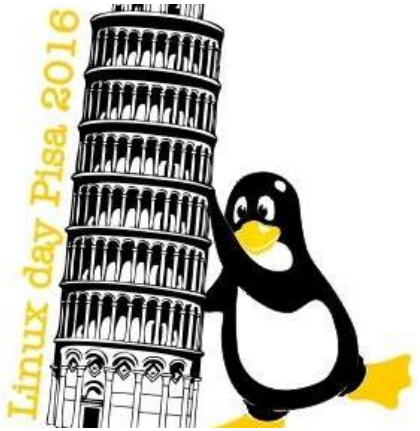


EVIDENCE®

EMBEDDING TECHNOLOGY

Virtualization techniques for automotive and industrial systems

LinuxDay 2016, Pisa

Stefano Garzarella
s.garzarella@evidence.eu.com

The company

Founded in 2002 as spin-off company of the
Real-Time Systems Lab at Scuola Superiore S.Anna

- ~20 qualified people with an average age of 34 years
- 10+ years of experience in academic and industrial projects
  - One third of the company has a PhD degree

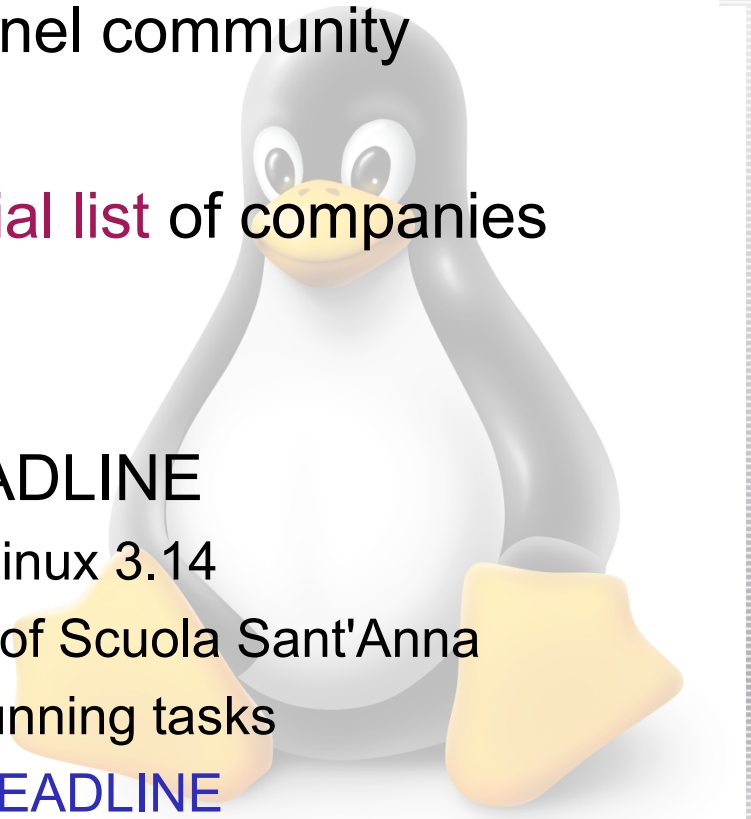
Our Mission:
design and development software for small electronic devices

Evidence and Linux

- Deep knowledge of kernel internals
- Constant collaboration with the kernel community

- Since 2008 Evidence is in the official list of companies that contributed to the Linux kernel

- Original developer of SCHED_DEADLINE
  - Real-time CPU scheduler merged in Linux 3.14
  - Made in collaboration with ReTiS Lab of Scuola Sant'Anna
  - It allows real-time isolation between running tasks
  - http://en.wikipedia.org/wiki/SCHED_DEADLINE



We already used Linux on...

Atmel:
- AT91RM9200
- AT91SAM9260
- AT91SAM9261
- AT91SAM9263

Digi:
- Net+ARM
- Wi9C

Manycores:
- Kalray MPPA
- TI Keystone II

Freescale:
- i.MX31
- i.MX25
- i.MX51
- i.MX53
- i.MX6
- MPC885

Intel:
- Atom
- x86
- IXP465

Realview:
- MPCORE

Renesas:
- SH4

Samsung:
- S3C2410
- S3C2440
- Exynos4412 Prime

Cirrus:
- EP9302
- EP9312

Xilinx:
- MicroBlaze
- Zynq

Something about ERIKA Enterprise

http://erika.tuxfamily.org

- ERIKA Enterprise is an RTOS OSEK/VDX certified
- ERIKA Enterprise implements an API inspired to a subset of the AUTOSAR API
- With a suitable open-source license allowing static linking of closed source code
- Typical footprint around 2-4KB Flash
- Used by various industries and research projects

OSEK/VDX compliance

OSEK/VDX compliancy done for:

