Virtual Open Systems

Company and technologies presentation

Mixed-critical virtualization
Done right

Virtual Open Systems: Profile

- Virtual Open Systems (VOSyS) is a French **fully independent & private software company** created and **operating since Jan 2011**:
  - **self-sustained, profitable**
  - share capital of 507 240€, **no debt with strong financial**
- The core activity is about **design and implementation of high-performance mixed-critical virtualization solutions** on low-power multi-core & heterogeneous Arm, x86 and RISC-V platforms:
  - VOSyS has been the first company to port KVM on ARM in collaboration with Columbia University
  - VOSyS created and is a key contributor of the Automotive Grade Linux Virtualization Expert Group
- Operating in market vertical segments requiring virtualization technologies addressing mixed-criticality:
  - **Automotive, Industrial, IoT-Edge Computing**, SATCOM, energy Power-Breakers, Drones, NFV, ..

Virtual Open Systems: Mission & strategy

Foundation company statements

- **Mission** – Enable customers to gain competitive advantage
- **Values** – Believe in open source, industry standards, Customer satisfaction
- **Vision** – Become worldwide leader in mixed critical virtualization and accelerators virtualization
- **Strategy** – Continuous re-inforcement of activity for competitive mixed-critical virtualization hw/sw solutions in Safety-aware & security constrained systems (e.g., Automotive, Industrial, IoT edge, ..)

Virtual Open Systems business model

Research, Innovation & International Visibility

- Innovation, open source and international exposure drives the company Services

Custom Design & Development services

- The company provides services in the virtualization domain on an international landscape to serve customers in different market segments
- Market segments includes mixed-critical systems (e.g., energy power breaker, industrial, automotive, etc.), cloud & edge computing, etc.
- Customers include first tier companies from EU, Far-East, North America

Virtualization Know-how Productization

- The acquired know-how in virtualization is being used by the Company to develop its own **Virtualization product roadmap**.

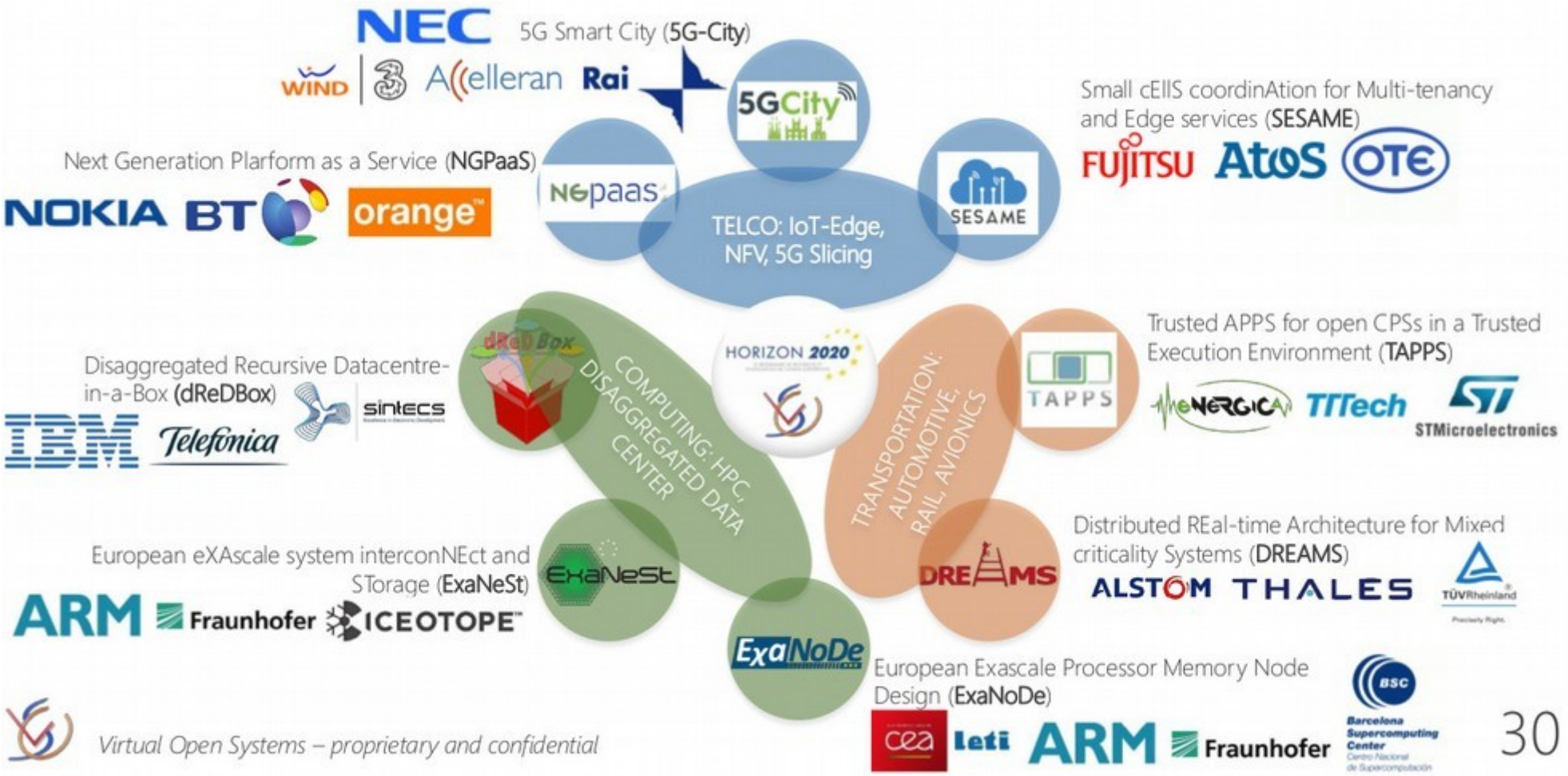
Research, Innovation & International Visibility

Virtual Open Systems: Visibility

International Exposure

- Involvement in several **software open source** projects:
  - Linux kernel, PSCI, VFIO
  - Automotive Grade Linux
  - KVM, QEMU, LibVirt, VirtIO, vhost-user, mttcg,
  - But also Snabb, OpenStack, OPNFV, etc..
- Partner in EU funded **research & innovation pr**
- Membership in international initiatives
- Several **scientific** papers & international events **dissemination**
- 6 **patents** filed in US and EU

Virtual Open Systems: R&D Projects history



ENOCH

Virtual Open Systems role:

- Design and development of a virtualized Electronic Control Unit for high performance electric motorbikes
- Target platform are STM32MP1 and Raspberry Pi 4

AERO

Accelerated EuRopean clOud (AERO) Horizon Europe Project

sednai · MANCHESTER 1824 The University of Manchester · codeplay · SIPEARL · PIERER INNOVATION · Università di Pisa · FORTH Foundation for Research and Technology - Hellas · ICCS · Red Hat

VOS role is related to the development of virtualization extensions:

- Virtualize EU processor hardware accelerators with extensions targeting KVM, rust-vmm and emerging lightweight virtual machines (VMs)
- Trusted-cloud computing extensions based on the VOSySmonitor product aiming at providing VMs with a secure enclave to process sensitive data

VITAMIN-V

Virtual Environment and Tool-Boxing for Trustworthy Development of RISC-V based Cloud Services (Vitamin-V)

VOS role in the project:

- Open source development for KVM, QEMU and rust-vmm on RISC-V
- Development of VOSySmonitoRV, a system partitioner for the RISC-V architecture which is inspired by VOSySmonitor
- Port the rust-vmm open source project to RISC-V support for exploitation on the VOSySzator company product

Nancy

NANCY

- An Artificial Intelligent Aided Unified Network for Secure Beyond 5G Long Term Evolution (NANCY)

NEC ERICSSON tecnalia OTE GROUP OF COMPANIES i2cat Italtel UBITECH THALES

VOS role in the project:

- Design and development of the an AI Virtualiser, to enable the exploitation of under-utilized resources
- VOSySmonitor extensions to provide an isolated execution environment where to isolate the offloaded tasks both on the edge and in the cloud

Virtual Open Systems: Last Publications

Virtual Open Systems disseminates its results through scientific publications at international conferences; it counts about 50 **publications**, of which the most recent:

- SVFF+: Kubernetes FPGA virtualization and reconfiguration for network virtualization, **ICT25**
- Cross-Compartment Virtio-Loopback: A Bare-Metal Virtualization Solution for the Edge, **ESARS-ITEC24**
- VOSySzator: A flexible embedded RISC-V system virtualizer targeting the cloud, **RISC-V Europe 24**
- Technical Overview & Performance Evaluation of Virtio-loopback, **ICAI 2024**
- Virtio-FPGA: a virtualization solution for SoC-attached FPGAs, **ESARS-ITEC 2023**
- SVFF: An Automated Framework for SR-IOV Virtual Function Management in FPGA Accelerated Virtualized Environments, **CITS 2023**.
- VOSySmonitoRV: a mixed-criticality solution on Linux-capable RISC-V platforms, **MECO 2021**
- x86 System Management Mode (SMM) Evaluation for Mixed Critical Systems, **APPLEPIES 2020**
- vFPGAmanager: A Hardware-Software Framework for Optimal FPGA Resources Exploitation in Network Function Virtualization, **EUCNC2019**
- Cloud and Edge Trusted Virtualized Infrastructure Manager (VIM) – Security and Trust in OpenStack **WCNC2019**
- The Next Generation Platform as a Service, Cloudifying Service Deployments in Telco-Operators Infrastructure, **ICT2018**
- Lightweight and Generic RDMA Engine Para-Virtualization for the KVM Hypervisor, **HPCS2017**

...

IP Protection by Patents

IP protection is a strategic investment for Virtual Open Systems.

