ECF EMBEDDED CONFERENCE FINLAND

SEPTEMBER 6 - 2022 - HELSINKI

RTS Safe Hypervisor

What it is and how it works

Andrea J Beuter

REAL-TIME SYSTEMS

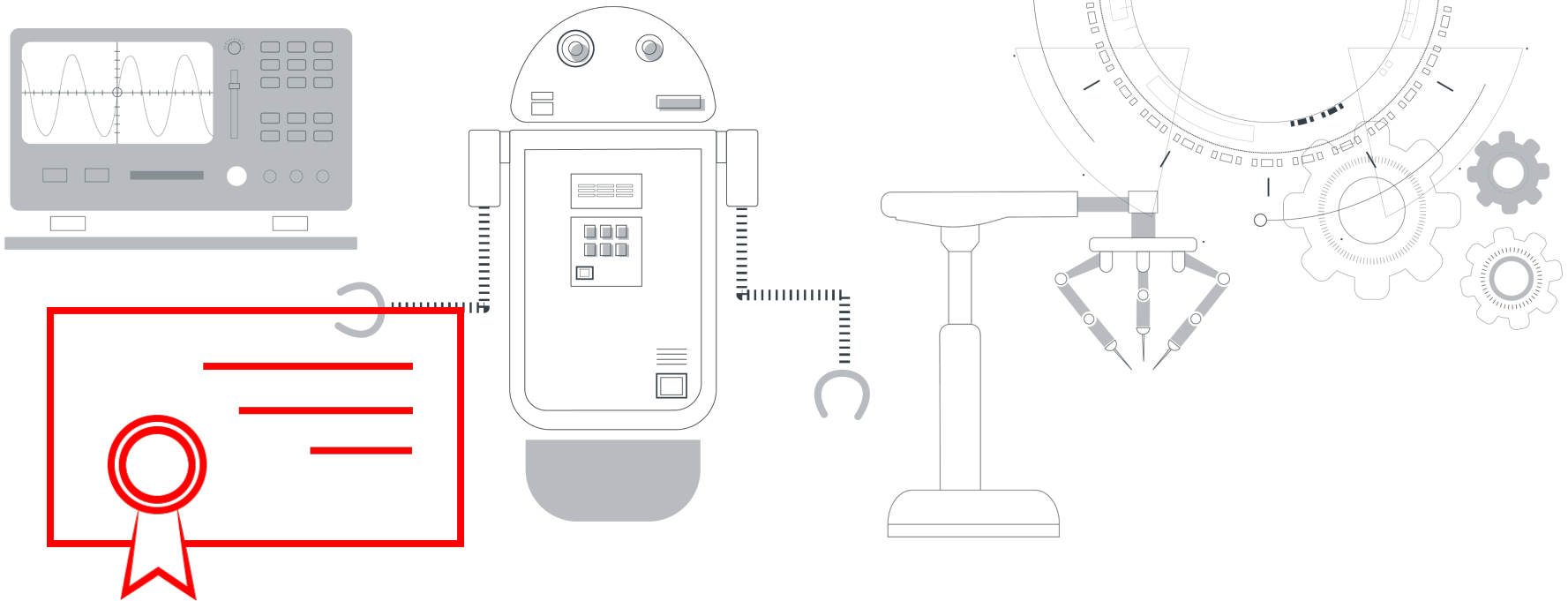
Who we are

- Market leader for hypervisor technology for the General Embedded market
- Experts in real-time virtualization
- Intel® co-development partner
- Founded 2006 in Ravensburg, Germany as spin-off from KUKA Robotics
- Member of Congatec since 2018
- Operating independently
- Customers in more than 25 countries worldwide
- More than 100,000 hypervisor systems in use