- ARM Cortex M4F (TI Stellaris) in August 2012
- Infineon Tricore 26x in February 2014

ERIKA Enterprise is the first open-source kernel which has been certified OSEK/VDX compliant

The compliancy is linked to the following:

- RTOS version
- compiler and development environment
- microcontroller

(some) customers

OSEK, microcontrollers, schedulability analysis, code generation

ENEA, PIAGGIO, ARISTON THERMO GROUP, Honeywell, Indesit Company, MAGNETI MARELLI, cobra, aprilia, FAAM GROUP, Ferrari, MTA Advanced Automotive Solutions

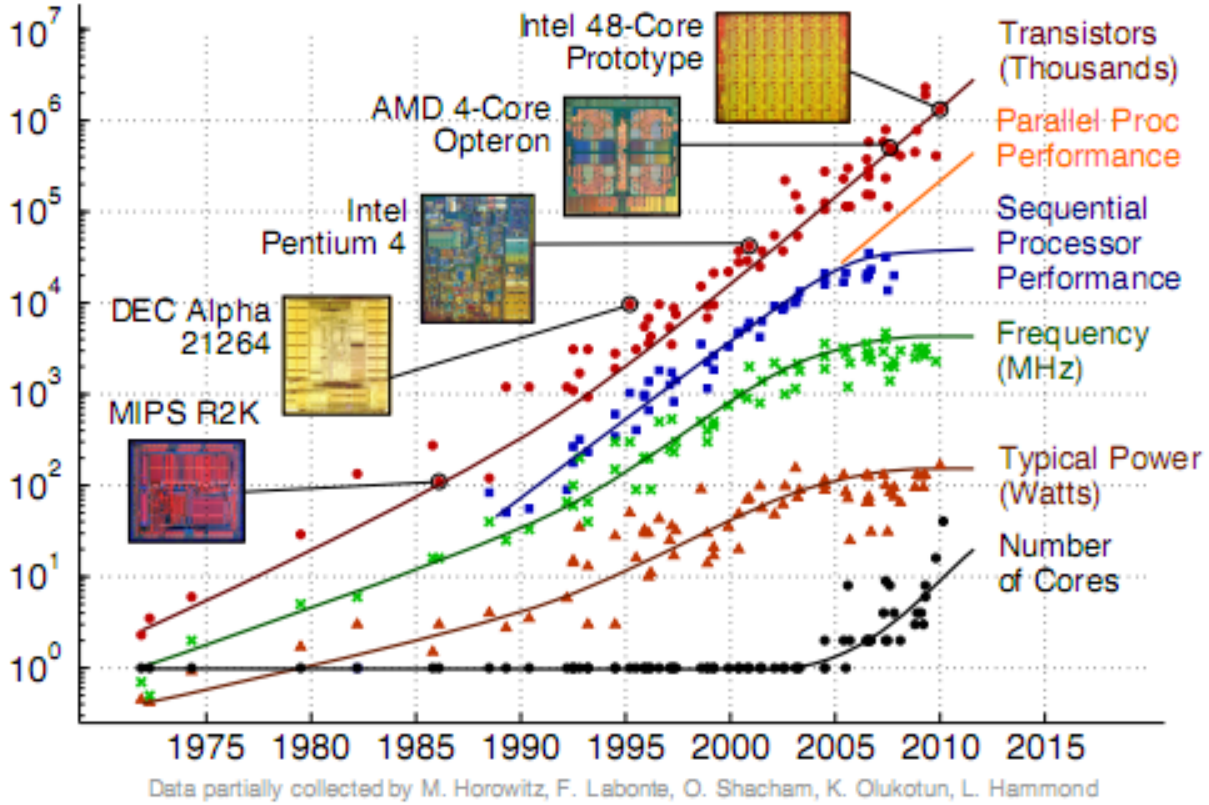
Linux, SW devel.

IMA Sharing Passions, intecs, ERICSSON, IDS INGEGNERIA DEI SISTEMI, KORG, NAVIONICS THE LEADER IN ELECTRONIC CHARTS, ALTRAN ITALIA, dexgate micro, CAENRFID, SIEMENS, Taggalo, COMECER, SISTEMI DINAMICI

Listed as 3rd party

LATTICE SEMICONDUCTOR, Recognized Microchip Third-Party Tool Provider, ALTERA, Digi, Qt Recognized Partner, ARM, RENESAS, XILINX ALLIANCE PROGRAM MEMBER, freescale Alliance Member

