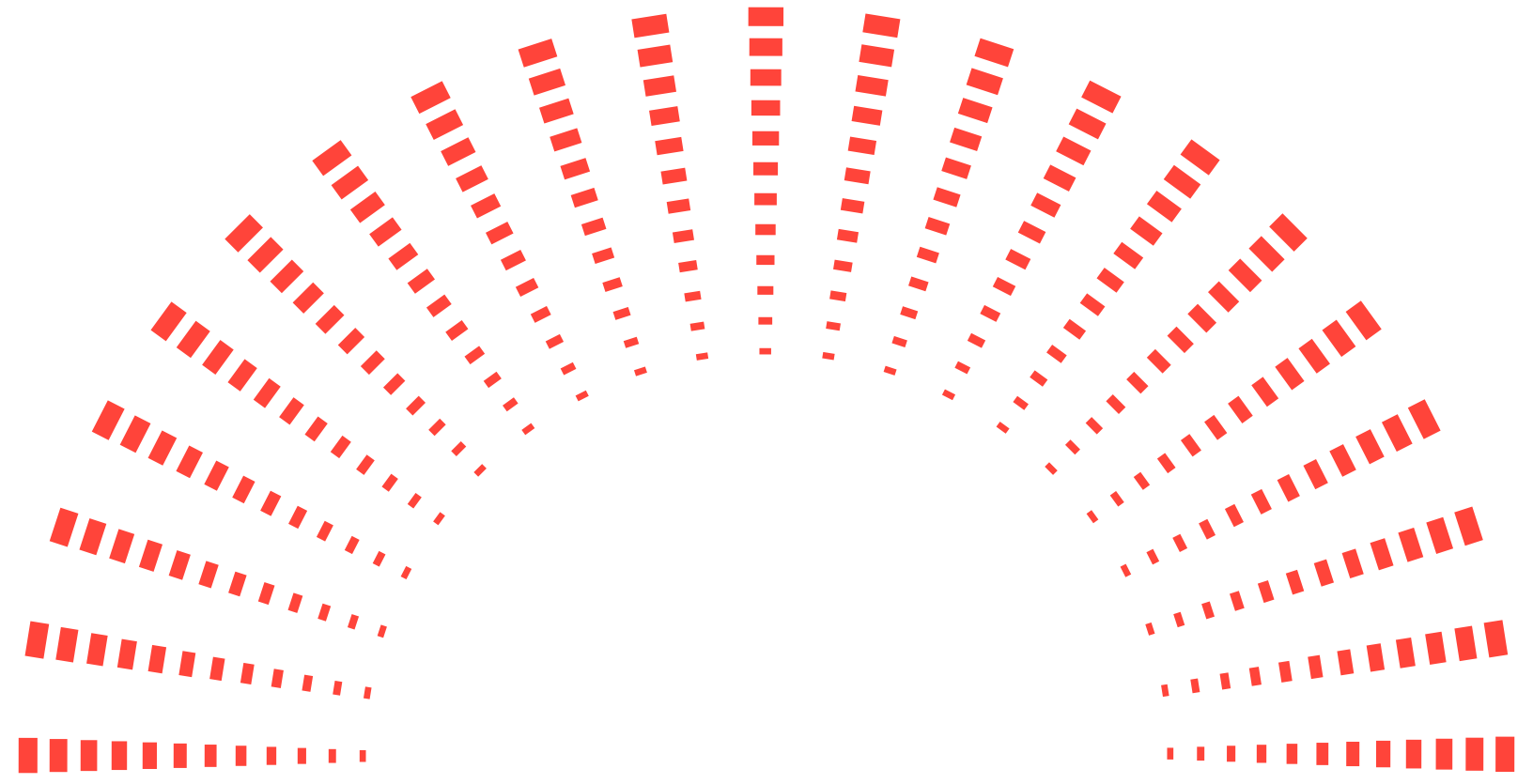
QNX

Solution Guide

Industrial Automation

Foundational Software for Resilient, Safe and High-Performance Industrial Automation Systems



Industrial Automation Requires a Strong Foundation

Industrial automation is moving beyond isolated controllers and fixed-function machinery toward software-defined, highly connected systems that must deliver real-time performance, strong cyber resilience, and easier lifecycle upgrades. Industry 5.0 adds another layer of pressure by emphasizing human-machine collaboration, resilience, sustainability, and responsible use of AI in operational environments.

