



# Elevating Safety and Security: New Industrial Automation and Advanced Robotics Breakthroughs

Safety-Critical Industrial IoT Applications Require Real-Time Responsiveness and Security Embedded in Silicon

WNRDRVR

# Developing Safe and Secure Industrial Applications Using Robotics



**Autonomous mobile robots, AI-controlled vehicles, automated smart factories, and advanced control systems are becoming increasingly common. As this trend transforms factories, warehouses, hospitals, retail establishments, and farms, safety has gained an elevated profile.**

Emerging use cases warrant a responsive real-time operating system (RTOS) and hardware-strengthened security. VxWorks®, a key component of Wind River® Studio, and Intel® Xeon® D-1700 and D-2700 processors deliver the requisite technologies for operating intelligently in safety-critical settings.

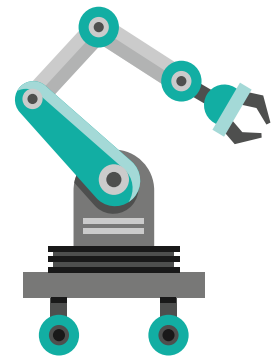
Innovative industry applications built using robotics are demonstrating capabilities for performing tasks that previously could only be accomplished by human actors. Next-generation robots that are equipped with breakthrough technologies in multiple industries are equipped to see, plan, and act. These skills depend on sensors — such as cameras — to function within different environments; on artificial intelligence to provide real-time decision making and plan activities; and on physical mechanisms for moving objects from place to place, navigating in the physical world, and building things out of individual components.

Industrial-class reliability, exceptional high-performance processing power, and a proven RTOS are at the heart of many new industrial IoT (IIoT) solutions. Intel Xeon D-1700 and D-2700 processors — representing entire systems in two form factors fabricated using a system-on-chip (SoC) design — have been enhanced for operation in rugged environments with features that enable augmented IoT and deep-learning applications.

Complementing this hardware platform, Studio features VxWorks Cert Edition, a proven and dependable RTOS that has been used in a wide range of demanding applications for aerospace, medicine, and transportation, as well as mission-critical industrial applications and robotics systems. Wind River Helix™ Virtualization Platform, a part of Studio, also contributes to IIoT solutions by consolidating multi-OS and mixed-criticality application onto a single edge compute software platform.

The automotive industry can gain up to **\$167 billion** in productivity gains through smart factories **by 2023**.

- Capgemini Research Institute,  
Automotive Smart Factories





Intel and Wind River share a long history as technology partners and together have provided the building blocks for a dizzying array of powerful, effective, and trend-setting solutions that have energized design and development of industrial automation and robotics systems across multiple segments. System architects and integrators, industrial equipment OEMs, IoT developers, and contractors can take advantage of the tools and technologies from Intel and Wind River to build durable, safety-certified, secure IIoT and robotics solutions with real-time deterministic capabilities.

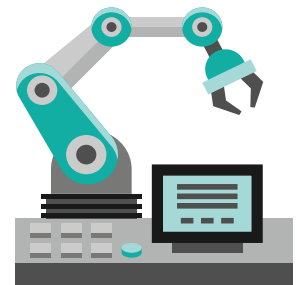
## The Rise of Autonomous Mobile Robots

Among the evolutionary changes sweeping through the industrial sector, autonomous robots are increasingly being deployed to improve business efficiency and effectively satisfy the expectations of customers. With greater responsibilities being applied to robotics systems performing tasks in which minimal human intervention is required, safety assurances are vital and certifications are necessary to ensure that robotics and industrial control systems operate as intended and present very low risk of causing damage or harm to individuals or structures. Safety-engineered solutions constructed using building blocks from Intel and Wind River make it possible to gain optimal performance while maximizing security and minimizing risk.

Figure 1 shows a conceptual view of a platform that supports an autonomous mobile robot in a typical use case. Autonomous mobile robots are actively engaging in tasks such as sanitizing hospitals, automating warehouse productivity and efficiency, handling baggage in airports, and improving customer experiences in hotels, stores, and airports.

