TeleTrusT
Pioneers in IT security.

Informationstag "IT-Sicherheit im Smart Grid"

Berlin, 13.06.2013

Systemsicherheit ermöglicht Energiewende

Jörn Müller-Quade, KASTEL, KIT

Karlsruher Institut für Technologie

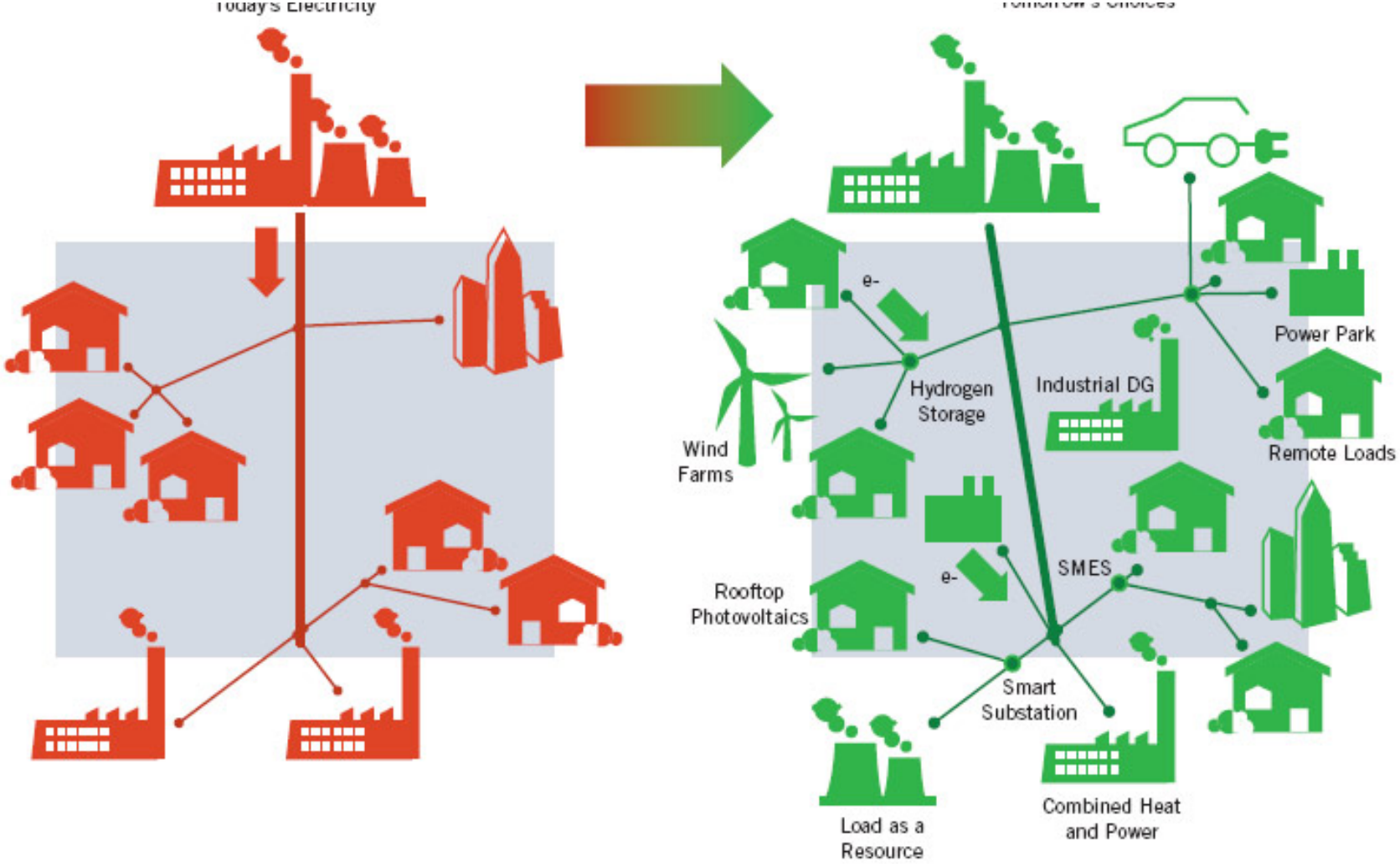
KASTEL

Systemsicherheit ermöglicht Energiewende

