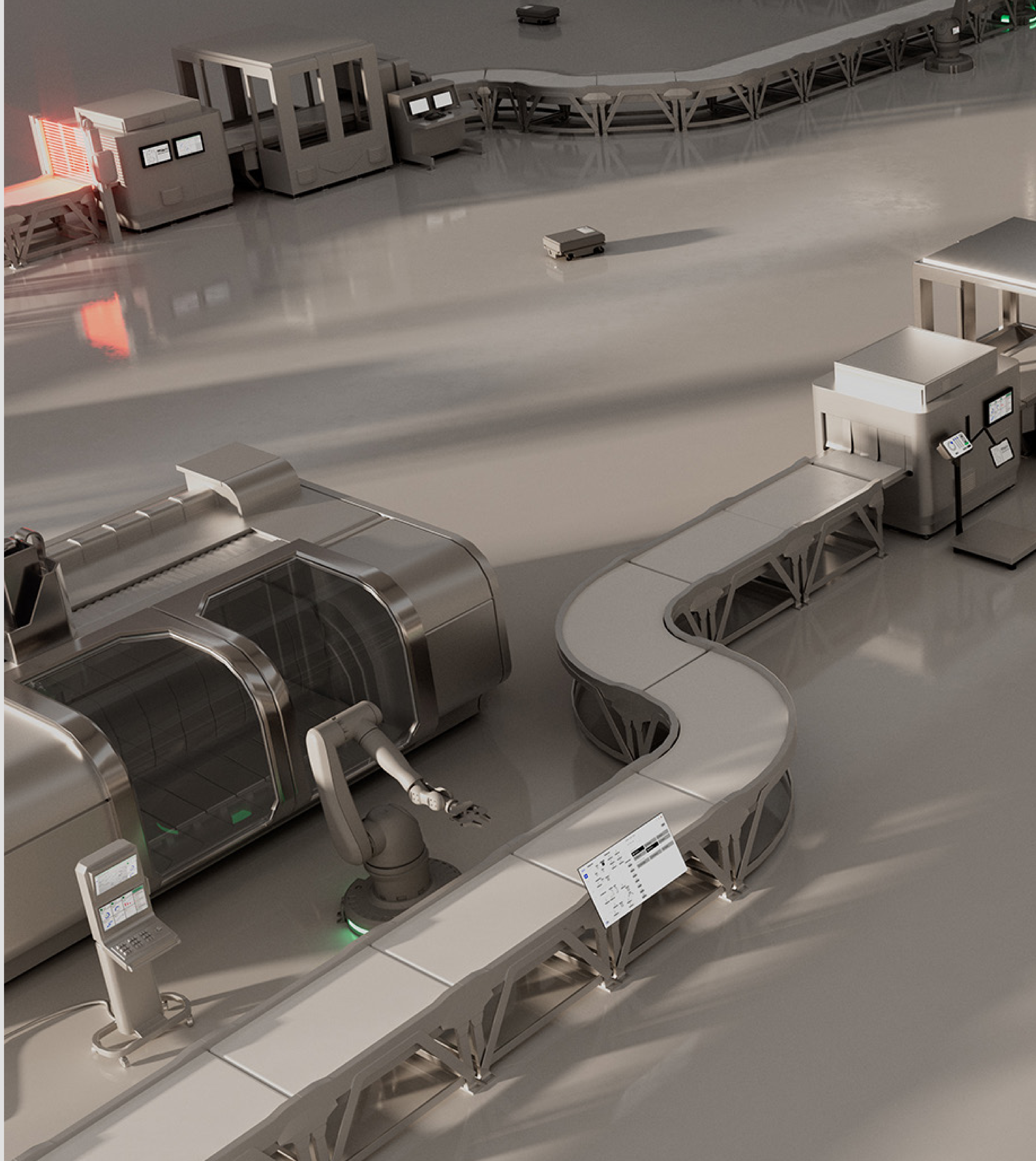
Qt Group

Cybersecurity in Industrial Automation

Securing the Future of Industrial Systems

2025



Executive Summary

Industrial automation is increasingly reliant on software, with connected IoT devices and integrated systems driving operations and exposing traditionally isolated processes to new risks. To shield against increasingly sophisticated cyber threats, manufacturers and software vendors must meet expanding regulatory requirements or face significant financial and reputational risks. This eBook will explore risks and common issues, and illustrate what cybersecurity and cyber-resilience measures can be put in place to, respectively, prevent vulnerabilities and promptly recover in case of attack.

The Urgent Imperative of Cybersecurity in Industrial Automation

Industrial Automation and Control Systems (IACS) underpin everything from power generation and manufacturing to transportation networks and chemical, oil, and gas processes. As digital innovation accelerates, these sectors have become prime targets for cyber attackers capable of halting production lines, triggering safety incidents, and inflicting trillions in economic damage.

