Sichere Open-Source-Software – Wie geht das?

Katrin Kahle, Hendrik Tews, **Matthias Lange** - Kernkonzept,
Michael Vogel - atsec information security,
23.05.2023

DAS L4Re OPEN SOURCE SOFTWARE PROJEKT UND KERNKONZEPT

01

L4Re Operating System Framework

- L4Re Operating System Framework – modularer Baukasten für individuelle mikrokernbasierte Betriebssysteme und Virtualisierungslösungen
- L4Re (und Vorläufer) seit 1997 an der TU Dresden als OSS entwickelt; anfangs mit Echtzeit-Orientierung
- Ab 2005 inhaltlicher Wechsel des Forschungsparadigmas zu IT-Sicherheit – Einführung der Object Capabilities
  - Basis für Zero Trust und Security by Design

Kernkonzept

- Vom Open-Source-Software-Projekt zur Gründung von Kernkonzept 2012
  - Von den beiden Maintainern Adam Lackorzynski und Alexander Warg
- Kernkonzept wird als juristische Person sicherer Maintainer und Gatekeeper um Qualität, Ansprechbarkeit und Zuverlässigkeit für Kunden aus der Industrie zu erfüllen (Kontrollierbarkeit)

Kernkonzept

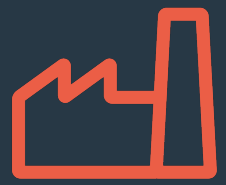
- Vision bei der Gründung von Kernkonzept: Ein sicheres und verfügbares Betriebssystem für Deutschland und Europa (Souveränität)

- Entscheidung: L4Re bleibt Open Source
  - OSS-Strategie für maximale Transparenz und Souveränität
  - Kernkonzept verwendet selbst zu 95 % Open-Source-Software

Adressierte Märkte

AUTO-
MOTIVE

HIGH
ASSURANCE



CYBER
SECURITY

SECURE
ENDPOINT

SMART
HOME

SECURE
CLOUD

INDUSTRIAL
IOT

AVIONICS

L4Re ist die sichere Basis von Produkten, die diese Labels bereits erreicht haben:

