TECHNISCHE UNIVERSITÄT DRESDEN

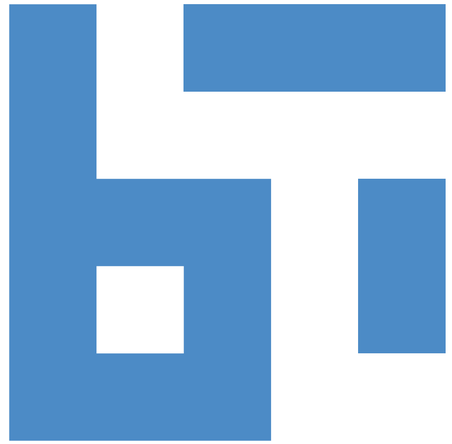
Faculty of Computer Science Institute of Systems Architecture, Operating Systems Group

RUNNING THE WORLD'S CODE FROM DRESDEN

MICHAEL ROITZSCH

ORGANISATION

Professur Betriebssysteme



Barkhausen-Institut

Systems Software Research is Irrelevant

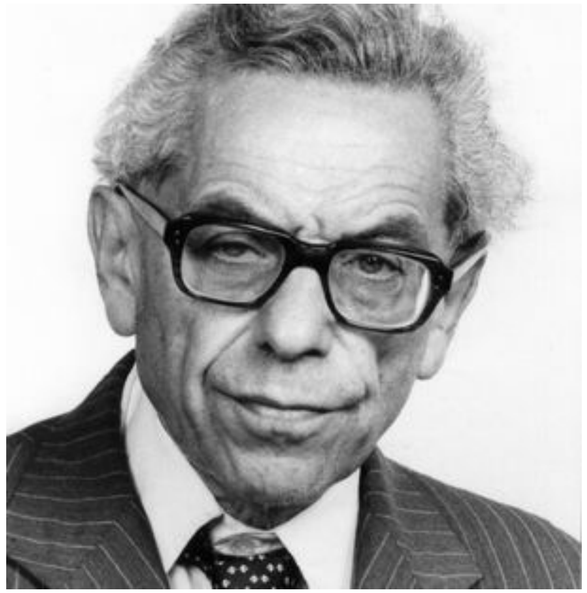
Rob Pike (damals Bell Labs, heute Google)

2000

METRIKEN

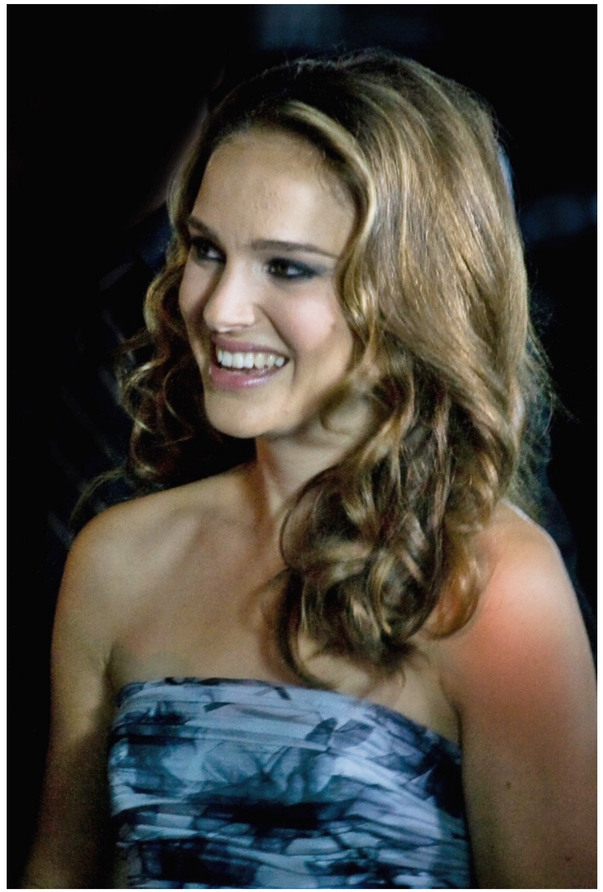
- Publication Count
- Citation Count
- H-Index