Where we are located

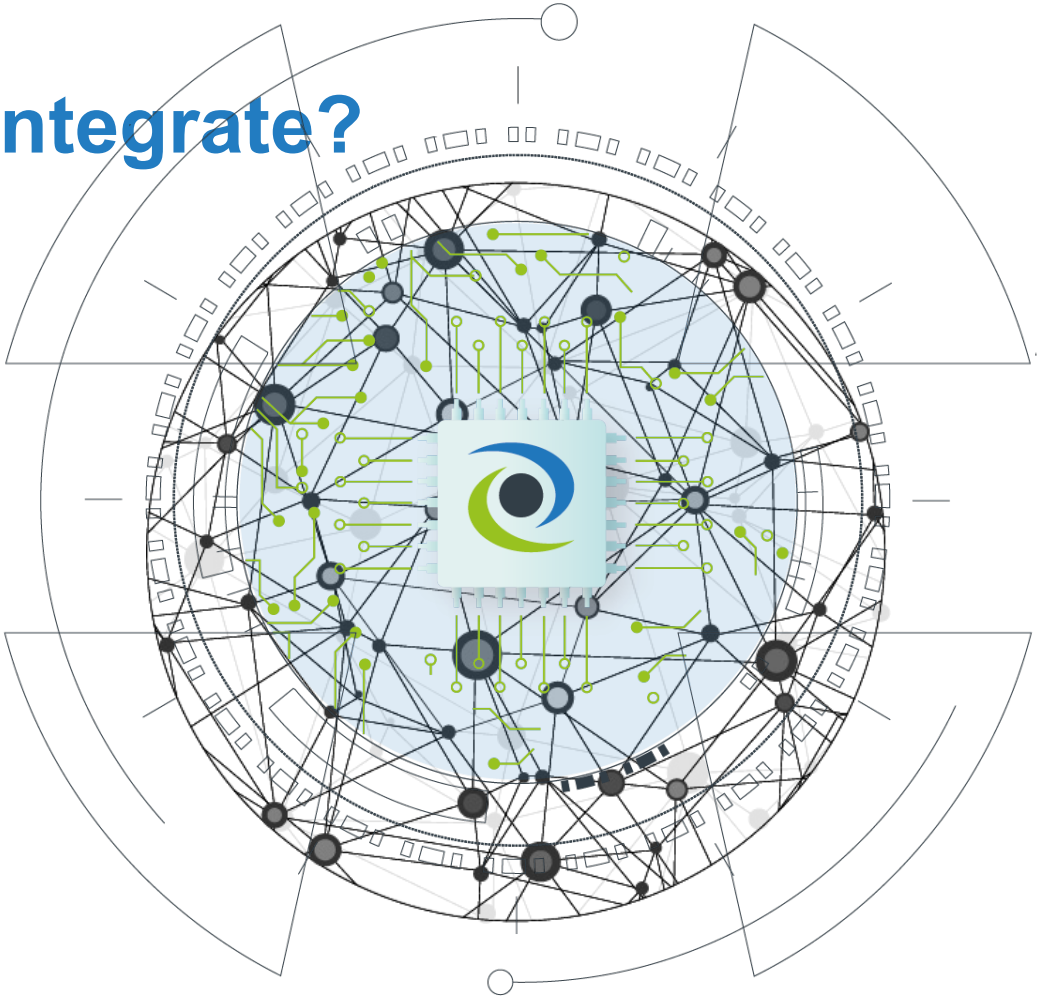
Situation to date

- Todays and future applications tend to offer more functionality

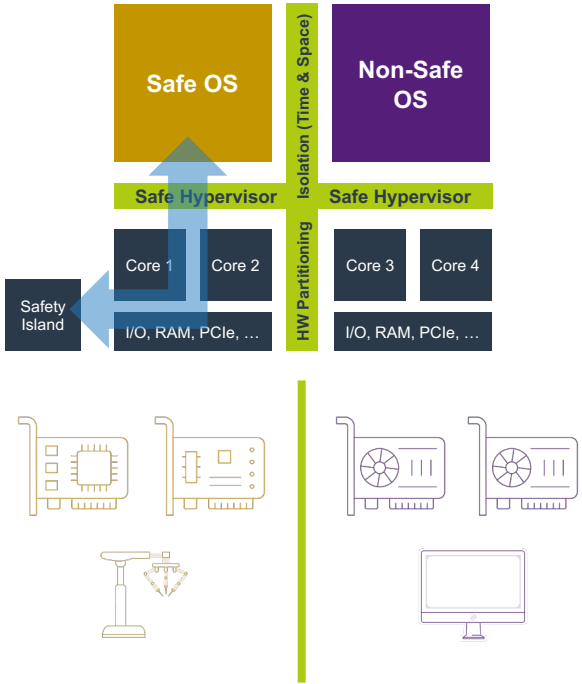


REAL-TIME SYSTEMS

How to integrate?



Basic Concept

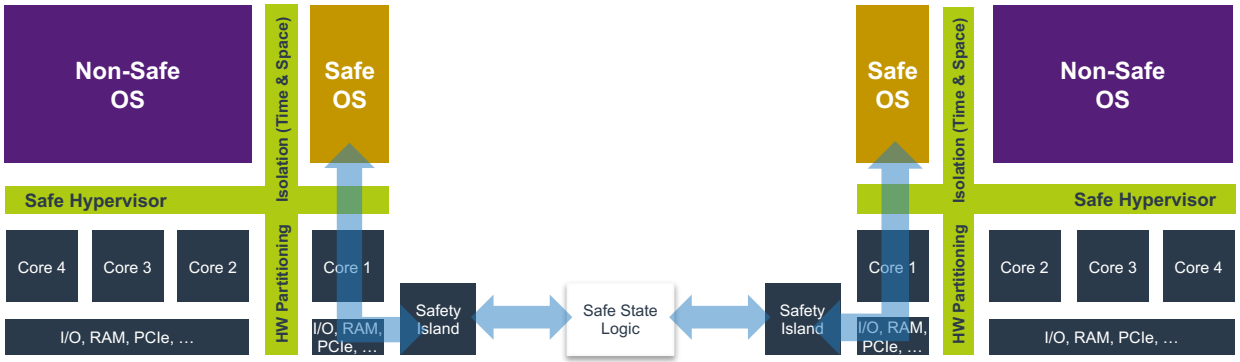


- Intel Atom, Core, or Xeon
- Example: Quad-core processor
  - Two processor cores per VM
- Integrated or external safety island pass-through
- PCI pass-through to exclusively assigned devices

