



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: Kernkonzept

THOMAS
KRENN

ENTSTEHUNG DES OSS- PROJEKTES AN DER TU DRESDEN

01



Vorgeschichte

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

```
commit 3752c0a6d43b2f0cce7376a6abe84b9f64b12af
Author: Michael Hohmuth <hohmuth@os.inf.tu-dre
Date:   Wed Oct 29 17:41:10 1997 +0000

    kernel-internal virtual address space layo

commit a48adb0def49810dde278fbc9f00043535f8b9b
Author: Michael Hohmuth <hohmuth@os.inf.tu-dre
Date:   Wed Oct 29 17:41:28 1997 +0000

    kernel modularization

commit 6d1233a7786f78962c27dc8ef9badb4ee0d6737
Author: Michael Hohmuth <hohmuth@os.inf.tu-dre
Date:   Thu Oct 30 18:14:25 1997 +0000

    first version of interface

commit 0a73dc980d009ef0409338c90e8fedbc900d471
Author: Michael Hohmuth <hohmuth@os.inf.tu-dre
Date:   Tue Nov 4 12:05:59 1997 +0000

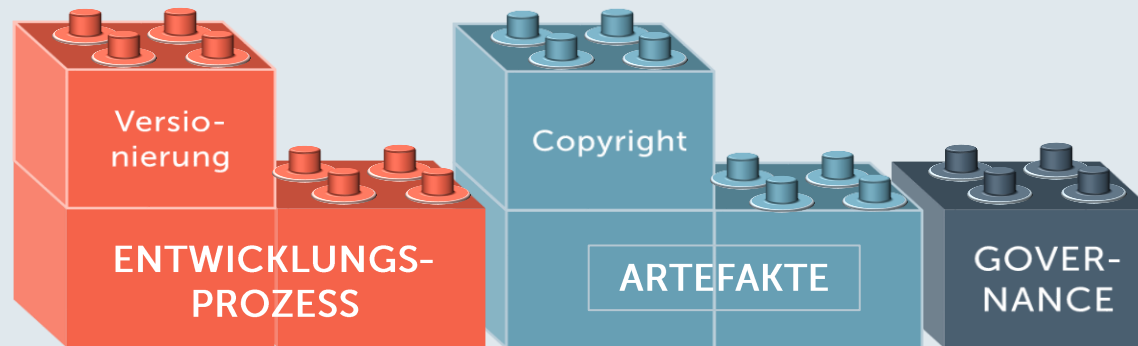
    additions/fixes
```

KERNKONZEPT

Geburtsstunde

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

**NUR DURCH
OPEN SOURCE GAB ES
ÜBERHAUPT EINE
WEITERENTWICKLUNG
AN L4**



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

← → ↺ os.inf.tu-dresden.de/drops/overview.html 133% ☆ ⌵ ⌵ ⌵ ⌵

[\[back to main page\]](#)

DROPS - The Dresden Real-Time Operating System Project

Overview

What is DROPS?

The Dresden Real-Time Operating Systems Project is a research project aiming at the support of applications with Quality of Service requirements.

Although much research has been done on networking support for continuous-media applications, very few projects tackle related operating system issues, such as scheduling and file system support for bounded response time. The DROPS project attempts to find design techniques for the construction of distributed real time operating systems whose every component guarantees a certain level of service to applications.

```
graph TD
    subgraph Applications
        TS[Time-sharing Component (L'Linux)]
        subgraph Drivers
            Display[Display]
            FS[File System]
            RT[RT-Protocol]
            DSP[DSP-Audio]
        end
        subgraph Drivers2
            DD[Display Driver]
            Disk[Disk-Driver]
            ATM[ATM-Driver]
            DSPM[DSP-Manager]
        end
    end
    TS <--> Drivers
    Drivers --> Drivers2
    Drivers2 <--> BRM[Basic Ressource Management (CPU, Memory, Buses, Caches)]
    BRM --> MK[DROPS - Microkernel]
```

