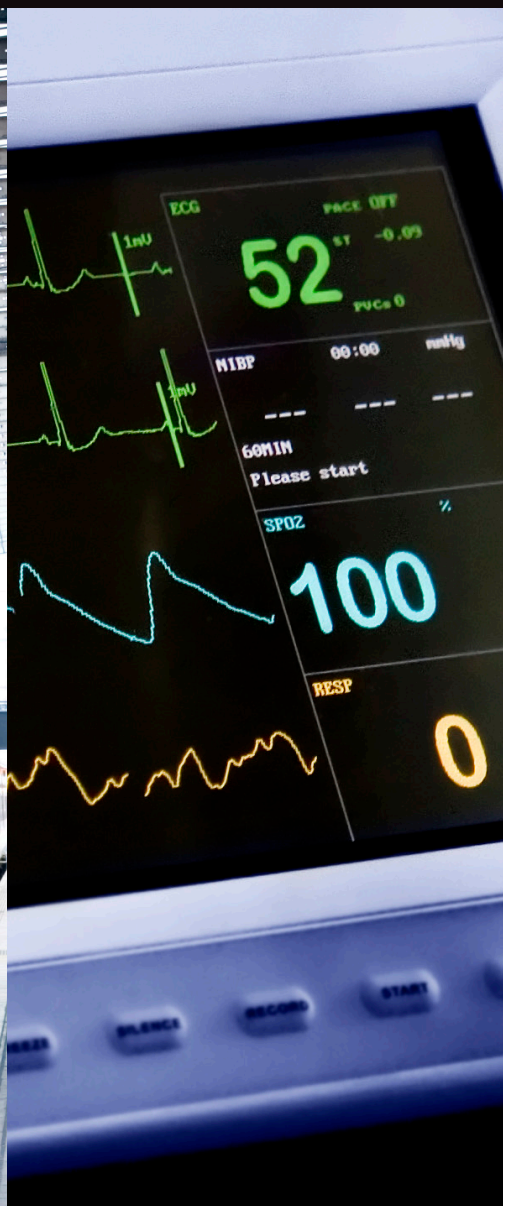
QNX | BlackBerry Subsidiary

PRODUKTÜBERSICHT

QNX OS for Safety 1.0

für eingebettete Systeme



In Branchen, die auf Echtzeitfähigkeit und betriebskritische Zuverlässigkeit angewiesen sind, ist funktionale Sicherheit ein zentrales Thema. Die Zertifizierung nach den entsprechenden Normen bringt eine ganz neue Dimension von Herausforderungen mit sich. Das QNX OS for Safety ist die Antwort auf diese Herausforderungen. Es ist speziell für industrielle Systeme, Eisenbahnsysteme und Robotiksysteme ausgelegt, die Normen für funktionale Sicherheit erfüllen müssen – wie die IEC 61508 und davon abgeleitete marktspezifische Normen. Das QNX OS for Safety wurde vom TÜV Rheinland als konforme Komponente zur Verwendung in Systemen bis zu IEC 61508:2010 SIL 3 vorzertifiziert.

Normkonform für betriebskritische Systeme

Das QNX OS for Safety wurde mit dem Ziel entwickelt, die Anforderungen der Norm IEC 61508 für funktionale Sicherheit zu erfüllen und damit auch die von abgeleiteten, marktspezifischen Normen wie die IEC 61511 für Fabrikautomation, Prozesssteuerung und Robotik, die EN 50128 für Zugsteuerungssysteme, die IEC 62304 für medizinische Diagnose- und OP-Technik und die ISO 26262 für Personenkraftwagen.

Die IEC 61508 verlangt spezielle Prozesse für funktionale Sicherheit und geht über die Anforderungen etwa der ISO 9001 an Standard-Qualitätsmanagementsysteme weit hinaus. Ein Unternehmen, das die IEC 61508 erfüllen will, muss in seinen Prozessen und allen Entwicklungs-Artefakten die Existenz von Elementen für funktionale Sicherheit nachweisen.