The demand for autonomous mobile robots (AMRs) has increased significantly, with the market expected to reach **\$7 billion in value by the end of 2022.**

— The Rodon Group



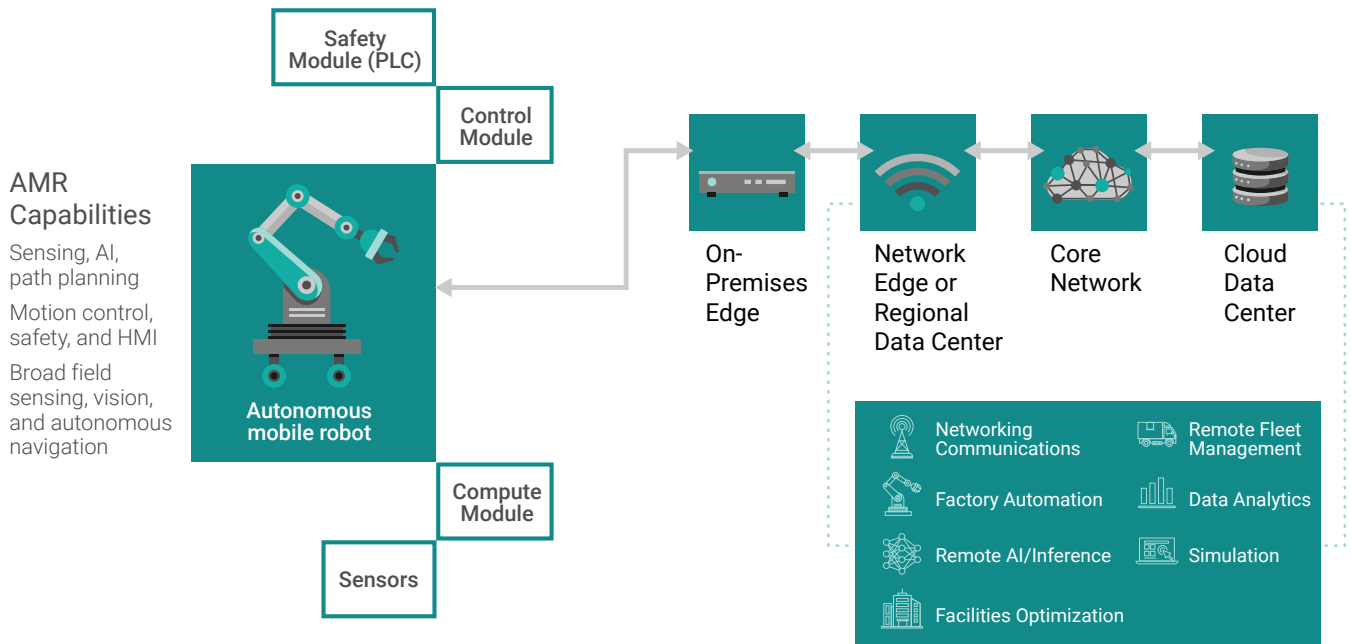


Figure 1. Conceptual view of an autonomous mobile robot platform (courtesy of Intel)<sup>1</sup>

A host of technologies combine to enable the use of autonomous mobile robots, including AI, networking communication, simulation software, and data analysis. For example, 5G networking is a vital component of AMR adoption. The Capgemini Research Institute said in an article, “**Realizing the Power and Promise of Industrial 5G**,” “5G greatly enhances the range and field of operations for robots and autonomous machinery – far exceeding the capabilities of current connectivity technologies such as WiFi. This becomes even more critical as autonomous mobile robots or drones become a more mainstream part of manufacturing operations. It can also help to adjust production lines faster.”

Beyond AMRs, the future of automation will encompass other types of robots and industrial systems, including:

- **Articulated robots:** Robot arms capable of emulating the motions and actions of human arms have a wide array of uses in factories, warehouses, pharmaceutical facilities, and more.

- **Automated guided vehicles (AGVs):** AGVs can traverse predefined routes for delivering and moving different materials and objects within a facility.
- **Humanoids:** Robots with human-like appearance and characteristics can play a role in different scenarios, such as offering information services, guidance, and way-finding tasks.
- **Cobots:** Working side by side with humans, cobots can streamline many different types of tasks, such as assembling equipment, performing operations in research labs, and helping with quality-control testing.
- **Hybrids:** New classes of robots that blend the skills and capabilities of the types discussed in this section will perform specialized, complex tasks.

As robots and automated systems become more widely integrated in human environments, sharing workspaces and performing a diverse range of tasks, certifications for safety-critical operations and secure performance will be essential.

<sup>1</sup> *Autonomous Mobile Robots. Intel. [www.intel.com/content/www/us/en/robotics/autonomous-mobile-robots/overview.html](http://www.intel.com/content/www/us/en/robotics/autonomous-mobile-robots/overview.html)*



## Wind River and Intel Technologies Underlie Safety-Critical Operations

Components built into robotics systems and IIoT systems co-engineered by Intel and Wind River have fully integrated features that contribute to the overall safety and security of operation.