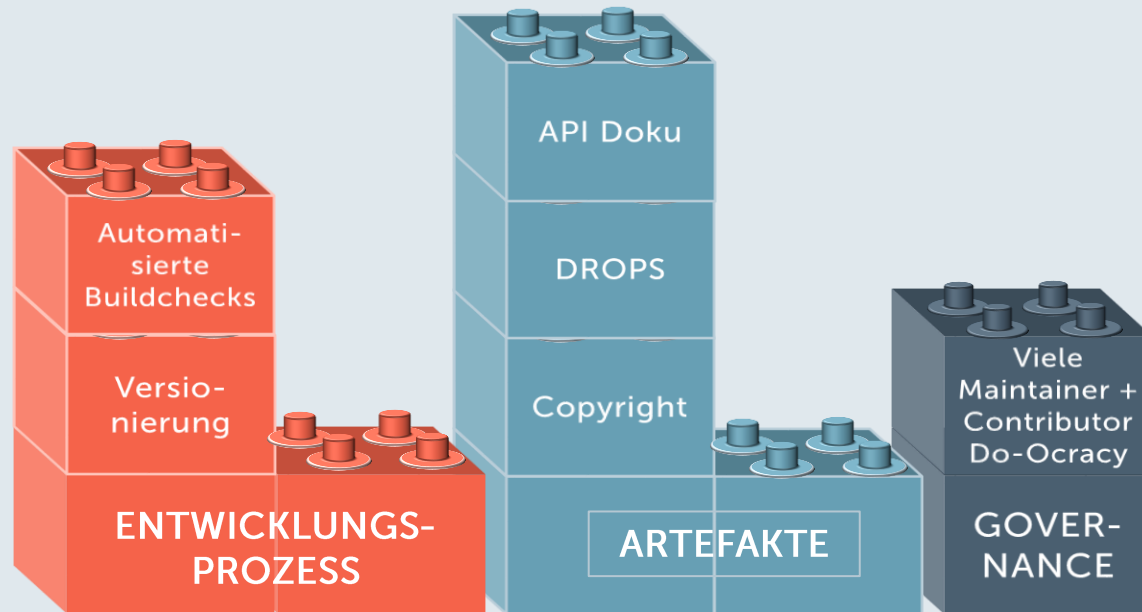
Site Navigation:

- [Overview](#)
- [Papers and reports](#)
- [Software projects](#)
 - [Fiasco](#)*
 - [L⁴Linux](#)*
 - [L4Env](#)*
 - [other...](#)
- [Download!](#)
- [Building and Using](#)
- [People behind DROPS](#)
- [Related work](#)
- [What's new](#)

(* = offsite link)

Quick links:

- [L4-Hackers list archive](#)
- [L4 website](#)
- [Back to the Operating Systems homepage](#)

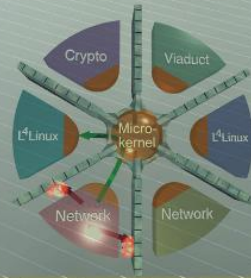
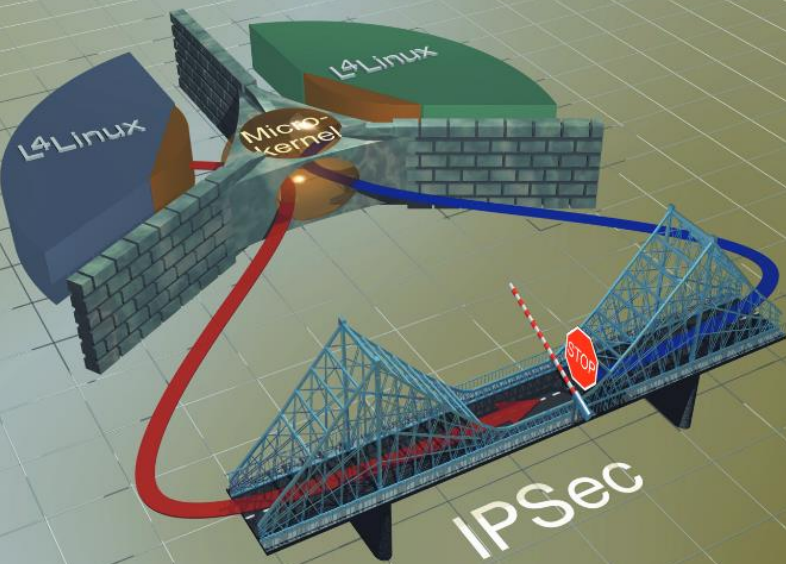