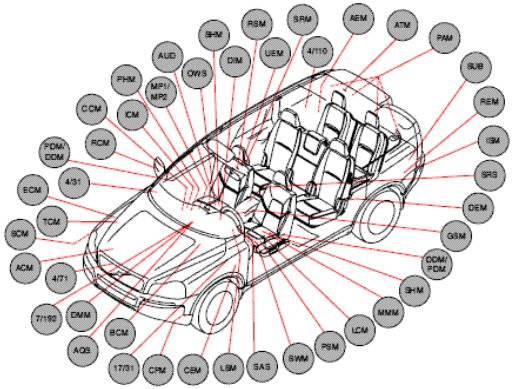
Multi-cores

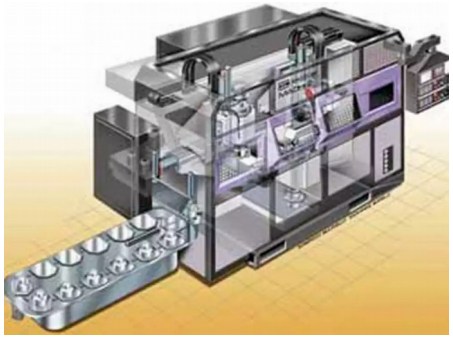


Prepared by C. Batten - School of Electrical and Computer Engineering - Cornell University - 2005 - retrieved Dec 12 2012 - http://www.csl.cornell.edu/courses/ece5950/handouts/ece5950-overview.pdf

Multi-OS: Motivations

- Idea: Reduce costs using multi-cores systems
- Automotive
  - A modern car may have up to 100 ECUs
  - Legacy systems support
  - Advanced driver assistance systems (ADAS)
- Industrial systems
  - RT Applications currently run only on one core
- Two kind of tasks
  - Safety critical → Erika Enterprise (RTOS)
    - Real time guarantees
    - Certifications (eg. OSEK/VDX)
  - User Interface (In-Vehicle Infotainment, GUI) → Linux
    - Network stacks (eg. TCP/IP, Ethernet, Wi-Fi, Bluetooth)
    - Graphic Libraries (eg. OpenGL, Qt)





Multi-OS: State of the art

- Different commercial solutions proposed by
  - Sysgo, Vector, Mentor Graphics, Green Hills
    - certified hypervisors that run complete AUTOSAR + Linux stack
- Our solution
  - totally based on top of open-source software
    - ERIKA Enterprise + Linux
    - With or without open-source hypervisor (eg. XEN, Jailhouse)

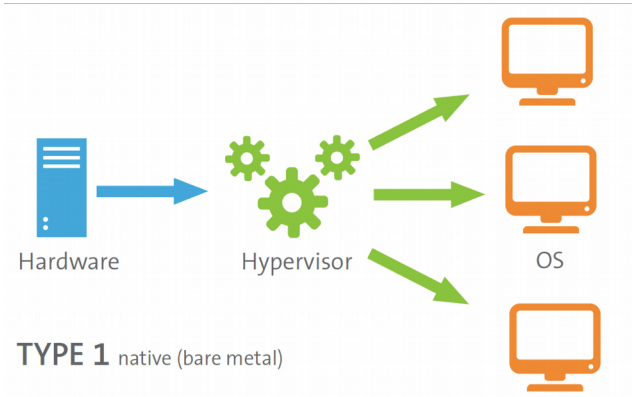
ERIKA ENTERPRISE + 

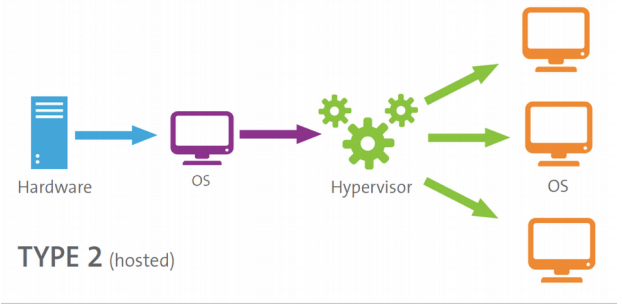
Multi-OS: Open issues

- Isolation
  - No CPU scheduler
- Low latency and exclusive access to the peripherals
  - Static allocation of peripherals
  - No emulation of peripherals
- Memory bandwidth
  - Guarantee minimum memory bandwidth for each core
- Safety
  - Separation of safety-critical from general-purpose apps
  - HW virtualization extensions

Hypervisors

- Type-1
  - native or bare-metal hypervisors
  - HYP runs directly on the host's hardware to control the hardware and to manage guest OSs
- Type-2
  - hosted hypervisors
  - HYP runs inside a general purpose OS (host) and a guest operating system runs as a standard process in the host.
- Exceptions
  - Linux's KVM and FreeBSD's bhyve are kernel modules that effectively convert the host operating system to a type-1 hypervisor.





