RTS Safe Hypervisor Will Enhance Intel Processors with New Functional Safety-Compliance Capabilities

New FuSA-capable hypervisor for Intel Atom@ x6000E Series processors to facilitate running safe and non-safe workloads on a single chip

Executive Summary

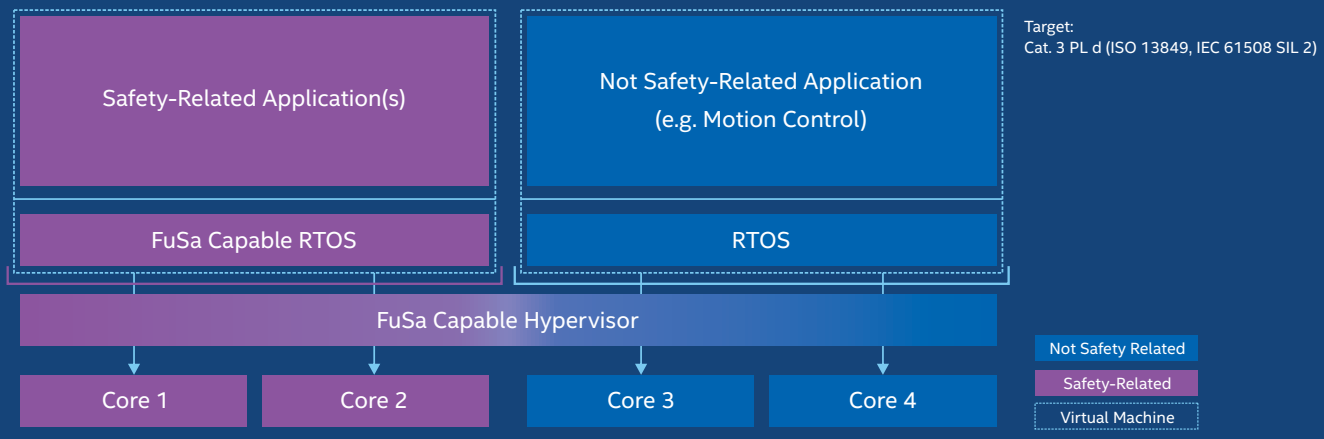
Users developing and deploying next generation Internet of Things (IoT) edge devices need processors and software elements that comply with the security and functional safety requirements of their industry. But compliance with functional safety (FuSa) standards has historically been a time-consuming and expensive process.

Compliance is about to be streamlined thanks to a new safe hypervisor – under development for Intel Atom® x6000E Series processors – that will enable multiple operating systems, applications, and IoT devices to safely and efficiently share a single hardware platform. Real-Time Systems (RTS) is developing the new hypervisor in partnership with Intel. The RTS Safe Hypervisor will facilitate the consolidation of both safety and non-safety workloads running on select multi-core processors. The FuSa-capable hypervisor also will help with the efficient management of hardware resource allocation and virtual machine applications.

Developing a New Safety Solution

Conventional hypervisors are not designed to meet industry safety certification requirements. By contrast, the addition of a safe hypervisor will facilitate and accelerate the development and deployment of FuSa-certified applications. Because it is designed for virtual computing environments, the RTS Safe Hypervisor will provide a more cost-effective, less complex, more efficient, and more versatile option for end-users than two-chip solutions. It also allows for the possibility of mixing and matching both safe and non-safe operating systems and applications on single chip.

Mixed Criticality on Multi-core Single Chip



Both safety & not-safety workloads consolidated onto a single computing platform

Safety is critical when it comes to FuSa-intensive applications and workflows — such as robotics, autonomous systems, and industrial controls. Intel's functional safety technology helps customers meet safety-critical requirements in industries ranging from manufacturing and machin automotive to medical equipment and transportation.

The RTS Safe Hypervisor is being optimized for mixed criticality solutions on a single multi-core chip. This will enable end-users to consolidate safe and non-safe workloads, while facilitating the separation of mixed criticality in a single Intel SoC platform.