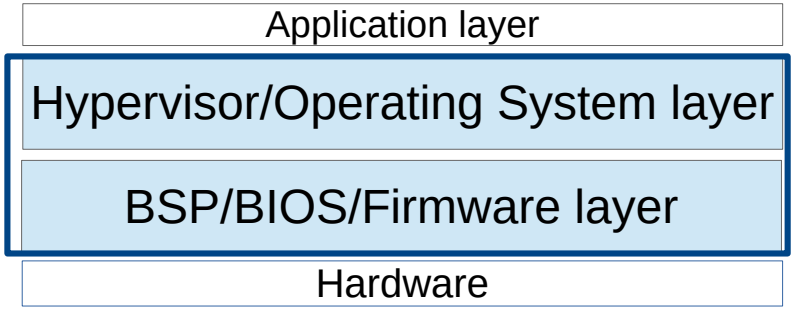
- **Compute node supporting virtual machine and services (US grant, EU exam.)**
  - A computing system able to accelerate multiple OSes in a mixed criticality environment, enabling IVI and Cluster coexistence in a single HW platform
- **Virtualization manager for reconfigurable hardware accelerators (US/EU exam.)**
  - HW IP enabling FPGA accelerators virtualization in a smart re-configurable, orchestrated manner for computer vision, networking and ADAS applications, space
- **Interrupt controller for mixed criticality virtual machines (US grant, EU exam.)**
  - ARMv8 Interrupt controller designed to improve performance and reduce interrupt latency in mixed critical and virtualized environments (e.g., automotive, industrial ..)
- **vSwitch for multi compartment mixed critical network communication (US/EU grant)**
  - Accelerated virtual switch infrastructure for accelerated compute node OSes with mixed levels of criticality. It enables high performance and secure communication between different critical worlds
- **Disaggregated Computing Architecture (US grant)**
  - Disaggregate computing architecture with independent physical address spaces between systems nodes in a single execution environment for data centers, smart cities, connected vehicles
- **System platform initializer for mixed criticality system (US grant, EU exam.)**
  - Execution of an isolated and secure operating system in x86 systems by means of the System Management Mode (SMM) and targeting cyber security, automotive, space

Custom Design & Development services

Customer activities

VOSyS development services focus on the development of the software lowest layers including mixed-critical systems and virtualization

- Performance profiling and optimization
- Embedded, mixed critical software and API/frameworks:
  - Design and development
  - Maintenance, porting, emulation, enhancements
  - Debug and problem solving
- Testing and continuous integration
- Open source projects extensions
- Documentation and knowledge transfer



Virtual Open Systems: Track Record
Top-player customers development services

- **With major outcome as open source contributions**
  - KVM on ARM => **Paving the way towards virtualization in embedded systems**
  - KVM and VCPU Hotplug for ARMv8 => **Better resource utilization in the Virtual Machines**
  - VFIO, IOMMU for ARMv7/8 => **Support for device pass-through in Linux**
  - Support of the VFIO framework on QEMU => **Support for device pass-through in QEMU**
  - RFC for QEMU infrastructure for ACPI and VFIO => **Emulation of ARMv8 servers**
  - Multithreaded TCG, atomic instruction emulation => **Real multi-core virtual machine emulation**
  - Vhost-user => **fast networking switches**

Virtual Open Systems: Track Record
Industrial Product Engineering

- Energy management top-player customer cases:
  - VOSySmonitor **designed-win** in several customer products
  - Development of firmware management layer for low/medium voltage power breakers based on **VOSySmonitor**
  - Development of custom firmwares for Renesas RZ-N1D and Altera Cyclone V based on **VOSySmonitor**

Altera Cyclone-V

Renesas RZ-N1D

Virtual Open Systems: Track Record Automotive Product Engineering

- Automotive top-player customer cases:
  - VOSySmonitor product **designed-in** at several **Tier-1** customers
  - Development of custom firmware for Renesas R-Car H3/M3, NXP iMX8, NXP S32G, Xilinx UltraScale+ MPSoC, Nvidia Jetson TX1, Mediatek MT2712 based on **VOSySmonitor**

Xilinx MPSoC US+

NXP S32G

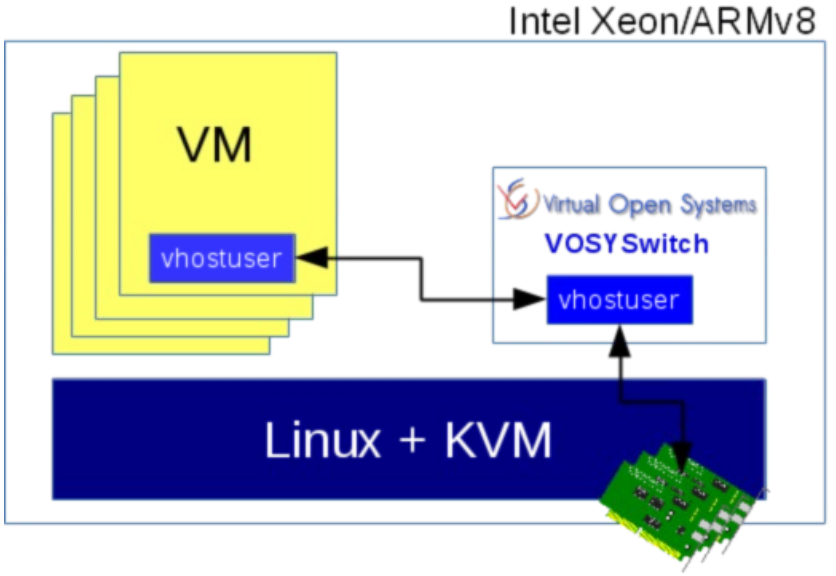
NXP iMX8

Renesas R-Car H3/M3

Mediatek MT2712

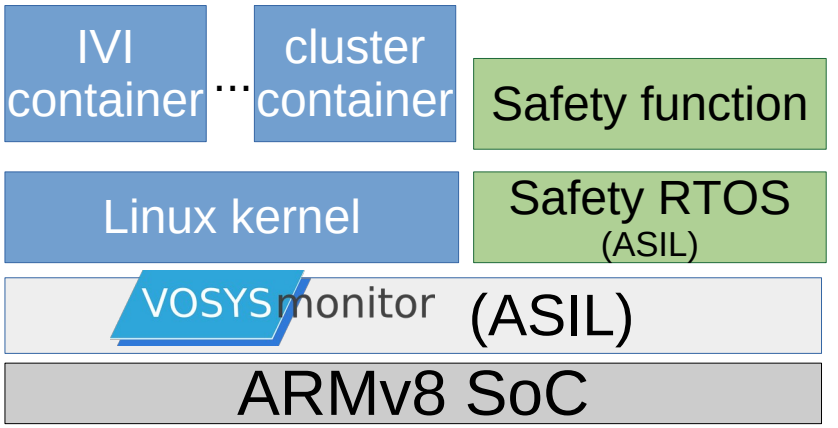
Virtual Open Systems: Track Record virtual switches customization

- Customization of open source network virtual switches
  - Support of custom setups based on DPDK and other networking solutions
  - Evaluation and benchmarking on optical links
- Optimization and tuning of virtualization technologies (KVM, IRQfd, vhost, etc.) to achieve the best performance across VMs and between the host and the VMs



Virtual Open Systems: Track Record
Containers extensions for automotive

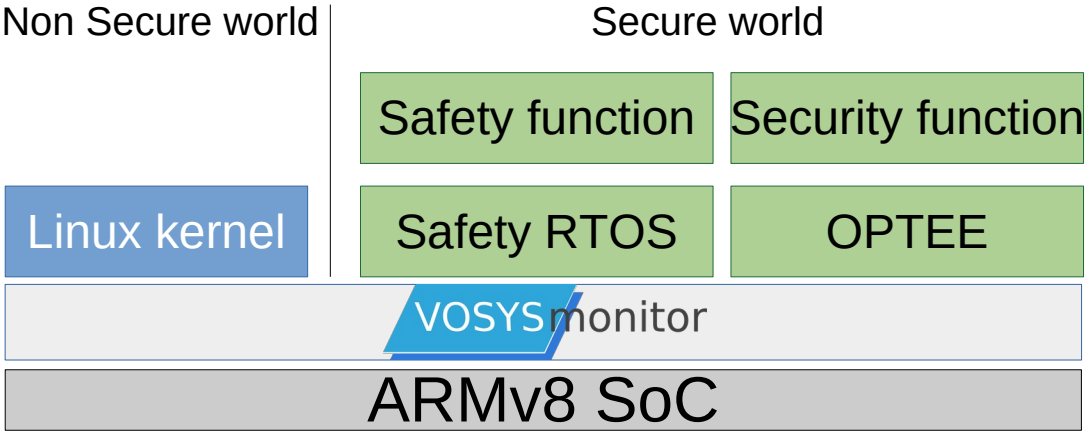
- Development services for extending existing container technologies to support mixed criticality environment
  - Customized devices passthrough (USB, GPU, etc) implementation and benchmarking
  - Multiple displays support
  - Safety and non safety communication mechanisms design and implementation



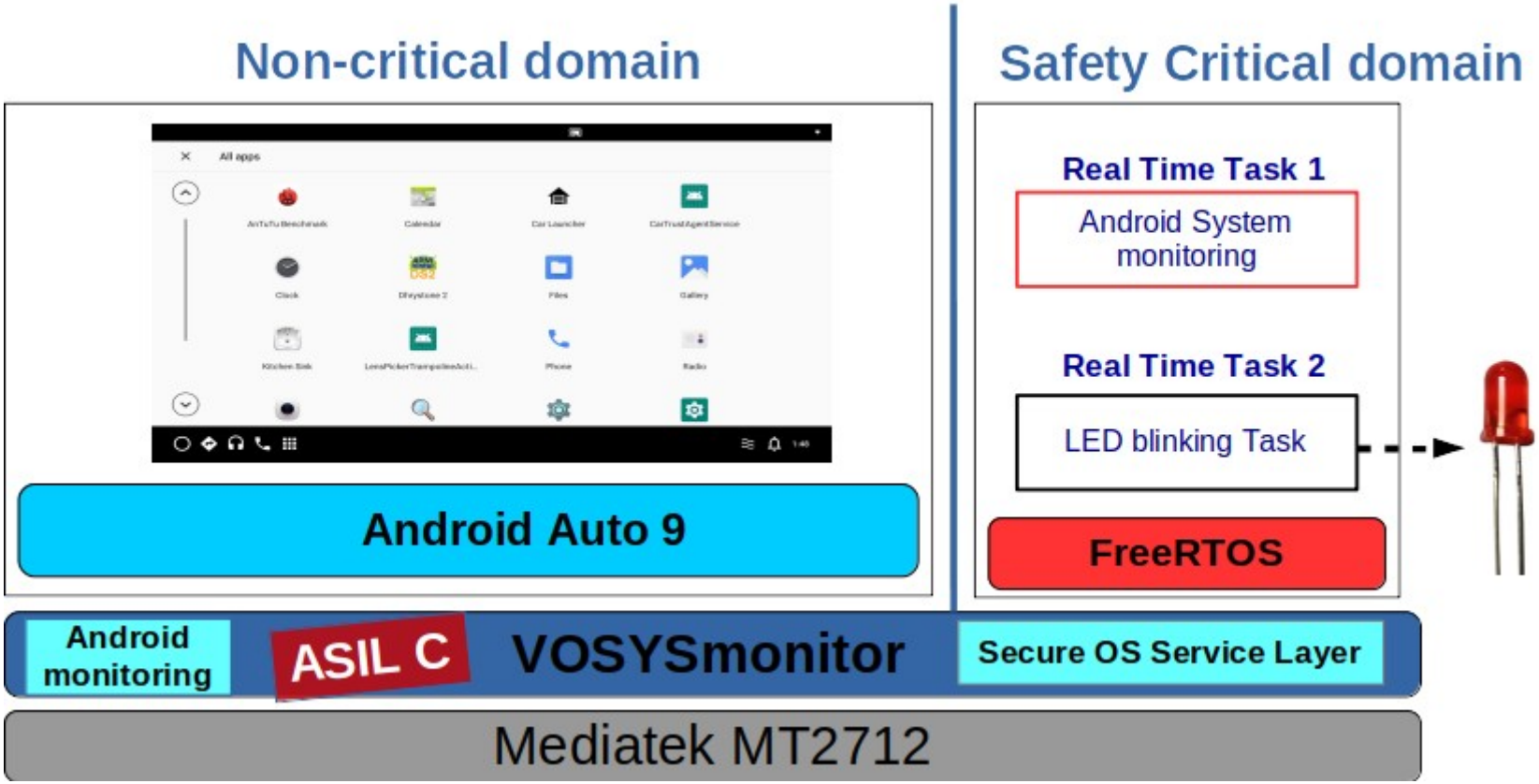
Virtual Open Systems: Track Record
VOSySmonitor porting and extensions

