certicom | BlackBerry Subsidiary

MANAGED PUBLIC KEY INFRASTRUCTURE (PKI) HOSTING SERVICES

MANAGING DIGITAL CERTIFICATES TO BECOME MORE RELIABLE, SECURE, AND TRUSTED

Off-load labour, reduce expense, and harden overall security.

Certicom is a recognized leader in public key infrastructure (PKI) security design, innovation, and delivery.

PKI is a foundational technology that has become the cornerstone of real world security across the internet, mobile, medical, financial, government, military, consumer, automotive, industrial, IoT, and just about every application that communicates information electronically.

Because Certicom solutions are resource optimized, certified, and practical, it is easy to obtain world class security and protect manufacturing supply chains to enhance revenue, increase profit, and protect brand equity.

Certicom's government validated crypto libraries, PKI certificate solutions, and asset management solutions make products, ecosystems, and manufacturing chains not just secure, but BlackBerry Secure.

CONFIDENTIALITY. INTEGRITY. AUTHENTICITY.

Most modern security systems are based on public key infrastructure, which uses digital certificates that must be managed carefully.

Certicom's PKI certificate hosting services are proven by a user known worldwide for high security and high volume, BlackBerry.

OFFLOAD YOUR PKI CERTIFICATE MANAGEMENT TO THE PROVEN HIGH VOLUME SECURITY EXPERT

Certicom helped make BlackBerry the iconic mobile security platform.

With PKI, authentication is enforced via digital certificates to provide very high levels of security. Certicom's managed PKI system was initially created for BlackBerry mobile devices, which speaks to both high security and large scale credibility.

The Certicom certificate management system performs four essential functions:

Managed PKI Services

- **ISSUE:** Automatically issue certificates to validated devices
- **MANAGE:** Track all of the issued certificates
- **RENEW:** Automatically renew active devices
- **REVOKE:** Disable certificates of lost or decommissioned devices

BENEFITS OF MANAGED PKI SERVICES

1 **Scaleable:** Originally created for BlackBerry mobile devices.

2 **Simple:** Off-loads security system design and operations.

3 **Risk reduction:** PKI based crypto is effective against attacks.

4 **Reliable:** Automated data back up and disaster recovery.

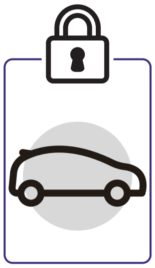
5 **Robust:** PKI is stronger than legacy password and symmetric keying methods. Security is protected by hardware security modules (HSMs).

6 **Lowers cost:** reduces/eliminates development and labor costs associated with in house approaches.

7 **Legacy support:** RSA available.

8 **Vetted:** Trusted vetting system verifies all certificate requests. On demand or fully automated bulk certificate issuance models are available.

EXAMPLE USE CASE: SECURING THE CAR & AUTOMOTIVE SUPPLY CHAIN



When it comes to embedding security into the autonomous connected car, it has to start with securing the supply chain, while making both in-car networks and external automotive infrastructure impervious to attacks. Automotive security is an inside, outside, and supply chain proposition with many requirements, for example:

- Security assets (i.e. crypto keys, serial numbers, etc.) must be installed into devices at manufacturing time
- Devices must be distributed to, and be installed into vehicles in globally located factories
- Devices must be warehoused worldwide for subsequent repairs
- Secure devices must be updateable at dealers and repair shops
- Aftermarket suppliers must be able to sell and update secure devices

