QNX NEUTRINO REAL-TIME OPERATING SYSTEM

PRODUCT BRIEF

MICROKERNEL RELIABILITY

The QNX Neutrino® Real-Time Operating System (RTOS) is based on a microkernel architecture that isolates every application, driver, protocol stack and filesystem in its own address space, 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 the rest of the system.

- Quickly add new drivers with confidence, knowing a driver failure won't mean a system failure.
- A self-monitoring high-availability manager (HAM) can perform multistage recovery when system services or processes fail or aren't responding properly.

The microkernel architecture also enabled us to safety-certify QNX OS for Safety, so you can focus on building and certifying what you build—not the OS you built it on.

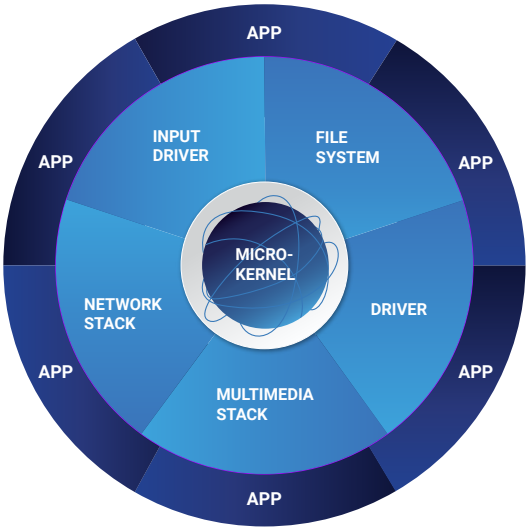


Figure 1:
QNX Neutrino Real-Time Operating System

REAL-TIME AVAILABILITY

The QNX Neutrino RTOS ensures system resources are available when needed, and tasks complete when they are supposed to complete (Figure 2).

Designed to scale on the latest generation of multicore systems-on-a-chip (SoCs), including ARMv8 and Intel x86-64, the QNX Neutrino RTOS supports both asymmetric multiprocessing (AMP) and symmetric multiprocessing (SMP), as well as bound multiprocessing (BMP), a QNX improvement on standard SMP processor affinity.

Our innovative adaptive partitioning enables you to guarantee that critical processes always get the CPU cycles they need. You can configure time partitions according to your particular system's requirements, so that processes that need additional power can access unused cycles from other processes' budgets.

COMPREHENSIVE, LAYERED SECURITY

The QNX Neutrino RTOS 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.

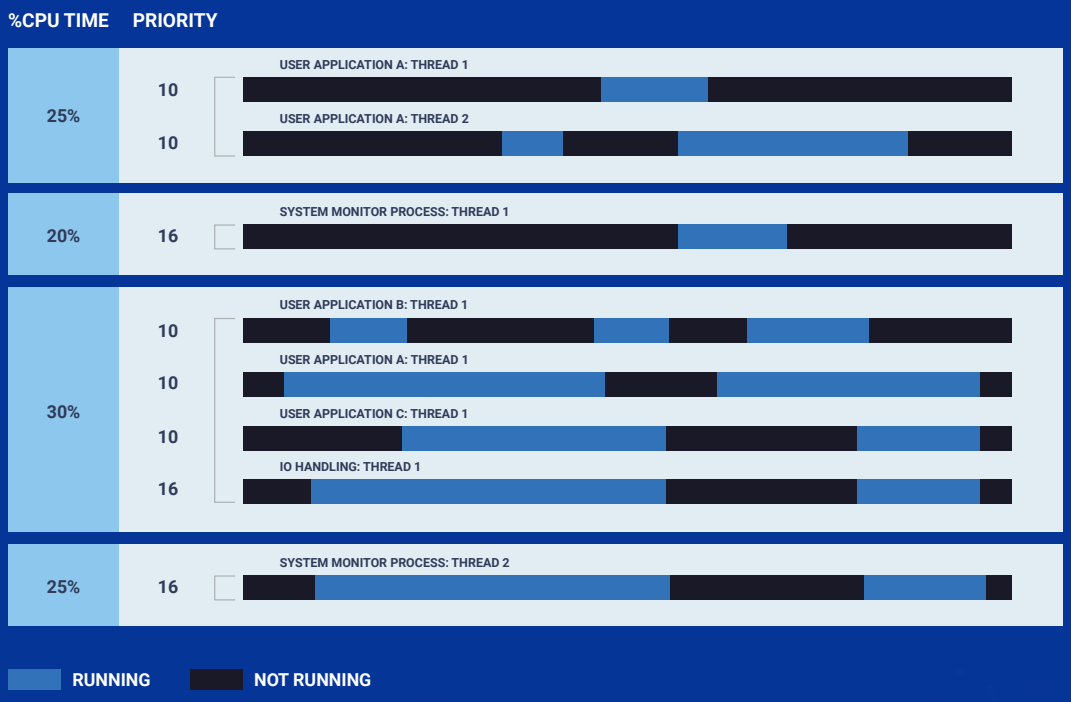


Figure 2:
The QNX Neutrino RTOS ensures temporal isolation while providing deterministic real-time performance.

