# Open-source automotive safety with the L4Re hypervisor


Michael Hohmuth, Adam Lackorzynski

Kernkonzept GmbH

# In this talk

Why Linux is not sufficient for critical applications

Why we need trusted microkernels for secure and safe systems

What is special about the L4Re system

What Kernkonzept does regarding security and safety certification

How certification and open source can mix

Opportunities for future joint projects

Research directions

# The problem

Software has bugs

Complex software has many bugs


1:20 PM
Remote
Lock
Unlock
Remote Start
Cancel Start
Horn & Lights
Stop Horn & Lights
Dashboard
Remote
More


www.President.ir

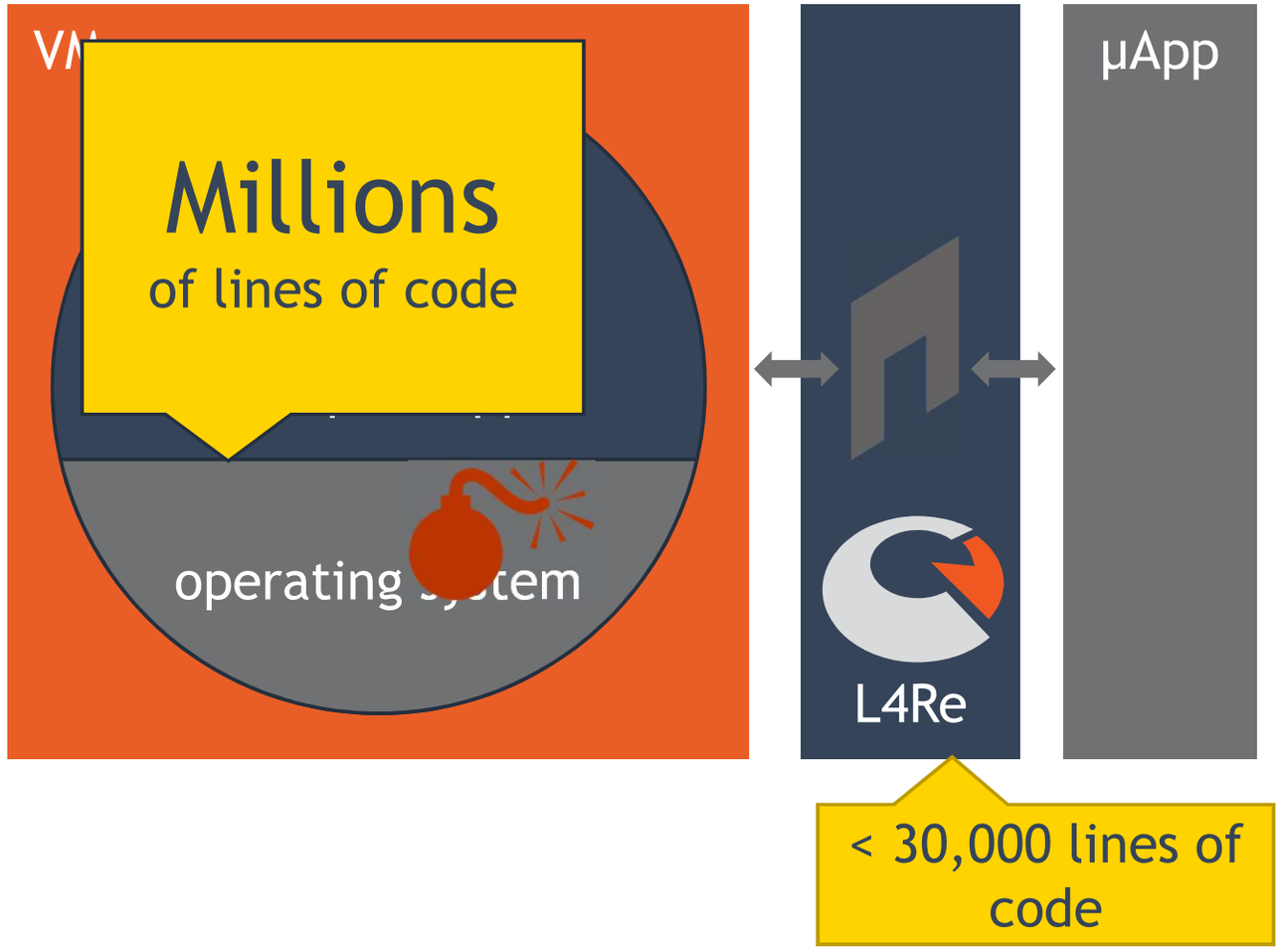

Bobby Vankavelaar
EXCLUSIVE
INVESTIGATION FOCUSED ON TESLA AUTOPILOT
abc ACTION NEWS
11:02
83°

