BlackBerry | QNX

PRODUCT BRIEF

QNX Hypervisor for Safety

The world's first ISO 26262 ASIL D certified commercial hypervisor

QNX Hypervisor for Safety is the world's first ISO 26262 ASIL D safety-certified commercial hypervisor

Safe and secure virtualization is a key technology in the software architecture of modern vehicles, from domain controllers (digital cockpits and vehicle gateways) to zone controllers (automated drive and control systems). The QNX Hypervisor for Safety provides the highest ASIL functional safety level in the industry, pre-certified to ISO 26262 ASIL D and IEC 61508 SIL 3, offering simpler and faster certification of your mission-critical systems.

Best-in-class technology with design flexibility

QNX Hypervisor for Safety provides the broadest design flexibility to allow system designers to build dependable systems without wasting hardware resources. At one end of the spectrum, guest operating systems (OS) can pin their virtual CPUs (vCPUs) to physical CPU cores and be given exclusive access to underlying hardware. At the other end of the spectrum, guest OS can share CPU cores and hardware devices using priority-based scheduling and standards-based VirtIO interfaces.

QNX OS for Safety may run as a guest on QNX Hypervisor for Safety, providing an even stronger foundation for systems that require advanced functional safety.

The QNX Hypervisor for Safety provides pre-certified software in three key areas:

- Virtual machine
- Hypervisor host environment
- Development tools

Safety-Certified Virtual Machine

A separate QNX virtual machine manager (qvm) is launched for each guest. Guest support includes unmodified Android, Linux, QNX OS for Safety, and other specialized 64-bit and 32-bit guest software (see Figure 1).

Each instance of the virtual machine manager:

- Implements a discrete security policy (e.g. Mandatory Access Control, rootless operation)
- Has one or more virtual CPUs (vCPUs) that can be pinned to cores or allowed to float across physical cores
- Can be dynamically shut down and restarted (a local Design Safe State)
- May be configured for pass-through to underlying hardware (see SMMU service)
- Supports industry-standard VirtIO-based devices
- May have multiple shared memory and peer network connections to other virtual machines

Safety-Certified Hypervisor Host Environment

The hypervisor host environment (also called host domain) provides the services needed to run the virtual machines. The host domain can be configured to be feature-rich or minimal. For example, an instrument cluster can run in the host domain and share graphics with infotainment running in a virtual machine. An AUTOSAR environment could run in the host domain or in a guest.

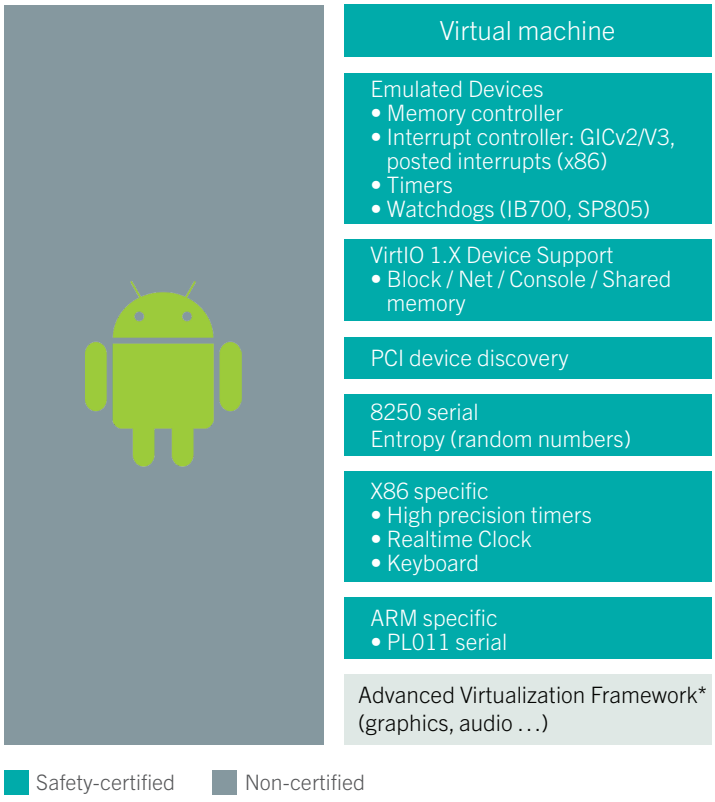


Figure 1: An Android virtual machine. Safety-certified components shown in green. Linux and QNX guests would have similar configuration.

The safe and secure hypervisor microkernel foundation allows for maximum flexibility in system design choices. Field-proven QNX microkernel technology provides the heart of the hypervisor runtime environment. This lets developers use trusted QNX services to meet key performance indicators (KPI) for fast and secure boot, camera on, early chimes, instant device activation, and splash screen display.

