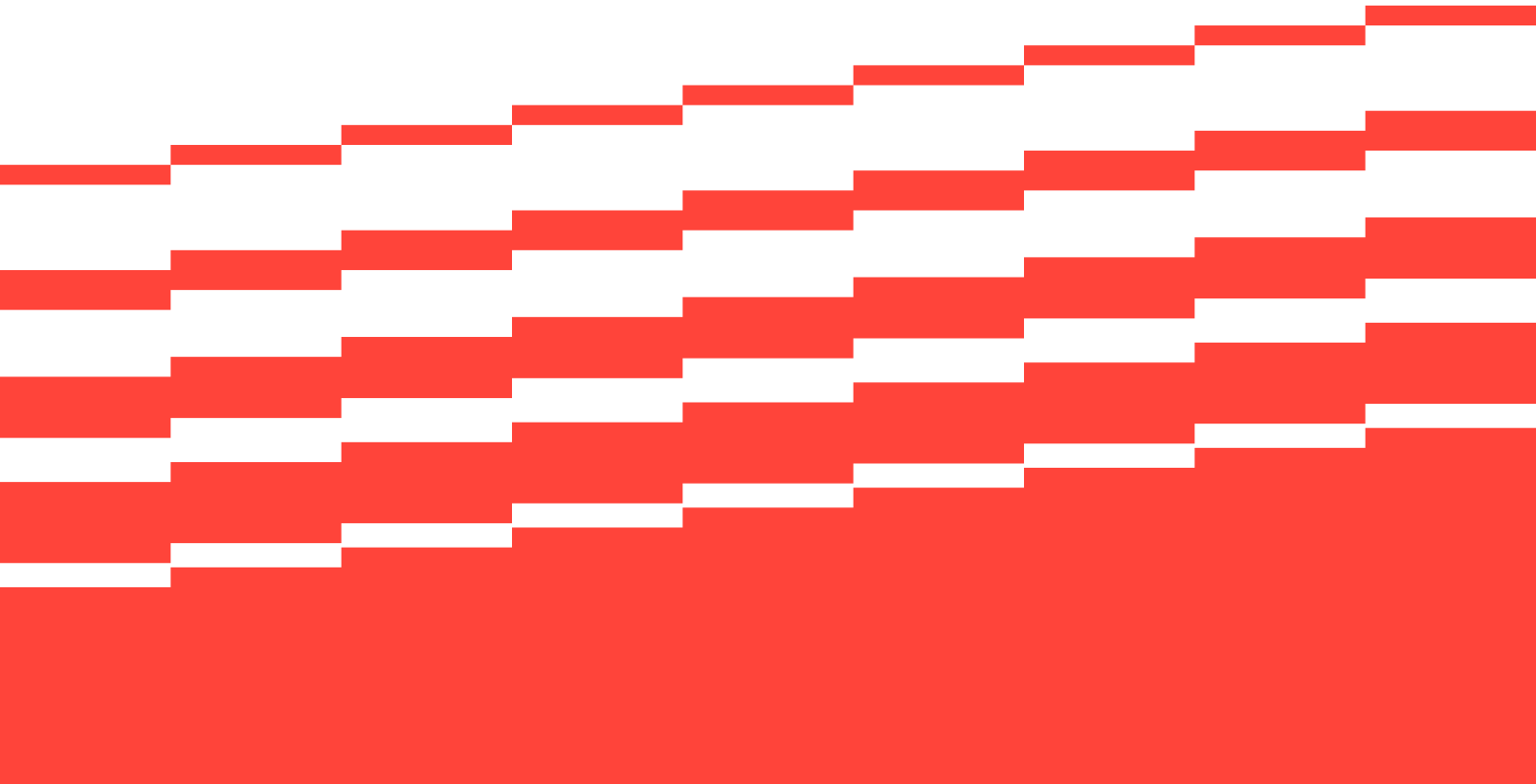
QNX

Solution Brief

QNX Hypervisor for Safety 8.0

Safety-Certified Virtualization for High-Integrity, Mission-Critical Embedded Systems



QNX Hypervisor for Safety 8.0

QNX Hypervisor for Safety is an embedded virtualization platform built on the proven QNX microkernel architecture. It enables multiple guest operating systems including Android™, Linux®, and QNX, to run securely and simultaneously on a single system-on-chip (SoC). Designed for mixed-criticality environments, QNX Hypervisor for Safety leverages the proven isolation and deterministic capabilities of the QNX microkernel to safely consolidate safety-critical and general-purpose workloads on a single embedded platform.

