Workshop 5, Technical support for safety critical systems:

Virtualization as a mean to isolate applications of different criticality in a multi-core system

4th Scandinavian Conference on SYSTEM & SOFTWARE SAFETY

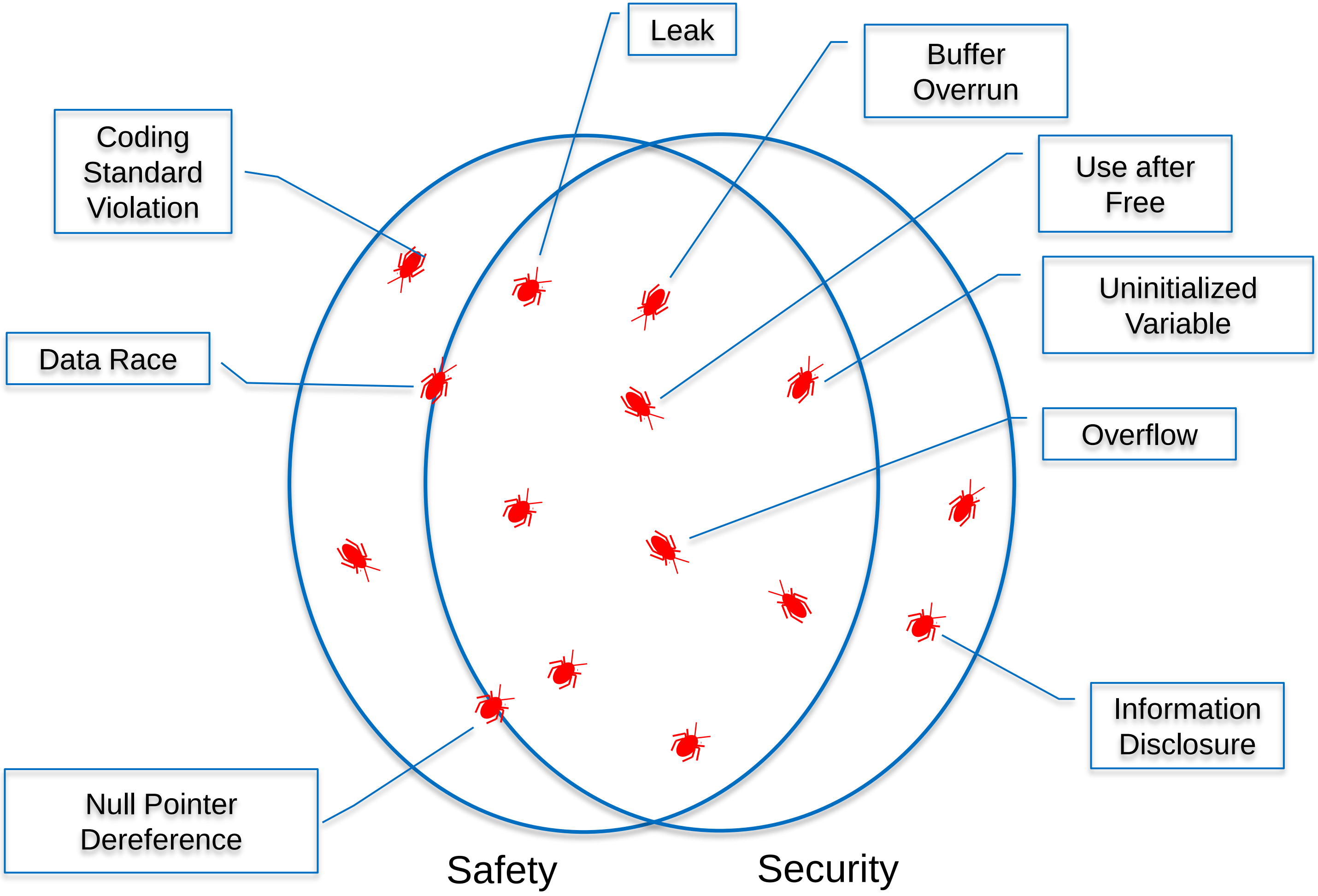
March 17, 2016

Joakim Nilsson
Nohau Solutions AB
Phone: +46 (0)40-59 22 08
joakim.nilsson@nohau.se
www.nohau.se

Nohau customers

ABB AB, ACTIA Nordic AB, ARRIS Sweden AB, Anite Telecoms Oy, Anoto AB, Atlas Copco Industrial Technique AB, Atlas Copco Rock Drills AB, Atlas Copco Secoroc AB, Autoliv Electronics AB, Autronica Fire and Security AS, Axis Communications AB, BAE Systems Hägglunds AB, Breas Medical AB, Bittium Wireless Ltd, BorgWarner TorqTransfer Systems AB, Broadcom Corporation, CPAC Systems AB, Clavia DMI AB, Coriant Oy, Delphi AB, Denso Sales Sweden AB, Eltek AS, Enea AB, Ericsson AB, European Spallation Source ERIC AB, FLIR Systems AB, Huawei Technologies Oy, Husqvarna AB, Hydroware Elevation Technology AB, Innokas Medical Engineering Oy, Intel Finland Oy, Kongsberg, Maquet Critical Care AB, Metso Flow Control Oy, Microsoft Mobile Oy, Nokia Solutions and Networks Oy, Norwegian Defence Communications, OY LM Ericsson AB, Planmeca Oy, Prevas AB, Posiva Oy, QRtech AB, RUAG Space AB, Saab AB, SCANIA CV AB, SECTRA Communications AB, Scandinavian Radio Technology AB, Siemens AB, Sigma Connectivity AB, Sony Mobile Communications AB, Space Systems Finland Oy, Structab AB, Suunto Oy, Teollisuuden Voima Oyj, Transmode Systems AB, VSM Group AB, VTT, Vacon Oyj, Volvo Car Corporation, Volvo Construction Equipment AB, Volvo Information Technology AB, Westermo Research and Development AB, Wärtsilä Finland Oy, ...

Concerns: Safety and Security!

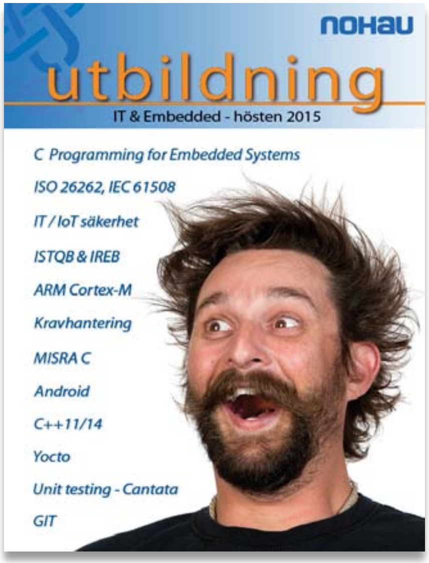


Nohau’s motto:

”Every Software Developer Deserves Great Tools and Support”

Strengthen embedded software development in the Nordics by bringing the right skills and advanced tool technology

(always scouting world-wide for better ways)


NOHAU

utbildning

IT & Embedded - hösten 2015

C Programming for Embedded Systems

ISO 26262, IEC 61508

IT / IoT säkerhet

ISTQB & IREB

ARM Cortex-M

Kravhantering

MISRA C

Android

C++11/14

Yocto

Unit testing - Cantata

GIT

- **Insight (visualization & measurements)**
- **Automation**
- **Right skills: Functional Safety (e.g. standards, MISRA), C/C++, tools)**