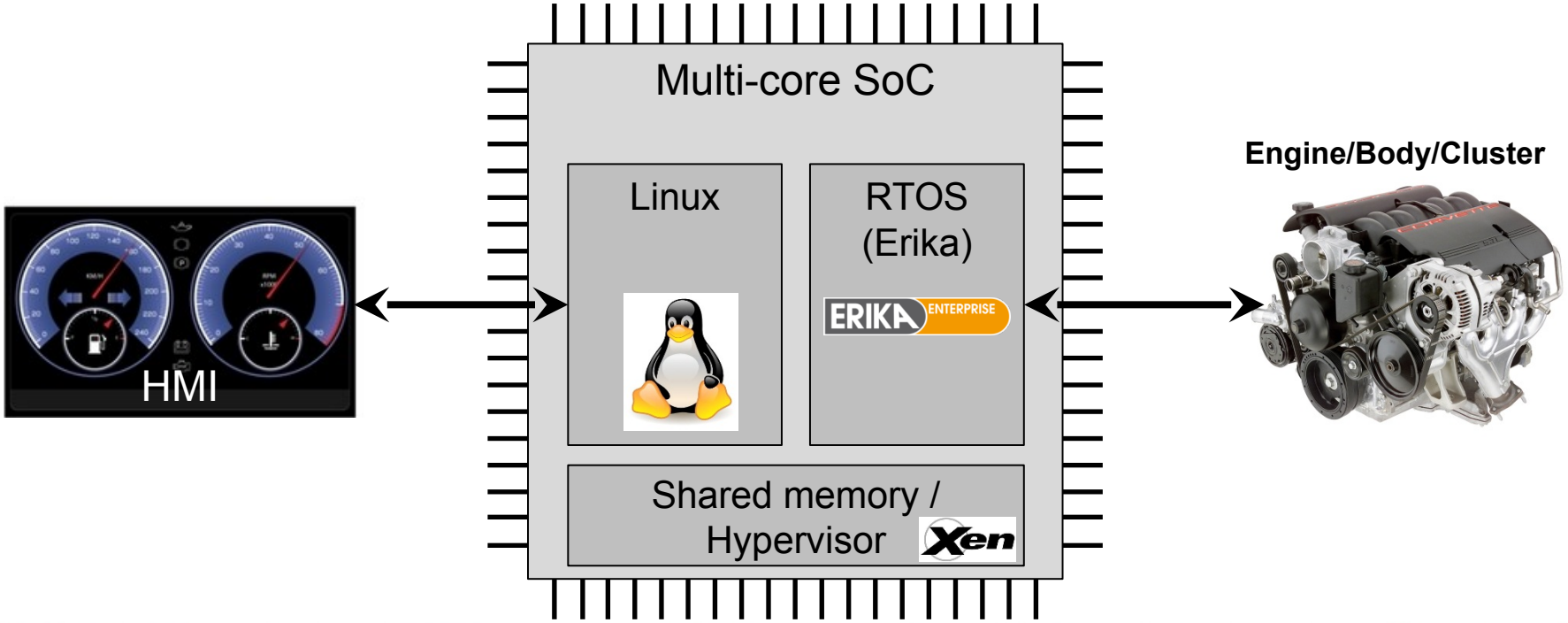
Hardware virtualization extensions

- x86
  - Hardware-assisted virtualization (Intel VT-x, AMD-V)
  - Page-table virtualization (Intel EPT, AMD RVI)
  - Interrupt virtualization (Intel APICv, AMD AVIC)
  - I/O MMU virtualization (Intel VT-d, AMD-Vi)
- ARM
  - ARM Architecture virtualization extension
  - Shadow page tables
  - Interrupt virtualization (VGIC)
  - System Memory Management Unit (SMMU)

Multi-OS: Linux + ERIKA on multicores

Real-time and quality of service for IVI systems with/without hypervisor!