- Development services for mixed criticality environments
  - Customization
    - Secure World Safety RTOSes porting (FreeRTOS, VxWorks, eMCOS, Linux, etc)
    - Secure World Multi Secure OS execution (OPTEE with RTOS, etc)
    - Shared memory commuinication extensions based on VOSYSVirtualNet
  - VOSySmonitor porting
    - TI AM64x, S32G,

      STM32MP1, RPi4, etc
    - Custom platforms
  - Testing and benchmarking



Virtual Open Systems: Track Record
VOSySmonitor MT2712 porting



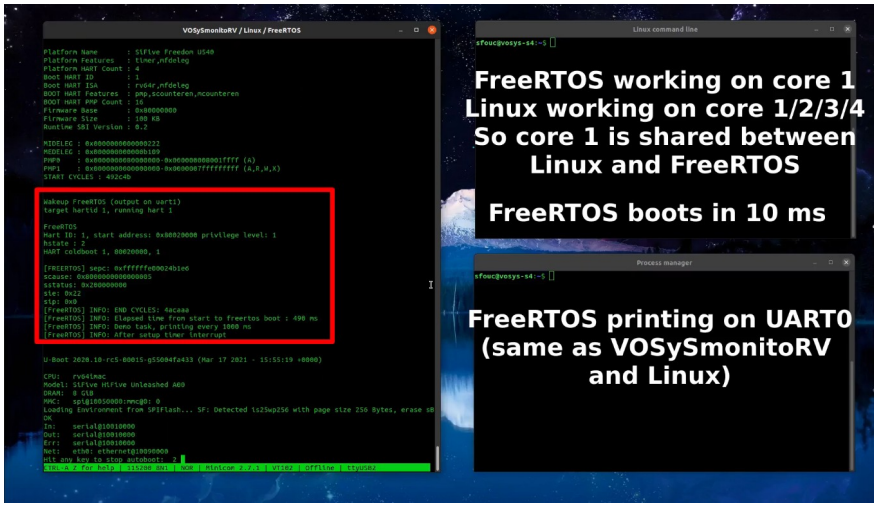
Virtual Open Systems: Track Record
VOSySmonitor MT2712 porting

Item	Description	Performance results
Safety critical OS boot time	Full boot time needed to enter in the Safety critical OS from a Power-On operation.	265ms (including **1ms** of VOSySmonitor setup time)
Safety critical OS FIQ latency	Overhead induced by VOSySmonitor context switch to forward an FIQ to Safety critical OS	Average = **1,6µs - 4,33µs**
Android AnTuTu benchmark	Benchmarks for Android devices that test/stress several parts of a device and assigns a score	Native Android: **91201** Android with VOSySmonitor: **86367**
Android Drhystone benchmark	Computing benchmark (integer) that allows to measure the general CPU performance	Native Android: **Avg=188,9ms** Android with VOSySmonitor: **Avg=191,1ms**
Non-critical domain IRQ latency	IRQ latency of non-critical domain induced by prioritizing Safety critical domain execution	Native Normal world app: **4,33µs** Normal world app with VOSySmonitor: **4,33µs**

VOSySmonitor benchmarked performances on Mediatek MT2712 platform

Virtual Open Systems: Track Record
RISC-V mixed criticality pioneering

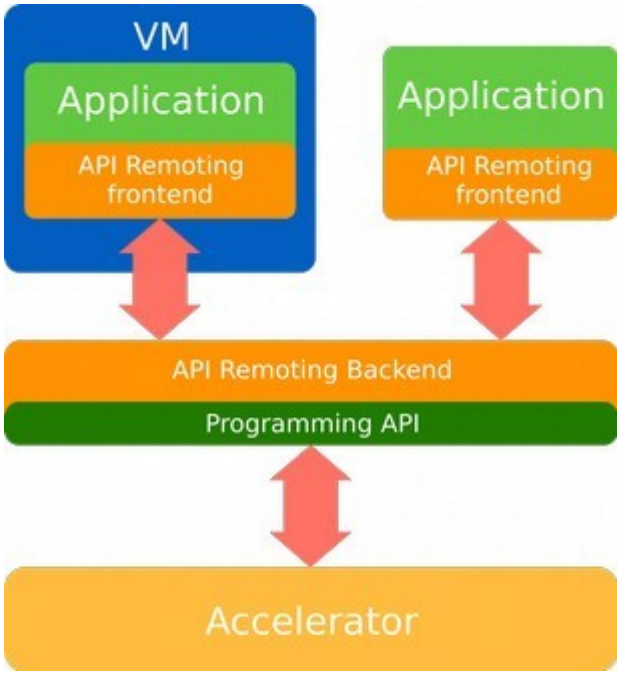
- Development and prototyping mixed critical solutions for emerging RISC-V platforms
  - VOSySmonitor porting to RISC-V (VOSySmonitoRV)
    - Reference hardware include: SiFive Unleashed, Andes ADP-XC7K
    - Concurrent execution of FreeRTOS and Linux, with core sharing enabled
    - Static core allocation supported
  - Targeting safety critical certification



Virtual Open Systems: Track Record
Virtualized access to custom IPs

- Innovative solutions in cloud and consumer cases:
  - Full design and implementation of **API remoting** solutions for **cloud servers** integrating innovative optical accelerators
  - OpenGLv2 API remoting: Full 3D acceleration within virtual machines on Odroid ARM

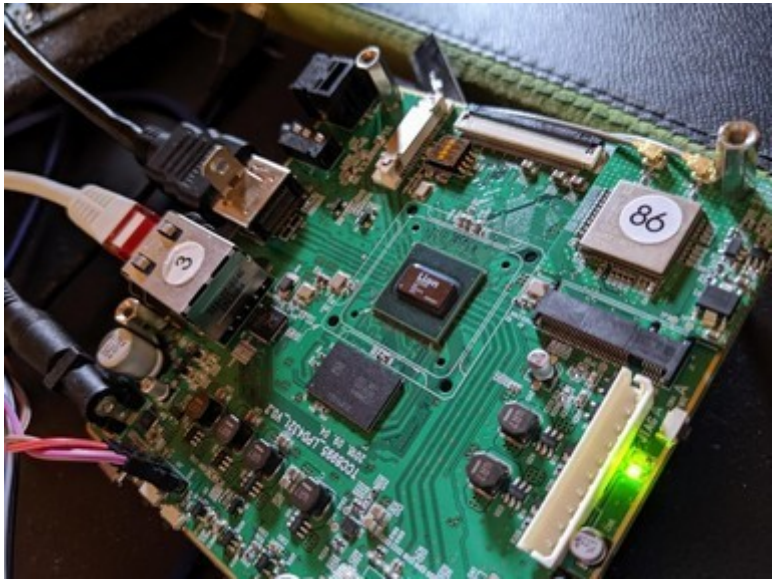
Odroid XU4



Virtual Open Systems: Track Record
High performance virtualization designs

- Design and development of custom pass-through solutions of multimedia, graphics and networking devices for All-in-one (Linux/Android Satellite, Internet, Streaming) user premises gateway of a major telecom Operator
  - Full 3D acceleration, 4K video playback and display management inside virtual machines

4K Playback inside VMs

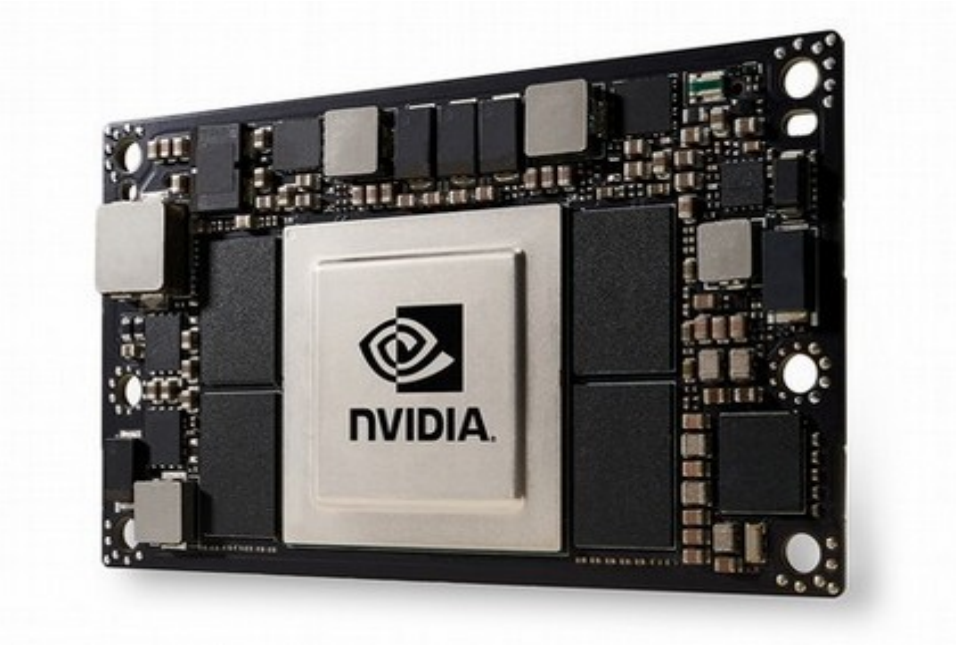


Telechips TCC8995

Virtual Open Systems: Track Record
Emulation of custom Platforms & OSs

- Development services for custom KVM extensions to run bare-metal firmwares in QEMU virtual machines on Nvidia Jetson TX1 and TX2 boards

Nvidia Jetson TX1



Nvidia Jetson TX2

Virtual Open Systems: Track Record

Virtualized development environment for rugged routers

- Development services for adapting the existing BSP of the Gateworks Newport GW6404 SBC to a virtualized execution
  - Easy applications development and debugging
  - Fast prototyping
  - No need to flash when updating the OS, a new VM image will be load
  - The router can change software stack just by switching the executing VM. Once OpenWRT is running and the following reboot another proprietary firmware is running.