Top-ranked solutions

SYSGO
EMBEDDING INNOVATIONS

SEGGER

fte.com
frontline™

wurldtech
A GE Company

TASKING™

ARM®

KEIL™
Tools by ARM

LAUTERBACH
DEVELOPMENT TOOLS

GRAMMATECH

PRQA
Programming Research

LATTIX

QA SYSTEMS
The Software Quality Company

Visure
the requirements company

Advanced Business Partner
IBM™

Borland®
A MICRO FOCUS COMPANY

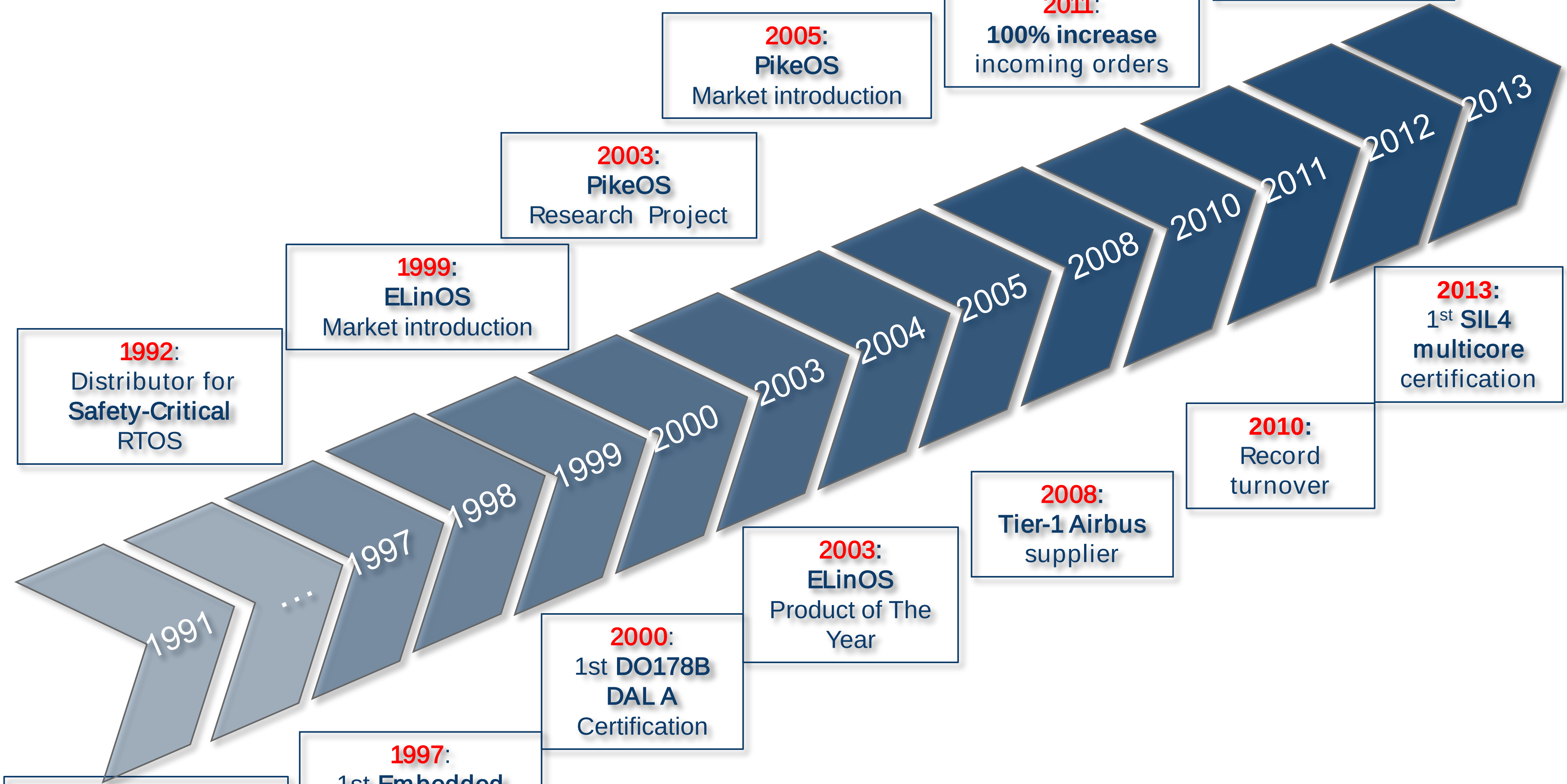
Today’s topic

Virtualization as a mean to isolate applications of different criticality in a multi-core system

SYSGO Facts

- An embedded software technology leader
  - COTS products & related services for most demanding industrial systems
- Founded in 1991, privately owned until 2012
  - Now owned by Thales Group
- Over 110 employees
- Business successful
  - Profitable
  - Growing
  - Strong financial backup
- International presence
  - Offices in Germany (Mainz, Ulm, Rostock, Hamburg), France (Paris, Lyon), The Czech Republic (Prague)
  - Distributors in Japan, Korea, Austria, Russia, Scandinavia

Company history



Foundation
as **RTOS**
Services Company

1992:
Distributor for
Safety-Critical
RTOS

1997:
1st **Embedded**
Linux project

1999:
ELinOS
Market introduction

2000:
1st **DO178B**
DAL A
Certification

2003:
PikeOS
Research Project

2003:
ELinOS
Product of The
Year

2005:
PikeOS
Market introduction

2008:
Tier-1 Airbus
supplier

2010:
Record
turnover

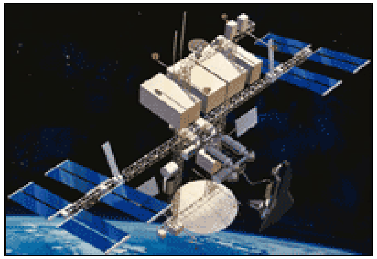
2011:
100% increase
incoming orders

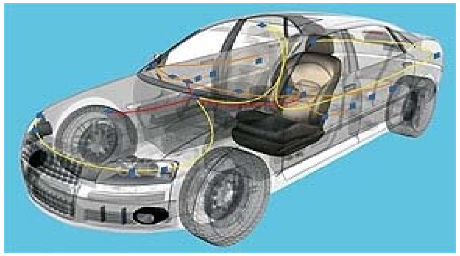
2012:
Part of Thales
Group

2013:
1st **SIL4**
multicore
certification

Markets

We consider our target markets to be all industries related to Embedded Systems in which safety, security and certification are required.