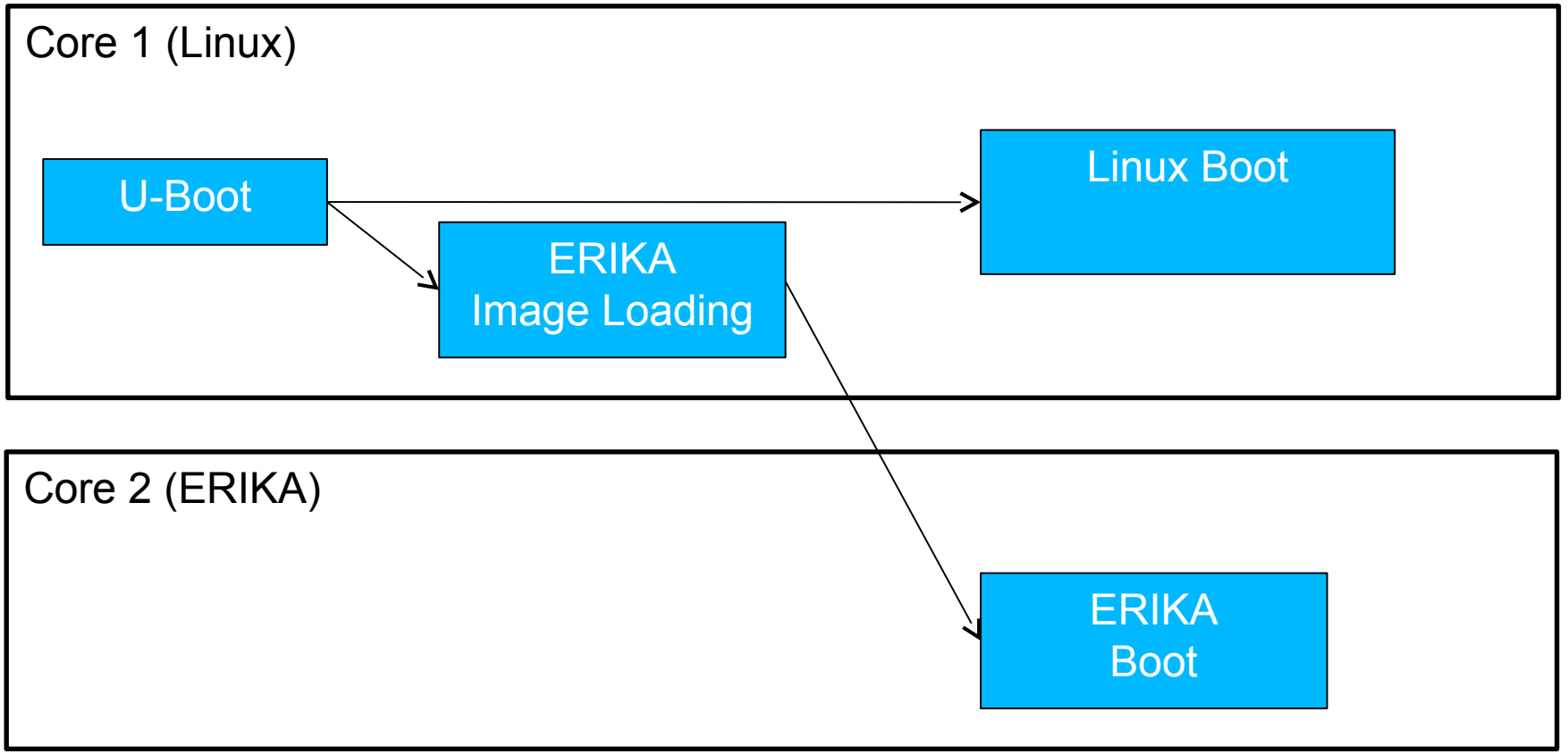
- ERIKA (RTOS) running on one core
- Linux on another core
- With or without Hypervisor (eg. XEN)



Multi-OS: Linux + ERIKA on multicores

- We need a infrastructure to allow applications running on different OS to share resources and exchange data
- Hypervisor and/or OSs capable of providing temporal isolation
- Possible implementation
  - with Hypervisor
    - resource reservation extended to all the system resources
    - isolation between guests
  - without hypervisor
    - more efficient in terms of memory and runtime overhead
    - concerns on the safety

Multi-OS without hypervisor



Interaction model

Linux → ERIKA

- Linux can trigger the following actions:
  - activate a task
  - set an event
  - start an Alarm
  - increment a counter

  (similar to those doable on a remote core of an AUTOSAR OS)
- Linux can stop and reload the ERIKA application

Linux ←→ ERIKA

- Simple asynchronous message passing allowing asynchronous read/write of variable length buffers on predefined channels

Multi-OS with hypervisor

+

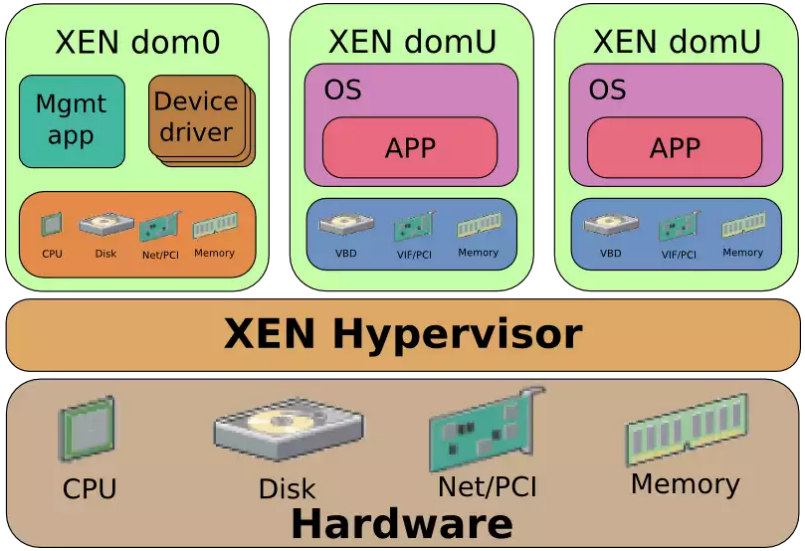
http://xenproject.org/about/events/viewevent/154-linuxcon-eu-integrating-linux-and-the-real-time-erika-os-through-the-xen-hypervisor.html