NEUAUSRICHTUNG AUF SECURITY AB 2005

03

Do you trust your
Operating System?

...we do not!



FEATURES

- Minimal-complexity microkernel in privileged mode
- Intercomponent communication via microkernel only
- Vulnerabilities locally restricted
- Increased reliability
- Reduced evaluation costs

APPLICATIONS

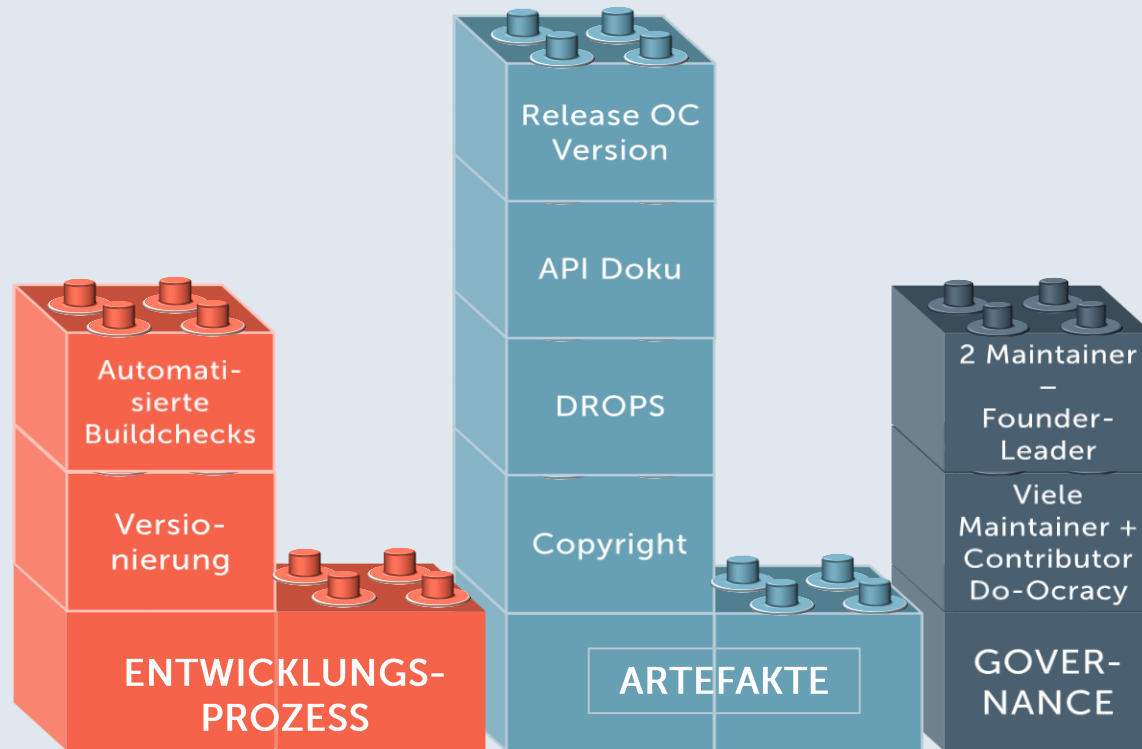
- Showcase implementation of a VPN gateway
- New platform for SINA (Secure Inter-Network Architecture)
- Protection of firewalls, routers, IDRS and web servers
- Trusted platforms

