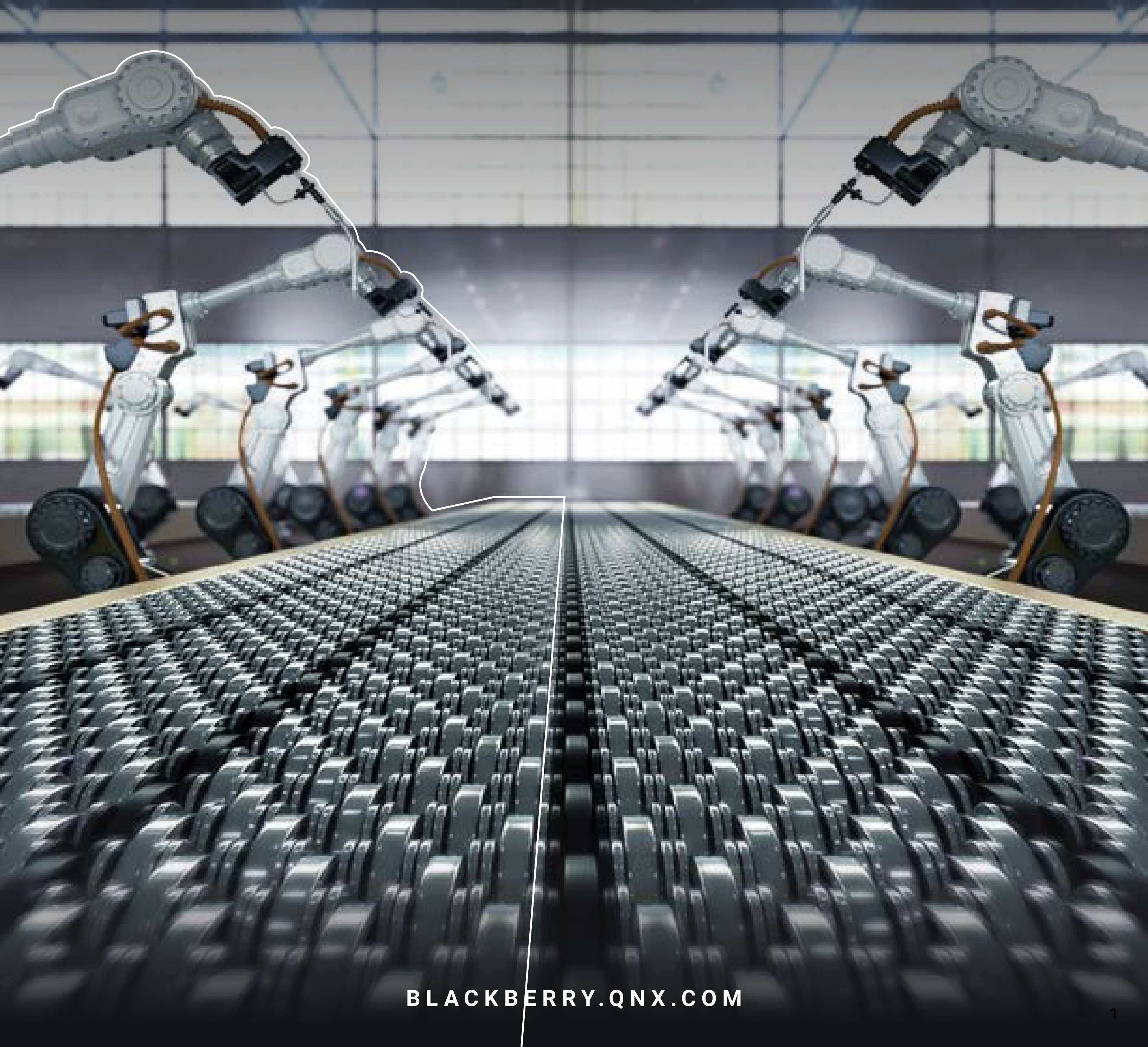
BlackBerry | QNX

FOUNDATIONAL SOFTWARE SOLUTIONS FOR

ROBOTICS AND AUTOMATION



BLACKBERRY.QNX.COM

THE FUTURE IS ROBOTICS

Industrial robots … have the potential to liberate skilled worker to focus on more complex tasks.