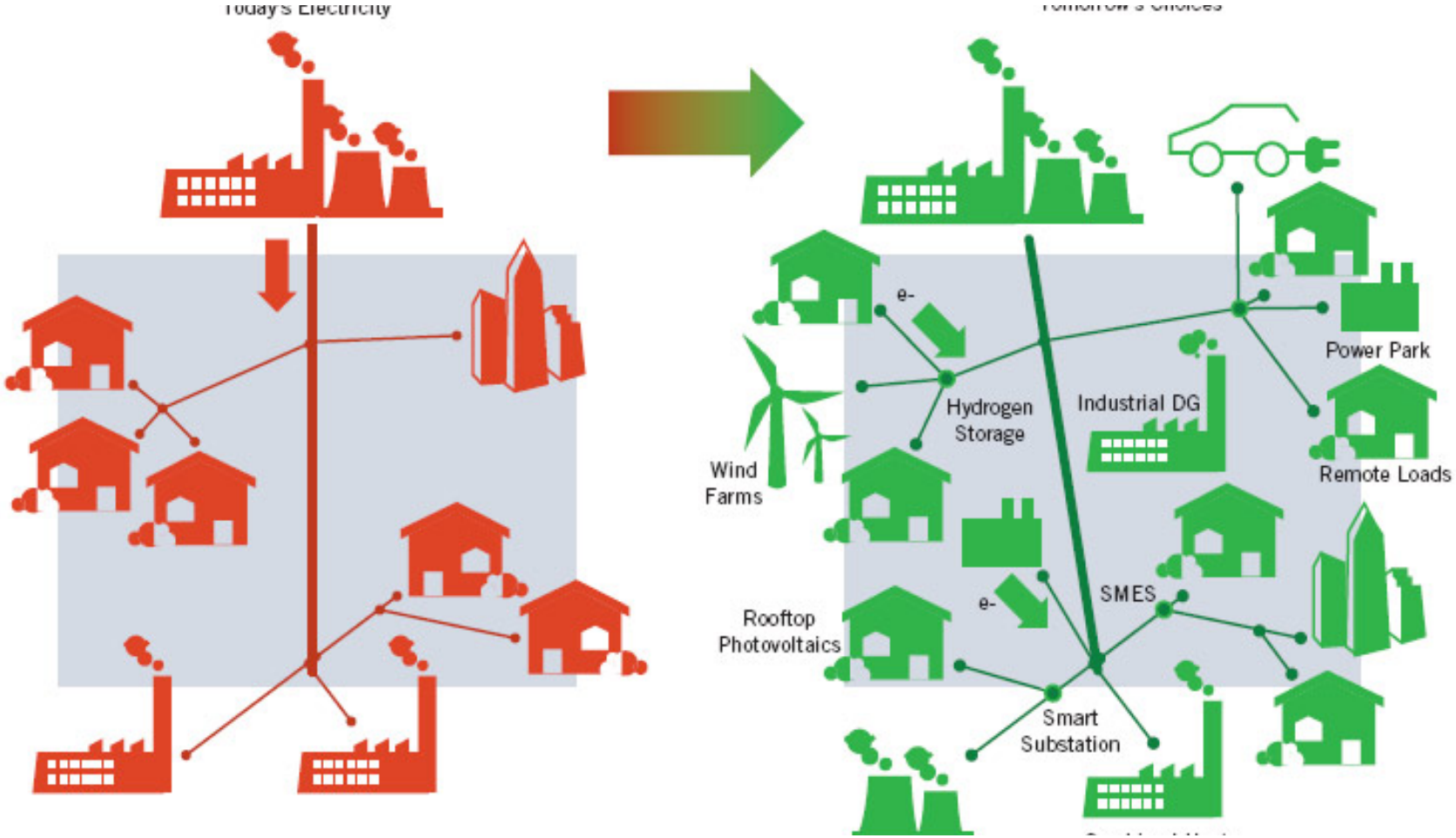
Jörn Müller-Quade, KASTEL, KIT

KOMPETENZZENTRUM FÜR ANGEWANDTE SICHERHEITSTECHNOLOGIE

The IEEE‘s version of a Smart Grid



The IEEE‘s version of a Smart Grid



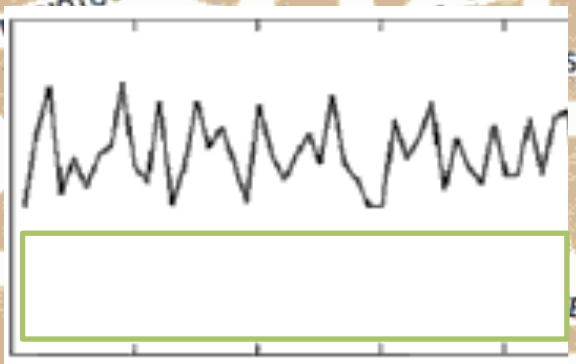
Komplex, Computergesteuert und Angreifbar

