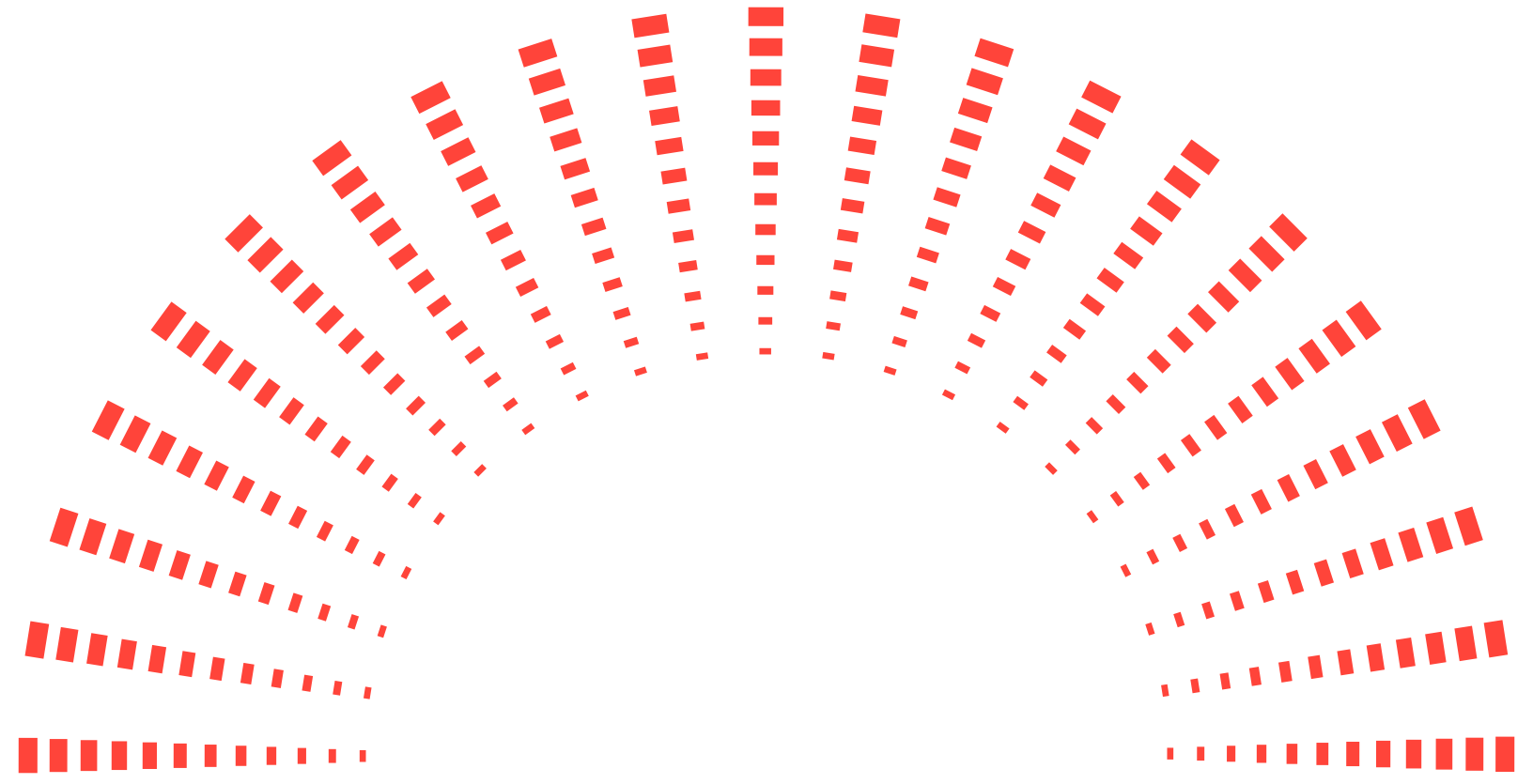
QNX

Solution Guide

Powering the Future of Software-Defined Defense



Redefining Defense Through A Software-First Strategy

Defense strategy is being reshaped by software-defined applications. Software has become the unifying foundation for operational capability and adaptability across complex, multi-system environments. This shift represents a foundational change in how mission systems are designed, deployed, and sustained.