Mega Online, “Rise of the Cobots”

Combining advanced robotics with other technologies, process enhancements, and structural layout changes can yield savings of up to 40%.

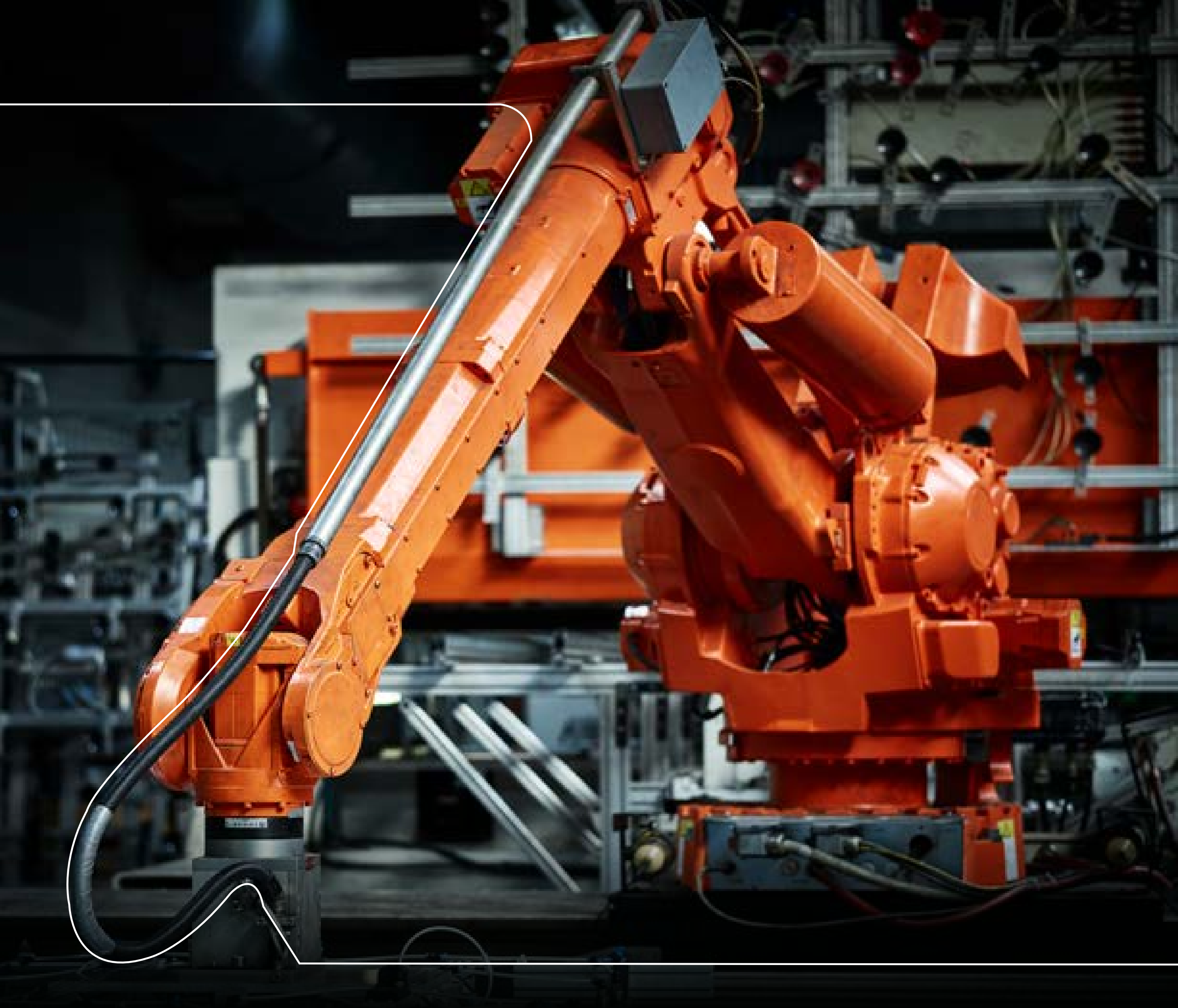
Boston Consulting Group, “Advanced Robotics in the Factory of the Future”

By using off-the-shelf components where possible to complement parts designed in-house, Odense firms can quickly assemble industrial robots with specialist applications and put together complete, working systems that meet clients’ needs.

