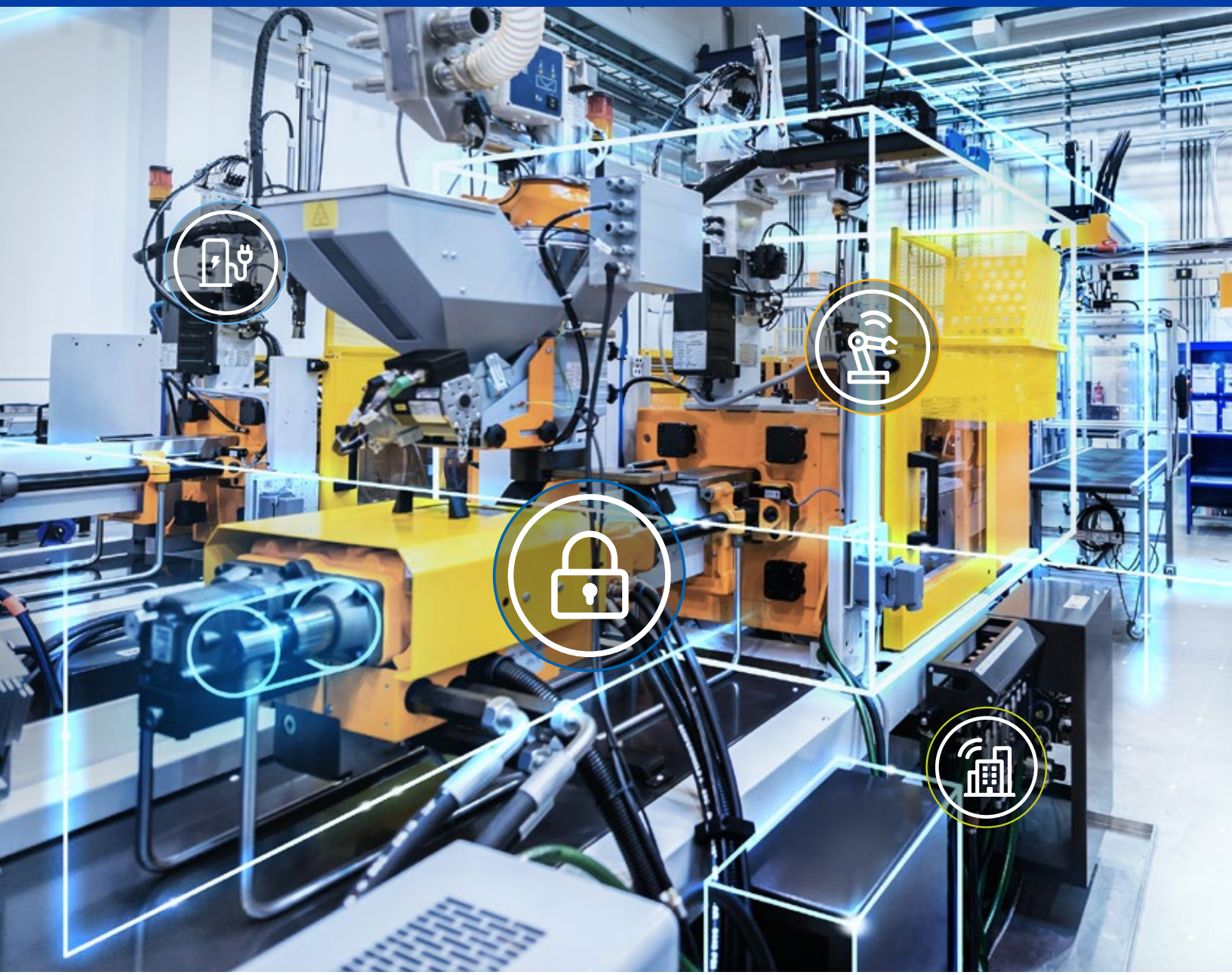
SECURING THE INDUSTRIAL IOT

Trusted Solutions for Embedded Systems



Industrial IoT (IIoT) is transforming the way industries operate. At its core, data is acquired, analyzed and turned into actionable insights to solve problems for faster decisions. But IIoT devices and infrastructure can become high-value cyber targets — a compromise could lead to financial, safety and even environmental threats. At NXP, we believe that security must be considered from the start of a design to achieve optimal protection. That's why we are relentlessly focused on our security engineering expertise, proven processes and understanding of emerging trends to deliver trusted solutions that meet your security needs.