Defense agencies are increasingly moving away from bespoke, hardware-bound platforms and toward flexible, software-driven architectures. At the core of this transformation is a growing reliance on commercial-first software platforms that accelerate deployment, reduce costs, enable interoperability, and support continuous innovation.

Key forces driving this shift include:

- The modernization of legacy systems into modular, software-centric architectures.
- The need for long-life, secure software that performs reliably in harsh and contested environments.
- The push for interoperability and upgradability across multi-domain operations.

This transformation is not just technical, it is organizational. Defense agencies are demanding faster innovation cycles, greater system interoperability, and more agile procurement models. The burden of delivering on these expectations falls largely on defense manufacturers and system integrators.

The Complexity Defense Manufacturers Must Navigate

The transition to software-defined defense is reshaping platforms, placing new operational, technical, and commercial demands on manufacturers and integrators. While agencies set the direction, it is industry that must deliver modular, interoperable, and continuously upgradable systems—often within legacy constraints.

Procurement & Integration Realities

Defense programs increasingly favor commercial-first software to reduce costs and accelerate deployment. This shift, however, introduces nuances that manufacturers must manage:

- **License Transferability**
  Software licenses often need to move from contractors to government end-customers, requiring flexible models that maintain compliance and control.

- **Modularity & Interoperability**
  Platforms must support open standards and API-driven architectures to enable multi-vendor integration and system-of-systems operation across domains.

Technical Barriers to Modernization

Manufacturers face several entrenched challenges as they evolve mission systems:

- **Modernizing Legacy Systems**
  Decades-old, hardware-bound platforms must be decoupled and rebuilt around modular, reusable software while maintaining backward compatibility.

- **Sustaining Secure, Long-Life Software**
  Mission-critical systems must remain secure and reliable for decades in harsh environments, supporting offline updates, managing obsolescence, and countering evolving threats.

- **Enabling Multi-Domain Interoperability**
  Joint operations demand real-time data sharing and coordination across diverse operational domains—requiring a common OS foundation.

- **Accelerating Capability Deployment**
  New features must be deployed quickly without compromising security or mission assurance, favoring proven commercial platforms with continuous update support.

- **Balancing Innovation with Certification**
  Safety and security certifications remain essential but slow technical progress. Pre-certified components and ready-made artifacts help teams innovate without increasing compliance risk.

QNX as an Agent of Change for Defense Manufacturers

Defense manufacturers are being asked to do more than deliver platforms, they are being asked to lead transformation. As defense agencies shift toward software-defined applications and commercial-first architectures, manufacturers must modernize legacy systems, integrate complex technologies, and meet evolving safety and security requirements, all while accelerating time-to-field.

QNX Enables Manufacturers to Rise to This Challenge

By providing a secure, modular, and certifiable software foundation, QNX equips manufacturers to build platforms that are not only compliant and resilient, but also agile enough to adapt to changing mission needs. This positions them not just as suppliers, but as strategic partners in defense innovation.

How QNX Enables Manufacturers to Lead

Accelerating Modernization
QNX supports the transition from hardware-bound systems to modular, software-driven platforms. Its architecture simplifies integration and enables scalable upgrades.

Reducing Certification Burden
With pre-certified components and safety artifacts aligned to IEC 61508 SIL 3, and ISO 26262 ASIL D, QNX helps manufacturers streamline compliance and reduce risk.

Supporting Multi-Domain Interoperability
QNX's support for open standards and modular frameworks allows manufacturers to build platforms that interoperate across diverse operational domains.

Delivering Long-Term Reliability
QNX has been around for over 45 years and is built not only for the long-haul but for harsh, contested environments. Its fault-tolerant microkernel architecture supports secure offline updates and protects against evolving cyber threats.

Enabling Agile Deployment
Real-time performance, secure OTA capabilities, and containerized workload support allow manufacturers to deploy new capabilities quickly and safely.