- In collaboration with the University of Modena
- ERIKA Enterprise as domU under XEN on a CubieBoard (Allwinner A20)

Presented at CloudCon Europe 2014, Dusseldorf

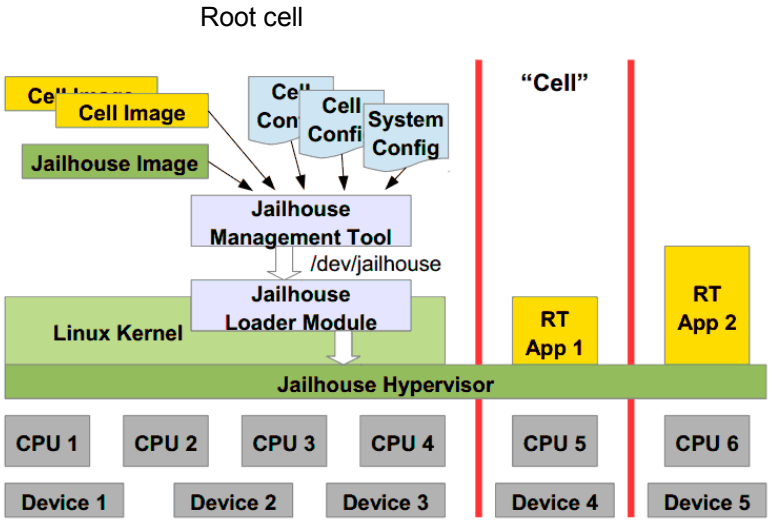
XEN

- Type-1 hypervisor
- Extensive and active community
  - Mature project (2003)
- It is main virtualization tool for virtual private servers and mainframes.
  - Amazon EC2, IBM SoftLayer, Liquid Web, Fujitsu Global Cloud Platform, Linode, OrionVM and Rackspace Cloud
- License: GPLv2
- Size: 150k SLoC



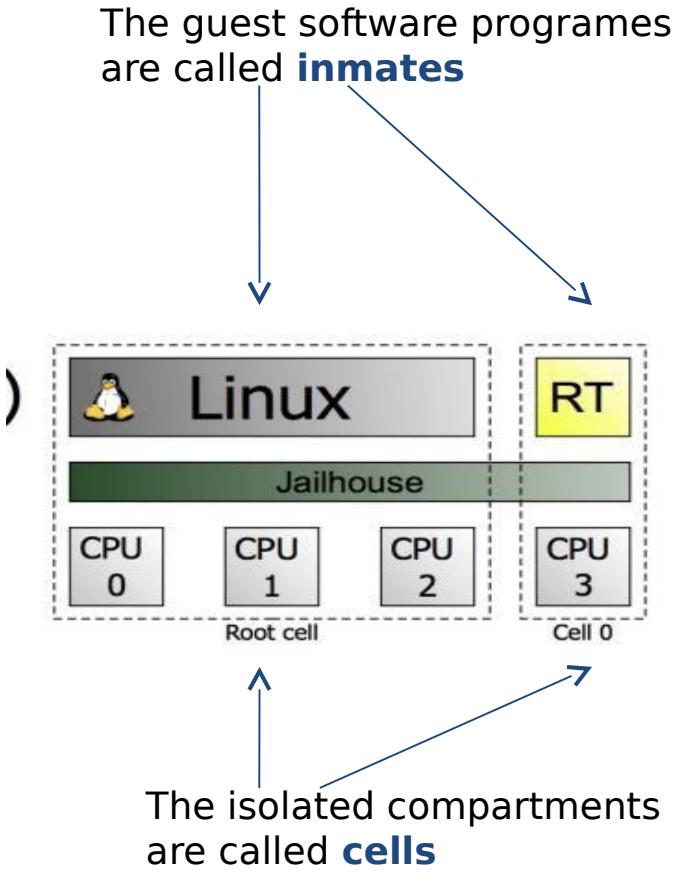
Jailhouse

- Small, lightweight hypervisor
- Young project (2013) by Siemens
- License: GPLv2
- Code hosted on GitHub
- Goals: safety-critical & certification
- Size: 10k SLoC