In 2025, cybercrime is predicted to cost the global economy $10.5 trillion, with estimates rising to nearly $12.2 trillion by 2031. Enterprises that ignore security in their control environments risk hundreds of billions in annual losses from operational disruptions, regulatory fines, and irreversible reputational harm.

The latest step that the EU has taken to secure the future is introducing the Cyber Resilience Act (CRA), which came into force in late 2024. At the same time, many device manufacturers are using ISA/IEC 62443—a series of standards from the International Society of Automation (ISA)—as a de facto benchmark for compliance.

At its heart, the CRA sets a common standard for every company selling products with digital elements (PDEs) in the EU market, regardless of origin, excluding specific industries already regulated. It also applies to PDEs that were previously outside the reach of established industry or EU rules, such as those outlined in the NIS2 Directive.

With the next CRA regulatory milestone set for September 2026, companies now face the very real risk of significant revenue losses and fines if unprepared. Recognizing this urgency, Qt Group has drawn on 30 years of industry expertise to craft solutions that address evolving market demands and meet stringent requirements.

This eBook outlines a clear pathway to achieving compliance with various regulations and bolstering operational resilience, ensuring critical systems remain protected, corporate reputation stays intact, and automated operations can advance securely into the future.

Supply chain vulnerabilities are a significant risk, with many industrial organizations depending on third-party software and hardware suppliers. If suppliers have weak security practices, attackers can exploit these gaps to infiltrate critical systems. To mitigate such risks—and to meet CRA requirements—a Software Bill of Materials (SBOM) is essential. It outlines the components and versions that a product consists of, enabling organizations to verify they are using secure, up-to-date software.

Notable aspects of the IEC 62443 series include:

IEC 62443-4-2 focuses on the security requirements for individual elements within the industrial control system, with each component designed and implemented securely.

IEC 62443-3-3 specifies detailed technical security requirements for industrial control systems, including network segmentation, access control, and data integrity.

Overall, security processes in product development are covered by IEC 62443-4-1. This standard outlines the requirements for a secure development lifecycle, including threat modeling, risk assessment, and security testing.

System integration and supplier competitiveness are addressed in IEC 62443-2-4.

Structured evaluations, ranging from document reviews and on-site assessments to vulnerability scans, are available through programs like the IECEE-CB Scheme and the ISASecure® Conformance Certification program.

CASE STUDY

The FrostyGoop Malware Attack

A Wake-Up Call for Industrial Cybersecurity

In January 2024, a cyberattack in Lviv, Ukraine, demonstrated the impact of industrial cybersecurity vulnerabilities. The FrostyGoop malware, a sophisticated form of ransomware, targeted heating control systems, disrupting services for approximately 600 apartment buildings during sub-zero temperatures.

How the Attack Unfolded

Hackers exploited weaknesses in the control system's firmware, rolling it back to a version that lacked monitoring capabilities. This prevented operators from detecting real-time issues. The attackers then manipulated system data, falsely indicating that water was heated when only cold water was being distributed. As a result, thousands of residents were left without heating in freezing conditions.

This attack highlights the increasing risks posed by cyber threats to industrial systems, particularly within critical infrastructure sectors like energy and utilities. Malware and ransomware attacks, such as FrostyGoop, demonstrate how cybercriminals can manipulate operational processes, leading to widespread service disruptions.

As industrial systems become more interconnected, the integration of Information Technology (IT) with Operational Technology (OT) introduces new attack vectors. Many organizations are not yet fully prepared for this shift, leaving their legacy systems exposed to cyber threats they were never designed to withstand.

Cybersecurity Challenges in Industrial Environments

Industry Insights from Qt Group's Experience

Qt Group's collaboration with more than 3,500 commercial clients in 70 industries over the past three decades has provided unique insights into embedded software systems, particularly concerning the recurring patterns of software quality that directly affect cybersecurity in industrial automation environments.

Observations consistently show that cybersecurity vulnerabilities originate from fundamental weaknesses in software architecture and code quality, specifically in how software components are designed and interact with each other. While these issues receive less attention than traditional security measures, they expose industrial environments to significant risks.

This eBook focuses on five categories that often arise across sectors and represent fundamental challenges and threats organizations must address.

Architecture Violations & Hidden Dependencies

✓ **Definition:**

Architecture violations occur when software components bypass intended design rules, creating undocumented or unintended couplings between modules.

✓ **Seen in the Industrial Context:**

- Multiple violations are consistently observed across industrial projects.
- Zero violations is the theoretical target in highly regulated industries.
- Some level of deviation appears in all systems in practice.
- High violation rates consistently reflect architectural erosion.
- Compliance is impacted, and there is a delay in audits.