METRIKEN



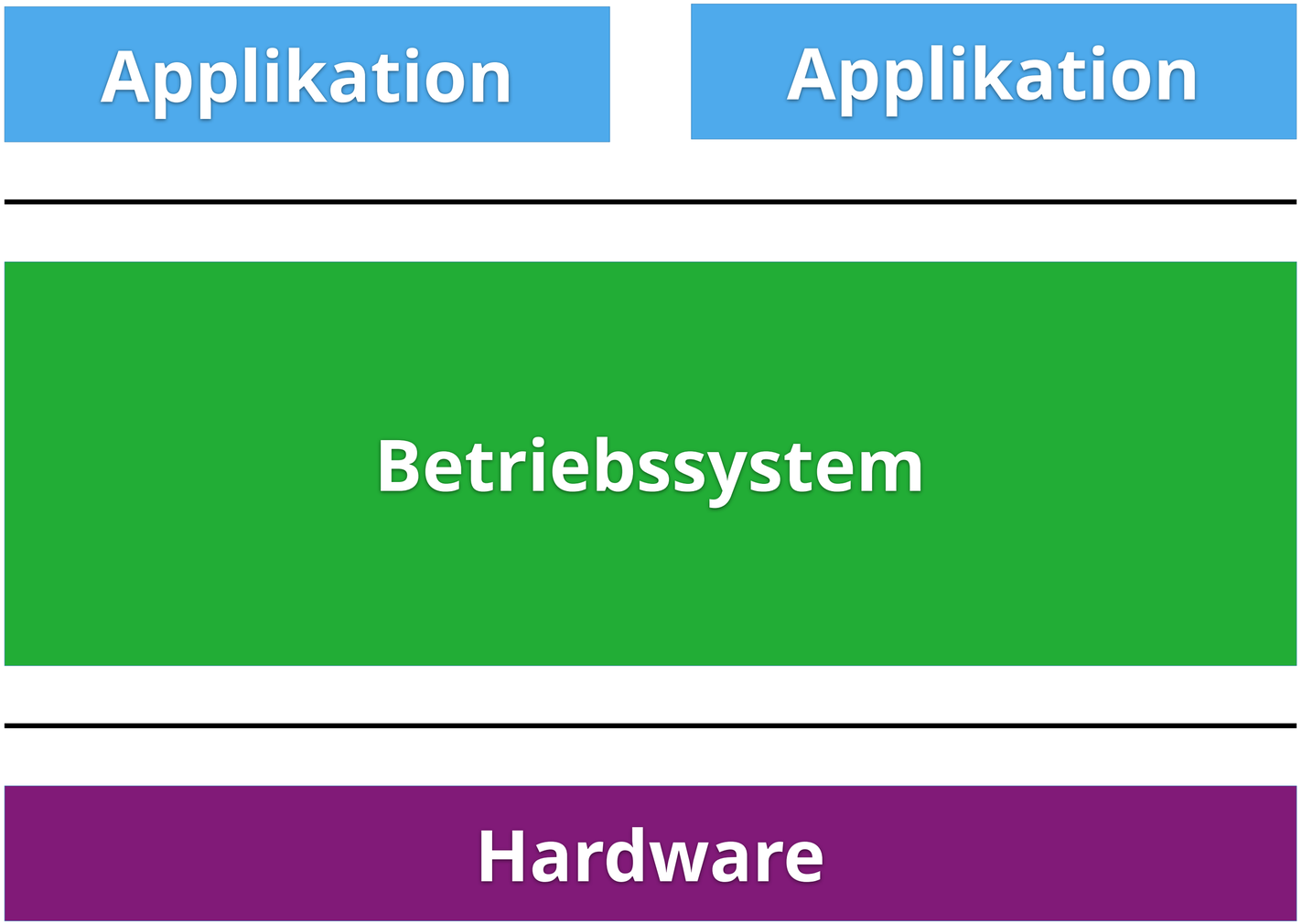
METRIKEN

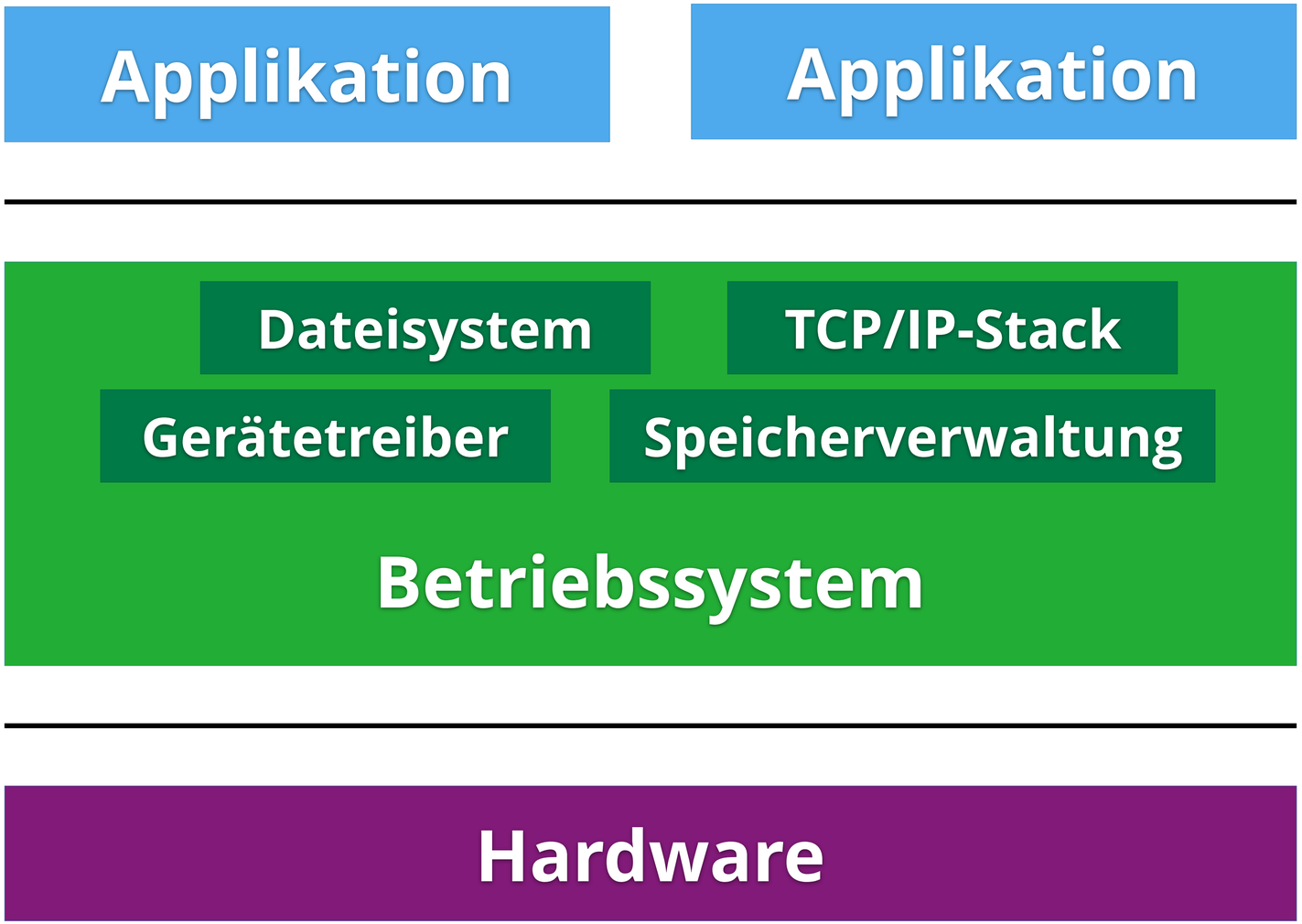
METRIKEN



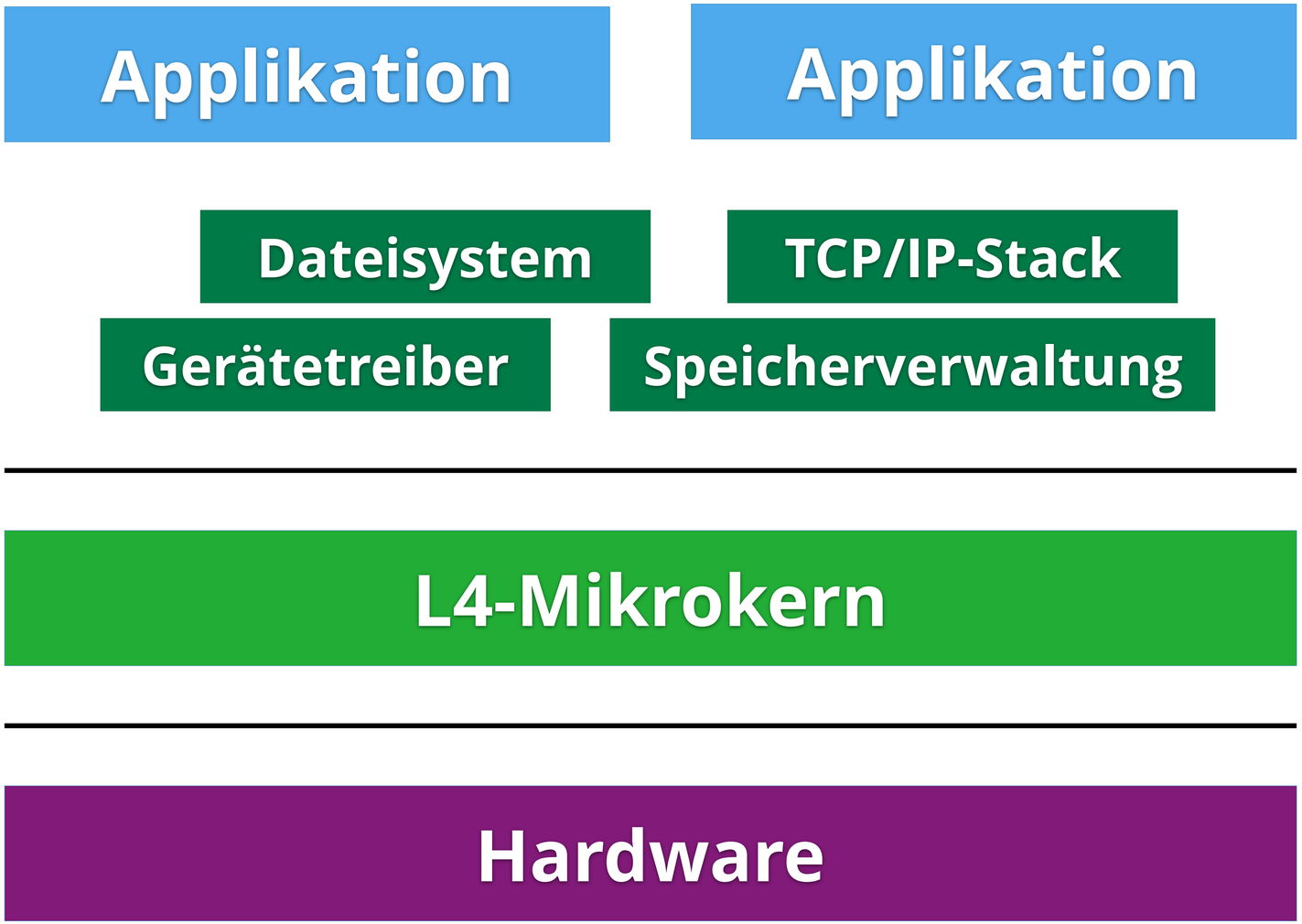
LEITLINIE

Funktionsfähige Systeme, die ein Problem mit praktischer Relevanz lösen.

