SAFETY FIRST FOR INDUSTRIAL AUTOMATION

Prioritizing safety has become more crucial than ever as industry reaches new frontiers of automation and autonomy. Ensuring that machinery, robotics, and vehicles are functionally safe for workers, customers, and the public is mandatory to protect lives and safeguard factories and operational areas. “Safety first” remains the top priority.

Contributing to this challenge is the growth of digital transformation, as the use of sensors, artificial intelligence (AI), machine learning (ML), wireless communication, and IT become integral to Industry 4.0 and industrial automation. According to a Market Research Future report, the market for functional safety is expected to grow from USD 14.4 billion in 2024 to USD 22 billion by 2032, at a CAGR of 5.4%. With this growth comes an increase in safety requirements and regulatory scrutiny.

Wind River® offers the products, services, and expertise to help developers in industrial and control automation build functional safety into their products and software systems. From understanding the principles of functional safety to navigating regulatory landscapes and embracing cutting-edge technologies, industrial automation developers can learn how to foster a culture of safety-first design.

WHAT IS FUNCTIONAL SAFETY?

At its core, functional safety refers to the proactive design and implementation of systems and equipment to ensure that they operate safely, even in the presence of errors or malfunctions. In the context of industrial automation, functional safety encompasses a holistic approach to risk mitigation that includes hardware, software, and operations. By integrating robust safety features, developers can safeguard workers, customers, system operators, assets, and the environment against potential hazards, fostering trust and confidence in their products.

Implementing functional safety requires designing and building in the proper automatic protection and safety functions, covering every component or subsystem. The standards focus largely on the safety regulations and requirements for electrical, electronic, and programmable systems.

Another priority is to provide detailed evidence that the system meets the functional safety requirements for the relevant industry. This comes through certification via the appropriate testing and accreditation bodies.

Challenges Facing Industrial Automation Developers

Rapid technological evolution presents challenges for developers, including:

- Hardware development
  - Proliferation of complex systems and interconnected components
  - Inherent risks requiring rigorous testing and validation
- Software development
  - The need to ensure integrity and reliability of code, especially in safety-critical applications
  - Potential catastrophic consequences from minor errors

- Convergence of hardware and software systems
  - The need for seamless integration and interoperability
  - Assurance of overall industrial automation equipment safety and performance
  - The challenges of obtaining safety certification

Security and Safety: Working Together

Developing functional safety features requires a multifaceted approach that integrates hardware, software, and operations. Model-based design methodologies and simulation tools facilitate the rapid prototyping and validation of safety-critical systems, streamlining the development process and accelerating time-to-market. Advancements in embedded systems, AI-based algorithms, and cybersecurity protocols further enable sophisticated safety-critical systems that are resilient to cyberthreats and external interference — though they also add to system complexity. Functional safety becomes even more important for software utilizing these advanced and autonomous systems.

And while safety focuses on mitigating risks associated with system malfunction and failure, security addresses threats posed by malicious actors and cyberattacks. When developers integrate robust security measures into safety-critical systems, they can mitigate the risk of unauthorized access, data breaches, and system tampering, safeguarding the integrity and reliability of their products.

Regulatory Landscape for Safety

The industrial automation industry is subject to stringent regulatory frameworks that govern safety standards and requirements. Standards such as IEC 61508 provide guidelines for the design, implementation, and validation of safety-related control systems, and ensuring compliance is essential to mitigate legal liabilities and to uphold reputation. Functional safety certification programs for IEC 61508 standards are offered globally by several recognized certification bodies, including Intertek, SGS, TÜV Rheinland, TÜV SÜD, and UL.

REAL-TIME OPERATING SYSTEMS FOR SAFETY-CERTIFIED APPLICATIONS

Any mission-critical device, system, or component in industrial automation, robotics, medical, automotive, or other industries needs to be safety certified. A robotic arm must not harm workers; an automatic braking system must work instantly when needed. To get this assurance, the system software needs to run on a real-time operating system (RTOS) that utilizes multi-core processing and that has been certified according to specific standards. This functional safety support needs to continue throughout the product's lifecycle, even in its legacy stage.

