KERNKONZEPT

VOM UNI-OPEN-SOURCE PROJEKT ZUR HOCHSICHER ZERTIFIZIERTEN SOFTWARE

Katrin Kahle, Head of Product at Kernkonzept
Matthias Lange, Customer Engineer Specialist
Stefan Ropertz (BSI), Ingo Hahlen (BSI)

Vor 10 Jahren

+ **Die Drehstuhl-schnittstelle**

Bild: pexels-cottonbro-studio-8453810

Bild: Kernkonzept

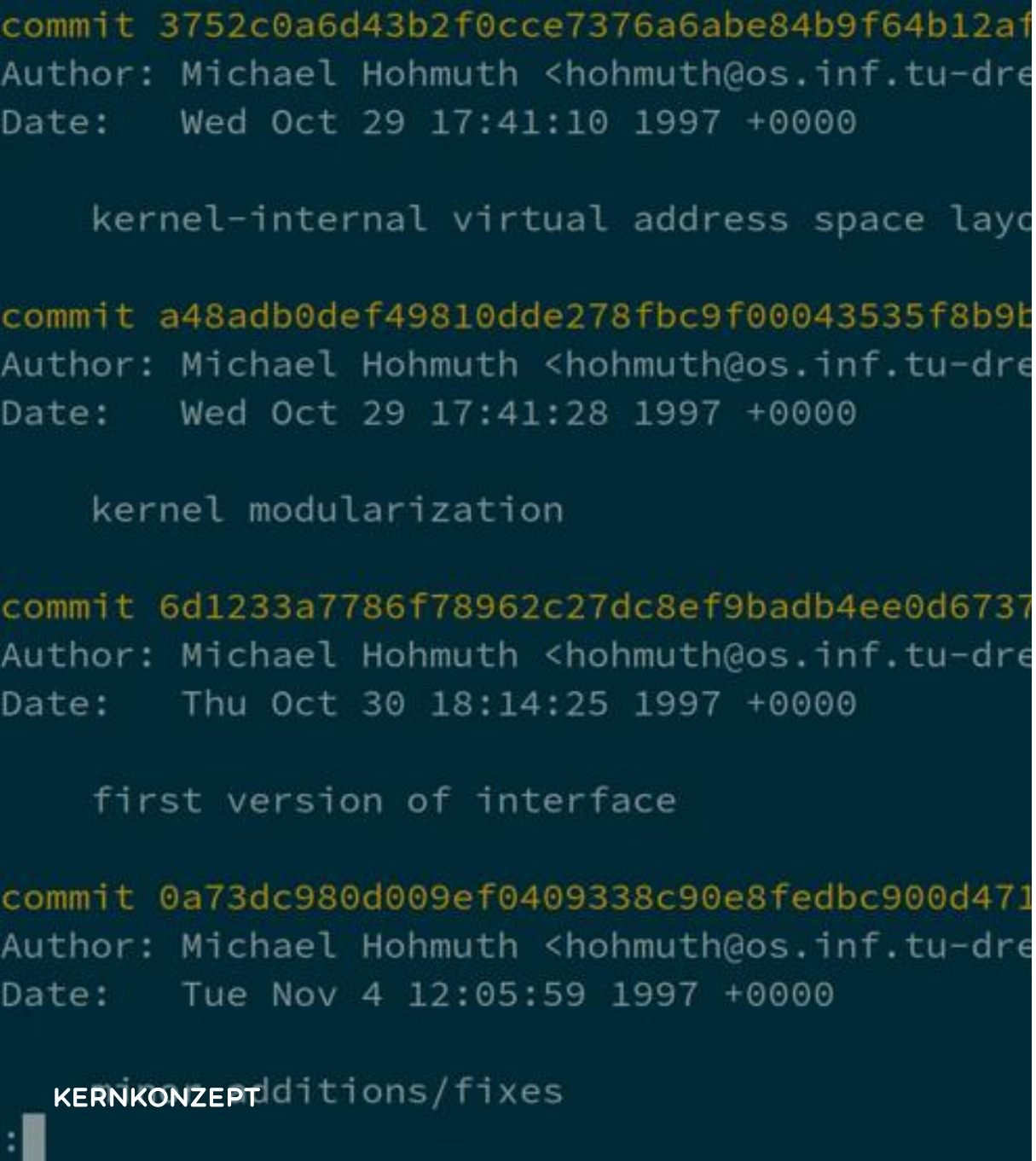
ENTSTEHUNG DES OSS-PROJEKTES AN DER TU DRESDEN