THE IIOT: DRIVING FORCE FOR TRANSFORMATION

The shift to digitization across industries is spurring new applications, from driverless transport and smart handling systems to autonomous robots that operate without human intervention. IIoT technologies are being deployed across power and energy, factories, buildings and healthcare industries. These interconnected devices — the industrial "Things" — include actuators, sensor nodes, servo drives, vision systems and programmable logic controllers. Together, they form industrial communication networks that enable devices to share vast amounts of data.

> IIoT systems generate, process and collect large amounts of sensitive data that must be protected and handled securely.

Some devices sense, analyze, acquire and communicate with automation control systems in real-time, such as edge devices with on-chip computational and machine learning capabilities that enable them to make immediate decisions. Some actuators directly influence the industrial process by operating a switch or a valve and gathering its data. These edge devices have computational capabilities that can directly impact a process without the need for data to propagate through the entire system.

Other edge devices gather and pass data to a centralized hub that processes and consolidates this data and sends the information to the cloud. This information can then be analyzed and processed by cloud-based applications and fed back to enhance production.

Greater energy efficiency, reduced costs, better quality products, improved decision-making and less equipment downtime are some of the advantages of an effective IIoT system. It's no surprise that digitalization is expanding in all sectors, with the potential for interconnection between multiple organizations in a supply chain.

Architecting for IIoT

While IIoT systems vary widely, they have similar architectural features. The data gathered by IoT devices in the manufacturing and logistics areas flow through gateways to the Operations Management area, Supervisory Control and Data Acquisition systems (SCADA) and Manufacturing Execution Systems (MES). These consolidate and convert the raw data into information for analysis by applications locally at the edge, are sent to cloud-based data centers or a combination of both.

Traditional operational technology (OT) systems that managed and controlled operations were "air-gapped" environments, meaning that they were not connected to external networks. However, across industries today, the lines have blurred between information technology (IT) and OT, bringing connected IT systems that handle email and data processing together with self-contained OT systems. There are many benefits of this convergence, from lowering operating costs by giving manufacturers greater transparency into performance and helping energy utility providers offer consumer engagement systems based on real-time usage and rates.

