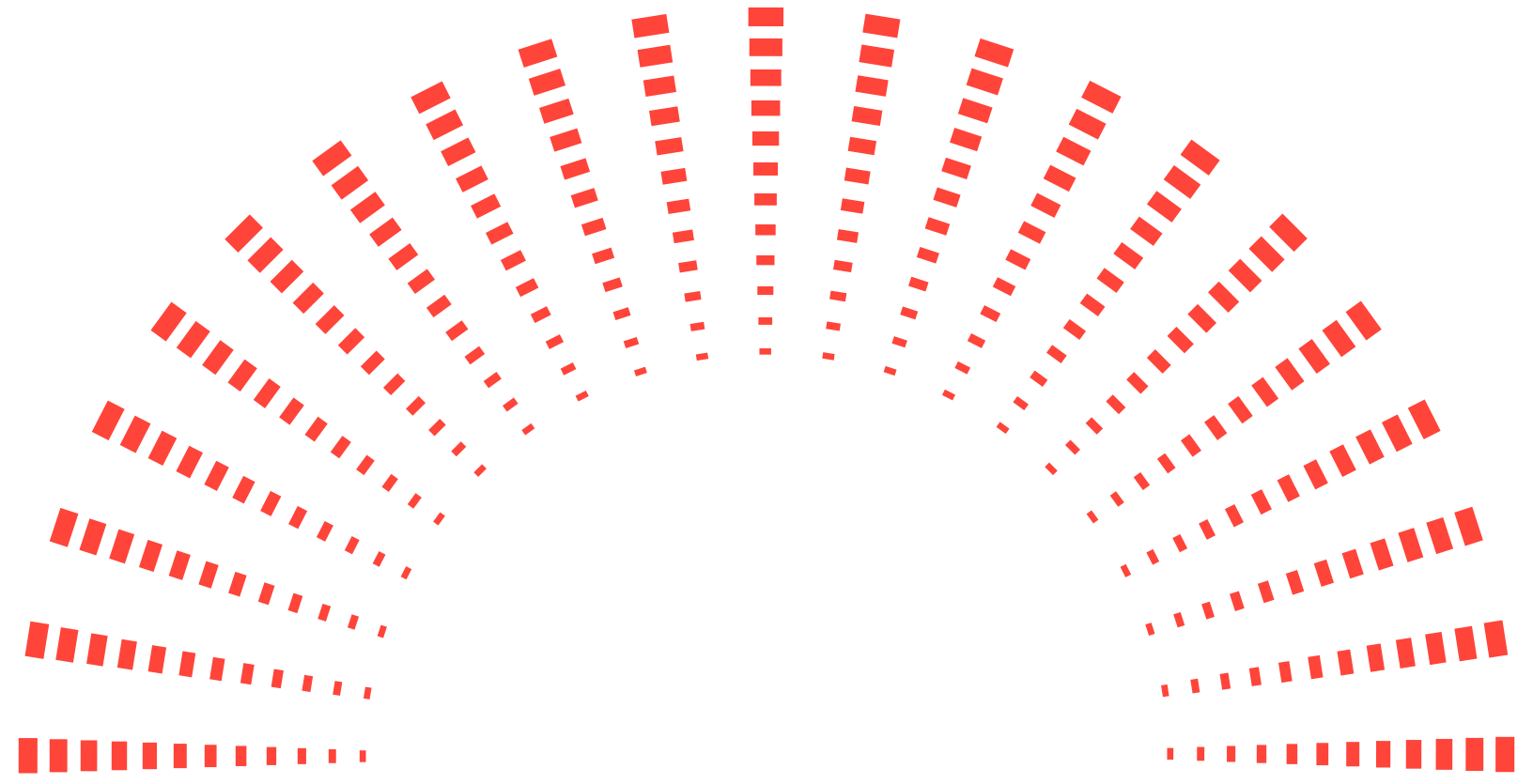
QNX

Solution Guide

Robotics

Foundational Software Solutions



How QNX is Transforming the Robotics Industry

96%
Of critical Linux exploits would not reach critical severity in a microkernel-based system

57%
Would be reduced to low severity

100%
Success rate in meeting SOP deadlines across 300+ programs

The Future Is Robotics

Industrial robots have the potential to liberate skilled workers to focus on more complex tasks—Mega Online, “Rise of the Cobots.”

