Virtual Open Systems

Company 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 (3 years operational liquidity)**

➤ 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**, energy Power-Breakers, Drones, NFV, ..

Virtual Open Systems

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

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** (VOSySmonitor, VOSySmonitoRV, VOSySmonitorX86) and its own Virtualization framework (VOSySzator), to serve any mixed-critical market segment.
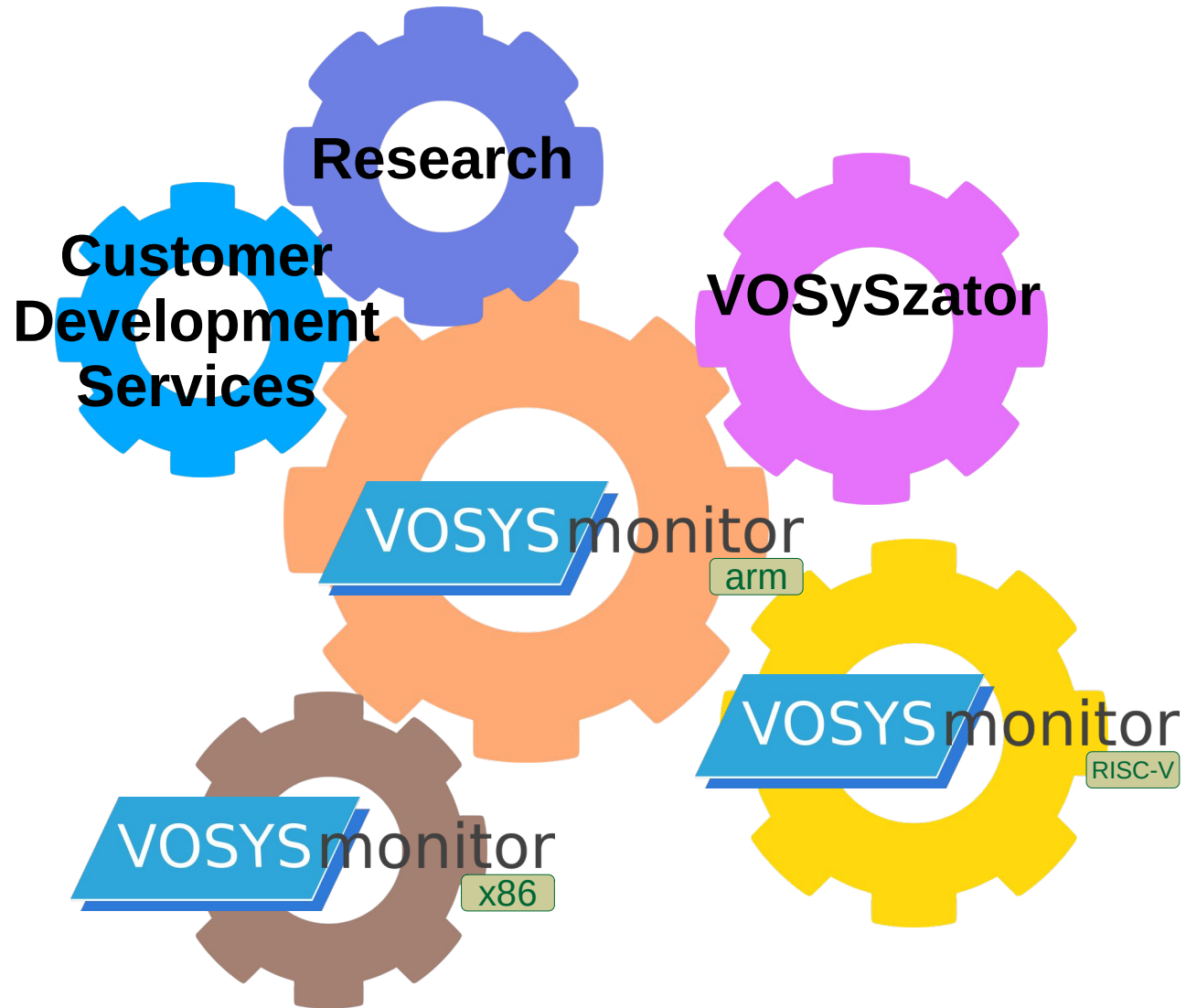
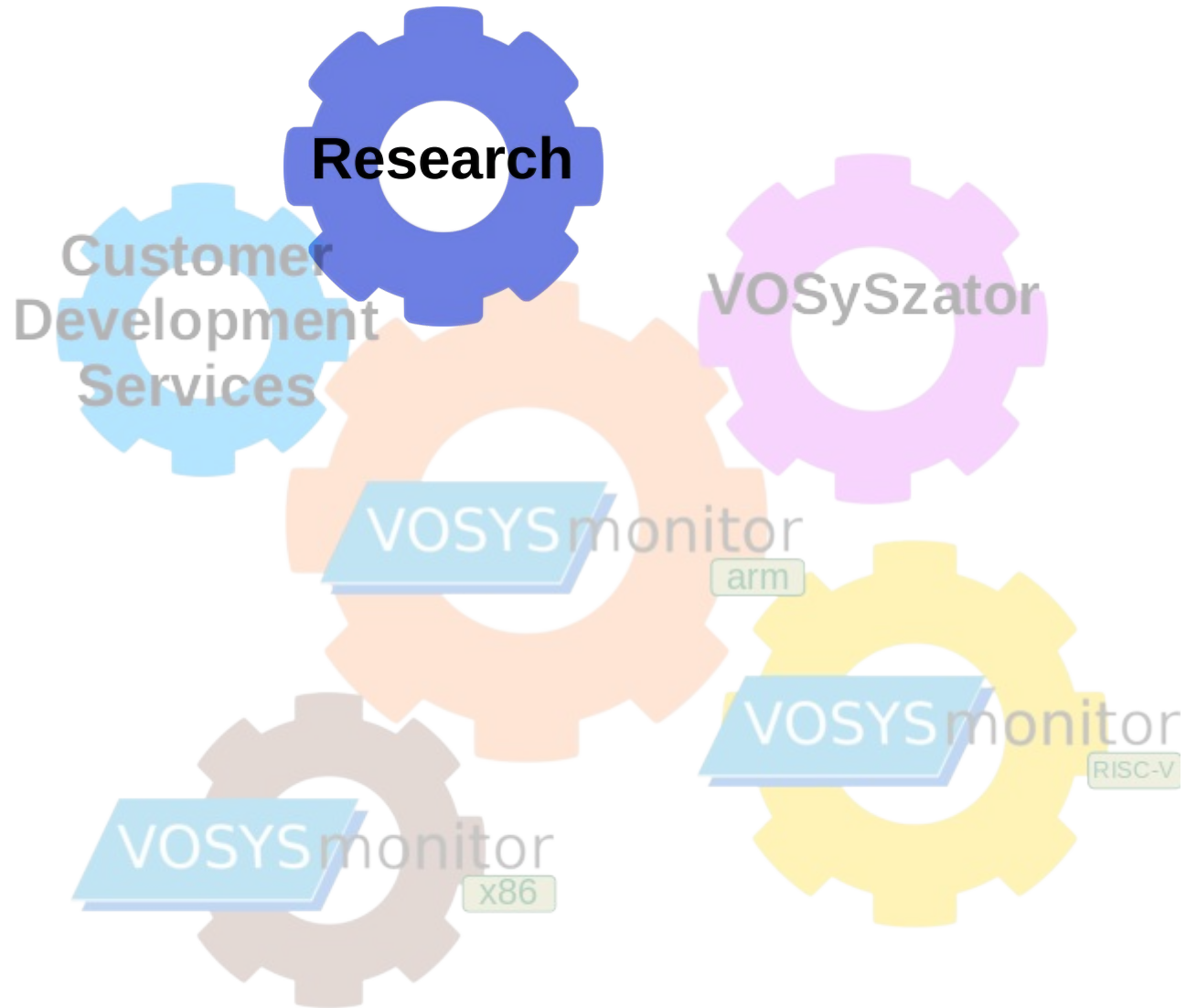VOSYS**monitor** arm   VOSYS**monitor** x86   VOSYS**monitor** RISC-V