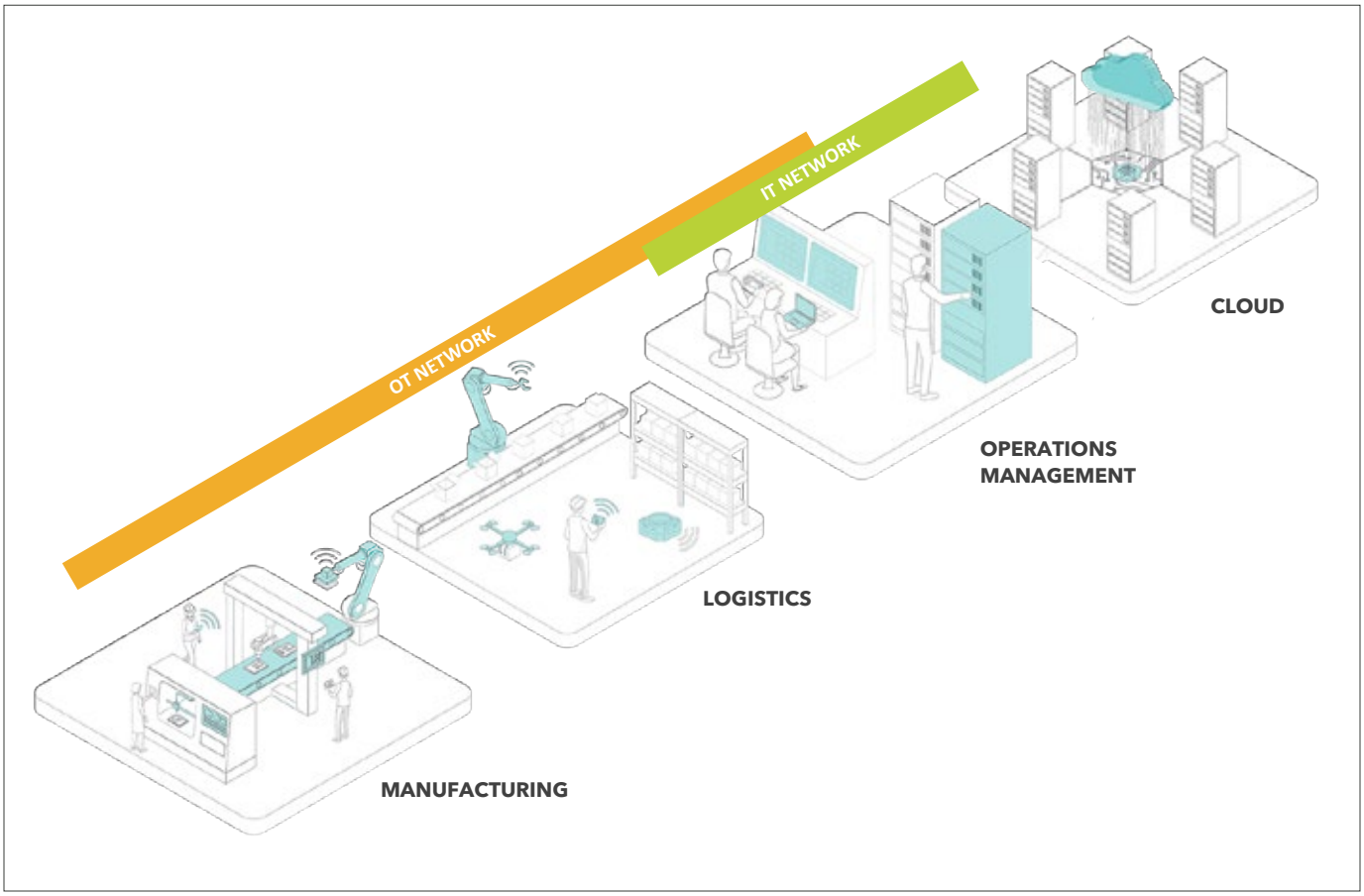


Figure 1. The convergence of IT and OT has significant benefits but increases the potential of scalable attacks that could impact across the entire supply chain.

Attack Surfaces Pose Risky Business

The convergence of IT and OT can also increase the potential attack surface of nearly every level within the infrastructure, from enterprise resource planning (ERP) to the factory shop floor.

For example, an organization could have access to a supplier's computer system for visibility into logistics and supply. Because a significant number of interconnected devices and systems are involved, the attack surface grows and can even serve as an entry point into financial and process management systems, and even cloud-based systems. Criminal actors are increasingly resourceful in determining the weakest link in a system and using it to bootstrap an attack on the entire network of interconnected devices.

Industry 4.0 includes IIoT devices that can communicate with each another and the outside world. If left unsecured, these devices represent a large attack surface for remote attacks. A malicious attack of a single device has the potential to reach any of the connected devices.

Many seemingly innocuous connected devices have had vulnerabilities exploited by cybercriminals. For example, vulnerabilities in a commercial access control system led to hackers gaining access to user credentials, controlling doors and launching denial of service (DoS) attacks. Programmable Logic Controllers (PLCs) with weak security on the factory floor have been harnessed by criminals to bring the production line to a standstill by sending erroneous data to the machines they control.

Malicious actors have used vulnerabilities to move up the production system chain by exploiting the device path of the target that provides interconnectivity between PLCs and ultimately IT networks. In some cases, safety can be a concern, such as an attack within a nuclear power station.

> Security goals for industrial environments are, first and foremost, designed to protect worker safety and system availability.

Many modern cyberattacks are "socially engineered" as a result of phishing emails. Converging IT and OT systems can provide a conduit for transferring malware from IT to OT.

Varying Life Cycles and Legacy Devices

Industrial facilities that were established before malicious attacks became as prevalent as they are today may feature an industrial IoT system that has evolved with devices varying in age and security levels coexisting within the same network. In some cases, the manufacturer may have closed, leaving a void in support before the product reaches the end of its lifecycle.