Simplifying System Consolidation
QNX Hypervisor enables safe co-hosting of multiple OS environments on a single SoC, allowing manufacturers to consolidate legacy systems while preserving real-time guarantees.

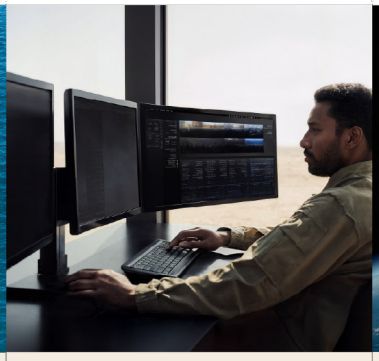
Why Defense Manufacturers Choose QNX

As a Canadian company, QNX benefits from neutrality and broad international acceptance, especially in multinational defense collaborations. Backed by BlackBerry, a globally recognized brand trusted for secure communications by NATO and 17 of the G20 governments, QNX opens doors with a legacy of security, reliability, and ubiquity.

QNX brings a uniquely transferable pedigree from the automotive Software-Defined Vehicle domain into defense. The same technologies that enable centralized compute, mixed-criticality separation, and real-time coordination of sensors, in modern vehicles directly map to the needs of defense ground platforms and unmanned systems. By relying on a foundation already proven, hardened, and safety-certified at global scale, defense programs can modernize faster with a mature, reliable, and future-ready software architecture.

In defense programs where both operational failure and cyber compromise carry mission-critical consequences, QNX stands apart with a dual capability in certified safety and defense-grade security, trusted across ground vehicles, weapons systems, unmanned platforms, C4I systems, ISR capabilities, and space-based technologies.

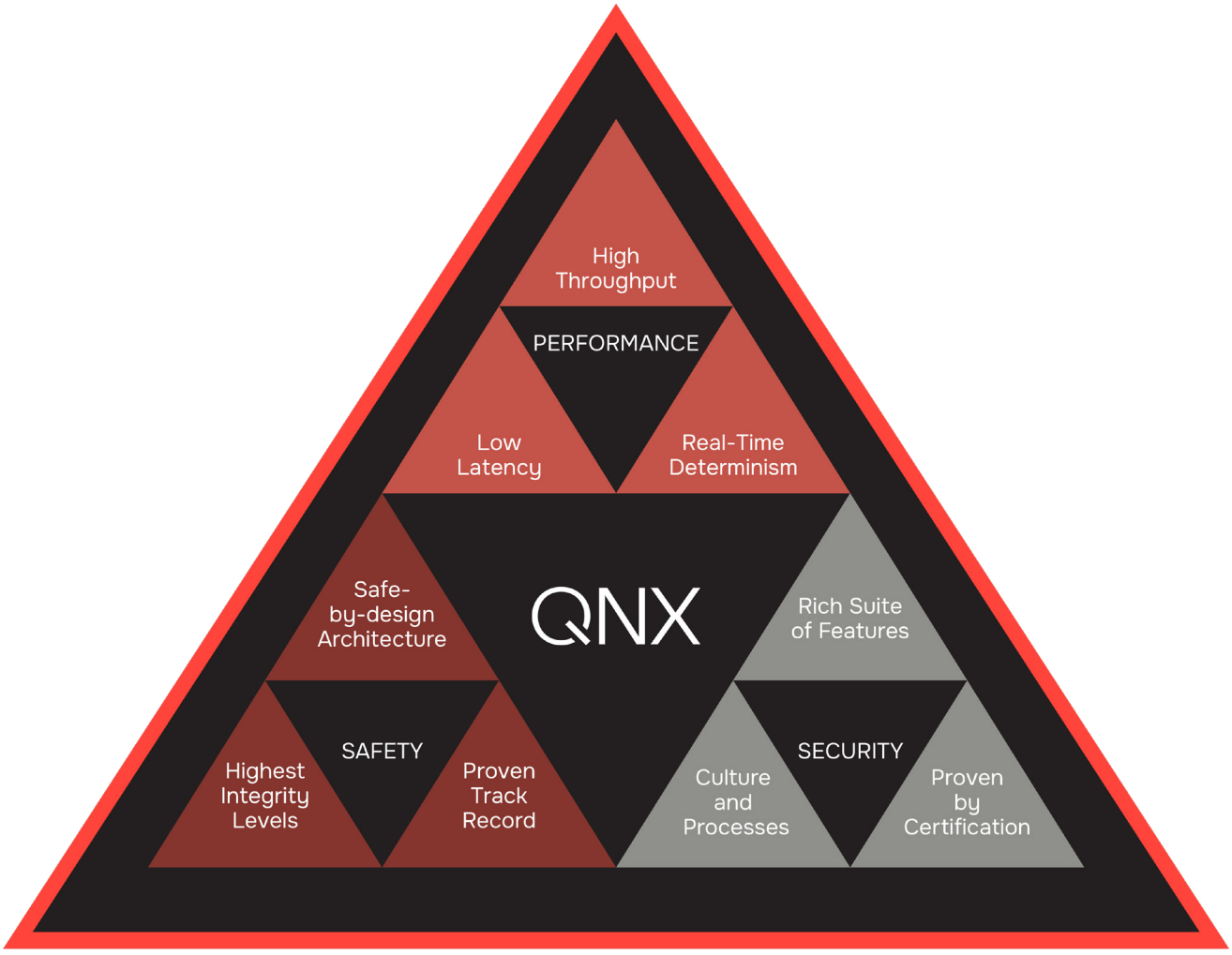
QNX Capabilities Across Defense Subsegments