Virtual Open Systems

Virtual Open Systems business model pillars

Virtual Open Systems business model pillars

Virtual Open Systems

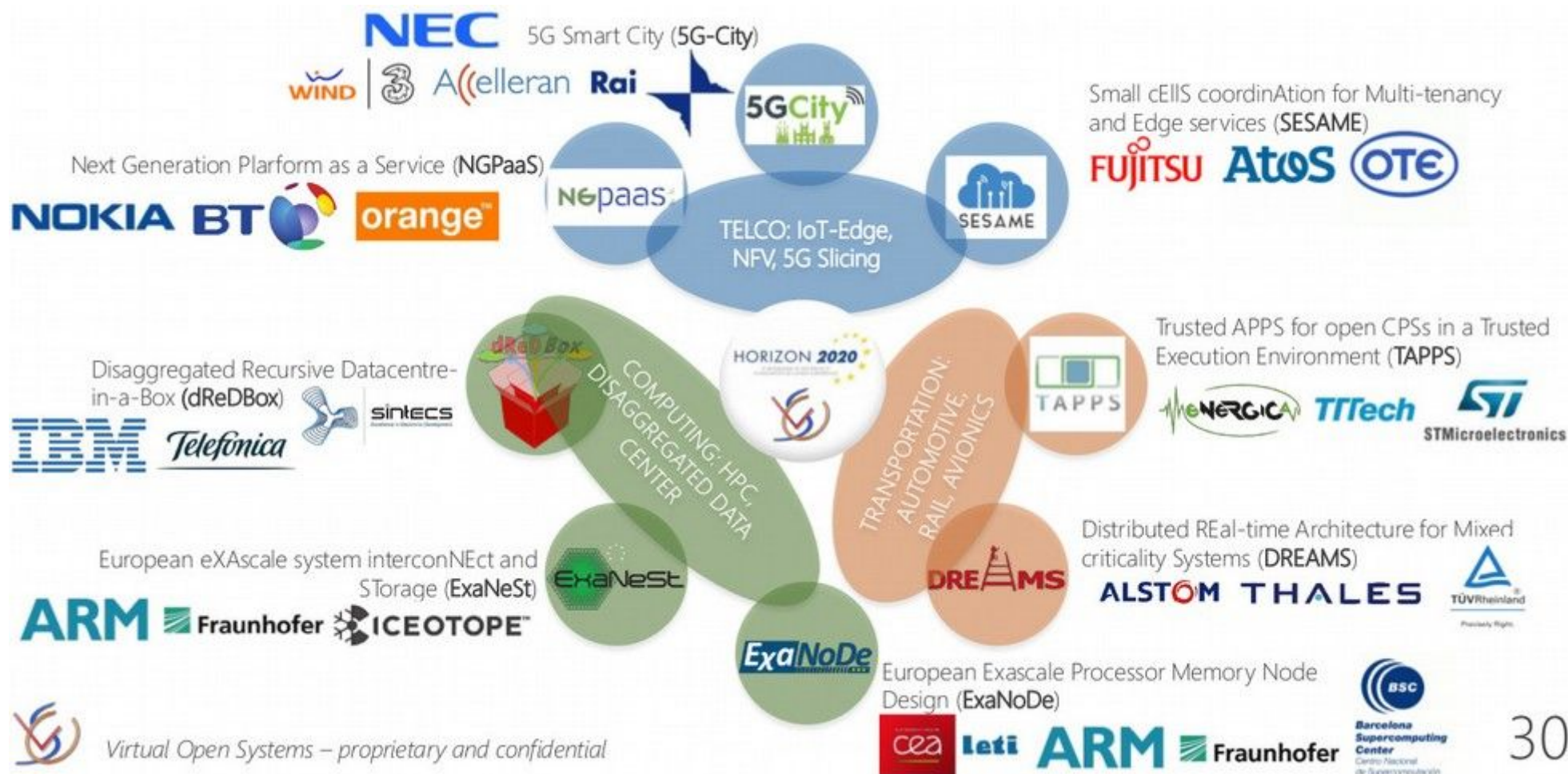# Virtual Open Systems: Visibility

International Exposure

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

Virtual Open Systems

Virtual Open Systems

Most recent R&D EU Project: EVEREST

Virtual Open Systems role:

➢ Design and development of FPGA and GPU Virtualization

➢ Virtual machines acceleration support for ARMv8, RISC-V and x86 CPU architectures to expose hardware configurable parameters to the applications

➢ Seamless integration of both servers and Edge nodes for Big Data analytics

Virtual Open Syste....