To provide an idea of the scale of replacement of human labor, analysts estimate that by 2040, the U.S. may have 8 million working humanoid robots, potentially impacting wages by $357 billion USD. By 2050, this number could rise to 63 million, affecting approximately 75 percent of occupations and $3 trillion USD in payroll—Morgan Stanley.

Combining advanced robotics with other technologies, process enhancements, and structural layout changes can yield savings of up to 40 percent—Boston Consulting Group, “Advanced Robotics in the Factory of the Future.”

By using off-the-shelf components where possible to complement parts designed in-house, Odense firms can quickly assemble industrial robots with specialist applications and put together complete, working systems that meet clients’ needs—Mega Online, “Rise of the Cobots.”

Currently, it is estimated that 10 percent of manufacturing tasks are performed by robots —Trendsformative, “Industrial Robots: The Start of a Megatrend.” But the global warehouse robotics market is projected to expand from $17.59 billion USD in 2025 to $55.74 billion USD by 2033. This growth is driven by increased demand for automation in e-commerce, manufacturing, and logistics—Straits Research.

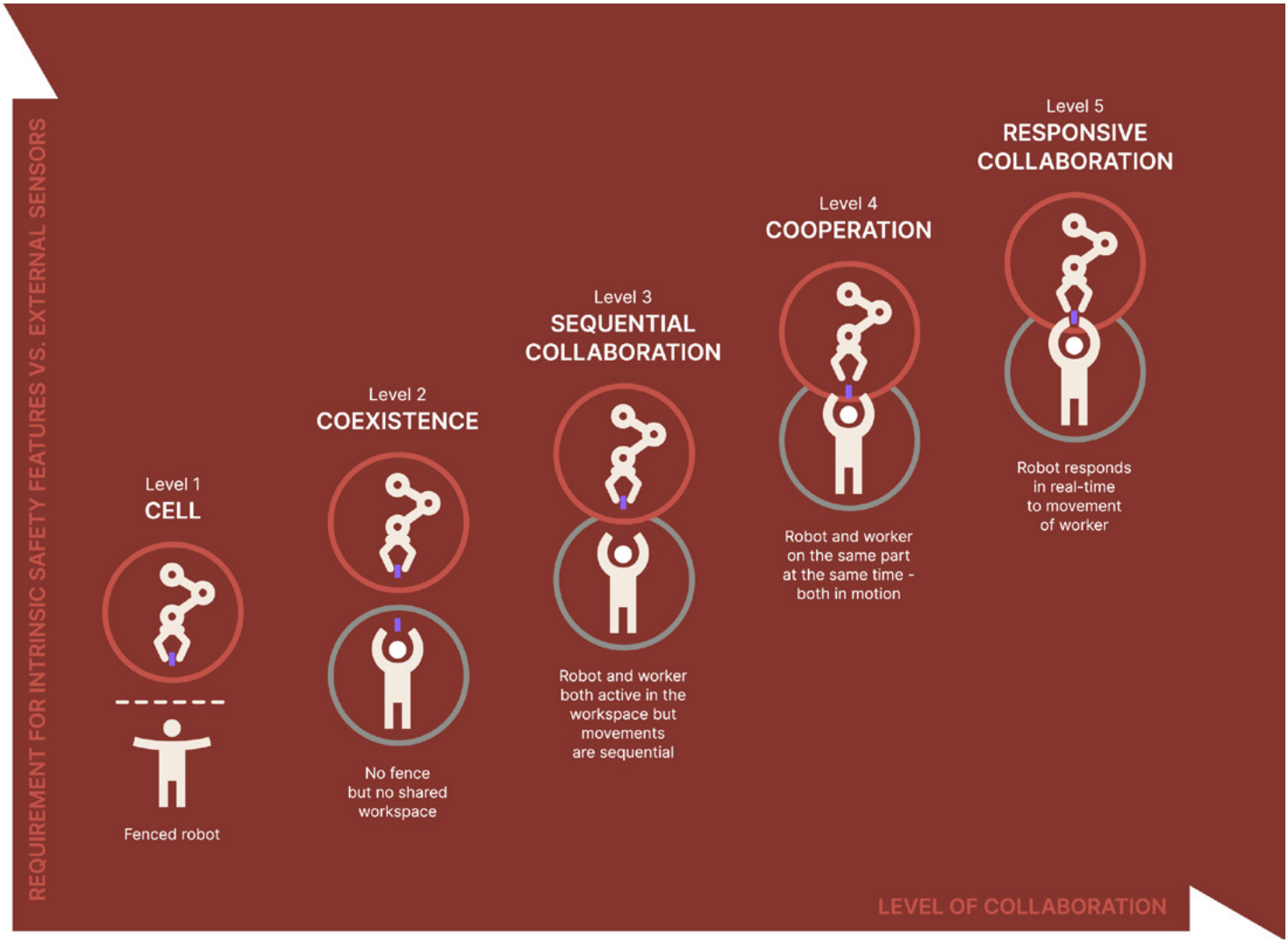
The robotics market is thriving, driven by technological advancements and widespread adoptions across a range of sectors. Studies indicated that the adoption of industrial robots has contributed to an annual GDP growth of approximately 0.36 percent across 17 countries, enhancing labor productivity and operational efficiency—Astute Analytica.