Additionally, a legacy product may not have the processing power or sufficient memory to handle over-the-air or technician-implemented updates, yet the systems they control may be too costly or disruptive to replace. A personal computer or an IoT platform within an OT system may be running a legacy operating system, making effective malware eradication more complex, particularly when securing such a system from evolving threats. Production line downtime costs are an additional consideration and can account for a reluctance to carry out such upgrades.

While not common in modern devices today, vulnerabilities in specific legacy embedded devices generated their initial sequence numbers (ISNs), a fundamental feature of transfer control protocol (TCP) between computers or internet-connected devices, have left millions of IoT devices vulnerable to attacks. The generation of ISNs should be random, preventing third parties from intruding on communications. However, certain legacy devices have shown a predictable pattern in generating these numbers, allowing hackers to anticipate them and launch a DoS attack. Alternatively, an intruder could access the communication and inject malicious code.

The Target for Ransomware

Cybercriminals consider "Industry" an attractive target for ransomware. The downtime of a halted production line can run into many thousands of dollars per minute. Evidence shows that more than half of ransoms are paid in the event of a successful ransomware cyberattack. In an independent survey of 1,100 IT and OT security professionals in critical infrastructure sectors, such as transportation, energy, chemical, smart buildings and smart cities, more than 60% paid the ransom. And more than half of those paid at least $500,000. A cyber-terror attack on these same sectors could result in catastrophic environmental impact or even loss of life. It is clear that the sphere of industrial cybersecurity is one of great importance as the digitalization of our world continues to accelerate.

> While no industry is safe from ransomware attacks, the manufacturing sector has been hit especially hard. In 2020, attacks on the industry had increased by 300% compared to the previous year.
>
> [Source NTT 2021 Global Threat Intelligence Report]

INDUSTRY FIGHTS BACK

Governments Establishing New Initiatives

The EU Cybersecurity Act, which came into force in June 2019, aims to establish a European Cybersecurity Certification framework for all OT products and services. Its scope includes EU cyber deterrence, law enhancements, identification of perpetrators, international cooperation and a diplomatic, political response. The European Agency for Cybersecurity, ENISA, participates in this new framework, establishing the link between standardization and certification.

In the United States, similar initiatives are in place with the National Industrial Security Program (NISP). Additionally, the Strengthening American Cybersecurity Act of 2022 (SACA) was signed into law in March 2022. It requires critical infrastructure operators to report "substantial cyber incidents" to the Cybersecurity and Infrastructure Security Agency (CISA) within 72 hours and report ransomware payments within 24 hours.

IEC 62243: A Path to Compliance

IEC 62443 is a series of international standards that address cybersecurity for operational technology in Industrial Automation and Control Systems (IACS). An industrial expert panel, including NXP security experts, worked to develop the series, which is divided into sections to encompass both procedural and technical requirements from the device level to the IACS level.

The IEC approved the 62443 series as horizontal standards, meaning they are used as a foundation when subject matter experts are developing sector-specific OT standards for cybersecurity. The standards provide a framework for all aspects of security as early as possible. This prevents confusion arising from the use of a myriad of sector-specific standards and creates a unified, interoperable approach to security — for example, standards relating to elevator cybersecurity built on IEC 62443. In addition to the technology that a control system may feature, the IEC 62443 series encompasses procedural "Best Practice" guidance, risk assessment and threat countermeasures and a benchmark for an organization creating their Cybersecurity Management System (CSMS).

The standards are organized into four parts:

- **Part 1** pertains to the terminology and methodology used.
- **Part 2** looks at the methods and security processes for different roles such as industrial facilities.
- **Part 3** discusses cybersecurity technical requirements for systems. The target audience is system integrators.
- **Part 4** is about the integration of cybersecurity in all the phases of a product life cycle and specifies the technical requirements for components themselves, such as embedded devices.

NXP'S SECURITY-BY-DESIGN APPROACH TO EASE 62443 COMPLIANCE

At its core, NXP has extensive security expertise and addresses the security demands of its products by leveraging its heritage in highly advanced secure elements for smartcards, government e-passports and automotive applications. The company rigorously tests its sites, systems and processes. In addition to ensuring the integrity of its secure components, NXP has a security-conscious culture within its organization, making security part of its DNA.