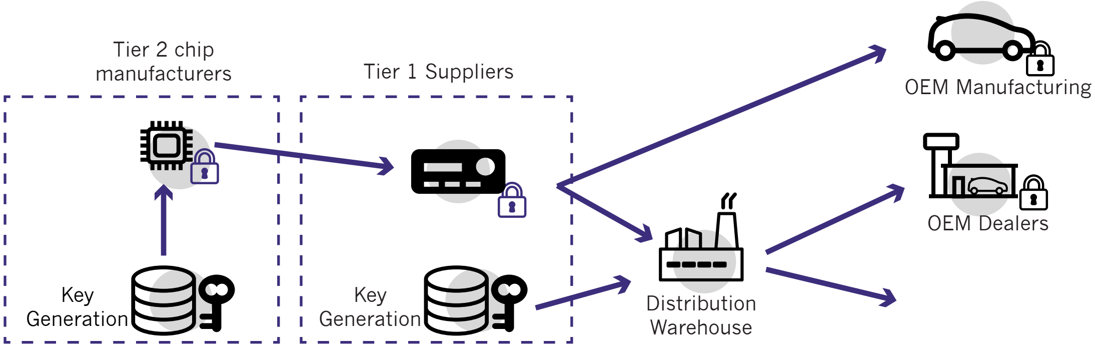
These requirements present a logistical tangle. Making a device such as a networked ECU on a CAN bus secure means that it will become one of a kind. This is the entire objective of personalization. However, by definition that device cannot be used anywhere else. It becomes a unique stock keeping unit (SKU), which is averse to the purpose of flexible, just in time manufacturing flows. Security versus flexibility is a serious trade off that must be managed carefully.

High profile automotive hacks have shown the world that automotive security is necessary, but it is difficult to apply, especially because it makes manufacturing more difficult and costly. Because security must be injected in the factory and beyond, a secure manufacturing system must have global reach, be manageable on a distributed basis, be updatable by various entities, and remain secure for years. Secure manufacturing, including injection and updating of security assets, will touch factories, warehouses, distributors, dealers, repair shops, and aftermarket parts stores. In addition, security updates will increasingly be over the air.

To maintain the maximum amount of flexibility, personalization and updating should be moved as close as possible to the very last minute. Each car maker will be faced with the same situation and will have to design and manage secure device manufacturing systems, security certificate management systems, and secure updating (OTA) systems that are global and long term in nature. **Fortunately, the tools to do that are available from Certicom; namely, the Managed PKI System and Asset Management System**. The way in which these systems get deployed will have to be designed to the specific logistical and security needs of the manufacturer. Therefore, the overall manufacturing blueprint must be designed with best practices in mind, right from the start, and BlackBerry Professional Services and help with that. Also, in-car and around the car security systems can be developed using Certicom's cryptographic libraries and architectural consulting services; and can be updated using BlackBerry's secure over the air (OTA) hosting service.

Blackberry brings it all together.

GLOBAL SECURE MANUFACTURING BLUEPRINT



CRYPTOGRAPHY BECOMING THE NEW SEATBELT

The evolution of the car into an electronic platform started with cockpit electronics and branched into safety and locomotion, giving rise to Electronic Control Units (ECUs). ECUs are little computers that intelligently control physical things like mirrors, lights, seats, AC, etc. in the body or cockpit; and provide better engine control, body and chassis electronics control, and other things that improve performance and safety. Cars today can have well over 100 ECUs, which can be a challenge to make truly secure. Fortunately, that is changing. Multi-core processor technologies are being harnessed to consolidate ECUs into a smaller number of powerful domain-controllers. A hidden benefit of the shift to domain controllers is that they lend themselves to being secured by modern cryptography. That is because they can run algorithms faster and store crypto keys more securely. Also, fewer controllers means fewer points for attack. In a connected autonomous car, safety comes from security, and security comes from cryptography. Because attacks can come from anywhere, at any time, and on any system, automotive security must be multi-layered, meaning everything has to have some sort of cryptography to protect from attackers.

Security awareness should start right at the beginning of design with disciplines such as penetration testing of the software and security audits to find vulnerabilities. These should be applied inside and outside of the car.

Once you have a good start you need to ensure a good ending, which means security updates, and that typically means over the air.

In between the beginning and the end there should be secure manufacturing and secure distribution of crypto keys and certificates. BlackBerry can help with all of that via security design and testing, OTA hosting, QNX's microkernel based RTOS, and Certicom's technologies for securing the supply chain and managing security certificates.

By now you can see that by providing the first line of defense for personal safety, cryptography is becoming like the new seatbelt.

ANCHORING TRUST IN THE SOFTWARE-DEFINED CAR

ECUs started out as discrete items that did one thing, but quickly became connected via in-car networks. Being networked means that they became vulnerable and should be secured cryptographically to ensure that the signals being sent have not been tampered with or corrupted. Connected cars are now targets for hackers, and ECUs represent a major part of the attack surface. The list below shows the top 15 attack points, which indicates just how vulnerable cars have become.