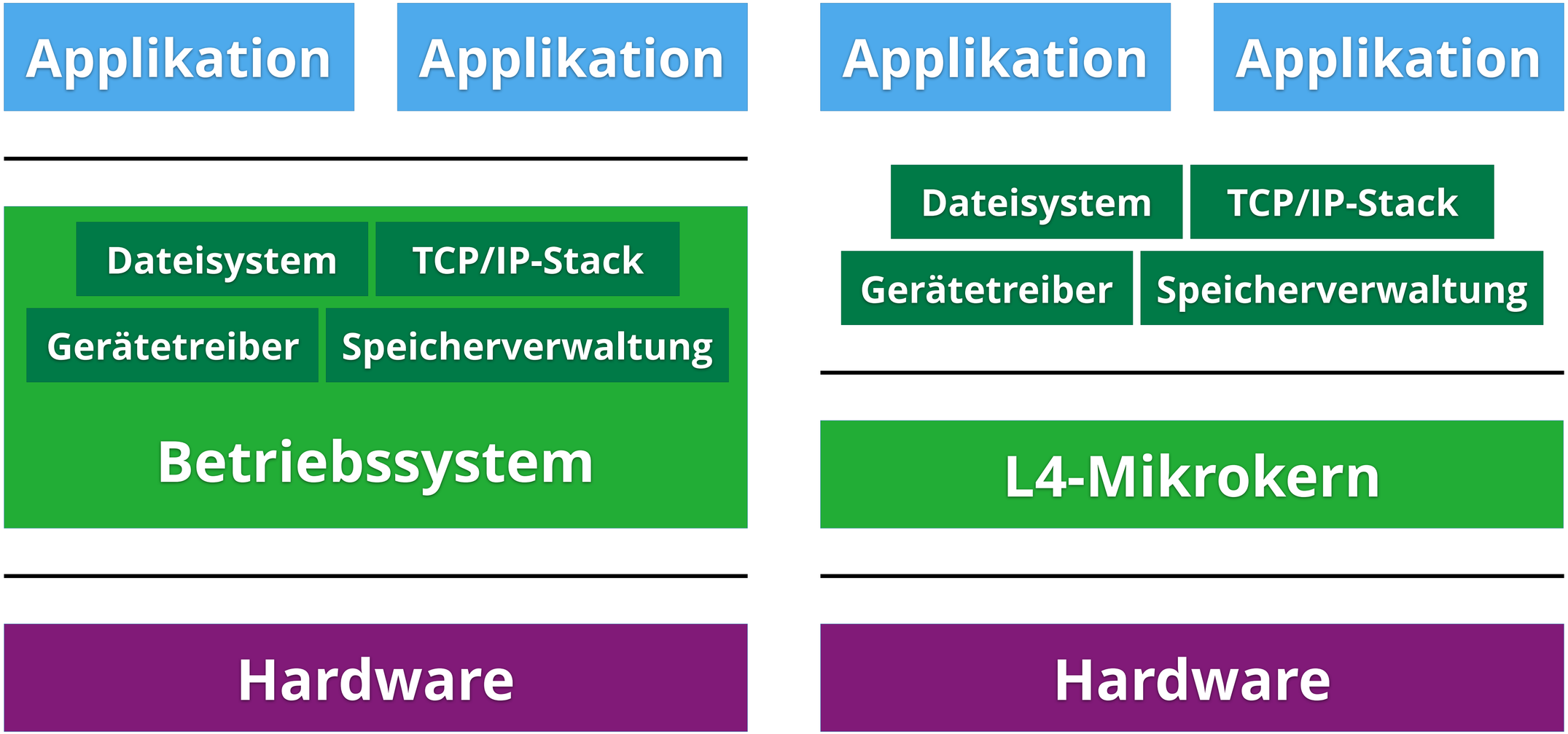

Applikation
Applikation
Betriebssystem
Hardware


Applikation
Applikation
Dateisystem
TCP/IP-Stack
Gerätetreiber
Speicherverwaltung
Betriebssystem
Hardware

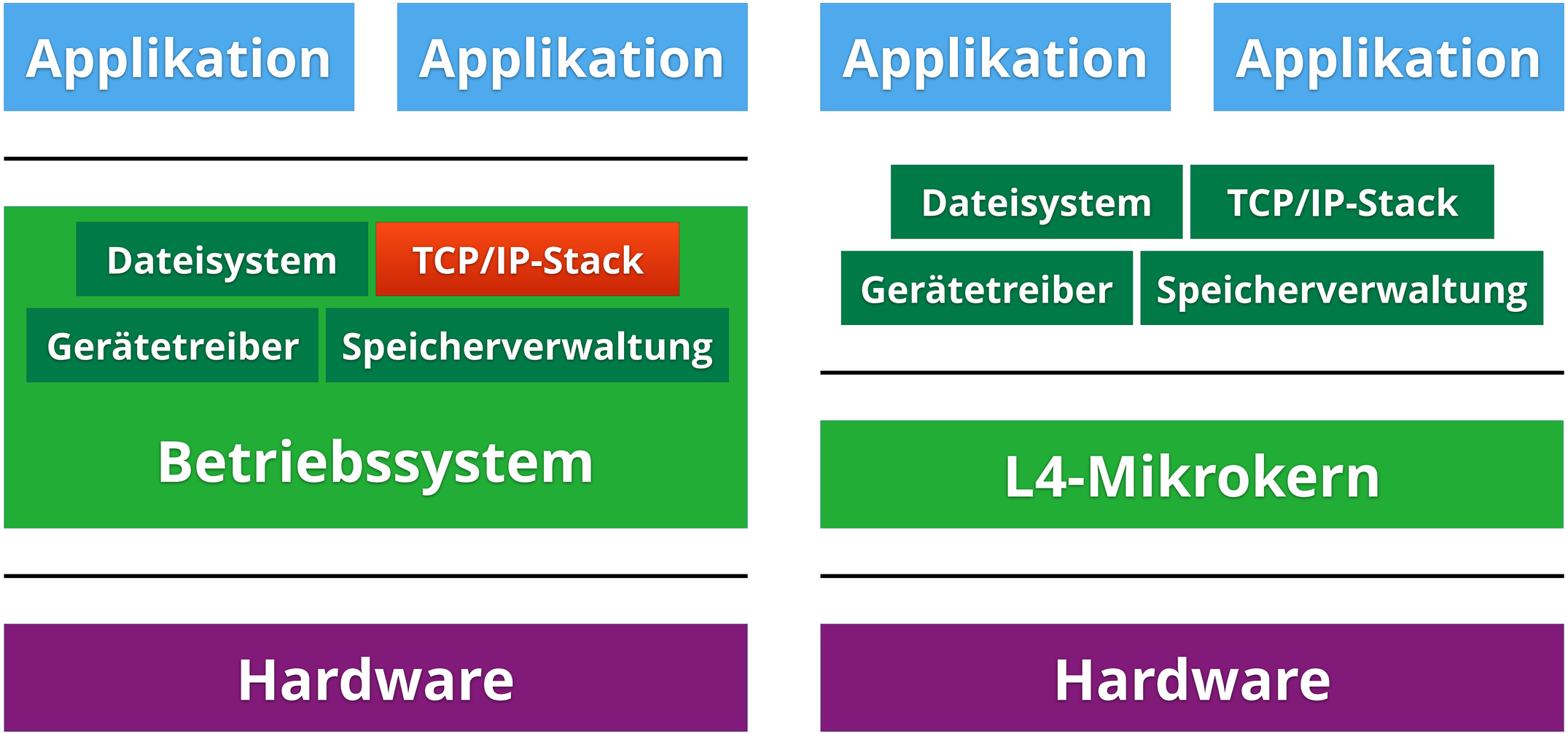
MIKROKERN


Applikation
Applikation
Dateisystem
TCP/IP-Stack
Gerätetreiber
Speicherverwaltung
L4-Mikrokern
Hardware