✓ **Cybersecurity Implications:**

- Added challenges in analyzing and securing systems due to reduced modularity and transparency.
- Unexpected attack paths that were never formally reviewed.
- Blind spots in the security posture that are difficult to identify during testing.

Cloned Code

Definition:

Duplicated code segments are typically created through copy/paste rather than proper abstraction.

Seen in the Industrial Context:

- Cloned code often makes up a significant portion of industrial codebases.
- Observed rates fall notably above recommended thresholds for safety-critical domains.
- The target for safety-critical domains is less than 1%.
- Errors found in one location are typically replicated across all clones.

Cybersecurity Implications:

- Increased risk of inconsistent patching when vulnerabilities are found.
- Vulnerability propagation by flaws that are duplicated across copies.
- Increased challenges in the correct implementation of systematic security updates.
- Complicated security audits and verification.

Dead Code

✓ **Definition:**

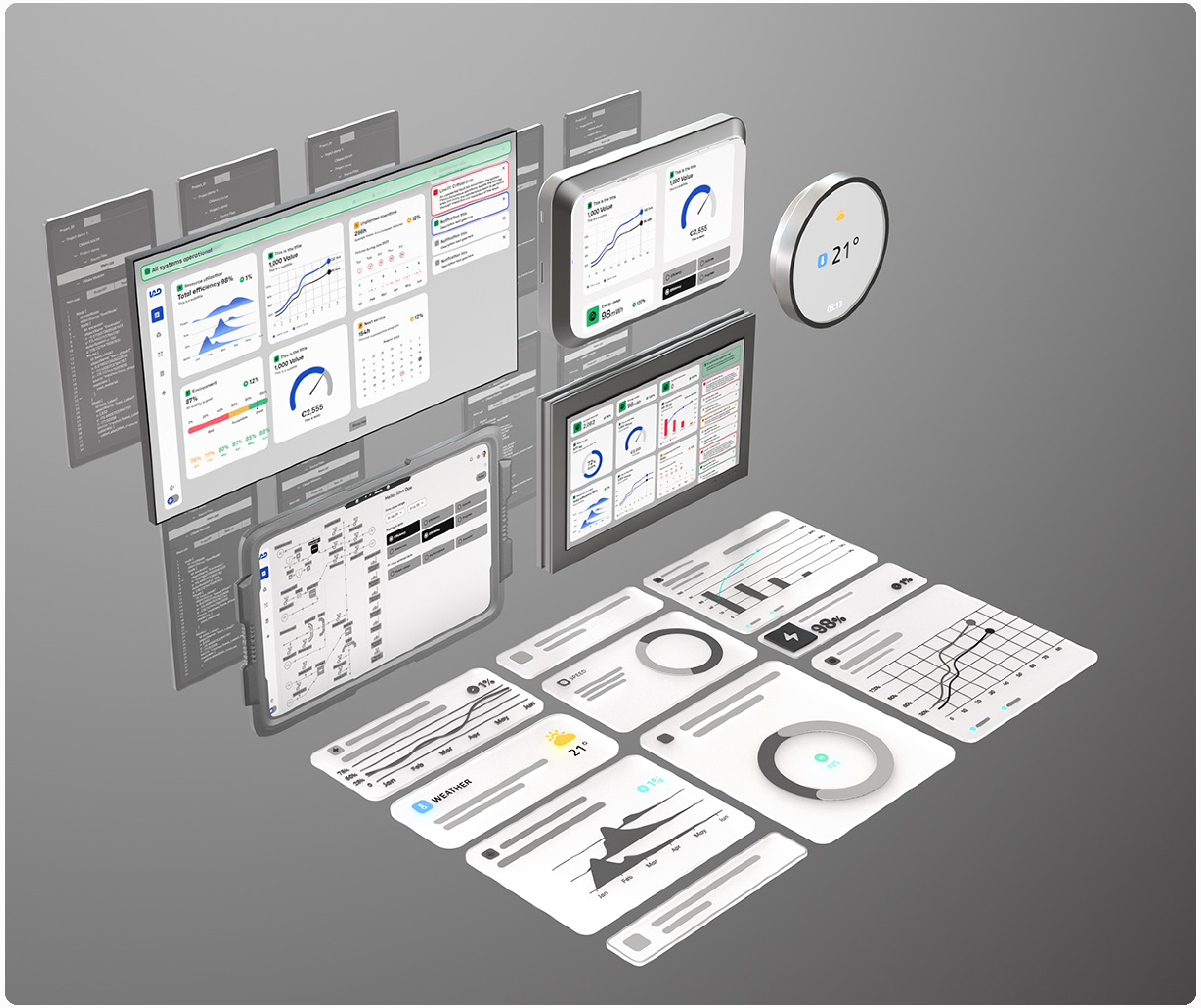
Unused or unreachable code that remains in the codebase.