NXP not only has security procedures documented but also put them into practice — and has achieved Maturity Level 3 (ML3) of IEC 62443-4-1. The certificate's scope includes NXP's Business Creation and Management (BCaM) product development process and the Product Security Incident Response Process (PSIRP). The NXP-wide BCaM framework is a product development process framework that covers all harmonized processes to successfully launch new products, including new technologies and software. The BCaM framework includes a security module with the Security Maturity Process (SMP) at its center; ensuring security standard compliance, including IEC 62443, can be achieved. With such a modular process structure, NXP is capable of introducing new products that target IEC 62443 compliance.

SECURITY EVALUATION STANDARD FOR IOT PLATFORMS (SESIP)

Orthogonal to the security standards like IEC 62443, NXP believes a certification standard designed to meet the broad and complex challenges of Industrial IoT security strengthens overall security.

GlobalPlatform announced a new certification standard called the Security Evaluation Standard for IoT Platforms (SESIP) in 2020. This allows for third party security certifications, which means that device manufacturers can demonstrate the claimed device security. This makes it much easier for our customers to know which devices they can trust.

SESIP is known for being practical, easy to use, and easy to reuse, and is backed by the strength of a recognized industry organization that operates on an international scale. By using a common-sense approach, mapping to major standards, and including a library of levels and security profiles, SESIP makes it easier for device manufacturers to verify the security of their offerings.

Platform definition

SESIP brings together common security requirements that a secure system should implement. This allows a component's certification to be re-used if it is integrated into other devices, such as secure microprocessors, connectivity libraries, and operating systems that provide the foundation for running connected applications.

SESIP scope

The SESIP threat model aims to protect personal data on the device, such as authentication credentials. It also protects data in transit, software code, as part of an application or platform, and data relating to product identity, configuration, system operation, and device life cycle.

Threats addressed

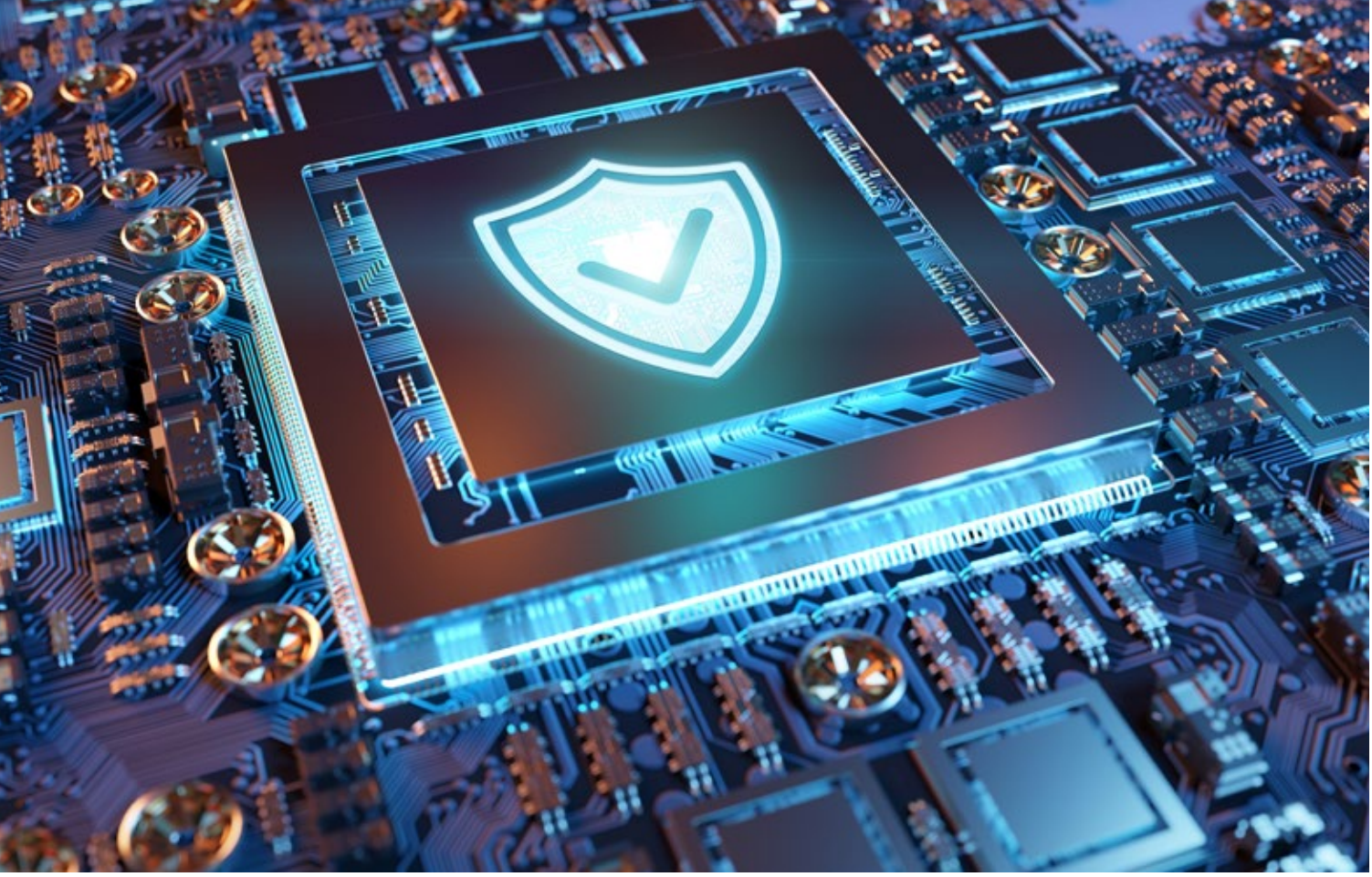
The ability to prevent, recover, and learn from attacks are part of the robustness assessment. Assessment covers baseline threat scenarios and may cover extended threat scenarios.