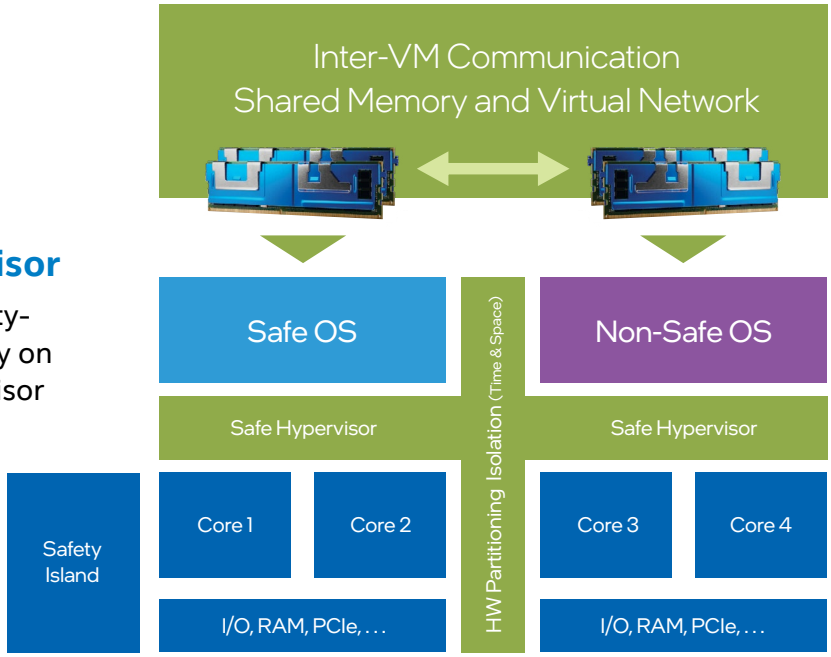
Users can choose which operating systems they prefer, while relying on the Intel Atom® x6000E Series and RTS Safe Hypervisor for functional safety. Intel Atom® x6000E Series processors, for example, include an integrated safety island and other integrity features in silicon, to support the execution of safety applications, and the detection and reporting of failure conditions. Safe hypervisors provide pass-through capabilities that enable connected devices to be more safely integrated by end users. Standard drivers and existing applications can be used.

Intel Atom® x6000E Series processors are built to drive performance, reliability, and versatility. Important features include:

- Extended Temperature
- Industrial Use Conditions
- In-Band Error Correcting Code (ECC)
- Intel® Virtualization Technology
- Hardware-embedded Security and Encryption
- Intel® TCC and Industry Standard TSN
- Integrated Intel® Safety Island Designed To Meet FuSa Requirements
- Ideal for High Performance, Low Power Computing

Integrating the RTS Safe Hypervisor

In order to facilitate the integration of safety-related and non-safety related functionality on one hardware device, the RTS Safe Hypervisor can be integrated on-chip and deployed alongside Intel's safety island. This scalable solution also will provide PCI pass-through to assigned devices, while controlling communication between operating systems in the virtualized environments.



The RTS Safe Hypervisor allows for inter-OS communications using shared memory and a virtual network. A virtual network provides for seamless socket-based communication, and information is exchanged via a dedicated area in the main memory. Virtual PCI memory can be shared between operating systems, and an interrupt mechanism allows for real-time signals to pass between the operating systems. Cache coherency is maintained automatically by the processor.

The RTS solution also includes drivers for managing virtual devices. Security is enhanced because interfaces can be selectively enabled or disabled as needed. Network devices in this real-time IoT processing environment use standard protocols and services. This serves as a bridge for passing external traffic through the internal network.

A slim bootloader enables all of the safety-related components from the RTS Safe Hypervisor to be flashed into the firmware on system power-up. Safe and non-safe virtual operating systems can be secured quickly and safely. Moreover, non-safe applications can be modified without affecting safety-related components.

The software stack developed by Real-Time Systems incudes the safe hypervisor, while Intel provides the software diagnostics that check the SoC health at boot and run-time. The RTS software also includes the firmware, drivers, and services required to secure all virtual machines.

Benefiting from safe hypervisor functionality

The primary benefit of the RTS Safe Hypervisor is that it enables the integration of safety-related and non-safety related functionality on one hardware device. This helps customers determine which applications are in scope with their industry's certification requirements. The safe hypervisor facilitates safety and workload consolidation, which reduces time to market and results in cost savings. In addition to enhancing hardware security and efficiency, the safe hypervisor also helps protect users from potentially high costs associated with vendor lock-in.

Functional safety is driven by international standards that require the use of proven technology for building systems that reduce risk and liability. For example, if a robot detects a

Applicable Standards

Intel is working with RTS on development of a safe hypervisor that will facilitate workload consolidation with functional safety. Select Intel Atom, Core, and Xeon processors will be certified to meet rigorous industry standards worldwide.