✓ **Seen in the Industrial Context:**

- Measured deviations are considerably higher than commonly recommended ranges (<2%).
- Eliminating dead code is the ideal, but some persist due to hardware variants or configuration.
- Values above the 2% guideline typically indicate poor code hygiene.

✓ **Cybersecurity Implications:**

- Outdated logic and unpatched vulnerability risks.
- Inaccessibility in regular testing cycles.
- Increased vulnerability through potential trigger points leading to breaches and threats.



Cyclomatic Complexity and Nesting Depth

Definition:

Cyclomatic Complexity quantifies the number of independent execution paths in code, while **Nesting Depth** measures the number of levels of deep control structures (e.g., if, while, for) embedded.

Seen in the Industrial Context:

- Embedded systems frequently exceed the recommended nesting depth of <2 and cyclomatic complexity of <5.
- Appropriate thresholds vary by system type, programming language, and performance constraints.
- Higher complexity metrics can mask subtle bugs and complicate testing.

Cybersecurity Implications:

- Increased risk of hidden security issues and behavioral anomalies.
- Hidden vulnerabilities, hard to detect even for senior developers.
- Increased risk of security patches due to unpredictable side effects.

Coding Style Errors

Definition:

Violations of coding guidelines, like MISRA, AUTOSAR, and others.

Seen in the Industrial Context:

- Industrial software frequently contains significant deviations from established guidelines.
- Deviating from style rules adds to overall compliance errors.
- Full compliance is the goal (estimate of <50 style errors), but large codebases often carry thousands of minor infractions.
- Security-relevant rules can get lost in the noise of other violations.

Cybersecurity Implications:

- Increased complexity in the detection of actual security risks.
- Hidden critical security issues.
- Increased effort on fixes, audit, test, and security.

Quality Enables Security

Qt Group's experience with customers who require safety-critical applications, including industrial automation, shows that software quality issues not only relate to technical debt—they create security risks that worsen over time.

Organizations must integrate quality and security throughout development. The standard division between quality assurance and security teams leaves many vulnerabilities unaddressed until they become serious problems. These issues impact both maintenance and compliance while exposing systems to security weaknesses by hiding potential attack paths.

To address these risks effectively, Qt Group recommends:

Have complete 360° visibility into your codebase—know all the ins and outs.

Design and implement security into the architecture from the beginning.

Use automated tools to detect quality issues before they become security problems.

Establish clear code-quality standards across development teams.

Monitor, analyze, and test continuously to catch issues early.

Note: The Qt Group's ideal software quality baselines presented combine insights from established industry standards, academic research, and 30 years of real-world implementation experience across industrial sectors.

What You Need to Do

To effectively address cybersecurity challenges in industrial automation, you should rely on trusted partners who discuss the need for long-term investment in security and a vast offering that can fulfill most needs. You should also prioritize the following strategies:

Enhance Cybersecurity Training, Expertise, and Culture

Ongoing training and education for development and operations teams help bridge the skills gap and integrate security best practices into daily workflows. In addition to technical training, building a culture that emphasizes early reporting of vulnerabilities, development of dedicated cybersecurity expertise, and meticulous documentation of software dependencies are crucial.

Strengthen Supply Chain Security

Implementing comprehensive supply chain risk management strategies and maintaining transparency through an SBOM can help mitigate external risks and ensure the integrity of software components. This holistic approach reinforces the overall security posture.

Proactive Security Integration Across the Development Lifecycle

Security should be an integral part of industrial system development, from initial design through deployment. Security must be considered at every stage, with cross-organizational efforts involving risk management, product lifecycle management, and effective communication of vulnerabilities.

Invest in Advanced Code Quality Assurance

Tools for architecture verification, clone detection, dead code analysis, and complexity monitoring, and more, allow companies to identify and mitigate vulnerabilities early in the software development cycle. This process includes the systematic review of every class and functionality, with documented risk severity and tailored guidance for developers.