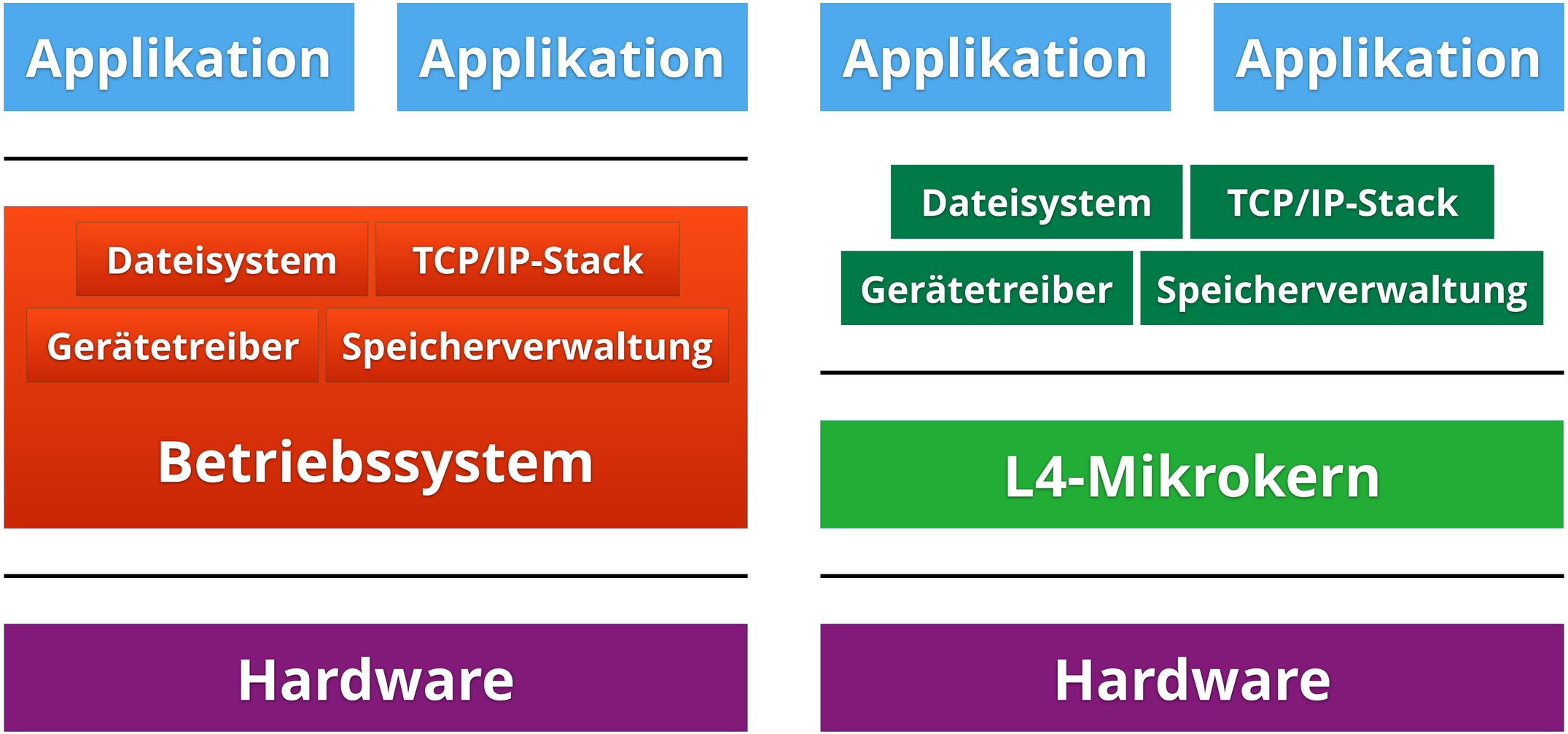
MIKROKERN


Applikation
Applikation
Dateisystem
TCP/IP-Stack
Gerätetreiber
Speicherverwaltung
Betriebssystem
Hardware
Applikation
Applikation
Dateisystem
TCP/IP-Stack
Gerätetreiber
Speicherverwaltung
L4-Mikrokern
Hardware

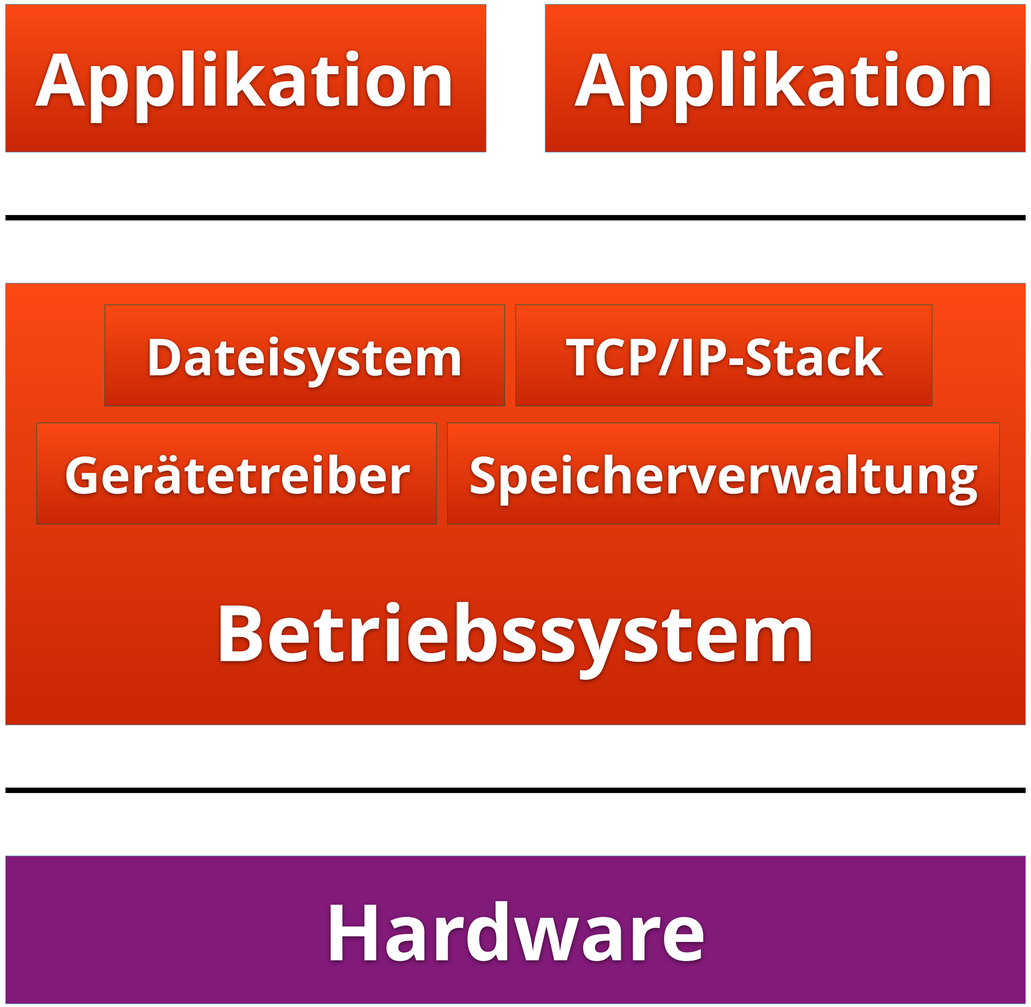
MIKROKERN

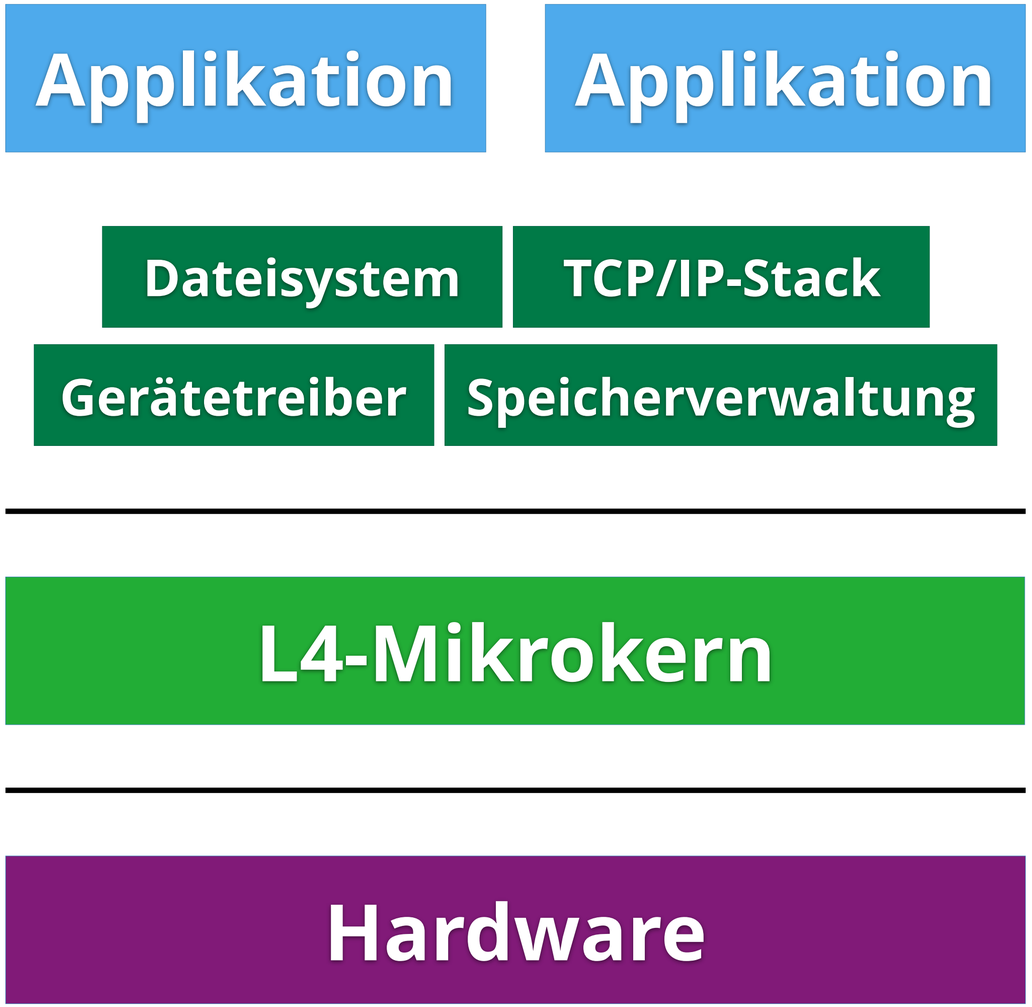

Applikation
Applikation
Dateisystem
TCP/IP-Stack
Gerätetreiber
Speicherverwaltung
Betriebssystem
Hardware
Applikation
Applikation
Dateisystem
TCP/IP-Stack
Gerätetreiber
Speicherverwaltung
L4-Mikrokern
Hardware