OpenWrt → dd-wrt.com → **Ubuntu**

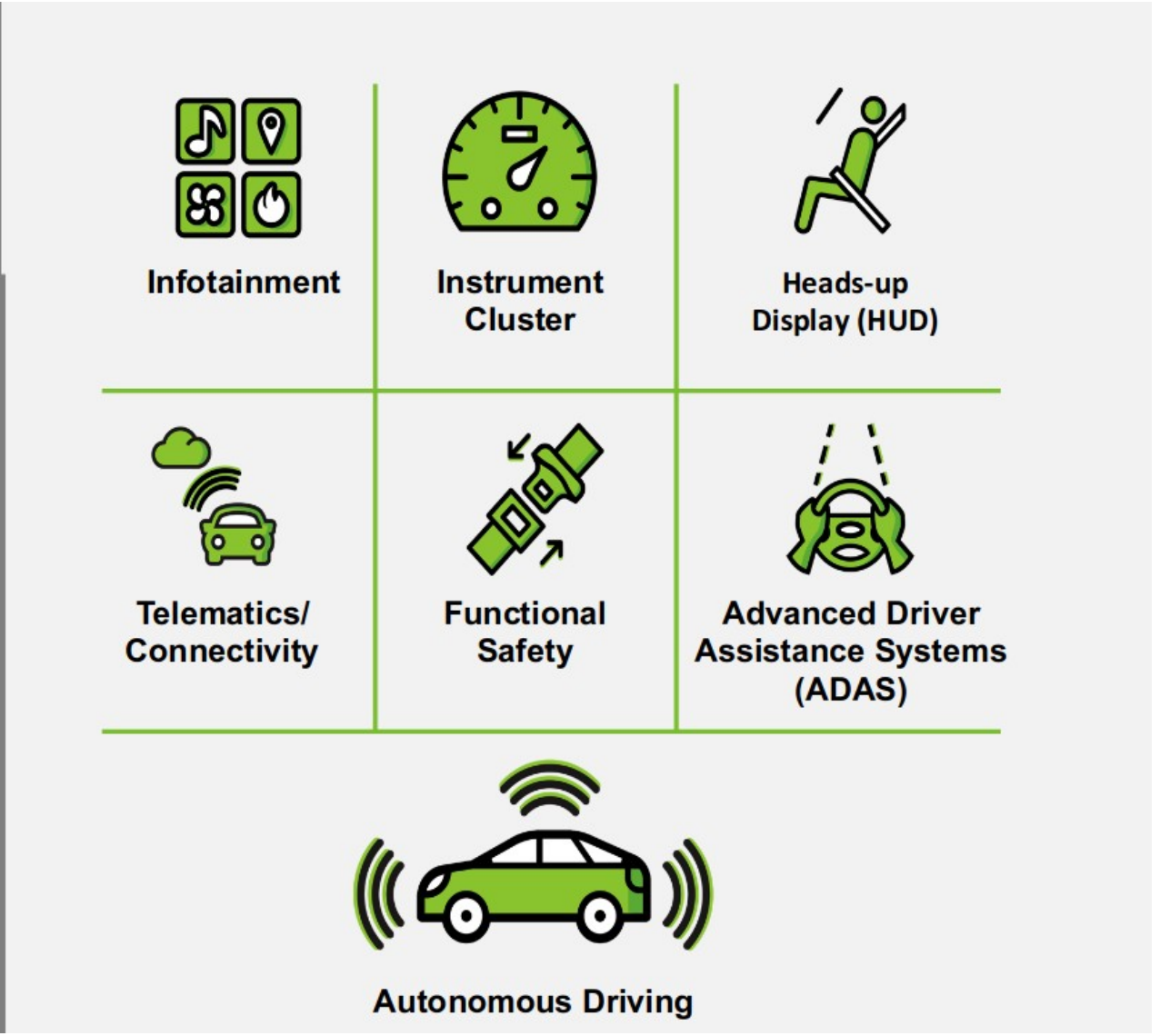
Virtual Open Systems: Track Record (RT)OS extensions

- Vast expertise in system programming suited for building complex software stacks from the ground up, including the design and implementation of components such as:
  - Drivers
  - POSIX-compliant API and their runtime
  - Testing frameworks
  - Low-latency inter-cluster communication solutions
  - KVM benchmarking and best practices in RT environments

Virtual Open Systems: Track Record: Open source/standardization activities

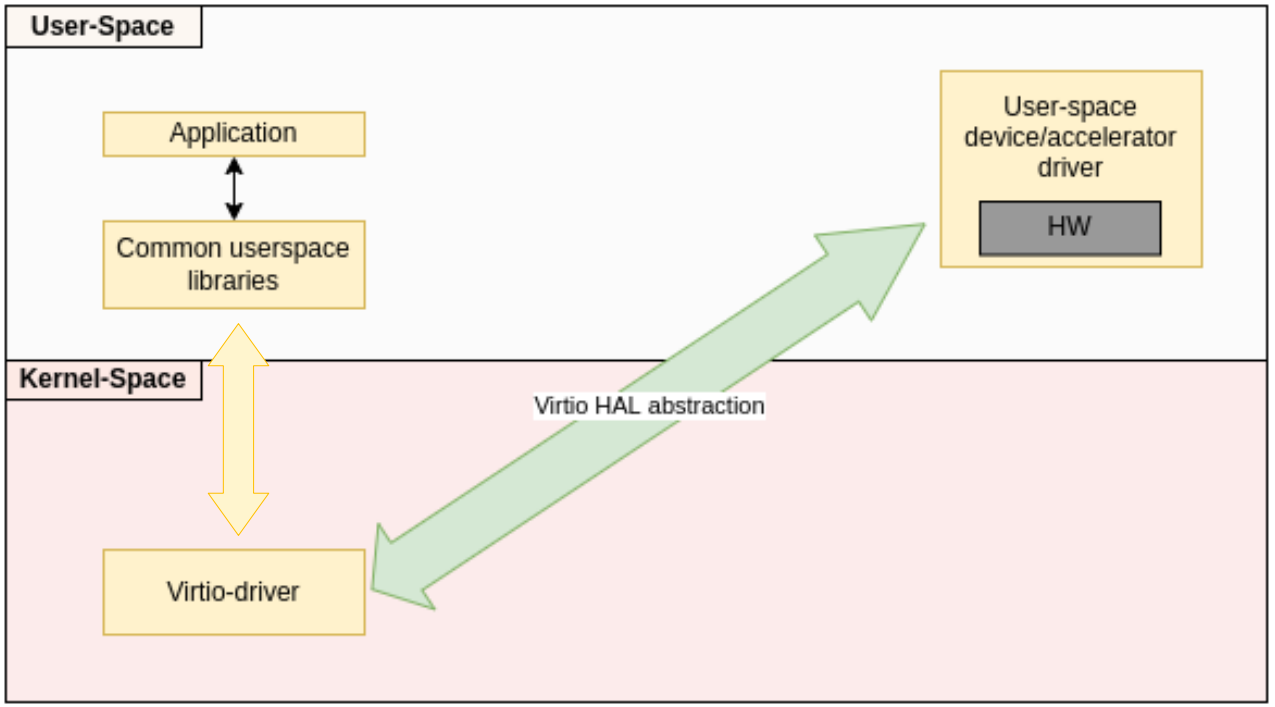
- Automotive Grade Linux (AGL)
- Waveform Architecture for Virtualized Ecosystems (WAVE)
- Rust vmm

Automotive Grade Linux



Virtio-loopback

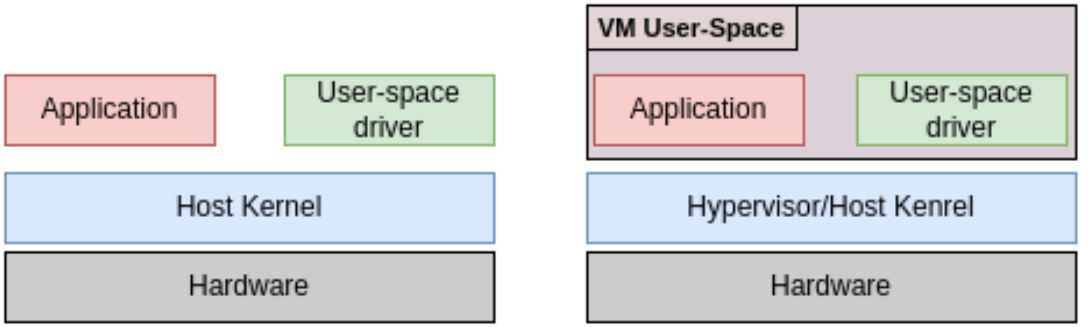
Virtio Loopback describes a new Hardware Abstraction Layer (HAL) for non-Hypervisor environments based on virtio. Development started in AGL during 2022.



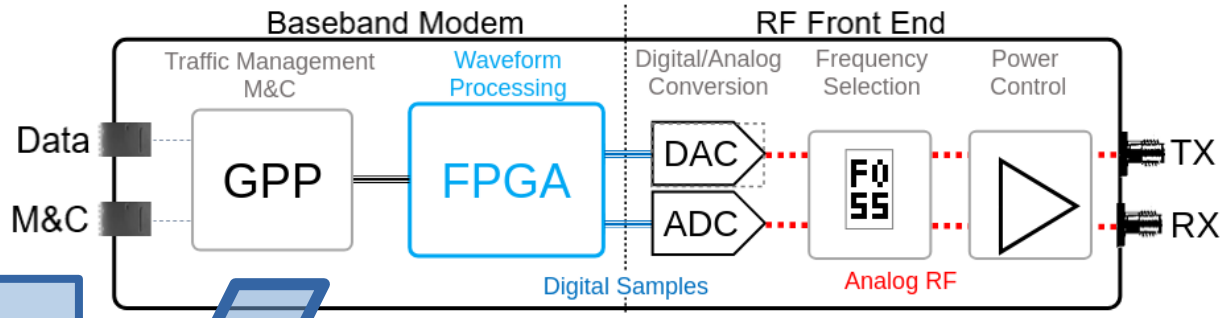
Virtio-loopback gives the ability to host user-space applications to take advantage of user-space drivers

Benefits of virtio-loopback

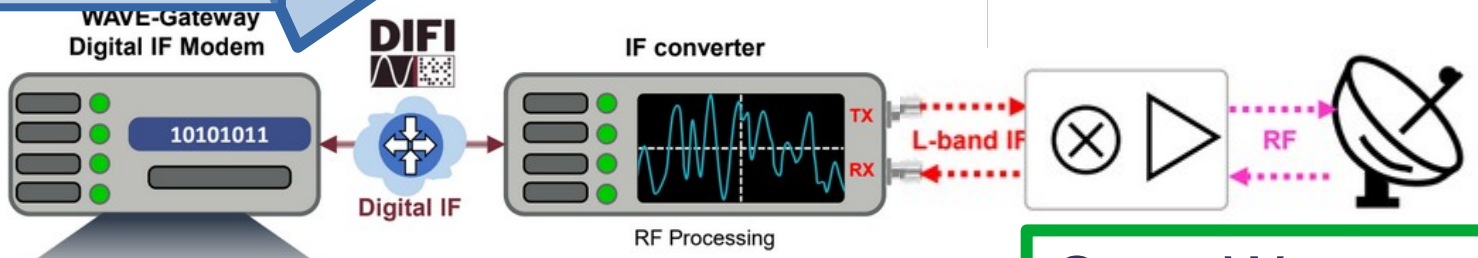
- Existing user-space application can be reused in both virtualized and non-virtualized environments
- Existing user-space driver implementations can be reused
  - Hypervisors that support virtio/vhost-user standards are fully compliant
  - No need anymore to write drivers specifically for virtualized systems
- Data (vrings) is shared between the virtio driver (kernel space) and the device (user-space)
  - No copies, higher performance!
- Host and user-space components of this architecture are fully compliant with virtio and vhost-user open standards
  - Guaranteed openness and stability

