HV Project Deep-dive topics for 2021 June and forward

The idea is to pick specific virtualization topics, separately from the AVPS specification writing, and to do deep-dive investigations.

We did something similar with Graphics Virtualization a while back, where we had a series of sessions that invited experts in the graphics frameworks as well as hardware vendors speaking about their specific silicon technologies. This gave everyone involved a big boost in understanding of the area.

Brainstorm list:

(Next step is voting/prioritizing on these.)

⚠️ Talk to your colleagues/experts in each area (not virtualization experts necessarily, but subject experts). Make them part of prioritization activity, have them tell us if they would like to attend a specific deep-dive on a topic.

⭐⭐⭐⭐✅🙂💡 = participant favorites so far

Blue = scheduling/planning started for these topics.

Hardware/virtual devices:

- ✅ Crypto / Security
  - Trusted Execution Environments
  - NXP accelerator blocks?
  - Firmware framework for Cortex-A, OPTEE, how to access secure computing from the general application, ...
- ⭐ **Ethernet AvB / Time Sensitive Networking**
  - NXP accelerator blocks?
  - Can the HW be partitioned, and use pass-through to more than one VM.
  - HW+SW stack, how is it divided up between HV, VMs, ...
  - Assume one or two "typical" intended use-cases or system designs and discuss from there.
- 🙂 Automotive networks, in particular CAN
- Accelerators
  - ⭐ Tensor-Processing Units
    - Will be used for some safety critical features? Is it feasible to virtualize?
  - DSPs (is that discussion done in AVPS or is there more?)
- 🙂 Camera
- 🙂⭐💡 Next-gen PCI and future interconnects. Used for example for inter-chip communication and peripherals
  - Automotive working group exists within PCI v6 work
  - Future interconnects: CCIX (pronounced "C-six"), CXL, Gen Z and other alternatives, NVidia alternative, ...
- Graphics (again...)

Platforms and environments

- ✅🙂 Google's Trout platform (likely subdivided into areas of interest)
- ⭐✅ Virtualization for Microcontrollers / small cores, non-MMU
  - Note there are more than one CPU architecture here... different strategies?
  - What is different between MCU virtualization and virt on full-featured CPUs/SoCs?
  - Is it a misunderstood term? Is isolating cores involved, but is that then virtualization?
  - MPU vs MMU, impact on virtualization implementations
  - Resource sharing/virtual devices vs resource partitioning / hardware-passthrough
  - Which hardware support for virtualization is built into popular MCU products?
  - Real-time demands vs. virtualization
  - Discussions ongoing on if VIRTIO can be implemented in MCUs?
  - Linux kernel running?
  - AUTOSAR Classic Microcontroller abstraction layer (MCAL) - how does it affect the discussion.

Aspects of hypervisor implementation and software stack in general

- 💡⭐ **IPC and Inter-Chip Communication**
  - Communication between different guests or hardware parts. *Does it affect the Virtual Platform or is it just run transparently on virtual socket?*
  - One specific use case is **inter-cpu communication**. Particularly in the case of converged SoCs, e.g. comms between app on RT and general purpose CPU.
  - Are there standard choices? Are there many vendor-specific proposals, like IC-COM? (Is that an AUTOSAR standard?)
    RPMSG https://www.kernel.org/doc/html/latest/staging/rpmsg.html
    NXP has some framework?
  - MCAL is intended to be abstraction layer for the actual communication choice?
    - ... but it still need to be implemented, (so actual choices matter at some level)
  - There are non-AUTOSAR implementations as well.
  - Impact and design of security.
  - Hypervisors using inter-chip communication somehow?
    - Example (Xen): HV controlling MFIS (Renesas specific) for communication between. Cortex-R / Cortex-A cores

        - VIRTIO usage as a protocol between system partitions (not only VM-to-HV but other types of partitioning)
            - Uses HW capability for the low-level mailbox / similar
            - Subset of VIRTIO (can't assume access to whole memory as often done by VIRTIO to HV implementation)
            - Can VIRTIO be transformed into a safety-optimized communication. E.g. some parts of memory only written by one party, read by the other. Also sealing needed (if it's a shared-memory buffer).
    - Additional compute platform topics?
        - Comparing hypervisors and simpler partitioning approaches (e.g. Jailhouse)