### Intel Safety and Security Highlights

Integrated safety and security features in the Intel Xeon D-1700/D-2700 SoCs include:

- **Hardware root of trust:** Platform-critical firmware, code, and data are checked during startup and during operation to protect against intrusions or bugs. Intel Boot Guard, Intel OS Guard, and Intel Trusted Execution Technology deliver hardened security.
- **Protected storage:** Tamper-resistant storage areas in silicon guard sensitive data, keys, or authentication data against unauthorized disclosure. Intel Total Memory Encryption and Discrete TPM 2.0 support elevate protection.
- **Cryptographic acceleration:** Built-in hardware acceleration features speed up cryptography and DRM protections. Intel Secure Key, Intel AES-NI, SHA N-I, and Asymmetric Encryption Support sharpen cryptographic operations.
- **Trusted execution:** Applications and workloads are periodically checked while running to protect against corruption or malicious activities. Intel Virtualization Technology, Intel Software Guard Extensions, and Intel Total Memory Encryption Multi-Tenant provide reliable, trustworthy operations.
- **Time Coordinated Computing (TCC):** A key component of safety in industrial automation and robotics systems is precise compute timing when performing real-time operations. Intel TCC ensures low-latency deterministic operation, complemented and enhanced by the real-time capabilities of VxWorks.
- **Time-Sensitive Networking (TSN):** TSN is essential in industrial systems that require standardized mechanisms for communicating over Ethernet connections. TSN supports accurate, deterministic network exchanges with a defined latency.

**64%** of respondents say their organizations are more likely to purchase technologies and services from technology providers that are leading edge with respect to innovation.

— Ponemon Institute

Proactive protections embedded in hardware work in concert with the Wind River capabilities listed in the following section. At present, VxWorks is the only RTOS that fully supports 3rd Gen Intel Xeon D-1700/D-2700 processors.

## Wind River Safety and Security Highlights

Wind River safety and security highlights include:

- **Extensive compliance support:** VxWorks safety certifications and compliance listings cover DO-178C, IEC 61508, ISO 26262, ARINC 653, POSIX®, and FACE™. Standards conformance and safety certification evidence has been demonstrated and documented on commercial off-the-shelf (COTS) systems.
- **Four decades of proven, mission-critical performance capabilities:** Wind River has a long and storied history working on some of the most challenging and safety-critical applications around the world.
- **Open Container Initiative (OCI) container support:** Wind River has engineered OCI container support into the latest version of VxWorks, which is now the only RTOS that supports deployment of applications using containers. Developers can use familiar languages, tools, and technologies to build and deploy solutions securely, enabling intelligent automation systems. Container technology can be used to perform rapid application updates and patches in response to newly detected vulnerabilities.
- **Vulnerability notices:** Wind River maintains continuous threat monitoring, rapid assessment and prioritization, and prompt customer notifications with advice on remediation. System threats in IIoT deployments can be quickly remedied before threats cause issues. Security patches are readily available and potential risks are identified through a searchable database linked to MITRE's list of Common Vulnerabilities and Exposures (CVEs).

- **Cyber testing:** Wind River Simics® lets developers run extensive cyber tests and detect system vulnerabilities, using modern simulation and automation technologies, without risking exposure to the actual hardware or software in IIoT and robotics systems under development.
- **Built-in security:** The integral security features built into VxWorks include a hardened kernel, secure communication, and data protection. VxWorks functions on multiple levels using a framework based on the CIA triad. Throughout the full range of system operations — from system startup through shutdown procedures — VxWorks provides access to features that let system architects integrate the appropriate level of security for applications and shut down potential risk vectors.

## Bedrock Security Is a Must for Businesses Deploying Robotics Systems

An equally important aspect to the deployment of industrial automation and robotics systems is security against intrusion and protection of system integrity. Autonomous vehicle operations in cities, drones moving through public airspace, robots in factories and warehouses, robots used for physical therapy or in hospital settings — all of these use cases have a potential for disastrous outcomes if systems are breached.

Intel and Wind River are leaders in hardware and software security innovation, with technologies that are layered and interoperable to anticipate threat vectors and guard against breaches.

Suzy Greenberg, vice president, Intel Product Assurance and Security, said, "The security threat landscape continues to evolve, becoming more sophisticated and challenging for organizations to defend against. Today, more than ever, companies are demanding assurance capabilities and hardware-enhanced security solutions that help protect the entire compute stack. Intel is in a unique position to deliver these innovations on behalf of our customers."<sup>2</sup>

<sup>2</sup> Intel Study: Secure Systems Start with Hardware. Intel Newsroom. April 2022. [www.intel.com/content/www/us/en/newsroom/news/study-secure-systems-start-hardware.html](http://www.intel.com/content/www/us/en/newsroom/news/study-secure-systems-start-hardware.html)