# The solution

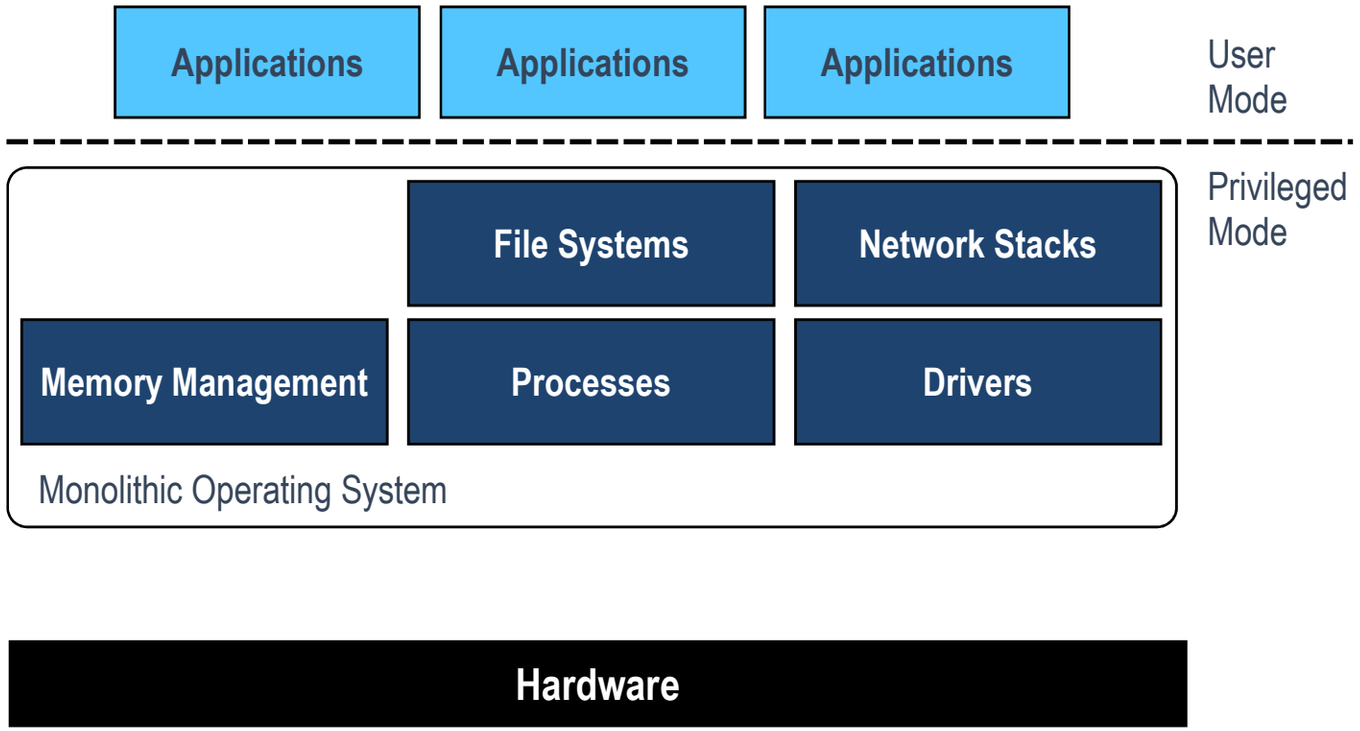
Isolation

Simplicity

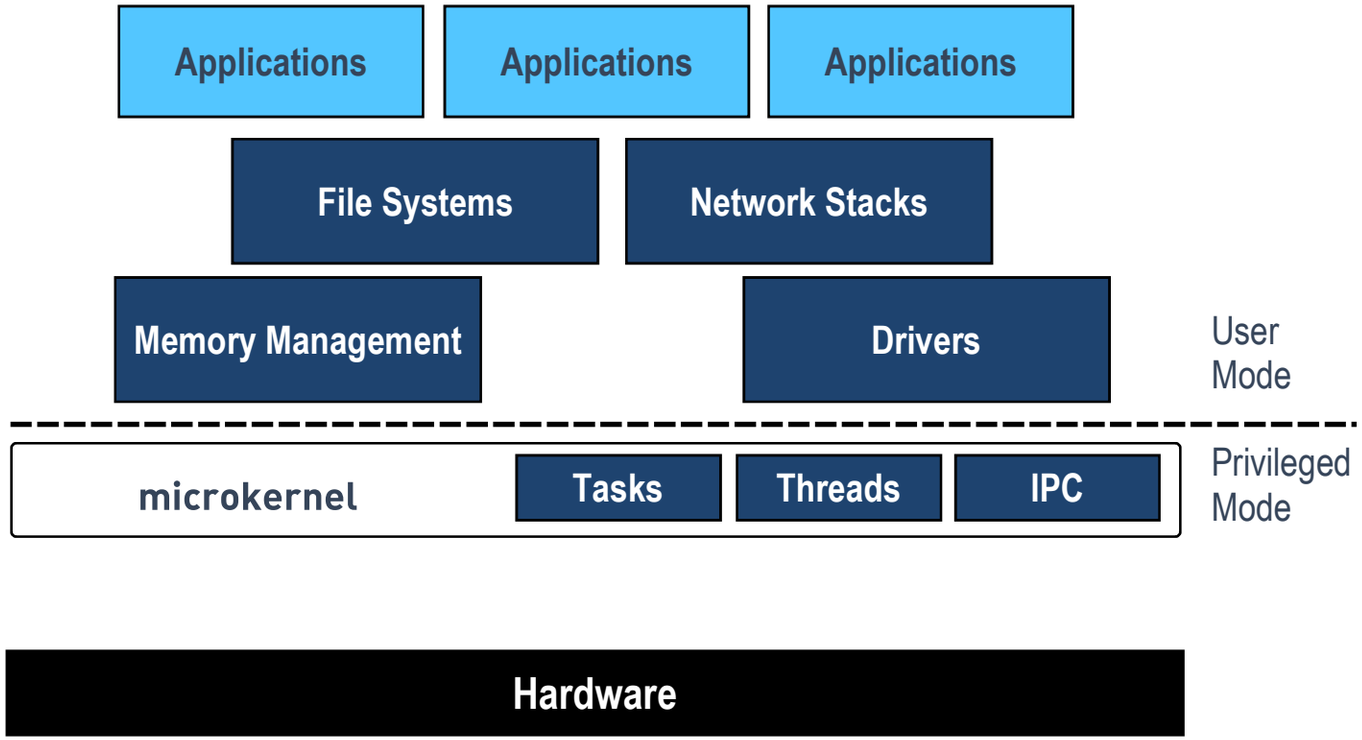
L4Re Microkernel



# Monolithic OS



# Microkernel OS



# Microkernel OS

Strong isolation / protection

Minimal trusted computing base

Small components – easy to validate

Customizability

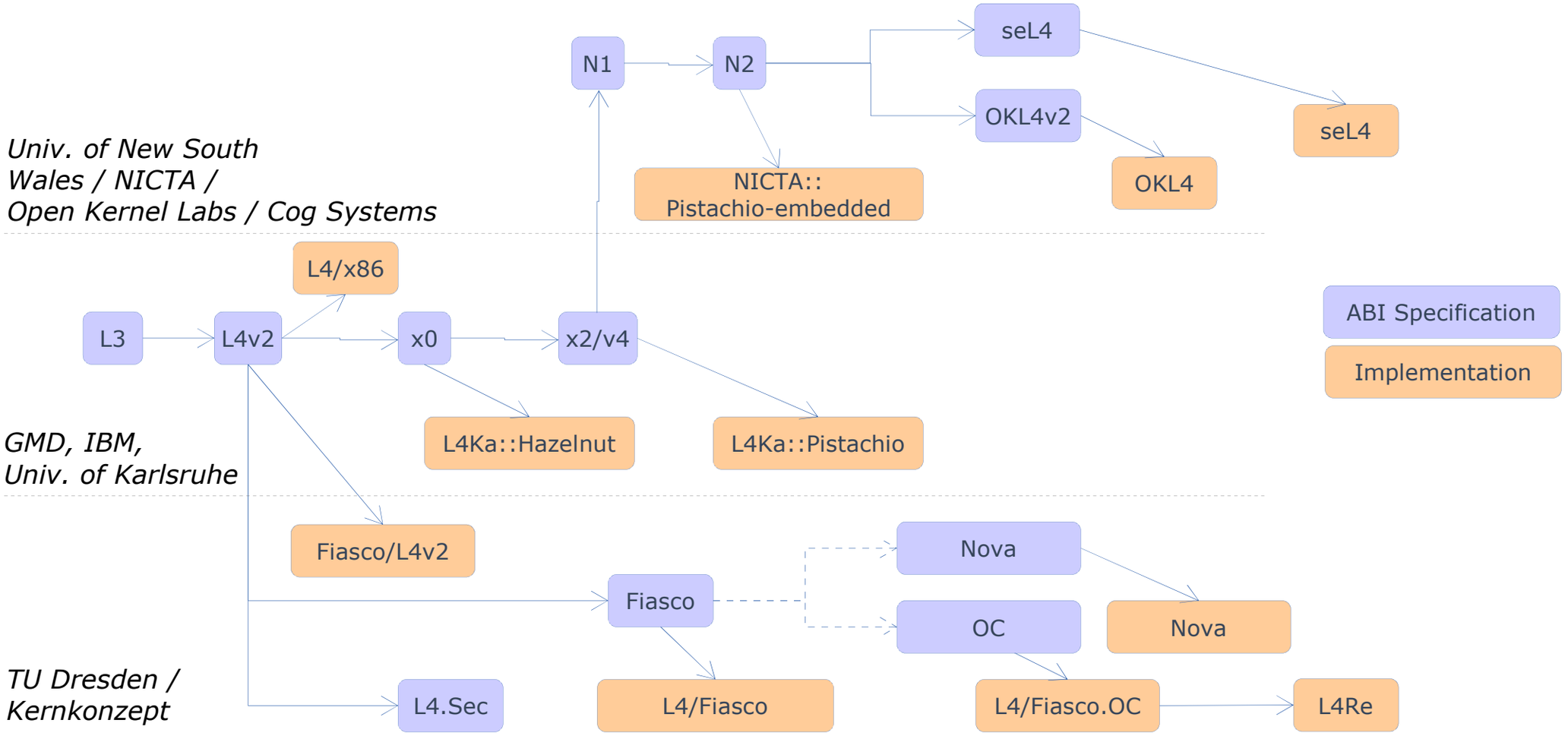
All OS services as user-level processes

Well-defined interfaces

Multi-personality OSes

Flexibility / Extensibility

# L4 Microkernel Family History



# L4Re Origins and Roadmap

TU Dresden: since 1997

**Before: Academic research in virtualization / real-time / security**

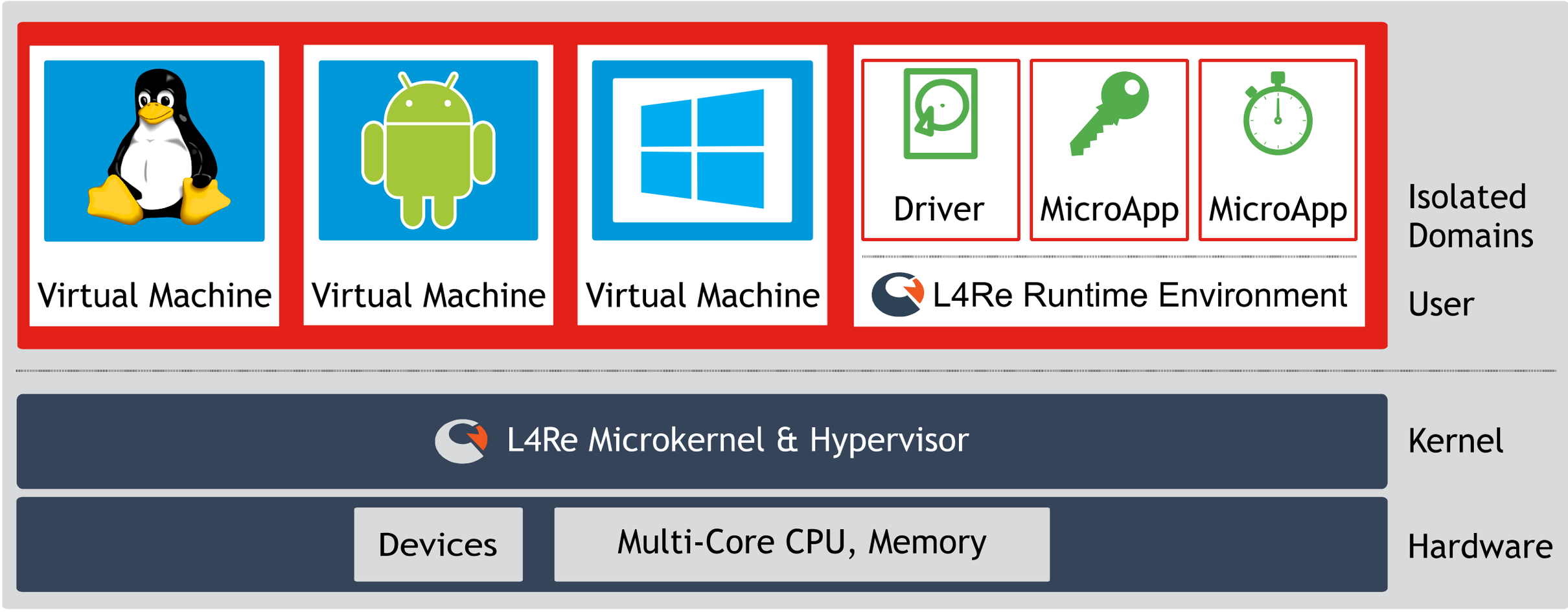