- Passive keyless entry
- Remote link app
- DSRC Receiver (V2V)

- Steering and braking ECU
- Engine and transmission ECU
- Airbag ECU
- Lighting ECU
- Vehicle access system ECU
- OBD II
- USB
- Bluetooth
- Smartphone

With a car having so many places to attack, how can trusted security be implemented?

Trust leads to safety

Trust is paramount in digital systems, especially automotive, and it comes from cryptographic solutions that:

- Securely store secret keys
- Securely issue, manage, renew, and revoke security certificates
- Include a mix of software and security hardened hardware devices, and
- Are manufactured in highly secure facilities

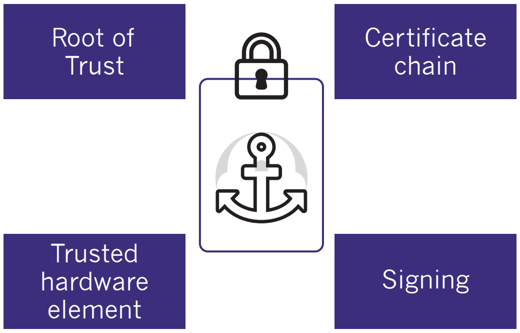
A major tenet of security is that each system and sub-system will have different types of threats and a range of options to provide countermeasures to those. However, two things are always common to cryptographic security: 1) a proven algorithm (e.g. ECC), and 2) a secret cryptographic key.

The challenge for the automaker is to choose the right algorithm and key length for the available processing resources, and to securely issue, manage/store, renew, and revoke digital certificates. Cryptographic strength comes from that. On a CAN bus, which was designed without security in mind, ECUs are exposed. That must change. Cars should employ best practices for security, but cost, complexity (especially of the supply chain), and time get in the way. Having said that, best practices will eventually prevail and we think that will include a hardware trust anchor system to establish, maintain, and update cryptographic processes.

From the diagram you can see the four things that create a PKI-based hardware trust anchor:

1) A trusted hardware anchor that stores the key
2) That key, which becomes the root of trust
3) The certificate chain anchored by the root of trust, and
4) A signing mechanism that creates the anchored certificate chain.

