ACCELERATE CONNECTED DEVICE DESIGN WITHOUT SACRIFICING DEVICE SECURITY

Organizations are increasingly realizing the value of deploying Internet of Things (IoT) devices to support intelligent digital capabilities for industrial and commercial use cases. Wireless devices can give organizations access to new data-driven insights, but managing these distributed systems comes with its own security challenges.

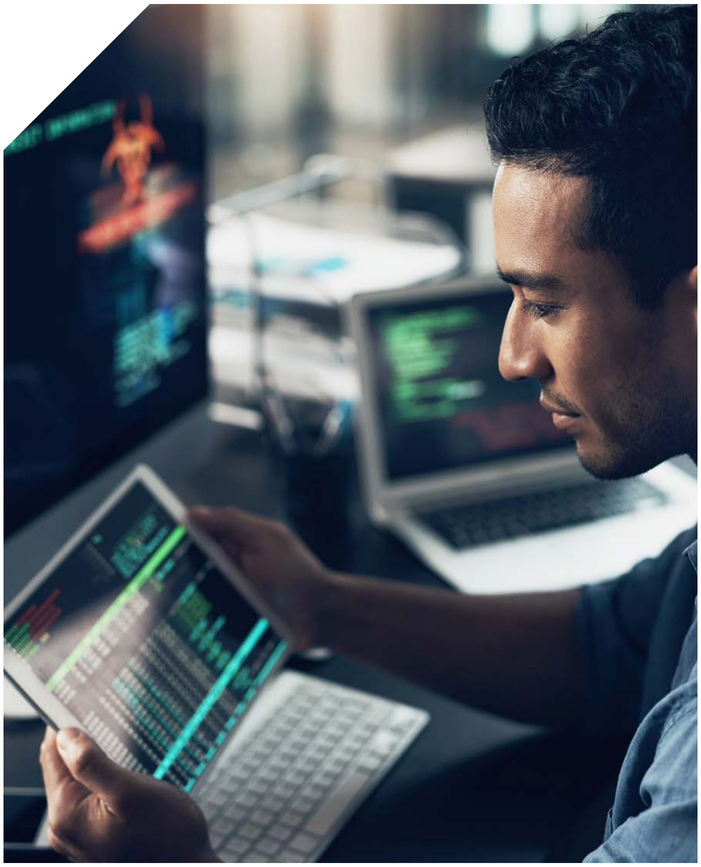
Today, IoT devices can be found everywhere — in hospitals, manufacturing plants, our homes, and our vehicles — which introduces new security risks. As a result, industrial IoT design requires product developers to adjust their design processes and priorities. In addition to product use cases and hardware-software trade-offs, designs must consider requirements from the start. Ensuring that security best practices are not only implemented during design but through the entire lifecycle of a product presents additional challenges.

In this white paper, we review how organizations can take advantage of system-on-module (SOM) solutions that provide building blocks for designing secure connected products. But first, we need to consider the unique security threats that affect IoT devices.

Challenges of Securing IoT Devices

Designing and managing connected devices at scale is challenging, and mistakes are costly. Product development teams must consider how hardware and software limitations, use case requirements, and device lifespan affect the risk profile of the product, all while staying within budget. According to a 2021 survey on IoT Security, 96% of IT decision makers "reported their organization's approach to IoT security requires an improvement." [1]

Often, industrial IoT devices have long product lifecycles, which provides cyberattackers with more time to research and learn the embedded systems' vulnerabilities before the devices reach their end of life. Additionally, these devices are commonly deployed in remote locations outside of traditional IT networks and security tools, and many systems are battery powered and not always connected. This makes IoT devices more difficult to monitor and update, and more vulnerable to unauthorized access and cyberattacks.



[1] Source: Palo Alto Networks, The Connected Enterprise: IoT Security Report 2021

Diverse Threats Affecting IoT Security

When it comes to IoT security, product designers must assume that every asset is exposed and that attacks can happen anywhere, at any time. Vulnerabilities can be introduced during the manufacturing, commissioning, operation or maintenance of products, as well as when applications are collecting, processing or transmitting data over the network.