Most recent R&D EU Project: 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

Virtual Open Systems: Last Publications

Papers Dissemination

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

➢ 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**

➢ VOSYSVirtualNet: Efficient Inter-world Network Channel for Mixed-Criticality Systems, **SIES2018**

➢ The Next Generation Platform as a Service, Cloudifying Service Deployments in Telco-Operators Infrastructure, **ICT2018**

➢ FPGA virtualization with accelerators overcommitment for Network Function Virtualization, **Reconfig17**

➢ Paving the way towards a highly energy-efficient and highly integrated compute node for the Exascale revolution: the ExaNoDe approach, **DSD2017**

➢ Lightweight and Generic RDMA Engine Para-Virtualization for the KVM Hypervisor, **HPCS2017**

➢ VOSYSmonitor, a Low Latency Monitor Layer for Mixed-Criticality Systems on ARMv8-A, **ECRTS2017**

Virtual Open Systems

IP Protection by Patents

IP protection is a strategic investment at 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

➤ **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/EU exam.)**

Virtual Open Systems
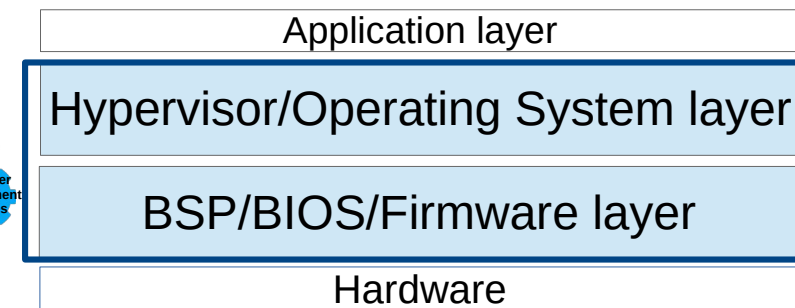
Virtual Open Systems business model pillars
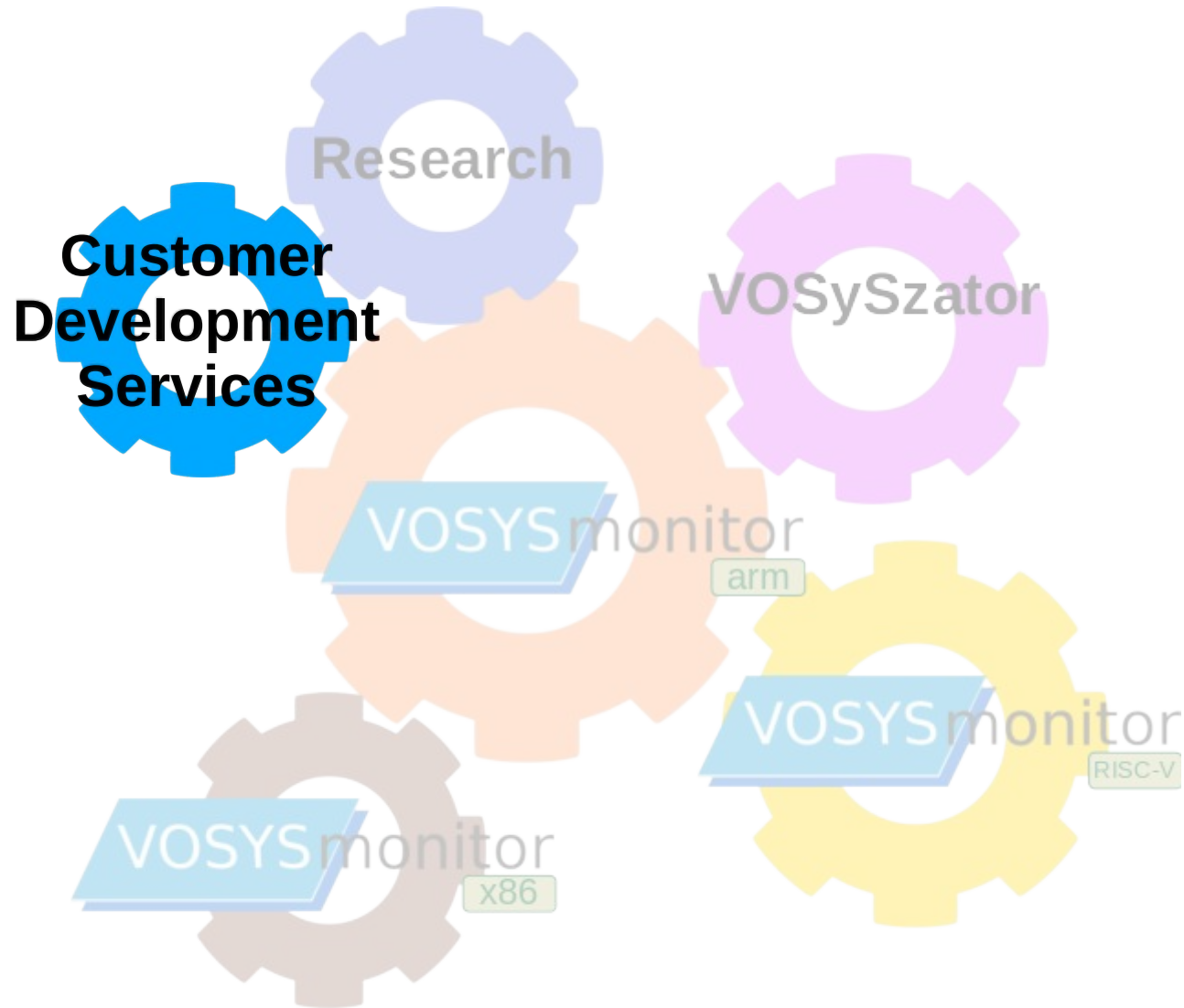
Custom design and development services: Know-how