Ground Vehicles	Unmanned Vehicles	Weapons Systems & Munitions	Advanced Space Capabilities
			
Defense ground vehicles require modular, fault-tolerant software platforms that support mixed-criticality workloads, secure communications, and autonomous operations. QNX enables real-time sensor fusion, precise control, and scalable software-defined architectures that enhance mission flexibility and safety.	Autonomous platforms require hard real-time control, low latency, and secure data handling to operate safely and effectively. QNX ensures precise maneuvering, sensor responsiveness, and reliable mission execution.	Weapons platforms rely on deterministic performance for guidance, targeting, and launch control. QNX delivers fault-tolerant microkernel architecture, secure boot, and runtime integrity to ensure precision and resilience under combat conditions.	Space-based ISR systems require secure communications and SWaP-optimized software. QNX supports encrypted data transmission, real-time decision-making, and long-life reliability in harsh, remote environments.
• Modular mission architectures, allowing diverse subsystems such as navigation, communication, sensing, and targeting to coexist safely in a single consolidated compute environment	• Hard real-time responsiveness, minimizing latency and jitter for ground, surface, or marine control loops.	• Real-time execution for guidance and targeting, ensuring loops run at predictable intervals for high-accuracy control.	• Optimized for low SWaP, delivering predictable real-time performance with a minimal footprint for satellites, payload controllers, and spaceborne processors.
• QNX's automotive SDV technologies can be adapted to defense ground vehicles, enabling scalable, mission-configurable software environments with enhanced safety and maintainability.	• Supports high -throughput sensor workloads by providing the deterministic, fault-tolerant foundation autonomy and perception software rely on for real-time decision making.	• Microkernel-based fault tolerance, preventing localized failures from propagating into mission-critical behaviors.	• Supported within NASA's Core Flight System (cFS), where QNX SDP 8.0 is an officially supported OS, enabling reusable, modular flight software across numerous NASA missions.

Trusted Foundation

In defense, safety, security, and performance are not optional, they are foundational. QNX delivers all three through a microkernel architecture, rigorous certification, and real-time determinism. Our platform is engineered to meet the demands of mission-critical operations across domains.

QNX's safe-by-design architecture ensures fault containment, low latency, and high throughput. Our security culture includes continuous vulnerability monitoring and ISO 21434 alignment. Defense customers choose QNX because it delivers predictable, resilient performance where failure is not an option.



Safety as a Strategic Imperative

In defense, safety is not a feature. It is a foundational requirement. Mission-critical systems must operate predictably and securely for decades in harsh and contested environments. QNX delivers a safe-by-design microkernel architecture supported by rigorous certifications and decades of proven reliability.