Kernkonzept: since 2012

**Now: Security – consulting / BSI approvals / certification**

**Next: Automotive - certification / product**

**After: Industry safety - certification / product**

# L4Re Operating System and Hypervisor




ARM/x86/MIPS, 32/64 bit, full/para-virtualization, dynamic/static, strong isolation, real-time, untrusted VMM, native microapps, POSIX subset, open source, mature

# Noteworthy L4Re features: Isolation

**Capabilities as references to kernel (and user-land) objects**

Provides information hiding (local naming) and access control

Enables reasoning about isolation and freedom from interference

- No capability to shared object → no way to communicate/interfere

**Designed to even allow preventing sharing 2nd-class kernel objects (allocators …) and invisible architectural state**

Not 100 % there yet

# Noteworthy L4Re features: Real time

**Real-time per-CPU scheduler: Fixed priority round robin**

WFQ (non-RT) also available

Cross-CPU thread/VCPU migration supported

Support for thread-group budget scheduling planned

**Short critical sections w/ IRQs off, preemption points**

**Fine-granular wait-free locking**

Excellent interrupt-response times

**No cross-CPU shared state in critical paths, no big kernel lock**

Excellent scalability

# Noteworthy L4Re features: Virtualization

## Hardware-assisted virtualization

Untrusted (user-level) virtual-machine monitors (VMMs) for platform emulation

- uvmm: Tiny VMM for Linux guests. Upstream ARM Linux “just works”
- l4-kvm: Uses Qemu/KVM in a Linux guest to provide platform for Windows guests (x86 only)

## Also available: Paravirtualization with L4Linux

A user-mode Linux kernel running on L4Re

# Noteworthy L4Re features: Microapps

**Microapps: Native L4Re applications**

Small TCB: no dependency on any rich OS, no Dom0

No dependency on VMM

no virtualization overhead

**POSIX subset for microapps: L4Re Runtime Environment**

Supports libc, C++ library, pthreads, etc.