MIKROKERN

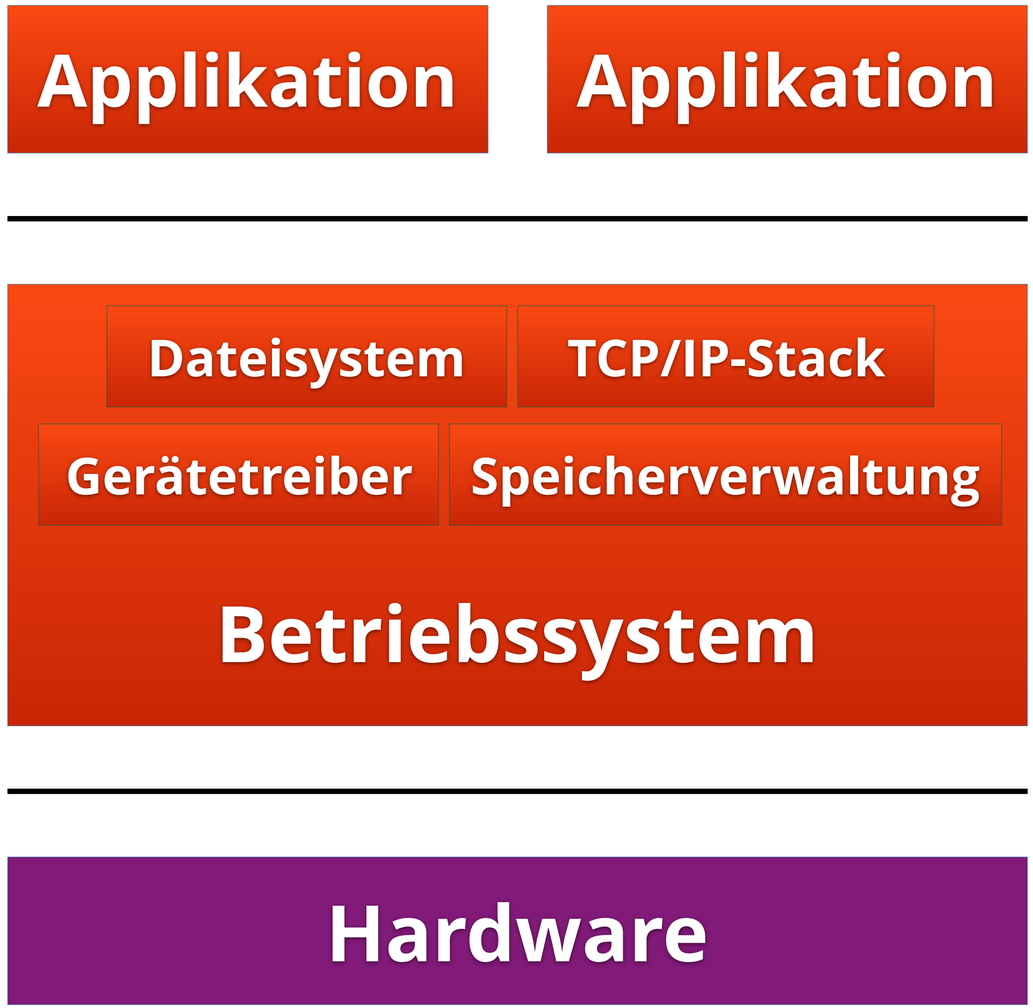

Applikation
Applikation
Dateisystem
TCP/IP-Stack
Gerätetreiber
Speicherverwaltung
Betriebssystem
Hardware
Applikation
Applikation
Dateisystem
TCP/IP-Stack
Gerätetreiber
Speicherverwaltung
L4-Mikrokern
Hardware

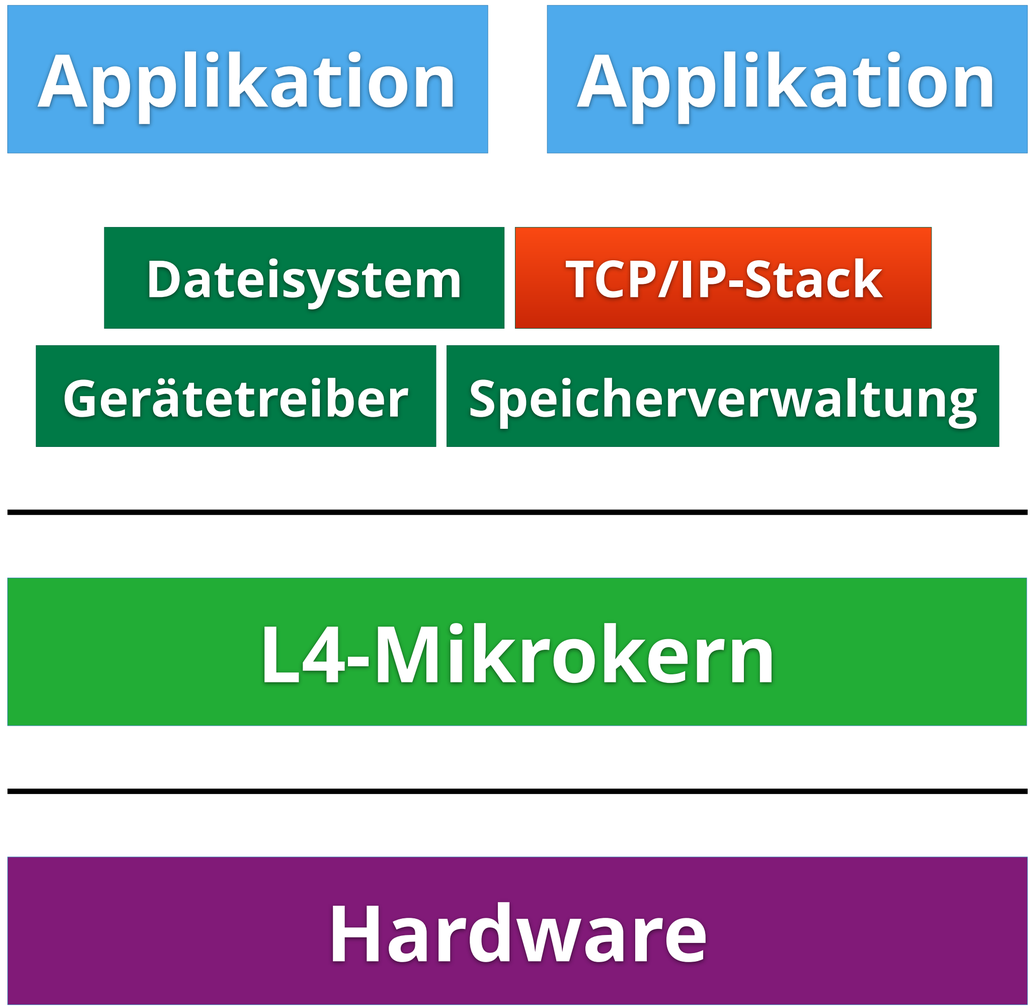
MIKROKERN


Applikation
Applikation
Dateisystem
TCP/IP-Stack
Gerätetreiber
Speicherverwaltung
Betriebssystem
Hardware