Jailhouse

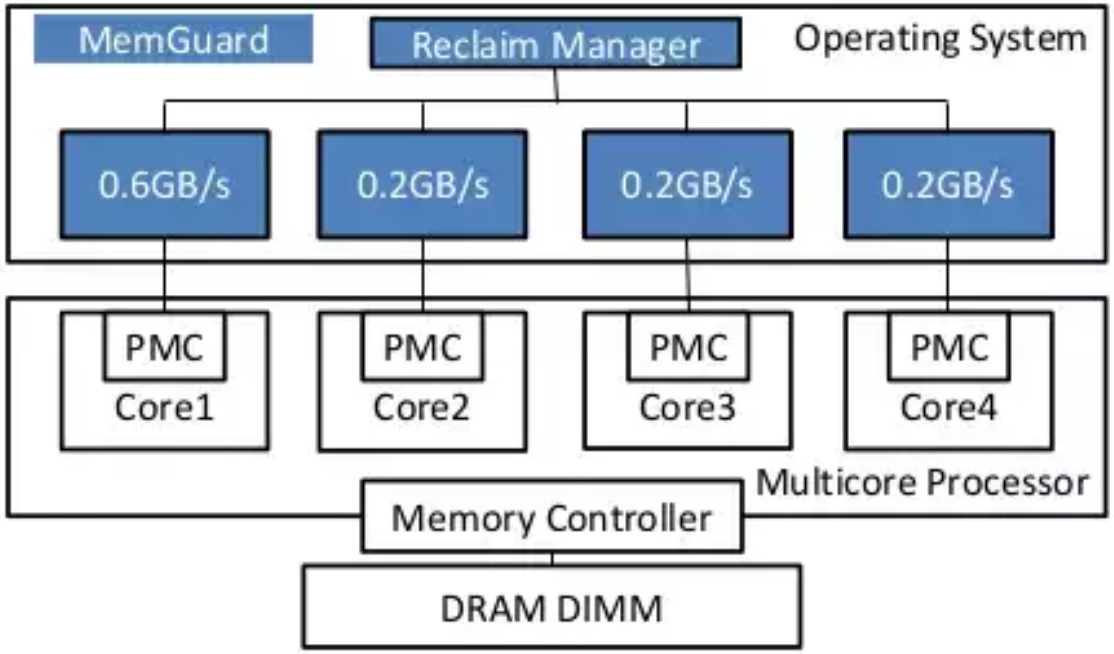
- Partitioning hypervisor
  - More focused on isolation than on virtualization
- Linux required
  - "Root" cell
  - Similar to Xen's dom0
  - Type-1 (Linux used only for management interface and load/unload guests)
- Can't run unmodified OSs
  - Even Linux on non-root cells need to be patched:
  - See http://git.kiszka.org (branch queues/jailhouse)



Jailhouse

- Static design:
  - 1:1 resource assignment
  - Guests can't share a core (no scheduling)
  - It doesn't support overcommitment of resources (like CPUs, RAM or devices).
  - No hardware emulation
- Real-time properties:
  - Must be provided by the guest

MemGuard [RTAS'13]



- Goal: guarantee *minimum memory b/w* for each core
- How: b/w reservation + best effort sharing