01

Vorgeschichte

- Jochen Liedtke
- L4 Mikrokern in Assembler – proprietär und zugleich Forschungswerkzeug
- “Fiasco”

Bild: https://de.wikipedia.org/wiki/Jochen_Liedtke#/media/Datei:Jochen_Liedtke.jpg
Adelheid Liedtke; CC BY 1.0

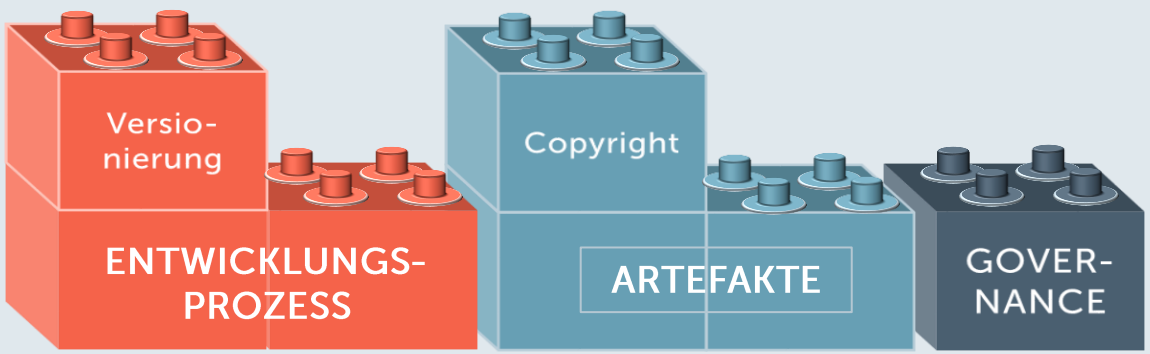


Geburtsstunde

- **1997: Start der Implementierung eines L4 Kerns an der TU Dresden**
- **In Hochsprache: C++**