Security

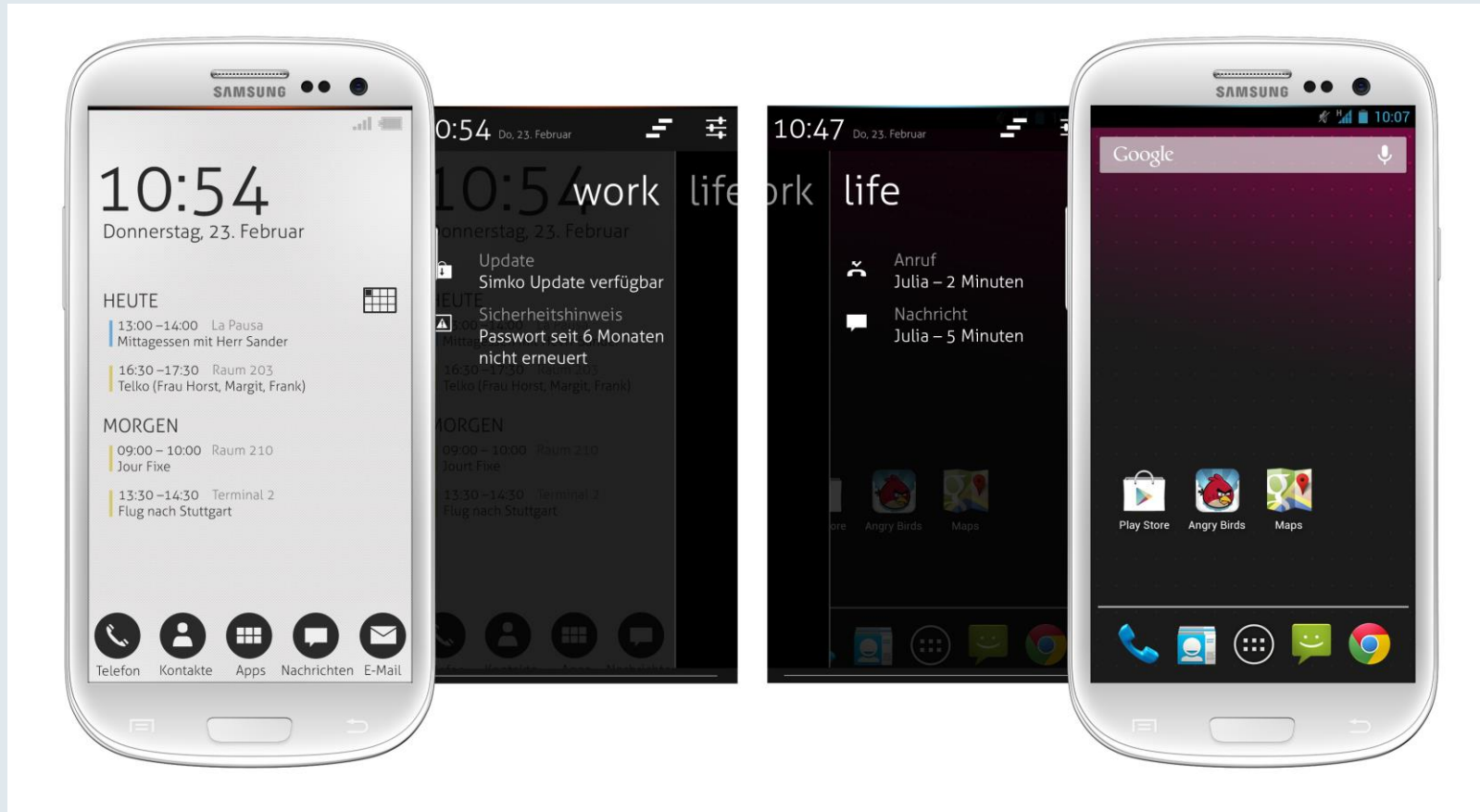
+ Mikrokerne für IT-Security

+ Access Control mit Object Capabilities

+ 2010 Release der neuen Version



PoC mit L4Re OSS mit TU Berlin und Telekom



**COMPANY BACKING
MUSS HER**

04



2012 – Gründung der Kernkonzept GmbH

Foto: SiMKo 3

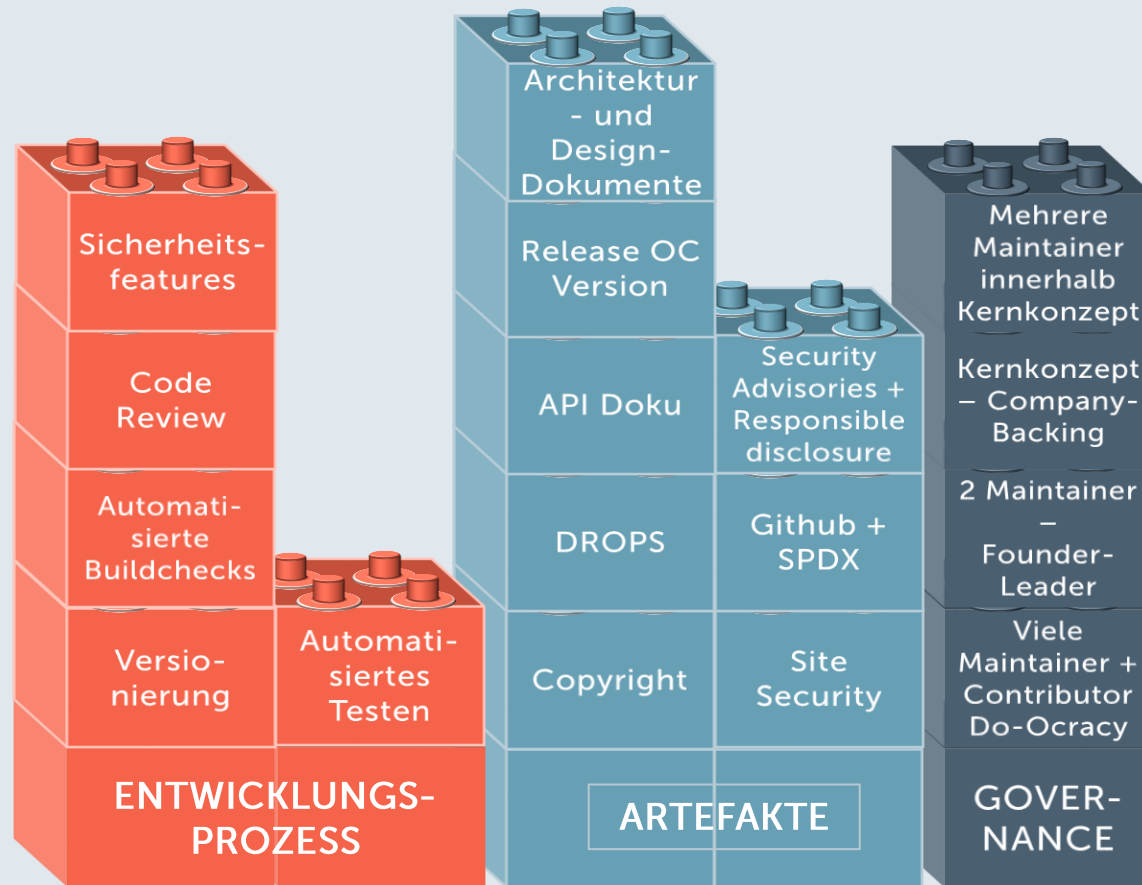




WACHSTUM DER KERNKONZEPT & L4Re

KERNKONZEPT

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



**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

A close-up, slightly angled view of a thick stack of books. The spines of the books are visible, showing various shades of cream and off-white. The stack is positioned on the left side of the frame, with the books fanned out slightly at the top.