Industrial Automation Is at an Inflection Point

Industry 5.0

Human-machine collaboration, resilience and sustainability are raising system requirements.

Mixed criticality

Safety Control, HMI, analytics, connectivity and AI increasingly need to run together.

Modernization pressure

Legacy plants and machines must evolve without sacrificing uptime or safety.

The Future of Industrial Automation is driven by continuous demands on modernizing infrastructure to redefining operations with futuristic technologies. Industrial teams are being asked to modernize aging equipment while also introducing higher-performance compute, richer user interfaces, analytics, digital twins, and AI-enabled features.

Across factories, energy systems, machine builders, warehousing environments, and process industries, engineering teams are being asked to deliver more flexibility without compromising determinism. They must connect machines to the cloud, build control automation, add data-driven optimization, and in many cases incorporate AI-enabled functions while still preserving predictable execution for mission-critical control.

This creates a new baseline: industrial platforms must be safe, secure, upgradable, and capable of consolidating diverse workloads on a single computing architecture. The foundational software layer becomes the enforcement point for timing, separation, fault containment, and lifecycle maintainability.

Industrial Automation Trends and Development Challenges

What is shaping the market	What is holding teams back
• Software-defined industrial systems that are easier to update and scale	• Need for reliable operation under hard real-time constraints
• Digital twins and virtual environments that reduce hardware dependence	• Growing cybersecurity exposure in connected operational environments
• Smart automation and optimization through IIoT, sensing, and analytics	• Difficulty integrating aging machinery with newer compute platforms
• Safe and secure-by-design architectures driven by regulation and risk	• Certification effort and shortage of safety/security expertise
• AI-powered autonomy and decision support at the edge	• Hardware delays, fragmented tooling, and long validation cycles

Legacy Development Needs Transformation

Many organizations still rely on legacy operating environments, custom patch stacks, and disconnected toolchains. As systems grow more compute-intensive and networked, those choices increase risk: more jitter, more integration burden, more exposure to vulnerabilities, and a slower path to certification or recertification.

The Big Shift From PLC-Centric Automation to Mixed-Criticality Platforms

PLC-centric automation remains valuable for deterministic field-level control, certified I/O, and long lifecycle deployments. But Industry 5.0 use cases now require more than a PLC-only architecture can comfortably provide on its own: richer HMIs, supervisory software, advanced analytics, vision processing, edge AI, secure connectivity, and fleet-wide software maintenance.

PLC-centric strengths

- Deterministic execution
- Built-in safety functions
- Simple, certifiable control loops
- Long service life in the field

Why additional MPU / SoC compute is being added

- Memory protection and virtualization
- Multi-core performance and hardware acceleration
- Consolidation of control, HMI, connectivity, and AI
- Cloud-connected workflows and OTA-style update models

The result is a mixed-criticality system: hard real-time safety control, soft real-time automation, and best-effort workloads such as analytics or AI all run on one platform. Hardware consolidation alone is not enough. The software foundation must enforce temporal and spatial separation, predictable execution, and fault containment.

This is why the RTOS (Real-Time Operating System) becomes the supervisory safety and security envelope. In modern industrial architectures, the operating system is not just a runtime environment; it is the mechanism that controls scheduling, isolation, recovery, and system integrity.