THE QNX NEUTRINO RTOS AT A GLANCE

MICROKERNEL ARCHITECTURE	POSIX COMPLIANCE	DETERMINISTIC PERFORMANCE	ADAPTIVE PARTITIONING
• Spatial isolation of OS from drivers and applications • Fine-grained fault isolation and recovery • Message-passing design for modular, well-formed systems • Comprehensive multi-core support • Asymmetric (AMP), symmetric (SMP) and bound multiprocessing (BMP) • Guard pages at the end of each virtual stack to protect against stack overflow	• Validation using PSE 54 test suite • Supports a broad range of POSIX API specifications	• Pre-emptive scheduler with choice of scheduling methods • Distributed priority inheritance	• Redistribute unused cycles to optimize CPU loading • Guarantee CPU cycles to critical processes without compromising system performance

HIGH AVAILABILITY	PROTECTED DIRECT MEMORY ACCESS (DMA)	PROCESSOR SUPPORT	LAYERED SECURITY
• Heartbeat for early fault detection • High availability manager (HAM) to restart failed or unresponsive processes and services • Intelligent restart and transparent reconnection	• IOMMU/SMMU Manager leverages x86 VT-d or Arm® SMMU derivatives to protect against unauthorized DMA • Configurable boundaries for access to bus devices • Boundary violation monitoring and management	• 64-bit support for the latest ARMv8 and x86-64 SoCs • Continued 32-bit support for ARMv7 SoCs	• Granular control of system privilege levels • Self-verifying filesystems with AES 256 encryption • Secure system activity logging • Heap, stack and memory protection • Rootless execution • Secure boot implementing TPM and TrustZone

THE QNX NEUTRINO RTOS AT A GLANCE

STANDARD AND HIGH-PERFORMANCE NETWORKING AND CONNECTIVITY

- IPv4 and IPv6 support
- Support for various network features including:
  - VLAN
  - Network bridging
  - Packet filtering
  - Multicast routing
  - IPsec
  - Internet Key Exchange (IKE)
- Network driver support including:
  - WiFi 802.11 a/b/g/n
  - USB 3.x, host, device and on-the-go (OTG)
  - PCIe
- Network integrations with:
  - eAVB
  - TLS
  - TSN
  - SOME/IP
  - RTPS
  - DBUS
  - DDS
- Support for various network applications and utilities, including:
  - NTP
  - FTP
  - NFS
  - SSH
  - DHCP
  - DNS

FILE SYSTEMS

- Image file system (IFS), RAM, Flash, QNX6 Power-Safe, QNX Trusted Disk, Compressed
- UDF, NVMe, HFS+, Linux, DOS, CD-ROM, CIFS, NFS and NTFS

GRAPHICS AND HMI TECHNOLOGIES

- Screen composition manager supporting multiple graphics technologies
- Single, unified interface from multiple UI sources
- Leverages GPU acceleration and supports multi-touch input and video capture
- OpenGL® ES and Vulkan® support

INSTRUMENTED MICROKERNEL

- System-wide performance analysis and optimization
- Rapid detection of timing conflicts, hidden faults, etc.

SUPPORT AND DOCUMENTATION

- Architecture overviews
- Programming and configuration guides
- Complete API references
- Board Support Packages

RELATED PRODUCTS

QNX OS FOR SAFETY

Need to safety certify your system? The QNX OS for Safety is the only embedded OS certified to IEC 61508 SIL3, IEC 62304 for Class C devices, and ISO 26262 at ASIL D.

QNX HYPERVISOR

Need to run diverse OSs on the same board? The QNX Hypervisor lets you run multiple OSs on the same SoC: QNX Neutrino RTOS, QNX OS for Safety, Linux and Android.

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 QNX. 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.

PORTING ASSESSMENT

This engagement will help you better understand the effort and resources required to port your prototype or project from your current OS to the QNX Neutrino RTOS.