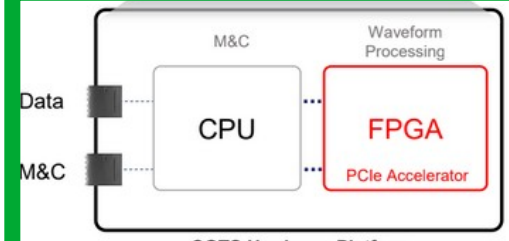


IEEE WAVE and VOS Open Wave objectives



IEEE WAVE aims at standardizing this transition

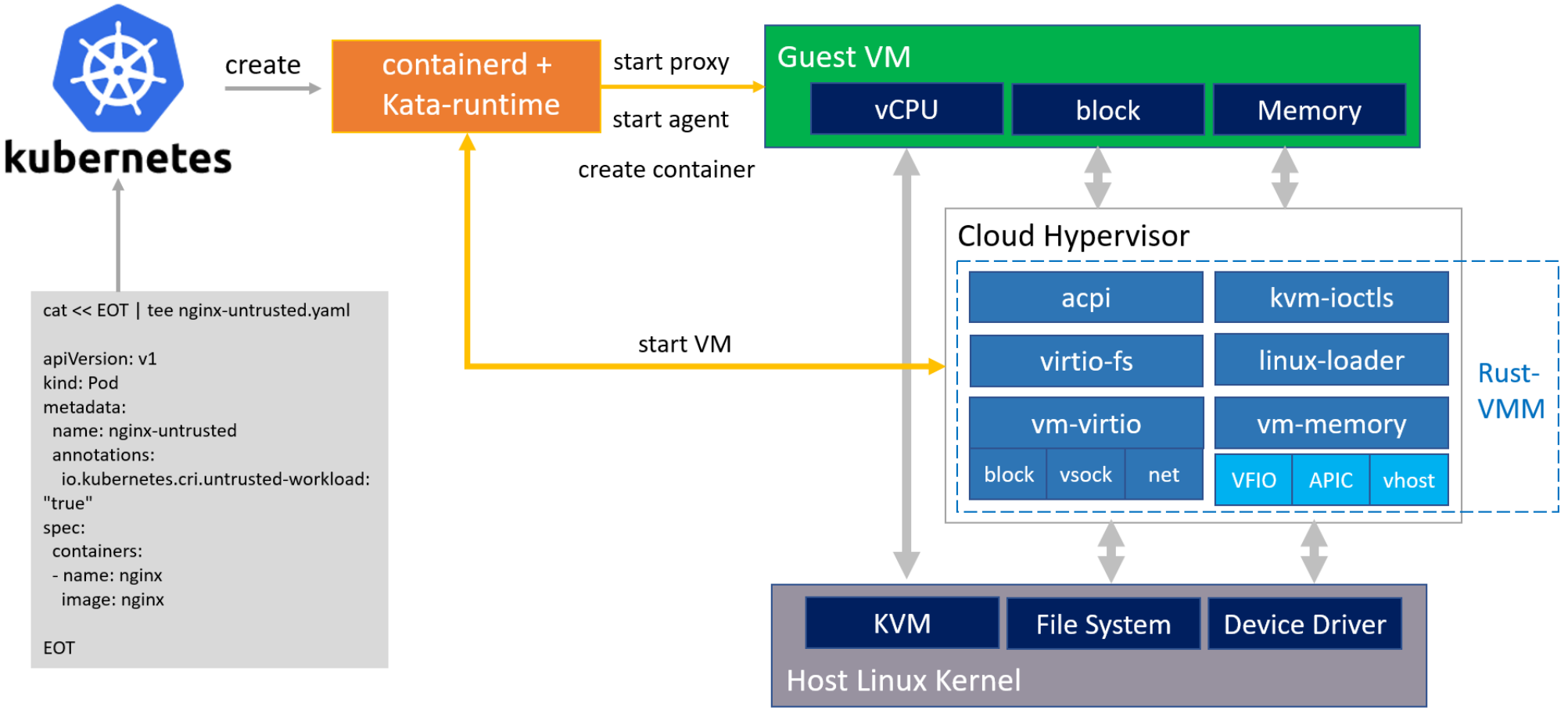




OpenWAVE project target

OpenWave targets to implement an open source version of the WAVE gateway

Rust-vmm

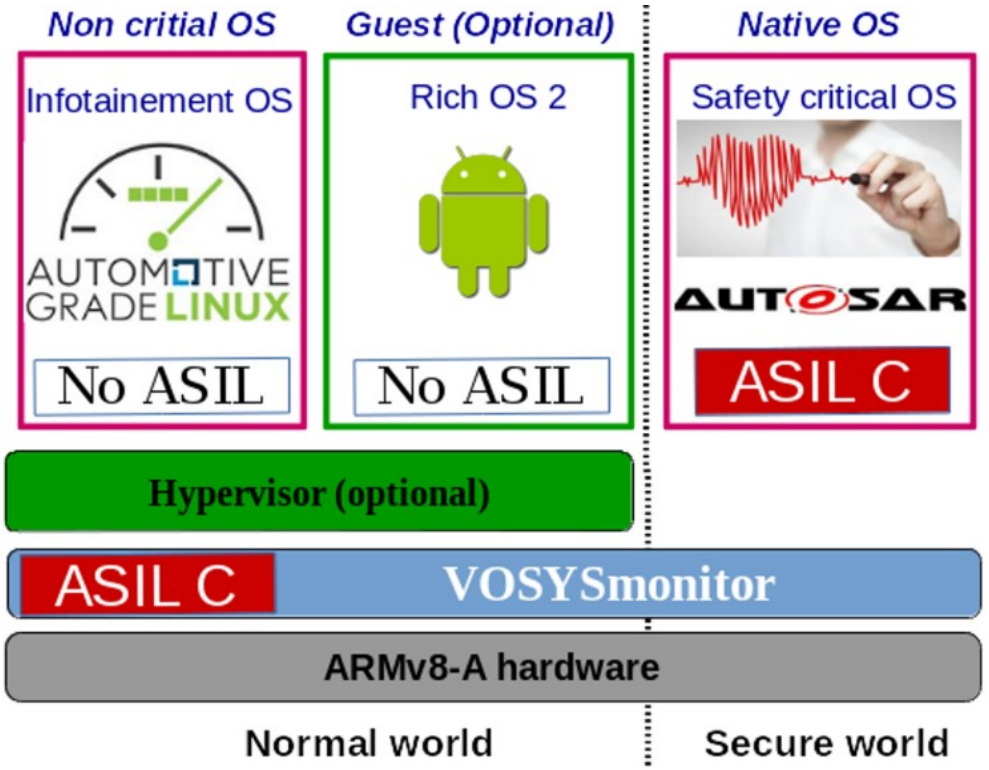


Virtualization Know-how Productization

Virtual Open Systems product: VOSYSmonitor

VOSySmonitor is an **ISO-26262 ASIL-C certified** TrustZone based virtualization layer, to maximize safety with dedicated features in strictly isolated system architecture, thus guaranteeing best in class protection for the satefy critical domain:

- A **superior isolation** building on top of ARM hw TrustZone
- **Better latency** performance while serving RTOS tasks (no context switch over-head)
- **Power management** support
- **Scaleability** to better support to increasingly complex use cases (only pay-for-what-customer-uses)



Virtual Open Systems product: VOSYSmonitor

VOSySmonitor is an **ISO-26262 ASIL-C certified** software Product

DNV·GL

PRODUCT CERTIFICATE

Certificate No.:
14390-2019-CE-FRA-ONV

Initial date:
18th March 2019

This certifies that the product

VOSYSmonitor Software Version 2.5.0 on Hardware Platform target Renesas R-Car M3 Salvator-X

Produced by

VIRTUAL OPEN SYSTEMS SAS

17 rue Lakanal - 38000 Grenoble - France

Has been assessed per the relevant requirements of:

ISO 26262 parts 1-9:2011
ISO 26262 part 10:2012

And meets requirements providing a level of integrity to:

ASIL C Capable

Safety Function:
Monitor Layer for Mixed-Criticality Systems on ARM architecture

Safety Manual
VOSYSmonitor Safety Manual - 2018-09-17

Specific Requirements:
The Safety Manual lists the Safety Related Application Conditions. The correct implementation of the Safety Related Application Conditions is in charge of the integrator.
Any changes in the product shall immediately be reported to DNV GL Business Assurance Italia S.r.l. in order to verify whether this Certificate remains valid.

Place and date:
Vimercate (MB), 18th March 2019

For the Certification Body

Zeno Beltrami
Management Representative

Lack of fulfilment of conditions as set out in the Certification Agreement may render this Certificate invalid.
DNV GL Business Assurance Italia S.r.l. Via Energy Park, 14, 20871 Vimercate (MB), Italy. Tel: 039 68 99 905. www.dnvgl.it/assurance

VOSYS monitor arm features and benefits: safety & security

VOSySmonitor has been designed to suit safety and security use cases:

- A **superior isolation** building on top of ARM hw trustzone. Exclusive allocation of devices

  Best suited for high security use cases

- Supports system-IO-security **Monitoring** features

  System metrics real time monitoring with highest security

- **ISO-26262** ASIL-C **certification** obtained

  Certifiable IEC61508, IEC61511, etc.

Mixed critical virtualization to RISC-V and x86

VOSySmonitor virtualization, security and safety concepts applied to other platforms than Arm:

- Safety critical workload is executed in System Management Mode (SMM), which guarantees isolation
- Enhances security of the existing BIOS implementation
- Compliant with Intel and AMD processors

VOSYSmonitor x86

- Multiple partitions are created leveraging the RISC-V M-mode
- Uses only standard RISC-V extensions
- No virtualization extensions needed

VOSYSmonitor RISC-V

Virtualization Framework for Embedded Systems: VOSySzator

Virtualization suite for transforming an embedded system into a VM.