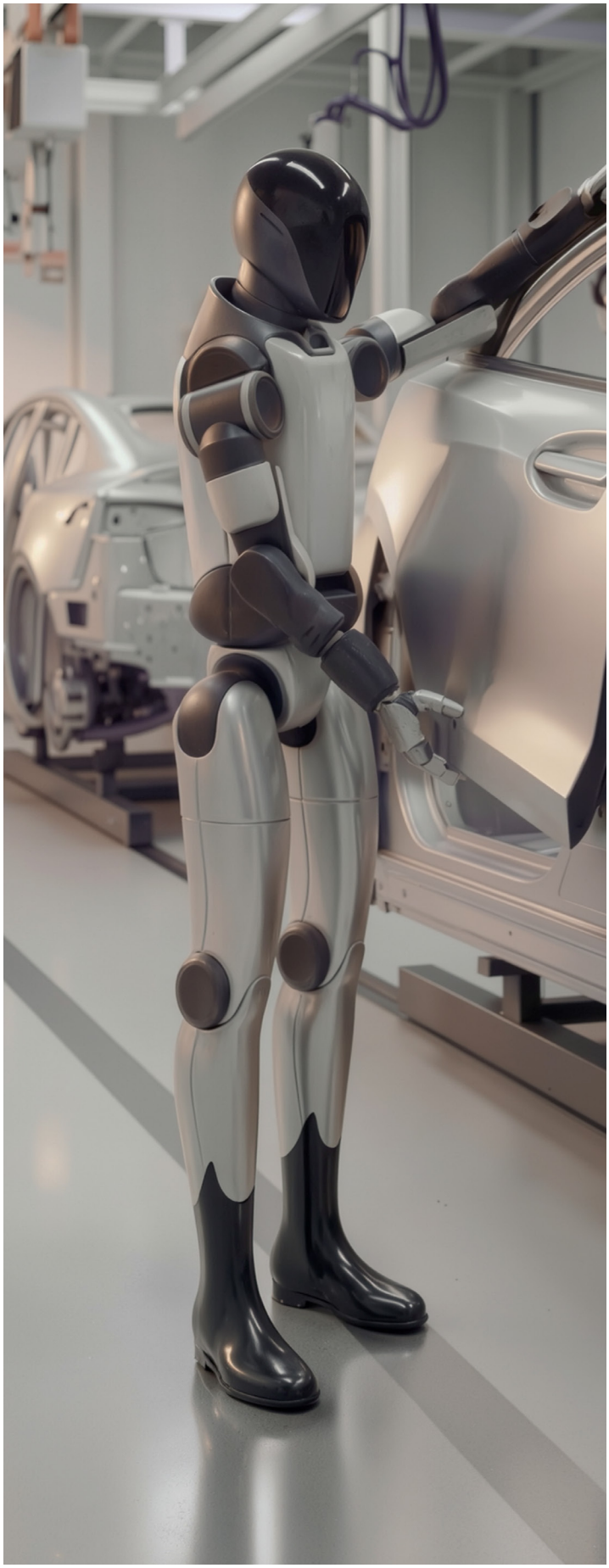
Preparing for the Shift

Industrial automation is shifting from PLC-only designs to architectures that combine controllers with higher-performance MPU and SoC platforms. A Microkernel-architecture-based QNX RTOS provides a durable path for building resilient, mixed-criticality industrial systems. QNX enables software-defined industrial automation with a certified, secure, and lifecycle-ready foundational stack.

While AI and advanced automation increase capability, they also increase architectural and regulatory risk. Here is where a QNX RTOS-based supervisory layer is essential for deterministic execution, separation, recovery, and compliance.

QNX Software Stack for Industrial Automation

The QNX General Embedded Development Platform (GEDP) provides the foundational stack needed to build software-defined industrial systems: software, hardware enablement, and development tooling packaged around a microkernel-based hard QNX real-time operating system.



QNX Provides the Foundational Software to Build Reliable Industrial Systems

Software

QNX OS, safety variants, hypervisor, middleware, frameworks, third-party integrations, and open-source support.

Hardware Enablement

Broad ARM and x86 support, board support packages, drivers, networking, graphics, and AI-ready platform compatibility.

Development Tools

Momentics IDE, VS Code tooling, command-line tools, profiling, debugging, support, training, and lifecycle services.

How QNX GEDP Addresses Industrial Automation Needs

Industrial Need	QNX General Embedded Development Platform
Deterministic execution	Priority-based real-time scheduling and microkernel design help critical tasks run predictably
Freedom from interference	Process isolation and hypervisor partitioning separate mixed-criticality functions
Certification efficiency	Pre-certified safety variants, safety artifacts, and qualified toolchains reduce certification scope
Cyber resilience	Reduced attack surface, secure boot, encryption, access control, and hardened system services strengthen the base platform
Lifecycle longevity	POSIX-based portability, BSP support, virtualization, and broad ecosystem access simplify migration and upgrades
Addressing Ongoing Regulations & Certifications	Regular major and minor updates for the QNX OS, QNX Hypervisor, QNX OS for Safety to address latest certifications and regulatory landscape.