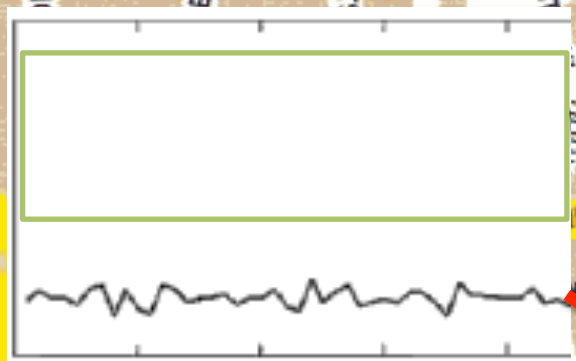
Privacy I

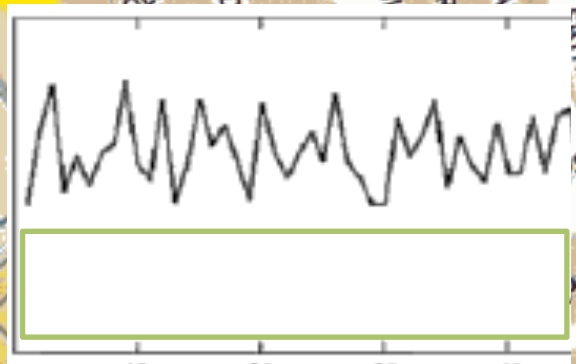
Stromverbrauch

verrät Lebensgewohnheiten

Privacy II







Sabotage

http://www.jfiveelectric.com/blog/wp-content/uploads/2011/02/Rolling-Blackout.jpg

IT-Systeme sind komplex

Stuxnet

Spiegel

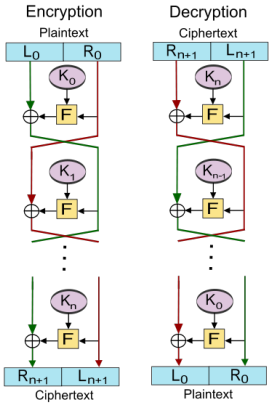
Stuxnet

Wir haben keine Systemsicherheit. Wer hat versagt?