- **IEC 61508**
  Functional safety of electrical/electronics/programmable electronic safety-related systems
- **ISO 13849**
  Safety of machinery - Safety-related parts of control systems
- **IEC 62304**
  Medical device software - Software life cycle processes
- **EN 50128**
  Railway applications - Communication, signaling and processing systems, and software for railway control and protection systems
- **ISO 6148**
  Photography - Micrographic films, spools and cores
- **IEC 62443-4**
  Security for industrial automation and control systems
- **ISO/SAE 21434**
  Road vehicles - Cybersecurity engineering

human presence it automatically adjusts its speed or torque in order to ensure safety.

Using the RTS Hypervisor will reduce the time required for a user to obtain system certification. Intel also supports certifiable boards with the documentation required to expedite the certification process. Intel's functional safety lifecycle is part of a development process that has been certified to meet applicable standards.

Simplified system architecture and the ability to integrate pre-certified hardware and software components will enable users to focus more of their resources on developing customized applications.

The RTS hypervisor is being customized for Intel x86 chips, with the ability to scale-up to 8 core, 16 threaded processors. Target platforms include Intel Atom®, Intel Core®, and Intel Xeon® systems.

This future-proof solution enables non-safety software to be updated without touching safety critical software, and will enable software to be re-used on next-generation platforms.

Virtual machines in the safe hypervisor environment use the unified EFI specification to support standard OS booting. This defines the interface between an operating system and the platform firmware.

In addition to supporting inter-VM communication, the safe hypervisor will be able to access the software diagnostics call interface. End-users also will benefit from the ability to integrate pre-certified hardware and software components. The RTS Safe Hypervisor will maximize user flexibility by working with commercial off-the-shelf devices, drivers, and software stacks.

Supporting numerous industry use cases

The RTS Safe Hypervisor enables real-time capabilities and determinism at the same time. Some of the industrial use case examples for the RTS Safe Hypervisor include motion control, PLC, and robotics. A user can, for example, control multiple axes in a CNC machine or a robot, in real-time. This is important for situations in which operational deadlines require control loops with less than a millisecond cycle times. In the safe hypervisor environment, real-time operations run in tandem with other applications, enabling the end-user to visualize and analyze the process.

The RTS Safe hypervisor is ideal for uses in which spatial and temporal separation are needed in order facilitate determinism – predictable functionality – and safety. In a healthcare operation application, for instance, the safe hypervisor can facilitate simultaneous device monitoring and patient communications.

In the transportation sector, a safe hypervisor can improve the functionality of railway switches. A train operator, for example, relies on functional safety in the railway signaling system to help ensure that the ability to safely switch tracks, and to maintain a safe distance from other trains.

Customers using a safe hypervisor can control multiple workloads on the same device. This means that single-chip high-end programmable logic controller (PLC) implementations can be enabled with secure enterprise cloud connectivity and a human machine interface (HMI) that facilitates command and control. Intel's HMI solution utilizes the Field Programmable Gate Array (FPGA) fabric, enabling HMI integration in the same SoC as the PLC. This frees the hard processor system from having to handle HMI-related graphics computations.

The RTS Safe Hypervisor is ideally suited for enterprise-level computing platforms. Customers can customize their own mix of operating systems and build applications that can be safely integrated. This enables enterprise users to provide customizable platforms with additional functionality for their own end-users.

Conclusion

Release of the RTS Safe Hypervisor is planned for the first half of 2023. The new hypervisor will complement Intel's functional, safety-enabled IoT processors. Customers will benefit from both Intel and RTS expertise, an optimized product lifecycle, proven software tools and methodologies, and comprehensive technical documentation.

Intel uses software tools and methodologies to standardize and automate the safety analysis of its SoC devices. Moreover, hardware-based diagnostics, software libraries, and related technical documentation help enable customers to create high-performance, functional, safety-compliant computing systems that are affordable and scalable. With the release of the RTS Safe Hypervisor, customers will get high-performance hardware solutions with unparalleled functional safety capabilities.

For more information about the RTS Safe Hypervisor, please visit real-time-systems.com or contact us at info@real-time-systems.com

For more information about Intel® IoT Technology and the Intel IoT Solutions Alliance, please visit intel.com/iot

Notices & Disclaimers