Certified for Mission Assurance

QNX provides a low-risk path to mission assurance with pre-certified components, safety documentation, and expert support. Defense programs benefit from:

- **QNX OS for Safety and QNX Hypervisor for Safety**
  Certified by TÜV Rheinland to:
  - IEC 61508 SIL 3
  - ISO 26262 ASIL D

- **Safety-Qualified Toolchains**
  C/C++ toolchains qualified to IEC 61508 and ISO 26262 standards.

- **Safety Artifacts**
  Comprehensive safety manuals, traceability reports, and certification-ready templates that reduce audit preparation effort.

- **Expert Assistance**
  Hands-on support from safety engineers through workshops, design reviews, and process consulting.

Engineered for Reliability

QNX's microkernel architecture ensures fault containment and real-time determinism:

- **Priority-based Scheduling**
  Guarantees timely execution of mission-critical tasks.

- **Fault Recovery by Design**
  Isolated drivers and services prevent system-wide failures. Failed components restart without rebooting.

- **Heartbeat Monitoring**
  Automatically detects and manages crashes or hangs to maintain uptime.

- **Rootless Architecture**
  Enforces strict access policies, minimizing attack surface and preventing privilege escalation.

Accelerating Certification Without Slowing Innovation

Defense programs often face long certification cycles. QNX shortens this path with:

- Pre-certified software components
- Standards-based APIs (POSIX-compliant)
- Modular architecture for mixed-criticality systems

QNX enables defense manufacturers to modernize faster, reduce certification risk, and deliver platforms that meet the highest safety standards without compromising agility.

Defense-Grade Security

Modern defense platforms operate in contested, intelligence-rich environments where cyber compromise is as damaging as kinetic failure. QNX delivers a security-first architecture that protects mission systems from the ground up, combining microkernel isolation, multi-layered defenses, and the legacy of BlackBerry's globally trusted security technology.

QNX is strengthened by BlackBerry's long-standing role securing classified communications and national infrastructure. BlackBerry technology is trusted by NATO and 17 of the G20 governments, bringing a proven security lineage into embedded mission systems. This heritage reinforces QNX as a credible, high-assurance foundation for defense platforms.

Secure-by-Design Architecture

The QNX microkernel architecture minimizes attack surface by running only essential components in kernel space. All other services operate in isolated user-space processes, providing inherent fault containment and ensuring that faults or malicious activity cannot spread to mission-critical logic. Rootless operation, strict privilege boundaries, and strong memory protection further reduce the risk of escalation or lateral movement inside the system.

Multi-Layered Defense and Hardening

QNX incorporates multiple layers of built-in hardening to defend against modern threats. Secure and trusted boot establish a hardware-anchored chain of trust. Encrypted filesystems and trusted storage safeguard mission data. Runtime protections help maintain system integrity during operation and granular access control ensures that only authorized components interact with critical services.

Secure Connectivity and Cyber-Resilient Sustainment

QNX supports secure, authenticated communication and resilient sustainment workflows across connected, hybrid, and disconnected environments. Its software update and provisioning infrastructure can be deployed on-premises or in sovereign clouds, allowing safe updates even for systems operating in air-gapped or forward-deployed conditions. BlackBerry cryptographic technology provides a trusted foundation for key management, code signing, and device identity across fleets.

Cybersecure by Design

Security is embedded in QNX's engineering culture. Continuous vulnerability monitoring, secure development processes, and deterministic system behavior make QNX suitable for defending mission-critical systems against sophisticated threats. When paired with the QNX Hypervisor, mixed-criticality workloads operate with strict separation, allowing untrusted applications, mission logic, and safety-critical control to coexist without risk of interference.

Interoperability Across Defense Domains

Modern defense programs require software that can integrate seamlessly across platforms, mission systems, and suppliers. As agencies increasingly mandate modular open architectures, interoperability has become foundational to mission readiness. QNX delivers this through decades of experience enabling portable, standards-aligned, and mixed-criticality systems across aerospace, automotive, industrial, and defense platforms.

