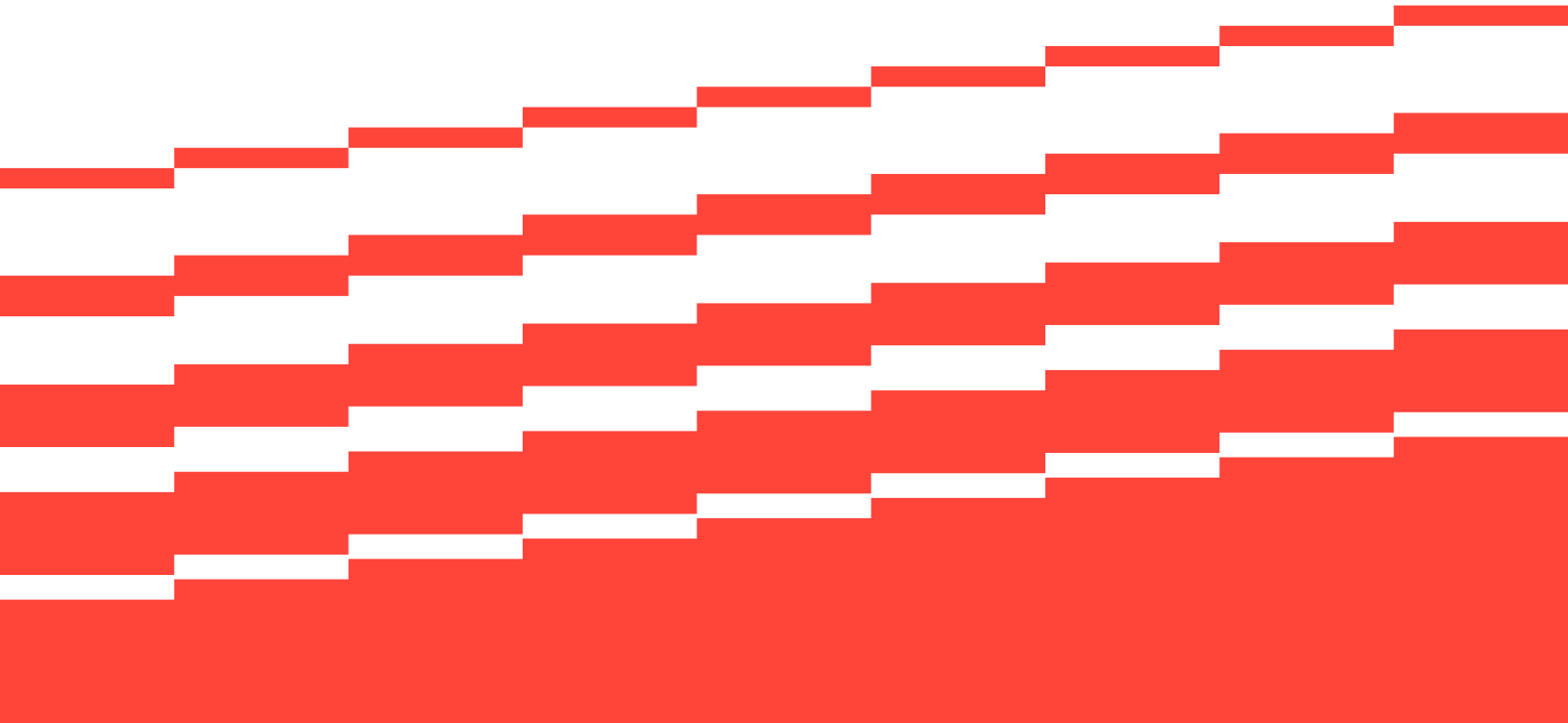
QNX

Product Brief

QNX OS for Safety

Synergizing, Safety, Security, and Performance for the Next Generation of Embedded Systems



QNX OS for Safety

The QNX® OS for Safety is the embedded OS certified to ISO 26262 ASIL D, IEC 61508 SIL 3, IEC 62304 for Class C devices, and ISO/SAE 21434.