The assets on these devices that require security can be highly diverse, making their security strategies a more complex challenge to solve. An organization operating IoT devices at distributed sites might need to secure anything from personally identifiable information (PII) to corporate data and infrastructure to intellectual property (IP).

When these assets are left unprotected, organizations risk significant financial losses and damage to their reputation. A single data breach or cyberattack through an IoT device or network can dramatically affect an organization's operations and impact other service providers. One global survey found that 80% of organizations experienced an IoT-focused cyberattack in a single year, averaging costs of more than $330,000 per incident.[2]

IoT-focused cyberattacks can occur in multiple ways, including attacks that prevent a system from booting, making critical services unavailable, or injecting malicious firmware onto embedded systems. And since these devices are often located outside the traditional data center, they are more vulnerable to physical attacks or unauthorized access to restricted resources, whether accidental or intentional. Since industrial IoT devices often have long lifecycles, their security needs to be designed with the complete lifespan in mind, including planning ways to securely purge data when decommissioning devices at the end of their lifespan.

Addressing Security Challenges in the Design Process

When implemented strategically, security should not be about doing everything you can for every product. Instead, your organization should determine what security is needed for each use case, based on the type of data involved, as well as how that data is processed, stored and transmitted.

During the design process for wireless industrial devices, product development teams must align their security strategies with the product's intended use case, environment, and functionality. Organizations should perform a risk evaluation that measures the financial impact of potential cyberattacks or breaches against the cost to protect against those risks.

When conducting a risk evaluation, product designers can use the elements of the CIA Triad[3] — confidentiality, integrity, and availability — as an established security framework to guide their design choices.

For example, a risk evaluation could involve asking questions like:

- **What is the risk that the device will be stolen?**
- **If that happens, what would the legal or financial impact be?**
- **What can be done to protect the system's data or IP against that risk?**
- **Would the cost of that protection be justified?**

This kind of evaluation allows product teams to assess the likelihood and significance of specific, relevant scenarios, determining which security features or capabilities best support business goals, product requirements and customer needs.

> "Since industrial IoT devices often have long lifecycles, their security needs to be designed with the complete lifespan in mind, including planning ways to securely purge data when decommissioning devices at the end of their lifespan."

[2] Source: Irdeto Global Connected Industries Cybersecurity Survey
[3] Source: Election Security Spotlight – CIA Triad

5 Best Practices for Designing Secure Wireless Products

From product development to deployment to management, design teams need to keep in mind how the findings of their initial risk evaluations affect every stage of the product lifecycle. Product teams must ensure that secrets provisioned in one stage are not made vulnerable when the product progresses to another stage or environment.

Threats affecting the IoT landscape are always evolving, and security strategies and capabilities must do so as well. Thoroughly understanding your product's use case requirements and the associated risks is critical for implementing the following five best practices for security throughout the product lifecycle:

- **Defense in depth**
- **Designing for the future**
- **Crypto-agility**
- **Security by default**
- **Continuous integration**

Defense in depth

Defense in depth is a security tactic that incorporates layered security measures, including physical, technical and administrative protections. Taking a defense-in-depth approach to IoT security means implementing multiple layers of security controls placed throughout the embedded system. This redundancy serves as a fail-safe — if one layer of security fails, the system remains protected.

Imagine that an IoT device in a hospital stores and processes sensitive data. That data can be protected using tamper detection controls that monitor for unauthorized physical access to the device. With a defense-in-depth approach — such as by adding data encryption as another layer of security — the data would remain secure even if the tamper detection fails and the data stores are accessed without authorization.

Designing for the future

It's not uncommon for IoT devices to remain in use for well over 10 or 15 years. In that time, security standards for firmware and other security controls can significantly change. The hardware in your product needs to be designed to support changing security requirements over time. Otherwise, your organization risks that it will either need to replace IoT devices well before their intended end-of-life or deal with data and network breaches due to the hardware's incompatibility with modern, more demanding security measures.