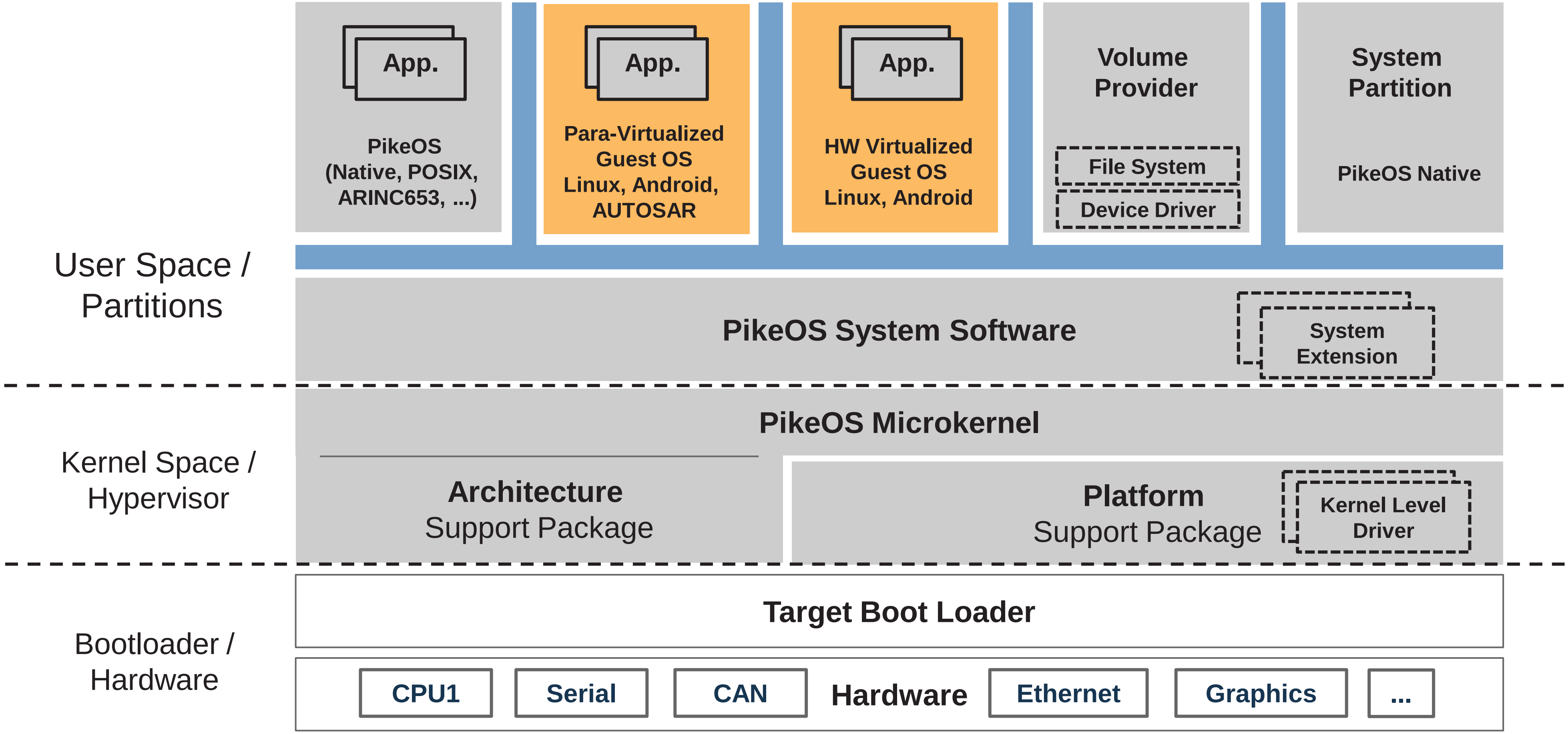


PikeOS in a Nutshell

Hard Real Time	• PikeOS is a hard real time operating system
Separation Kernel Architecture	• Fast and efficient Micro-Kernel with separation capabilities
Safe & Secure Hypervisor	• PikeOS is a virtualization platform for safety and security critical systems
Mixed Criticality	• Applications with different safety and security levels can run on the same hardware, protected from each other by means of software partitioning
Multiple Guest OS - Personalities	• OS-environments: Linux, Android, AUTOSAR, Posix, … • APIs and Run-time environments: ARINC-653, Java, ADA, …
Highly Portable	• Supports all important CPU Architectures like ARM, x86, PowerPC, MIPS and Sparc (requires at least a 32bit processor with MMU)
Certifiable	• Certifiable according to Highest Safety and Security Standards • Certification Kit for Safety Critical Avionics (DO-178B), Industrial Automation (61508) and Transportation Applications (55128); working on Automotive (26262) and security (CC EAL6)
No export restrictions	• Fully European source, no export controls, no ITAR controls

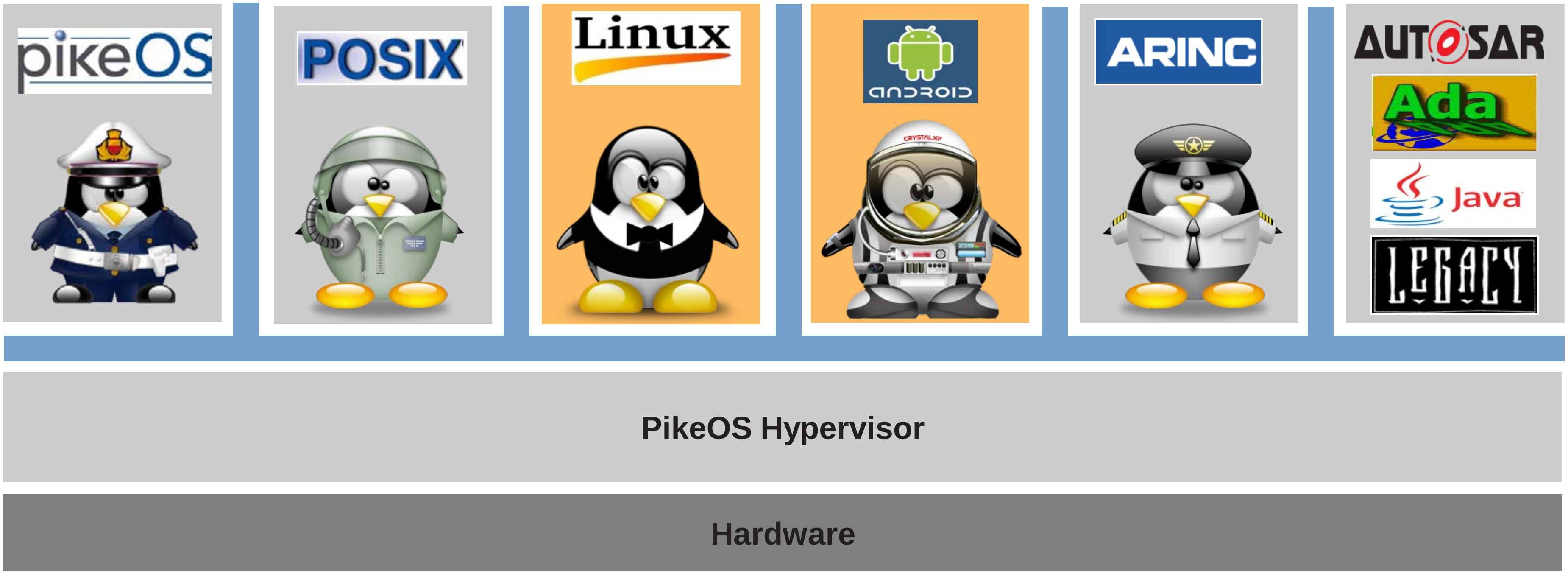
SYSGO
EMBEDDING INNOVATIONS

PikeOS Architecture – RTOS With Virtualization



SYSGO
EMBEDDING INNOVATIONS

PikeOS - Personalities



PikeOS Hypervisor

Hardware

Technical features

- Up to 63 resource partitions
- Up to 63 time partitions
- 253 priorities
- Less than 30 ms boot time
- 192kB RAM, 192kB ROM

