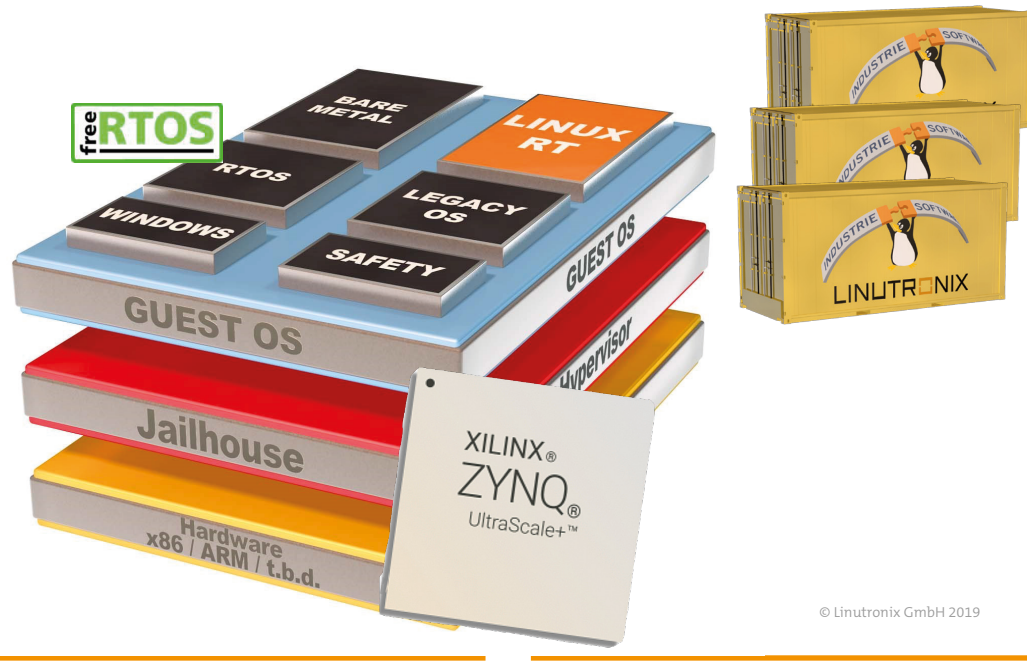
LINUTRONIX

JAILHOUSE

Hypervisor, Real-time, Linux and more for UltraScale+



ARM/FPGA Hybrid

Modern SoCs are becoming increasingly complex and diverse. This reflects both the trend towards the standardization of many functions of an embedded system in a hardware as well as the increased requirements regarding security and safety.

Whereas in the multi-core world mainly homogeneous solutions (i.e. n-CPUs of the same architecture, e.g. x86) were common in the past, heterogeneous multi-core CPUs are now entering the (embedded) market. This is where different CPU architectures and programmable logic (FPGA) are combined to offer an optimal solution 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. And, of course, those parts containing know-how that you don't want to pass on to third parties.

UltraScale+

How can you make sure that the different SW parts do not interfere with each other? On the hardware side there is the division into different processor platforms. And within an architecture platform (e.g. all Cortex A53 CPUs) you have the separation by a hypervisor.

UltraScale+ by Zynq offers a wide range of technologies that can be used to separate secure and non-secure processes. The most important components are:

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

Hypervisor Support - allows the use of a real-time hypervisor such as jailhouse.

System MMU, XMPU and XMPU - different technologies for isolating DMA-enabled devices on the ARM A53 cores, for separating access from different subsystems to memory areas, or for isolating peripherals.

Secure Boot

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 either the Cortex-R5 or the Cortex A-53 processors. At the early stage of this boot process the hardware can be divided into isolated subsystems. The entire boot process 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).