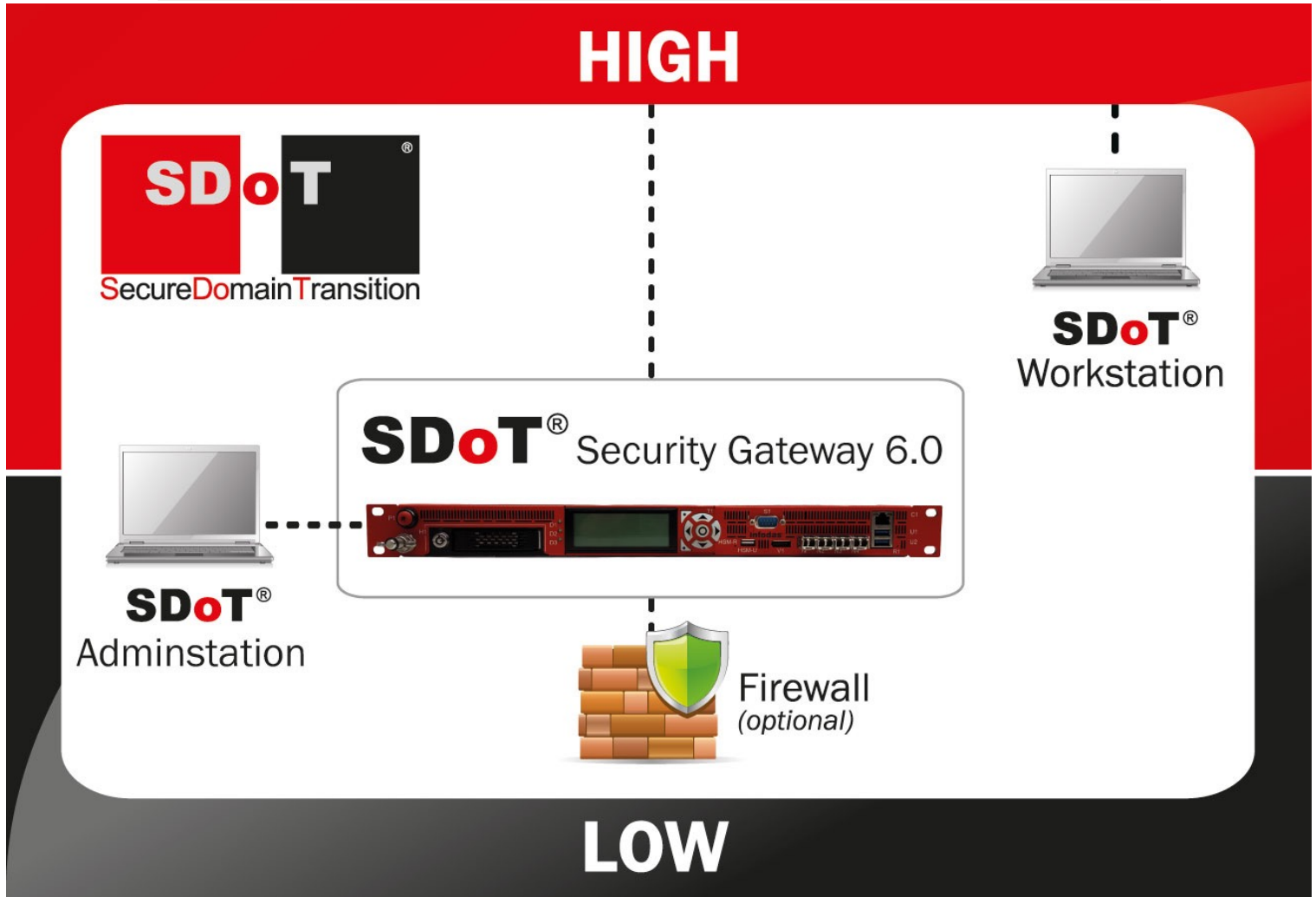
GERMAN
SECRET

EU
SECRET

NATO
SECRET

infodas

connect more. be secure.



genua.