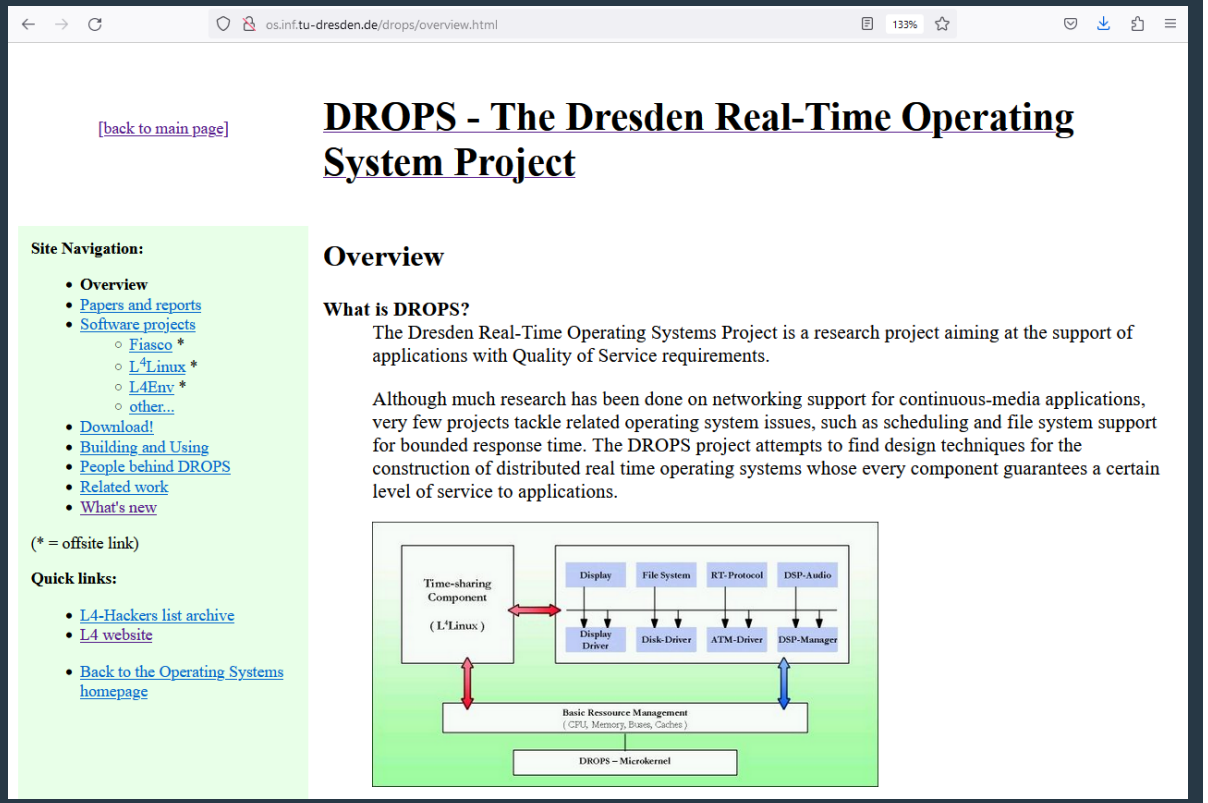
Bild: Screenshot Michael Hohmuth

NUR DURCH OPEN SOURCE GAB ES ÜBERHAUPT EINE WEITERENTWICKLUNG AN L4


Versio-
nierung
ENTWICKLUNGS-
PROZESS
Copyright
ARTEFAKTE
GOVER-
NANCE

ENTSTEHUNG VON OSS-PROJEKTEN UM L4 AN DER TU DRESDEN 1997 BIS 2005

02

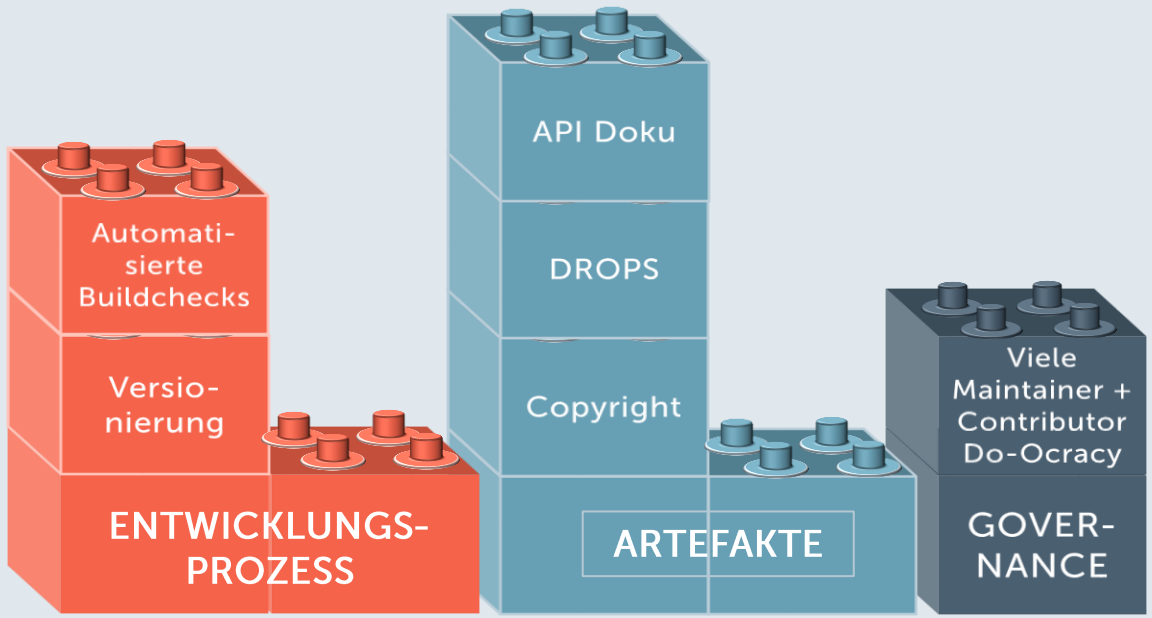


+ Do-Ocracy:

- Über 30 Personen entwickeln viele Komponenten – viele Maintainer

+ DROPS als OSS Distribution

+ Starkes Forschungskonzept

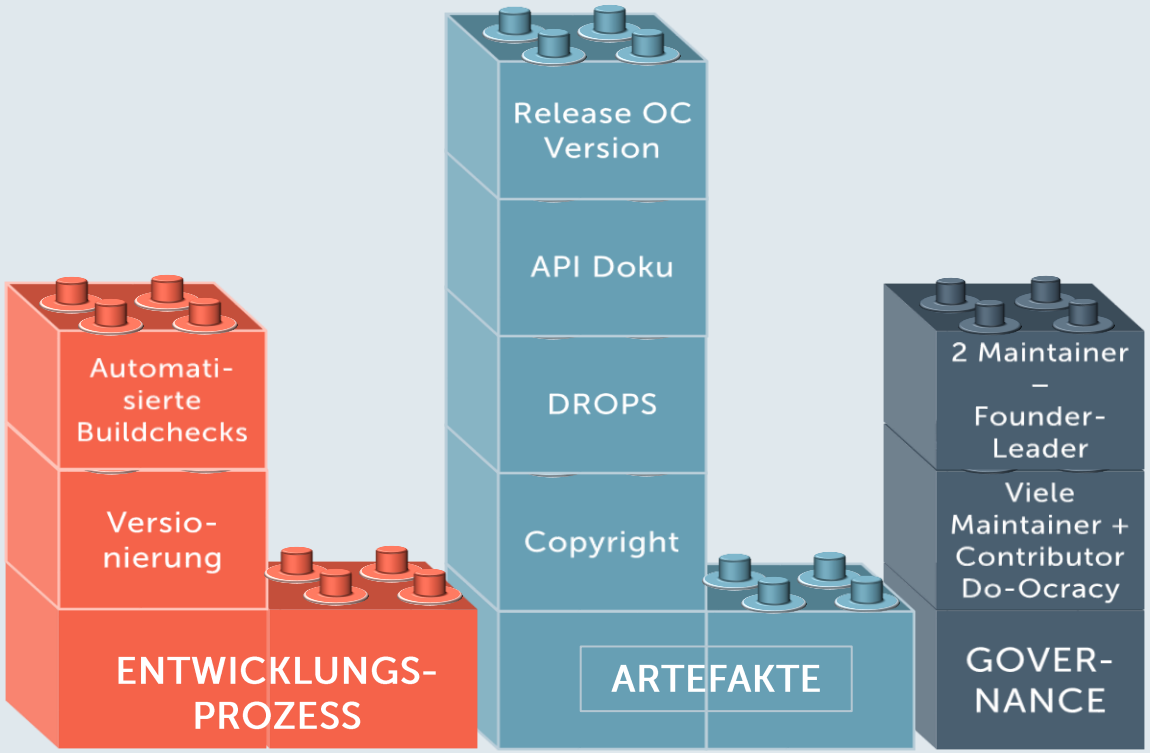

Automati-
sierte
Buildchecks
Versio-
nierung
ENTWICKLUNGS-
PROZESS
API Doku
DROPS
Copyright
ARTEFAKTE
Viele
Maintainer +
Contributor
Do-Ocracy
GOVER-
NANCE

NEUAUSRICHTUNG AUF SECURITY AB 2005

03

Security

+ **Mikrokerne für IT-Security**
+ **Access Control mit Object Capabilities**
+ **2010 Release der neuen Version**