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

Application layer
Hypervisor/Operating System layer
BSP/BIOS/Firmware layer
Hardware

Customer Development Services

Virtual Open Systems

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

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

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

Virtual Open Systems: Track Record
Containers extensions for automotive

➢ Development services for extending existing container technologies to support mixed criticality environment

– Customized devices passhthrough (USB, GPU, etc)

  implementation and benchmarking

– Multiple displays support

– Safety and non safety communication

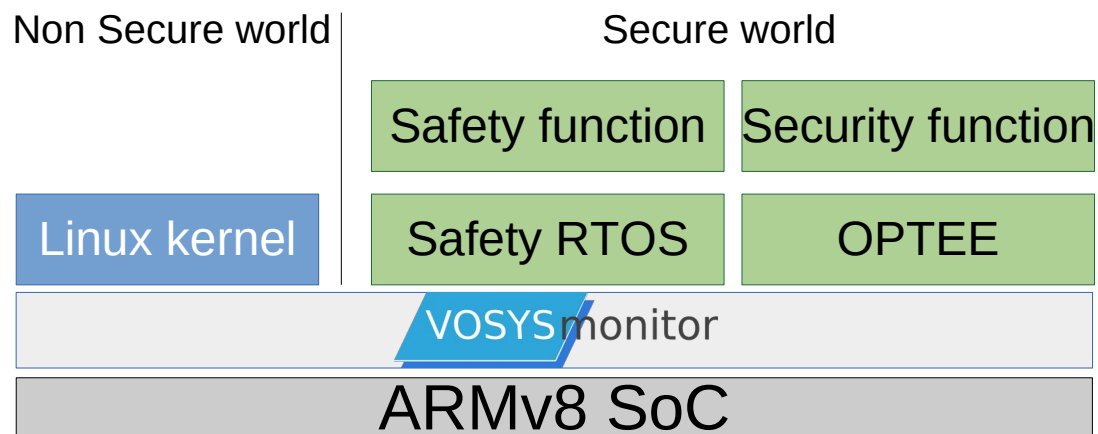 mechanisms design and implementation

Virtual Open Systems
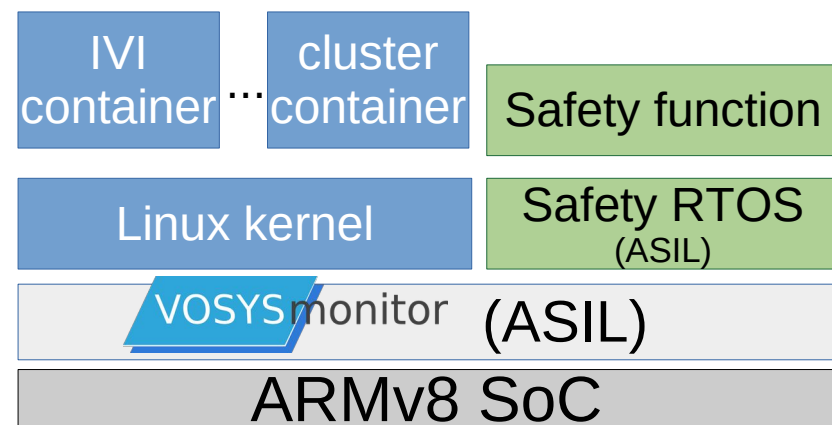
Virtual Open Systems: Track Record
VOSySmonitor porting and extensions

➢ **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

Non Secure world	Secure world	
	Safety function	Security function
Linux kernel	Safety RTOS	OPTEE
	VOSYSmonitor	
ARMv8 SoC		

Virtual Open Systems

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

    from design to implementation phases

FreeRTOS working on core 1
Linux working on core 1/2/3/4
So core 1 is shared between
Linux and FreeRTOS