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

EB corbos Hypervisor

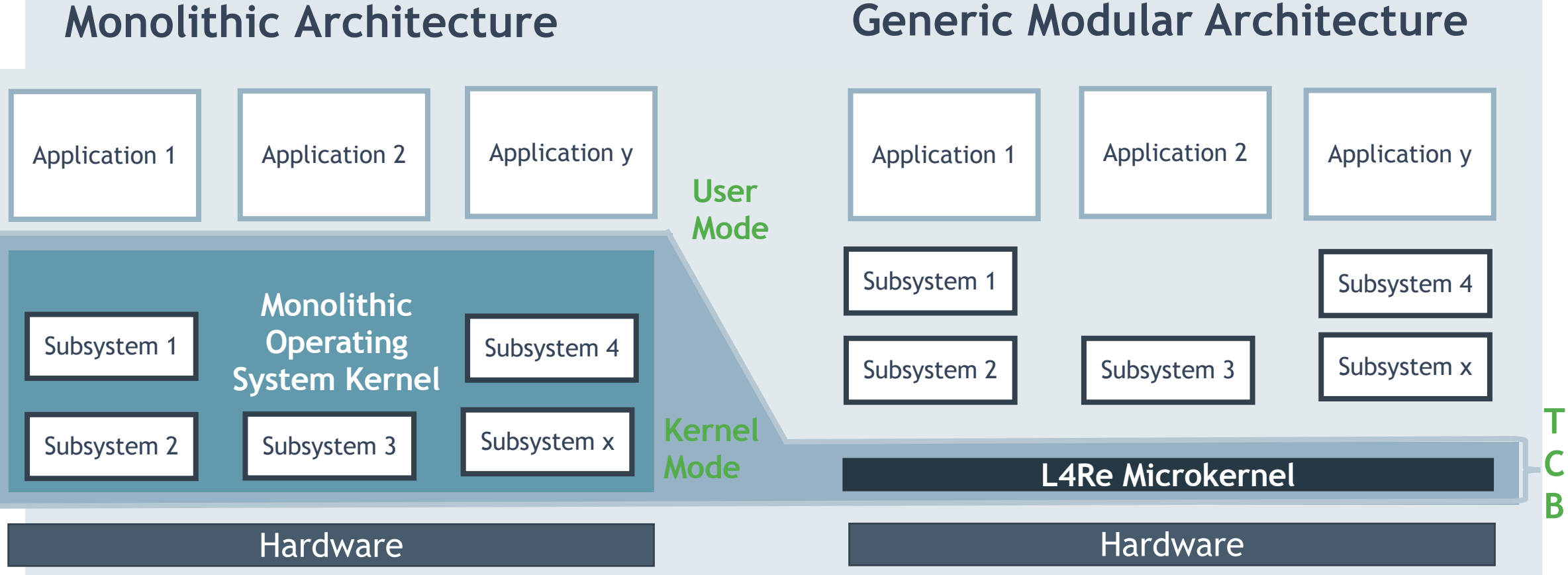

Electrolux

WARUM ENTSCHEIDEN SICH KUNDEN FÜR L4Re? Warum halten Sie es für eine sichere OSS?