Mega Online, “Rise of the Cobots”

Automation will add $800 billion to US Gross Domestic Product (GDP) by 2024, and potentially $12 trillion by 2035.

ARK Invest, “Big Ideas 2020”



Currently, it is estimated that 10% of manufacturing tasks are performed by robots, a figure that could rise to 25% by 2025.

Trendsformative, “Industrial Robots: The Start of a Megatrend”

The funding environment is the strongest it has ever been. On the eve of the COVID-19 pandemic, the robotics ecosystem is in a strong position to weather economic hardship, and retains significant backing from outside investors.

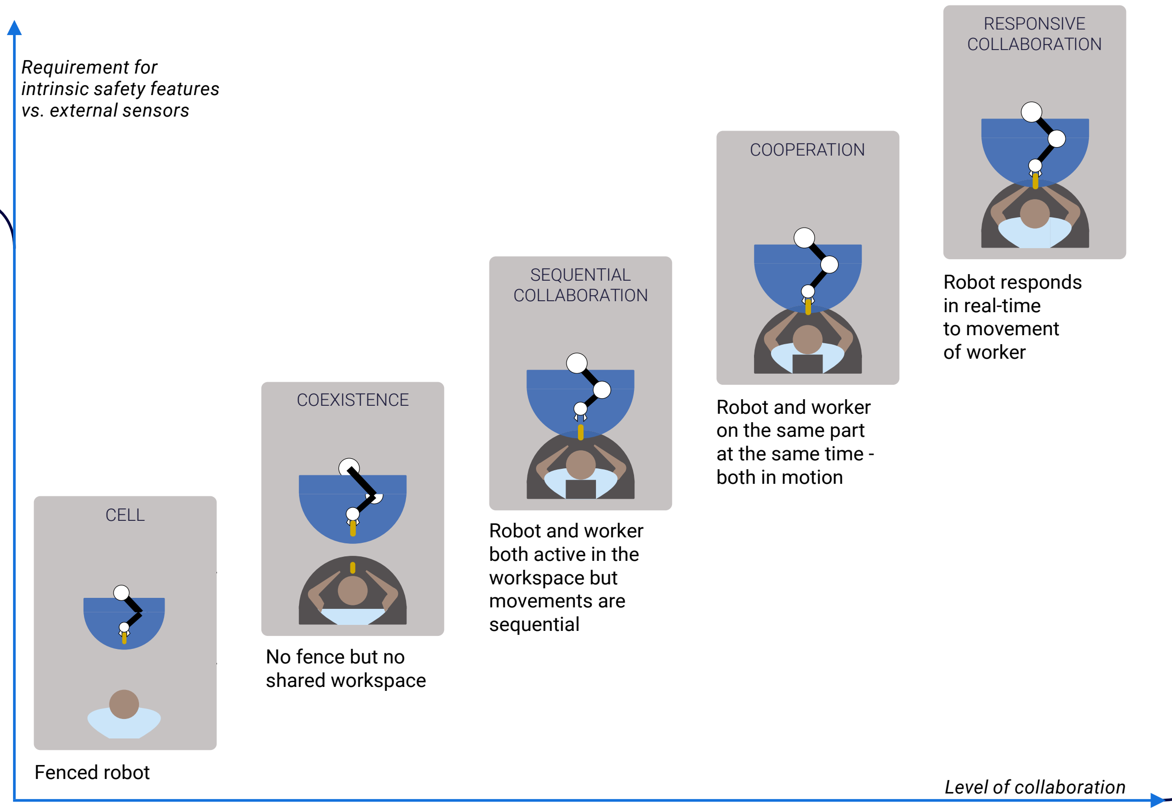
ABI Research, “Robotics: Investments, Acquisitions, and Market Trends for 2019”

INDUSTRY TRENDS & CHALLENGES

Robotics includes everything from ultra-high precision medical devices to gantries in factories and warehouses, autonomous home vacuum cleaners, and beyond. Thanks to advances in embedded hardware and software, there are few domains where robotics systems aren't already essential, and new possibilities are constantly emerging. It is no wonder, then, that investments in new robotics companies continue to grow, and that in many mature industries robotics present ideal new cost-saving and revenue opportunities.