KU KANSAS

EU projects

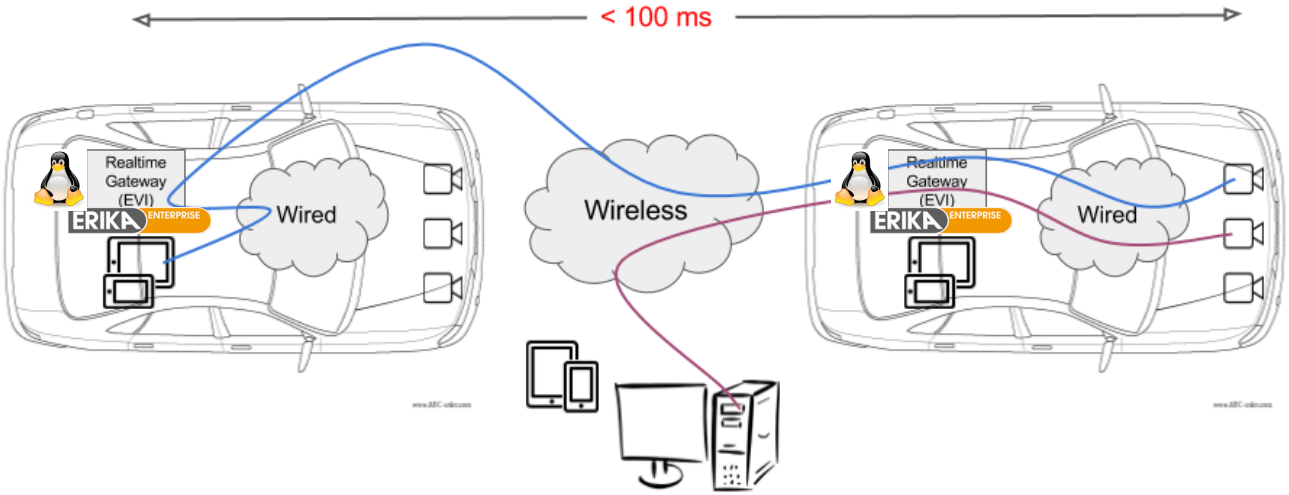
- RETINA

  - Real-time support for heterogeneous networks in automotive application
  - 2 years Eurostar-awarded project (Ends 2018-Q1)
    - SMEs: Time Critical Networks (coordinator), Alkit Communications, SWE & Evidence Srl, ITA
    - Research Institutes: Viktoria Swedish ICT & TNO, NL
    - Academia: SSSA, ITA & UL, FRA

EU projects

- RETINA

  - will provide integrated software tools to predict, simulate, test and support real-time communication in heterogeneous vehicular networks
  - Interesting use case
    - Sending time-sensitive HD video streams from camera to receiving processing unit

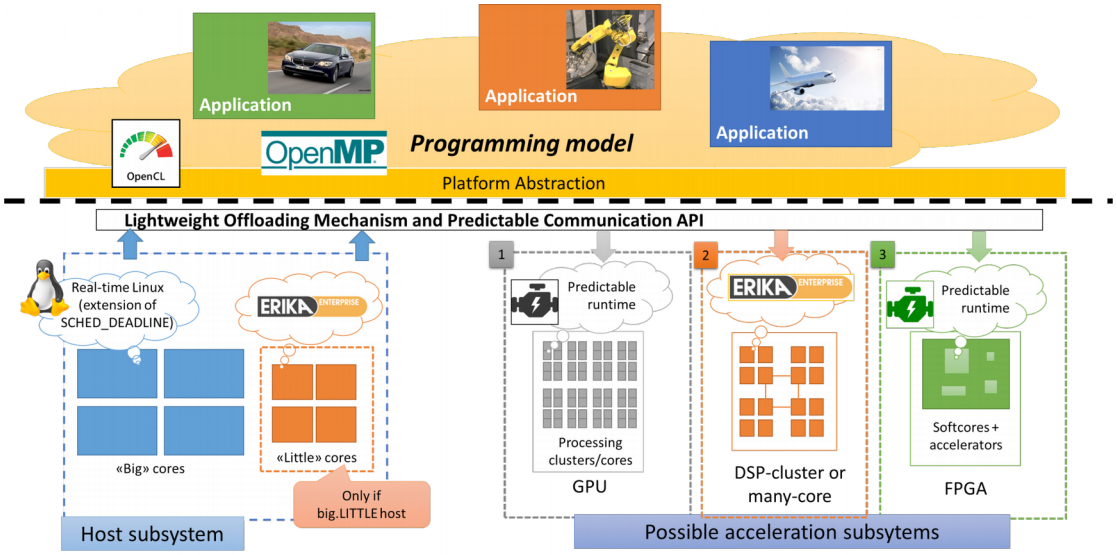


EU projects

- HERCULES
  - High-Performance Real-time Architectures for Low-Power Embedded Systems
  - 3 years European Union's Horizon 2020 research and innovation programme (Ends December 2018)
    - Partners: University of Modena, Czech Technical University in Prague, ETH Surich, Evidence Srl, Pitom snc, Airbus Gmbh, Magneti Marelli

EU projects

- HERCULES
  - will provide a software framework to simplify the development of next-generation real-time applications on heterogeneous COTS platforms
    - Performance with real-time guarantees
    - Low power/Low cost



Contacts

We often look for
Linux Software Developers,
please send us your CV at
info@evidence.eu.com

Evidence Srl
Via Carducci 56
56010 S.Giuliano Terme
Pisa - Italy

Web: http://www.evidence.eu.com
E-mail: info@evidence.eu.com
Phone: +39 050 99 11 224

Jailhouse

- Safety:
  - Locking of the configuration interface for some cells.
  - To prevent Linux from unintentionally shutting down safety-critical cells.
  - Certain cells are configured to vote over management decisions. (optional)
  - Jailhouse itself is not mapped into cells. This way, it is protected from unwanted guest access.

Jailhouse

- Inter-cell communication
  - Cells can communicate through virtual PCI devices
    - Model similar to ivshmem device from Qemu
    - Currently available only on x86
  - No multicast communications possible