04

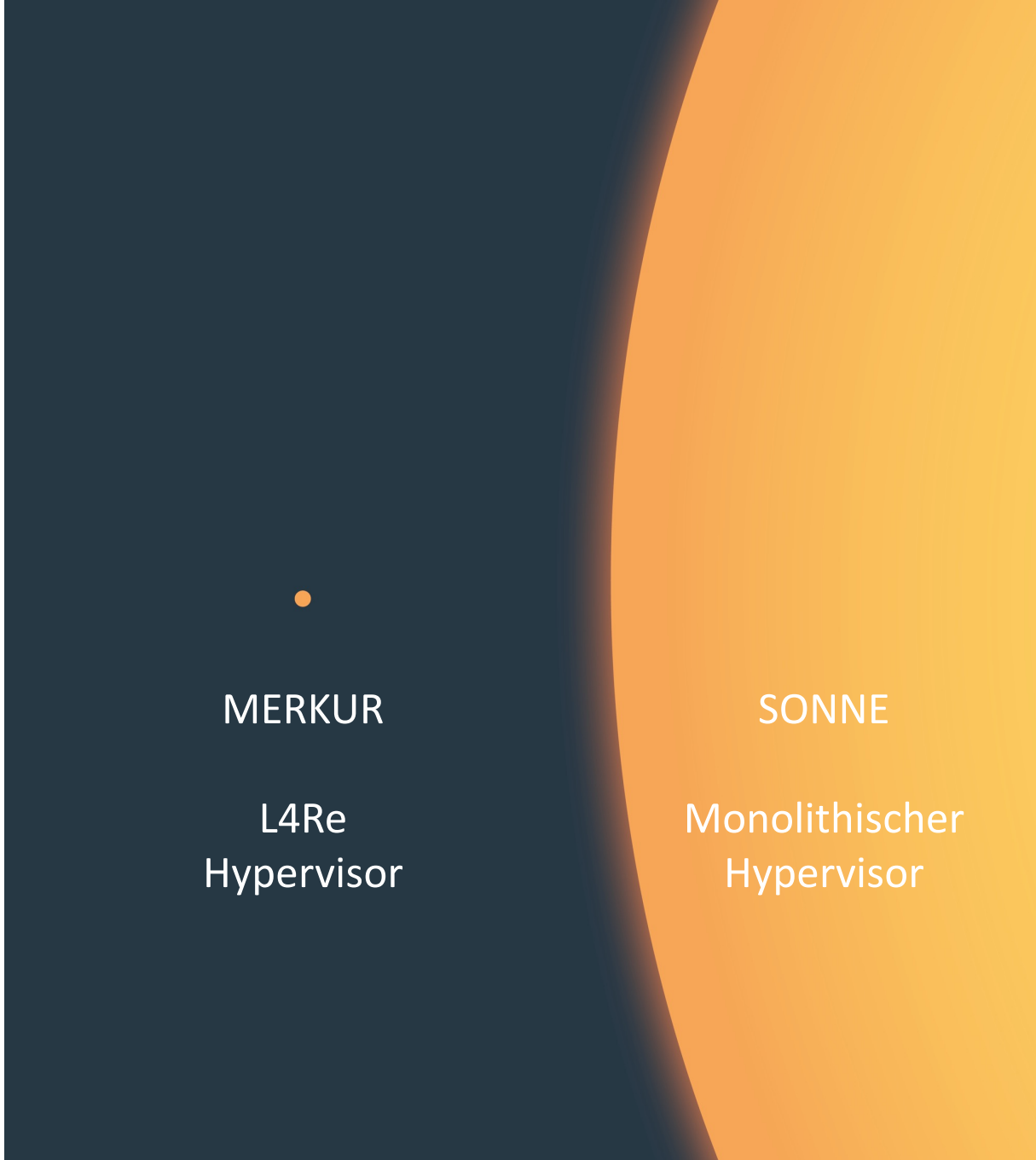
1. FUNKTIONALITÄT

Trusted Computing Base



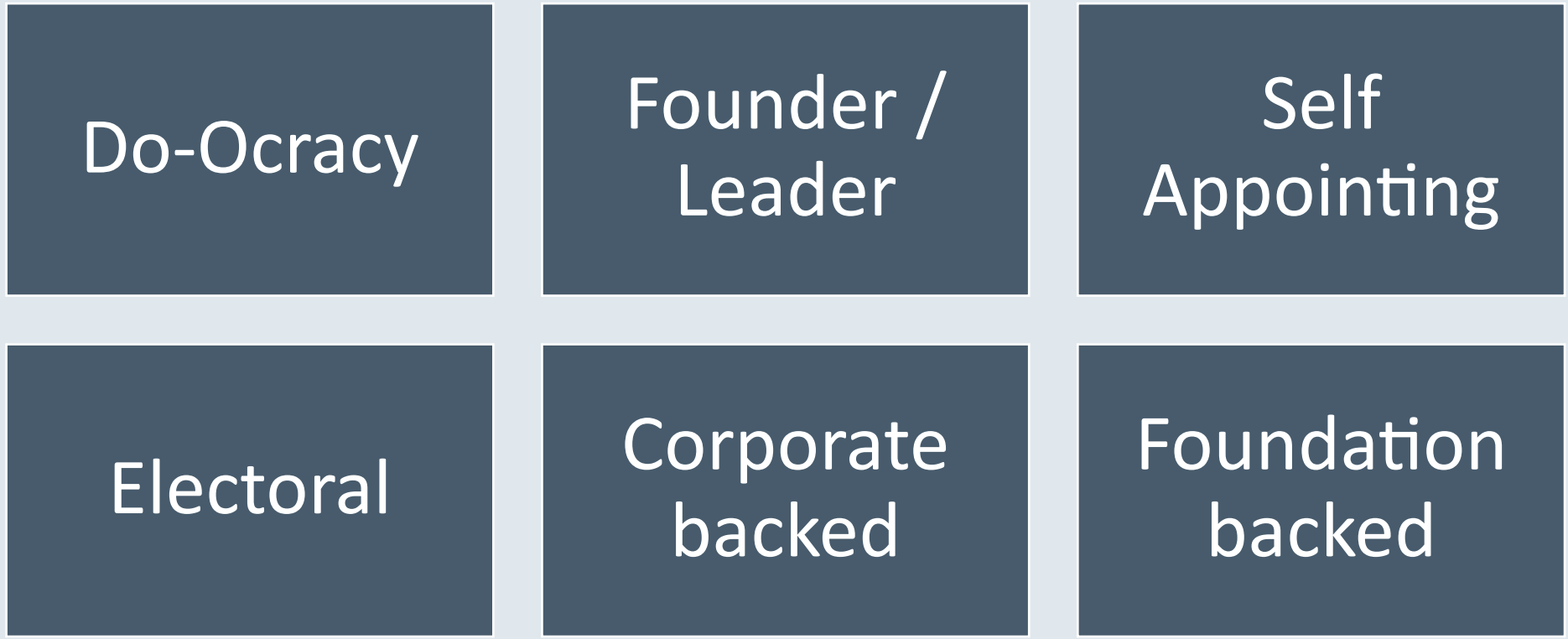
TCBs im Vergleich

- Verhältnis von 30.000 Zeilen Code zu vielen > 10.000.000 Zeilen Code (z.B. Linux)
- Code der TCB muss geprüft werden
- Fehleranfällig: 7 Bugs je 1000 Lines of Code



