QNX

Modern Industrial Automation Needs a Safer Software Foundation

Industrial Automation is Entering a New Phase

For decades, manufacturers and industrial operators have relied on tightly controlled, hardware-centric systems to deliver repeatable performance, long lifecycle reliability and deterministic control. That foundation still matters. But the environment around it is changing quickly. Industry 5.0 is expanding the role of automation beyond productivity alone, placing greater emphasis on resilience, human-machine collaboration, sustainability, flexibility and responsible technology adoption.

> **“As Industrial Systems Become More Software-Defined, Connected And AI-Enabled, Deterministic Performance, Safety And Security Need To Move From Individual Components Into The Platform Itself.”**

At the same time, industrial systems are becoming more intelligent and more connected. AI, machine learning, edge computing, digital twins, real-time monitoring, IIoT platforms and richer human-machine interfaces are creating new possibilities for optimization, autonomy and operational insight. These capabilities can help industrial organizations improve efficiency, reduce downtime, accelerate development and respond faster to changing business requirements. But they also introduce new demands on the underlying architecture.

Industrial automation is approaching a tipping point:

50%
Of CEOs

Are demanding accelerated growth and operational excellence.

More than
80%

Of organizations report increased or continued investment in hyper - automation initiatives.

More than
25%

Of industrial companies’ capital spending over the next five years is expected to go towards automated systems.

88%

Of manufacturing leaders say Industry 4.0 will increase productivity – underscoring the pressure on industrial organizations to modernize architectures, scale automation and adopt platforms that can support safer, more efficient transformation.

The result is an inflection point for industrial automation. The next generation of industrial systems must be deterministic, performant, safe, and secure.

From PLC-centric Automation to Software-Defined Industrial Platforms

PLC-centric automation has served industry well. In many environments, they remain vital control islands for field-level operations, certified I/O and safety functions.

But Industry 5.0 is demanding more than what PLC-only architectures were designed to provide. Modern industrial systems increasingly need to run hard real-time safety control, soft real-time automation and best-effort AI, analytics and connectivity workloads together. They need to support human-machine collaboration, real-time monitoring, high-performance computing, richer visual interfaces, cloud connectivity and continuous software updates. They also need to manage rising safety and cybersecurity requirements without compromising predictable execution.

This means evolving architecture. Industrial organizations are moving towards models where PLCs continue to perform critical control functions, while MPU-based and high-performance compute platforms provide supervisory safety, security, AI, connectivity and consolidation layers. In this model, the software foundation becomes the enforcement layer that helps ensure real-time behavior, workload separation, fault containment and compliance readiness.

The Modernization Challenge

As machines, plants and devices become more connected and more intelligent, engineering teams face a broader set of challenges. They need to ensure reliable operation in unpredictable, high-demand environments. They need to integrate ageing machinery with newer software and hardware platforms. They need to protect connected systems from growing cybersecurity risks. They need to reduce jitter and latency to maintain repeatable precision. They need to manage hardware delays, supply chain constraints and limited access to physical prototypes. They also need to satisfy evolving safety standards while building and retaining the right technical expertise.

These pressures are magnified by the move towards mixed-critical systems. Industrial platforms increasingly need to consolidate safety and non-safety functions, real-time and non-real-time workloads, and multiple software environments on a shared compute foundation. Without strong isolation and predictable execution, consolidation can introduce unacceptable risk. Without security-by-design, increased connectivity can expand the attack surface. Without a safety-certified foundation, certification efforts can become slower, more expensive and harder to manage. For industrial automation teams, the message is clear: incremental updates are no longer enough.

> **QNX helps industrial teams build software-defined embedded systems with deterministic performance, microkernel-based isolation, safety-certified software and security-by-design.**

QNX Provides the Trusted Foundation for Resilient Industrial Systems

The operating system as the supervisory safety and security envelope

QNX provides foundational software for industrial organizations building resilient, safe and secure embedded systems. Its portfolio is designed to help developers modernize industrial platforms, consolidate workloads and accelerate development while preserving the real-time behavior and reliability required for mission-critical environments.

At the center of this value proposition is a simple idea: as industrial systems become more complex, the operating system and hypervisor are no longer background infrastructure. They become the supervisory safety and security envelope for the system. They help determine whether timing-critical tasks execute predictably, whether failures are contained, whether mixed workloads can coexist safely and whether the architecture can support compliance requirements as technology evolves.

Deterministic Performance Where Timing Matters

Industrial automation depends on timing. Whether the system is controlling machinery, coordinating production processes, monitoring critical equipment or supporting safety functions, delays and unpredictability can have operational consequences. QNX OS is designed for deterministic real-time behavior, helping developers build software architectures that support high availability, high performance and reliable execution.

