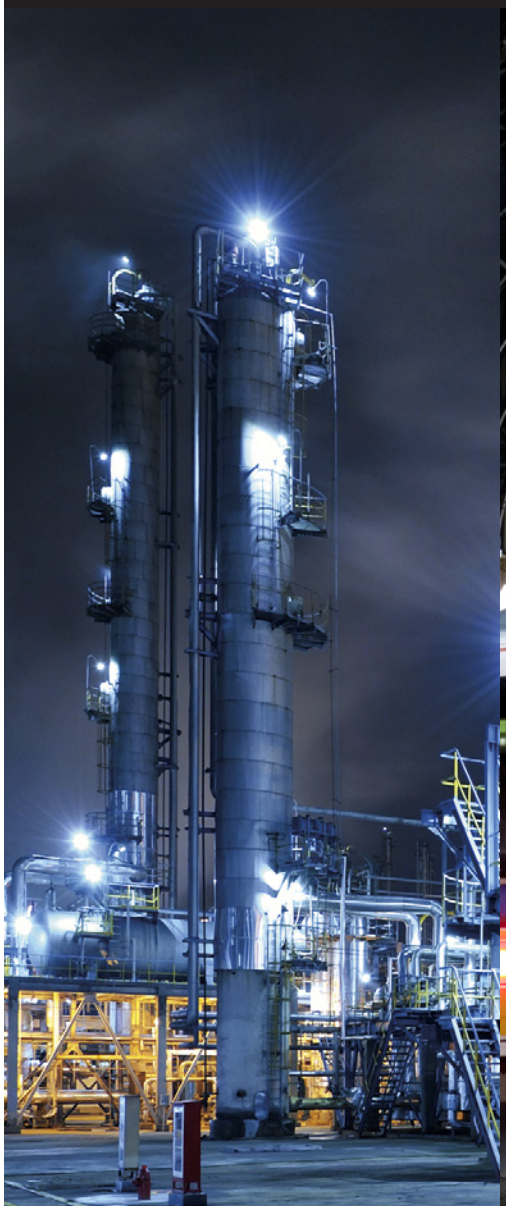
QNX
A Subsidiary of BlackBerry

PRODUCT BRIEF

QNX OS for Safety 1.0

General Embedded Systems



Functional safety is a key requirement in industries where real-time performance goals and mission-critical reliability is imperative. Achieving certification to functional safety standards brings a new dimension of challenges. To address these challenges the QNX® OS for Safety is designed specifically for industrial, railway transportation and robotic systems that are required to be compliant with functional safety standards, such as IEC 61508 and market-specific standards derived from it. The product has been pre-certified by a leading auditing firm, TÜV Rheinland, as a compliant item for use in systems up to IEC 61508:2010 SIL3.

Standards-compliant for mission-critical systems

The QNX OS for Safety is designed to meet the IEC 61508 functional safety standard and those market-specific standards derived from it including IEC 61511 for factory automation, process control, and robotics, EN 50128 for train control systems, IEC 62304 for medical diagnostics machines, and surgical equipment, and ISO 26262 for passenger vehicles.

IEC 61508 demands specific processes related to functional safety above and beyond what's found in standard quality management systems such as those overseen under ISO 9001. To comply with IEC 61508, a company must demonstrate the existence of the functional safety elements of the process and any development artifacts generated.

Mission-critical system pedigree and certification experience

Certification requirements can significantly increase the scope of a project, consuming more money and time. QNX Software Systems is a true expert in functional safety and certification, reducing certification risk and providing realtime operating systems for millions of mission critical field installations. The QNX OS for Safety has a fundamental architecture designed to maximize availability without compromising safety. Using a pre-certified component of key importance to the overall integrity of the system, especially when the component is the OS, can contribute to a greater level of safety and make overall system certification much easier.

Microkernel architecture for increased separation

The microkernel architecture inherent in the QNX Neutrino RTOS ensures that any system faults are contained so that it affects only the faulty component. Failed components can be restarted dynamically while the system continues to operate. QNX adaptive partitioning technology further safeguards the operation of the safety-critical components by ensuring they are never starved of CPU cycles. This microkernel architecture reduces the scope of certification as traditional OS services are now contained in separate, hardware-protected address spaces in the same manner as applications.

Ideal foundation for safety-critical components

The QNX OS for Safety underwent stringent evaluation and testing by TÜV Rheinland, providing comprehensive assurance of a platform that truly meets the IEC 61508:2010 compliance requirements. The target software, including QNX® Neutrino® microkernel and process manager (with multicore support and adaptive partitioning scheduler), libc, and an API identical to the QNX Neutrino standard RTOS has been certified as a compliant element. The certification also includes the qualification of the toolchain – the C compiler, linker, and assembler that is an essential part of the QNX® Momentics® Tool Suite. Classified as TCL 3, the tool chain has been certified to be compliant with the requirements for supporting tools according to IEC 61508.

	Project without Certification Requirements	Project with Certification Requirements
Developer Head Count	12 people	18 people
Key Activities Duration (lapse in time)		
System Design	5 weeks	8 weeks
Detailed Design	3 weeks	5 weeks
Coding	4 weeks	5 weeks
Testing	6 weeks	12 weeks
Certification	–	20 weeks
Total Budget	$1.2 M	$3 M
Project Duration	8 months	24 months

Figure 1: The certification requirement can significantly increase the scope of a project, consuming more time and money.
Source: QNX data validated with customers.

Product package

- Binaries and header files for microkernel, process manager and libc
- Safety manual
- Installation and usage guide

Optional offerings:

- Hazard and risk analysis
- Safety case

Note: The QNX OS for Safety must be installed on top of an existing SDP 6.5 SP1 development seat (not included).

Hardware support

- ARMv7
- x86

Certifications

- IEC 61508:2010
- ISO 26262:2011
- Certified by TÜV Rheinland

Professional Services:

Safety-focused training courses:

- Interpreting the Safety Manual
- Developing a Dependable Application

Professional services to assist with:

- System hazard and risk analysis
- Safety case construction
- On-site audit services
- Functional safety design consulting
- Certifiable BSPs

About QNX Software Systems

QNX Software Systems Limited, a subsidiary of BlackBerry, is a leading vendor of operating systems, development tools, and professional services for connected embedded systems. Global leaders such as Audi, Cisco, General Electric, Lockheed Martin, and Siemens depend on QNX technology for vehicle infotainment units, network routers, medical devices, industrial automation systems, security and defense systems, and other mission- or life-critical applications. Founded in 1980, QNX Software Systems Limited is headquartered in Ottawa, Canada; its products are distributed in more than 100 countries worldwide. **Visit www.qnx.com**

QNX
A Subsidiary of BlackBerry