2. GOVERNANCE MODELL ERMÖGLICHT VERTRAUEN

Governance-Modelle in Open Source



3. SICHERER ENTWICKLUNGSPROZESS

Sicherer Entwicklungsprozess

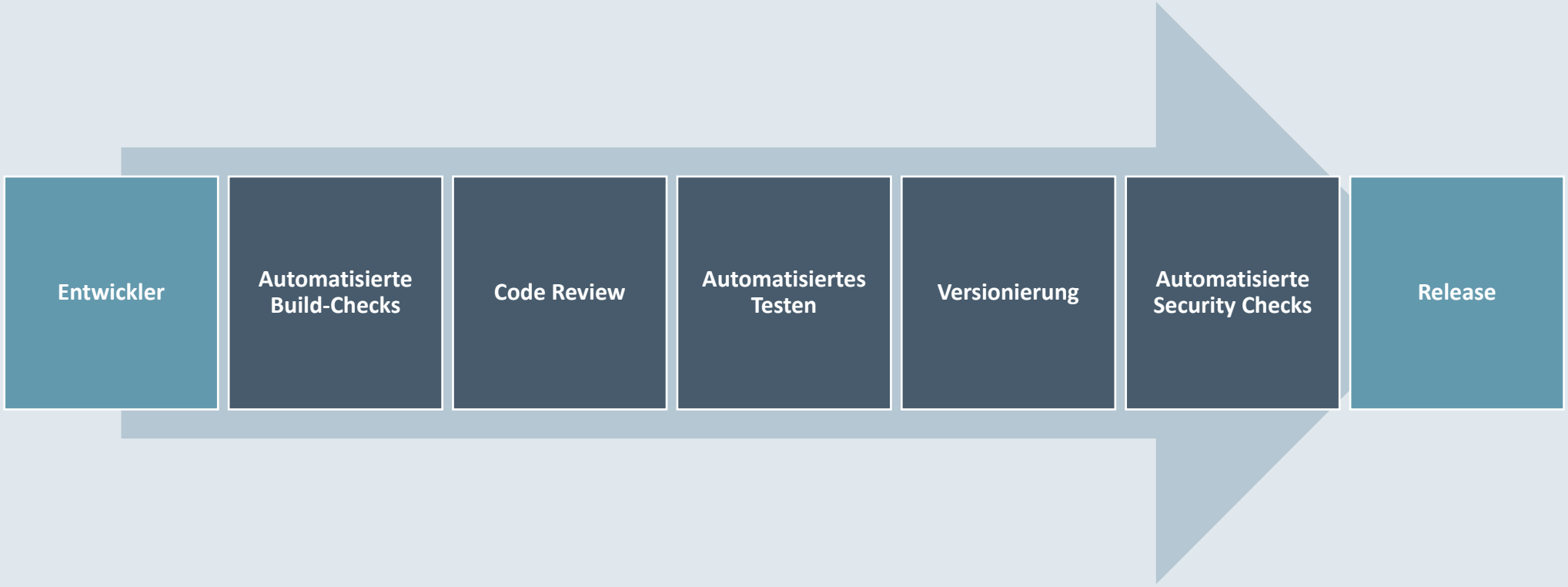
- Weil wir es mit einem sicheren Entwicklungsprozess entwickeln
  - Grundlagen bereits an der Uni gelegt (Versionierung, Build)
  - Bei Kernkonzept weiterentwickelt