The hypervisor host domain environment includes:

- The hypervisor microkernel that schedules the virtual machines based on priority, provides virtual machine runtime guarantees (Adaptive Partitioning), and enforces security policy
- A POSIX runtime environment for adding services to host domain
- Support for IOMMU/SMMU (System Memory Management Unit) for bounds checking of pass-through devices both in virtual machines and for drivers running in host domain
- Safety-certified C library (libc), Math library (libm), and logging support
- Back-end services (disk, console) to support VirtIO-based and non-VirtIO-based front-end devices
- A server monitor for timeout detection and recovery

Safety-Certified Development Tools

The QNX Hypervisor for Safety is integrated with the QNX Momentics Tool Suite so developers can use the safety-certified toolchain to:

Build		Expand		Analyze	
Compile and link	Use Image Builder to build the host	Create new back-end services	Build from sample sources	Capture hypervisor events using trace tools	Pause and resume a virtual machine
Code in POSIX	Set Set security and safety policy	Design new custom virtual devices	Add VirtIO support	Use system logging	Debug a running guest
Configure virtual machines	Build QNX OS for Safety guests	Use Virtual Device Developer's Guide	Integrate other QNX products	Examine virtual machine state in realtime	Do postmortem debugging

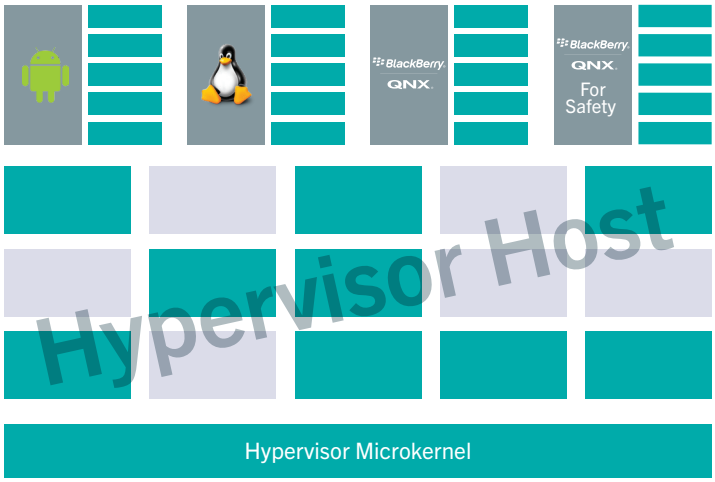
Figure 2: Safety-certified toolchain.

Support Technical Specifications

Virtualization is supported on any Intel x86_64 VT-x and ARMv8 AArch64 hardware, including popular reference hardware such as the Intel® Atom™ C3XXX product family, Renesas R-Car, Qualcomm® Automotive Compute platforms such as SA8155, Xilinx™, Mediatek™, Texas Instruments™, and NXP® product families (i.MX8 and S32).

A Foundation for QNX Advanced Virtualization Framework*

A highly optimized, integrated, and hardware-independent advanced virtualization framework is also available to extend support for the sharing of graphics controllers, display controllers, audio interfaces, video streaming services, cameras, input devices, and other system peripherals such as USB. As Android hardware abstraction layers (HALs) continue to evolve and change, the Advanced Virtualization Framework and a safety-certified and secure hypervisor provide the necessary foundation to support different iterations of guest operating system software.



Safety-certified services: C library (libc), math library (150+ functions), libfdt (device tree), shared memory, security manager, logging services (slogger), SMMU manager, server monitor

Optional services: TCP/IP stacks, block filesystems, rearview camera, AUTOSAR environment, instrument cluster, acoustic processing (additional fees may apply). Run alongside virtual machines, not safety-certified, but monitored to ensure proper interaction with safety components

Figure 3: Host domain shown with hypervisor microkernel and MMU-protected services that support the virtual machines

QNX Hypervisor for Safety Features Summary

- Type 1 Hypervisor architecture that scales up to Type 2 environments
- Safety Elements out of Context (SEooC) pre-certified to ISO 26262 ASIL D and IEC 61508 SIL 3
- Virtual CPU model allows for pinning to cores or sharing cores based on priority
- Adaptive partitioning provides CPU time guarantees of virtual machines
- 64-bit and 32-bit guests: QNX, QNX OS for Safety, Linux, Android, RTOS
- POSIX host hypervisor environment for expanding system services and virtual environment
- Zero-copy shared memory (guest-to-guest and guest-to-host) with triggering
- VirtIO 1.X device sharing
- Peer-to-peer networking (guest-to-guest and guest-to-host) with bridging. Guest-to-guest requires no back-end services in host
- Failure detection and restart of guests
- Virtual watchdogs for guest runtime checking
- Graphical tools for analysis and debug of guest environments and virtual machines
- Virtual Device Developer's Guide for building custom virtual devices
- Safe and secure foundation for QNX Advanced Virtualization Framework*

*QNX Advanced Virtualization Framework sold separately

About BlackBerry QNX

BlackBerry QNX is a leading supplier of safe, secure, and trusted operating systems, development tools, and professional services for connected embedded systems. Global leaders such as Ford, Audi, Cisco, General Electric, Lockheed Martin, and Siemens depend on BlackBerry QNX technologies for their next generation of secure vehicle software platforms, network routers, medical devices, industrial automation systems, security and defense systems, and other mission and/or life-critical applications. BlackBerry QNX is headquartered in Ottawa, Canada, with its products distributed in over 100 countries worldwide.

© 2019 BlackBerry QNX, a subsidiary of BlackBerry. All rights reserved. QNX, Momentics, Neutrino, are trademarks of BlackBerry Limited, which are registered and/or used in certain jurisdictions, and used under license by BlackBerry QNX. All other trademarks belong to their respective owners. 433.116