Industry Trends and Challenges

Robotics includes everything from ultra-high precision medical devices to gantries in factories and warehouses, autonomous home vacuum cleaners, and beyond. Thanks to advances in embedded hardware and software, there are few domains where robotics systems aren't already essential, and new possibilities are constantly emerging. It is no wonder, then, that investments in new robotics companies continue to grow, and that in many mature industries robotics present ideal new cost-saving and revenue opportunities.

Despite the vast differences in the environments where they are used and the tasks they carry out, robotics systems share a great deal in common, and require much of the same characteristics and behavior in their foundational software.

Types of Collaboration With Industrial Robots



Source: IRF, based on Bauer et al. (2016) **mega.online/en/articles/collaborative-robots-market-expansion**

Whether they are in your corner diner working cooperatively with the staff to prepare food then deliver it to patrons at their tables, or scouring the ocean floor counting manganese nodules, robotics systems need:

Reliability

The OS and hypervisor must perform as specified, without failures, for as long as required without a restart, be that a few hours or a few decades.

Performance

The OS and hypervisor must consistently provide specified performance and, especially, ensure that critical tasks run and complete deterministically.

Secure Connectivity

System connectivity should be robust, versatile and secure, making available the best communications channels for diverse operating environments.

Safety Certification

Both software and hardware should be certified to functional safety standards to mitigate risks of systematic and random faults that could result in accidents.

Diverse Systems and Mixed-Criticality

The foundational software often must support running safety-critical and non-safety components on the same system-on-a-chip (SoC).

Comprehensive Cybersecurity

A system is only as safe as it is secure; the foundational software must ensure protection from malicious interference.

Development and Maintenance

Development tools must be familiar and standards-based so you can focus on value add.

System Longevity

Hardware upgrades must not render legacy code obsolete, and software upgrades must be simple to perform and bring minimal risk.

Why Choose QNX

QNX provides manufacturers of robotics systems with a complete software foundation on which to develop their technologies and expand their businesses. Our microkernel real-time operating system (RTOS) architecture has a 45-year track record in critical embedded devices and systems as varied as proton therapy systems (PTS), autonomous forklifts and solar-powered aircraft.

QNX foundational software is standards-based and offers common development tools to address the needs of engineering teams developing both safety-critical and non-safety systems. QNX® OS 8.0 and the QNX® Hypervisor are complemented by their safety variants: the QNX® OS for Safety and the QNX Hypervisor for Safety, which are certified IEC 61508 SIL 3.

Whether it's for consumer-grade autonomous vacuum cleaners, surgical assistant cobots or autonomous camera drones, QNX provides the foundational software that lets your teams focus their time and talents on developing value-add systems and components. Plus, our professional services teams offer their decades of experience to see your robotics software systems through from design to market, and help you maintain them throughout their operational life.

Safety-Certified OS

The QNX OS for Safety is certified by TÜV Rheinland to IEC 61508 SIL 3, ISO 26262:2018 ASIL D and IEC 62304 Class C.

Safety-Certified Hypervisor

The QNX Hypervisor for Safety is certified by TÜV Rheinland to IEC 61508 SIL 3 and ISO 26262:2018 ASIL D.