Meeting Modern Embedded Demands Through Safety-Certified Virtualization

Embedded systems are growing in complexity as software-defined architectures, connected services, and advanced workloads converge on a single high-performance SoC. This integration significantly reduces cost, power consumption, and hardware footprint, while streamlining system designs. Industries such as automotive, medical, industrial automation, and defense demand the highest levels of safety and reliability, requiring embedded systems that are both efficient and robust.

The QNX Hypervisor for Safety is pre-certified to ISO 26262 ASIL D, IEC 61508 SIL 3, and IEC 62304 Class C, and includes key safety artifacts to streamline the development and certification of safety-critical systems.

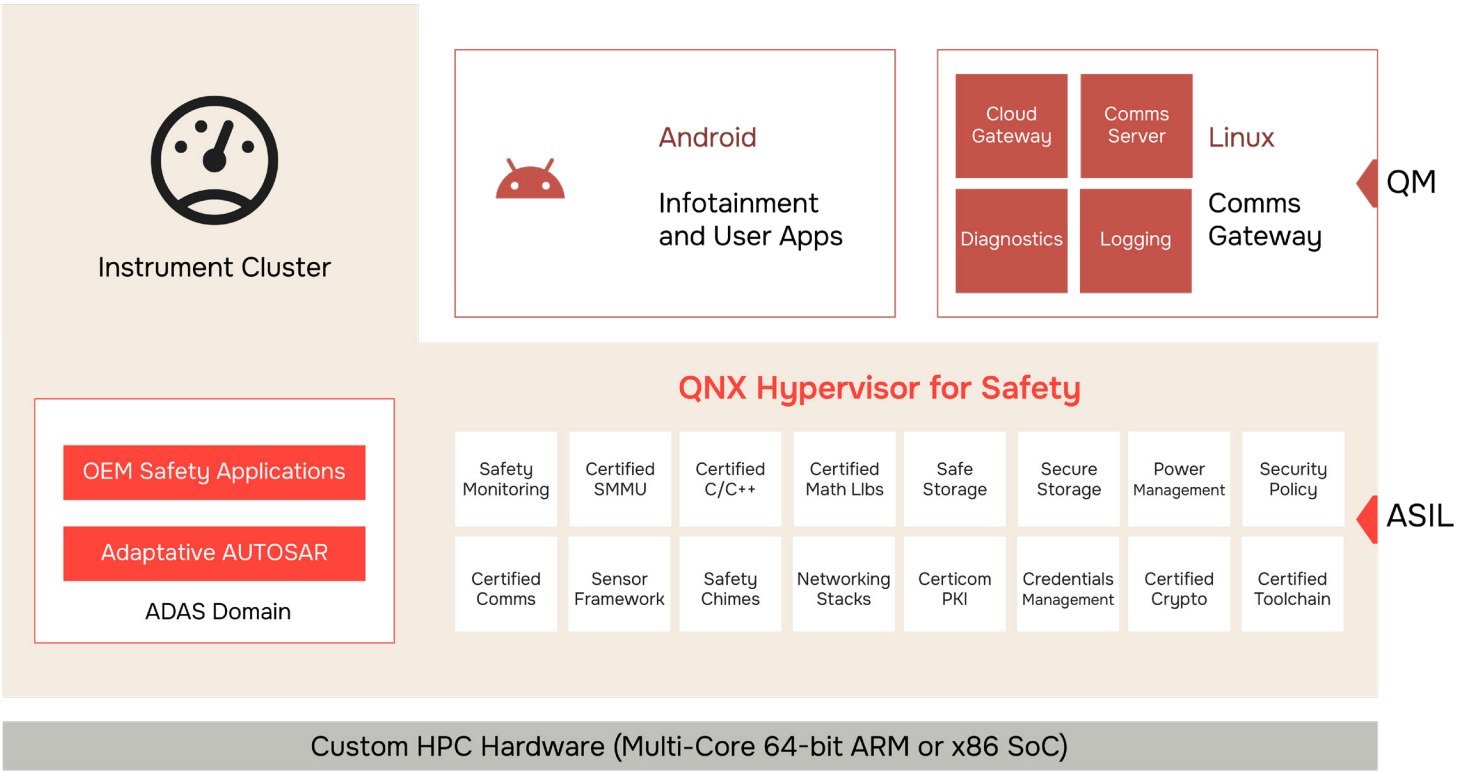
Built upon the QNX OS for Safety, it enables mixed-criticality consolidation, allowing safety-certified real-time workloads to run alongside general-purpose guest operating systems on the same hardware. This consolidation is supported by strong isolation and controlled resource management, which ensures that faults and crashes in one domain do not affect others.