- Starke Shift-left Orientierung
  - Probleme und Fehler so zeitig und zu so geringen Kosten wie möglich entdecken und beheben

```
commit 3752c0a6d43b2f0cce7376a6abe84b9f64b12af2
Author: Michael Hohmuth <hohmuth@os.inf.tu-dresden.de>
Date:   Wed Oct 29 17:41:10 1997 +0000

    kernel-internal virtual address space layout

commit a48adb0def49810dde278fbc9f00043535f8b9be
Author: Michael Hohmuth <hohmuth@os.inf.tu-dresden.de>
Date:   Wed Oct 29 17:41:28 1997 +0000

    kernel modularization

commit 6d1233a7786f78962c27dc8ef9badb4ee0d67370
Author: Michael Hohmuth <hohmuth@os.inf.tu-dresden.de>
Date:   Thu Oct 30 18:14:25 1997 +0000

    first version of interface

commit 0a73dc980d009ef0409338c90e8fedbc900d4711
Author: Michael Hohmuth <hohmuth@os.inf.tu-dresden.de>
Date:   Tue Nov 4 12:05:59 1997 +0000

    minor additions/fixes
:
```

Erster Commit für den heutigen L4Re Microkernel

Entwicklungsprozess bei Kernkonzept



WAS BEDEUTET DAS FÜR SICHERE OSS?

Sichere OSS

+ Governance
+ Softwareentwicklungs-prozess

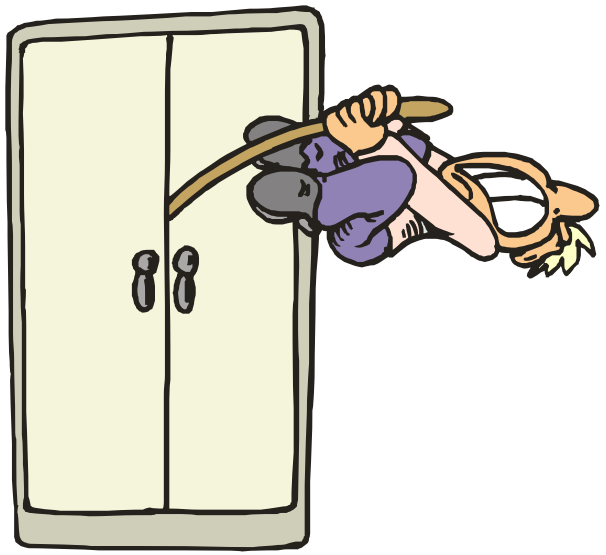
- Ist Testing von außen sichtbar / einsehbar?
- Artefakte wie Dokumentation
- SBOM

Motivation für Evaluierung

- L4Re Separation Kernel ist Plattform bei mehreren 'VS-zugelassenen' bzw. CC-zertifizierten Produkten.
- Relevante Anteile des L4Re Separation Kernels werden immer wieder bei Evaluierung von Produkten 'mit betrachtet'.
- Herstellernachweise zum L4Re kommen vom Produktentwickler.
- Eine potenzielle Schwachstelle im L4Re könnte Auswirkungen auf die Sicherheit einer ganzen Reihe verschiedener Produkte haben.
- **=> Dedizierte Evaluierung des L4Re durch unabhängige Prüfstelle zusammen mit dem Entwickler des L4Re.**

Durchführung der Evaluierung

- Erst-Evaluierung -> Hoher Aufwand für die Erstellung der Herstellernachweise
- Evaluierung ADV 'abgeschlossen' (Sicherheitsarchitektur, Funktionale Spezifikation, TOE Design – High Level Design, Low Level Design, Code Review)
- Testworkshop in Vorbereitung
- Derzeit Durchführung Schwachstellenanalyse
- 'Confidentiality'-Anforderung bei ALC_DVS -> Open-Source
- Kernkonzept ist alleiniger 'Maintainer' für den L4Re Main Branch -> Kontrolle über Release Versionen
- Funktionierender FLR-Prozess