Natural extension of kernel API with useful OS abstractions

- e. g. for address-space management

# Noteworthy L4Re features: I/O virtualization

**Device pass-through to VMs or driver microapps**

DMA security via IOMMU

**Native drivers and multiplexing for various buses and devices**

PCI, serial console, AHCI, framebuffer

**Virtual networking among VMs supported**

Virtual Ethernet switch or p2p connection

Virtual socket connections

**Virtio supported**

# Open Source - where to get L4Re

Superior trust - nothing up our sleves

Low barrier to entry

Go to www.kernkonzept.com/download.html

Or www.l4re.org

Snapshots / SVN

Early access via GitHub

# Licensing and development model

**(Mostly) GPL version 2**

**Commercial licenses: Dual licensing capability**

Require CLA for contributions

Essential for attracting investments needed for certification

Also, a customer requirement in Automotive

**Kernkonzept serves as maintainer & gatekeeper for contributions**

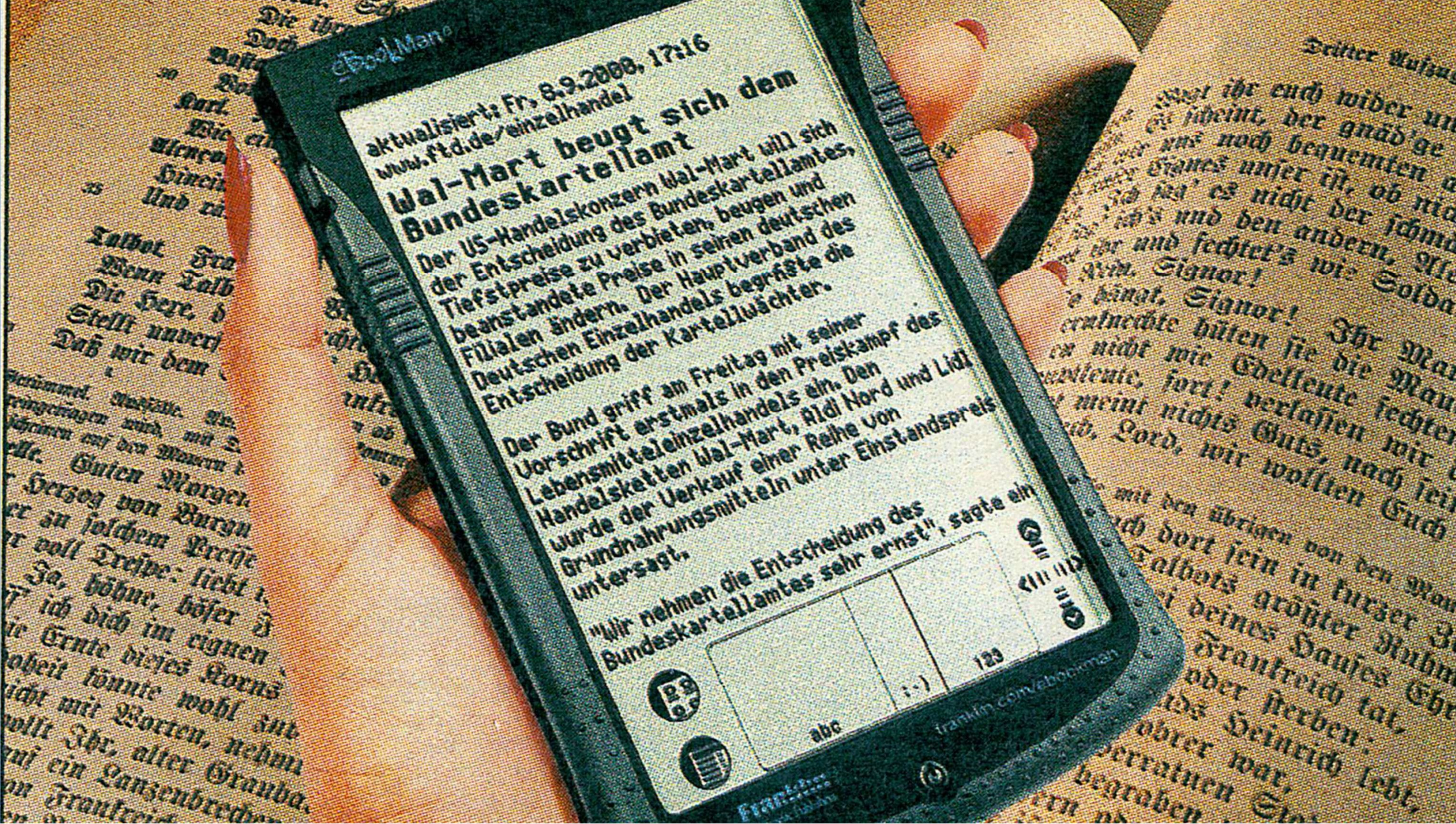
Required for quality and integrity management

Precondition for certification

KERNKONZEPT

# L4Re use cases today

MICROKERNEL MADE IN GERMANY


BookMan
aktualisiert: Fr, 8.9.2006, 17:16
www.ftd.de/einzelhandel
Wal-Mart beugt sich dem Bundeskartellamt
Der US-Handelskonzern Wal-Mart will sich der Entscheidung des Bundeskartellamtes, Tiefstpreise zu verbieten, beugen und beanstandete Preise in seinen deutschen Filialen ändern. Der Hauptverband des Deutschen Einzelhandels begrüßte die Entscheidung der Kartellwächter.
Der Bund griff am Freitag mit seiner Vorschrift erstmals in den Preiskampf des Lebensmitteleinzelhandels ein. Den Handelsketten Wal-Mart, Aldi Nord und Lidl wurde der Verkauf einer Reihe von Grundnahrungsmitteln unter Einstandspreis untersagt.
"Wir nehmen die Entscheidung des Bundeskartellamtes sehr ernst", sagte ein
abc
123
frankfurter