Advantages over the bare-metal execution:

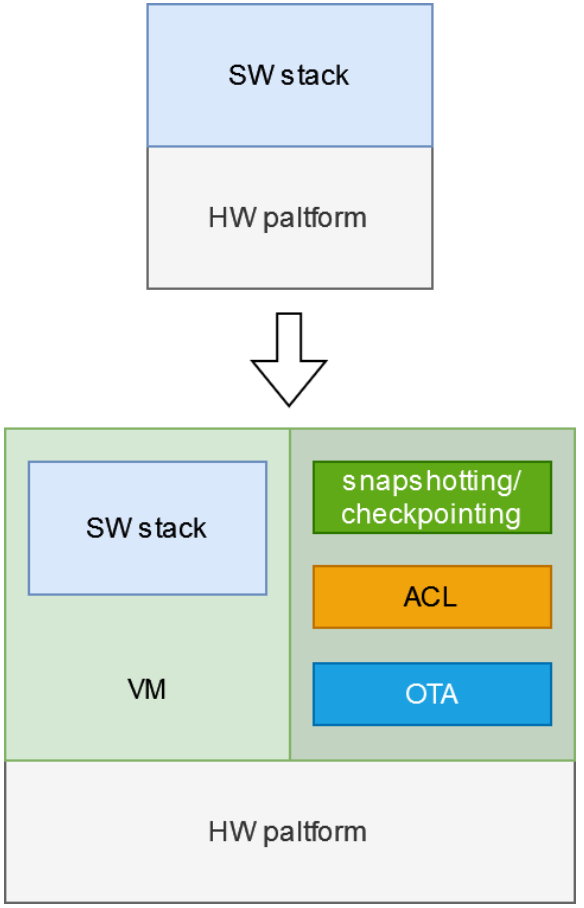
- Execution of an existing software stack inside an ad-hoc virtual machine to have full control over:
  - Accessed devices
  - Visible (physical) memory
- Simplified and safe OTA procedures with immediate roll-back
- Transparent restore points mechanism

Increased system availability and minimal down-time in set-top boxes, routers, kiosks and alike

VOSySzator framework

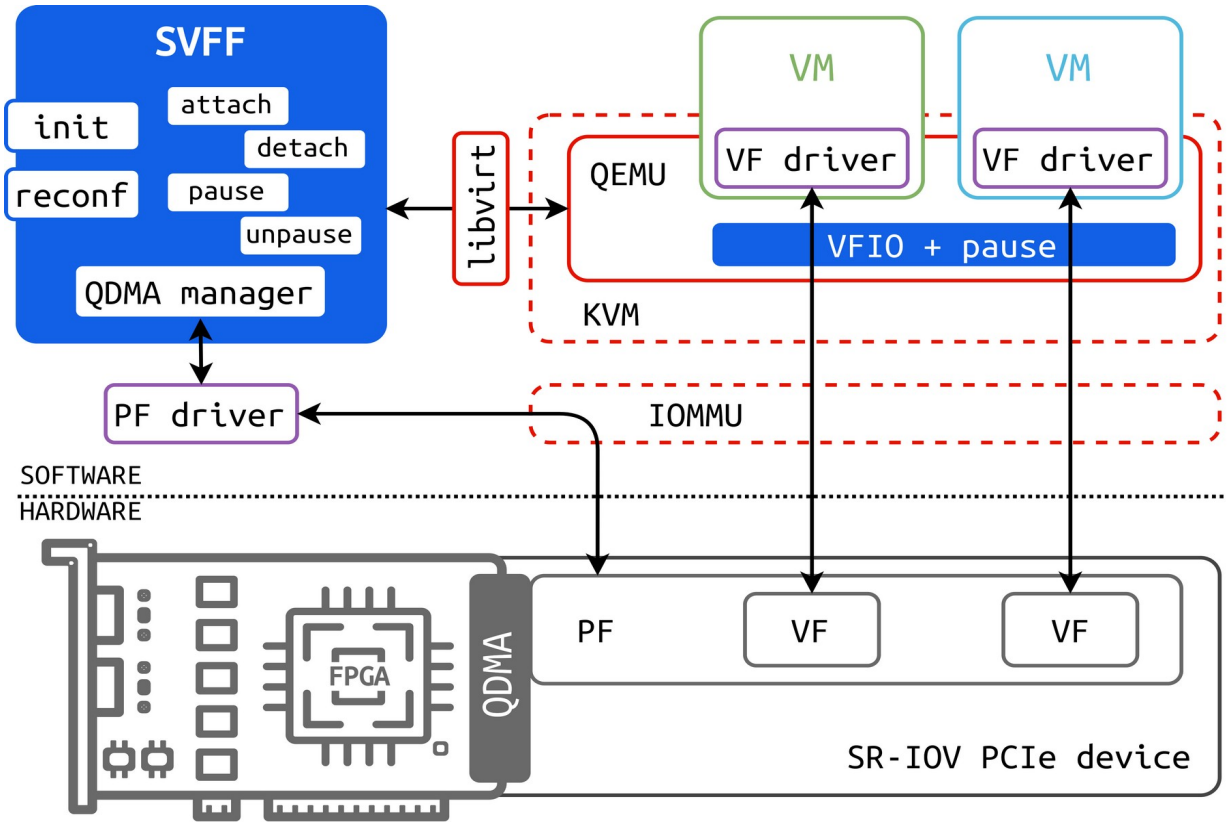
Virtualization framework including designing/building tools as well as runtime to:

- Configure the memory layout of the virtual machine
- Selectively pass-through physical devices into the virtual machine to limit the exposure of the hardware to the software
- When needed, mediate the access of the guest to existing devices and implement ACL-like functionality
- Low-overhead periodic snapshotting/checkpointing



VOS SR-IOV Virtual Functions Framework (SVFF)

- Simplify and enhance the management of VF
- Solve the lack of SR-IOV re-configuration support on guests
- Enhances performance, resource utilization, and overall system efficiency
- Pause functionality
- K8S plugin under development



LittleTorino
On-premises isolated communication server

LittleTorino is a privacy-first server solution for offices, factories, edge sites.

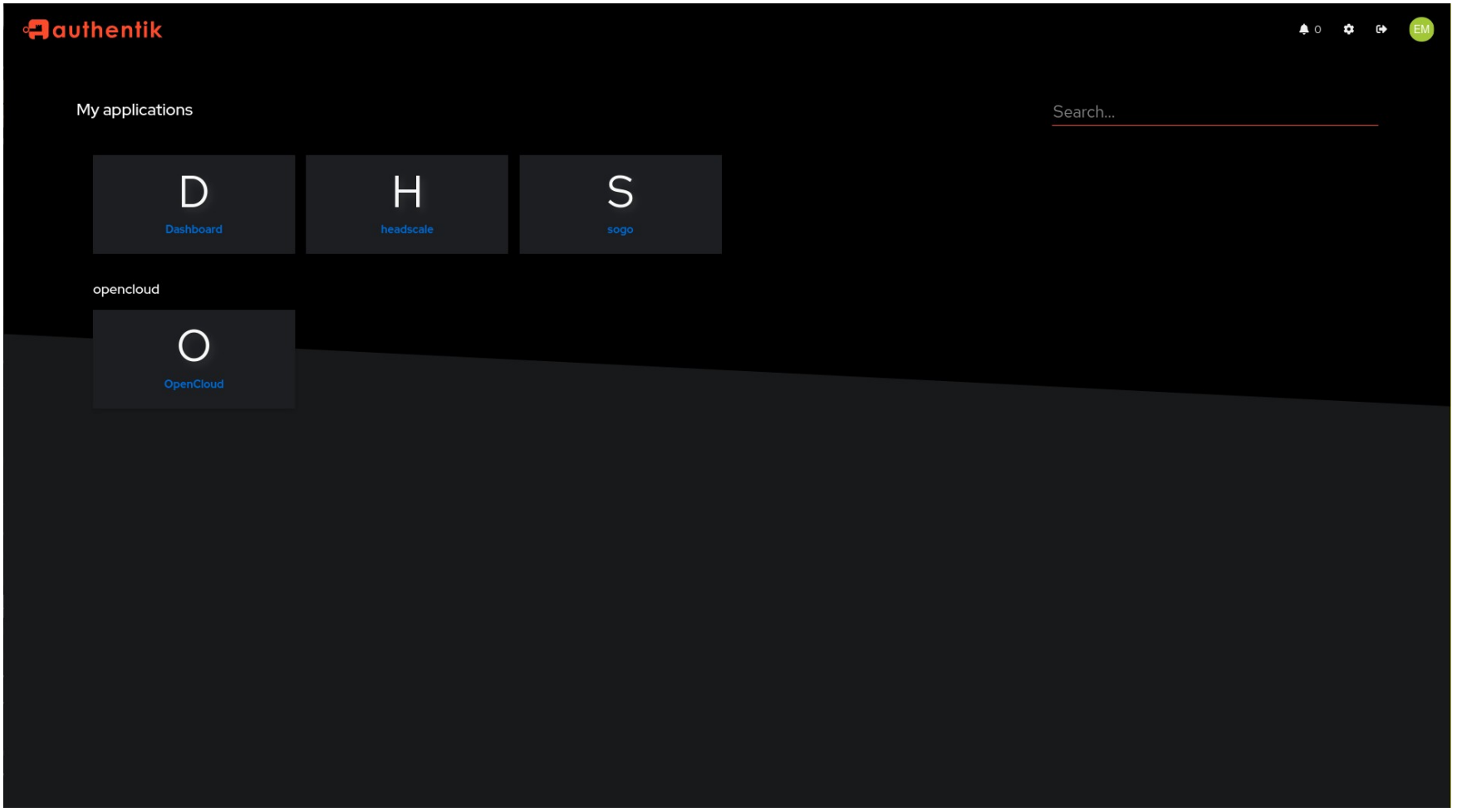
- Implements a self-hosted email server, office suite and meeting suite that provides best privacy and performance, both in premises and on the go
- Based on Arm SoC, including disk redundancy and fast inference solutions
- Employs advanced networking techniques (DNS , VPN, etc.) to maximize reliability and bandwidth.

LittleTorino
On-premises isolated communication server

- Specially designed to provide protected and highly controllable communications for high-sensitivity information exchange for isolated user base
- In this scenario, a dedicated subdomain of a bigger network can be used to reach the services provided by the box
- Given the size of the case, the LittleTorino box can be stored in ad-hoc places to comply with the most stringent regulation in terms of security and safety
- The fact that all the outgoing and incoming connections are going though a proxy and bound to specific ports, makes LittleTorino the ideal target of firewall rules and other network monitoring solutions