Release OC Version
API Doku
DROPS
Copyright
Automati-sierte Buildchecks
Versio-nierung
ENTWICKLUNGS-PROZESS
ARTEFAKTE
2 Maintainer – Founder-Leader
Viele Maintainer + Contributor Do-Ocracy
GOVER-NANCE

PoC mit L4Re OSS mit TU Berlin und Telekom

COMPANY BACKING MUSS HER

04

2012 – Gründung der Kernkonzept GmbH

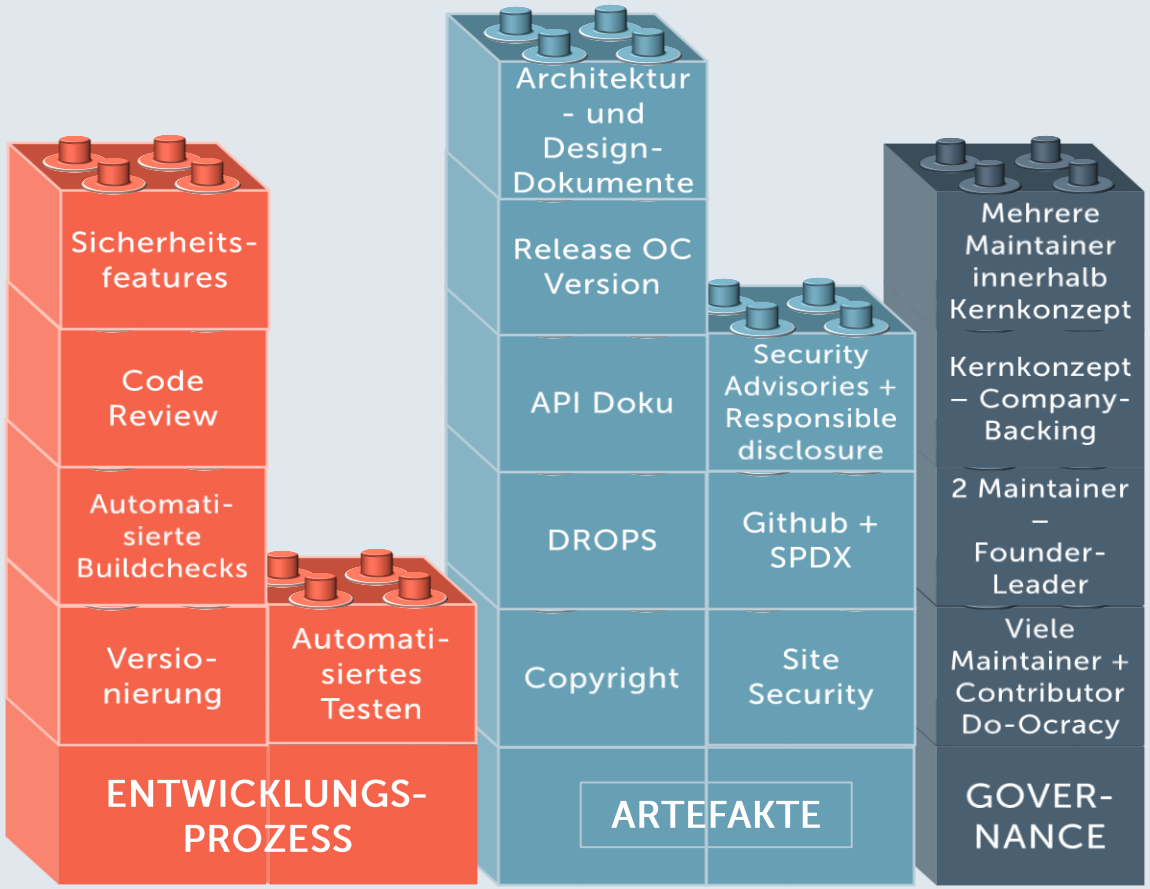
Foto: SiMKo 3


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
work
Update
Simko Update verfügbar
Sicherheitshinweis
Passwort seit 6 Monaten nicht erneuert
10:47 Do, 23. Februar
life
VS-
NfD
in
2013
SAMSUNG
10:07
Google
Angry Birds
Maps