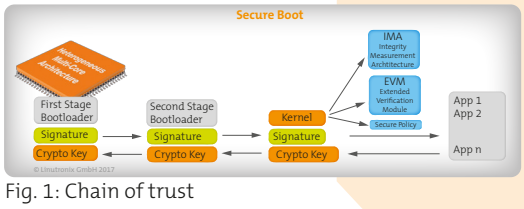


Fig. 1: Chain of trust

This high configurability allows the UltraScale+ to meet a variety of requirements. Thus it would be possible that SAFETY applications run on the Cortex-R5 cores, while the A53 cores are used under Linux for typical IoT applications and a GUI. Another typical case could be that a hypervisor (jailhouse) is used to assign the A53 cores to the applications, and thereby different levels of data integrity (multilevel security) are attained.

An overview of the possibilities of the UltraScale+ processor can be found in Figure 2.

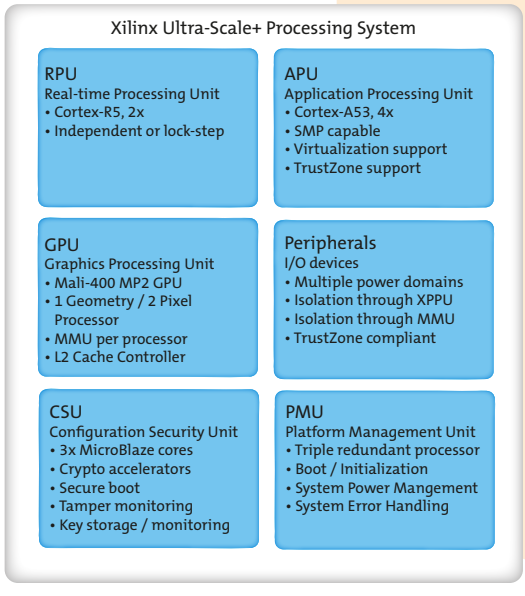


Fig. 2: Processing System

Linutronix solutions

Linutronix offers full UltraScale+ support.

Industrial Grade Linux with Preempt-RT for the A53 cores and freeRTOS for the Cortex-R5 processors, and the openAMP framework for communication between the subsystems.

And jailhouse as a hypervisor implementation. With this, latencies in the range of max. 12 -15 µsec. can be achieved also in the guest system under Linux with Preempt-RT (see Figure 3). The hypervisor's overhead is in the range of <3 µsec. jailhouse allows running any OS or bare metal applications on the cores.

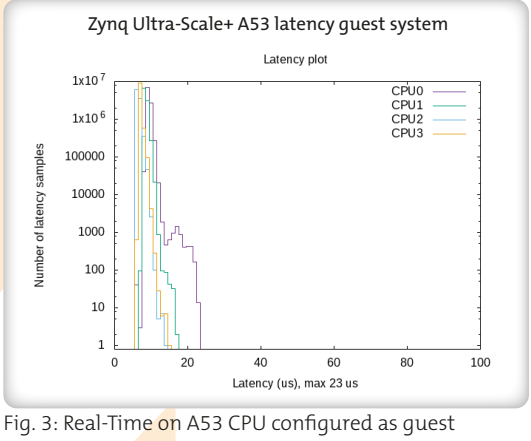


Fig. 3: Real-Time on A53 CPU configured as guest

The Cortex-R5 processors, operated under freeRTOS, show a response to external events in the order of < 10 µsec. (see Figure 4).

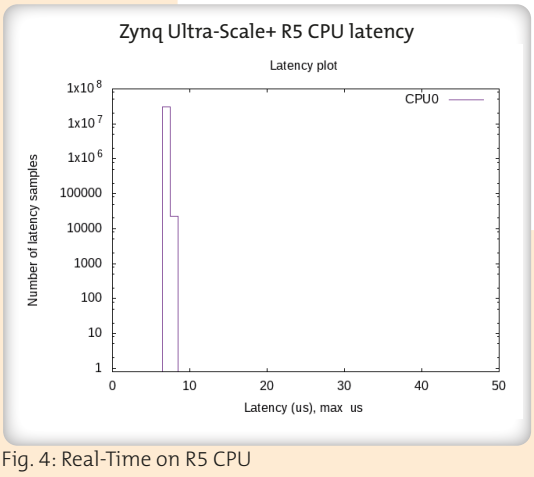


Fig. 4: Real-Time on R5 CPU

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

02/2019_V1.0

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