Spiegel

The End of Crypto

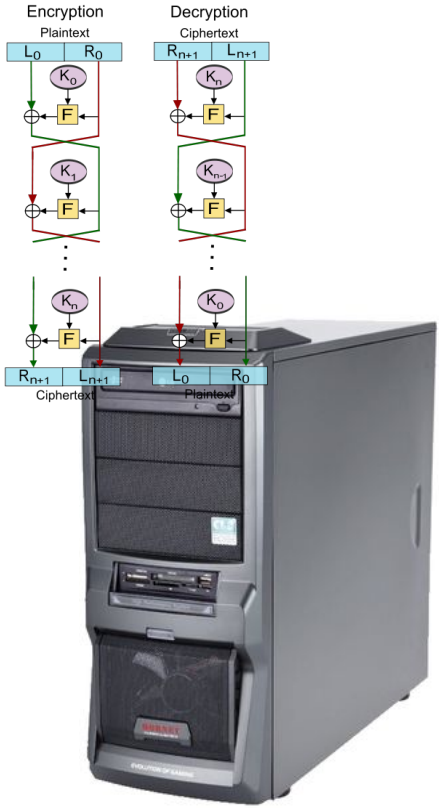
Große Fortschritte



The End of Crypto

Computer sind frei programmierbar

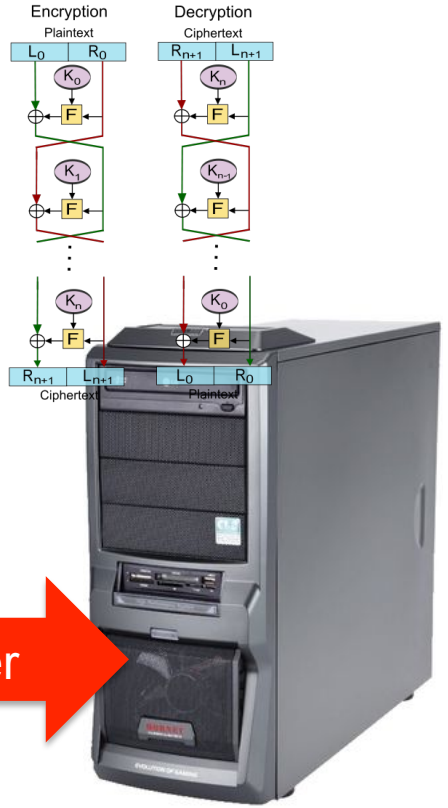
Große Fortschritte



The End of Crypto

Computer sind frei programmierbar

Große Fortschritte



Trotzdem unsicher

Malware direkt auf dem Computer macht allen weiteren Schutz obsolet

PRISM/US-984XN
Overview

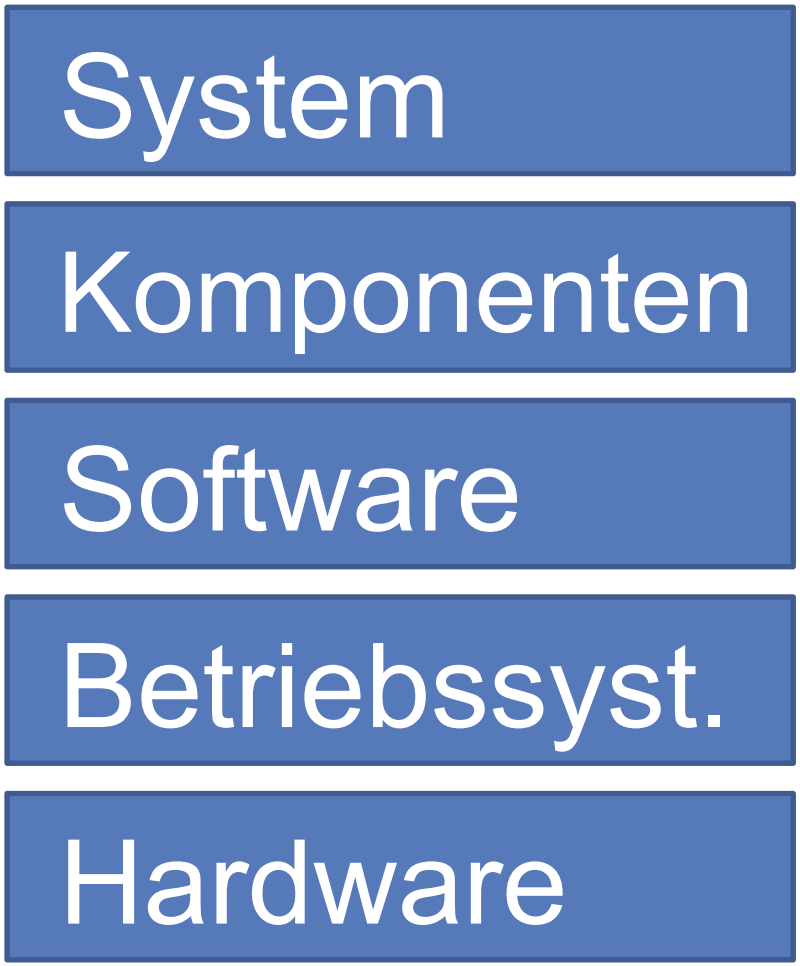
OR

*The SIGAD Used **Most** in NSA Reporting*
Overview

[redacted]