PikeOS in Automotive

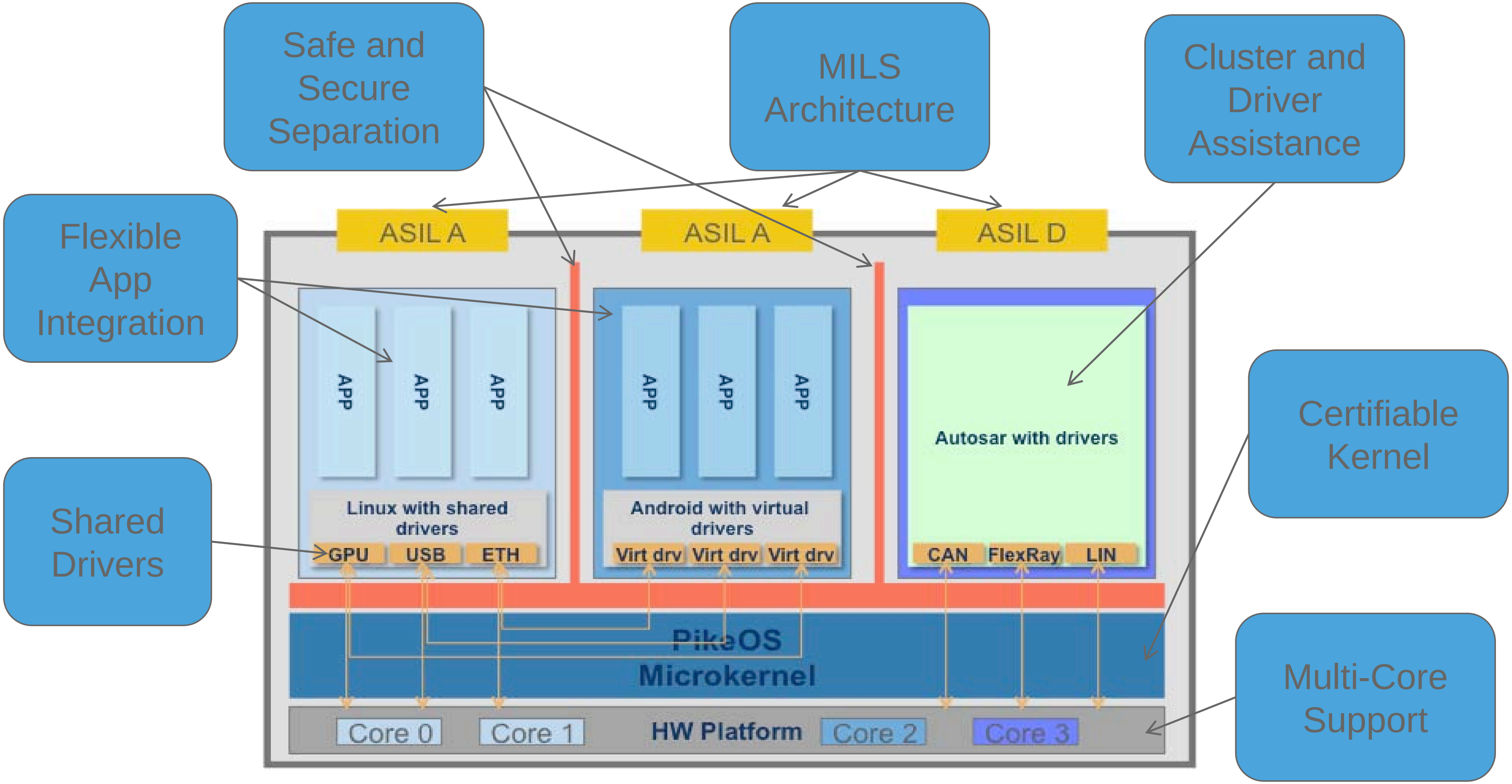
- **Certification-ready for ISO 26262**
- **Mixed safety and security levels possible on one system**
  - Safe & secure partitioning on a proven hypervisor technology
- **Ideal coexistence with automotive APIs**
  - AUTOSAR, POSIX, PikeOS Native, Linux, Android
- **Provide fast boot functionality**
  - Bring up critical partitions first
- **Boost your time to market**
  - 3rd party supplier products in separated partitions
  - Reduce dependencies and limit error propagation

Integrated Automotive Platform

- Clustering software functions
- Reduce number of ECUs
- Software separation
- High responsiveness
- Secure SW updates
- Secure boot
- High-performance shared graphics
- Applications of different security levels, different criticality levels, real-time or non-real-time, can run concurrently on a single SoC

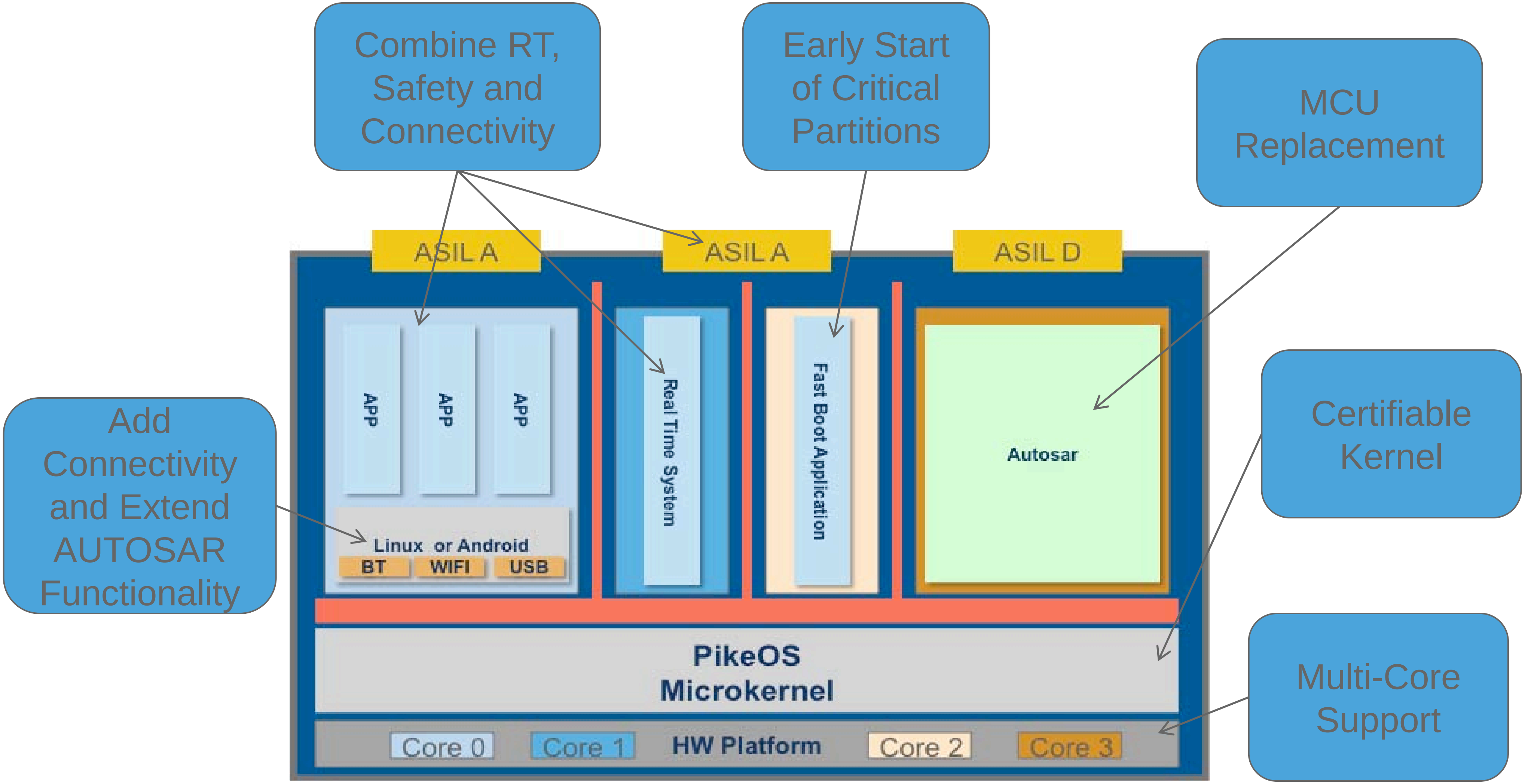
- Safety and Security are essential!