Despite the vast differences in the environments where they are used and the tasks they carry out, robotics systems share a great deal in common, and require much of the same characteristics and behavior in their foundational software.

TYPES OF COLLABORATION WITH INDUSTRIAL ROBOTS


Requirement for intrinsic safety features vs. external sensors
CELL
Fenced robot
COEXISTENCE
No fence but no shared workspace
SEQUENTIAL COLLABORATION
Robot and worker both active in the workspace but movements are sequential
COOPERATION
Robot and worker on the same part at the same time - both in motion
RESPONSIVE COLLABORATION
Robot responds in real-time to movement of worker
Level of collaboration

Blue area: robot's workspace: Grey area: worker's workspace
Source: IRF, based on Bauer et al. (2016) mega.online/en/articles/collaborative-robots-market-expansion

Whether they are in your corner diner working cooperatively with the staff to prepare food then deliver it to patrons at their tables, or scouring the ocean floor counting manganese nodules, robotics systems need:

RELIABILITY

The OS and hypervisor must perform as specified, without failures, for as long as required without a restart, be that a few hours or a few decades.

PERFORMANCE

The OS and hypervisor must consistently provide specified performance and, especially, ensure that critical tasks run and complete deterministically.

SECURE CONNECTIVITY

System connectivity should be robust, versatile and secure, making available the best communications channels for diverse operating environments.

SAFETY CERTIFICATION

Both software and hardware should be certified to functional safety standards to mitigate risks of systematic and random faults that could result in accidents.

DIVERSE SYSTEMS AND MIXED CRITICALITY

The foundational software often must support running safety-critical and non-safety components on the same system-on-a-chip (SoC).

COMPREHENSIVE CYBERSECURITY

A system is only as safe as it is secure; the foundational software must ensure protection from malicious interference.

DEVELOPMENT AND MAINTENANCE

Development tools must be familiar and standards-based so you can focus on value add.

SYSTEM LONGEVITY

Hardware upgrades must not render legacy code obsolete, and software upgrades must be simple to perform and bring minimal risk.

QNX ROBOTICS FACTS & STATS

UNPARALLELED DEPENDABILITY

“The only way to stop the [QNX® Neutrino® RTOS] software from working was to shoot a bullet through the machine”.

Fortune Magazine

INHERENTLY SECURE

“96% of critical Linux exploits would not reach critical severity in a microkernel-based system, 57% would be reduced to low”.

-Biggs, Lee and Heiser (University of New South Wales)
“The Jury Is In: Monolithic OS Design Is Flawed”

A RELIABLE PARTNER FROM REQUIREMENTS TO RETIREMENT

BlackBerry® QNX® has a 100% success rate meeting start of production (SoP) deadlines for close to 300 automotive programs.

SAFETY-CERTIFIED OS

The QNX® OS for Safety is certified by TÜV Rheinland to IEC 61508 SIL 3, ISO 26262:2018 ASIL D and IEC 62304 Class C.

SAFETY-CERTIFIED HYPERVISOR

The QNX® Hypervisor for Safety is certified by TÜV Rheinland to IEC 61508 SIL 3 and ISO 26262:2018 ASIL D.

CERTIFY YOUR CODE, NOT YOUR TOOLCHAINS

Our C and C++ toolchains are qualified to IEC 61508-3:2010 SIL 3: TCL3 and T3 and ISO 26262-8:2018 ASIL D: TCL3 and T3.

EASILY PORT FROM LINUX

Our APIs are POSIX-compliant and our tools are standards-based so you can easily port from Linux® to the QNX® Neutrino® RTOS or the QNX OS for Safety.

WHY CHOOSE BLACKBERRY QNX?