ARCHITECTURE ASSESSMENT

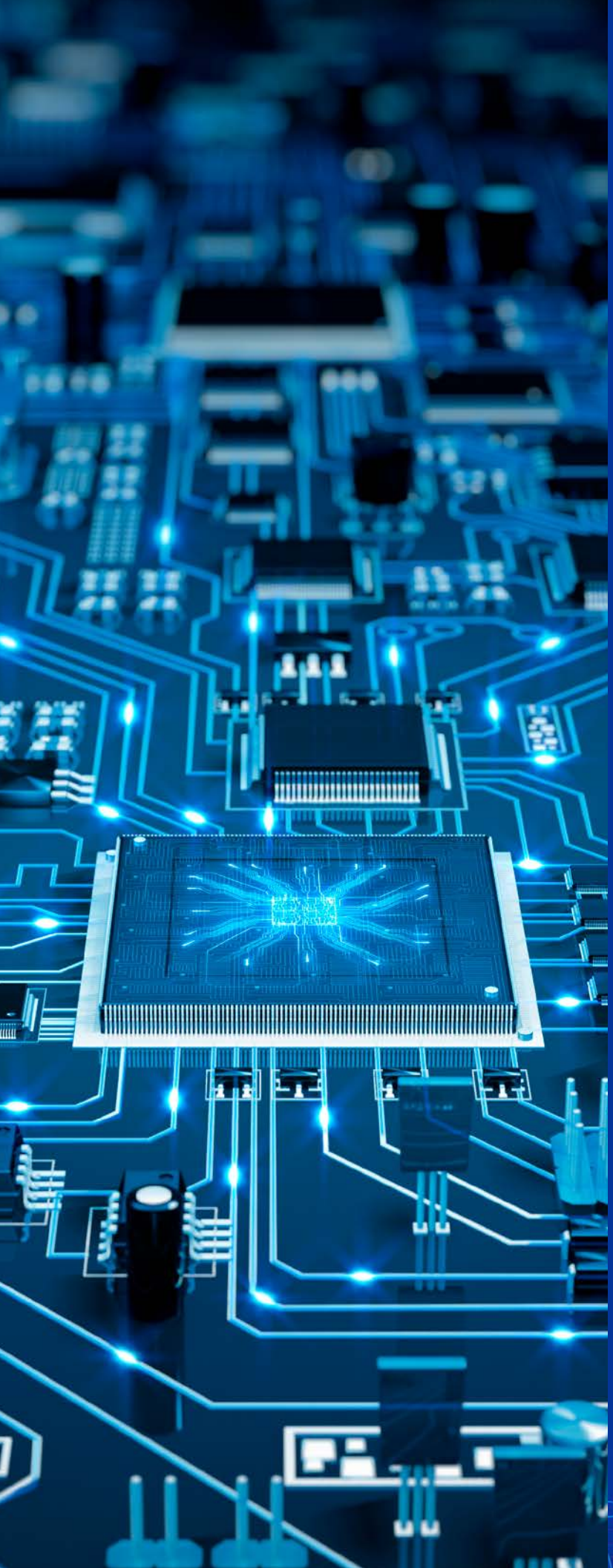
An experienced architect will do a thorough review of your embedded system or application architecture and provide recommendations and artefacts to help you increase reliability and shorten time-to-market.

SAFETY SERVICES

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

SECURITY SERVICES

We can evaluate your software assets to identify vulnerabilities and recommend specific remediation actions. From penetration testing to a holistic appraisal of your company's security posture, our teams of security experts can assess and address security issues with your processes or products at every stage of your software development life cycle (SDLC).



ADDITIONAL NOTES

GUARANTEE CPU CYCLES

The QNX Neutrino RTOS offers the determinism only a real-time OS can provide. Techniques such as adaptive partitioning guarantee critical processes get the cycles they need to complete their tasks on time, while maintaining the performance your complex embedded systems require.

HOLISTIC SECURITY

With the QNX Neutrino RTOS's layered security features and access to QNX security experts, you can take a holistic approach to security and ensure your systems are protected.

RESTART FAILED COMPONENTS

With the QNX microkernel architecture, a component failure doesn't bring down other components or the kernel. The failed component is simply shut down and restarted without adversely affecting the rest of the system.

BOARD SUPPORT PACKAGES

BlackBerry QNX has an extensive library of board support packages (BSPs) for a broad selection of ARMv8, x86-64 and older platforms.

QNX SOFTWARE CENTER

Take the guesswork out of managing multiple, complex software installations. With the QNX Software Center, product dependencies are automatically managed and pro-active alerts are sent when relevant product releases, patches or security updates are available.

About BlackBerry QNX: BlackBerry QNX is a trusted supplier of safe and secure operating systems, hypervisors, frameworks and development tools, and provides expert support and services for building the world's most critical embedded systems. The company's technology is trusted in more than 215 million vehicles and is deployed in embedded systems around the world, across a range of industries including automotive, medical devices, industrial controls, transportation, heavy machinery and robotics. Founded in 1980, BlackBerry QNX is headquartered in Ottawa, Canada and was acquired by BlackBerry in 2010.

BlackBerry® QNX® software and development tools are standards-based and enable companies to adopt a scalable software platform strategy across product lines and business units. The BlackBerry QNX software portfolio, including safety pre-certified products, is purpose-built for embedded systems and scales from single-purpose devices to highly complex systems of mixed criticality. Because we are successful only when you are, you can rely on our support and professional services teams to provide the expertise you need, when you need it—throughout the entire product development life cycle.

QNX-NRTOS-03-ENG-(0822)-PB-DF