PikeOS Automotive Infotainment Example



EMBEDDING INNOVATIONS

PikeOS Automotive Connectivity Example



Combine RT, Safety and Connectivity

Early Start of Critical Partitions

MCU Replacement

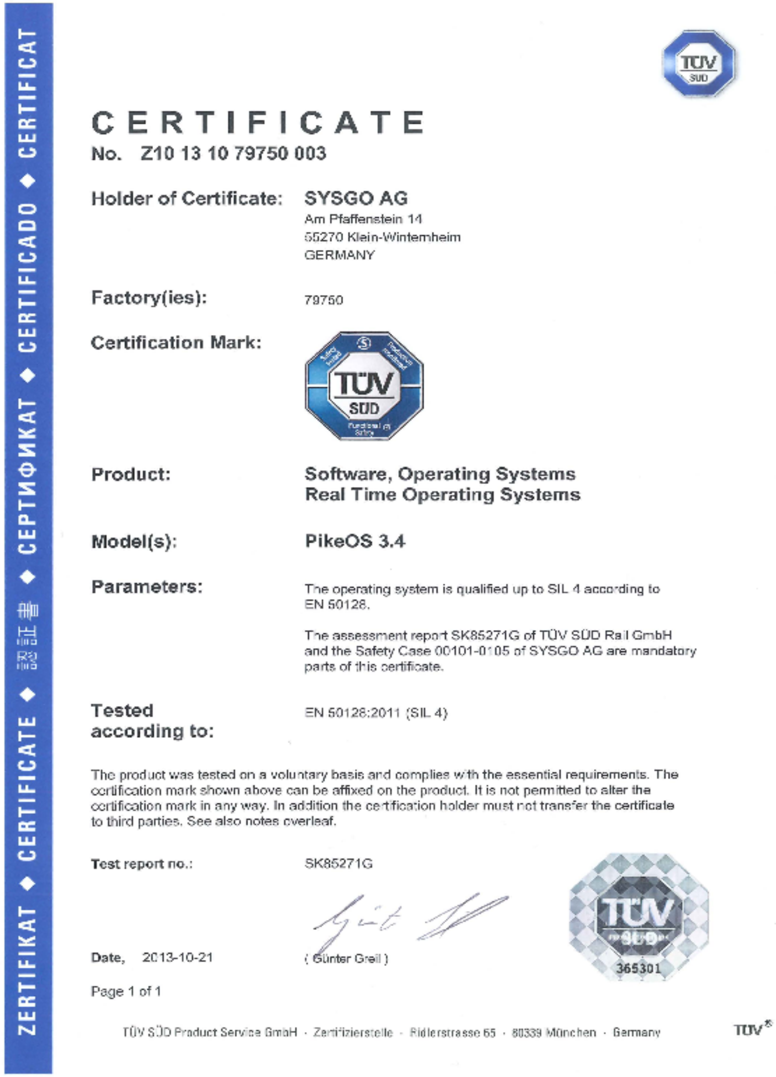
Add Connectivity and Extend AUTOSAR Functionality

Certifiable Kernel

Multi-Core Support

SYSGO PikeOS Certified Projects

- **IEC 61508 SIL3/4**
- **EN 50128 SIL 4**
- **EN 50128 SIL4 on Multi-Core**
- **DO-178B DAL B / DAL A**
- **CSPN** (France) **≈ EAL 4+**
- **BSI EAL 5+/6** (in progress)



ZERTIFIKAT ◆ CERTIFICATE ◆ 認証書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

CERTIFICATE

No. Z10 13 10 79750 003

Holder of Certificate: **SYSGO AG**
Am Pfaffenstein 14
55270 Klein-Winternheim
GERMANY

Factory(ies): 79750

Certification Mark:

Product: **Software, Operating Systems**
Real Time Operating Systems

Model(s): **PikeOS 3.4**

Parameters: The operating system is qualified up to SIL 4 according to EN 50128.

The assessment report SK85271G of TÜV SÜD Rail GmbH and the Safety Case 00101-0105 of SYSGO AG are mandatory parts of this certificate.

Tested according to: EN 50128:2011 (SIL 4)

The product was tested on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition the certification holder must not transfer the certificate to third parties. See also notes overleaf.

Test report no.: SK85271G

Date, 2013-10-21

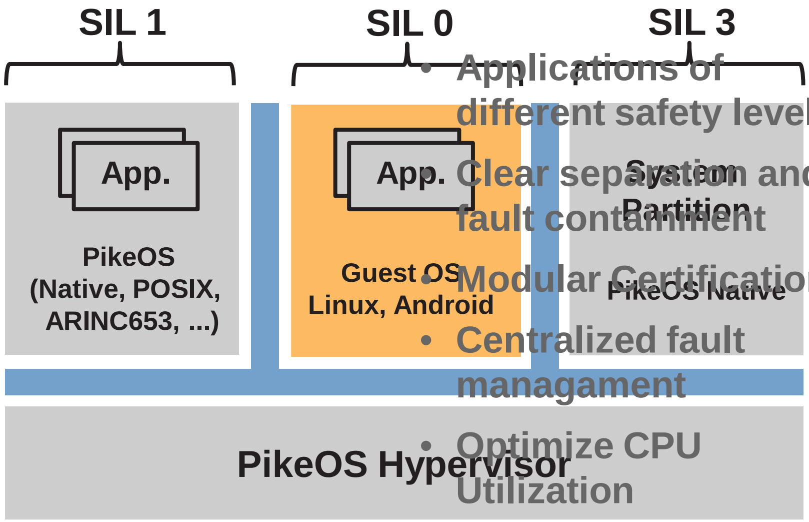
(Günter Greil)

365301

Page 1 of 1

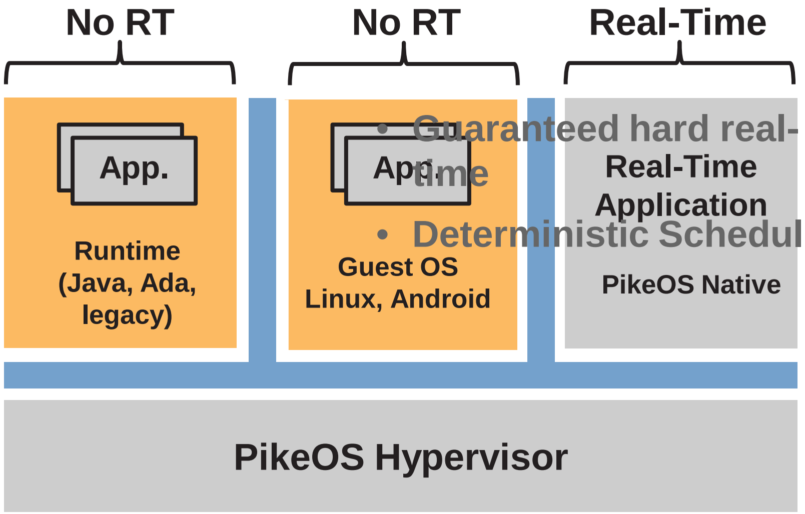
TÜV SÜD Product Service GmbH · Zertifizierstelle · Ridlerstrasse 65 · 80339 München · Germany

Mixed Criticality



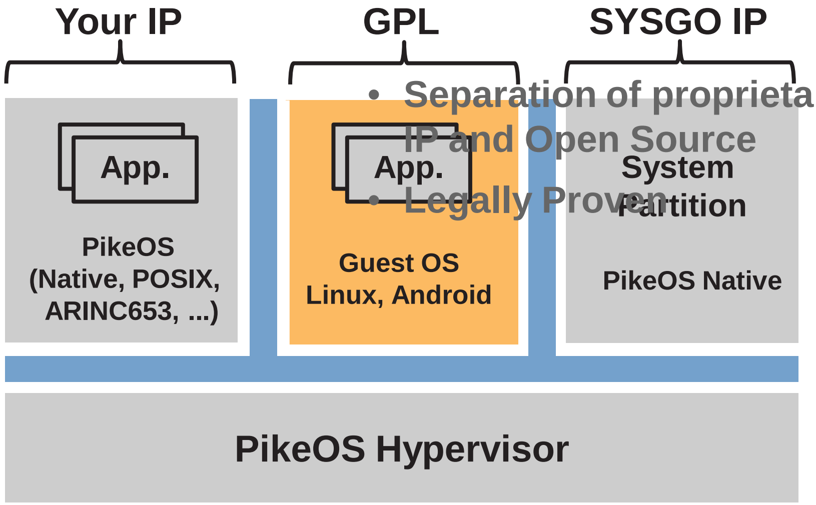
- Applications of different safety levels
- Clear separation and fault containment
- Modular Certification
- Centralized fault managament
- Optimize CPU Utilization