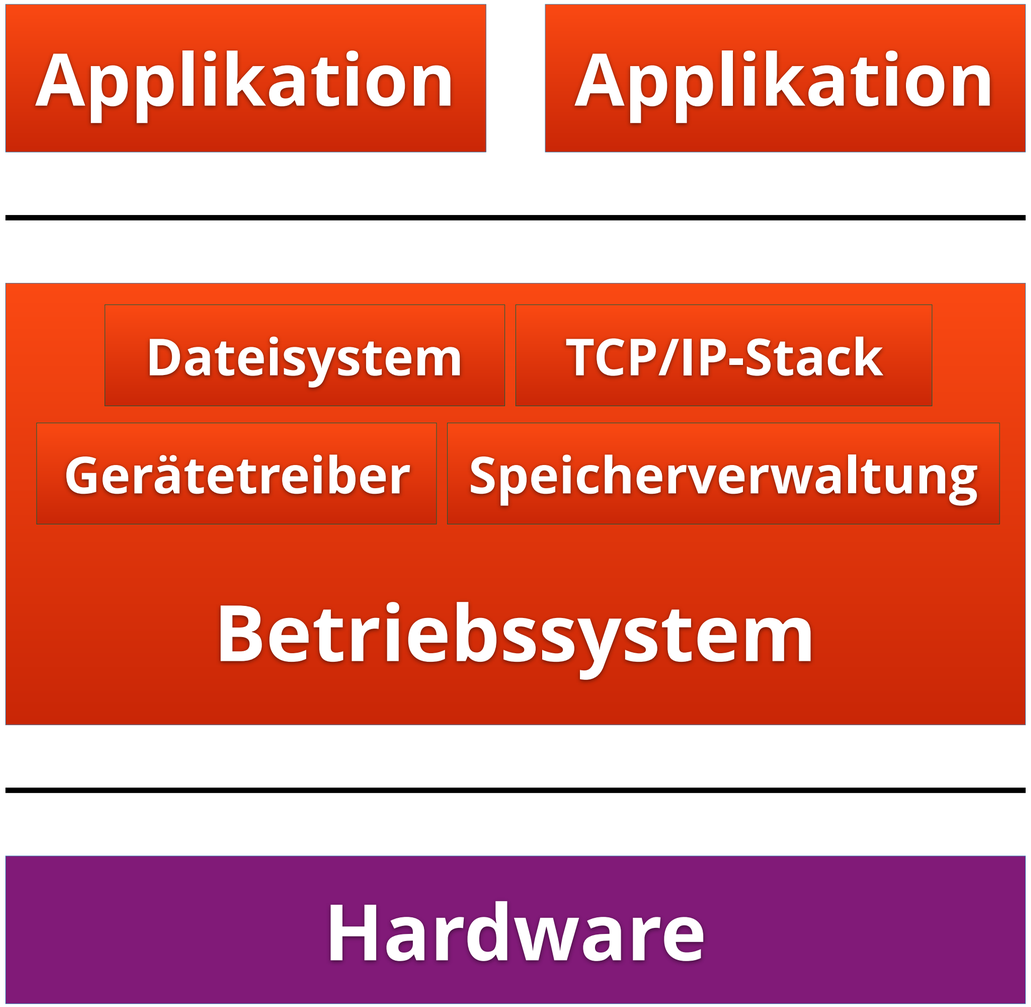

Applikation
Applikation
Dateisystem
TCP/IP-Stack
Gerätetreiber
Speicherverwaltung
L4-Mikrokern
Hardware

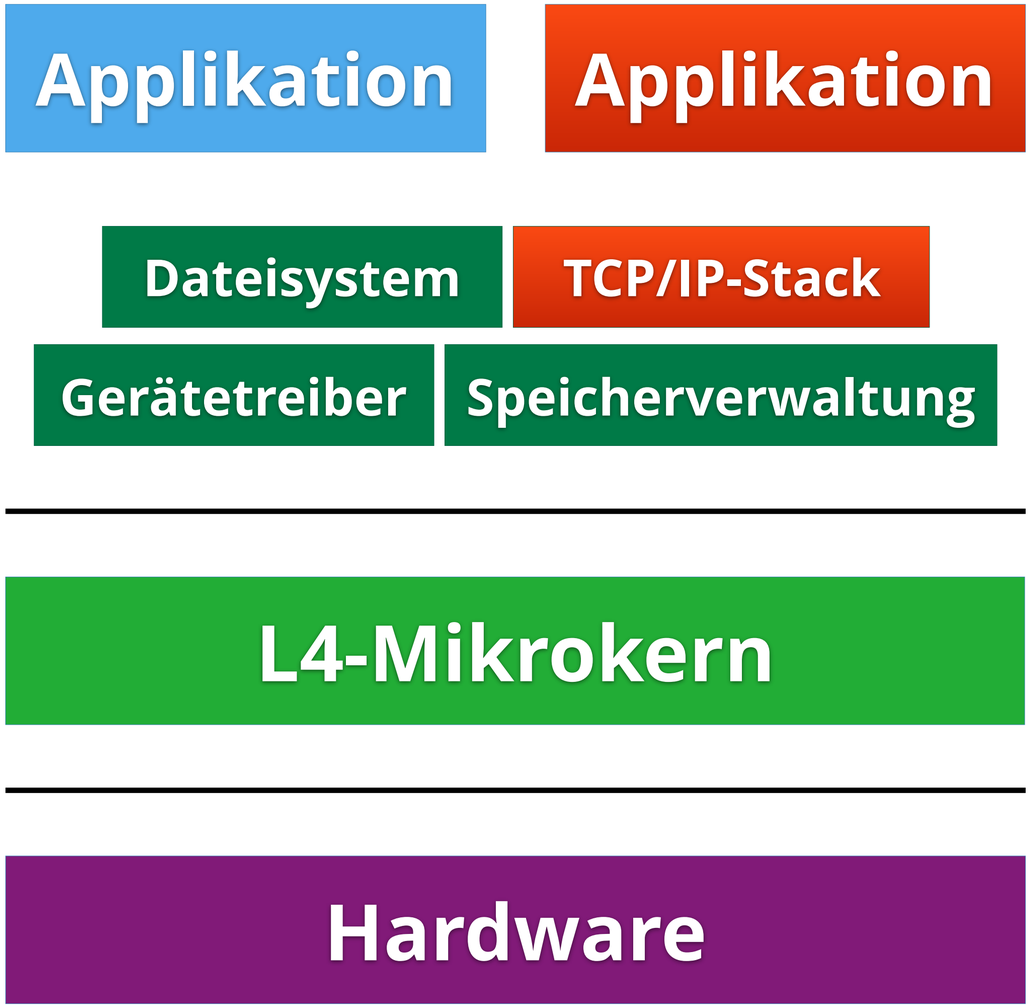
MIKROKERN


Applikation
Applikation
Dateisystem
TCP/IP-Stack
Gerätetreiber
Speicherverwaltung
Betriebssystem
Hardware


Applikation
Applikation
Dateisystem
TCP/IP-Stack
Gerätetreiber
Speicherverwaltung
L4-Mikrokern
Hardware

MIKROKERN


Applikation
Applikation
Dateisystem
TCP/IP-Stack
Gerätetreiber
Speicherverwaltung
Betriebssystem
Hardware

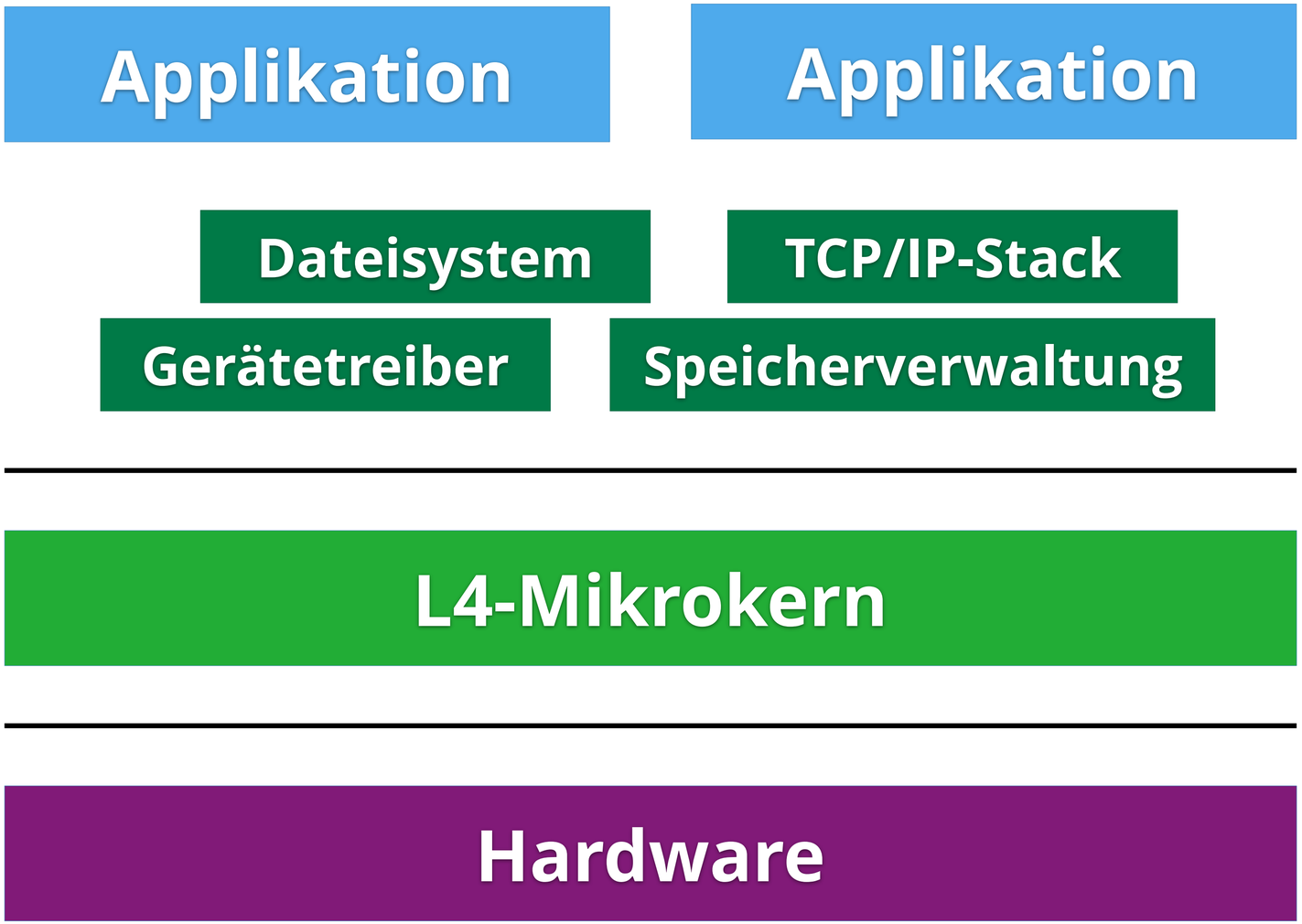

Applikation
Applikation
Dateisystem
TCP/IP-Stack
Gerätetreiber
Speicherverwaltung
L4-Mikrokern
Hardware