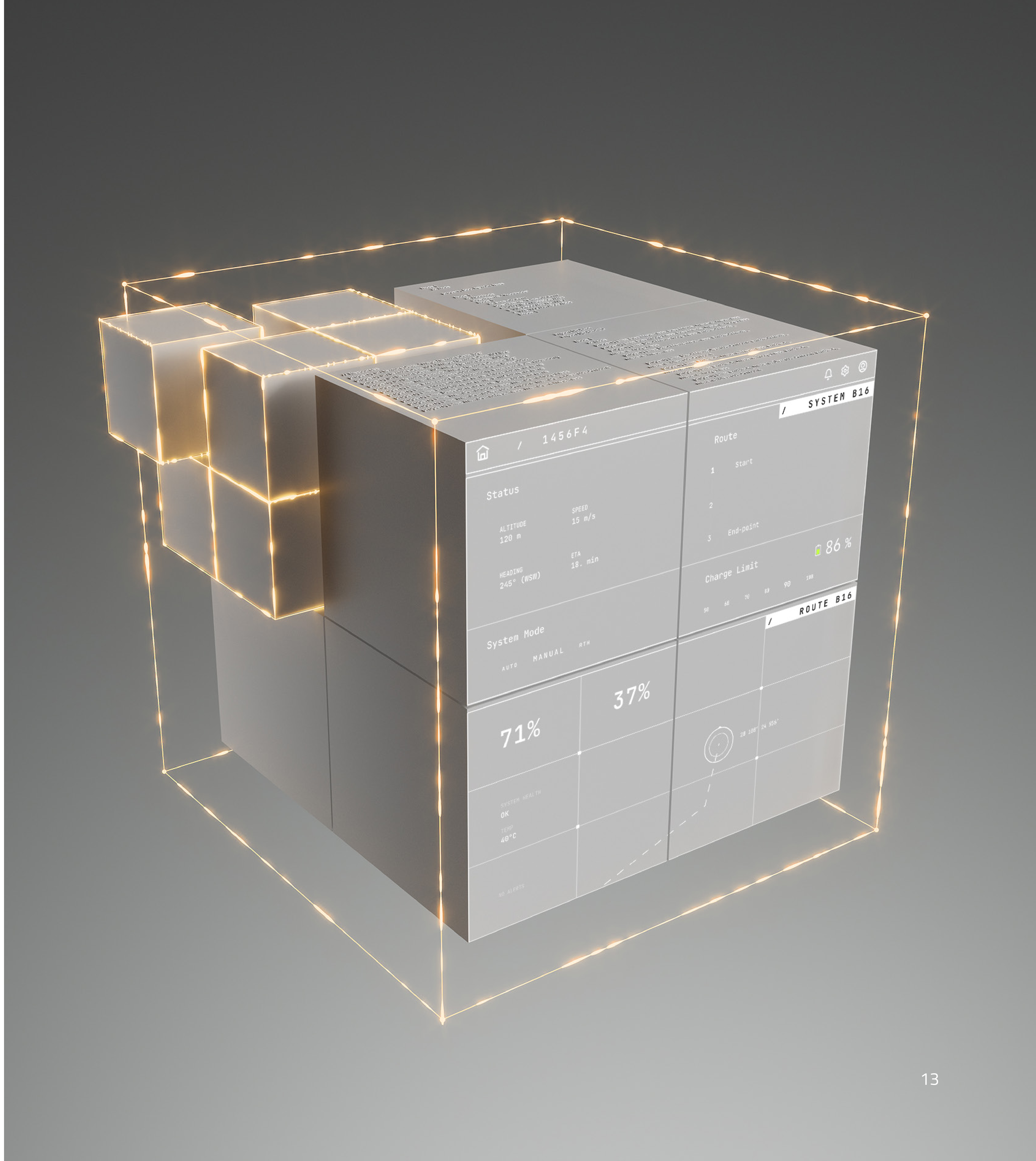
How Qt Group Can Help

With its strong presence in highly regulated industries, like the medical and automotive sectors, Qt Group took security and cybersecurity as first-class concerns long before the introduction of Europe's CRA. With 30 years of industrial presence, Qt Framework has been developed with security at its core to offer industrial companies across sectors software libraries that deliver safe, reliable devices.

On the cybersecurity side is a series of libraries and tools within Qt that help prevent breaches and vulnerabilities, such as Qt Application Manager, data encryption, and more.

On the cyber-resilience side, a strong apparatus of reparative measures is in place to take prompt action in case of vulnerability breaches, including long-term support, vulnerability management, and transparency.

More recently, software quality has been at the core of Qt Group's investment in a dedicated Quality Assurance portfolio (Squish, Coco, Test Center, and Axivion) that helps counteract many of the challenges discussed above. We'll delve into that first, and then look into preventive and reparative measures.



Code Quality and Security Require Advanced Capabilities

Organizations need powerful tools to detect and address vulnerabilities before they become security problems. Axivion provides targeted solutions that address the fundamental code quality issues identified earlier.

Prevention Through Advanced Analysis

Axivion integrates seamlessly with CI/CD pipelines, providing a full 360° view of the codebase and architecture. By systematically analyzing source code, development teams can detect potential security issues at their earliest stages before they enter production environments.