Certify Your Code, Not Your Toolchains

Our C and C++ toolchains are qualified to IEC 61508-3:2010 SIL 3: TCL3 and T3 and ISO 26262-8:2018 ASIL D: TCL3 and T3.

Easily Port From Linux

Our APIs are POSIX-compliant and our tools are standards-based so you can easily port from Linux® to the QNX® OS for Safety.

Deliver Real-Time Reliability and Performance

Support for compute-intensive and time-critical operations for critical systems.

Whether it's controlling an autonomous underwater vehicle (AUV) or a robot waiter, the OS powering a robotics system must meet its designed criteria for dependability—it must be available to perform tasks when needed, and it must perform these tasks within the specified time.

The QNX OS 8.0 is designed specifically to meet these demands. Its priority-based scheduling and adaptive time-partitioning ensure that critical tasks run and complete when required. With its microkernel architecture, the QNX OS 8.0 isolates every application, driver, protocol stack and filesystem in its own address spaces outside the kernel. This means that a failed component won't take down other components or the kernel; it can be restarted immediately, with minimal impact on system performance, providing a high-performing and robust foundation for the most demanding robotics systems.

Streamline Safety Certification

A clear, low-risk and limited-cost path for certifications to functional safety standards such as IEC 61508.

Certifying a system to standards such as IEC 61508 is a time-consuming and costly undertaking requiring highly specialized knowledge and skills. Certified to IEC 61508 SIL 3 by TÜV Rheinland, the QNX OS for Safety and QNX Hypervisor for Safety provide foundations that can significantly reduce the scope, risk, length and cost of your certification processes.

Our safety experts can provide training and hands-on workshops designed specifically for your key people developing functionally safe embedded systems. We can help you foster the safety culture you need to continue delivering functionally safe systems and, of course, we can help you design, deliver and maintain the best safety solutions from your product's development through to the end of its operational life.

Manage Diverse, Mixed-Criticality Systems

A simple, low-cost consolidation strategy for systems with different safety and reliability requirements.

Driven by the need to cap initial bills of materials (BOM) as well as hardware weight, power consumption and thermal footprints, many embedded systems requirements call for consolidation of multiple systems onto a single system-on-a-chip (SoC). Often, these systems have differing reliability or safety requirements, and some may even be legacy systems running on diverse OSs.

The QNX Hypervisor leverages the latest ARMv8 and x86-64 hardware virtualization extensions to enable developers to integrate diverse operating systems (e.g., QNX, Linux, Android™) and mixed-criticality components and applications onto a single SoC, while maintaining performance, and enforcing clear separation and isolation between systems to guarantee freedom from interference for safety-critical systems.

Board Support Packages

QNX® Board Support Packages (BSPs) provide an abstraction layer of hardware-specific software that facilitates the implementation of the QNX OS 8.0 on your board. Our extensive BSP library includes BSPs for SoCs manufactured by leading hardware manufacturers. In addition, our professional services can develop customized solutions for you and support your safety and security requirements.