BlackBerry® QNX® provides manufacturers of robotics systems with a complete software foundation on which to develop their technologies and expand their businesses. Our microkernel real-time operating system (RTOS) architecture has a 40-year track record in critical embedded devices and systems as varied as proton therapy systems (PTS), autonomous forklifts and solar-powered aircraft.

BlackBerry QNX foundational software is standards-based and offers common development tools to address the needs of engineering teams developing both safety-critical and non-safety systems. The QNX Neutrino RTOS and the QNX Hypervisor are complemented by their safety variants: the QNX OS for Safety and the QNX Hypervisor for Safety, which are certified IEC 61508 SIL 3.

Whether it's for a consumer-grade autonomous vacuum cleaners, surgical assistant cobots or autonomous camera drones, BlackBerry QNX provides the foundational software that lets your teams focus their time and talents on developing value-add systems and components. Plus, our professional services teams offer their decades of experience to see your robotics software systems through from design to market, and help you maintain them throughout their operational life.

7 REQUIREMENTS, 7 VALUE-ADDS FROM BLACKBERRY QNX

DELIVER REAL-TIME RELIABILITY AND PERFORMANCE

Support for compute-intensive and time-critical operations for critical systems

Whether it's controlling an autonomous underwater vehicle (AUV) or a robot waiter, the OS powering a robotics system must meet its designed criteria for dependability—it must be available to perform tasks when needed, and it must perform these tasks within the specified time.

The QNX Neutrino RTOS is designed specifically to meet these demands. Its priority-based scheduling and adaptive time-partitioning ensure that critical tasks run and complete when required. With its microkernel architecture, the QNX Neutrino RTOS isolates every application, driver, protocol stack and filesystem in its own address spaces outside the kernel. This means that a failed component won't take down other components or the kernel; it can be restarted immediately, with minimal impact on system performance, providing a high-performing and robust foundation for the most demanding robotics systems.

MANAGE DIVERSE, MIXED-CRITICALITY SYSTEMS

A simple, low-cost consolidation strategy for systems with different safety and reliability requirements

Driven by the need to cap initial bills of materials (BOM) as well as hardware weight, power consumption and thermal footprints, many embedded systems requirements call for consolidation of multiple systems onto a single system-on-a-chip (SoC). Often these systems have differing reliability or safety requirements, and some may even be legacy systems running on diverse OS's.

The QNX Hypervisor leverages the latest ARMv8 and x86-64 hardware virtualization extensions to enable developers to integrate diverse operating systems (e.g., QNX, Linux, Android™) and mixed criticality components and application onto a single SoC, while maintaining performance, and enforcing clear separation and isolation between systems to guarantee freedom from interference for safety-critical systems.

STREAMLINE SAFETY CERTIFICATION

A clear, low-risk and limited-cost path for certifications to functional safety standards such as IEC 61508

Certifying a system to standards such as IEC 61508 is a time-consuming and costly undertaking requiring highly specialized knowledge and skills. Certified to IEC 61508 SIL 3 by TÜV Rheinland, the QNX OS for Safety and QNX Hypervisor for Safety provide foundations that can significantly reduce the scope, risk, length and cost of your certification processes.

Our safety experts can provide training and hands-on workshops designed specifically for your key people developing functionally safe embedded systems. We can help you foster the safety culture you need to continue delivering functionally safe systems and, of course, we can help you design, deliver and maintain the best safety solutions from your product's development through to the end of its operational life.

BOARD SUPPORT PACKAGES

QNX® Board Support Packages (BSPs) provide an abstraction layer of hardware-specific software that facilitates the implementation of the QNX Neutrino RTOS on your board. Our extensive BSP library includes BSPs for SoCs manufactured by leading hardware manufacturers. In addition, our professional services can develop customized solutions for you and support your safety and security requirements.

Learn more about our library of BSPs.

STRENGTHEN CYBERSECURITY

Current and configurable security policies that ensure system integrity, including secure over-the-air (OTA) updates

Isolated systems belong to the past. Robotics systems are now connected, at least some of the time, and hence vulnerable to cybersecurity breaches that can put operators, materials and infrastructure, and the public at risk. Building and maintaining a secure robotics system requires—at a minimum—a reliable and secure OS, and a secure supply chain. Connected systems also require secure over-the-air (OTA) software updates, managed public key infrastructure (PKI) authentication, and FIPS (Federal Information Processing Standards)-certified encryption.