FreeRTOS boots in 10 ms

FreeRTOS printing on UART0
(same as VOSySmonitoRV
and Linux)

Virtual Open Systems

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
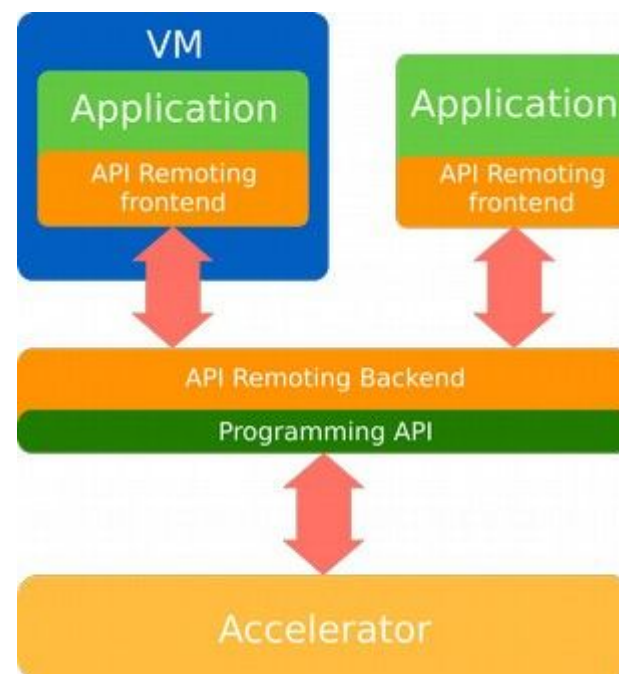
Virtual Open Systems: Track Record
High performance virtualization designs

➢ 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

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
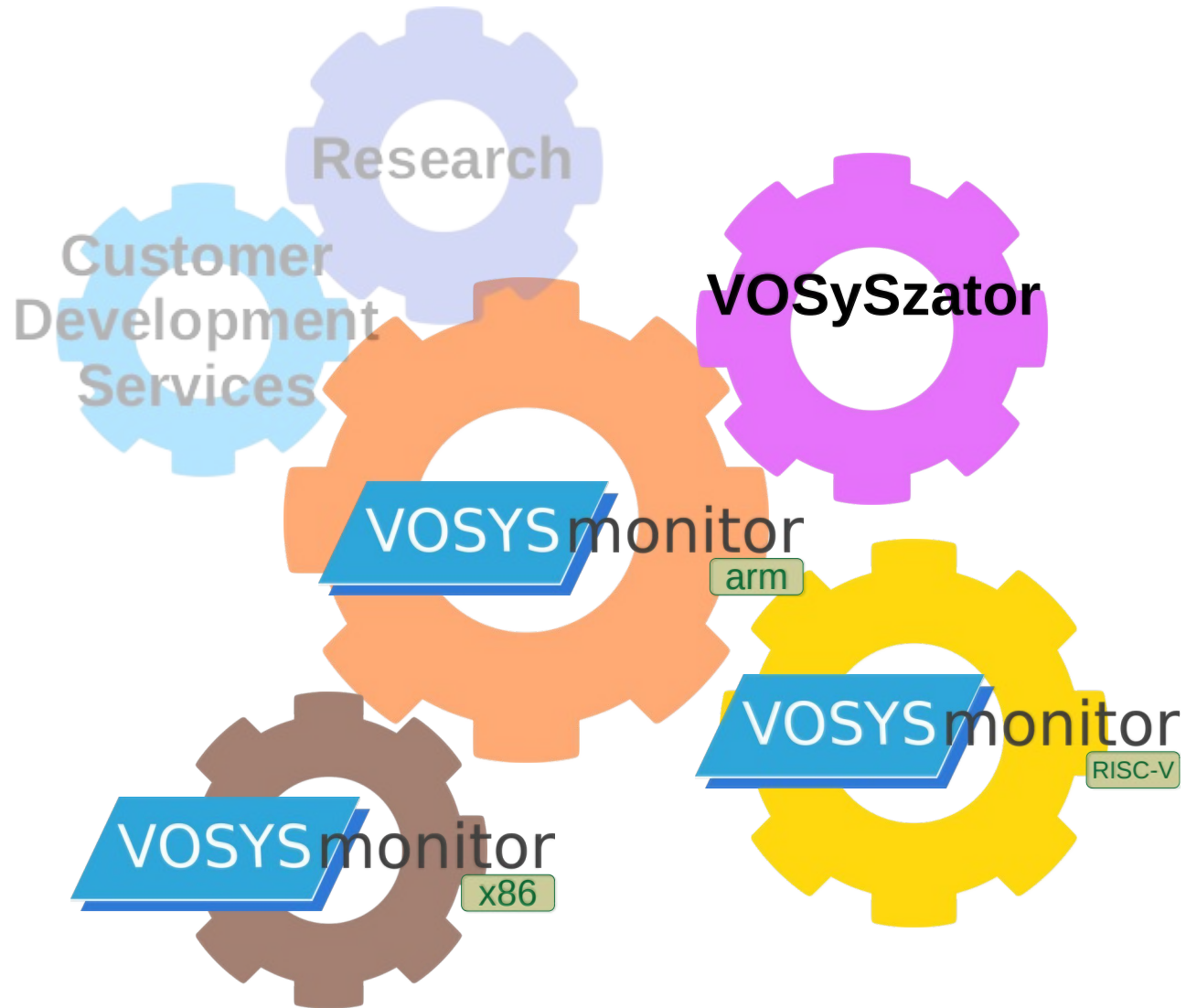
Virtual Open Systems: Track Record
Virtualized development environment for rugged routers