The tools also ensure software implementations remain aligned with their intended architecture, preventing the gradual drift that creates hidden dependencies and security blind spots. This directly addresses the architecture violations we identified as a significant security risk in industrial systems.

Building Secure Industrial Systems

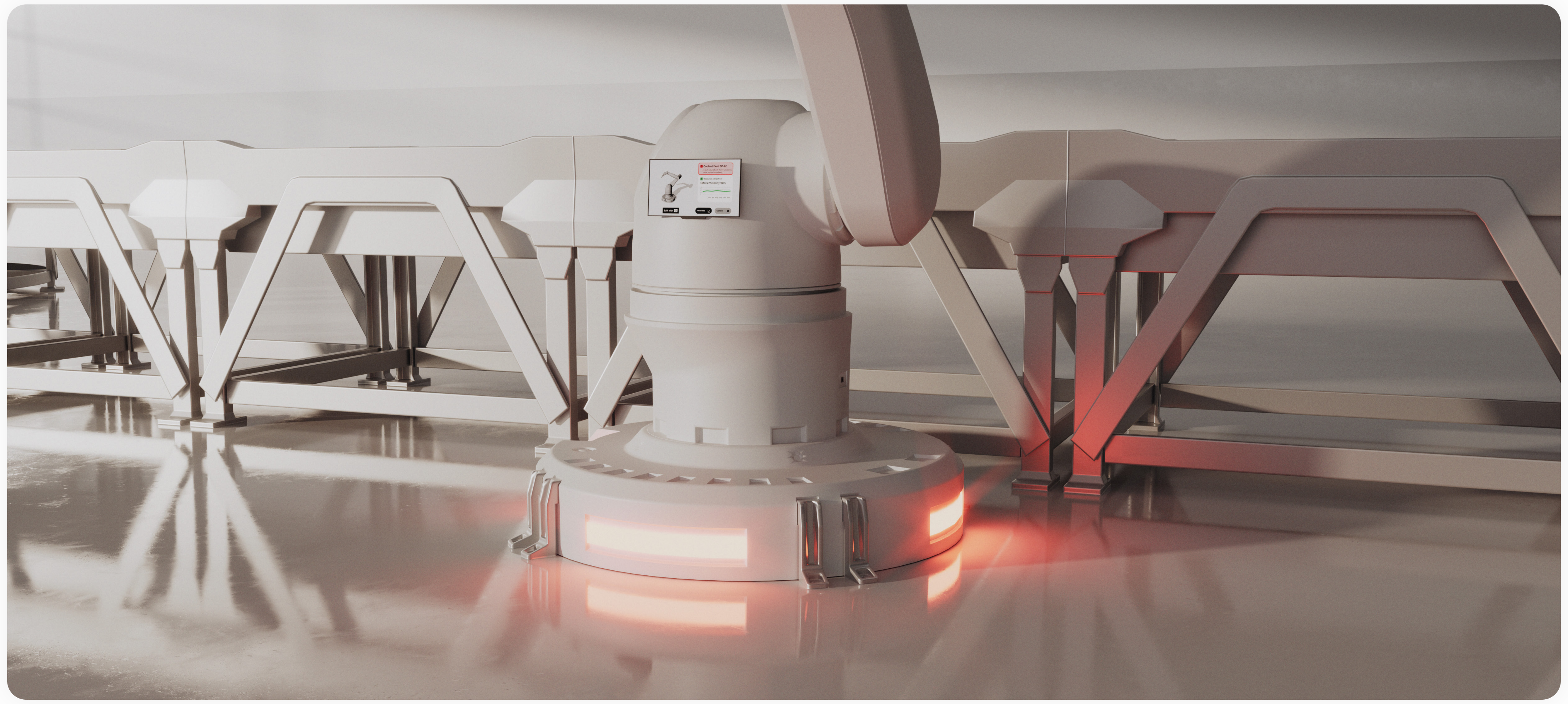
Axivion provides a comprehensive solution for implementing security measures in two ways:

Architecture Verification provides an automated solution to standardize and ensure structural integrity by equipping developers with tools to follow the intended system architecture. By making architecture violations and technical debt visible, Axivion prevents code erosion that may lead to security vulnerabilities. Beyond functional architecture checks, the tool verifies that safety and security specifications are correctly implemented.

Static Code Analysis identifies security weaknesses by analyzing the code, even in highly complex industrial environments. The analysis detects:

- Vulnerabilities that might otherwise remain hidden.
- Violations of coding standards (e.g., MISRA, CERT C/C++, CWE, etc.) that may lead to non-compliance.
- Problematic patterns and common coding pitfalls that can introduce defects.
- Quality issues that impact long-term maintainability.

Additionally, by allowing the definition of specific sets of rules, Axivion enables teams to handle edge cases and unique complexities arising in regulated industries.