TRUSTED COMPUTING BASE

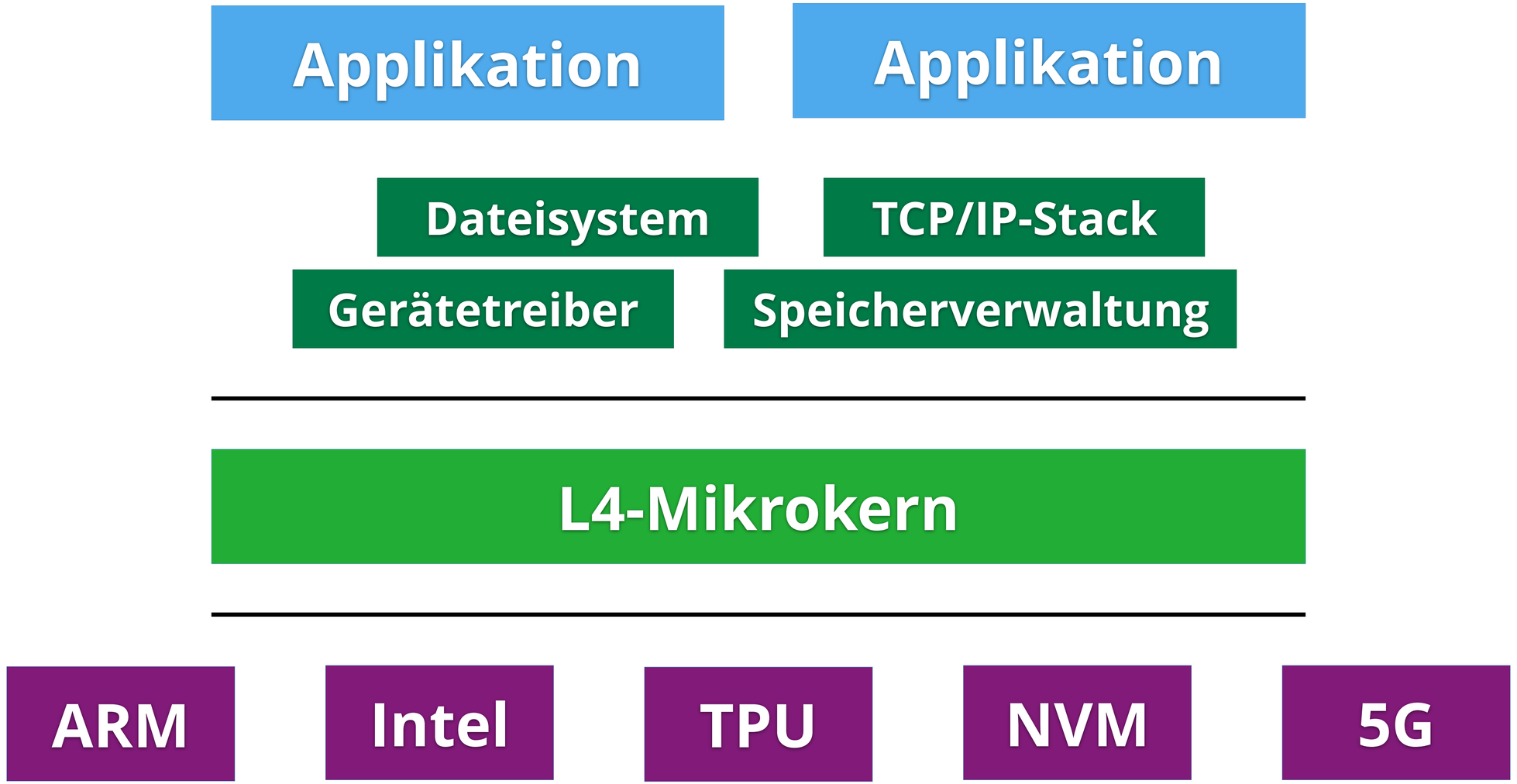
- **Trusted Computing Base (TCB):** Menge an Komponenten, denen eine Anwendung für das Erbringen ihrer Funktionalität vertrauen muss
- abhängig von Anwendung und Funktionalität
- Mikrokerne ermöglichen minimale, anwendungsspezifische TCBs

Mikrokerne helfen, wachsende Komplexität von Systemen durch Zerlegung beherrschbar zu machen.

MIKROKERN

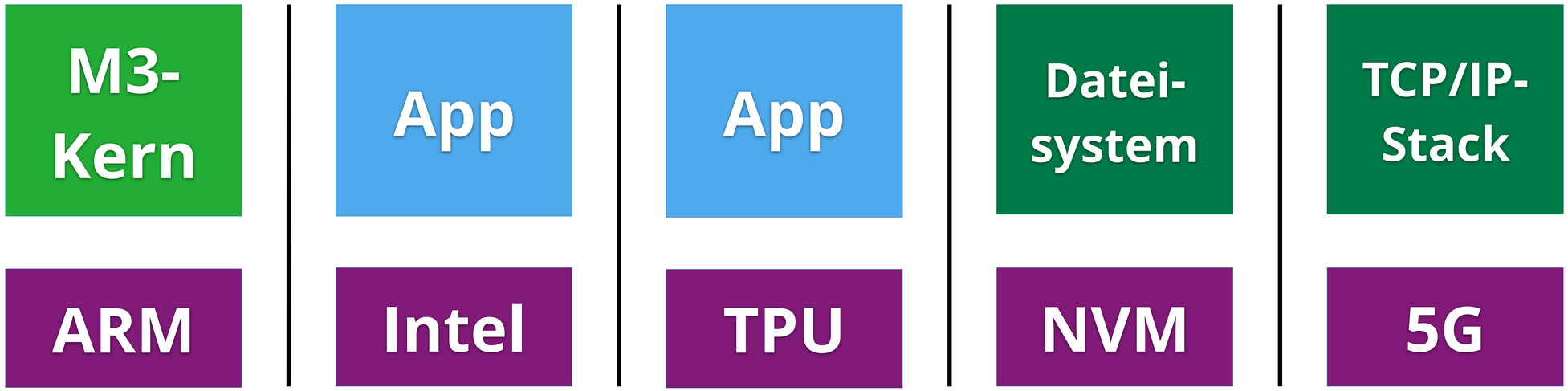

Applikation
Applikation
Dateisystem
TCP/IP-Stack
Gerätetreiber
Speicherverwaltung
L4-Mikrokern
Hardware

MIKROKERN


Applikation
Applikation
Dateisystem
TCP/IP-Stack
Gerätetreiber
Speicherverwaltung
L4-Mikrokern
ARM
Intel
TPU
NVM
5G

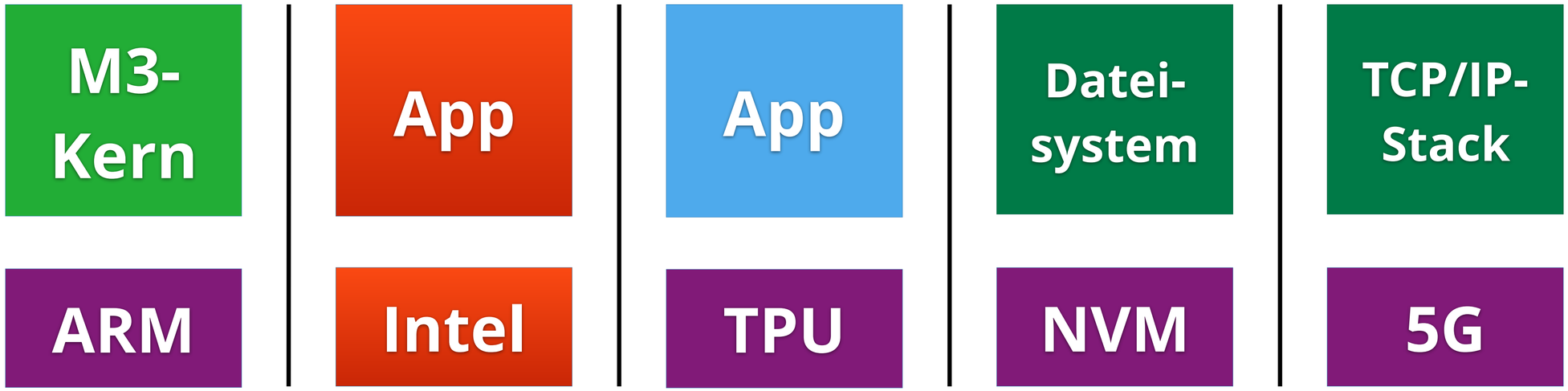
barkhausen institut

Plattform für IoT



barkhausen institut

Plattform für IoT



fTPM: A Software-only Implementation of a TPM Chip

Himanshu Raj, Stefan Saroiu, Alec Wolman, Ronald Aigner, Jeremiah Cox, Paul England, Chris Fenner, Kinshuman Kinshumann, Jork Loeser, Dennis Mattoon, Magnus Nystrom, David Robinson, Rob Spiger, Stefan Thom, and David Wooten*
Microsoft