- ➢ Development services for adapting the existing BSP of the Gateworks Newport GW6404 SBC to a virtualized execution

  - Easy applications development and debugging
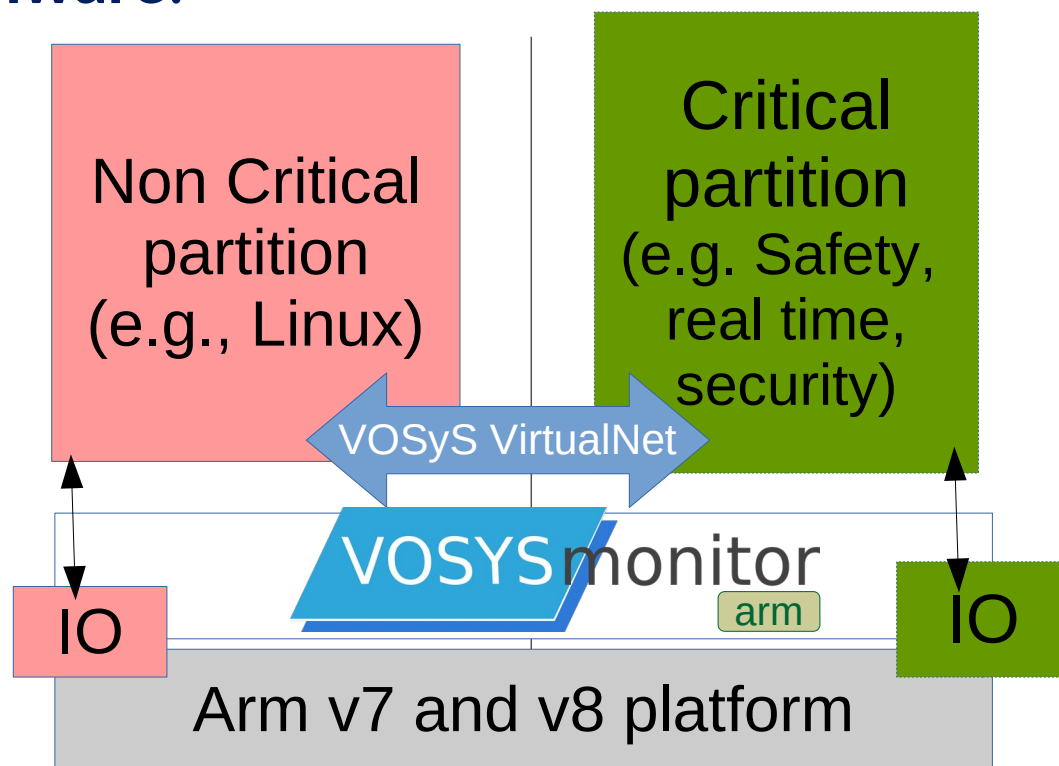
  - Fast prototyping

QEMU

Virtual Open Systems

Virtual Open Systems business model pillars

Virtual Open Systems

Virtual Open Systems product: VOSYSmonitor arm

VOSySmonitor is a certifiable TrustZone based **virtualization firmware.**

Non Critical partition (e.g., Linux)

Critical partition (e.g. Safety, real time, security)

VOSyS VirtualNet

VOSYSmonitor arm

IO

IO

Arm v7 and v8 platform

Disrupting features:

➕ Software features

➕ Security

➕ Safety & reliability

🔴 Hardware costs

🔴 Maintenance

It targets powerful machines, edge devices as well as low power and safety critical embedded systems.

