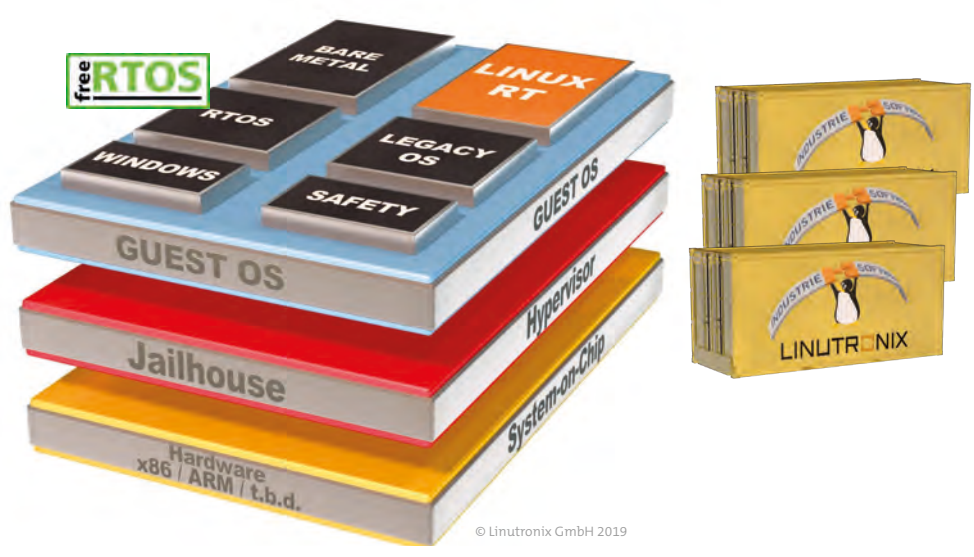
LINUTRONIX

JAILHOUSE

Hypervisor and Realtime for heterogeneous Multi-Core CPUs



Modern SoCs are growing increasingly complex and diverse. On the one hand, this shows the trend of consolidating many embedded system functions in one hardware, on the other hand, it also reflects the increased requirements with in terms of security and safety.

In addition to homogeneous solutions (i.e. n-CPUs of the same architecture, e.g. x86), more and more heterogeneous multi-core CPUs are entering the (embedded) market. Different CPU architectures and programmable logic (FPGA) are combined to offer optimal solutions for different requirements.

High-performance ARM Cortex A processors, combined with graphics (GPU) and video processors, for use as GUI / HMI interfaces are combined with ARM Cortex R or M types for real-time tasks. An FPGA takes over computing-intensive tasks or extremely time-critical tasks from the CPUs. Or maybe those parts the know-how of which you don't want to pass on to third parties.

How can you ensure that the different hardware components do not influence each other, if they have not already been separated by hardware design? Looking at CPU clusters of type Cortex A, isolation or separation is the answer to this question. Heterogeneous multi-core CPUs offer a wide range of technologies that can be used to separate secure from non-secure processes, safety from non-safety relevant processes.

Separation

The most important components for separation are:

ARM TrustZone - separates hardware and software into a secure and a non-secure part.

Hypervisor - a real-time hypervisor like jailhouse.

System MMU, XMPU and XMPU - different technologies for isolating DMA-enabled devices on the ARM A cores, for separating access to storage areas from different subsystems or for isolating peripherals.

The boot process, initiated by the Platform Management Unit (PMU), is highly configurable. The First Stage Bootloader (FSBL), which is subsequently loaded, can be run on the Cortex-M or R or on the Cortex A processors. Yet during this boot process the hardware can be divided into isolated subsystems. The entire boot pro-

JAILHOUSE

cess can be executed as a „secure“ process, i.e. each component can be signed and verified by a chain-of-trust (see also Figure 1).

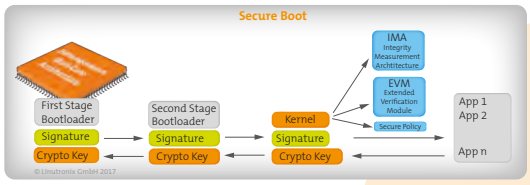


Fig. 1: chain of trust

Hypervisor

The Open Source Realtime Hypervisor jailhouse, a Type I representative, is an excellent tool for partitioning Cortex-A clusters and thus enabling an increased level of security. The real-time capability in the guest system is almost unaffected, the impact is in the range of < 3 µsec. Jailhouse allows any combination of Linux, other operating systems, bare metal applications and assignment of CPUs to an operating system.

Jailhouse allows to easily consolidate existing solutions on a SoC. Figure 2 shows an example.

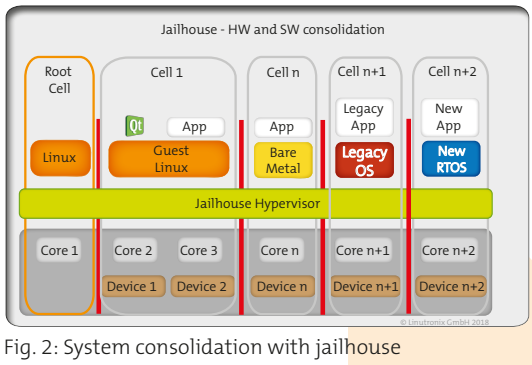


Fig. 2: System consolidation with jailhouse

Intercore Communication

Communication between the individual CPUs of any asymmetric multiprocessor design is a challenging task. Open Source solution OpenAMP helps to simplify this task and allows solutions between single CPUs of a cluster as well as between heterogeneous CPUs without having to consider the operating system used. Even for bare metal applications corresponding libraries are available. Figure 2 shows a typical solution.

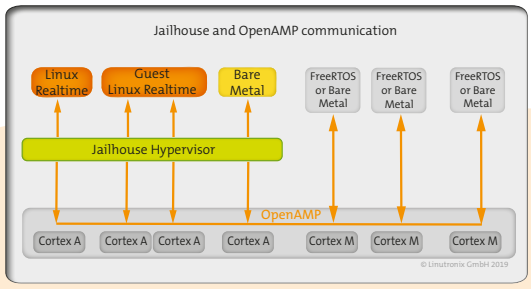


Fig. 3: OpenAMP communication

Linutronix solutions

Linutronix offers complete support for heterogeneous multi-core CPUs.

- Linux with Preempt-RT for the Cortex-A Cores and freeRTOS for the Cortex-R and -M processors respectively
- openAMP Framework for communication between the subsystems
- jailhouse as hypervisor implementation
- Based on our Industrial Grade Linux, the operating system can optionally be created as a hardened variant.
- Industrial Grade Linux optionally allows the use of containers for the individual applications.
- (OTA) Update options are available on request, either as a redundant system or analogous to Android with an update kernel. Also available as a solution with signed updates to ensure system security.
- Also available with an associated device management and roll-out server.

Are you interested? Would you like to learn more about our products and solutions? Simply contact us via telephone or email.

02/2019_V1.1

LINUTRONIX GMBH
Bahnhofstrasse 3 | D-88690 Uhldingen - Mühlhofen
Telefon +49 7556 25 999 0 | Fax +49 7556 25 999 99
sales@linutronix.de | www.linutronix.de

LINUTRONIX
LINUX FOR INDUSTRY