LittleTorino

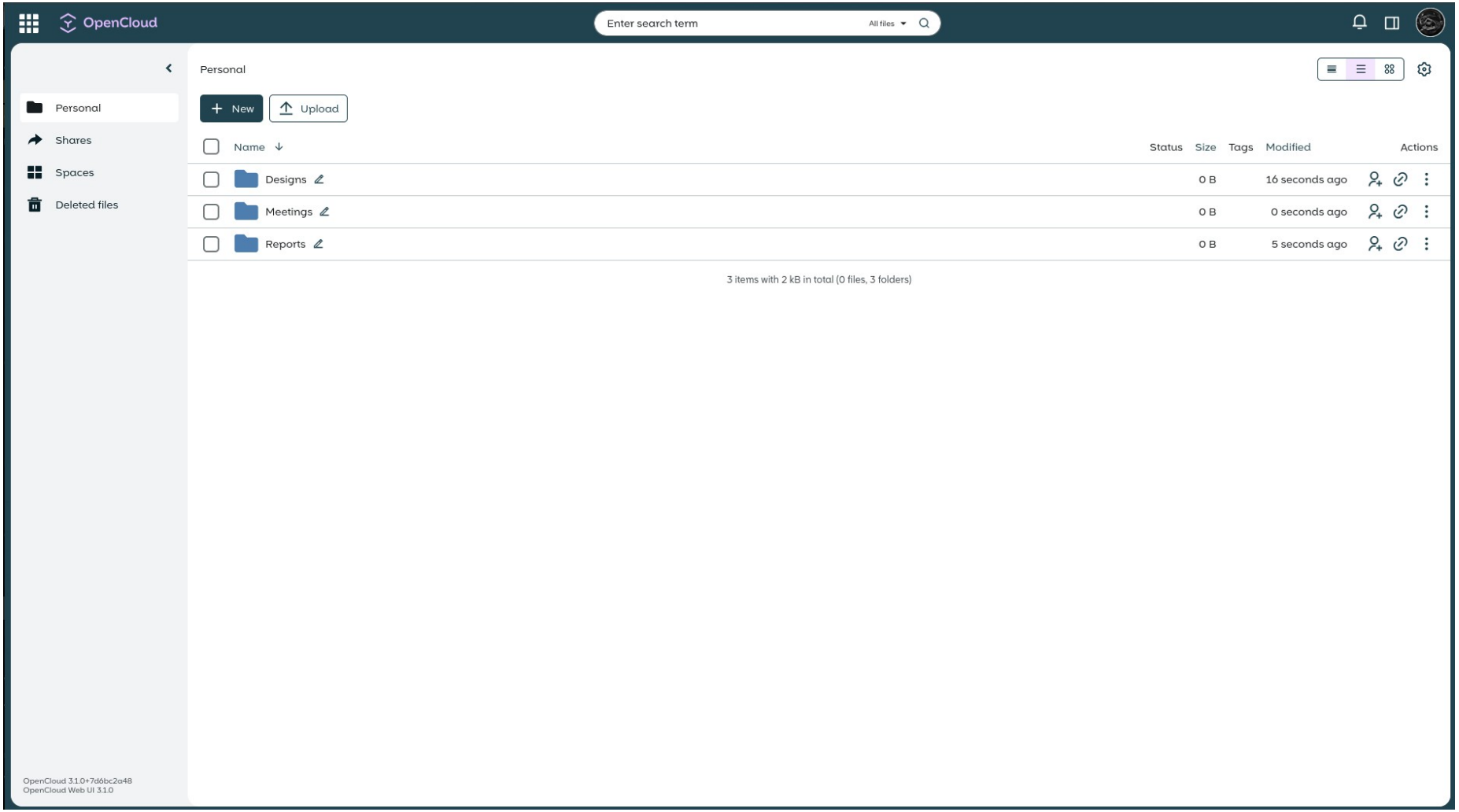
On-premises isolated communication server



Services list from the identity provider

LittleTorino

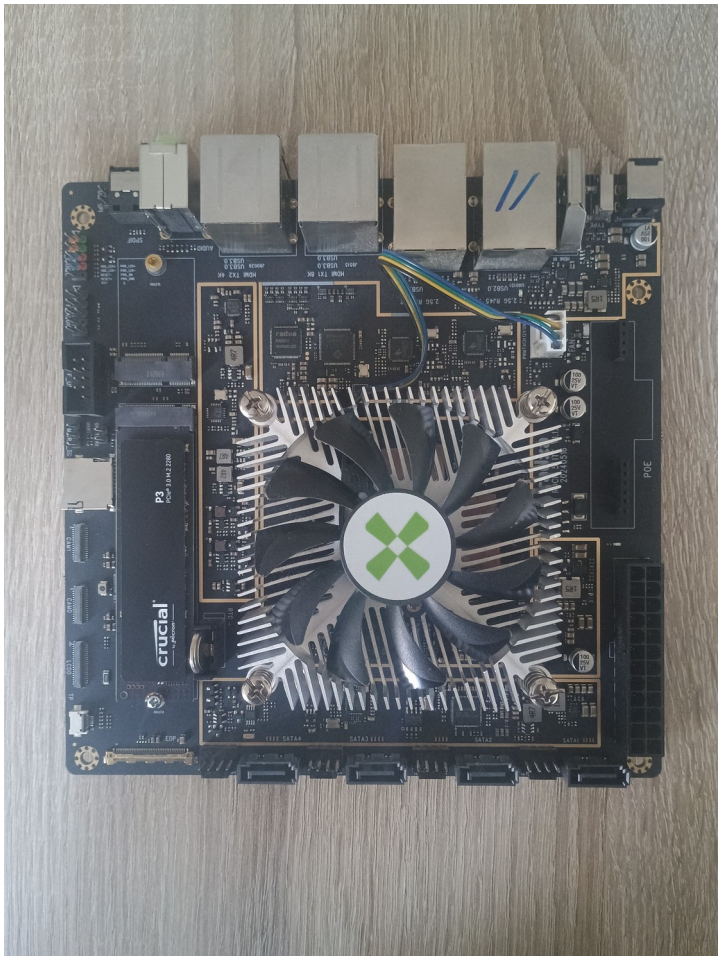
On-premises isolated communication server



Documents collaboration/editing tool

LittleTorino

On-premises isolated communication server



Mini-ITX ARMv8 board, coupled with double SATA SSDs configured in RAID1 and one NVME for the OS

Conclusions

Virtual Open Systems is an independent company with 10+ years exeperience in embedded systems.

- We provide first class design and development services and we are committed to open source technologies
- We develop cutting edge B2B products
- We are open for win-win cooperations in the fields of interest for the company

Isolation for Safety Critical application

As stated before, Virtual Open Systems has developed various PoCs based on bembedded architectures (ARMv7, ARMv8 and RISC-V) to provide heterogeneous systems where different execution environments with different criticalities had to be executed

- **Some of these made to production**

The main building block in all those systems was **VOSySmonitor** for the the ARMv7 and ARMv8 architectures and **VOSySmonitoRV** for the RISC-V architecture. **The objective is creating isolated execution environments where to execute a Linux OS or an RTOS.**

Technologies map

Technology	What for	How
VOSySmonitor	SAFETY and MIXED-CRITICALITY in the same board/SoC	Isolate the OSes with diverse levels of criticality in different hardware partitions using VOSySmonitor
virtio-based transport	Communication between hardware partitions	Create a link between partitions based on a virtio device and an ad-hoc asynchronous protocol
vManager	More dynamic use cases	Dynamically create partitions at runtime

Safety and Mixed criticality: **VOSySmonitor**

Especially in RISC-V, we can have multiple executing environments (and thus OSes) executing simultaneously in the same hardware.

The alternatives? Many chips/clusters connected together on the same board or multiple boards

- More complex synchronization
- Less predictable communication
- Waste of resources

Towards safety critical use-cases

Two important concepts can be explored with this design:

- Safety: An execution compartment for safety-related applications can be created and be subject of an ASIL certification process
- Real-Time: The configuration of the cores can be tuned according to the use-case. For instance, one execution environment can run with the cache disabled to achieve a more predictable execution
  - This can be fully exploited with an RTOS which, if configured ad-hoc, can meet hard real-time constraints

Towards safety critical use-cases

What can I do inside a partition/execution environment?

Almost everything that you can do in a dedicated SoC/SoM/SBC. The only limiting factor has to do with the devices that are allocated to the partition.

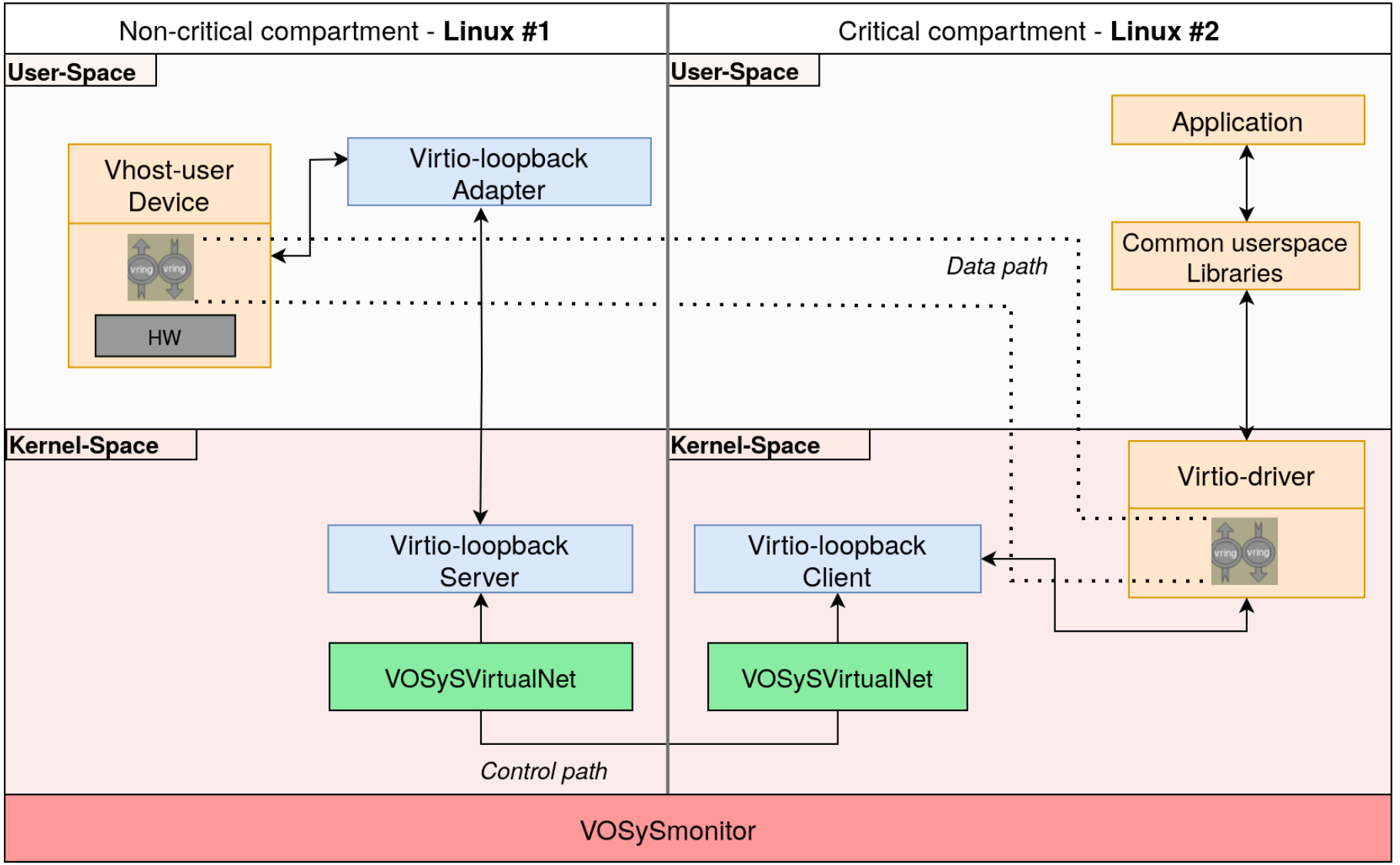
According to the platform in use, the devices can be « allocated » to different partitions by reserving the MMIO papped devices to the desired partition.

In this scenarios, the setup of the partition is static and happens in the early boot stages.

Communication between partitions: Virtio-based transport layer

In this context, a device can be also shared across one or more partitions with a technology called cross-world/partition virtio, which extends the concept of virtio-loopback across partitions.

Virtio-based transport layer



Towards more flexible use-cases: **vManager**

Some use-cases demands more dynamism and the static creation/allocation of partitions is not enough.