SAMSUNG
10:54
Donnerstag, 23. Februar
HEUTE
13:00 –14:00 La Pausa
Mittagessen mit Herr Sander
16:30 –17:30 Raum 203
Telko (Frau Horst, Margit, Frank)
MORGEN
09:00 – 10:00 Raum 210
Jour Fixe
13:30 –14:30 Terminal 2
Flug nach Stuttgart
Telefon
Kontakte
Apps
Nachrichten
E-Mail
0:54 Do, 23. Februar
work
life
Update
Simko Update verfügbar
Sicherheitshinweis
Passwort seit 6 Monaten
nicht erneuert
10:47 Do, 23. Februar
life
Anruf
Julia – 2 Minuten
Nachricht
Julia – 5 Minuten
Angry Birds
Maps
SAMSUNG
10:07
Google
Play Store
Angry Birds
Maps

genua

Security first.

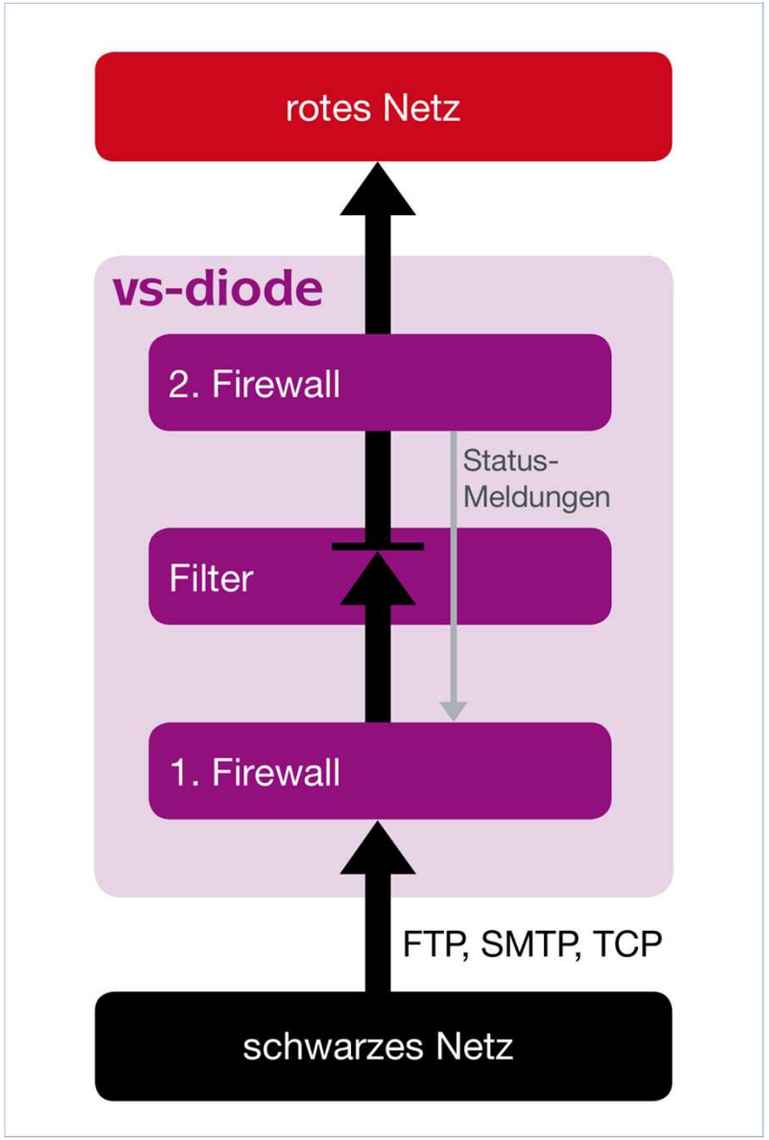
# Security Laptop vs-top

## Providing High Security Access for Mobile Users Connecting to Classified Networks

Employees on the road frequently must connect to their company network to access and modify data, use internal applications online etc. In addition, easy connections via all sorts of protocols and methods are needed. These user requirements raise a very important question indeed: How can reliable IT security be implemented for teleworking? Very serious security issues need to be addressed, such as the download of sensitive data to employee laptops via the Internet, as well as access to your LAN and all sorts of confidential information. It is therefore essential that third parties cannot read or manipulate the data being transferred, nor misuse access to your LAN.