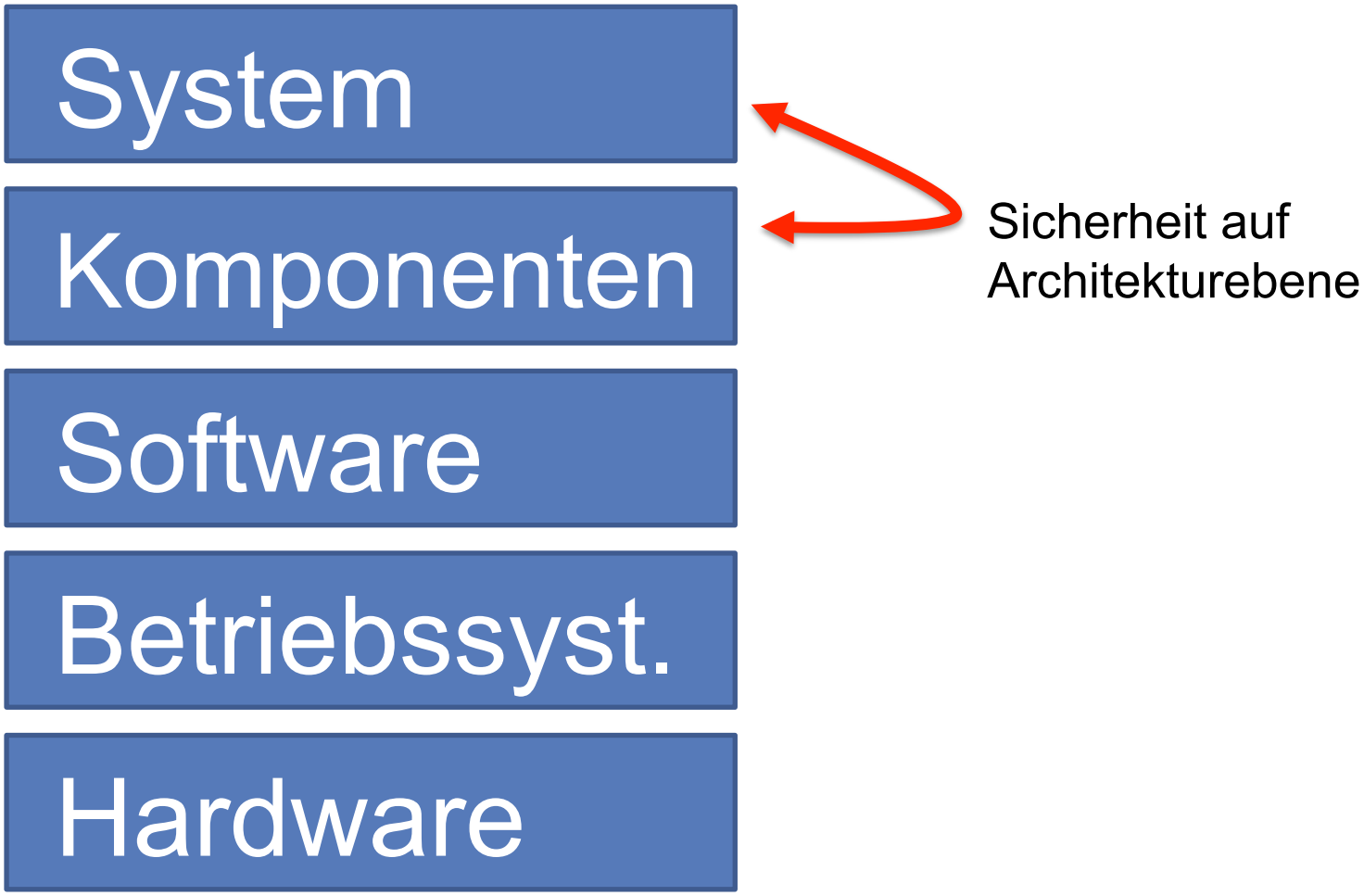
April 2013

Securing the *Complete* Technology Stack

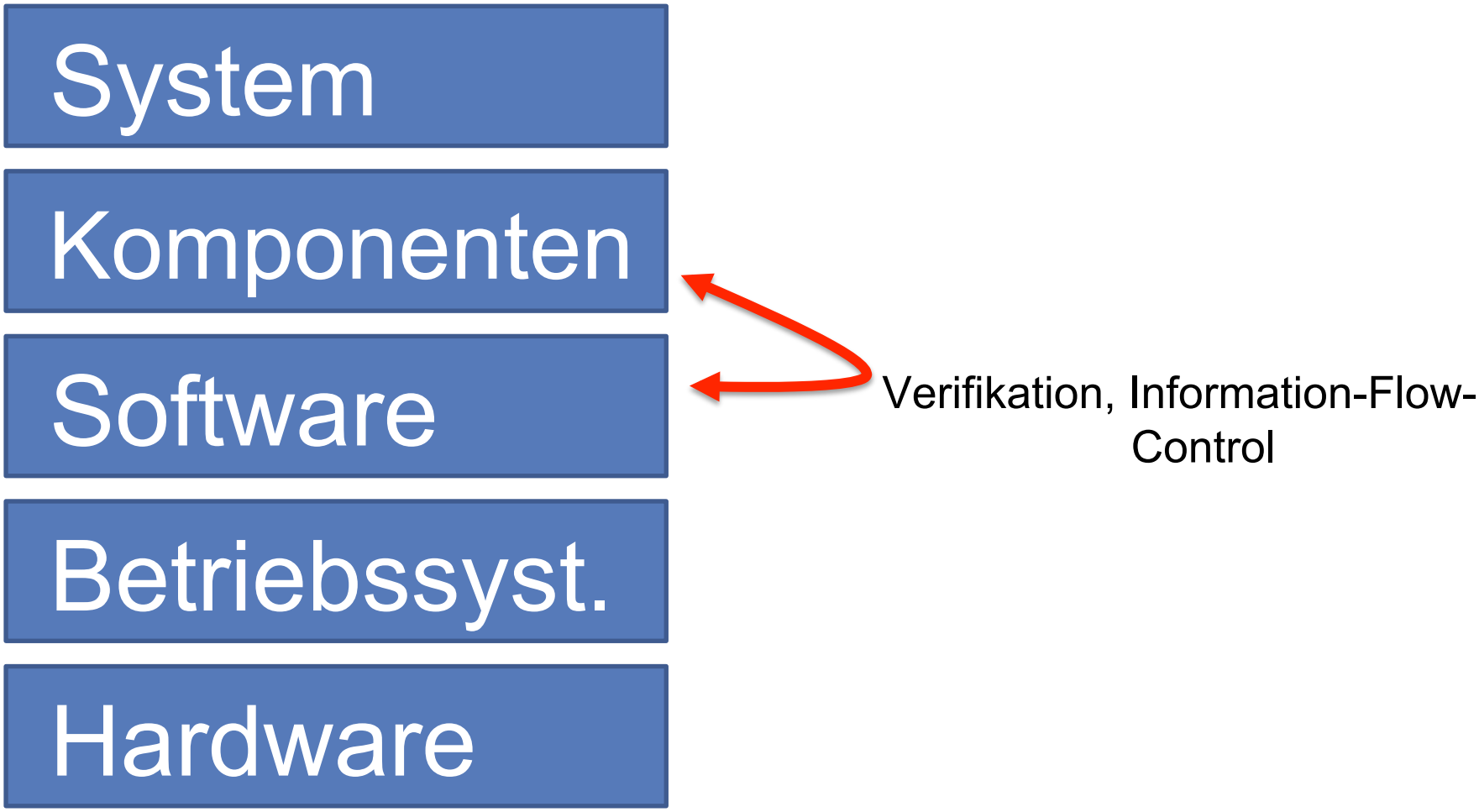


- Jede Schicht gibt Garantien (nach oben)
- Jede Schicht benutzt Annahmen und Garantien von der darunterliegenden Schicht
- Bisher werden die Schichten unabhängig voneinander geschützt.
- Bisher keine durchgängige Garantie