Ideally, a device's embedded system can scale in terms of compute performance and available memory to keep pace with changing industry standards. Designing a system that can achieve this is a challenging feat and since you cannot foresee what those future requirements will be, crypto-agility — which we discuss next — is also an important capability.

Crypto-agility

Designing embedded systems with crypto-agility means building in support for rapid adaptations of new cryptographic primitives and algorithms. Think about security algorithms and keys in use seven years ago — the same way you would not want to rely on those protections today, you will not want to rely on today's security capabilities seven years from now.

Crypto-agility acts as a safety measure or an incident response mechanism when an installed cryptographic primitive of a system is discovered to be vulnerable. Enabling crypto-agility for embedded systems of IoT devices means organizations can react to vulnerabilities or adapt to new security standards more easily. Instead of having to make significant changes to system infrastructure, the process to deploy updated cryptographic algorithms to devices should be simple and ideally partly automated.

Security by default

When shipped to the field, products should have the most secure configuration settings by default. But without preemptive planning and design consideration, this practice may not be sufficient. Often, the most secure configuration has poor usability, motivating users to disable those settings at their own risk. To overcome this challenge, product teams should conduct both risk analysis and usability testing during the design process.

Continuous Integration Throughout the Product Lifecycle

As previously discussed, the length of device lifespans poses a significant challenge for ensuring IoT security, which is why future-proofing and crypto-agility are such important practices to follow. An approach of continuous integration of security fixes during the lifetime of a product is essential to keep your product as secure as possible.

Your organization can use continuous integration to streamline and accelerate the patching and update process, simplifying the maintenance of your connected devices without compromising on security. There are specific methods recommended to use at the different stages of the development cycle:

Static Application Security Testing (SAST): With static analysis, you can assess your source code for memory leaks, unsafe operations, buffer overflows and other design conditions indicative of security vulnerabilities.

Software Composition Analysis (SCA): Once you have built your software, software composition analysis can be used to validate all the packages used in the build — the software bill of material — assessing them for known vulnerabilities.

Dynamic Analysis Security Testing (DAST): During product testing, your organization can automate dynamic analysis to conduct overall software security testing on operational devices.

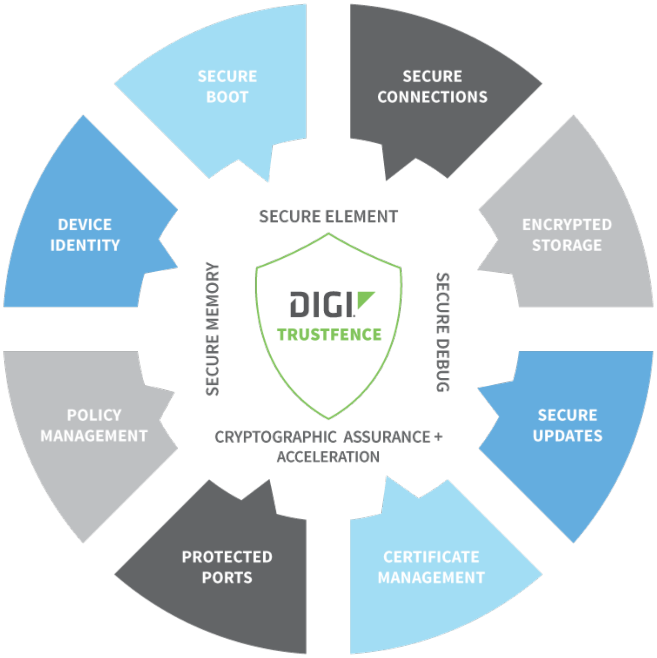
Interactive Application Security Testing (IAST): After a product release, using penetration testing and other interactive security testing can expose security holes and issues that need to be addressed in the next patch or update.

Security issues uncovered during any of these tests need to be patched in the source code and updated software needs to be deployed to the device. With each patch and update, the cycle should repeat, throughout the entire life cycle of the product.

Digi's Approach to Wireless Device Security

Designing secure connected devices requires a proactive approach. Due to the complexities involved and the unique skills required, many organizations lack the internal resources and expertise to implement all the best practices for scalable IoT security. However, with trusted system-on-module (SOM) solutions, organizations can have all the building blocks they need to design highly secure embedded systems for their wireless products.