### Simple to Operate

The vs-top security laptop ensures that mobile personnel


MICROKERNEL MADE IN GERMANY

HIGH

SDoT®
SecureDomainTransition

SDoT® Workstation

SDoT® Security Gateway 6.0

SDoT® Adminstation

Firewall
*(optional)*

LOW

KERNKONZEPT

# Use cases - in development

# EB corbos Hypervisor

Elektrobit

# Automotive use cases for hypervisors

**ECU consolidation**

IVI-Cluster integration

- Please visit our demo: 2 × AGL on L4Re

**ADAS**

Integration of complex components

- machine learning, deep neural networks, hardware accelerators

**Gateway**

Integration of network stacks and hardware

# L4Re for Automotive

**Upcoming: ISO26262 ASIL-D certification as a SEooC**

ASIL is a hard requirement for high-volume markets

**Licensing model**

Code still developed as open source

But certification docs / some tests / QA tools remain proprietary

Sponsor gets exclusive commercial relicensing rights for automotive market

Kernkonzept retains commercial exploitation rights for other markets

# Automotive partnership with Elektrobit

**Tier1 software supplier buy-in**

**OEMs can buy from trusted source**

Tier1 partner assumes most risks, covers liability & indemnification

Closed source

**Open Source benefits**

Start R&D now from community version, buy certified version later

# L4Re for High-Assurance Security

**Upcoming: Common Criteria EAL4+ certification**

Not a precondition for BSI application approvals, but speeds things up

For new applications that require a trusted platform

**Licensing model**

Code still developed as open source

But certification docs / some tests / QA tools remain proprietary

Sponsor gets exclusive commercial relicensing rights for gov. market

Kernkonzept retains commercial exploitation rights for other markets

# L4Re for Industrial Safety

**Planned: IEC61508 SIL-3 certification**

A hard requirement for hypervisors in industrial functional safety

**Licensing model**

Code still developed as open source

But certification docs / some tests / QA tools remain proprietary

Sponsorship / licensing not finalized yet

**Now soliciting requirements and partners**

# Certification considerations

**L4Re open-source code base, plus:**

Product considerations: Definition of functional scope and properties

Requirements tracking

Static analysis and testing: Test suite, testing infrastructure

Tool qualification

Technical documentation: Specification, design, user guidance

Quality management: QA, processes for: business security, flaw resolution, code integrity, supplier management, …

# Community/commercial opportunities

**Certification partnerships**

Functional safety

**Open-source-community development**

Managing contributions, visibility, PR

**Usability**

Developer experience, documentation

**Security hardening**

Even better isolation for new attacker models

Formal methods, static analysis

# Formal methods

**Complete formal verification: Infeasible for L4Re today**

Tradeoffs re: installed base, features, flexibility

**But we can reap the low-hanging fruit**

Ex.: Formal specification, proof of isolation, model-based testing, automatic test-case generation, model checking for critical components

**Work on acceptance problem**

Develop a “language” to enable certification labs / users to trust formal methods

# Summary: Why L4Re for automotive functional safety?

Open Source

Mature, high-quality implementation, rich feature set

Commercial licensing / liability coverage available

Kernkonzept covers QM / development process requirements

Unique business model that attracts the investment needed for certification

**Please visit our demo at the Kernkonzept/Elektrobit booth!**

KERNKONZEPT

# Thank you!

www.kernkonzept.com

MICROKERNEL MADE IN GERMANY

KERNKONZEPT

# Backup

www.kernkonzept.com

MICROKERNEL MADE IN GERMANY

KERNKONZEPT

# Research directions

MICROKERNEL MADE IN GERMANY

# Further directions for L4Re

**Versatility: An OS core for a plethora of use cases**

Multi-tenant devices: Home gateways, smart-meter gateways, 5G base stations

Mixed-criticality systems; manageability

**Explore and support new hardware technologies**

Memory technologies (NVM); security technologies

**Scalability**

Manycore systems; HPC; heterogeneous systems; microcontrollers