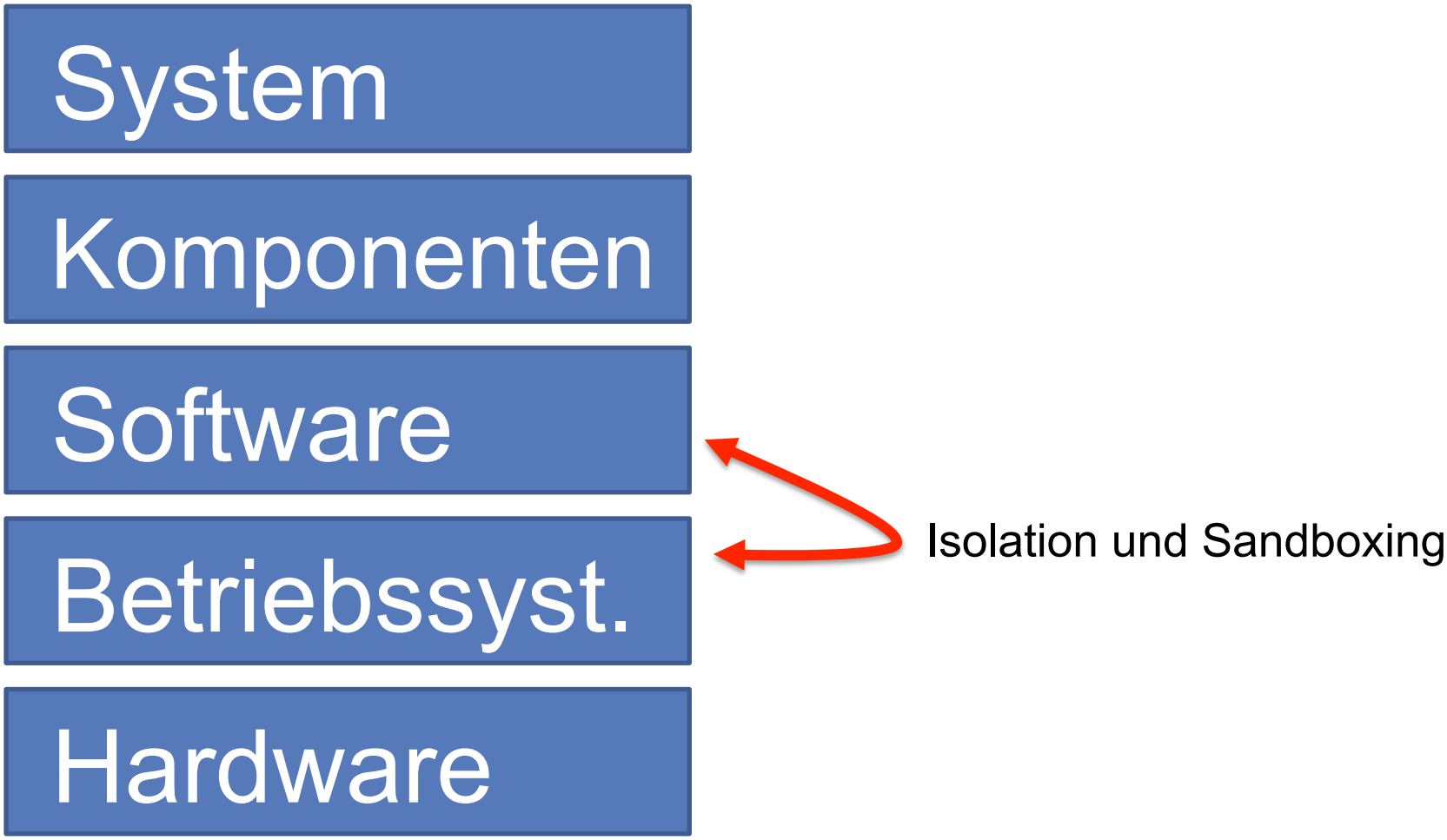
Securing the Technology Stack



Securing the Technology Stack



Securing the Technology Stack



Securing the Technology Stack

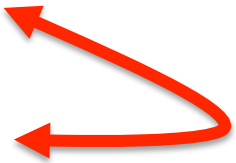
System

Komponenten

Software

Betriebssyst.