Ergebnis: Bessere Dokumentation

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

```
+= "Text", r.resetText||n.data("resetText",n[i]()),n[i]||this.option
class(t).attr(t,t):n.removeClass(t).removeAttr(t)},0}},t.prototype.toggl
'buttons-radio"]');e&&e.find(".active").removeClass("active"),this.$elem
n=function(n){return this.each(function(){var r=e(this),i=r.data("butto
his,s)),n=="toggle"?i.toggle():n&&i.setState(n)}}},e.fn.button.defaults
fn.button.noConflict=function(){return e.fn.button=n,this},e(document).
function(t){var n=e(t.target);n.hasClass("btn")||(n=n.closest(".btn")),
t";var t=function(t,n){this.$element=e(t),this.$indicators=this.$elemen
pause=="hover"&&this.$element.on("mouseenter",e.proxy(this.pause,this))
le:function(t){return t||(this.paused=!1),this.interval&&clearInterval(
&(this.interval=setInterval(e.proxy(this.next,this),this.options.interv
s.$element.find(".item.active"),this.$items=this.$active.parent().child
)}{var n=this.getActiveIndex(),r=this;if(t>this.$items.length-1||t<0)ret
ction(){r.to(t)}:n==t?this.pause().cycle():this.slide(t>n?"next":"prev
ed=!0),this.$element.find(".next,.prev").length&&e.support.transition.
,this.cycle(!0)),clearInterval(this.interval),this.interval=null,this},
("next")},prev:function(){if(this.sliding)return;return this.slide("pre
tem.active"),i=n||r[t](),s=this.interval,o=t=="next"?left:right,u=t
pause(),i=i.length?i:this.$element.find(".item")[u](),f=e.Event("slide
return;this.$indicators.length&&(this.$indicators.find(".active").remov
=e(a.$indicators.children()[a.getActiveIndex()]));t&&t.addClass("active"
le")){this.$element.trigger(f);if(f.isDefaultPrevented())return;i.addCla
ment.one(e.support.transition.end,function(){i.removeClass([t,o].join("
].join(" ")),a.sliding=!1,setTimeout(function(){a.$element.trigger("sli
ted())return;r.removeClass("active"),i.addClass("active"),this.sliding=
this}};var n=e.fn.carousel,e.fn.carousel=function(n){return this.each(f
{}},e.fn.carousel.defaults,typeof n=="object"&&n),o=typeof n=="string"?n
mber"?i.to(n):o?i[o]():s.interval&&i.pause().cycle()})),e.fn.carousel.d
usel.Constructor=t,e.fn.carousel.noConflict=function(){return e.fn.caro
ta-slide],[data-slide-to],function(t){var n=e(this),r,i=e(n.attr("dat
/,""),s=e.extend({},i.data(),n.data()),o;i.carousel(s),(o=n.attr("data
.preventDefault()))}(window.jQuery),!function(e){"use strict";var t=fun
n.collapse.defaults,n),this.options.parent&&(this.$parent=e(this.option
constructor:t,dimension:function(){var e=this.$element.hasClass("width"
r,i;if(this.transitioning||this.$element.hasClass("in"))return;t=this.d
rent&&this.$parent.find("> .accordion-group > .in");if(r&&r.length){i=r
collapse("hide"),i||r.data("collapse",null)}this.$element[t](0),this.tr
ition&&this.$element[t](this.$element[0][n])},hide:function(){var t;if(
=this.dimension(),this.reset(this.$element[t]()),this.transition("remov
et:KERNKONZEPT t=this.dimension();return this.$element.removeClass(
ent[e!="null?"addClass":"removeClass"]("collapse"),this},transition:func
(),i.transitioning=0,i.$element.trigger(r)};this.$element.trigger(n);if
```