Mixing Real-Time and Non real.Time



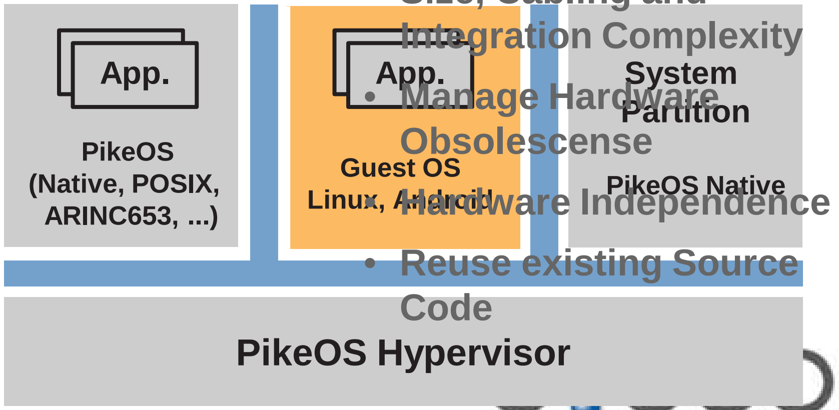
- Guaranteed hard real-time
- Deterministic Scheduling

GPL Isolation



- Separation of proprietary IP and Open Source
- Legally Proven

Hardware Convergence



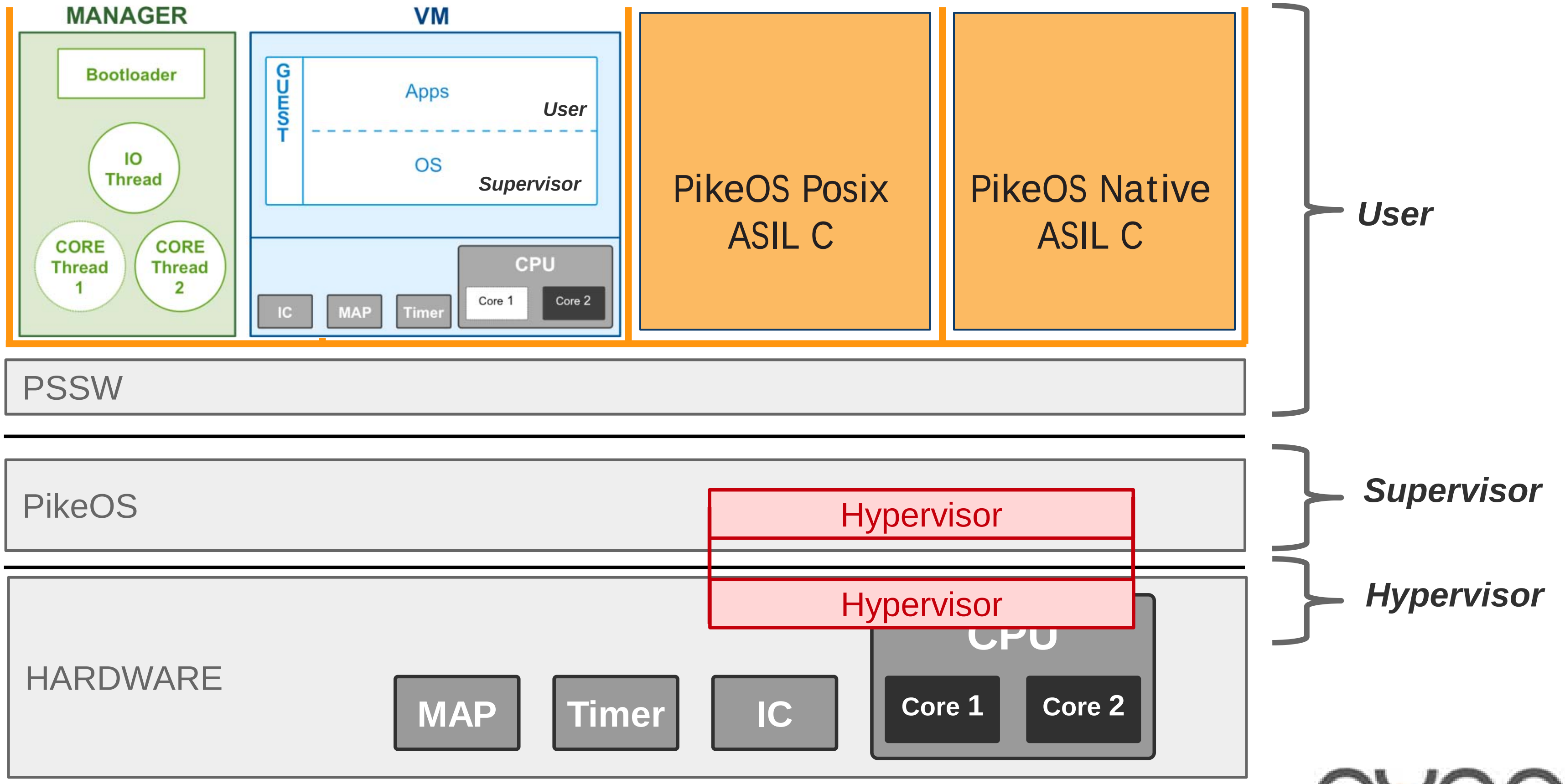
- Reduce Cost, Weight, Size, Cabling and Integration Complexity
- Manage Hardware Obsolescense
- Hardware Independence
- Reuse existing Source Code