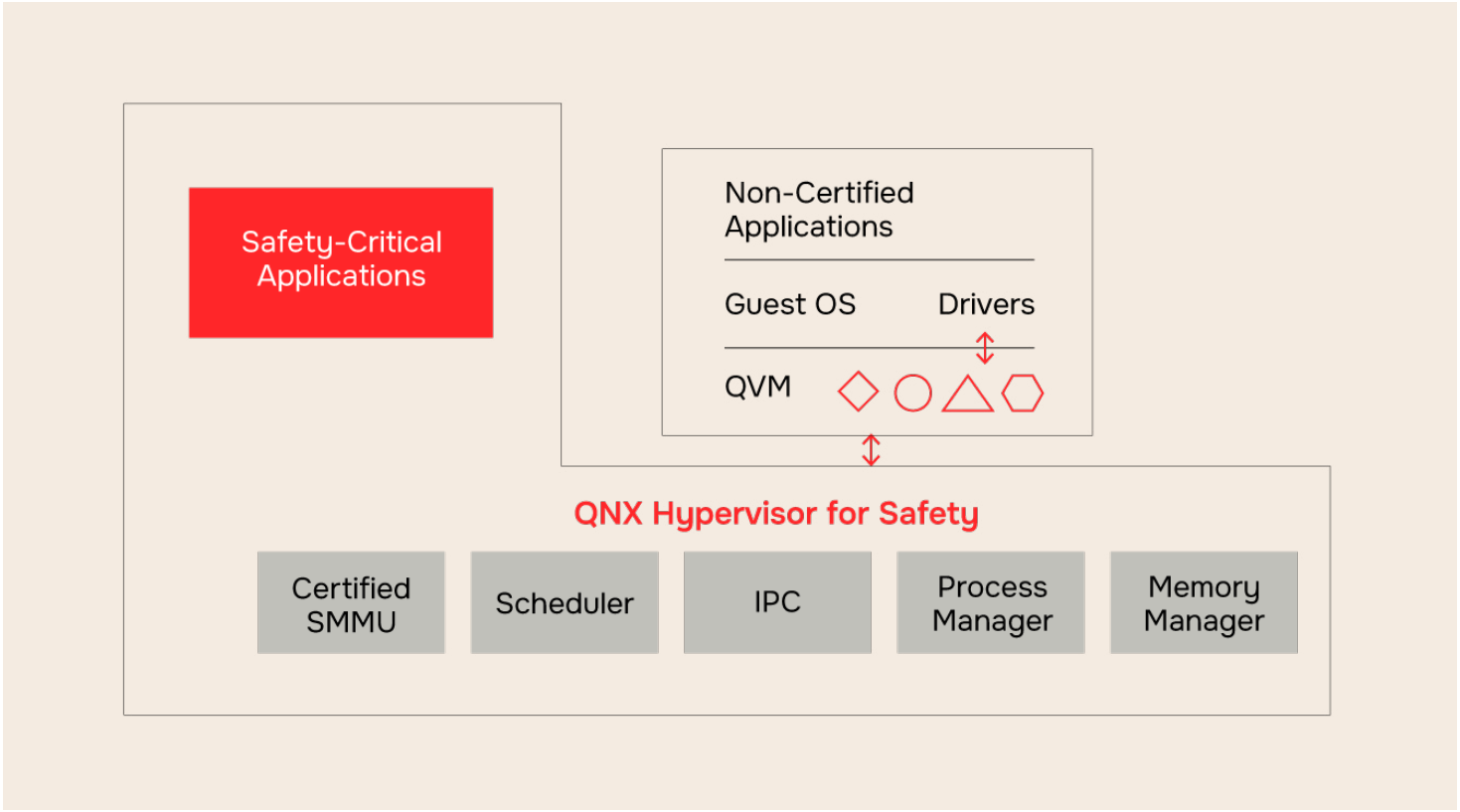
The QNX Hypervisor for Safety leverages the proven next-generation QNX microkernel and extends pre-certification scope to the hypervisor, enabling developers to streamline system integration, optimize resource utilization, and accelerate safety certification across complex embedded platforms.