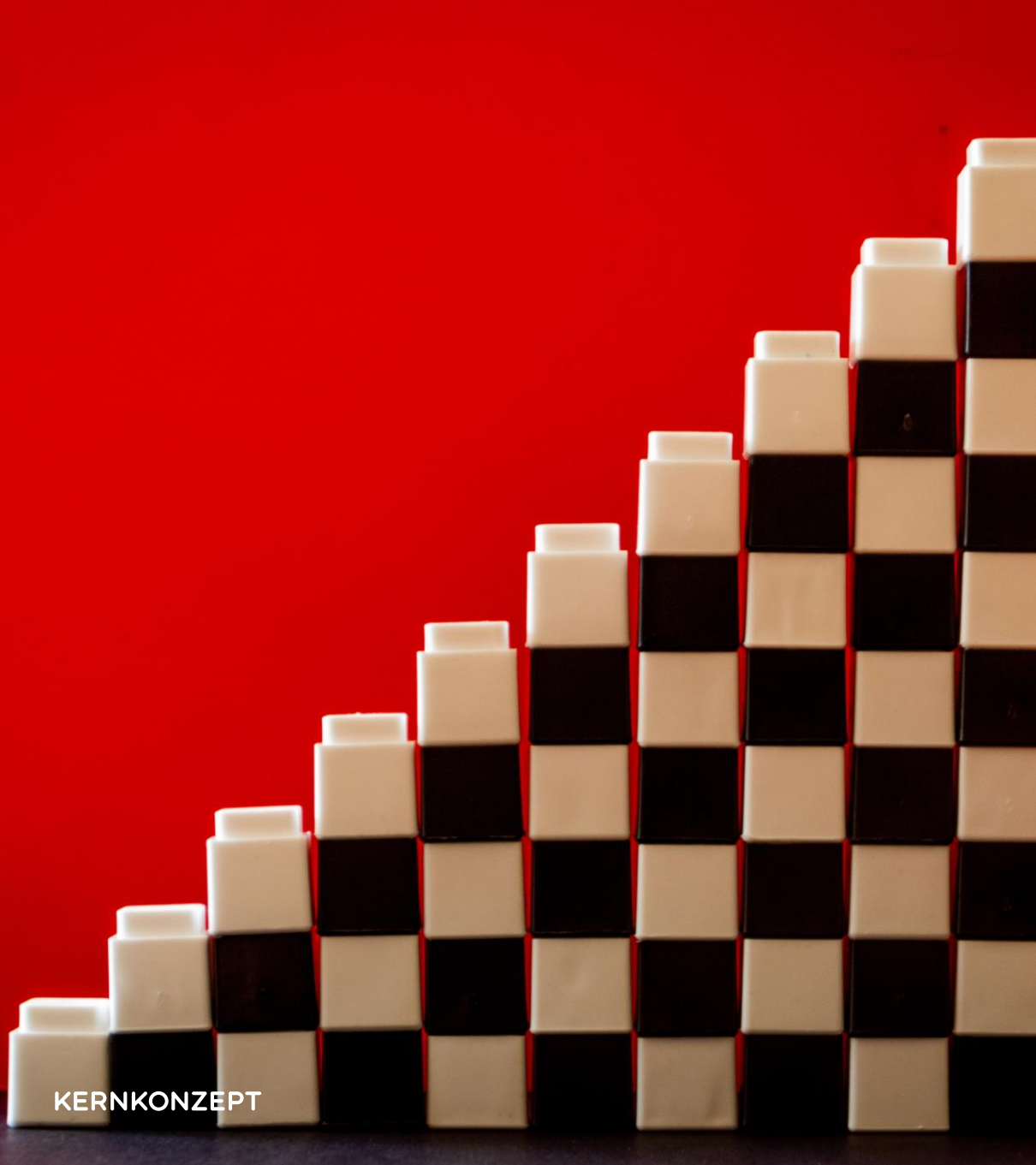
Ergebnis: Software ist jetzt sicherer

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



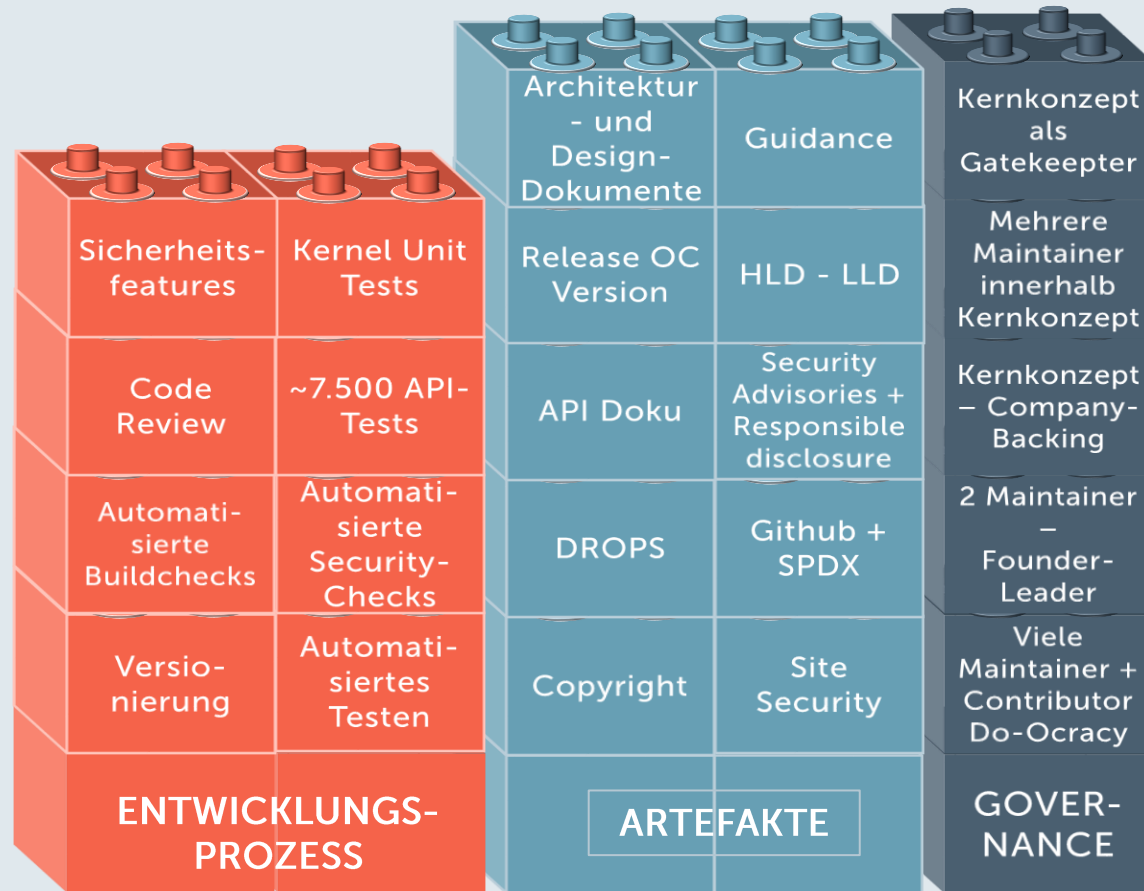
Ergebnis: Bessere Nutzbarkeit für User

- + Mehr als 50 Seiten Guidance-Dokumentation
- + Prozessdokumentation: Life Cycle



Ergebnis: Softwarequalität - Testing

- + 7351 Tests, 4247 relevant für TOE, +2123 Kernel-Unit-Tests**
- + Tests jetzt vollständig zu allen Schnittstellen**



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



VIELEN DANK!

MATTHIAS, KATRIN, INGO und STEFAN.