Digi offers SOM solutions that help organizations secure their connected products faster and more cost-effectively. Rather than investing significant resources in building embedded systems and security features from scratch, our customers can focus on their core competencies and differentiators while designing connected devices with our trusted SOM solutions.



Digi ConnectCore for a Complete SOM Development Platform

The Digi ConnectCore® portfolio delivers more than hardware to use for your IoT device design. This complete SOM development platform includes a broad suite of capabilities that reduce time-to-market and offer remote management capabilities to monitor and maintain devices in the field. Digi ConnectCore scales with new product and security requirements and it includes a free-of-charge security stack — Digi TrustFence®, providing essential security features. A fully validated BSP, Linux and Android operating system software, development tools, wireless connectivity options, and integration with cloud services are part of the solution. In combination with Digi ConnectCore, your organization can also use Digi XBee® to extend the secure wireless communication capabilities in your products.

With Digi TrustFence, your organization can implement proactive, built-in security that simplifies your product design process. Digi TrustFence is a security framework that guides you through implementing features like secure boot, secure firmware updates, encrypted file system and certificate management. This framework is scalable and upgradable, supporting long lifecycles and addressing common security implementation challenges.

Digi XBee provides simple, flexible wireless connectivity options for your IoT devices. Digi XBee modules can be used without any additional microcontroller or host processor, or they can be connected to a Digi ConnectCore SOM, delivering additional wireless connectivity options for your products. Digi XBee is easy to use and pin-compatible, simplifying the update process and making your products future-ready.

By leveraging our common platforms and software environment, you can quickly integrate our SOM solutions into your full range of embedded system products, all in line with your needs and budget.

Hardware-enabled, Software-defined

Digi takes a systems approach to integration, a strategy we call hardware-enabled, software-defined. We provide customers with a suite of product design and development tools that accelerate and simplify product development and design. And we partner with industry leaders to bring complete solutions to market. Digi ConnectCore, our industry-leading SOM solution, provides all the building blocks your organization needs to design a highly secure wireless product for industrial and medical use cases and maintain these in the field throughout their entire lifecycle.

Digi ConnectCore Security Services

For OEMs seeking assistance with the security of their designs and proactive, ongoing security management, Digi offers **Digi ConnectCore® Security Services**. These are services and tools that enable OEMs to keep products secure after deployment, and throughout the entire lifecycle.

These services enable the monitoring and analysis of security risks and vulnerabilities for a custom software bill of material (SBOM) and binary image running on Digi ConnectCore system-on-modules (SOMs).

To help remediate identified issues, the services include a curated vulnerability report highlighting critical issues, a security software layer including patches for common vulnerabilities and consulting services.

Digi ConnectCore Security Services provide an additional meta-security software layer for Digi Embedded Yocto (DEY) with added protection and support.

Digi Meta-Security-Fixes Layer

- A collection of pre-integrated security patches for Digi Embedded Yocto
- A collection of pre-integrated security patches for the board support package (BSP), Linux kernel and bootloader

Digi Meta-Security-Tools Layer

- Includes tools and documentation to diagnose systems
- Additional diagnostics capabilities to analyze system security

CVE Monitoring and Analysis

Ongoing monitoring and analysis for common vulnerabilities and exposures (CVEs) are best practices for developers of connected products, in order to manage new and evolving threats. Digi ConnectCore Security Services provide these reports to enable OEMs to proactively manage potential cyberthreats and risks.