Designing Embedded Systems That Can Evolve Safely

As embedded systems become increasingly connected and software-defined, organizations need platforms that can evolve without hardware redesign. QNX Hypervisor for Safety delivers a stable, flexible, and pre-certified virtualization foundation that enables safe system evolution. Developers can add new applications, update services, or migrate legacy code, all while maintaining strict isolation for safety-critical functions.

This architecture lets organizations build their embedded platforms with confidence. Organizations can introduce new capabilities, upgrade existing functions, and incorporate emerging technologies without compromising certified safety-critical operations. QNX Hypervisor for Safety supports modular growth and scalable designs, ensuring systems remain compliant, high-performing, and adaptable to future requirements over their entire lifecycle.


Instrument Cluster
Android
Infotainment and User Apps
Cloud Gateway
Comms Server
Diagnostics
Logging
Linux
Comms Gateway
QM
QNX Hypervisor for Safety
Safety Monitoring
Certified SMMU
Certified C/C++
Certified Math Llbs
Safe Storage
Secure Storage
Power Management
Security Policy
Certified Comms
Sensor Framework
Safety Chimes
Networking Stacks
Certicom PKI
Credentials Management
Certified Crypto
Certified Toolchain
ASIL
OEM Safety Applications
Adaptative AUTOSAR
ADAS Domain
Custom HPC Hardware (Multi-Core 64-bit ARM or x86 SoC)


Safety-Critical Applications
Non-Certified Applications
Guest OS
Drivers
QVM
QNX Hypervisor for Safety
Certified SMMU
Scheduler
IPC
Process Manager
Memory Manager