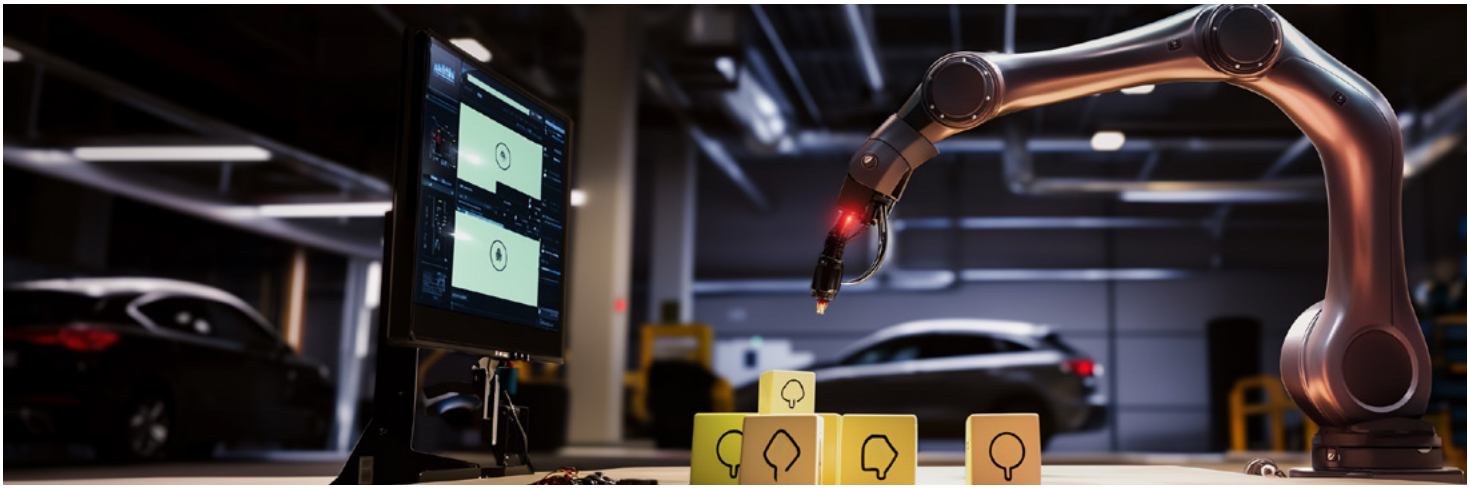
Learn more about our library of BSPs →

Strengthen Cybersecurity

Current and configurable security policies that ensure system integrity.

Isolated systems belong to the past. Robotics systems are now connected, at least some of the time, and hence vulnerable to cybersecurity breaches that can put operators, materials and infrastructure, and the public at risk. Building and maintaining a secure robotics system requires—at a minimum—a reliable and secure OS, and a secure supply chain. Connected systems also require managed public key infrastructure (PKI) authentication, and FIPS (Federal Information Processing Standards)-certified encryption.

The QNX OS 8.0 reduces the surface open to cyberattacks by running all services outside the kernel space, and provides multi-layered protection with layered security policies: granular control of system privilege levels, encrypted and self-verifying filesystems implementing AES 256 encryption and lockable encryption domains, secure logging of system activities, heap, stack and memory protection, and secure boot implementing TPM and TrustZone.



Support Secure Connectivity

Few robotics systems still operate entirely unconnected from the rest of the world. Whether it's receiving orders for meals it will deliver, uploading vending machine data, sharing its location with its peers distributed across the oceans, or uploading sensor data for predictive maintenance analysis, a robotics system today relies on dependable and secure communications channels.

The QNX OS 8.0 offers a full network stack suitable for communication at whatever network level is most appropriate to your implementation–everything from real-time video feeds to software updates.

Facilitate Development

A foundation and tools that facilitate development and ensure you meet your deadlines.

Both QNX® Software Development Platform (SDP) 7.1 and 8.0 are POSIX-compliant, support validation with the PSE 54 test suite, look and feel like Linux, and use the familiar Eclipse development environment, including the GNU compiler collection. They also include C and C++ toolchains qualified to IEC 61508-3:2010 SIL 3: TCL3 and T3, so you can spend your time developing and certifying your code, not your toolchains.

Support System Longevity

A simple, maintainable mechanism for porting legacy code and prototypes, and for implementing upgrades.

The QNX OS 8.0 microkernel architecture makes it easy to quickly add new drivers, confident that a driver failure won't mean a system failure. This reduces the risks to the software system when introducing drivers for new hardware.

With the QNX Hypervisor and its safety variant, the QNX Hypervisor for Safety, you can contain entire systems with their OSs as guests in hypervisor virtual machines. This means that you can port legacy code built on different OSs (e.g., Android, Linux) onto new SoCs and run them concurrently with your latest product. You can also implement new features or upgrade entire systems in virtual machines, confident that the new code won't affect other systems, including safety-critical systems, running on the SoC.

QNX Support & Services

Proven Experience

Thousands of person-years in development, support and integration.

Service Excellence

100% success at meeting OEM start of production (SOP) deadlines.

Global Footprint

Regional experienced teams in US, EMEA and APAC.

Commitment

Dedicated, dependable and trusted staff.

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.

Safety & Security

Functional safety services, safety cases, hazard and risk analysis, penetration testing, security best practices, safety and security training.

Application

UI/UX design/development, application development, protocol development, middleware design and development, application stack design, application profiling and optimization.