- Optimized for embedded systems with native Yocto integration
- Vulnerability database with intelligence for improved accuracy, security rating and remediation information
- More actionable information for developers compared to National Vulnerability Database (NVD)
- Transparency — readable reports that can be shared
- Additional security insights through binary image scans

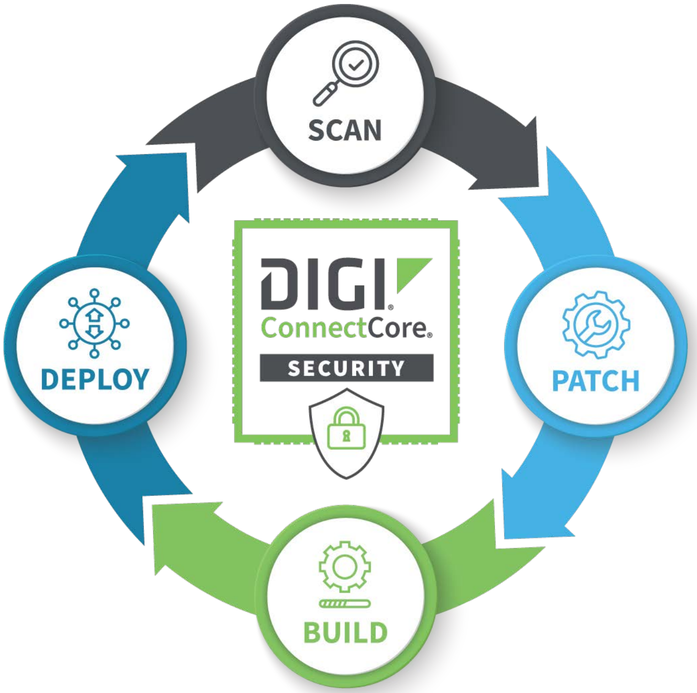
The Lifecyle Security Management Paradigm

Today OEMs are seeking ways to improve customer service and ensure their products can be updated with the latest security updates. Digi ConnectCore Security Services support complete security lifecycle management. The main benefits of these services are:

- Make security easier and more accessible by providing a curated security analysis
- Provide visibility on the security status of Digi Embedded Yocto, making vulnerability reports available
- Identify security issues in Digi ConnectCore DEY-based customer products
- Monitor and maintain security in devices throughout the entire product lifecycle
- Utilize Digi engineering and consulting services to help resolve security issues
- Take advantage of SBOM analysis and CVE monitoring
- Review binary image scans for additional vulnerability insights

Learn more. **Download the Digi ConnectCore Security Services Datasheet**

Digi ConnectCore Security Services Lifecycle



Why Digi?

Digi is a complete IoT solutions provider, supporting every aspect of your project, from mission-critical communications equipment to design and deployment services to get your application designed, installed, tested, and functioning securely, reliably and at peak performance.

Digi builds its products for high reliability, high performance, security, scalability, and versatility so customers can expect extended service life, quickly adapt to evolving system requirements, and adopt future technologies as they emerge. Digi embedded modules, routers, gateways, and infrastructure management solutions support the latest connected applications across verticals, from the enterprise to transportation, energy, industrial and smart cities use cases.

Our solutions enable connectivity to standards-based and proprietary equipment, devices, and sensors, and ensure reliable communications over virtually every form of wireless or wired systems. Our integrated remote management platform helps accelerate deployment and provide optimal security using highly efficient network operations for mission-critical functions such as mass configuration and firmware updates, as well as system-wide monitoring with dashboards, alarms, and performance metrics.

Company Background

- Digi has been connecting the "Internet of Things" — devices, vehicles, equipment and assets – since 1985
- Digi is publicly traded on the NASDAQ stock exchange: DGII
- Headquartered in the Twin Cities of Minnesota, Digi employs over 800 people globally, and has connected over 100 million devices worldwide

As an IoT solutions provider, Digi puts proven technology to work for our customers so they can light up networks and launch new products. Machine connectivity that's relentlessly reliable, secure, scalable and managed — and always comes through when you need it most. That's Digi.

Learn more on our About Digi page.

Contact a Digi expert and get started today

PH: 877-912-3444
www.digi.com

Digi International Worldwide Headquarters
9350 Excelsior Blvd. Suite 700
Hopkins, MN 55343

/digi.international @DigiDotCom /digi-international

While every reasonable effort has been made to ensure that this information is accurate, complete, and up-to-date, all information is provided "AS IS" without warranty of any kind. We disclaim liability for any reliance on this information. All registered trademarks or trademarks are property of their respective owners.