Hardware



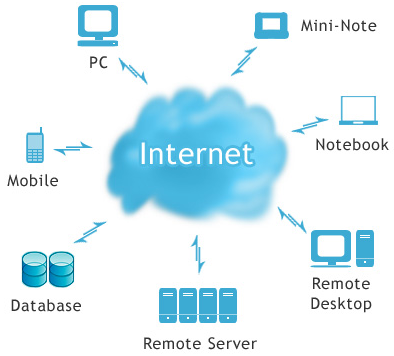
Harvard Architektur
HW-Verifikation?
Hilft nicht gegen HW-Trojaner

Interdisziplinär

- System
- Komponenten
- Software
- Betriebssyst.
- Hardware

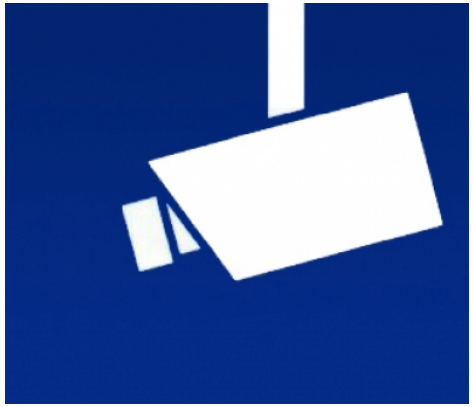
Drei Prototypen

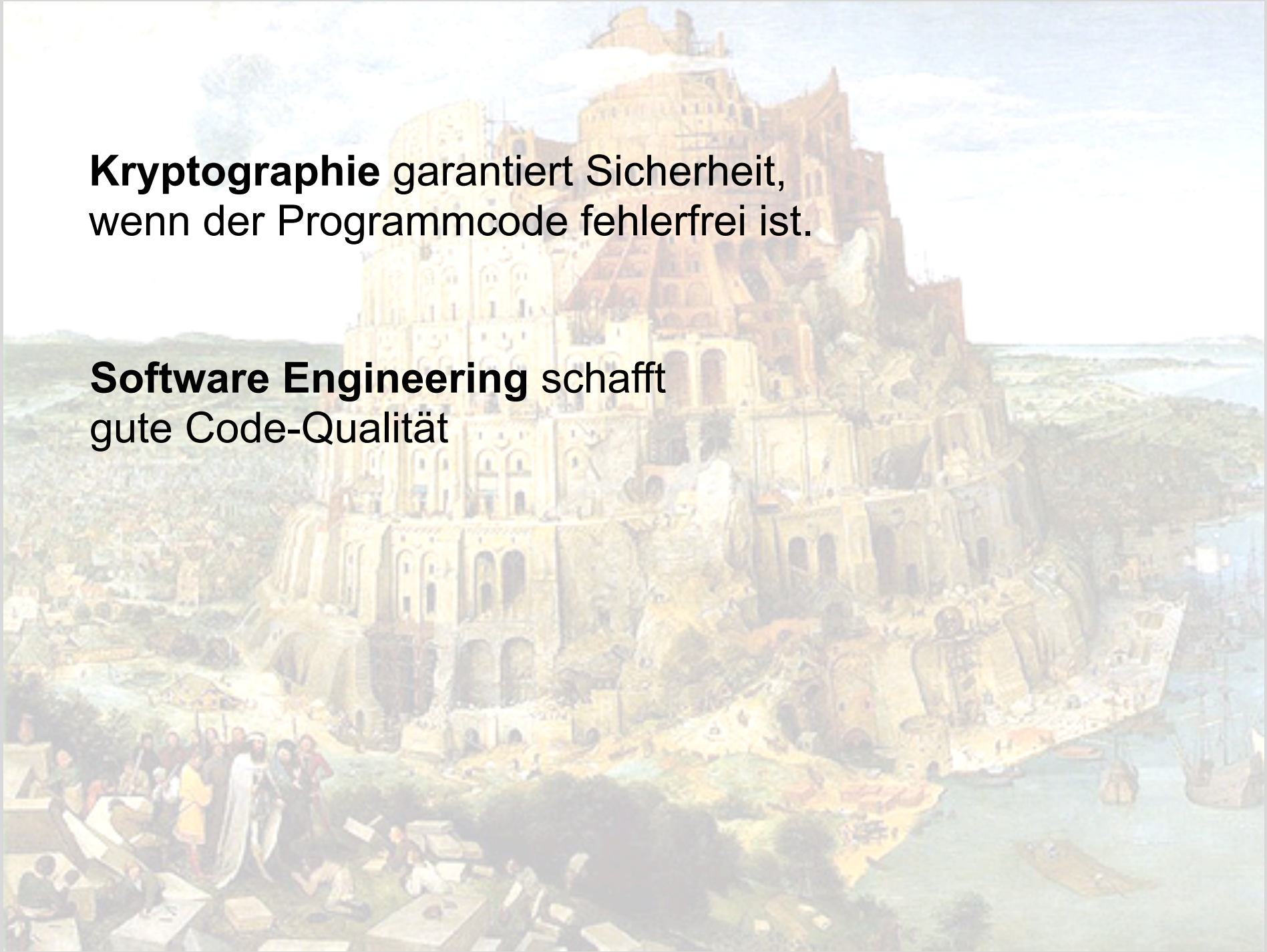
Cloud



eEnergy

Sicherheit in öffentlichen Räumen





Kryptographie garantiert Sicherheit,
wenn der Programmcode fehlerfrei ist.

Software Engineering schafft
gute Code-Qualität

Kryptographie garantiert Sicherheit,
wenn der Programmcode fehlerfrei ist.