Streamline the Development And Certification of Your Safety-Critical Embedded Systems

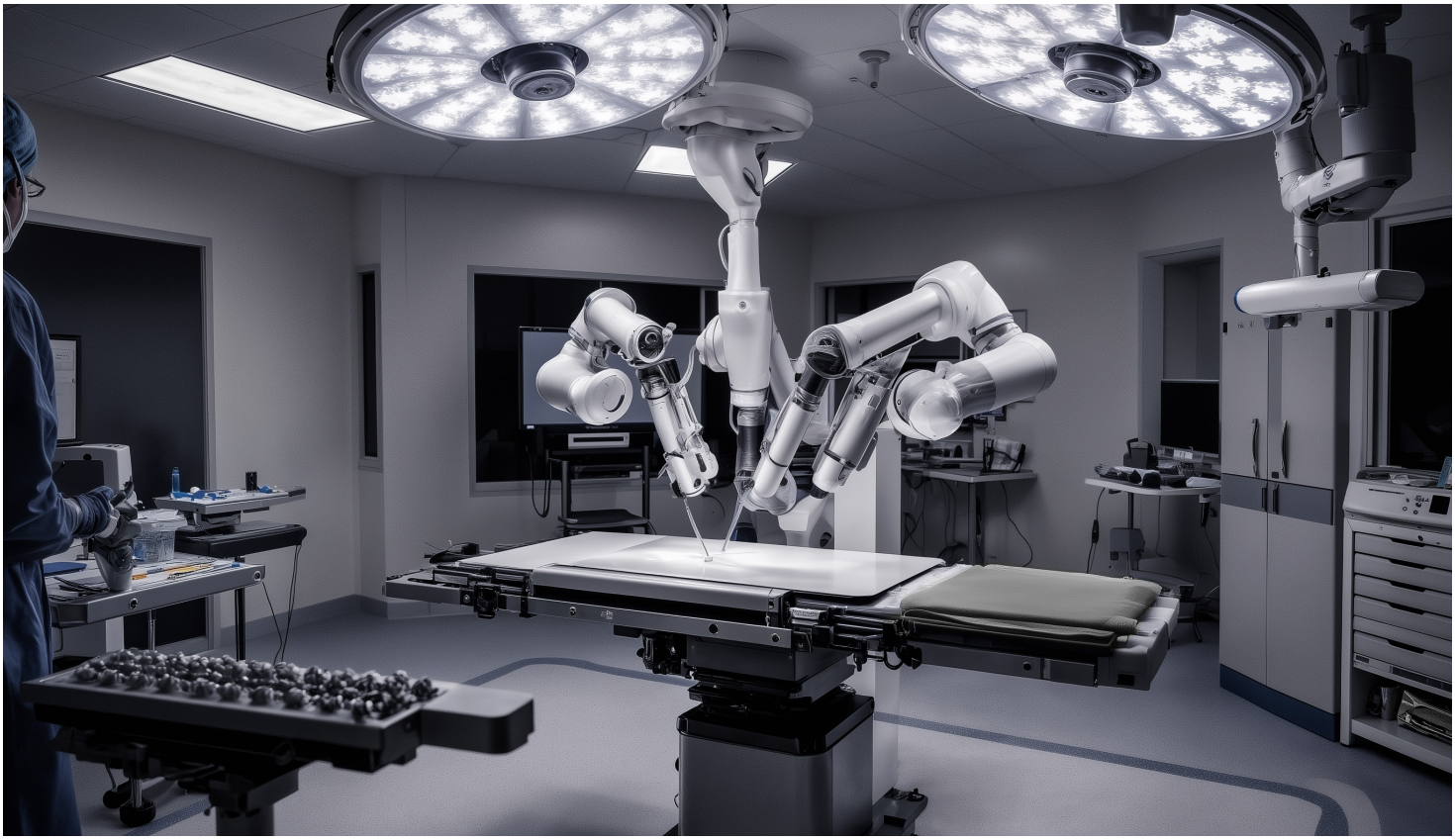
Our certified QNX Operating System for Safety (QOS), based on our high-performance next-generation microkernel, provides the following:

- A fully featured Hard Real-Time OS based QNX Software Development Platform 8.0, certified to ISO 26262 ASIL D, IEC 61508 SIL 3, and IEC 62304 Class C, and ISO/SAE 21434
- C/C++ toolchains qualified to ISO 26262 TCL3 and IEC 61508 TL3
- Key safety artifacts that streamline the development and certification of your safety-critical systems

The QNX OS for Safety is relied upon in various key industries including automotive, medical, industrial controls, aerospace, defense, power generation, robotics, and rail transportation. Built with safety and security by design, the QNX OS for Safety has been relied upon by customers to build safety compliant embedded systems for more than 15 years. QNX also has more than 45+ years of experience in building foundational software platforms where reliability, safety and security is of utmost importance.

Embedded Systems Are Becoming More Complex

Embedded systems are rapidly increasing in power and capability. As a result, these devices are moving away from purely passive roles, becoming increasingly automated and leveraging innovations such as AI inference to identify, process, and actuate their decisions. The correct operation of such devices in key areas where both safe and secure operation is paramount, such as transportation, surgery, and power generation. But when attempting to combine integration of novel features with the fortification of the system, the complexity of the work handed to the manufacturer increases across many axes.