SECURITY PRIMITIVES

Determining the necessary product security features in a specific use case can be challenging, given the complexity of cybersecurity for modern IIoT systems. To aid with the process of establishing the necessary level of security, NXP has defined a comprehensive set of security definitions that helps approach security in a structured way. These definitions, also called "Security Primitives," describe security features that are split into different categories. to aid in the selection of suitable products or related security standards based on a given use case or a high-level idea of security requirements.

https://www.nxp.com/securityprimitives

NXP's security primitives offer a starting point to help you map your security requirements to products in a structured way. Find out more at **nxp.com/securityprimitives**.



NXP PRODUCTS

Because every use case is different, the security should be as well. That's why at NXP, we offer a broad EdgeVerse™ product portfolio for a wide range of use cases and protection. Depending on your application, you can choose from SoCs with integrated security capabilities, ready-to-use secure elements or a combination of both. Trust provisioning and cloud onboarding services complement our solutions. Our portfolio is designed to protect against basic software threats all the way up to sophisticated hardware attacks on the most critical and high-value systems.

MCUs and Processors with Integrated Security

NXP addresses secure IIoT requirements with its EdgeVerse™ processing platform, a range of microcontrollers and processors that deliver power and performance scalability, rich mixed-signal and security integration, as well as system-level solutions and software enablement to ease embedded development.

In recent years, hardware based security in a microcontroller has become a principal design criteria for embedded system development, whether the MCU acts as a host controller in a connected end point, or a companion device in an IIoT gateway or networking solution. Security is at the forefront when developing our latest Arm® Cortex®-M based microcontrollers, such as the recently launched LPC5500 MCU series, which integrates a range of benchmark security features, from secure boot with immutable hardware root-of-trust, SRAM PUF-based unique key storage, certificate-based secure debug authentication. Cryptography acceleration is further enhanced within LPC5500 for faster key exchange with dedicated accelerators for AES-256 and SHA2-256, as well as asymmetric algorithms, such as ECC and RSA for public key infrastructure.

Offering protection and isolation, NXP has integrated an EdgeLock® secure enclave into some of NXP's latest i.MX applications processors and i.MX RT crossover MCUs. This preconfigured, self-managed and autonomous on-die security system provides a rich set of security services and platform security functions which it manages independently without impacting the function of the processor or controller.

NXP's i.MX RT1180, a purpose-built crossover MCU for industrial edge applications, is the first from NXP to include a secure enclave, as well as a 5 Gbps cut-through ethernet switch with multi-protocol support for both time-sensitive networking and real-time industrial ethernet. Additionally, by mapping system-level industrial security requirements into NXP's target SESIP component certification, i.MX RT1180 will ease the effort required by OEMs to comply with IEC 62443 standards.