WACHSTUM DER KERNKONZEPT & L4Re

- **Stabilisierung der Software und Artefakte**
- **Zulassung VS-Geheim als Teil einer sicheren Ablaufplattform**
- **Kernkonzept als Gatekeeper**

Bild: pexels-photomix-company-1002703


Sicherheits-features
Code Review
Automati-sierte Buildchecks
Versio-nierung
Automati-siertes Testen
ENTWICKLUNGS-PROZESS
Architektur - und Design-Dokumente
Release OC Version
API Doku
DROPS
Copyright
Security Advisories + Responsible disclosure
Github + SPDX
Site Security
ARTEFAKTE
Mehrere Maintainer innerhalb Kernkonzept
Kernkonzept – Company-Backing
2 Maintainer – Founder-Leader
Viele Maintainer + Contributor Do-Ocracy
GOVER-NANCE

AB 2018 – ENTSCHEIDUNG ZU EXTERNER EVALUATION VON L4RE

05

L4RE UND DAS BSI

Ingo Hahlen (BSI) und Stefan Ropertz (BSI)

06

L4Re im BSI

+ **L4Re ist in vielen zugelassenen Produkten im VS-Kontext im Einsatz**

+ **VS-Anforderungsprofil an Separation Kernel Betriebssysteme**
  - BSI möchte Verbesserung durch Abdeckung der Anforderungen
  - OS als sehr vertrauenswürdige Basis für hochsichere Produkte

+ **Breite Verwendung durch Contribution für OSS unterstützen**

Contribution des BSI zu evaluiertem L4Re

+ **BSI unterstützt Evaluierung inklusive Dokumentation**

+ **Evaluierung (bisher) erfolgreich mit Anleitung zur sicheren Integration, Bestätigung durch das BSI noch ausstehend**

Contribution des BSI zu evaluiertem L4Re

+ **Bestätigung der Vertrauenswürdigkeit soll zur Nutzung ermuntern**

+ **Maintainer durch Firma wichtig, da Lebenszyklus inclusive Patch-Management Teil der Vertrauenswürdigkeitsaussage**

ERGEBNISSE DES EVALUATIONSPROZESS

07

Ergebnis: Bessere Dokumentation

- + High Level Design (~130 Seiten)
- + Low Level Design (~400 Seiten)
- + 249 APIs vollständig in Doxygen als FSP dokumentiert

Bild: pexels-cottonbrostudio-4855324

Ergebnis: Software ist jetzt sicherer

- 101 Tickets angelegt
- 23 davon haben echte Bugs aufgedeckt, davon 11 sicherheitskritisch