The attack surface broadens as we move into the intelligent machine age. Writing for Wind River BrandVoice, Barbara Cosgriff said, “We’re a connected society, living in a machine economy. Critical infrastructure players are connecting their devices to get data out of them and offer new services, provide functional and security updates to the software, introduce new features, or integrate the devices in a larger system. Devices are not alone anymore. They are part of a global cyber-physical system that spans hyperscale clouds, edge clouds, and the electro-mechanical edge.”<sup>3</sup>

## A Platform for Building World-Class IIoT Solutions: Wind River Studio

Studio brings together a comprehensive collection of tools and technologies well aligned with the needs of developers building IIoT solutions and robotics systems. Studio delivers a full lifecycle management platform equipped with technological support for intelligent edge solutions powered by AI and machine-learning components.

Studio is optimized for DevSecOps processes, giving developers a ready means to implement continuous integration (CI) and continuous delivery (CD) workflows using agile development practices. [Learn more](#) about Studio.

## Intel Partner Alliance Benefits

 Wind River is a long-term member of the Intel Partner Alliance, collaborating with other hardware and software vendors on solutions for IoT implementations. Wind River is particularly active in the IoT Solutions Community, which brings together like-minded organizations to unlock opportunities across a global marketplace. Benefits include advanced training, access to a wide range of development resources, and many promotional benefits. To get involved, visit this page: [Let’s Get You Registered for Intel’s Partner Program](#).

Kevin Dallas, writing for Wind River BrandVoice, said, “At Wind River, we have 40 years of experience with delivering mission-critical, intelligent systems with the highest safety standards. We believe that it is our responsibility to constantly advance our technologies, while at the same time advancing the positive impact that such technologies will have on the world. In the case of AI-driven robotics, it means that we are proactive about delivering systems that meet — or exceed — the trust, transparency, fairness, and privacy that people expect from AI.”<sup>4</sup>

<sup>3</sup> Cosgriff, Barbara. *The Art of Defense: Mitigating Cyber Exposure with Threat Modeling*. Forbes. May 2022.

[www.cryptoverwrite.com/dallas.com/sites/windriver/2022/05/06/the-art-of-defense-mitigating-cyber-exposure-with-threat-modeling](https://www.cryptoverwrite.com/dallas.com/sites/windriver/2022/05/06/the-art-of-defense-mitigating-cyber-exposure-with-threat-modeling)

<sup>4</sup> <https://www.forbes.com/sites/windriver/2022/03/01/ai-robotics-and-ethics-harnessing-the-power-of-intelligent-machines-to-benefit-humans/?sb=650d60d76be>

## Software and Hardware Interoperating for Maximum Security and Safety

Any vulnerable point in an IIoT system — whether a single device without sufficient protection or a software program that is unguarded — can put the entire platform at risk. Maximum security is achieved in trustworthy systems built on a foundation with tight interoperability between hardware components and system software. This approach is central to the latest generation of IIoT solutions built on Intel hardware platforms running VxWorks in a Helix Platform environment.

Helix Platform — a component of Studio — unifies operating environments by supporting legacy applications and modern applications within a single virtualized environment that can be partitioned to avoid security intrusions into sensitive applications. Providing a single-pane-of-glass view into complex heterogeneous cloud platforms, on-premises equipment, or hybrid environments, Helix Platform offers an invaluable management tool that can drive multiple hypervisors.

Developers building industrial automation and robotics systems can save time and effort by relying on certifications of key components to satisfy industry requirements. Intel Xeon D-1700/D-2700 processors provide a clear pathway for meeting AC-20 193 and AMC-20 193 objectives for demonstrating effective, safety-aligned multi-core processor usage. Intel safety evidence packages are also available for IEC 61508.

VxWorks has also earned an outstanding reputation in the IIoT sector and achieved certifications and evidence packages supporting DO-178C, IEC 61508, IEC 62304, and ISO 26262 safety standards. VxWorks delivers multi-core and multiprocessor support and can run on 32-bit and 64-bit multi-core processors that are based on Intel, Arm, Power, and RISC-V architectures.

Intel, Wind River, and fellow ecosystem partners continue to acquire certification evidence packages and to meet emerging industry standards. These certifications and evidence packages simplify developer efforts to create safety-critical IIoT and advanced robotics solution stacks for the latest Intel processors and Wind River software components.

### Additional Resources

To explore the ways in which VxWorks provides RTOS capabilities for embedded systems, connect to [VxWorks: Redefining the Role of the RTOS](#) and download the free ebook on this topic.

To learn more about the safety-critical applications supported by Intel Xeon D-1700/D-2700 processors, visit [this page](#).

To learn more about certification of safety-critical applications, visit [VxWorks Safety Platforms](#).