Training

QNX offers hands-on, instructor-led training, online or in-person, using real-world examples to equip development teams with essential skills.

Consulting

Architectural reviews, on-site consulting (long/short term), cloud architecture integration, expert consultation, service retainers.

Learn more about our professional services and service packages →

Foundation Products/Initiatives

QNX Software Development Platform 8.0

QNX® Software Development Platform (SDP) 8.0 is the foundational development platform for the next generation of mission and safety-critical systems merging unprecedented performance with unparalleled security and reliability—without compromise. It features our next-generation QNX Operating System built on a future-ready architecture designed to maximize silicon advancements thanks to our advanced microkernel design.

Learn more →

https://blackberry.qnx.com/en/products/foundation-software/qnx-software-development-platform

QNX Advanced Virtualization Frameworks

Make use of our diverse set of industry-standard, hardware-independent frameworks to enable guest operating systems to share hardware and software services such as graphic displays, acoustic environments, touchscreens, media storage devices, video streams and cameras. The QNX® Advanced Virtualization Frameworks provide extended capabilities to the QNX Hypervisor.

Learn more →

https://blackberry.qnx.com/en/products/foundation-software/qnx-hypervisor/advanced-virtualization-frameworks

QNX Hypervisor

An embedded virtualization solution with a microkernel architecture so multiple OSs (Android, Linux, QNX) can safely operate on the same system-on-a-chip (SoC).

Learn more →

https://blackberry.qnx.com/en/products/foundation-software/qnx-hypervisor

QNX Accelerate

QNX® Accelerate is an initiative that makes cloud-enabled versions of our foundational products available. This reduces embedded software development cycles and improves time-to-market.

Learn more →

https://blackberry.qnx.com/en/products/accelerate

Safety-Certified Products

QNX OS for Safety

Built on the same microkernel architecture as the QNX® OS 8.0, the QNX OS for Safety is pre-certified to ISO 26262 ASIL D and to IEC 61508 SIL 3. Easily port Linux-based prototypes to the QNX Real-Time OS (RTOS) and get all the documentation and support you need for certification.

Learn more →

https://blackberry.qnx.com/en/products/safety-certified/qnx-os-for-safety

QNX Hypervisor for Safety

This real-time microkernel hypervisor provides the reliability and performance of the QNX OS and allows multiple OSs to safely operate in isolation and in parallel on the same system-on-a-chip (SoC). It is the first embedded hypervisor pre-certified to ISO 26262 ASIL D and to IEC 61508 SIL 3.

Learn more →

https://blackberry.qnx.com/en/products/safety-certified/qnx-hypervisor-for-safety

Security Solutions

QNX Cybersecurity

For more than 40 years, QNX has provided safe and secure embedded software solutions for automotive, industrial controls, robotics, medical devices, and other mission-critical applications. QNX cybersecurity is built on a strong culture, product excellence, and an ecosystem that enhances the company's security capabilities.

Learn more →

https://blackberry.qnx.com/en/products/security/qnx-security

Automotive Functions

QNX Cabin

QNX® Cabin is a hardware-portable, pre-integrated digital cockpit software reference implementation that provides a development framework for designing digital cockpit systems. By increasing software portability and supporting cloud-first development, QNX Cabin helps reduce development costs and accelerates time-to-market.

Learn more →

https://blackberry.qnx.com/en/products/automotive/qnx-cabin

QNX Multimedia Suite

The QNX® Multimedia Suite is middleware delivered with the QNX Software Development Platform. It can be implemented as an independent standalone system or fully integrated with other QNX products, including the QNX Platform for ADAS.

Learn more →

https://blackberry.qnx.com/en/products/automotive/multimedia

QNX Platform for ADAS

QNX® Platform for ADAS is a foundation for building ADAS and automated driving applications. The modular, sensor/processor-agnostic framework allows for code to be written once and re-used. Optimized for automotive silicon and compatible with a variety of processing cores.

Learn more →

https://blackberry.qnx.com/en/products/automotive/qnx-adas

QNX Sound

QNX® Sound is a holistic software environment that lets you design the next generation of vehicle audio with a holistic software environment that manages the entire vehicle soundscape.

Learn more →

https://blackberry.qnx.com/en/products/automotive/qnx-sound

August 2025

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 255 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 →