Inside QNX Hypervisor for Safety

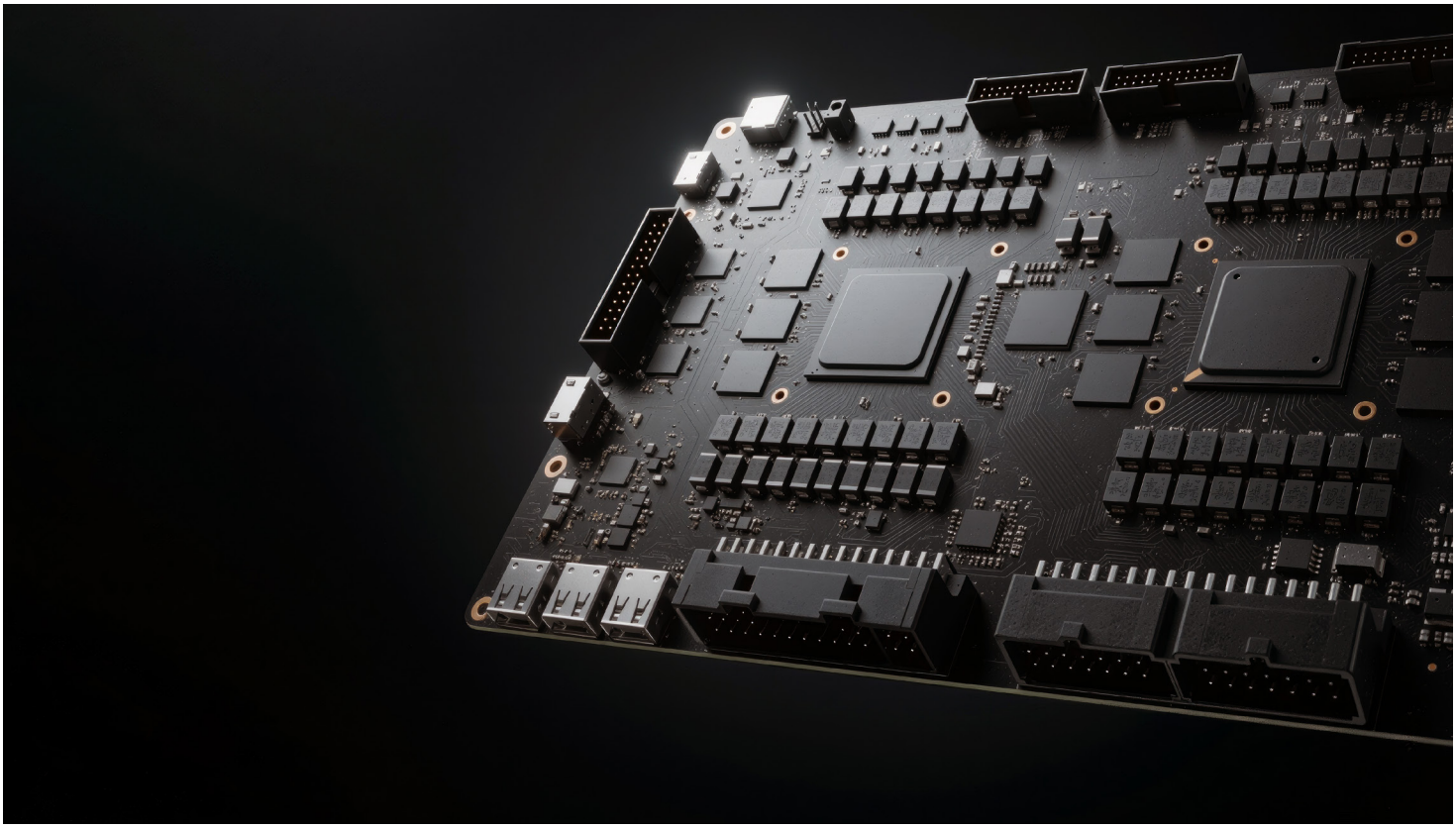
QNX Hypervisor for Safety provides a secure virtualization layer through a host process that allows multiple guest operating systems to run concurrently on the same SoC. It manages memory, CPU, and device access while enforcing strict isolation between guests.

The QNX Hypervisor for Safety leverages the QNX Host's microkernel, which provides controlled and predictable execution of virtualization workloads. Para-virtualized devices enable efficient communication between guests and the host. At the hardware level, the hypervisor manages ARMv8/v9 or x86-64 resources such as Direct Memory Access (DMA) and physical devices to ensure fault containment, safety, and consistent performance.
By combining deterministic execution, secure device handling, and hardware-assisted virtualization, QNX Hypervisor for Safety gives developers a flexible way to scale platforms, support diverse use cases, and accelerate the development of complex embedded applications.

Support for Virtualization Host Extensions

QNX Hypervisor for Safety supports Virtualization Host Extensions (VHE) on ARMv8 AArch64 processors. This allows the hypervisor to run at Exception Level 2 (EL2), the hardware privilege level designed for virtualization. Operating at EL2 reduces the overhead of switching between guests and the hypervisor, improving performance and keeping system timing predictable.

Each guest virtual machine runs as its own isolated execution context, with virtual CPUs scheduled independently. The hypervisor supports both Symmetrical Multiprocessing (SMP) and Bound Multiprocessing (BMP), allowing virtual CPUs to be pinned to specific cores or moved across cores as needed. These capabilities ensure the system maintains reliable and predictable performance across varied workloads.