EMBEDDING INNOVATIONS

PikeOS HW Virtualization Support

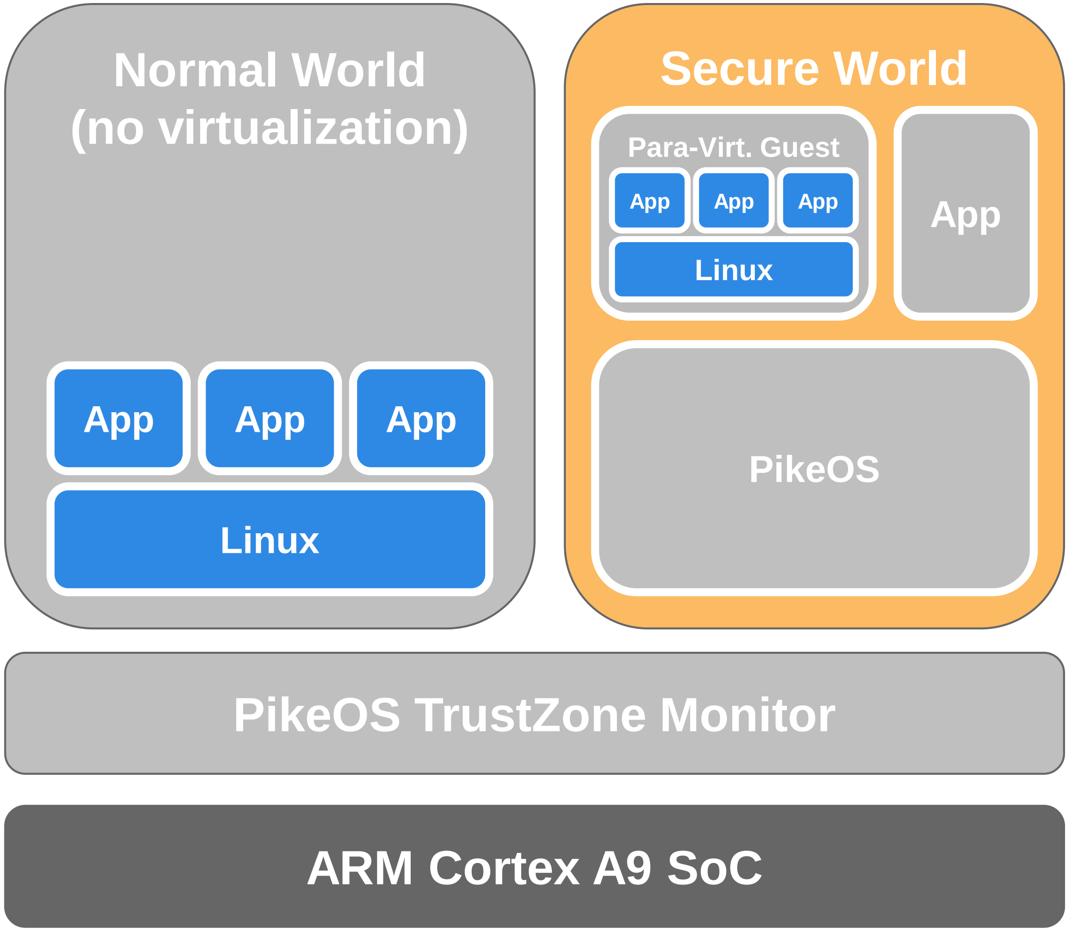
PikeOS Para Virtualization Support

- All virtual machines execute within separated partitions
- Partitions are protected by safe and secure segregation
- Virtualization is a common option, but not mandatory



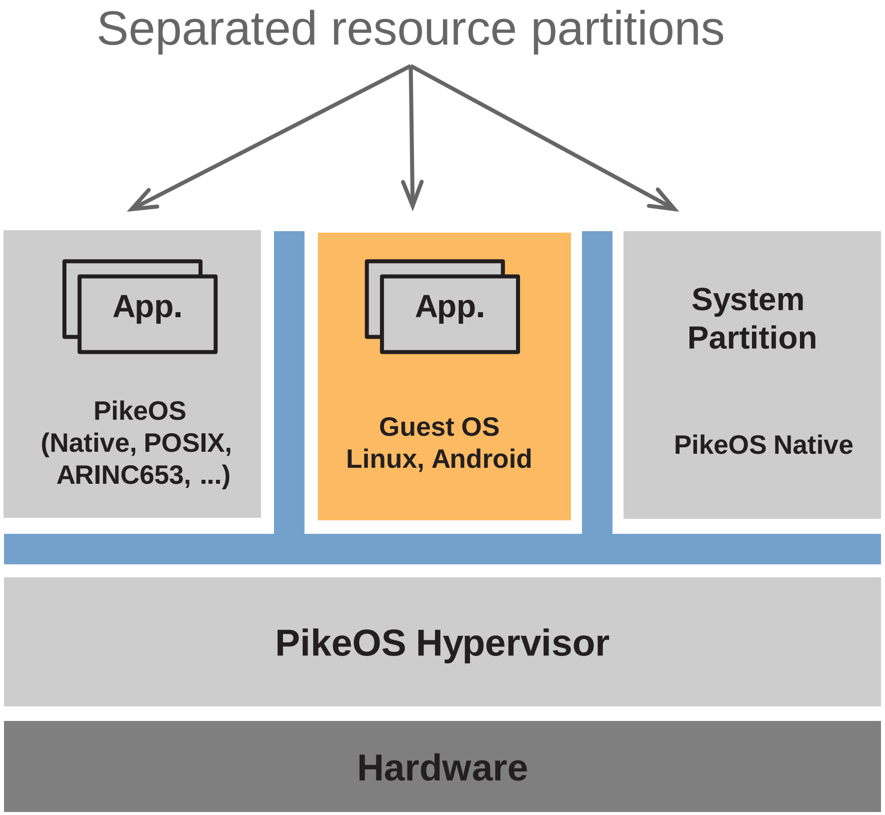
The Hypervisor - ARM TrustZone Support

- **PikeOS implements TrustZone Monitor**
  - CPU Cores are allocated to “Normal” and “Secure World”
- **PikeOS is running in “Secure World”**
  - All features of PikeOS are available
  - Para-Virtualized guest operating systems are supported
- **Unmodified guest OS can run in “Normal World”**
  - Runs with native performance
  - Direct access to hardware when enabled for “normal world”
- **Communication between “trusted” and “normal” world through P4-Bus**
  - Access to File Provider, Port Provider, Console, Part. Control, Target Control, Time Part. Control, ...

