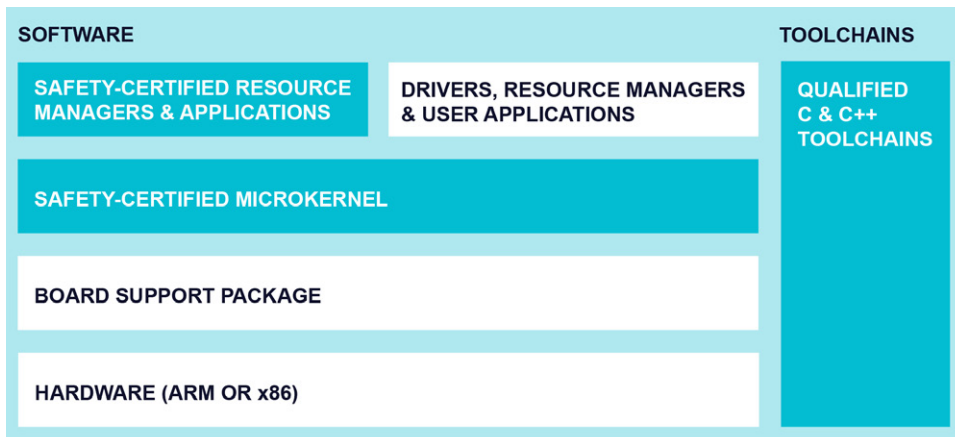


QNX OS for Safety



Approved for Use as SEooC

The QNX OS for Safety can be used as a Safety Element out of Context (SEooC) in order to realize safety goals up to IEC 61508 SIL 3, ISO 26262 ASIL D, and IEC 62304 Class C.

The C++ Library (optional) is certified to ISO 26262 ASIL B.

A Safety-certified Foundation

Streamline your products' functional safety certifications with a microkernel operating system pre-certified specifically for safety-critical embedded systems, and toolchains pre-qualified for building these systems.

Ideal for building complex safe systems, the QNX® OS for Safety is a safety-certified real-time operating system designed for use in every sector where safe, reliable embedded software is critical: medical devices, industrial controls, aerospace, automotive, power generation, robotics and rail transportation.

Certified by TÜV Rheinland to IEC 61508 SIL 3, ISO 26262 ASIL D, and IEC 62304 Class C, the QNX OS for Safety lets you focus your talents and efforts on developing the systems your customers need. Your OS will meet your performance and dependability requirements and facilitate your systems' safety-certifications.

Streamline Your Product Certifications

With the QNX OS for Safety you'll be starting out with your most critical software component pre-certified. And, especially since the QNX OS for Safety's certifications include IEC 61508, from which many other standards such as EN 50128 (rail) and IEC 60880 (nuclear power generation) are derived, you'll already be well on the way to certification, regardless of the specific safety certification you need.

Easily Port from Linux

The QNX OS for Safety is POSIX-compliant, so you'll have no trouble porting prototypes built with Linux.

Safe and Secure

The QNX OS for Safety implements layered security. You can specify the security profiles most appropriate for your system and its environment.

Protect Critical Functionality

The QNX OS for Safety includes a safety-certified variant of the QNX Neutrino® RTOS along with associated pre-qualified C and C++ toolchains. This microkernel design has proven its fundamental dependability over 40 years in hundreds of millions of embedded systems. It protects itself and your system both from internal faults and outside interference:

- All OS services are separate user processes; a failure in one process doesn't impact the system or other processes.
- Key OS functions (e.g., networking) are separated from other services, removing vulnerabilities to errors in application code.
- Adaptive partitioning guarantees CPU resources to critical services.
- Adherence to the POSIX standard ensures proper handling of OS privileges.
- The microkernel architecture minimizes the attack surface hackers can exploit.

Certify Your Code, Not Your Toolchains

A safety-certified OS and qualified toolchains mean that you'll have greater confidence in the software you build, and you'll have a shorter and smoother certification process.

With the QNX OS for Safety you'll be able to build your systems with C and C++ toolchains classified as TCL3 and T3 according to ISO 26262 and IEC 61508. You'll need to certify only the parts of the system you build, not the OS you build it on or the toolchains you use to build it.

Familiar QNX Neutrino RTOS API

If you're familiar with the QNX Neutrino RTOS you'll require no ramp-up time to begin your development work: the QNX OS for Safety is fully API-compatible with the QNX Neutrino RTOS API.

You'll be able to develop non-safety as well as safety-critical applications on the same foundations, and of course you'll be able to continue using the QNX Momentics® Tool Suite.

Comprehensive, Layered Security

Only a secure system can be a safe system. The QNX OS for Safety provides a comprehensive, layered approach to security. You can easily configure security profiles with the granularity you need for your systems, as well as monitor and audit their integrity.