Bild:pexels-sabrina-gelbart-249798

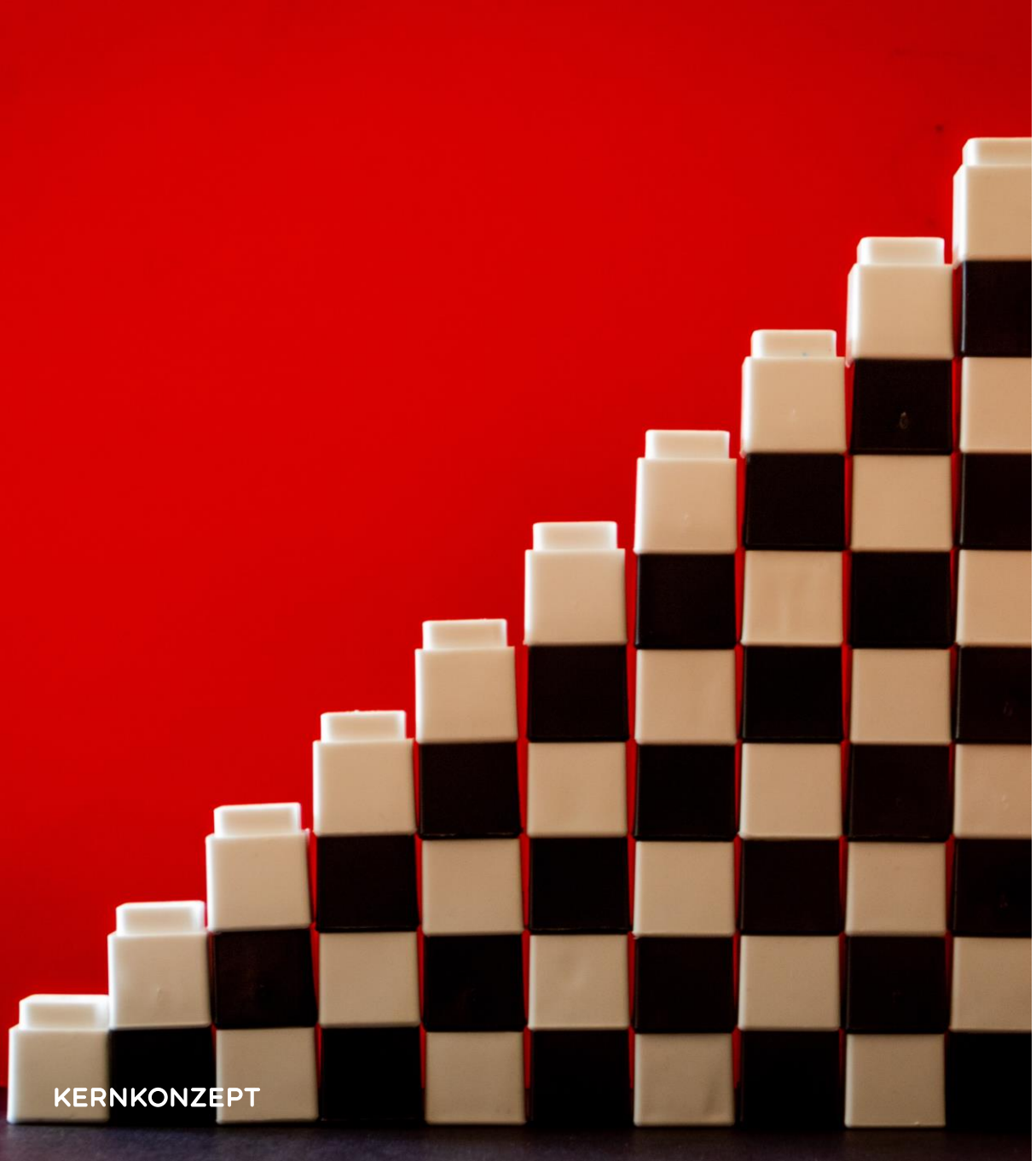
KERNKONZEPT

Ergebnis: Bessere Nutzbarkeit für User

+ **Mehr als 50 Seiten Guidance-Dokumentation**

+ **Prozessdoku-mentation: Life Cycle**

Bild: pexels-Tuesday-temptation-833317

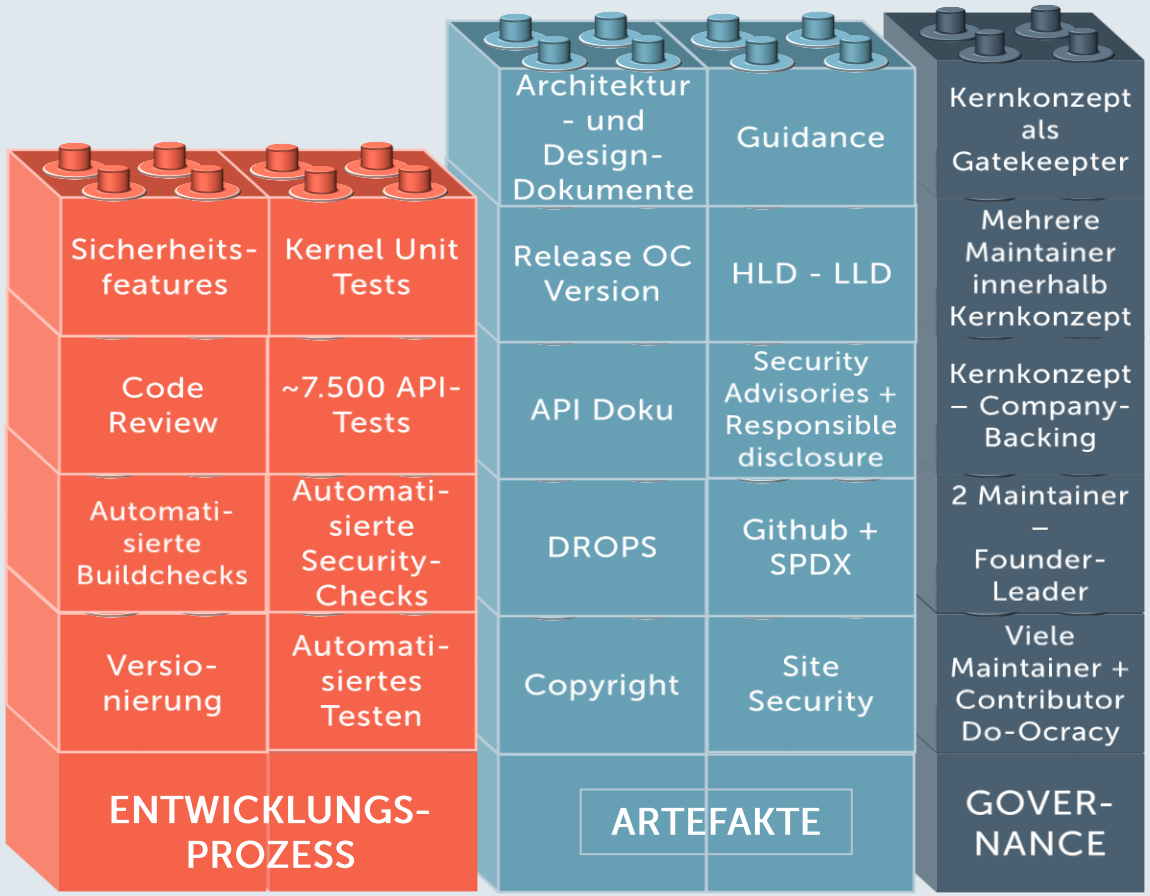


Ergebnis: Softwarequalität - Testing

+ 7351 Tests, 4247 relevant für TOE, +2123 Kernel-Unit-Tests

+ Tests jetzt vollständig zu allen Schnittstellen

Bild: pexels-magda-ehlers-1329328


Sicherheits-features
Kernel Unit Tests
Code Review
~7.500 API-Tests
Automati-sierte Buildchecks
Automati-sierte Security-Checks
Versio-nierung
Automati-siertes Testen
ENTWICKLUNGS-PROZESS
Architektur - und Design-Dokumente
Guidance
Release OC Version
HLD - LLD
API Doku
Security Advisories + Responsible disclosure
DROPS
Github + SPDX
Copyright
Site Security
ARTEFAKTE
Kernkonzept als Gatekeepter
Mehrere Maintainer innerhalb Kernkonzept
Kernkonzept – Company-Backing
2 Maintainer – Founder-Leader
Viele Maintainer + Contributor Do-Ocracy
GOVER-NANCE

FAZIT

08

Blick in die Zukunft

+ Positiv

- So viel gewonnen – viel mehr Artefakte
- Viele Fehler gefunden und behoben
- Für alle sicherer
- Produkte leichter zertifizierbar mit evaluiertem Operating System

+ Herausfordernd

- Security ist auch Aufwand
- Fortwährende Dokumentations- und Evaluierungsaufwände bei KK
- Wie wird es mit der Zahlungsbereitschaft aussehen?
- Community-Arbeit

KERNKONZEPT

VIELEN DANK!

MATTHIAS, KATRIN, INGO und STEFAN.