Core QNX General Embedded Platform Components

QNX OS

Hard real-time microkernel foundation with deterministic performance, efficient resource management, reliability, and fault isolation.

QNX OS for Safety

Safety-certified variant for systems targeting IEC 61508 SIL 3 and other high-integrity domains.

QNX Hypervisor

Microkernel-based virtualization for consolidating multiple OS environments on a single SoC while maintaining separation.

QNX Hypervisor for Safety

Safety-certified virtualization layer for mixed-criticality and consolidated embedded architectures.

Supporting Services and Frameworks

- OS services such as Filesystem for Safety and Communications for Safety
- Frameworks for sensors, graphics/HMI, security, audio, multimedia, and advanced virtualization
- Containers support for OCI-compliant application packaging with OS-level restrictions and isolation
- Third-party ecosystem support for industrial protocols such as DDS, TSN, Profinet, EtherCAT, CANOpen Safety, Modbus, and more
- Open-source software access for components such as OpenCV, ROS 2, TensorFlow, PyTorch, SQLite, Fast-DDS, gRPC, and related packages

> **In AI-driven industrial systems, intelligence decides — but a safety-certified QNX RTOS enforces and executes deterministically.**

Why Choose QNX for Industrial Automation

Real-time reliability and performance	Priority-based scheduling, adaptive partitioning, and fault isolation help critical workloads run and recover predictably.
Functional safety readiness	Pre-certified OS and hypervisor variants, safety artifacts, and qualified toolchains streamline certification programs.
Cybersecurity by design	Microkernel isolation, reduced attack surface, encrypted and self-verifying filesystems, secure boot, and layered security controls protect system integrity, ongoing support for CRA (Cyber Resilience Act).
System consolidation	QNX Hypervisor helps co-host safety and non-safety workloads, including legacy environments, on a single processor platform.
Portability and longevity	Better Interoperability with POSIX-compliant interfaces, OCI (Open Container initiative) compliant Containers, hardware abstraction, virtualization, BSPs, and broad ecosystem support making migration and lifecycle maintenance easier.

Accelerate the Development and Deployment of Industrial Systems with QNX

Using QNX GEDP, companies can accelerate the development and deployment of safe, secure, and scalable industrial automation applications with the following benefits:

- Cloud-enabled and virtualized development approaches can reduce dependence on early hardware prototypes.
- Faster, consistent development with VS Code and OCI-compliant containers, enabling portability across development environments, runtimes and dependency-free deployment across local, cloud, and edge environments.
- Pre-integrated software components help teams avoid repeated integration of custom patches and unsupported toolkits.
- Broad protocol, middleware, and open-source support reduce friction when building modern industrial applications.
- Professional services, training, and consulting can help teams with BSPs, migration, hypervisor design, safety cases, and cybersecurity practices.

QNX Support & Professional Services

Proven Experience

Multiple decades of collective expertise designing, integrating, and supporting complex embedded systems.

Service Excellence

A proven track record of supporting OEM programs to critical production milestones.

Global Footprint

Shared knowledge across experienced teams located in NA, EMEA, and APAC.

Commitment

Dedicated experts who can work as an extension of your team.

QNX Professional Services Expertise

Hardware

Prototyping, board support packages, driver development/customization, system optimization, fast boot, hypervisor support.

Porting & Integration

Linux/Android hypervisor guests, middleware integration, open-source porting/integration, legacy OS migration.

Security & Safety

Security & safety guidance spanning functional safety services, safety cases, hazard and risk analysis, penetration testing, security best practices, and security & safety training.

Middleware Enablement

Graphics pipelines and implementation, protocol development, middleware design and development, architectural stack review, system profiling and optimization.

Training

Hands-on training, online or in-person, using real-world examples to equip your team with essential QNX skills.

Consulting

Early & ongoing engagement - architectural reviews, on-site consulting (short & long term), cloud architecture integration, expert guidance, and service retainers.

Let us enable your teams — talk to a QNX expert about your project needs →

August 2026

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 defence. Founded in 1980, QNX is headquartered in Ottawa, Canada.

Learn more at qnx.com →