A Proven Foundation for Portability

QNX is built on a POSIX-compliant architecture that supports portable, standards-based software development. This enables developers to maintain consistent application behavior across different hardware configurations and mission environments without restructuring core logic. QNX's long history with POSIX-

aligned systems has made it a trusted foundation in programs that require open interfaces and predictable integration across vendors.

Interoperability Rooted in Microkernel Architecture

The QNX microkernel architecture was designed for modularity, clean separation of components, and predictable interactions. By running drivers, services, and non-critical components outside the kernel, integrators can add or update mission applications, autonomy modules, sensor pipelines, and legacy components independently while preserving strict freedom from interference. This reduces integration risk and simplifies the evolution of complex, multi-supplier systems.

FACE Conformance for Reuse Across Programs

QNX has achieved conformance to the Future Airborne Capability Environment (FACE) Technical Standard. FACE conformance allows QNX-based software components to be reused across airborne and defense programs, supports modular and multi-vendor integration, and aligns with government initiatives aimed at reducing cost and preventing supplier lock-in. It also provides a validated, standards-aligned path for building scalable mission-system architectures.

Although originally developed for military airborne systems, the FACE Technical Standard has expanded into commercial as well as military ground vehicles, enabling a common, modular open-systems approach across air and ground domains.

Interoperability Accelerated Through QNX Everywhere

QNX Everywhere strengthens this interoperability advantage by giving defense labs and engineering teams free, non-commercial access to QNX Software Development Platform (SDP) 8.0 for prototyping. This enables developers to quickly experiment, validate designs, and build early mission concepts on accessible hardware using the same deterministic behavior they will rely on in production.

Through QNX Everywhere, teams can:

- Rapidly prototype mission and autonomy applications
- Explore mixed-criticality architectures early
- Onboard new developers quickly
- Transition prototypes into production with minimal rework

This shortens early-stage development and helps ensure that prototypes, once validated, can be integrated cleanly into certified, mission-ready platforms.

Reduced Integration Burden for Defense Manufacturers

With POSIX-aligned APIs, microkernel separation, FACE conformance, and rapid prototyping through QNX Everywhere, QNX helps defense organizations:

- Integrate multi-vendor components more reliably
- Modernize legacy systems without breaking established interfaces
- Design mixed-criticality architectures with predictable behavior
- Reuse software across programs and mission profiles
- Align naturally with MOSA and SOSA principles

QNX's interoperability pedigree, forged over decades of real-world mission system deployments, provides defense programs with a mature and future-ready foundation for software-defined capabilities.

Products

QNX's full-stack offering includes OS services, communication frameworks, virtualization, and safety-qualified toolchains. Defense developers gain access to a robust, maintainable embedded stack that supports real-time performance, secure partitioning, and modular development of mission-critical systems.

QNX GEDP

QNX General Embedded Development Platform (GEDP) is a pre-integrated embedded platform designed to accelerate development of mission-critical systems. It delivers secure virtualization, modular tooling, and real-time performance to support ground vehicles, unmanned platforms, weapons systems, C4I infrastructure, ISR capabilities, and space-based technologies.

Safety-Certified

QNX GEDP integrates **QNX OS for Safety** and **QNX Hypervisor** to support high-assurance systems. Certified to ISO 26262 ASIL D and IEC 61508 SIL 3, it provides deterministic performance, fault isolation, and secure partitioning for mixed-criticality workloads.

QNX Cabin

QNX Cabin is a portable, pre-integrated cockpit software framework that accelerates the development of mission-ready interfaces for defense vehicles. It supports real-time graphics, sensor fusion, and secure communications, enabling intuitive, situationally aware operator environments.

QNX Containers

QNX Containers deliver secure, modular deployment of defense software. Built on the QNX microkernel, they ensure real-time performance, isolation, and cybersecurity. Ideal for mixed-criticality systems, they consolidate trusted and untrusted workloads on one platform.

April 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 defense. Founded in 1980, QNX is headquartered in Ottawa, Canada.

Learn more at qnx.com →