Tieferer Einblick in den Evaluierungsprozess

- Schnittstellen-Evaluierung erfolgte nach entsprechenden Betriebssystem-Ansätzen
  - Systemrufe? Linux: 330 (x86) bzw. 290 (Arm64), L4Re Mikrokern: 1
  - Feinerer Ansatz: alle Schnittstellen des TOE aufgezählt und kategorisiert
    - 249 Schnittstellen, davon 61 SFR-relevant
- Ausserdem ausgehend von der Kernel Interrupt- und Exception-Vektortabelle alle erreichbaren Kernel-Code-Pfade evaluiert
- Design-Evaluierung umfasst Kern sowie L4Re Benutzerprogramme und Bibliotheken, die in der evaluierten Konfiguration laufen.
- Evaluator-Tests umfassen Analyse von Fehlerbehandlungen der Capability-Protokolle.
- => Einige Security Advisories als Ergebnis des Evaluierungsprozesses

Neuartigkeit: Evaluierung einer sog. Proxy-Spezifikation

- Gemeinsame Nutzung von Resourcen durch voneinander zu isolierende Kompartments (z.B. NVMe) benötigt Multiplexer (=Proxy) um Isolationseigenschaft zwischen den Kompartments durchzusetzen.
  - Im L4Re Betriebssystemframework meist mit Virtio implementiert
- Evaluation einer entsprechenden Proxy-Spezifikation und Dokumentation, dami Dritthersteller sichere Proxies schreiben können.

Ergebnisse für Kernkonzept (1)

- Dokumentation erstellt
  - HLD (~130 Seiten)
  - LLD (~400 Seiten)
  - 249 APIs vollständig in Doxygen als FSP dokumentiert
  - 101 Tickets wurden dabei erstellt
    - 23 davon haben echte Bugs aufgedeckt, davon 11 sicherheitskritisch
- Guidance (~50 Seiten)

Ergebnisse für Kernkonzept (2)

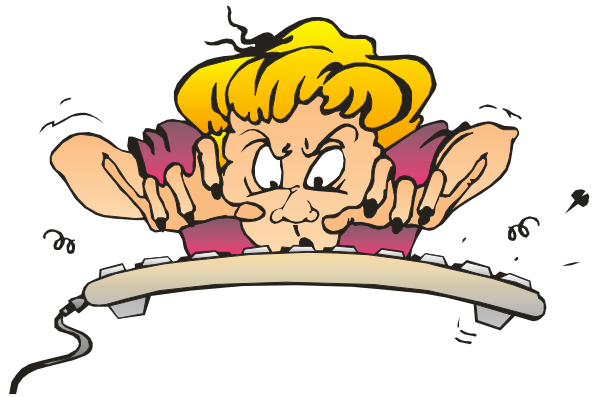
- Testing
  - 7351 Tests, 4247 relevant für TOE, +2123 Kernel-Unit-Tests
  - 1243 Tests zu SFRs verlinked
    - Jetzt wissen wir, dass die Tests vollständig sind
  - Testmatrix
  - Essential Tests: müssen immer erfolgreich sein
- Prozessdokumentation
  - Life cycle

Ergebnisse für Kernkonzept (3)

- Statische Code-Analyse im Rahmen einer Safety-Zertifizierung
  - Sehr viele false-positives (185 von 309) mussten manuell dokumentiert werden
  - Insgesamt 2 echte Fehler

Ergebnisse

- Unabhängige Analyse und Bewertung der Sicherheitseigenschaften des L4Re als Plattform mehrerer sicherheitskritischer Produkte
- Positiver Effekt durch Änderungen (Advisories), die sich aus der Evaluierung ergeben haben.
- Wiederverwendung der Ergebnisse für CC-Evaluierungen von Applikationen, welche das L4Re Betriebssystemframework als Plattform nutzen, in Diskussion (evtl. Composition)
- Wiederverwendung der Ergebnisse für Zulassungsprojekte in Diskussion



Fragen?

Quelle: https://www.pexels.com/de-de/foto/mann-der-braune-jacke-tragt-und-grauen-laptop-benutzt-874242/

Vielen Dank für Aufmerksamkeit!

Was wir tun:

- **Zulassungsunterstützung**
- **Common Criteria Evaluierungen**
- **Beratung zu Evaluierung, Zulassung, Herstellerqualifizierung, Validierungen, etc.**
- **FIPS140-3 Validierungen (atsec US)**
- **…**

Dr. Michael Vogel
atsec information security GmbH
Steinstr. 70
81667 München
mvogel@atsec.com