Whether it's dedicated accelerators for machine learning, graphics and vision, or an integrated EdgeLock® secure enclave, our i.MX applications processor families, including our i.MX 8ULP that targets a variety of low-power use cases and the mainstream i.MX 9 series, are designed to meet the increasing security requirements of IIoT applications.

Secure Elements

The EdgeLock SE05x product family is a group of ready-to-use plug and trust secure element devices that are Common Criteria (CC) EAL 6+ certified and offer root of trust at the IC level, providing strong end-to-end security for IIoT devices. Delivered as a ready-to-use solution, the EdgeLock SE05x family offers a complete product support package that provides integration with major operating systems such as Linux, Windows, RTOS and Android. An extension to a variety of MPUs and MCUs, they streamline design-in and reducing time to market. Design tools such as use case sample code and compatible development kits for our microcontrollers facilitate rapid integration.

Using the EdgeLock SE05x secure element with its pre-integrated security features eases compliance with IEC 62443 component requirements while eliminating much of the complexity of the security implementation. In particular, the EdgeLock SE05x provides the IIoT device with a secure identity that is then used with mutual authentication, sensor authentication, cloud onboarding and other IIoT tasks. This allows the OEM to further strengthen the IIoT device against logical and physical attacks, helping future-proof devices.

EdgeLock Assurance

Security is at the core of NXP components and solutions. When you see the EdgeLock Assurance trustmark, you'll know the product is designed with industry standards in mind. Proven processes and validation assessments help ensure you receive trusted solutions for your security challenges. Find out more at **www.nxp.com/edgelockassurance**

SECURE, FLEXIBLE IOT SERVICE PLATFORM

EdgeLock 2GO

EdgeLock 2GO security service platform is designed for easy, secure deployment and management of IoT devices embedding NXP EdgeLock SE05x secure element or EdgeLock A5000 secure authenticator. This turnkey solution provides secure device credential management in manufacturing or in the field, over-the-air and throughout the complete device lifecycle. EdgeLock 2GO services are based on secure hardware protecting the credentials and sets up secure end-to-end connection with this secure hardware. This combination of security hardware and services can significantly reduce development time and cost of ownership for industrial devices. With EdgeLock 2GO, device manufacturers don't have to invest in new manufacturing equipment to support device security management, including device onboarding and lifecycle management.

Transforming Beyond Industry 4.0: i.MX RT Industrial Drive Development Platform

The i.MX RT industrial drive platform provides the development starting point to take advantage of NXP's strong security offering in hardware and software for next-generation secure and cyber-resilient industrial drives. It features advanced motor control algorithms for multi-axis control and ample bandwidth to support Human-Machine Interfaces (HMIs), deterministic Ethernet Time-Sensitive Networking (TSN) communication, data logging and fault detection. It is intended to be certified for IEC 62443-4-1, 4-2 SL3. The i.MX RT1170 MCU and the onboard NXP EdgeLock SE05x secure element provide a ready-to-go multi-board development platform for evaluating and validating various industrial applications.

THE FUTURE OF INDUSTRIAL CYBERSECURITY

Cyber threats continue to evolve in sophisticated and surprising ways, and the risk levels that legacy devices pose can increase over time. That's why NXP is preparing by advancing innovations to counter these new cyber threats.

Post-Quantum Cryptography

Bit by qubit, there has been slow yet steady progress in the development of quantum computers. A general-purpose quantum computer can perform certain complex calculations that are intractable to the strongest supercomputers we can build. These calculations can solve optimization problems with potential breakthrough applications in areas such as GPS, metrology, pharmaceutical research and machine learning. However, one cannot overestimate the threat potential of quantum computing to society at large to internet security, IoT devices and legal infrastructure based on the currently used cryptographic systems.

Systems and solutions that could reasonably be regarded as secure today may be weakened or fully broken in such a quantum future. The data (including code) contained in such systems may suddenly be compromised. NXP's security engineers and cryptographers are leading this PQC transition by contributing to frontrunners in the NIST PQC standardization effort and ensuring that any upcoming PQC standard takes core requirements of embedded security, such as physical secure implementations and resource limitations into account.