Tailored Linux Development for AI, ML, and Deep Learning (DL)

As industrial automation and robotics incorporate autonomous middleware, AI, ML, and deep learning (DL), much of the software system development will depend on Linux. For devices and equipment to operate in the field, it is critical to minimize the Linux distro.

In safety-critical scenarios, this entails integrating Linux into a system traditionally reliant on an RTOS. The inclusion of AI/ML algorithms, often affiliated with Linux, then becomes imperative. This necessitates applications and systems capable of bridging both operating systems, prompting system integrators to adeptly navigate and harmonize their diverse requirements.

Hypervisor Technology for Interoperation

Silicon technology is advancing: The latest processors currently contain 24 to 40 cores on a single system-on-chip (SoC); more cores will be on future versions. For systems to comprise a safety-certified RTOS and an embedded Linux OS, operating side by side on a single SoC, developers rely on virtualization and software container technology. It is critical to have the means to monitor both systems with high-speed communication. This is where a hypervisor that is certified, rapid, and capable of managing the host operating system(s) is a requisite.

WIND RIVER PRODUCTS AND SERVICES FOR FUNCTIONAL SAFETY

Wind River offers long experience and an extensive portfolio of software and services that lead the way in functional safety development in industrial automation:

- More than 40 years working with industrial automation developers
- Safety-certified products
- Products and services that enable modern Industrial 4.0 technologies
- Support for delivery of 5G wireless communication to the industrial segment
- Support for implementation of safety systems in industrial, aerospace, automotive, defense, robotics, medical, rail, and more

Wind River has extensive expertise and experience meeting the safety-critical standards of crucial sectors, including flight safety (DO-178C DAL A), industrial (IEC 61508), rail (EN 50126/8/9), and automotive (ISO 26262).

FUNCTIONAL SAFETY–CERTIFIABLE SOFTWARE

VXWORKS CERT EDITION

VxWorks® Cert Edition is a platform for safety-critical applications that require DO-178C, ISO 26262, IEC 61508, IEC 62304; or certification evidence in the avionics, automotive, industrial automation, and medical device industries.

>> Learn More About VxWorks Cert Edition

WIND RIVER HELIX VIRTUALIZATION PLATFORM

Wind River Helix™ Virtualization Platform, a Type 1 hypervisor, consolidates multi-OS and mixed-criticality applications onto a single edge compute software platform, simplifying, securing, and future-proofing critical infrastructure solutions. Helix Platform is designed to be certified and to simplify the certification of safety-critical applications according to DO-178C, IEC 61508, and ISO 26262 requirements.

>> Learn More About Helix Platform

WIND RIVER STUDIO LINUX SERVICES

Wind River Studio Linux Services delivers embedded Linux platform services for solution design, safety and certification, security, and lifecycle management capabilities that help reduce open source project risk while accelerating time-to-application-deployment, so you can lower your total cost of ownership and focus your valuable resources on innovation.

>> Learn More About Studio Linux Services

WIND RIVER STUDIO DEVELOPER

Wind River Studio Developer is a modern DevOps platform that accelerates development, deployment, and operation of robust mission-critical embedded systems for the intelligent edge. Assisting in the development of functional safety solutions, Studio Developer consists of five main components: Wind River Studio Pipelines, Wind River Studio Virtual Labs, Wind River Studio Test Automation, Wind River Studio Over-the-Air Updates, and Wind River Studio Digital Feedback Loop. Flexible installation options provide control over security and compliance, both in the public cloud and in on-premises infrastructure.

>> Learn More About Studio Developer

WNDRVR

Wind River is a global leader of software for mission-critical intelligent systems. For 40 years, the company has been an innovator and pioneer, powering billions of devices and systems that require the highest levels of security, safety, and reliability. Wind River offers a comprehensive portfolio of software and expertise that are accelerating digital transformation across industries.