Cybersecurity

Cybersecurity has to do with the preventive measures designed to prevent breaches and vulnerabilities from occurring in the first place.

Sandboxing

By isolating applications to run within a container and managing access via application digital signature, Qt Application Manager offers a secure, controlled environment for running applications. It prevents unauthorized interaction with core system functions and ensures sensitive data protection. The key benefits of sandboxing include:

- **Isolated environments:** preventing data leakage across apps.
- **Hardware binding:** reducing exposure by tying containers to designated hardware.
- **Lifecycle management:** enabling secure deployment, updates, and monitoring.
- **Multi-industry support:** offering strategic advantages such as centralized control, multi-vendor system assurance, and scalability.

Data Encryption & Secure Communication

Default encryption tools such as TLS and X.509 protect sensitive information both in transit across HMIs and at rest, preventing interception and tampering while supporting compliance with IEC 62443-3-3 and IEC 62443-4-2.

Memory Profiling

Tools like Memcheck, Valgrind, and Cppcheck in Qt Creator enable developers to track memory usage, detect leaks, and avoid buffer overflows.

Authentication and Authorization

Integration with various authentication frameworks ensures that user identities are verified and permissions are correctly managed, fulfilling IEC 62443-3-3 requirements, including only authorized personnel being permitted to interact with critical HMI functions.

Secure Coding Practices

A strong emphasis on secure coding practices is fundamental to meeting IEC 62443-4-1 requirements. Regular code reviews, static analysis, and adherence to secure coding guidelines form the backbone of the development process.

Build Customization

By including only essential libraries and supporting static builds, the exposure to third-party vulnerabilities can be reduced. This approach aligns with modern supply chain security practices by limiting dependency footprints.

Cyber-Resilience

Cyber-resilience has to do with the reparative measures aimed at handling breaches and vulnerabilities once they are detected. They are concerned with documenting the vulnerability, notifying stakeholders, fixing the issue, and providing patches.

Vulnerability Management

With decades of production history in Industrial Automation, Qt Group has robust security protocols and practices in place to efficiently handle a variety of vulnerabilities and issues. The security issue handling process includes third-party-originated issues, with documentation of all verified issues.

As an authorized CVE Numbering Authority (CNA), Qt Group assigns unique IDs to any discovered cybersecurity issue, contributing to the Common Vulnerabilities and Exposures (CVEs) Program's mission to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities. This helps prevent the chaos of unverified, duplicate, or inaccurate reports.

Transparency

Qt Group promptly communicates any newly found issues to its customers to mitigate any impact.

Device Malfunction SP-L2

An unexpected fault occurred with SP-L2's cooling. Operations were discontinued to limit device damage. The maintenance team has been notified to perform a thorough inspection of the issue.

SBOM

By providing a detailed software bill of materials (SBOM), Qt Group helps the Qt community and ecosystem take immediate action whenever a security flaw is discovered.

Long-Term Support

Five-Year Long-Term Support (LTS) gives access to updates and security patches, ensuring market presence over time. For those who need maintenance and support beyond the LTS period, Qt Group offers various additional services, such as delivering security patches and providing extended customer support. Such stability simplifies adherence to industry regulations, including CRA and IEC 62443, while reducing the operational overhead typically associated with short-term maintenance implementations.

OSS & Commercial

The availability of open-source and commercial software variants helps strengthen the community, quality, and innovation.

- **Open source** nurtures rapid innovation through community collaboration. In the case of Qt, a community of over 1.5 million developers actively using and vetting the code on innovative research projects. However, incorporating open source into a product requires managing updates and documentation independently.

Commercial users benefit from innovation and large-scale software testing by the open-source community, while enjoying the advantage of keeping their intellectual property protected. They also benefit from less frequent version updates, as well as Qt Group providing monitoring, security updates, and reporting. In terms of regulatory compliance, commercial customers get a wealth of the work needed to meet requirements, ready-made for Qt's part of their product.

