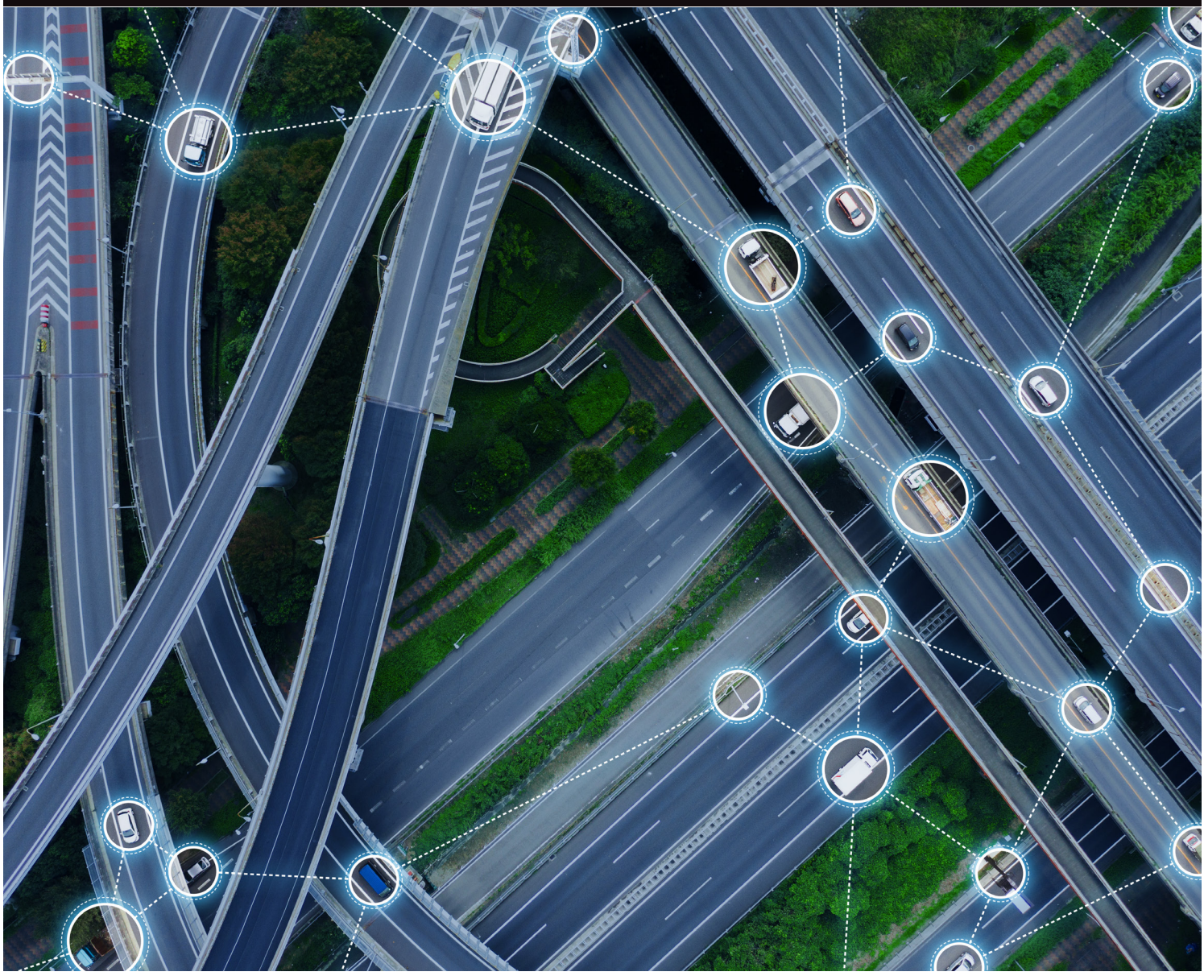
BlackBerry | QNX

PRODUCT BRIEF

QNX® Black Channel Communications Technology

Functionally safe data communication pre-certified to ISO 26262 ASIL D



Most embedded systems are connected and have many nodes of communication which can put the safety of the system at risk. To make data communication functionally safe, and reduce the scope and complexity of certifying these systems, BlackBerry® QNX® has developed a pre-certified data communications solution that leverages a Black Channel approach.