Proven Reliability

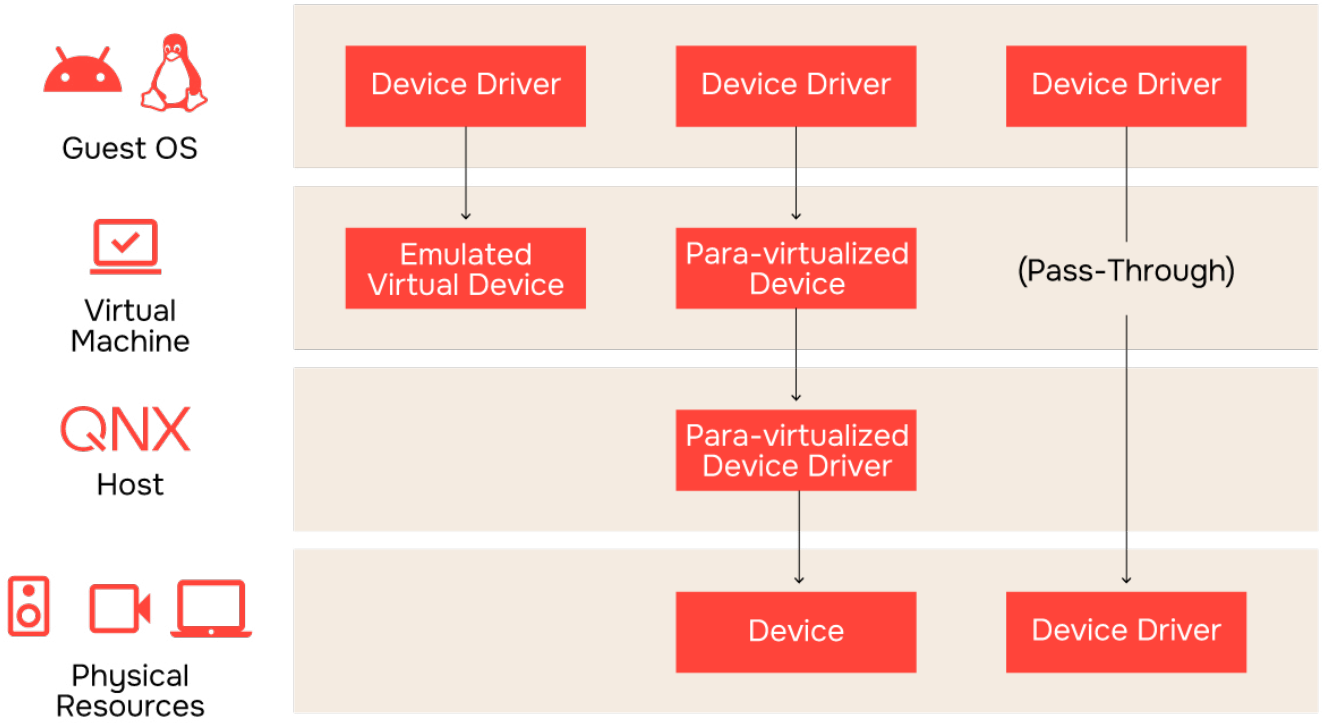
The QNX Hypervisor for Safety builds on virtualization extensions to the QNX OS microkernel, providing a proven foundation validated across four decades and hundreds of millions of mission-critical deployments. Its real-time deterministic behavior, spatial isolation, and robust fault containment make QNX a trusted cornerstone for embedded systems where reliability is essential and failures cannot be tolerated.

Ensure System Isolation

System integrity and isolation are core strengths of the QNX Hypervisor for Safety, which is built on the proven QNX OS microkernel and its virtualization extensions. By enforcing strict boundaries on memory, CPUs, interrupts, and devices, the hypervisor ensures that faults or interference, whether originating from guest virtual machines or external sources, cannot compromise other system components.

When virtual machines are configured, each guest's memory regions and access to physical or virtual devices are explicitly defined. These assignments are validated at system startup and strictly enforced at runtime. Any attempt to exceed assigned permissions, whether accidental or malicious, is immediately blocked to preserve system stability and isolation.

To further enhance isolation, the QNX Hypervisor for Safety includes the SMMU manager service (smmuman), which works in conjunction with hardware System Memory Management Units (SMMUs) to confine Direct Memory Access (DMA) devices. This ensures that DMA-initiated transfers cannot reach memory beyond approved regions, with any violations detected and contained by the hardware and manager service.



Virtual Machines & Device Configuration

Each QNX Hypervisor for Safety virtual machine is configured like a physical board, with memory and devices explicitly assigned to either the guest or the hypervisor. Devices can be configured in three ways:

- Emulated: The hypervisor fully emulates the device, ensuring broad compatibility without requiring guest driver changes.
- Para-virtualized (VirtIO compliant): Optimized virtual drivers enable the guest OS to access physical devices efficiently, reducing overhead and improving performance.
- Physical pass-through: The guest OS accesses the physical device directly, delivering native performance with minimal latency.