Abstract: *Commodity CPU architectures, such as ARM and Intel CPUs, have started to offer trusted computing features in their CPUs aimed at displacing dedicated trusted hardware. Unfortunately, these CPU architectures raise serious challenges to building trusted systems because they omit providing secure resources outside the CPU perimeter.*

This paper shows how to overcome these challenges to build software systems with security guarantees similar to those of dedicated trusted hardware. We present the design and implementation of a firmware-based TPM 2.0 (fTPM) leveraging ARM TrustZone. Our fTPM is the reference implementation of a TPM 2.0 used in millions of mobile devices. We also describe a set of mechanisms needed for the fTPM that can be useful for building more sophisticated trusted applications beyond just a TPM.

Secure Enclave

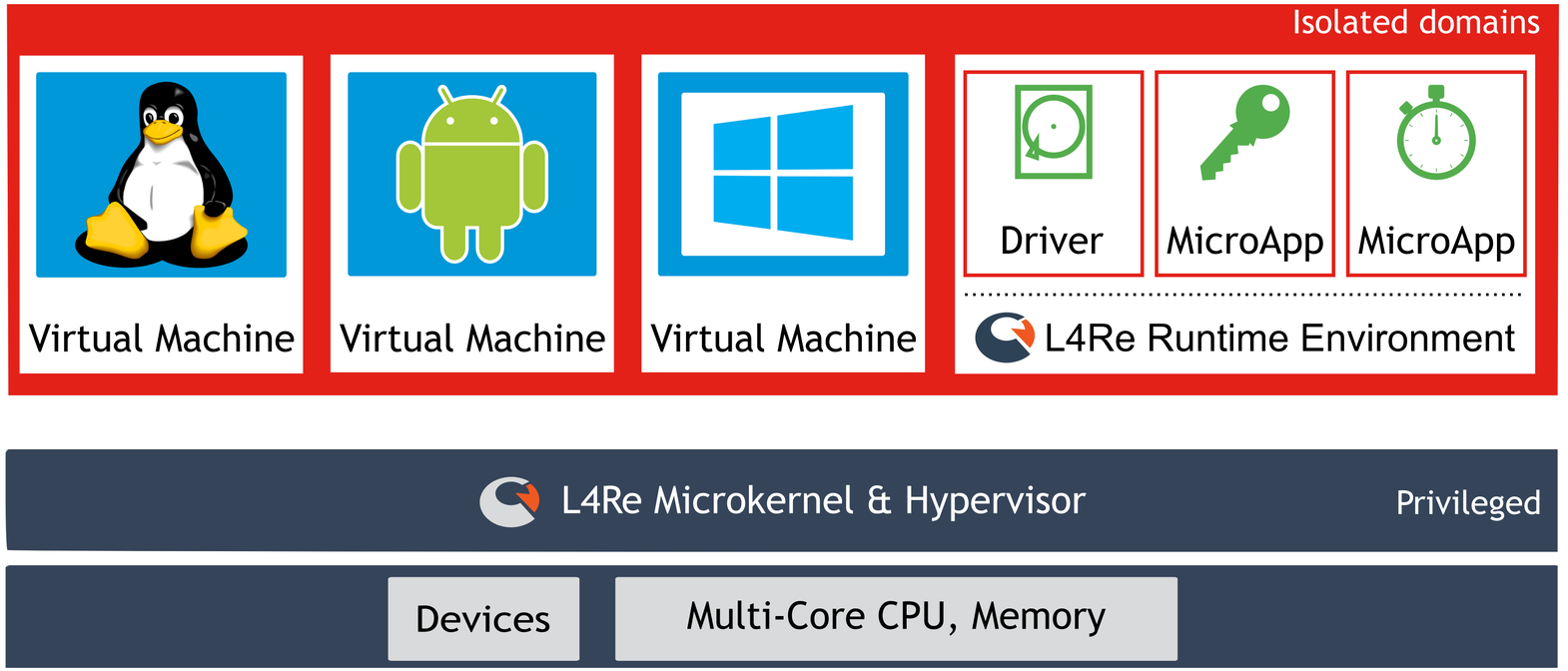
The Secure Enclave is a coprocessor fabricated within the system on chip (SoC). It uses encrypted memory and includes a hardware random number generator. The Secure Enclave provides all cryptographic operations for **Data Protection** key management and maintains the integrity of Data Protection even if the kernel has been compromised. Communication between the Secure Enclave and the application processor is isolated to an interrupt-driven mailbox and shared memory data buffers.

The Secure Enclave includes a dedicated Secure Enclave Boot ROM. Similar to the application processor Boot ROM, the Secure Enclave Boot ROM is immutable code that establishes the hardware root of trust for the Secure Enclave.

The Secure Enclave runs a Secure Enclave OS based on an Apple-customized version of the L4 microkernel. This Secure Enclave OS is signed by Apple, verified by the Secure Enclave Boot ROM, and updated through a personalized software update process.

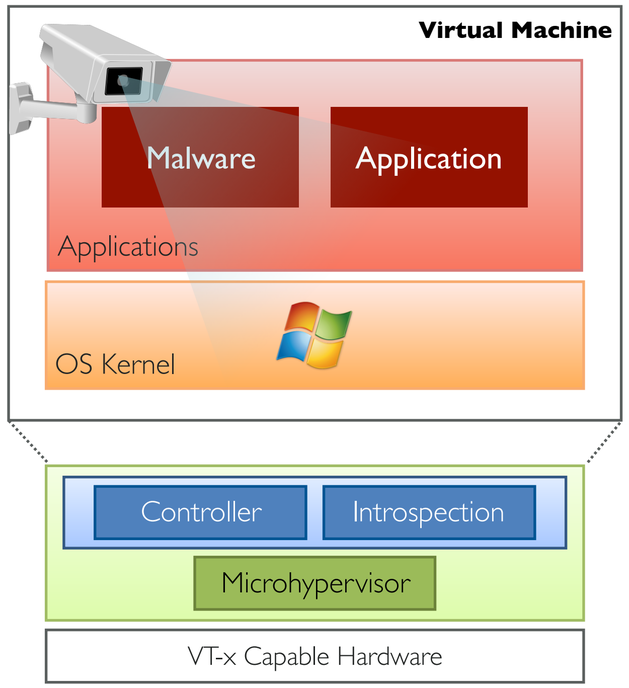
FIRMEN IN DRESDEN

KERNKONZEPT



FIRMEN IN DRESDEN

CYBERUS
TECHNOLOGY



CYBERUS TECHNOLOGY

Meltdown: Reading Kernel Memory from User Space

Moritz Lipp[1], Michael Schwarz[1], Daniel Gruss[1], Thomas Prescher[2], Werner Haas[2], Anders Fogh[3], Jann Horn[4], Stefan Mangard[1], Paul Kocher[5], Daniel Genkin[6,9], Yuval Yarom[7], Mike Hamburg[8]

[1]*Graz University of Technology,* [2]*Cyberus Technology GmbH,*
[3]*G-Data Advanced Analytics,* [4]*Google Project Zero,*
[5]*Independent (www.paulkocher.com),* [6]*University of Michigan,*
[7]*University of Adelaide & Data61,* [8]*Rambus, Cryptography Research Division*

CYBERUS
TECHNOLOGY

LazyFP: Leaking FPU Register State using Microarchitectural Side-Channels

Julian Stecklina
Amazon Development Center Germany GmbH
jsteckli@amazon.de

Thomas Prescher
Cyberus Technology GmbH
thomas.prescher@cyberus-technology.de

FIRMEN IN DRESDEN

ZUSAMMENFASSUNG

- Arbeit an „echten“ Systemen
- enge Zusammenarbeit mit Mitarbeitern der Professur
- vielseitige Firmen- und Forschungs-Landschaft

Systems Research: More Relevant than Ever.