Safety and Security of Embedded Systems is Paramount

To account for the risk of harm to individuals who interact with these devices, a manufacturer must ensure the way the design, develop, and maintain the hardware and software in these systems is appropriate for the context in which it will operate. That knowledge is encapsulated in standards such as ISO 26262, IEC 61508, and IEC 63204, covering the safety requirements of functional areas such as automotive, medical, robotics and industrial automation. In addition to the existing risk of accidental errors introduced during software development, the increasingly interconnected nature of these devices introduces an increasing risk of malicious actors violating the confidentiality, integrity, or availability of their devices. Attacks in any of these key areas can disrupt key functionality responsible for maintaining the safe operation of an embedded device.

Safety and Security Certification is Key in Building Complex Mission-Critical Embedded Applications

Accounting for the synergy of safety and security is crucial for ensuring reliable and trustworthy operation of these devices out in the field such that they can be relied upon. Embedded systems can achieve a robust defense against both unintentional and intentional threats while also leveraging the latest technological innovations to build the most advanced embedded systems in the world. Similar to the safety certifications, structured and disciplined processes for properly accounting for cybersecurity risk in a product lifecycle are accounted for in cybersecurity certifications such as ISO/SAE 21434.

What Is the QOS?

Ideal for building complex and powerful embedded systems, the QNX OS for Safety is a full-featured, real-time Operating System designed for use in every sector where reliability must meet performance to achieve mission success. The QOS is certified by TÜV Rheinland to ISO 26262 ASIL D, IEC 61508 SIL 3, and IEC 62304 Class C, and ISO/SAE 21434. Many key industries including automotive, medical devices, industrial controls, aerospace, defense, power generation, robotics, and rail transportation depend on QOS to build their safety critical applications.

QOS Aligns to SEooC Design

The QOS is a feature-rich, hard real-time operating system that has been designed and developed in a manner complying with safety and security standards. As a Safety Element out of Context (SEooC), the QOS can be integrated into a safety-critical system as a foundational building block to create an end system that needs to be certified within context. Its existing certifications and accompanying documentation ensure the QOS can be leveraged by a manufacturer to meet product requirements without requiring repeated safety analysis of the underlying components. Delivering a device that operates in a safety or security-critical environment means taking full ownership for the behavior of said device out in the field, even if using software and hardware components delivered by a third party. If using such a component, they need evidence the product supports their safety goals. Using QOS means using a product certified to existing standards, which greatly reduces the work required to certify the device within context.

Save Time and Reduce Re-Work on Safety Certification With Hardware-Agnostic Microkernel

The microkernel-based design of the QOS makes it agnostic from the underlying hardware. Manufacturers designing systems on QNX have the flexibility to transition their design into different SOCs or hardware architectures without the need to recompile and recertify the underlying software components provided by the QOS. QOS is also delivered with various built-in mechanisms designed to provide the freedom from interference needed to protect the system from both internal faults and outside threats. Through mechanisms such as a virtual memory manager, QOS provides spatial isolation to ensure software components operate with their own set of resources that do not overlap with each other, In addition, Temporal Isolation ensures software components are allocated specific time slots for execution, QOS's built-in preemptive priority-based scheduler provides systems with the temporal isolation it needs to ensure discrete software components can perform as expected without interfering with each other's timing and performance.

Pre-certified and Ready-To Use Foundational Software

In summary, QOS provides a pre-certified foundational software solution that encapsulates the safety and security within the product itself and provides users of said system a blueprint to employ it to meet safety goals. This provides manufactures with the ability to maximize their resources to developing and certifying the components they know best, with the trust that the foundation software they use to build has been built with the highest levels of safety and security in mind. QOS is built for safety and security from the start. It is developed, verified, and certified using best practices described in safety standards, including static analysis and formal verification techniques.

What's Included

- A fully featured Hard Real-time OS based QNX Software Development Platform 8.0, including:
  - Next-generation microkernel
  - Process manager
  - Memory manager
  - Pathname manager
  - Inter-process communication
- C library
- C++ library (ISO 26262 ASIL D, pending certification to IEC 61508 SIL 3 and IEC 62304 Class C)
- Math Library
- Server monitor
- Security policies
- System logger library
- QNX cryptography library
- SMMU Manager
- Certified Toolchains to streamline development QOS-based applications:
  - Certified GCC-based toolchain, including a compiler, linker, and assembler
  - Suite of utilities including ar, strip, objcopy
  - C++ 17 headers and templates (ASIL B/SIL 1, certifiable to ASIL D/SIL 3)
- Safety Manuals consolidating key guidance on using QOS for safety-critical applications:
  - Presents a set of safety restrictions and recommendations to be abided by to ensure the system can operate safely and within constraints compatible with safety certifications accompanying the QOS.
  - Created with the knowledge distilled through Hazards and Risk Analyses (HARA) of QOS components, ensuring safety is formally accounted as a stakeholder before being used in an end system.
- Security Manual providing guidance for the mitigation of cybersecurity risk:
  - Presents a set of constraints under which the product should operate in a secure QOS-based system, distilled through a Thread Analysis and Risk Analysis (TARA) of the key components of the QOS by cybersecurity experts.
  - Abiding to the restrictions of the security manual allows facilitates the certifications of QOS systems to security standards such as ISO/SAE 21434:2021.

