features of the NXP i.MX6 CPU as the root of trust for ensuring that only trusted firmware is running on the device

Safe and secure charging is crucial to mass adoption of electric vehicles (EVs), from securing operation and managing access to protecting user data whether it's stored or shared with the cloud. ABB Electrification, as the market leader in DC EV fast-charging stations, uses in one of its solutions NXP's i.MX6 CPU as the root of trust for ensuring that only trusted firmware is running on the device. Besides NXP ABB is also relying on Microsoft technology. The configuration backend of the charging stations is running on Microsoft Azure.

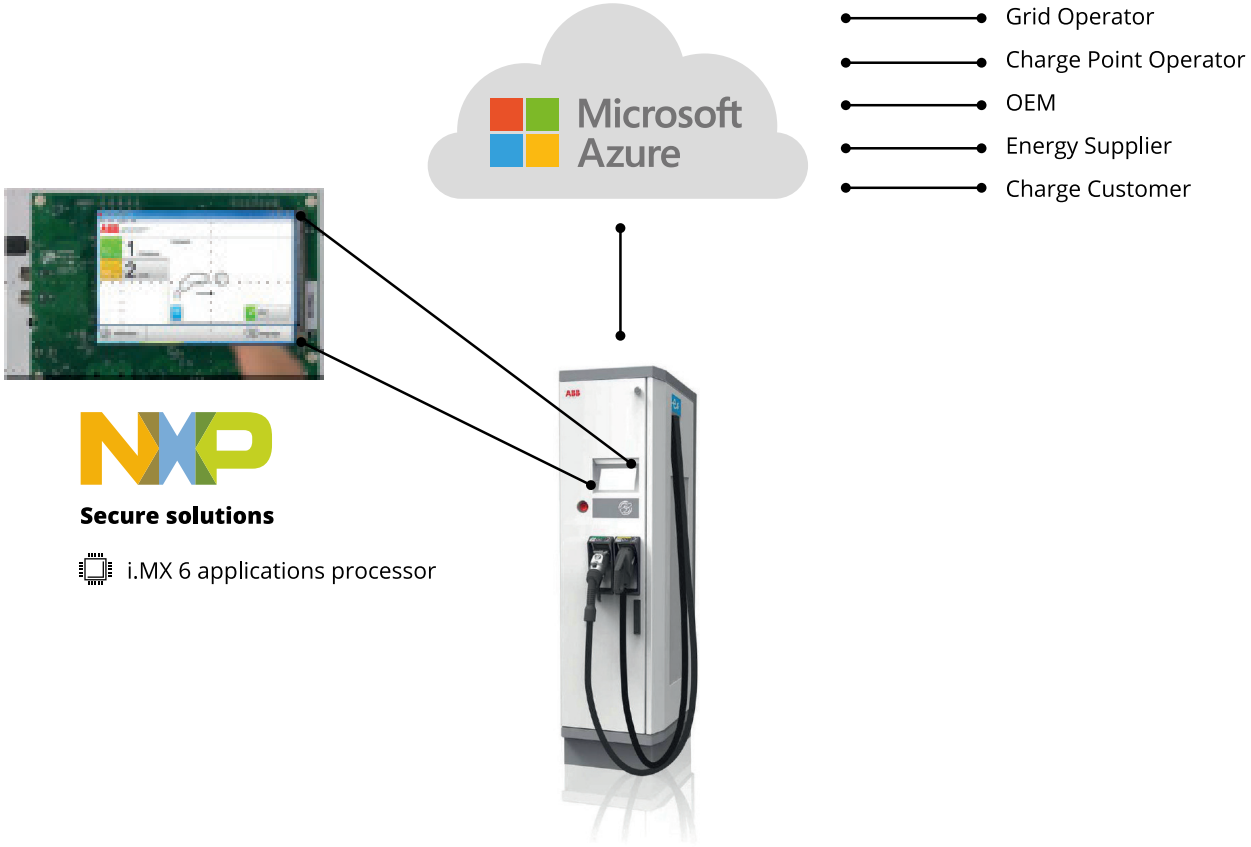

Figure 7: DC EV fast-charging stations - ABB Electrification relies on Microsoft and NXP technologies

Conclusion

The digital transformation of industries around the world requires data and system protection. Whether your IoT implementation is a monitoring system for offshore wind turbines, an agriculture drone to monitor plant health, or security surveillance system, business decision-makers can benefit tremendously from the secure solutions made possible by ABB, Microsoft, and NXP.

Cybersecurity is critical at all stages of the lifecycle of the IoT implementation. You must consider security during the conception phase, development, manufacturing processes, while in use and through the end of life.

ABB, Microsoft and NXP are leaders in creating and protecting technologies, products, and systems that span from the cloud to the edge. We strongly believe that working together to deliver a secure edge-to-cloud solution presents opportunities for you – our customers and partners – and can help you address your cybersecurity needs while pursuing your business opportunities.

Additional resources

See the following resources for more information on secure IoT offerings from ABB, Microsoft, and NXP:

- ABB IoT security
- Microsoft Azure IoT security
- NXP IoT Security

Next steps

Whether your organization designs its next generation IoT device, drives a digital transformation process, or creates a digital twin for a manufacturing plant, ABB, Microsoft and NXP are ready to engage with you and discuss your secure IoT ambitions and concerns. To find out more about how your business can gain from the diverse and comprehensive IoT security expertise of the three parties, get in contact with either of the three companies.