QNX Black Channel Communications Technology, certified to ISO 26262 ASIL D, encapsulates the data being exchanged and performs essential safety checks to validate it at both ends. This solution protects data communication from systematic software faults, random hardware faults and transient faults and helps in the automatic prevention of damages from these failures, all with minimal impact on system performance. When paired with a safety-certified RTOS, like the QNX® OS for Safety, certification scope and cost can be greatly reduced.

Functionally Safe Communication

For data communication to be considered functionally safe, there must be an automatic prevention mechanism of accidents from random faults or data corruption, whether from internal or external interference.

Ideally this prevention mechanism does not require software updates or changes to the system after it has been deployed. IEC 61508-2 has data communication requirements to ensure safe data communications within a system. These requirements can be met with two approaches: white channel or black channel.

- White Channel requires that any hardware and software involved in information exchange must meet industry-specific safety standards. This expands the scope of safety certification and makes development more expensive, time consuming and burdensome especially if you plan to use the same network hardware or software for safety and non-safety elements.
- Black Channel handles safety at the application level by adding a safety layer to the application data. This means that the functional safety standard development and certification is limited to the safety layer. The network layer can be standard components and can be excluded from the certification. This approach provides reliable data transmission and consumption but is less time consuming to develop and network and communications components can be used for mixed criticality systems.

QNX Black Channel Communications Technology is a Safety Element out of Context (SEooC) pre-certified to ISO 26262 ASIL D and can be certified to other standards, including IEC 61508 and IEC 62304.

QNX Black Channel Communications Technology provides safety checks for:

- Data integrity
- Data reliability
- Fault detection
- Data authentication of identity and origin

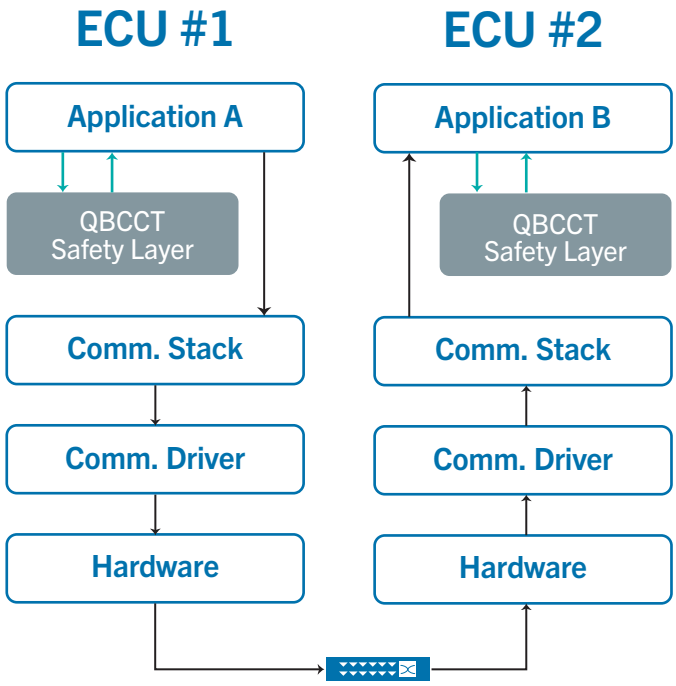


Figure 1: Architecture overview showing how QNX Black Channel Communications Technology will protect data communication between two ECUs

Fault Detection

QNX Black Channel Communications Technology uses the application or the Inter Process Communication (IPC) middleware to generate a safety header and encapsulate the data payload within a safety frame.

This solution detects a variety of faults including:

- Incorrect message addressing
- Data insertion
- Data corruption
- Data masquerade
- Data repetition
- Asymmetric data
- Invalid message sequencing
- Data loss