The QNX platform supports timing-critical tasks that require rapid and consistent response. It is designed to help industrial teams reduce latency and jitter, support real-time prioritization and preserve predictable execution across increasingly complex embedded environments. For systems that must respond correctly under demanding conditions, this real-time foundation is essential.

Isolation for Mixed-Criticality Consolidation

As industrial platforms evolve, more functions are being consolidated onto shared compute architectures. Safety control, automation, AI, analytics, connectivity, HMI and system services may need to coexist on one platform. That creates a clear architectural requirement: workloads must be separated so that one component cannot compromise another.

QNX addresses this challenge through its microkernel architecture and virtualization capabilities. In the QNX architecture, applications, drivers and services run in their own address spaces outside the kernel, helping prevent crashes from taking down other components or the kernel itself. Failed components can be restarted without rebooting the system or disrupting overall performance, while high-availability and heartbeat monitoring can detect and manage process failures, crashes or hangs.

For teams consolidating diverse systems, QNX Hypervisor adds another layer of flexibility. It enables multiple isolated environments to coexist on a single system-on-chip and supports the safe co-hosting of QNX, Linux and Android. This can help simplify consolidation, support legacy integration and preserve separation between workloads with different safety, timing or functional requirements.

Safety and Security Built Into the Foundation

Modern industrial systems need to be both safe and secure. Connected machines and software-defined platforms face increased cybersecurity exposure, while safety requirements remain central to mission-critical industrial operations. QNX is designed to support both needs at the foundational software layer.

QNX reduces attack surface by using a minimal amount of kernel-mode code, while drivers and services run outside kernel space to help protect mission-critical functionality. The platform also supports layered security policies, granular control of privilege levels, encrypted and self-verifying filesystems, secure logging, memory protection, secure boot, trusted boot and chain-of-trust capabilities.

For safety-critical development, QNX provides pre-certified software and supporting artefacts that can help reduce certification scope, risk, time and cost. QNX OS for Safety and QNX Hypervisor for Safety are certified by TÜV Rheinland to IEC 61508 SIL 3, ISO 26262:2018 ASIL D and IEC 62304 Class C. QNX C/C++ toolchains are qualified to IEC 61508:2010 SIL 3 and ISO 26262-8:2018 ASIL D.

This gives industrial teams a more confidence-inspiring path to modernization: one that embeds safety and security into the development foundation rather than treating them as downstream validation tasks.

Faster Development Without Unnecessary Complexity

Industrial organizations need to modernize, but they also need to control cost, risk and engineering complexity. QNX helps teams accelerate development through a combination of pre-integrated components, pre-ported open-source libraries, cloud-powered workflows and expert support. The deck notes that many commonly used libraries in industrial automation engineering are pre-ported, and that QNX supports modern workflows such as CI/CD, QNX-based virtual machines and cloud development on AWS and Azure.

This matters because software-defined industrial development requires more than a real-time operating system. It requires a development environment that helps teams iterate, test, scale and deploy efficiently, without sacrificing the determinism, safety and security required in production systems.

In Practice: Modernizing Critical Gas Analysis Platforms

A provider of premium gas analysis for critical environments and complex applications illustrates the kind of industrial use case where this foundation matters. Its gas analyzers are used in environments requiring high precision, high availability and high resilience, including energy production, chemical manufacturing, industrial and medical gas production, and semiconductor manufacturing.

In these systems, accuracy, response and timing are critical. The customer required a robust platform capable of supporting real-time performance, security and safety certification needs. A high-performance QNX RTOS platform running on an NXP i.MX93 applications processor, supported the customer's need for a reliable and robust gas analyzer platform.

Build the Next Generation of Industrial Automation on QNX

Industrial automation is moving from fixed, PLC-centric control towards software-defined, AI-enabled and mixed-criticality systems. The path forward is not simply more compute. It is a safer, more deterministic and more secure software foundation that can help industrial teams modernize with confidence.

QNX gives developers that foundation. With deterministic real-time performance, microkernel-based isolation, hypervisor-enabled consolidation, safety-certified software and security-by-design, QNX helps industrial organizations build resilient embedded systems for the next era of automation.

Modernize industrial automation with a foundation built for deterministic performance, safety, security and scale.

Learn more →

Get started →

About QNX

QNX, a division of BlackBerry Limited, enhances the human experience and amplifies technology-driven industries, providing a trusted foundation for software-defined businesses to thrive. The business leads the way in delivering safe and secure operating systems, hypervisors, middleware, solutions, and development tools, along with support and services delivered by trusted embedded software experts. QNX® technology has been deployed in the world's most critical embedded systems, including more than 275 million vehicles on the road today. QNX® software is trusted across industries including automotive, medical devices, industrial controls, robotics, commercial vehicles, rail, and aerospace and defense. Founded in 1980, QNX is headquartered in Ottawa, Canada.

Learn more at qnx.com →