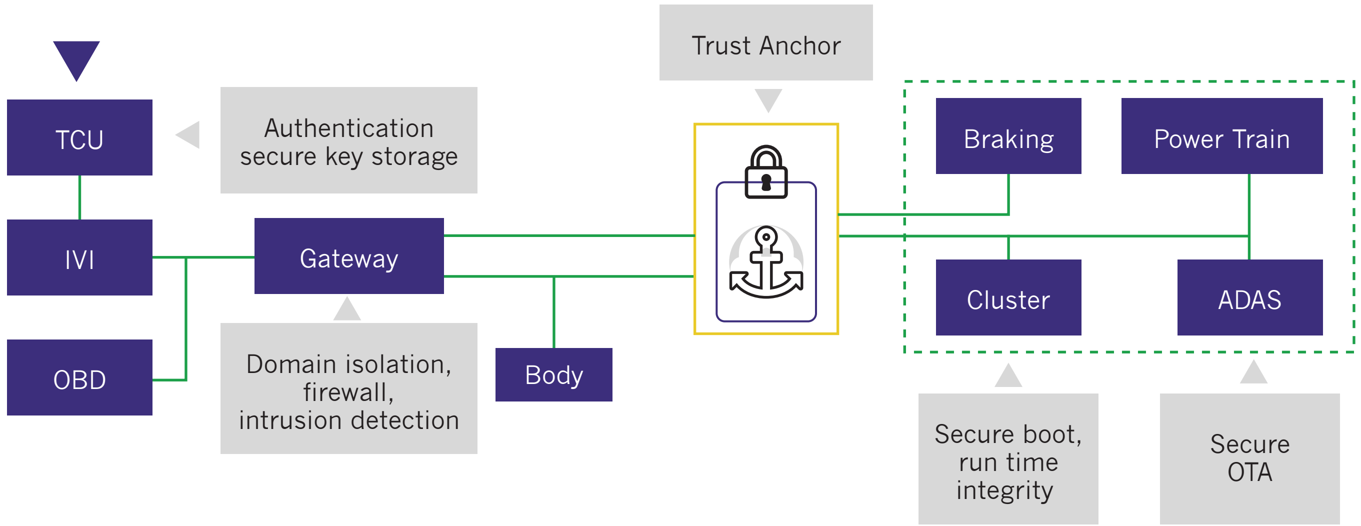
Trust Anchor



Multi-Level Security

Because there are so many systems in the increasingly software-defined car, security has to be multi-layered and fit the specific application. In other words, it must be tailored. You have to figure out what you are securing, what threats that system will face, and what countermeasures should be employed. You have to pick what pillars of security to apply; namely, confidentiality, data integrity, and authentication. Making sure you are doing the right security things on each system is what Blackberry is positioned to help you with, from consulting, to design, testing, certificate management, securing the supply chain, making updates, and applying cryptography to the in-car and around the car networks.

MULTI-LEVEL SECURITY


Trust Anchor
TCU
Authentication secure key storage
IVI
Gateway
OBD
Domain isolation, firewall, intrusion detection
Body
Braking
Power Train
Cluster
ADAS
Secure boot, run time integrity
Secure OTA

Blackberry Secure OTA

BlackBerry and Certicom are combining cryptographic and connectivity expertise to create innovative solutions that now include the BlackBerry secure over the air (OTA) software update management service. This fully hosted, globally scalable service securely establishes a cryptographic root of trust, provisions devices, performs authentication, and securely makes software updates via easy to use web based tools. The service actively monitors, logs, and analyses the threat profile and can deploy incidence response teams to ensure rapid containment and continuity. This combination of endemic capabilities makes security provisioning and updating reliable, secure, and trusted.

BLACKBERRY OTA SECURITY - END TO END

Device Provisioning

- Certicom
  - Silicon asset management (AMS)
  - X.509 certificates
- QNX OS
  - QNX layered security
  - Secure boot
  - Access control
  - Intrusion detection
  - Etc...

Authentication

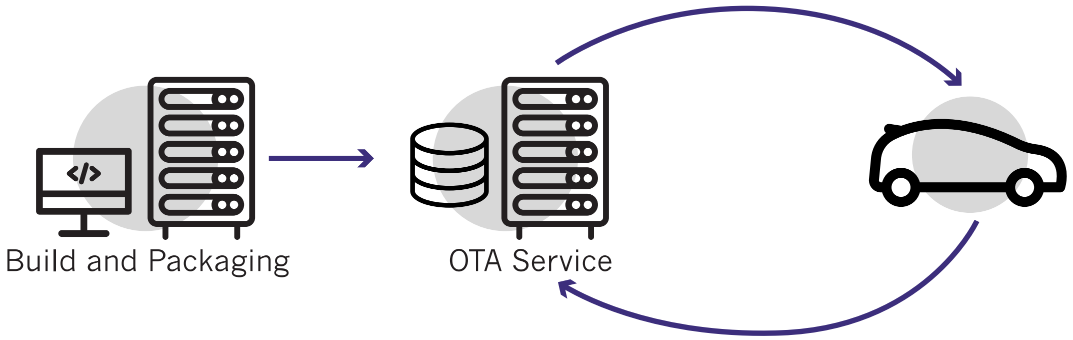
- Certicom
  - Root certificate authority to verify vehicle certificate
  - Certificate issuing, management, renewal, & revocation (Managed PKI Services)
- Device and User Auth Flows
  - Mutual Authorization
  - OAuth 2.0
  - Permissions firewall
- Service token
  - AES 256
  - Token Revocation

Secure Data Transmission

- TLS 1.2 encrypted data channels
- ECDSA 521 bit packet signing
- Strong hash on package contents
- Signed manifests
- Forward secrecy so historical packages cannot be decrypted

Threat Response

- 24/7/365 monitoring of applications, infrastructure and services
- Proactive penetration testing
- Incidence response teams
- Threat containment
- Global redundancy
- Security consulting



EXAMPLE USE CASE: ZIGBEE SMART ENERGY

Simple provisioning and installation for a robust wireless ecosystem.