Virtual Open Systems

VOSySmonitor brings efficient hardware resources utilization through system partitioning:

➢ Highest **efficiency** and smallest overhead leveraging hardware partitioning capabilities

Perfect solution for microcontrollers and low power platforms

➢ **Better latency** performance while serving RTOS tasks (no context switch overhead)

Best fit for real time use cases

➢ **High portability**. Software runs directly on the hardware, there is no need to port existing drivers

Compliant with legacy applications

➢ **High reliability:** Runtime system monitoring to implement healing function

Reboots operating systems/applications in case of crash

Virtual Open Systems

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.

Virtual Open Systems

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

➢ Multiple partitions are created leveraging the RISC-V M-mode

➢ Uses only standard RISC-V extensions

➢ No virtualization extensions needed

VOSYSmonitor x86

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
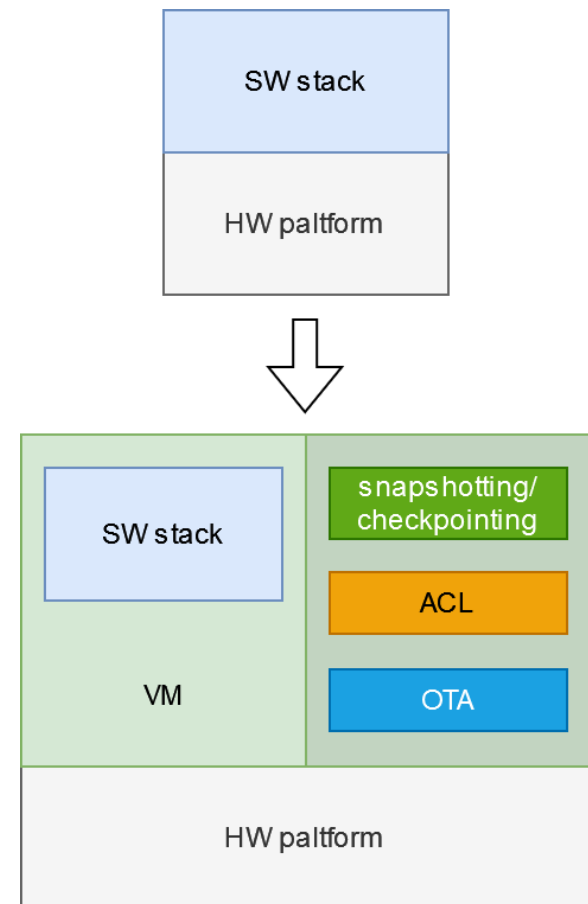- ➤ Transparent restore points mechanism

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

Virtual Open Systems

Virtualization Framework for Embedded Systems: VOSySzator

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

Virtual Open Systems

Demos

http://www.virtualopensystems.com/en/solutions/demos/vosysmonitorv-core-sharing-virtualization-demo/

http://www.virtualopensystems.com/en/solutions/demos/vosysmonitorx86-demo/

http://www.virtualopensystems.com/en/solutions/demos/vosysmonitorv-risc-v-demo/

http://www.virtualopensystems.com/en/solutions/demos/vosysmonitor-mt2712/

http://www.virtualopensystems.com/en/solutions/demos/virtualizing-fpga-accelerators/

http://www.virtualopensystems.com/en/solutions/demos/virtualizing-stb-lower-tco/

http://www.virtualopensystems.com/en/solutions/demos/vosysmonitor-emcos-ew2019/

Papers

http://www.virtualopensystems.com/en/research/scientific-contributions/vosysmonitorv-risc-v-meco2021/

http://www.virtualopensystems.com/en/research/scientific-contributions/x86-smm-mixed-criticality-applepies2020/

http://www.virtualopensystems.com/en/research/scientific-contributions/5gcity-edge-virt-5gwf2019/

http://www.virtualopensystems.com/en/research/scientific-contributions/vfpgamanager-eucnc2019/

http://www.virtualopensystems.com/en/research/scientific-contributions/geofencing-trustedvim-eucnc2019/

http://www.virtualopensystems.com/en/research/scientific-contributions/trustedvim-wcnc2019/

http://www.virtualopensystems.com/en/research/scientific-contributions/vosysmonitor-safety-fruct23/

http://www.virtualopensystems.com/en/research/scientific-contributions/microvm-benchmark-eucnc2018/

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/