The QNX Neutrino RTOS reduces the surface open to cyberattacks by running all services outside the kernel space, and provides multi-layered protection with layered security policies: granular control of system privilege levels, encrypted and self-verifying filesystems implementing AES 256 encryption and lockable encryption domains, secure logging of system activities, heap, stack and memory protection, and secure boot implementing TPM and TrustZone.

And BlackBerry® Jarvis®, our software composition analysis solution, can help you uncover and remediate software vulnerabilities in components from across your complex supply chain.

SUPPORT SECURE CONNECTIVITY

Few robotics systems still operate entirely unconnected from the rest of the world. Whether it's receiving orders for meals it will deliver, uploading vending machine data, sharing its location with its peers distributed across the oceans, or uploading sensor data for predictive maintenance analysis, a robotics system today relies on dependable and secure communications channels.

The QNX Neutrino RTOS offers a full network stack suitable for communication at whatever network level is most appropriate to your implementation–everything from real-time video feeds to over-the-air (OTA) software updates. QNX® Over the Air (OTA) is a customized remote software update solution that can be tailored to update seamlessly and securely, and manage the endpoints on embedded systems and QNX® Black Channel Communications Technology, pre-certified to ISO 26262 ASIL D, to help ensure the safety of your system's data communication even when it is over unsafe communication links (UDP, TCP, CAN).

FACILITATE DEVELOPMENT

A foundation and tools that facilitate development and ensure you meet your deadlines

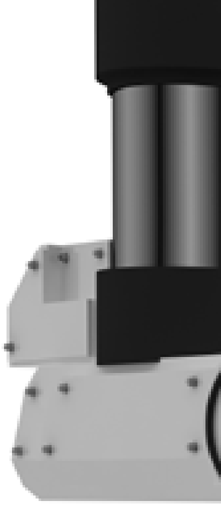
The QNX® software development platform (SDP) includes the QNX® Momentics IDE and tools. They are POSIX-compliant, support validation with the PSE 54 test suite, look and feel like Linux, and use the familiar Eclipse development environment, including the GNU compiler collection. They also include C and C++ toolchains qualified to IEC 61508-3:2010 SIL 3: TCL3 and T3, so you can spend your time developing and certifying your code, not your toolchains.

SUPPORT SYSTEM LONGEVITY

A simple, maintainable mechanism for porting legacy code and prototypes, and for implementing upgrades

The QNX Neutrino RTOS microkernel architecture makes it easy to quickly add new drivers, confident that a driver failure won't mean a system failure. This reduces the risks to the software system when introducing drivers for new hardware.

With the QNX Hypervisor and its safety variant, the QNX Hypervisor for Safety, you can contain entire systems with their OS's as guests in hypervisor virtual machines. This means that you can port legacy code built on different OSs (e.g., Android, Linux) onto new SoCs and run them concurrently with your latest product. You can also implement new features or upgrade entire systems in virtual machines, confident that the new code won't affect other systems, including safety-critical systems, running on the SoC.



SUPPORT AND SERVICES

BlackBerry QNX is your partner throughout your product lifecycle. We offer a range of services to help you reach your goals faster. The BlackBerry QNX professional services teams have deep knowledge of embedded systems, functional safety and cybersecurity, and a 100-percent success rate in helping our customers achieve safety certifications.

We back our products with top-quality support, best-in-class documentation and expertise from the developers and engineers who built the QNX products you use. Whether you want help with staff augmentation, kickstarting a project or certifying products, our embedded systems development and OS experts can provide the proper knowledge and experience at the right time.