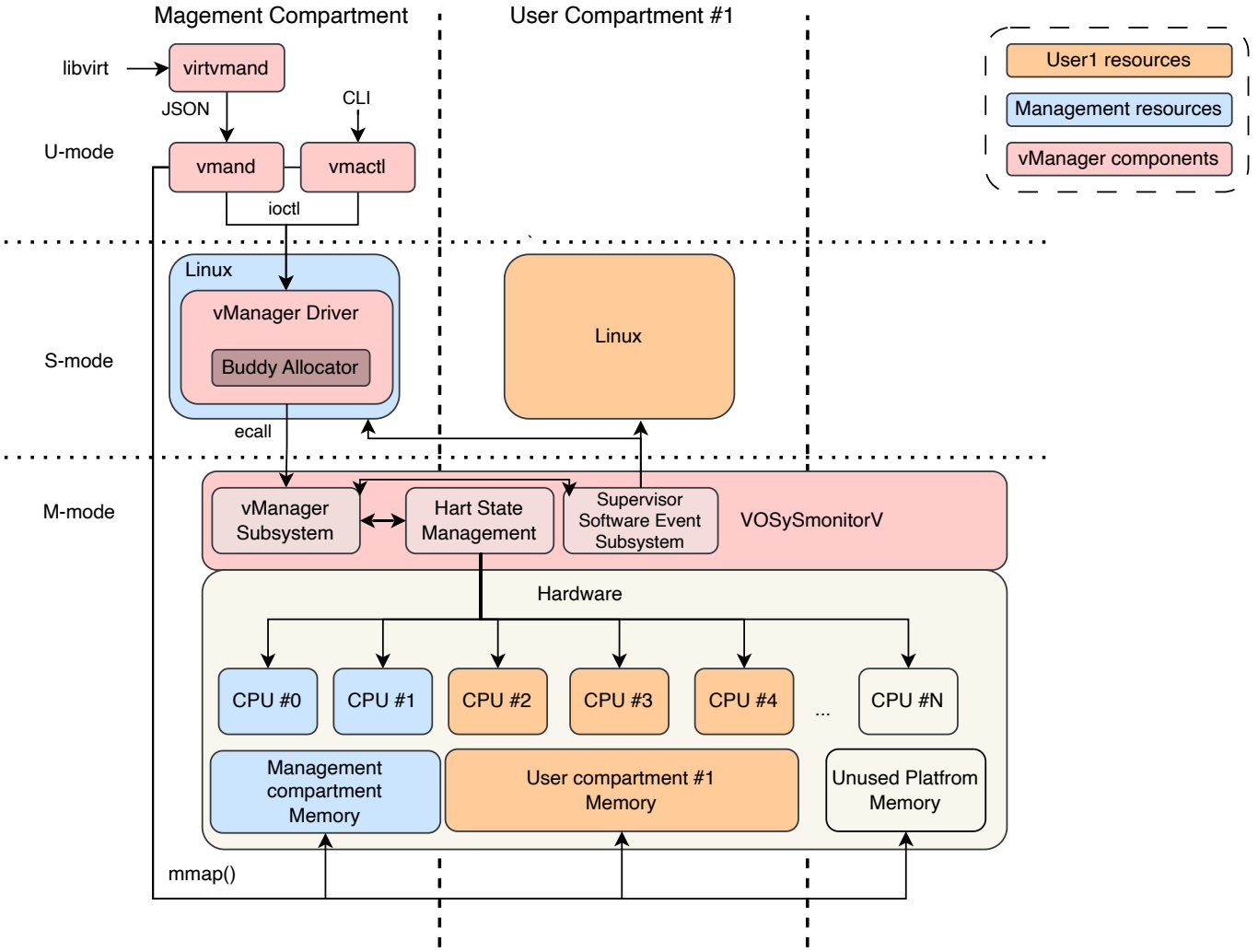
In contexts like the edge, where multiple virtual functions might be executed possibly isolated in a dedicated partition, a more high-level component can manage the lifecycle of the partitions.

These are the reasons why we create vManager(V), a partition manager.

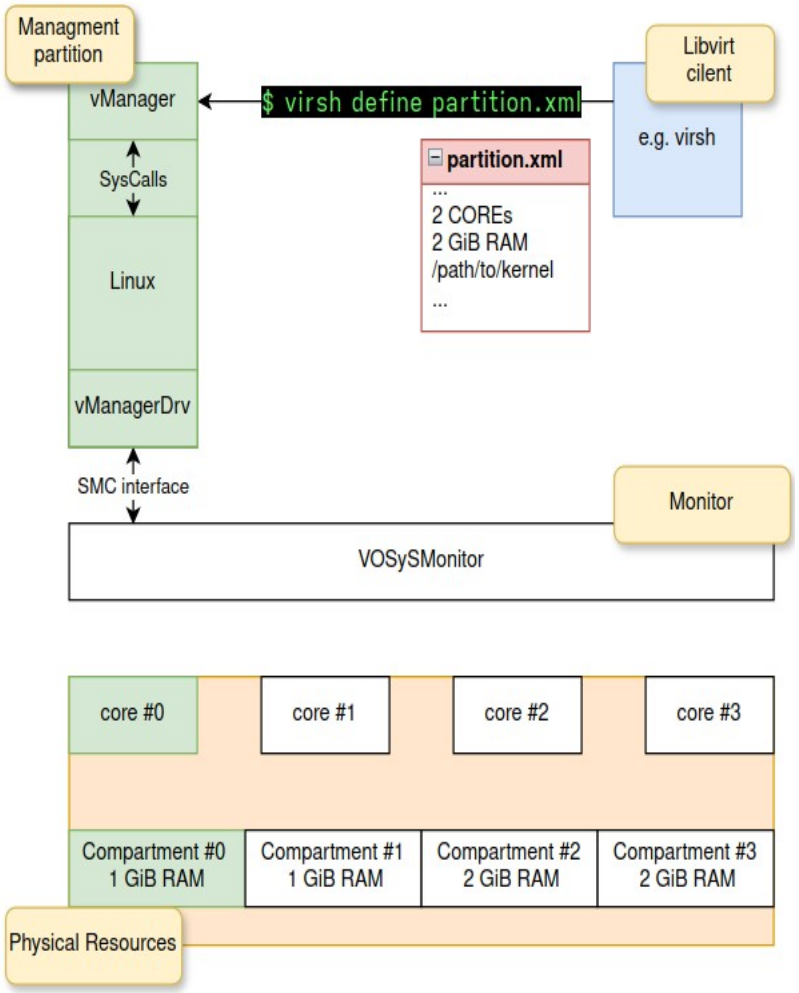
Towards more flexible use-cases: **vManager**

- vManager is the software framework that enables orchestrators to manage partitions' life-cycle by leveraging the monitor layer's functionalities.
- Each partition has its own set of hardware resources, physically separated from the others.
- With vManager, the partitions can be managed almost like VMs, thanks also to the integration with libvirt
  - Partitions can be paused, restored and rebooted
- This lowers the gap between the hardware partitioning brought by VOSySmonitor and virtualization

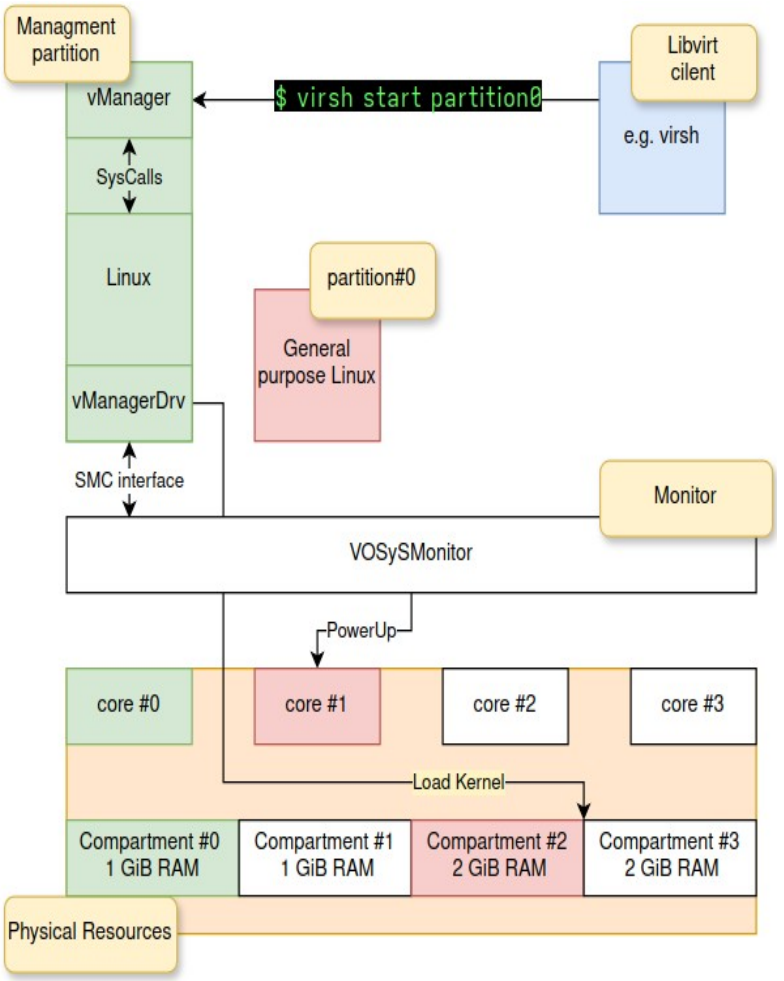
Towards more flexible use-cases: **vManager**



Towards more flexible use-cases: **vManager**



1. Partition Creation



2. Deployment

Use-cases summary overview

Summary of use-cases:

- Static partitioning for fast bring-up times, ad-hoc for safety critical applications
  - Resulting architecture well-suited for certification (**it does not require to certify Linux**)
- Edge computing: dynamic instantiation of partitions
- A mix of the two previous use-cases
- Confidential computing and storage
  - OTP like use case (~OPT-EE): OTP devices only accessible from some partitions

Use-cases: Focus on security

By combining what we have seen so far, we can design a system targeting secure, trusted and confidential computing

- A trusted boot can be implemented to propagate the root-of-trust (RoT) up to a statically-defined partition (the secure partition)
  - There, OTP devices can be accessed securely, independently by any other partitions with network access
- Encryption and decryption happens in the dedicated partition (any security assets does not have to leave the partition)

Use-cases: Focus on security

A fixed shared memory can be identified to exchange data between the secure partition and the rest of the system.

Thanks to an asynchronous signaling technology based on virtio-loopback, we can implement a rich communication protocol among partitions allowing to put the data to be encrypted/decrypted and to fetch the processed data.

Demonstrations

- **Video demos**
  - Mixed-criticality: RISC-V architecture
    - VOSySmonitoRV
    - vManagerV + VOSySmonitoRV
  - Mixed-criticality: ARMv8 architecture
    - VOSySmonitor
  - VNF reconfiguration demo (SVFF)

contact@virtualopensystems.com

Web: virtualopensystems.com

VOSySmcs: virtualopensystems.com/en/products/vosysmcs/

Demos: virtualopensystems.com/en/solutions/demos/

Guides: virtualopensystems.com/en/solutions/guides/

Research projects: virtualopensystems.com/en/research/innovation-projects/