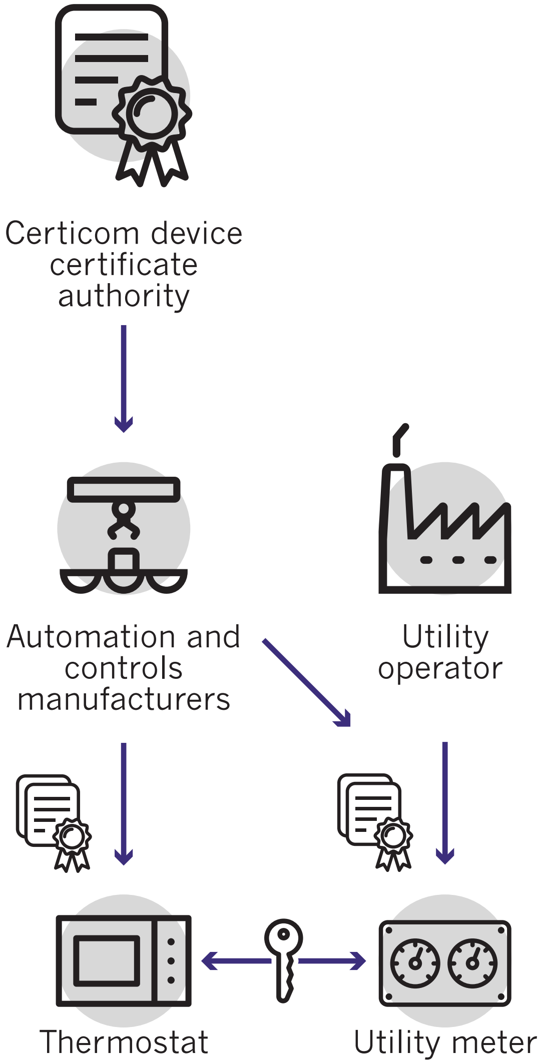
Out-of-box interoperability makes it easy to manage ZigBee Smart Energy device certificates.

In a smart energy system, a certification authority (CA) securely stores the trusted (private) key, which signs the certificate data in the thermostat, meter, or another communicating network node. The certificate data contains Vendor IDs and the unique MAC (Media Access Control) address.

Binding public-private key pairs via a trusted signature to the device's MAC address and vendor IDs (e.g. dates, times, manufacturing ID, etc.) is used to authenticate the IDs and uniqueness of the MAC address. Once the vendor ID, Mac address, and public key (all of which together comprise certificate data) are signed by the certificate authority, the certificate is issued.

Certificates contain the identities of nodes, MAC addresses, signatures and the signers' public keys. The certificate authority acts as the root of trust and ultimate signer. Certificates are used to authenticate the nodes by using an algorithmic process based upon Elliptic Curve Cryptography (ECC). Certicom issues, manages, renews, and revokes certificates as specified by the ecosystem provider.

Certificates are issued in batch mode (up to approximately 1 million certificates per hour) and certification can be controlled to apply to ZigBee Smart Energy certified devices only.


Certicom device certificate authority
Automation and controls manufacturers
Utility operator
Thermostat
Utility meter

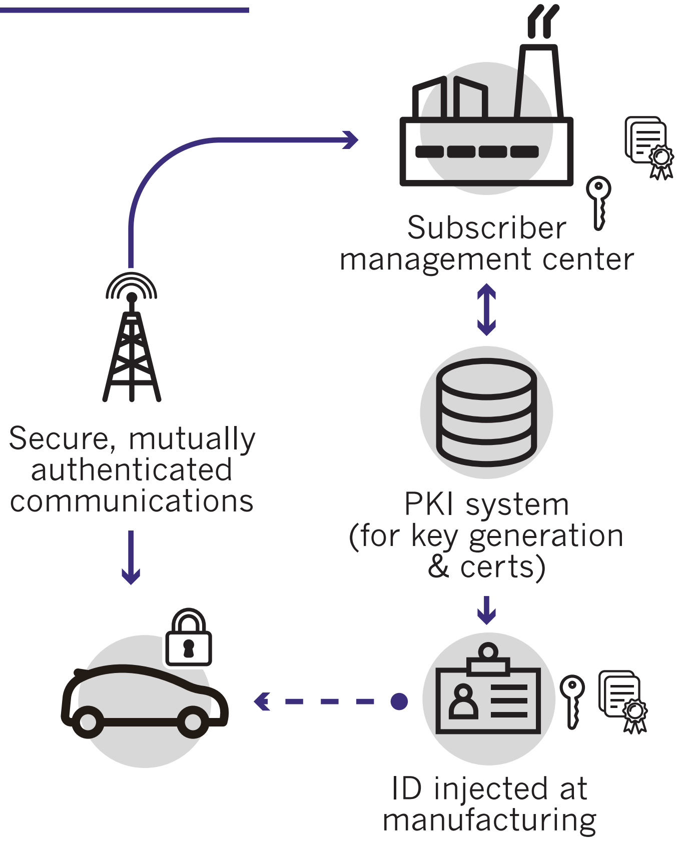
EXAMPLE USE CASE: SATELLITE RADIO KEY INJECTION

Secure conditional access management via digital certificates.