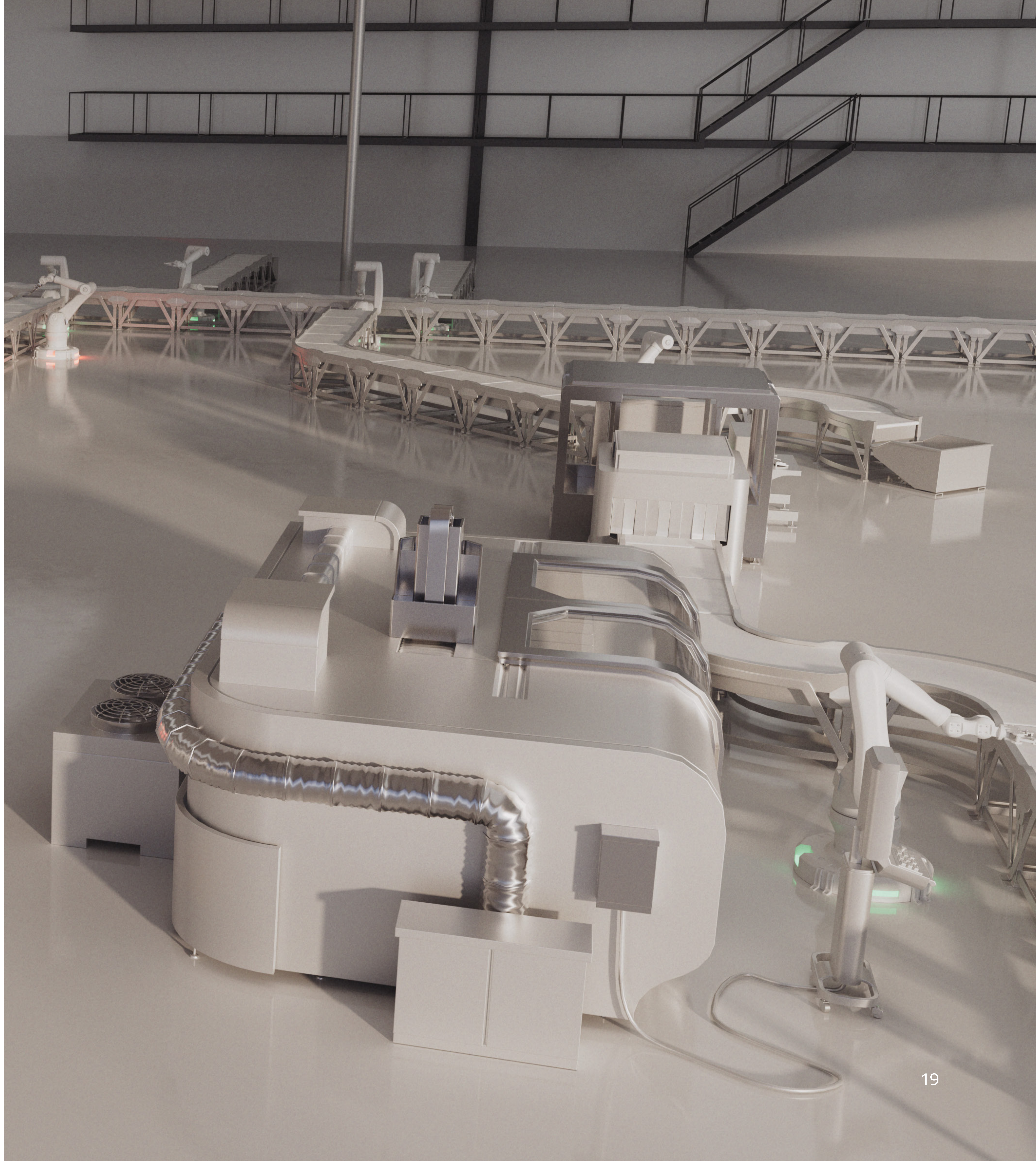
Aspect	Advantages of OSS	Risks of OSS
Cybersecurity	Transparent code for inspection and customization	Large patching obligations on end users
Cost	Free or low-cost upfront	Hidden costs in customization, compliance, and maintenance
Support	Community and paid third-party support	Slow response times or insufficient expertise
Flexibility	High adaptability for specific industrial needs	Strong in-house expertise required

Conclusion

Modern industrial environments are no longer isolated islands but rather dynamic, interconnected ecosystems in which cybersecurity risks require forward-thinking strategies. The rise of IoT connectivity and evolving regulatory pressures, exemplified by the CRA, highlight the urgency for manufacturers and software vendors to reconsider their security approaches.

With Qt Group as your technology partner, you can rely on high-quality software and solutions that help you reduce cyber threats and support your factory operations in transitioning into a connected world.

The information contained in this document does not constitute legal advice. It is provided for informational purposes and discussion of the subject matter only. Content is subject to change and Qt Group does not guarantee the accuracy or currentness of the contents of this document. The information contained here is not, and should not be used as, a substitute for legal advice.



Qt Group

Qt Group offers cross-platform solutions for the entire software development lifecycle.

Qt Group (Nasdaq Helsinki:QTCOM) is a global software company, trusted by industry leaders and over 1.5 million developers worldwide to create applications and smart devices that users love. We help our customers to increase productivity through the entire product development lifecycle - from UI design and software development to quality management and deployment.

Our customers are in more than 70 different industries in over 180 countries. Qt Group is headquartered in Espoo, Finland, and employs over 800 people globally.

Qt.io