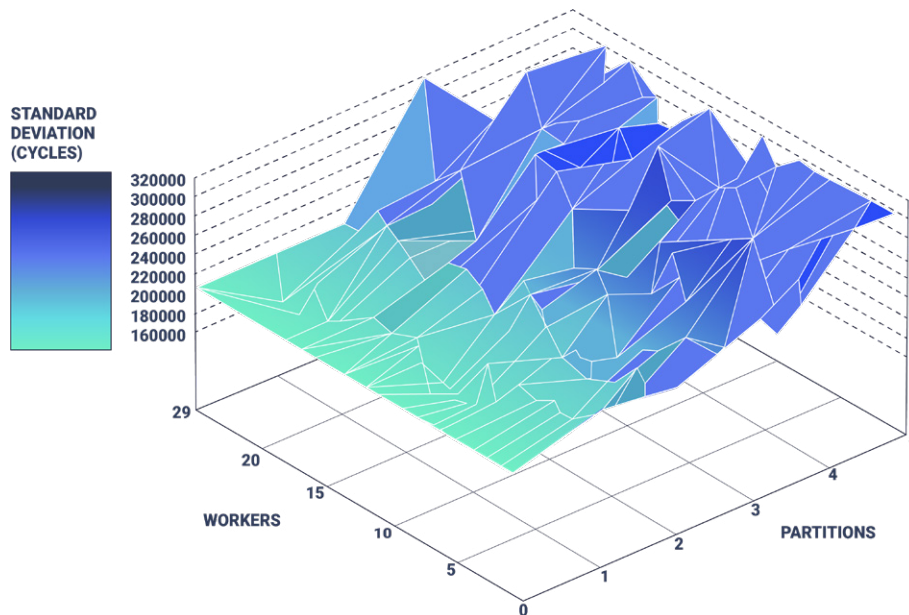
This layered approach allows you to implement exactly the security protocols you need to mitigate threats and harden your systems, including: granular control of system privilege levels, encrypted and self-verifying filesystems implementing AES 256 encryption and lockable encryption domains, secure logging of system activities, heap, stack and memory protection, and secure boot implementing TPM and TrustZone.

Safety Services

If you're uncertain about how to see your safety-critical product through to market, our safety experts can assist you at every stage—from design to certification.

Safety-certified Software

- Microkernel
- SMMU manager
- C library
- Math library
- C++ library (optional)
- Security management utilities



Example of latency investigation for the QNX OS for Safety

The QNX OS for Safety at a Glance

Software Safety Certifications

- Certifications by TÜV Rheinland, most recently in 2020
- IEC 61508:2010 SIL 3
- ISO 26262:2018 ASIL D
- IEC 62304 Class C

Certified C Library

- IEC 61508:2010 SIL 3
- ISO 26262:2018 ASIL D
- IEC 62304 Class C

Certified C++ Library

- ISO 26262:2018 ASIL B

Qualified C and C++ Toolchains

- IEC 61508-3:2010 SIL 3: TCL3 and T3
- ISO 26262-8:2018 ASIL D: TCL3 and T3

POSIX Compliant

- Validation using PSE 54 test suite
- Supports a broad range of POSIX API specifications

Safety Documentation

- Safety Certificates
- Safety Manual
- Installation and Usage Guide
- Hazard and Risk Analysis
- Safety Case
- Release Notes

QNX Neutrino RTOS Features

The QNX OS for Safety provides you with a safety-certified foundation on which to build your systems *and* the benefits of a full-featured, deterministic OS for embedded systems, including:

- Microkernel architecture
- High availability manager
- Protected direct memory access (DMA)
- Adaptive partitioning
- Layered security
- Instrumented microkernel
- Complete set of user documentation

Processor Support

- 64-bit support for the latest ARMv8 and x86-64 SoCs

Related Products

QNX Neutrino RTOS

Not building a system that needs certification? The QNX Neutrino Real-time Operating System (RTOS) powers hundreds of millions of embedded systems in every industry where reliability matters, including automotive, medical devices, robotics, transportation and industrial automation.

QNX Black Channel Communications Technology

Concerned about data integrity? Certified by TÜV Rheinland to ISO 26262 ASIL D, QNX Black Channel Communications Technology helps ensure the safety of your system's data communication.

QNX Hypervisor for Safety

Need to run a safety-certified system alongside non-safety systems? The QNX Hypervisor for Safety is safety-certified, so you can run safety-critical systems and non-safety systems on the same SoC.

QNX Momentics Tool Suite

Work with a mix of languages (e.g., C, C++ and Python), and develop for multiple SoC architectures (ARM and x86) simultaneously in a familiar Eclipse-based environment.

BlackBerry QNX Professional Services

We've helped thousands of clients build safe, secure and reliable systems on the QNX OSs. BlackBerry QNX system architects and engineers are here to guide you through the complex process of aligning software, hardware and processes to achieve your project goals.

Safety Services

We offer functional safety training, consulting, custom development, root cause analysis and troubleshooting, and system-level optimization and onsite services across a range of industries and systems. Let us help you with your certification journey.

Porting Assessment

If you built your prototype on Linux or another OS but aren't able to certify the open source components, we will help you better understand the effort and resources required to port your prototype or project to the QNX OS for Safety.

About BlackBerry® QNX®

BlackBerry QNX is a leading supplier of safe, secure, and trusted operating systems, middleware, development tools, and engineering services for mission-critical embedded systems. BlackBerry QNX helps customers develop and deliver complex and connected next generation systems on time. Their technology is trusted in more than 175 million vehicles and hundreds of millions of embedded systems in medical, industrial automation, energy, and defense and aerospace markets. Founded in 1980, BlackBerry QNX is headquartered in Ottawa, Canada and was acquired by BlackBerry in 2010.

For more information, visit blackberry.qnx.com and follow [@QNX_News](https://twitter.com/QNX_News).

 **BlackBerry**®

QNX®