Satellite radio is a classic example of a subscriber-based conditional access system.

The success of satellite radio has meant that there are millions of subscribers and hundreds of specialized channels.

Certicom provides a complete security solution including consulting, security architecture, custom design, and custom implementation, including firmware, middleware, and key provisioning.


Subscriber management center
Secure, mutually authenticated communications
PKI system (for key generation & certs)
ID injected at manufacturing

3RD PARTY MANAGED CERTIFICATE SERVICE

For high volume device makers.

Certificate issuance and validation is conducted on-line, using the highly scalable BlackBerry PKI architecture and code base, which helps OEMs secure device identities and enforce ecosystem certification requirements.

Secure device identities are established for small cell base stations, telematics, and other Machine to Machine (M2M) applications. The service can be augmented with the Certicom Asset Management System (AMS) for product identity provisioning and secure manufacturing.

This service enforces ecosystem certification and security robustness rules, for example for ZigBee and Wi-Fi Alliance. Managed PKI services solve the problem of sensor networks by being inherently scalable, using the most advanced authentication algorithms (e.g. Elliptic Curve Cryptography), storing/managing root keys, and distributing keys and certificates in a very efficient manner.

RELIABLE, SECURE, AND TRUSTED

There is a reason that BlackBerry is synonymous with mobile security. It is because security is as elemental to an electronic system as DNA is to an organism–and security is BlackBerry's DNA.

Robust security cannot just be bolted on. It must be infused right from the start, which is why BlackBerry Security has been trusted by world leaders for over two decades and is the mobility partner of all G7 governments, 16 of the G20 governments, 10 out of 10 of the largest global banks and law firms, and the top five largest managed healthcare, investment services, and oil and gas companies. BlackBerry Security has earned more than 70 government certifications and approvals, which is greater than any other mobile vendor.

The iconic example of the depth of trust in BlackBerry Security is probably the NSA's licensing (and standardizing) of Certicom's Elliptic Curve Cryptography (ECC) algorithms, which are quickly becoming the accepted crypto standard for enterprise, government, automotive, mobile, medical, industrial, and IoT security.

Vulnerabilities are growing rapidly and present a serious risk for public and private sector organizations, so BlackBerry continues to expand its coverage with advanced technologies, tools, design consulting, and testing services for true end-to-end, layered security.

In mobile, coverage begins at the crucial hardware root of trust. OS and software authenticity is securely verified every single time any BlackBerry device in the world boots up. Data is encrypted right on the devices, in the trusted network, and behind the corporate firewall. In operating systems, the BlackBerry-QNX Neutrino microkernel ensures safe, secure, and reliable operation robust enough for over 60 car models, the space shuttle, and nuclear plants. It is designed to fail safe, and protect against malware, tampering, and data leakage. Thanks to Certicom's Security Builder Software Libraries, certificate management solutions, and secure manufacturing systems, it is easy to obtain government approved (FIPS 140-2 Level 1) validation, manage security certificates, and secure manufacturing lines without becoming a crypto expert.

BlackBerry and its subsidiaries, Certicom and QNX, provide products and services that make things Reliable, Secure, and Trusted.

Certicom Corp., subsidiary of BlackBerry manages and protects the value of content, applications, and devices with government-approved security. Elliptic Curve Cryptography (ECC) provides the most security-per-bit of any known public key scheme. As the global leader in ECC, Certicom has licensed its security offerings to hundreds of multinational technology companies, including IBM, General Dynamics, and SAP. Founded in 1985, Certicom's corporate office is located in Mississauga, Ontario, Canada.

www.certicom.com

QNX Software Systems Limited, 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.

www.qnx.com