    - Go through operating system kernel special needs for each popular OS choice.
        - e.g. Is VIRTIO reasonably supported for RTOSes or other requirements?
        - e.g. What is the impact of new RTOS initiatives, as well as migration of legacy code from dedicated hardware to a virtualized environment (because the hardware goes out of production or similar). Thread-X, AUTOSAR (OSEK), Zephyr, FreeRTOS, Arm MBed, (and no-RTOS bare-metal VMs).
    - ⭐🙂 Clock synchronization, real-time clock abstraction (probably a good topic for the AVPS)
        - Discussed today for the purpose of synchronized logs... but are not there more reasons? E.g. systems that can do load-balancing, redundancy (offloading, transferring tasks), don't they need a common time?
    - 🙂 Timer paravirtualization
        - CPU scheduling reporting HV<->VM, e.g. kernels do not get accurate information about system load. Steal time reporting. The time while a VM was not scheduled, even though it should run (= Steal time).
        - A spec from Arm ("Arm para-virtualized time" DEN0057A) covers how to report steal time.
    - ⭐ General topic: Needs for (easier, better) virtualization support in future SoCs.
        - Still examples of how IP-block diversity and limitations causes issues (32 bit device in an otherwise 64-bit architecture)
        - Is virtualization truly a top priority for SoC vendors?
    - Agreed definition of *virtualization*. Non-MMU systems seem to use the term even if the implementation is rather hardware separation.

Analyzing virtual platform characteristics and general areas

- Real-timeish stuff
    - *What are the special considerations we need to work out to support real-time demands?*
- ✅ Impacts from safety certification, ASIL?
    - Look into Linaro presentation, Xen progress, etc. for some starting ideas. Also input from ELIZA project?

Proposals for leader/expert invitations

OPTEE maintainer Renesas. OPTEE related topics - Volodomyr Babchuk

TSN - Torsten (Renesas) is interested.
- Previous material (Torsten made presentation in AMM Munich (2019?))

IPC - Thomas Bruss (Renesas)

... requested some guidance on topics first.

PCI - Thomas Bruss

Microcontrollers

- (RH850) Juergen Himmelberg?
... some details are proprietary (partners/NDA only)
... idea: discussion group among companies that have NDA setups with silicon vendor (not ideal)

- Adam and Oleksandr interested
- ARM representative - discussing with Bernhard

- What is different between MCU virtualization and virt on full-featured CPUs/SoCs?
- Is it a misunderstood term? Is isolating cores involved, but is that then virtualization?
- MPU vs MMU, impact on virtualization implementations
- Resource sharing/virtual devices vs resource partitioning / hardware-passthrough
- Which hardware support for virtualization is built into popular MCU products?
- Real-time demands vs. virtualization
- Discussions ongoing on if VIRTIO can be implemented in MCUs?
- AUTOSAR Classic Microcontroller abstraction layer (MCAL) - how does this affect the discussion?

- Also: https://xen2021.sched.com/event/jAF7/introducing-xen-to-armv8-r-aarch64-with-mpu-support-wei-chen-penny-zheng-arm

Harald (OpenSynergy) works on CAN Virtio

Someone on NXP for TEE and Networking?

Bernhard (Arm) - back on 18 Oct.
- Security, firmware framework for Arm-A (link) , optee
- CCIX, CXL ...
- Real-time aspects. ARMv8-R device virtualization specification? (early draft circulated, might be available to us around September)
- Clock synchronization

Ask Linaro representatives
- working on implementation (on Xen) of various VIRTIO areas. Reach out to Francois to understand most challenging areas?

Fulup checking with team who might be best suited to each topic.
(Monday 10 AM is not a good time slot)

Participants invitations and outreach

IPC topic

- Thomas, OpenSynergy, Peter (BMW), Kai,
- Francois-Frederic Ozog. Other Linaro representatives?
- Volodomyr (EPAM)
- AGL participants (Virtualization group? Instrument Cluster group?, etc.)
- GENIVICOVESA mailing list outreach
- Stefano Stabellini (Xilinx)? (PST time zone, so 10 AM CET is not appropriate time)