Lange Tradition mit betriebskritischen Systemen

Sind Zertifizierungen erforderlich, kann dies den Projektrahmen wesentlich vergrößern und viel Geld und Zeit verschlingen. QNX Software Systems ist spezialisiert auf funktionale Sicherheit und Zertifizierung. QNX-Lösungen senken das Risiko bei der Zertifizierung, und die Echtzeit-Betriebssysteme von QNX sind millionenfach in betriebskritischen Applikationen im täglichen Einsatz. Die grundlegende Architektur des QNX OS for Safety ist dafür ausgelegt, die Verfügbarkeit zu maximieren – ohne Kompromisse bei der Sicherheit. Die Nutzung einer vorab zertifizierten Komponente an einer Schlüsselposition im System trägt zu mehr Sicherheit bei und vereinfacht die Zertifizierung des Gesamtsystems deutlich – besonders wenn es sich bei dieser Komponente um das Betriebssystem handelt.

Microkernel-Architektur für bessere Trennung

Die Microkernel-Architektur des QNX Neutrino RTOS schottet Systemkomponenten gegeneinander ab. So wird die Auswirkung eines Fehlers auf die Komponente beschränkt, in der er auftrat. Ausgefallene Komponenten können dynamisch neu gestartet werden, während das System weiterarbeitet. Des Weiteren sichert die QNX-Technologie für adaptive Zeitpartitionierung die Funktion der sicherheitskritischen Komponenten zusätzlich, indem sie dafür sorgt, dass ihnen nie die CPU-Zyklen ausgehen. Diese Microkernel-Architektur reduziert den Umfang der Zertifizierung, weil traditionelle Betriebssystemdienste jetzt auf gleiche Weise wie Applikationen in abgetrennten Adressräumen voneinander abgeschottet sind, die per Hardware geschützt werden.

Ideale Grundlage für sicherheitskritische Komponenten

Das QNX OS for Safety hat eine strenge Untersuchung und Prüfung durch den TÜV Rheinland durchlaufen. Diese hat bestätigt, dass die Plattform allen Konformitätsanforderungen der IEC 61508:2010 voll genügt. Die geprüfte Software – der QNX® Neutrino® Microkernel mit Prozessmanager (inkl. Multicore-Unterstützung und Scheduler mit adaptiver Zeitpartitionierung), die libc sowie eine API identisch mit der des QNX Neutrino Standard-RTOS – hat die Zertifizierung als konformes Element erlangt. Auch die Toolchain – C-Compiler, Linker und Assembler als zentraler Bestandteil der QNX® Momentics® Tool Suite – wurde im Rahmen der Zertifizierung qualifiziert. Sie wurde als TCL 3 klassifiziert und ist als konform mit den Anforderungen für unterstützende Tools gemäß IEC 61508 zertifiziert.

	Projekt ohne Zertifizierungserfordernis	Projekt mit Zertifizierungserfordernis
Anzahl Entwickler	12	18
Dauer zentraler Aktivitäten		
Systemdesign	5 Wochen	8 Wochen
Detailliertes Design	3 Wochen	5 Wochen
Programmieren	4 Wochen	5 Wochen
Tests	6 Wochen	12 Wochen
Zertifizierung	–	20 Wochen
Gesamtbudget	1,2 Millionen US-$	3 Millionen US-$
Projektdauer	8 Monate	24 Monate

Abbildung 1: Ist eine Zertifizierung erforderlich, kann dies den Projektrahmen wesentlich vergrößern und viel Geld und Zeit verschlingen.
Quelle: mit Kunden gegengeprüfte Daten von QNX.

Produktpaket

- Binaries und Header-Dateien für Microkernel, Prozessmanager und libc
- Sicherheitshandbuch
- Installations- und Benutzerhandbuch

Optionale Zusatzangebote:

- Gefahren- und Risikenanalyse
- Safety Case

Hinweis: Das QNX OS for Safety muss über eine vorhandene SDP 6.5 SP1 Entwicklerlizenz installiert werden (nicht enthalten).

Unterstützte Hardware

- ARMv7
- x86

Zertifizierungen

- IEC 61508:2010
- ISO 26262:2011
- Zertifiziert vom TÜV Rheinland

Dienstleistungsangebote

Trainingskurse zum Thema Sicherheit

- Interpretieren des Sicherheitshandbuchs
- Entwickeln verlässlicher Applikationen

Professionelle Unterstützung durch:

- Gefahren- und Risikenanalyse
- Aufbau eines Safety Case
- Audit vor Ort
- Designberatung unter Aspekten der funktionalen Sicherheit
- Zertifizierbare Board Support Packages

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.com

QNX | BlackBerry Subsidiary