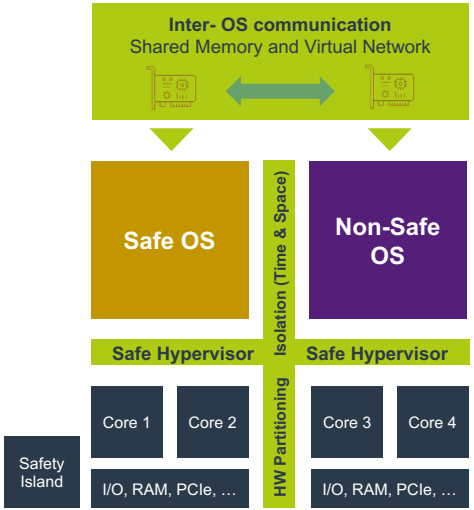
REAL-TIME SYSTEMS

Example: 1 out of 2 Configuration

- Two Atom, Core, or Xeon processors
- 2, 4, 6, or 8 cores per processor
- One core per processor used for the Safe OS



Inter-OS Communication

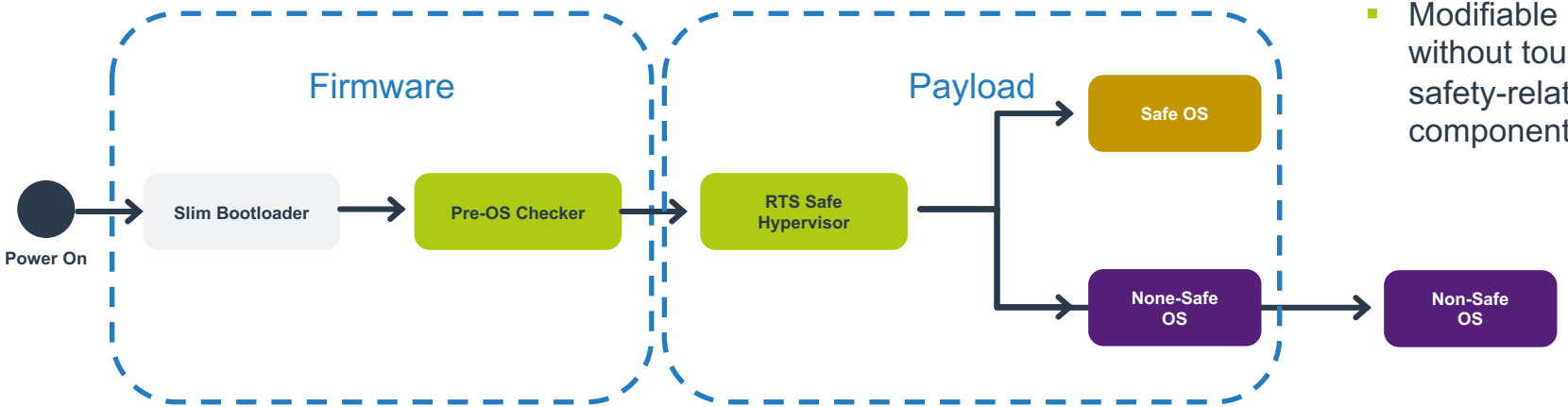


- Emulated PCI devices are shown to every OS:
  - Shared Memory and Interrupt device
    - “Virtual PCI memory” is shared between the OSs.
    - Interrupt capability allows OSs to signal each other (doorbell mechanism).
  - Network device
    - Use standard protocols and services.
    - “Bridge” external traffic through the internal network.
- State-of-the-art virtual devices, drivers exist for multiple OSs.
- Security: Selectively turn interfaces on or off.

