BlackBerry | QNX

PRODUCT BRIEF

QNX OS for Safety 2.0

General Embedded Systems

The general embedded market (GEM) is vast, with numerous and diverse systems. Functional safety is a critical requirement for many sub-segments in this market, meaning that mission-critical embedded systems must be designed in such a way that they are fault-tolerant and fail-safe. As these systems become increasingly complex, safety design becomes a greater challenge. The QNX OS for Safety is a software solution that meets this challenge, providing the reliable foundation necessary for building safe and competitive GEM systems in a cost-effective manner.

Benefits

- Pre-certified to IEC 61508 SIL3 to reduce development, certification cost and risk
- Freedom from interference mechanisms to enable and simplify the design of systems with a mix of safety and non-safety critical functions
- Qualified C and C++ toolchain to ease the certification workload for customers
- Fully API-compatible with standard QNX Neutrino RTOS to minimize ramp up time and allow code re-usage

Safety Certified

Functional safety has always been a requirement for many GEM applications. Industrial automation, robotics, energy generation and high-speed trains are just a few obvious examples where failure of the system can lead to severe consequences of human life and property damage. As GEM applications adopt more powerful hardware and sophisticated software, meeting functional safety requirements becomes a greater challenge.

IEC 61508 has been the dominant international standard for functional safety in GEM. Many sub-segment specific safety standards for GEM are derived from IEC 61508 (e.g. EN 50128 for railway applications, IEC 60880 for nuclear applications and IEC 62304 for medical devices). Building a system compliant with a safety standard is a significant task, especially for manufacturers who are not familiar with functional safety at all levels of the design. To help mitigate risk of non-compliance and reduce development and certification costs, BlackBerry QNX provides a reliable RTOS foundation that is pre-certified to IEC 61508 SIL 3. Using the QNX OS for Safety, as the foundational building block, can greatly relieve the certification burden for manufacturers and give them the peace of mind they need when building systems with safety-critical requirements.

Freedom from Interference

GEM systems can often be very large in scale, which is measured in lines of code for software. Sometimes such systems have mixed criticality, which means these systems combine safety critical functions and non-safety critical functions. The part of the system with functional safety requirements (safety critical) needs to be deterministic and reliable, while other parts of the system (non-safety critical) may need to be dynamic, connected and flexible. While these two design goals are very different, both must be satisfied. Therefore, the mechanism to support the design of systems with such mixed criticality becomes crucial. The QNX OS for Safety is based on the QNX Neutrino RTOS, which has a microkernel architecture that comes with the inherent ability to separate multiple domains spatially and temporally at the application level. This significantly eases the task of ensuring *freedom from interference* in systems with such mixed criticality. By adequately separating safety-critical and non-safety-critical domains, the design can be greatly simplified. A simpler design also leads to a simpler safety case, which translates, overall, into a lower certification effort.

Qualified Toolchains

IEC 61508 not only places requirements on the hardware and software that make up the system, but also demands proper qualification of the tools that are used to create the system. Tools are classified into various categories depending on the impact they have on the safety of the work product, ranging from tool confidence level T1 to T3, with T3 being the highest level. Understanding the importance of the toolchain correctness, the QNX OS for Safety includes the qualification of the C and C++ toolchain to T3. The C and C++ compiler, linker and assembler for the ARM and x86 architecture are crucial to the correct generation of the software that will run on the microprocessors in a safety-critical system. By taking on the qualification of these toolchains, BlackBerry QNX offloads this certification task from customers saving them valuable time and effort.

API Compatibility

The QNX OS for Safety is fully API-compatible with BlackBerry QNX's standard RTOS release. Version 2.0 of the product is compatible with QNX Software Development Platform 7.0. Developers who are already familiar with the standard RTOS require no ramp-up time when working with the safety-certified product, and can use the same QNX Momentics tool suite development environment to develop safety-critical systems. The API compatibility not only eases the learning curve for the development team, but also makes it possible for customers to leverage one common platform for safety-critical and non-safety-critical applications, thus maximizing code re-usage.

Technology

Product Package

The QNX OS for Safety includes software and documentation, all pre-certified to IEC 61508 SIL 3

Software

- QNX Neutrino RTOS microkernel, process manager with multicore support and adaptive partitioning technology
- POSIX compliant libc

Documentation

- IEC 61508 SIL 3 certificate, issued by TÜV Rheinland
- Safety Manual
- Installation and Usage Guide
- Safety Requirements document
- Hazard and Risk Analysis
- Safety Case
- Release Notes

Hardware Support

QNX OS for Safety is supported on the 32- and 64-bit ARM and x86 architecture. The product is enabled and tested on many popular hardware including Intel Apollo Lake and NXP i.MX 8. The product can be adapted to run on a customer's chosen hardware through BlackBerry QNX's experienced team of safety professionals and technical support experts.

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. This includes full software lifecycle management via secure over the air software updates. Founded in 1980, BlackBerry QNX is headquartered in Ottawa, Canada, with its products distributed in over 100 countries worldwide.

BlackBerry | QNX