IP Protection

Intellectual property (IP) traditionally involved patenting an idea to register and protect the considerable research and development time that went into it from plagiarism. In a software scenario, this protection is more complicated and might involve digital watermarking. This is a process whereby a digital file contains information pertaining to it that is covertly stored within it. Within the sphere of industrial electronics, specifically machine learning, copyright information could relate to intellectual property.

For example, a preventive maintenance application based on a machine learning model could be used. This machine learning model contains IP and could be copied to avoid the cost of the maintenance contract. Digital watermarking is a promising direction to prevent IP theft by protecting your machine learning models.

Cyber-Resilience for Industrial IoT Devices

Cybersecurity is never static; in fact, it is a healthy attitude to assume that even the most secure devices will get hacked at some point in the future. In order to achieve security even in this challenging scenario, it is of utmost importance to have a multilayered defense strategy combining protection with detection and recovery mechanisms. The resulting cyber-resilient devices are always able to swiftly recover even from currently unknown remote cyberattacks back to a trusted state. In the best case, this happens automatically if the device detects the compromise — but even if not, an administrator will always be able to recover the devices remotely as a last resort. NXP's strategies for comprehensive cyber-resilience and recovery are outlined online **nxp.com/cyres**

Blockchain

Blockchain technology is increasingly used in industry as a way to keep track of logs and transactions produced by connected industrial IoT devices. These devices may belong to internal and external entities and organizations that do not necessarily share a trust relationship (e.g., in a supply chain). Blockchains use cryptographic mechanisms to ensure the integrity and immutability of the chain of transactions at any time so that each party can trust the information that is published.

To ensure only authorized devices are publishing transactions in the blockchain, transactions can be signed by IoT devices and verified by the blockchain upon reception. Securely storing the private keys that are used to sign transaction requests in a Secure Element (SE) is, therefore, of utmost importance to guarantee the authenticity of transactions. NXP has been developing solutions that can leverage our microcontrollers' high-security features to support the authentication of blockchain transactions.

Private Networks

Security solutions relating to communication are increasingly important as the number of interconnected devices within Industrial IoT systems increases. A growing number of Industrial enterprises use in-house private networks where the data never enters the public domain and are, therefore, better protected from malicious actors. Private networks also guarantee consistent, reliable coverage. The wireless technology utilized can be traditional 802.11 Wi-Fi or cellular protocols.

Wi-Fi 6 and 5G will likely feature in many future industrial IoT systems. Wi-Fi 6 offers reduced power consumption and considerable performance improvements over previous Wi-Fi standards. 5G boasts Ultra-Reliable Low-Latency Communications (URLLC) fast enough to allow a smart factory featuring augmented reality, artificial intelligence and advanced robotics to use it. These technologies herald an exciting future for Industry 4.0. NXP is central to developing and implementing these technologies. One example is the Layerscape® family of processors, which enable software-defined radio setups to transmit Open Platform Communications Unified Architecture (OPC UA) data over a private 5G network.

Conclusion

The IIoT offers enormous efficiency and cost benefits for all Industrial sectors, whether in power generation, transportation or smart city infrastructure. To this end, the number of electronic devices that communicate is expanding in both proliferation and complexity across all sectors. This increased deployment broadens the risk footprint and increases the likelihood of cyberattacks.

Robust cybersecurity measures must be intrinsic to all industrial IoT designs to avoid potential catastrophes. Securing such systems from malicious attacks requires careful planning to embed security by design. An IIoT system that features a carefully planned scalable architecture built using secure products, while considering the convergence of OT and IT systems within it, will be better equipped to withstand cyberattacks from evolving threats than one that has grown ad hoc with scant regard to its architecture or connections. A trained staff that embraces the security-conscious culture within an organization will also play a vital part in recognizing and countering threats. Regular threat testing and ongoing audits lead to improvements and optimization that will increase industrial IoT cyberattack resilience.

Cybersecurity regulations, standards and frameworks all serve to address an increasing threat spectrum, guide sectors in best practices and assist organizations in creating their cybersecurity management systems. NXP, with its successful history in security, will play an essential role in securing the future.

www.nxp.com

Document Number: INDSECWP REV 0