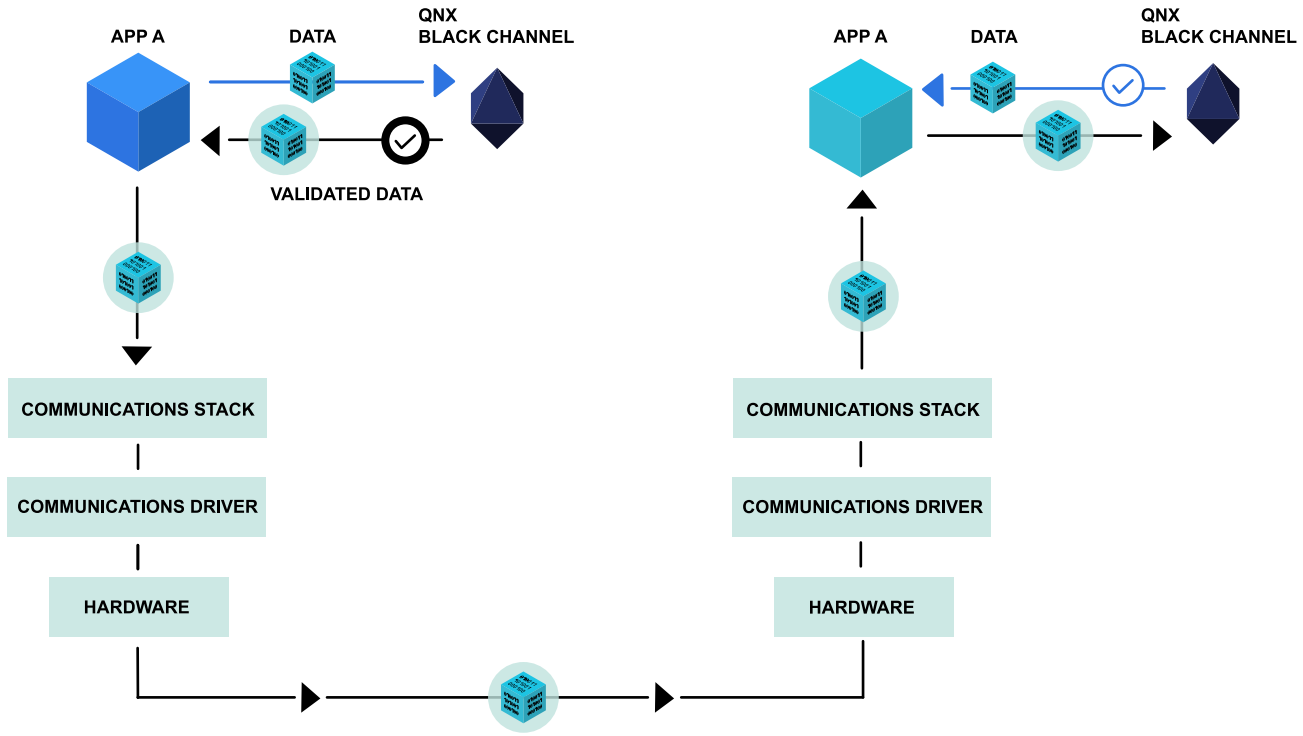


Figure 2: QNX Black Channel Communications Technology processes the data prior to transmission or consumption on the receiver side. The application or IPC makes a call for QNX Black Channel Communications Technology to perform integrity, fault detection and authentication checks and encapsulate/decapsulate the data.

Communication Efficiency for Safety-Critical Systems

QNX Black Channel Communications Technology is a lightweight process that requires minimal computing resources to execute and supports the bandwidth required of safety-critical systems. QNX Black Channel Communications Technology takes at most 0.03 milliseconds to process one message (4KB). For example, for a typical 4 KB message on 2.0 GHz processor using Secure Hash Algorithm (SHA) 512, the QNX Black Channel Communications Technology will process at a minimum 30,000 messages per second. Performance was also tested against AUTOSAR profiles and performance was approximately 2-3 times faster.

QNX Black Channel Communications Technology can be used on either regular systems or safety-certified systems and is compatible with OSs such as QNX® Neutrino® RTOS, Linux® and SafeRTOS.

Specification	Profile	CRC/HMAC
AUTOSAR SW-C E2E	1	CRC8
	4	CRC32
	6	CRC16
	7	CRC64
Custom	17	HMAC (SHA 256)
	17	HMAC (SHA 512)

Table 1: QNX Black Channel Communications Technology supports a broad range of specifications and profiles.

About BlackBerry® QNX®

BlackBerry QNX is a leading supplier of safe, secure, and trusted operating systems, middleware, development tools, and engineering services for mission-critical embedded systems. BlackBerry QNX helps customers develop and deliver complex and connected next generation systems on time. Their technology is trusted in over 150 million vehicles and more than a hundred million embedded systems in medical, industrial automation, energy, and defense and aerospace markets. Founded in 1980, BlackBerry QNX is headquartered in Ottawa, Canada and was acquired by BlackBerry in 2010.

BlackBerry | QNX