Key Benefits

- Full API-compatibility with QNX SDP 8.0, ensuring seamless migration between QOS 8.0 and QNX OS 8.0-based systems and the ability to leverage the extensive feature-set of QNX SDP 8.0.
- Hardware-agnostic design makes it easy to migrate existing designs across SOCs or Hardware architectures.
- Consolidated guidance on how to design and deploy a QOS-based system in a system that is safe, secure, and compliant with relevant regulations.
- Certified components that can be used as key building blocks in a system, including scheduling, memory isolation, timing, and inter-process communication.

Use Cases

QOS is deployed in wide variety of critical contexts, including but not limited to the following:

- Automotive Cockpit Domain Controllers
- Advanced Driver Assist Systems and Autonomous Driving
- Industrial PLCs, automation and warehouse robotics.
- Medical devices and surgical robotics
- Power generation
- Aerospace and Defense

Related Products

QNX SDP 8.0

QNX Software Development Platform (SDP) 8.0 is the foundational development platform for the next generation of mission, safety- systems—merging unprecedented performance with unparalleled security and reliability—without compromise.

QNX SDP 8.0 features our next-generation QNX Operating System built on a future-ready architecture designed to maximize Silicon advancements thanks to our advanced microkernel design. QNX SDP 8.0 forms the baseline for all future QNX OS and Hypervisor products, enabling compute-intensive platforms like autonomous drive systems or industrial robots across the Internet of Things, with consistent and blazing-fast, real-time performance for today and tomorrow.

QNX Filesystem for Safety

QNX® Filesystem for Safety (QFS) is a POSIX-compliant read-only filesystem certified to ISO 26262 ASIL B. It verifies the integrity of the filesystem contents upon access at runtime, allowing users to detect if corruption has taken place and take the necessary actions to maintain the safety of the system. QFS is an independent filesystem driver that works in conjunction with other read-write filesystems in the system. It is built upon the QNX Trusted Disk security feature and is compatible with Pathtrust and other QNX OS for Safety security features. QFS offers a read-only POSIX Filesystem which is certified to ISO 26262 ASIL B. It supports various encryption algorithms to protect and secure filesystem contents, including SHA-256, while including various configuration options to tailor performance. QFS runs concurrently with other filesystems and is hardware-agnostic.

QNX Hypervisor

QNX® Hypervisor is an embedded virtualization solution with a microkernel architecture that enables multiple operating systems, including Android™, Linux®, and QNX, to safely operate on the same system-on-a-chip (SoC).

Pre-certified by TÜV Rheinland to ISO 26262 ASIL D, IEC 61508 SIL 3 and IEC 62304 Class C, it offers simpler and faster certification of your automotive, industrial, and medical mission-critical systems.

This powerful solution offers virtual memory, CPUs, interrupt controllers, and pass-through, emulated, and para-virtualized devices, providing unparalleled scalability across CPU cores with extremely low jitter. With QNX Hypervisor, designers can share and isolate CPUs and devices (graphics, audio, etc.) between guests and the host without the fear of hitting hypervisor-based bottlenecks.

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.

QNX Safety Consulting

QNX® Safety Services complement and enhance your company's strengths in functional safety for embedded systems. This includes training, consulting and custom safety software development across a range of embedded systems.

QNX Professional Services and Support

QNX offers customized professional services to bring safe and reliable products to market on time, on budget and with excellent quality.

QNX Certifications Scope

Safety QNX Products Certifications	QOS	QHS	QFS
ISO / SAE 21434	✓	✓	In Progress
ISO 26262: ASIL D	✓	✓	In Progress
ISO 26262: ASIL B	✓	✓	✓
IEC 61508: SIL 3	✓	✓	In Progress
IEC 62304: Class C	✓	✓	In Progress

Start Right Now

Learn more about the QOS, based on our latest major release of our Software Development Platform, QNX SDP 8.0:

QNX SDP 8.0 QuickStart Guide →

QNX SDP 8.0 System Architecture Guide →

QNX SDP 8.0 System Security Guide →

Free Course: Introduction to the QNX Neutrino Real-Time Operating System (RTOS) →

Learn More

Free Evaluation →

Non-commercial license

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 →