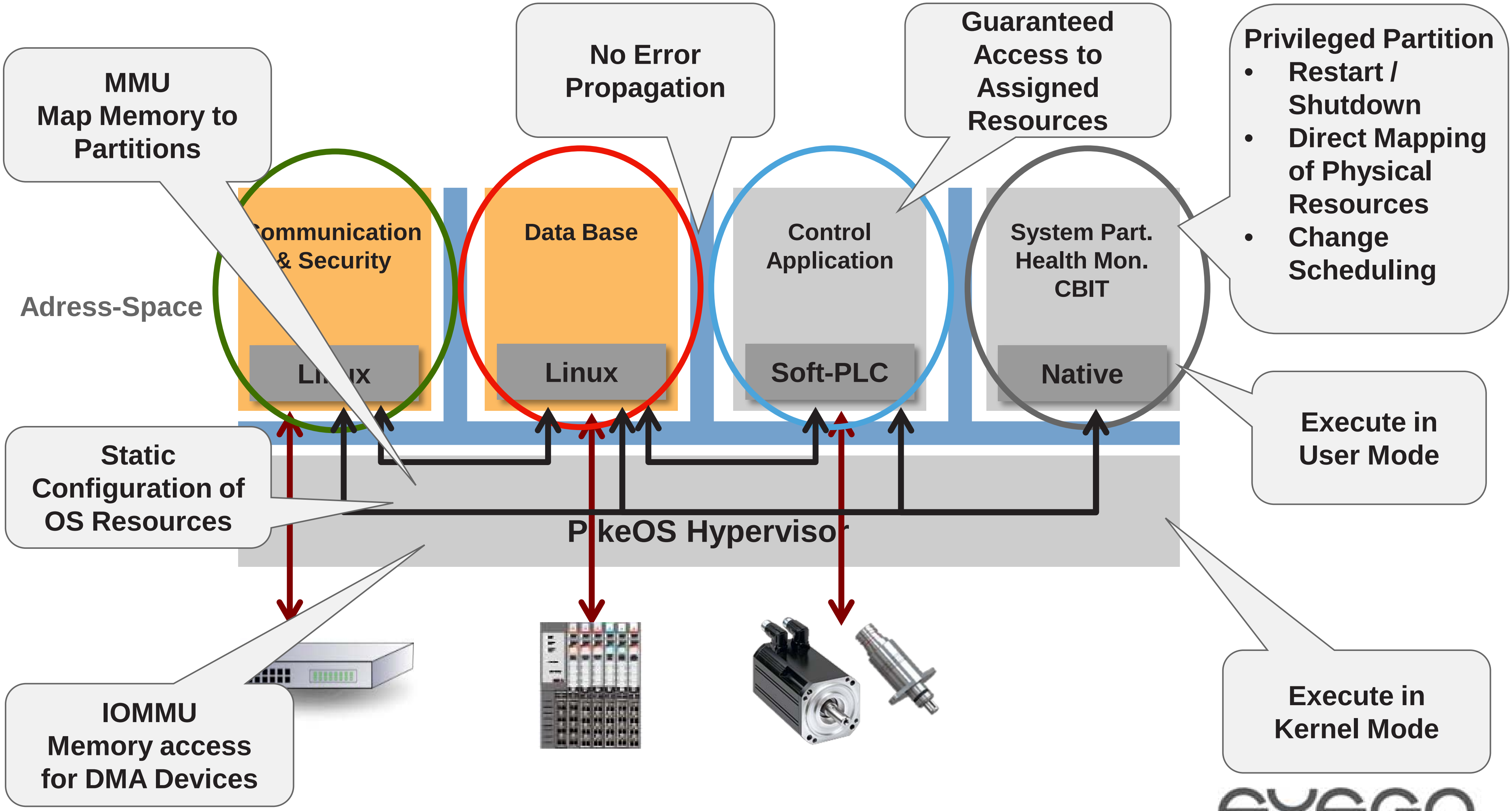


PikeOS Resource Partitioning

- **Container for User Applications**
- **One or more applications can share a resource partition**
- **Static configured set of resources and privileges**
- **Application has guaranteed access to assigned resources**
  - No Access to resources of other partitions if not explicitly configured
  - No error propagation throughout other partitions
- **Memory protection enforcement using Hardware (MMU)**
- **All partitions execute in user mode**

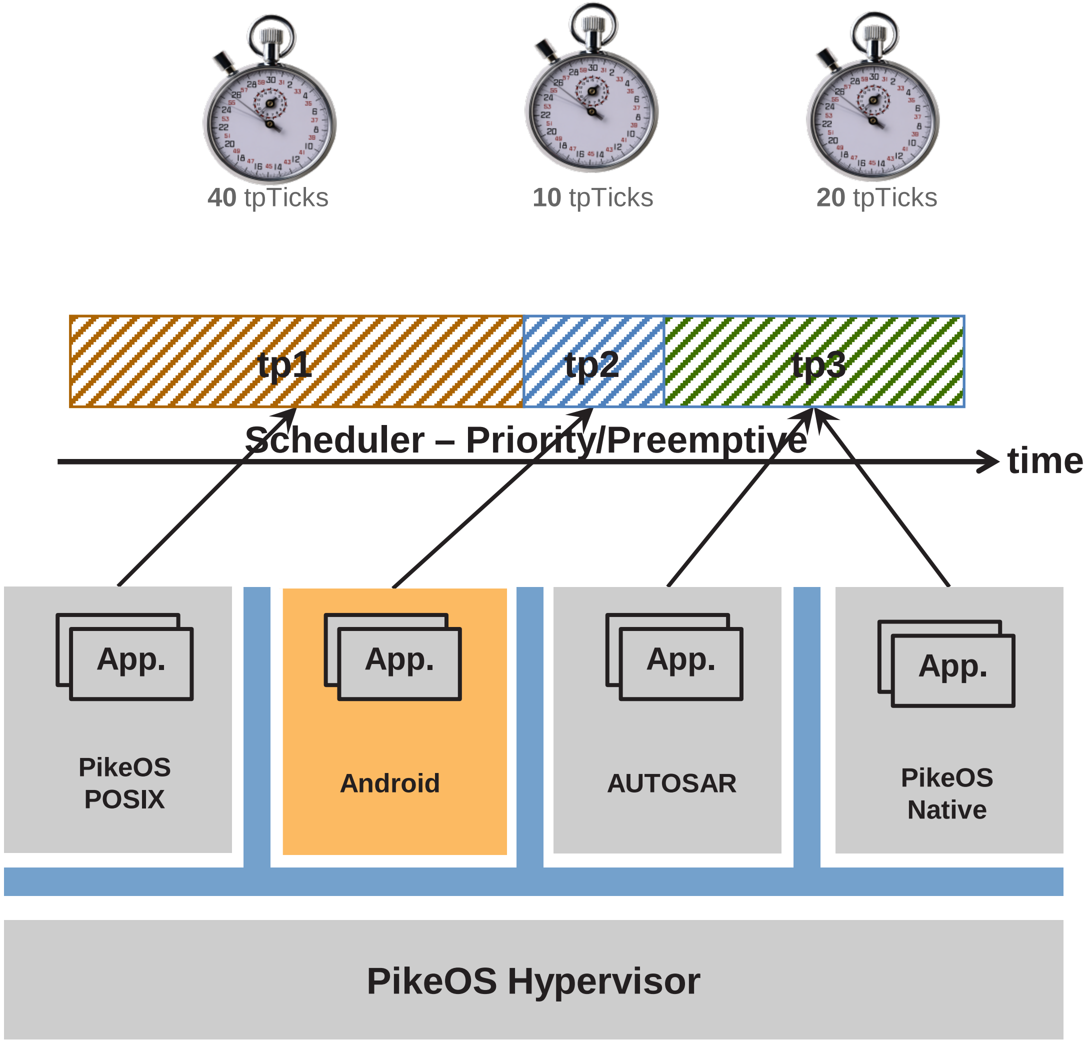


Resource Partitioning



PikeOS Time Partitioning

- **Static configuration of execution order and duration**
- **Deterministic Hard Real-time**
  - Guaranteed WCET
- **Shortest response time**
  - Dedicated thread with superior priority
- **Best possible CPU usage**
  - Partition '0'
  - Threads with high priority can preempt active partition
  - Threads with low priority can act as global idle-job



Hardware ecosystem

freescale™ semiconductor
ecrin SYSTEMS
AMCC
EMERSON. Network Power
kontron
men
CURTISS WRIGHT Controls Embedded Computing
ADVANTECH
FANUC
GE Fanuc Intelligent Platforms
TQ components Embedded Systeme
intel
ARM
NEC
AMD
XILINX®
MIPS TECHNOLOGIES
EPSON
IC INTERFACE CONCEPT
ATMEL
ELTEC systems
RENESAS Everywhere you imagine.
congatec the rhythm of embedded computing
MOTOROLA
PHYTEC TECHNOLOGIE HOLDING AG
TTTech

Software ecosystem

AbsInt

Quantum3D

aicas realtime

atego

ESTEREL Technologies

IBM

AdaCore The GNAT Pro Company

escrypt Embedded Security

OPENSYNERGY

scisys

OBJECTIVE INTERFACE

SAFE RIVER Safety & Security Forge

LAUTERBACH DEVELOPMENT TOOLS

tieto

SYMTA VISION

PRISMTECH

PRESAGIS

Systerel Solutions temps réel sécurisées

VECTOR software

SYSGO's Users

NASA
Rockwell Collins
Continental
ROHDE&SCHWARZ
MEGGITT smart engineering for extreme environments
THALES
AIRBUS DEFENCE & SPACE
HAMILTON MEDICAL
AIRBUS
MBDA MISSILE SYSTEMS
B|BRAUN SHARING EXPERTISE
NEC
ESG
LOCKHEED MARTIN
RHEINMETALL DEFENCE
Ansaldo STS A Finmeccanica Company
GENERAL DYNAMICS
ROLLS ROYCE
Honeywell
SIEMENS Transportation Systems
esa
FINMECCANICA
GÖRLITZ
ZODIAC AEROSPACE
EADS astrium
TAI
ONERA THE FRENCH AEROSPACE LAB
nsn
DLR
SAES
SAMSUNG
SAMSUNG SDS
SAFRAN Sagem
KNORR-BREMSE
EMBRAER