The QNX Hypervisor for Safety enforces strict isolation between guests, the hypervisor core, and other SoC components, ensuring secure and deterministic operation. Combined with runtime management, this allows context switching and event handling without disrupting system integrity, enabling multiple operating systems and applications to run safely and efficiently on the same hardware.

Flexible Deployment Models

The QNX Hypervisor for Safety leverages ARMv8 AArch64 and x86-64 hardware virtualization to provide versatile deployment options for modern embedded systems. Developers can run full operating systems and applications in virtual machines while the hypervisor handles only critical events and exceptions. Alternatively, a complete native system can run directly on the host alongside guest VMs, including drivers and resource managers. This flexibility simplifies system integration and accelerates time-to-deployment for complex embedded applications.

Leverage QNX OS Technologies

QNX Hypervisor for Safety is built on the QNX OS microkernel and Software Development Platform, using core OS services to deliver reliable, high-performance virtualization. The QNX scheduler manages guest execution, the process manager coordinates system activity, and the memory manager enforces strict isolation and controlled shared memory access.

By leveraging QNX's modular architecture and resource managers, the hypervisor can expose virtual devices, handle interrupts, and manage I/O consistently across guests. POSIX-compliant APIs and the QNX tool suite give developers familiar ways to integrate applications, debug issues, and profile workloads while taking advantage of the OS's determinism, scalability, and safety features.

Enhanced System Observability

QNX Hypervisor for Safety provides built-in monitoring and diagnostic capabilities that give developers insight into the behavior of virtual machines and system resources. Using QNX development tools, such as the Momentics IDE and command-line utilities, developers can monitor CPU usage, memory allocation, and I/O operations across guests, identify performance bottlenecks, and trace execution events. This visibility simplifies debugging and performance tuning for both real-time and general-purpose workloads, enabling consistent and predictable operation of multiple operating systems on the same hardware.

Pre-Certified and Ready-to-Use Virtualization Foundation

In summary, QNX Hypervisor for Safety provides a pre-certified virtualization foundation that encapsulates safety, isolation, and mixed-criticality support within the platform itself. This lets developers and system architects focus their engineering efforts on building and certifying the unique application logic and higher-level system components, rather than foundational virtualization infrastructure.

The safety-certified hypervisor is developed, verified, and validated using industry-recognized best practices, delivering a trusted baseline that reduces certification risk and accelerates development. By offering a proven, safety-focused virtualization core, QNX Hypervisor for Safety helps organizations build embedded systems with confidence and predictable outcomes.

Related Products

QNX OS

Not building a system that needs certification? The QNX OS powers hundreds of millions of embedded systems in every industry where reliability matters, including automotive, medical devices, robotics, transportation, and industrial automation.

QNX OS for Safety

Don't need a hypervisor system, but need a safety-certified system? The QNX OS for Safety is certified by TÜV Rheinland to IEC 61508 SIL 3, ISO 26262 ASIL D, and IEC 62304 Class C, so you can focus your talents and efforts on developing the systems your customers need.

QNX Hypervisor

Looking for a high-performance virtualization solution without safety certification requirements? QNX Hypervisor 8.0 delivers strong isolation, efficient resource management, and support for advanced workloads across ARM and x86 platforms, making it ideal for complex mixed-criticality embedded systems.

QNX Tooling Suite

QNX provides a comprehensive development suite to boost productivity. The Momentics IDE, Eclipse-based, supports C, C++, and Python across ARM and x86 architectures. For lighter workflows, the QNX Toolkit for VS Code integrates key tools like System Profiler and System Information, enabling efficient coding, debugging, and system analysis within developers' familiar environments.

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 on-site services across a range of industries and systems. Let us help you with your certification journey.

Virtualization Assessment

If you built your prototype on Linux or another OS but don't know how to proceed with virtualization, we will help you better understand the effort and resources required to port your prototype or project to a QNX Hypervisor for Safety system.

QNX Certification Scope

Safety QNX Products Certifications	QNX OS for Safety	QNX Hypervisor for Safety	QNX Filesystem for Safety
ISO / SAE 21434	✓	In Progress	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 QHS, 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 Security Guide →

QNX SDP 8.0 System Architecture Guide →

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

March 2026

QNX

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 →