PROVEN EXPERIENCE

Thousands of person-years in development, support, integration

INTEGRATION & OPTIMIZATION

High-performance software for custom hardware, delivered when you need it

GLOBAL FOOTPRINT

Regional experienced teams in North America, EMEA, APAC

SERVICE EXCELLENCE

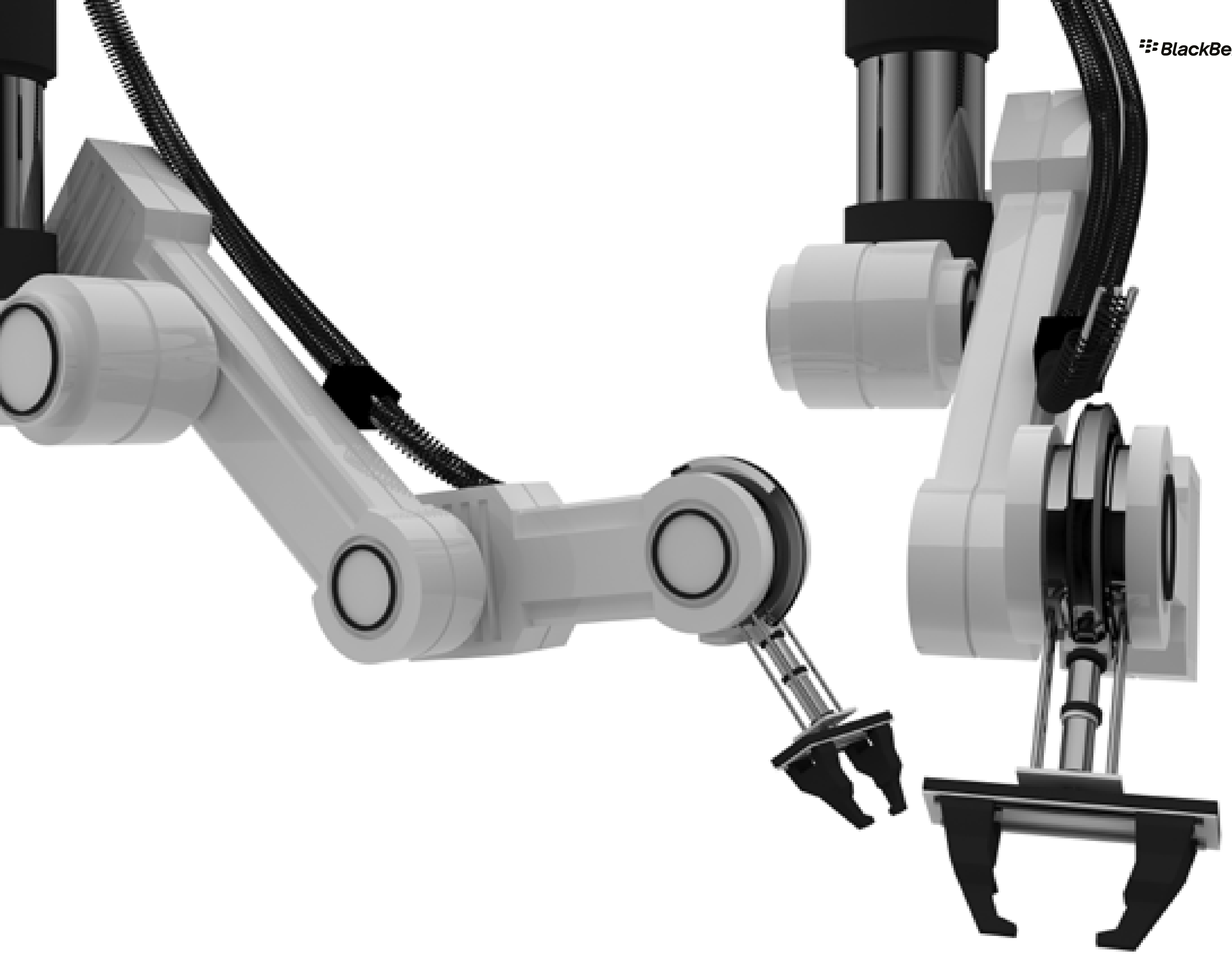
100% success at meeting start of production (SOP) deadlines

DEEP EXPERTISE

Experts in all areas of embedded system software

COMMITMENT

Dedicated, dependable, trusted staff



SAFETY AND SECURITY SERVICES

The BlackBerry QNX safety and security services teams possess deep knowledge of functional safety and security. With a legacy in cybersecurity, BlackBerry has the expertise you need to secure both systems and supply chains.