Boot Sequence

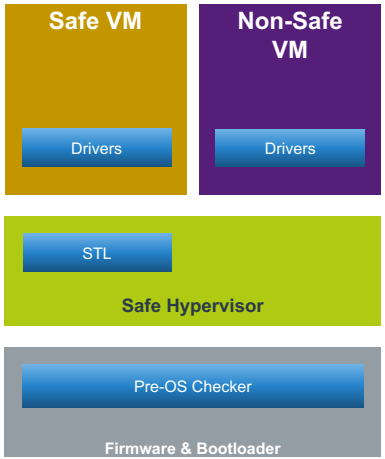
- Slim Bootloader
  - Open source https://slimbootloader.github.io/
  - Safety-related Pre-OS Checker integrated
  - Container for certifiable or locked components
    - Flashed into the firmware or loaded from the disk

- Non-safe OS located on the disk
  - Modifiable without touching safety-related components



REAL-TIME SYSTEMS

Software Stack



Provided by RTS:

- Safe Hypervisor
  - Including Software Test Libraries (STL)
- Pre-OS Checkers for all target platforms
- Drivers & Services for OS
  - Inter-VM Communication
  - Safety Island access

REAL-TIME SYSTEMS

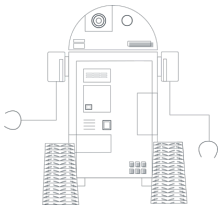
Markets / Applications

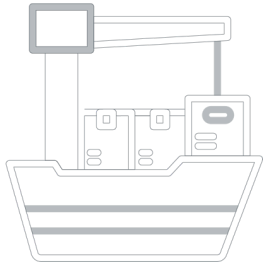
- Collaborative Robots and Devices
- Autonomous Vehicles / Robots
- Transportation / Railway
- Medical Equipment
- Heavy Machinery
- Agriculture
- Industrial Automation

REAL-TIME SYSTEMS

Applicable Standards

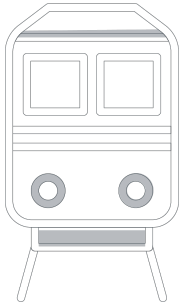
IEC 62304

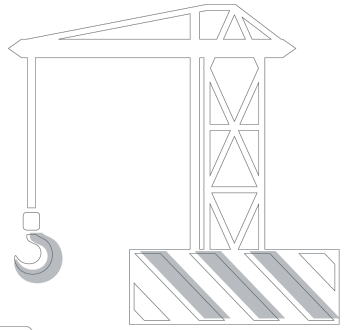




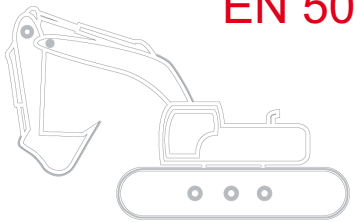
IEC 62443

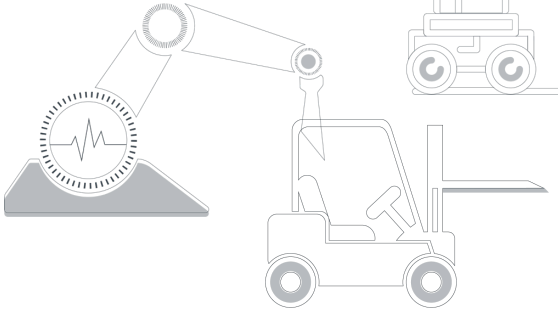
IEC 61508

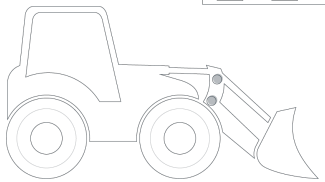




EN 50128







ISO 13849

REAL-TIME SYSTEMS

Applicable Standards

- **IEC 61508 SIL 3**
  - Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems
- **ISO 13849 PLe**
  - Safety of machinery – Safety-related parts of control systems
- **IEC 62304 Class C**
  - Medical device software – Software life cycle processes
- **EN 50128 SIL4**
  - Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems

- **IEC 62443-4-1** and **IEC 62443-4-2**
  - Security for industrial automation and control systems

REAL-TIME SYSTEMS

Target Platforms

- Intel Atom (Elkhart Lake)
  - Safety Island integrated in SOC
  - IEC 61508 certified
  - Dual-core / Quad-core
- Intel Core / Intel Xeon (Tiger Lake)
  - External Safety Island
  - i-5 / i-7 Quad-core
  - Xeon W Six-core or Eight-core

REAL-TIME SYSTEMS

Benefits

- Independent
  - Choose which operating systems to use, no vendor lock-in
  - Update non-safety software without touching safety critical software
- Optimized
  - Specifically developed for x86
  - Scales from **Atom** to **Core** to **Xeon**, up to 8c/16t
- Future-proof
  - Benefit from x86 performance and flexibility
  - Re-use software on next-gen platforms

- Save costs
  - Run safety related and non-safety related software side-by-side on a single hardware platform
  - Less hardware, simplify the system architecture
- Shorter Time-to-Market
  - Integrate pre-certified hardware and software components, focus on your application
  - Use COTS devices, drivers, software stacks
- Designed for hard real-time
  - Pass-through for assigned devices

Thank you for your attention.

www.real-time-systems.com