PROFESSIONAL SERVICES

The BlackBerry QNX global professional services teams help companies bring safe, secure and reliable products to market on time and within budget. We closely fit our expertise to your needs, including custom development.

TRAINING

BlackBerry QNX offers project-customized courses on best practices in functional safety and embedded design, all of which are hands-on, instructor-led and use real-world examples.

SUPPORT AND MAINTENANCE

BlackBerry QNX provides unmatched support packages and services that span the entire lifecycle of systems built with BlackBerry QNX solutions, including regular updates, fixes and technical advice from developers, engineers and architects.

SOFTWARE AT-A-GLANCE

FOUNDATION PRODUCTS	
QNX Neutrino RTOS	A deterministic, yet flexible foundation for your next-generation products. Its unique microkernel architecture provides dependability, scalability and layered security.
QNX Hypervisor	An embedded virtualization solution with a microkernel architecture so multiple, diverse OS's (Android, Linux, QNX Neutrino) can safely operate on the same SoC.
QNX Software Development Platform	The power of QNX Neutrino RTOS plus the QNX® Momentics® Tool Suite to provide you with a POSIX compliant, Linux-like development platform.

SAFETY-CERTIFIED PRODUCTS	
QNX OS for Safety	The safety variant of the QNX Neutrino RTOS, the QNX OS for Safety is pre-certified to IEC 61508 SIL 3. Easily port Linux-based prototypes to the QNX OS for Safety environment and get all the documentation and support you need to support your certification efforts.
QNX Hypervisor for Safety	The QNX Hypervisor for Safety is the safety variant of the QNX Hypervisor. Comprised of the QNX OS for Safety plus safety-certified virtualization extensions, it is the first embedded hypervisor pre-certified to IEC 61508 SIL 3.
QNX Black Channel Communications Technology	Certified to ISO 26262 ASIL D, this solution helps ensure that communication exchanges are safe, and that data is not altered or impacted during transmission.

SECURITY SOLUTIONS	
BlackBerry Jarvis	A cloud-based software composition analysis solution that blends system exploration technology and expert services to examine software for security vulnerabilities and software craftsmanship.
QNX Over the Air	QNX Over the Air (OTA) is a remote software update solution enabling seamless and secure updates and management of endpoints on a variety of embedded systems.

MIDDLEWARE & FRAMEWORKS	
QNX Advanced Virtualization Frameworks	Complementing the QNX Hypervisor, the QNX® Advanced Virtualization Frameworks enable you to build out your own virtualization solutions, including virtual devices designed to the VirtIO standard.
QNX Sensor Framework	Integrate sensor feeds from diverse sources (camera, radar, LiDAR, IMU, GPS sensors, etc.) into your critical embedded systems.
QNX Multimedia Suite	Easily implement media capabilities including playback and recording of rich audio and video content in your embedded systems.
QNX Speech Framework	Designed to ease and accelerate the development of voice-controlled embedded systems, this framework abstracts the complexities of speech recognition and natural language processing engines from the operating system platform and applications. Available through BlackBerry® QNX® Professional Services.

ABOUT BLACKBERRY QNX

BlackBerry QNX is a trusted supplier of safe and secure operating systems, hypervisors, frameworks and development tools, and provides expert support and services for building the world's most critical embedded systems. The company's technology is trusted in more than 195 million vehicles and is deployed in embedded systems around the world, across a range of industries including automotive, medical devices, industrial controls, transportation, heavy machinery and robotics. Founded in 1980, BlackBerry QNX is headquartered in Ottawa, Canada and was acquired by BlackBerry in 2010.

BlackBerry QNX software and development tools are standards-based and enable companies to adopt a scalable software platform strategy across product lines and business units. The BlackBerry QNX software portfolio, including our safety pre-certified product versions, is purpose built for embedded systems and scales to support everything from single-purpose devices to highly complex, mixed-criticality platforms.

Because we believe we are not successful until you are, you can rely on our support and professional services teams to provide the expertise you need, when you need it–throughout the entire product development lifecycle.

BlackBerry® | QNX®

BLACKBERRY.QNX.COM