Software Engineering schafft
gute Code-Qualität

Aber, sind die Fehler, die SE vermeidet
dieselben Fehler, die Sicherheit kosten?

Was steht über Sicherheit in der Spezifikation?

Kryptographie garantiert Sicherheit,
wenn der Programmcode fehlerfrei ist.

Verifikation beweist, dass die Spezifikation erfüllt ist

Kryptographie garantiert Sicherheit,
wenn der Programmcode fehlerfrei ist.

Verifikation beweist, dass die Spezifikation erfüllt ist

Sind die Spezifikationen vollständig?
Was verifiziert man bei einem OS?

Implizieren die Eigenschaften, die verifiziert werden Sicherheit?

Security ist **C**onfidentiality, **I**ntegrity und **A**vailability

Kryptographie modelliert Availability nicht.

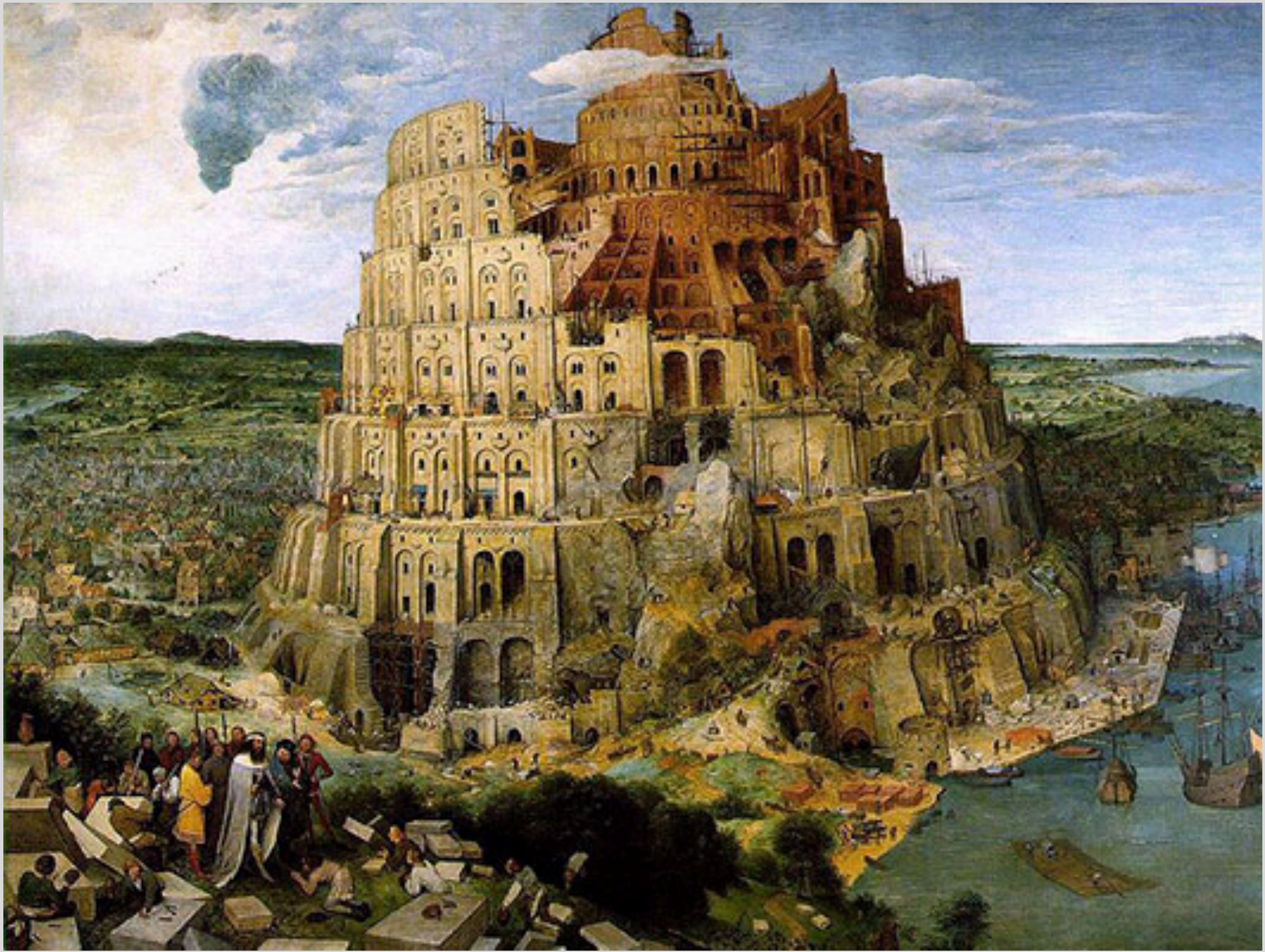
Security ist **C**onfidentiality, **I**ntegrity und **A**vailability

Kryptographie modelliert Availability nicht.

Was bedeutet CIA für datenschutzkonforme Überwachung?

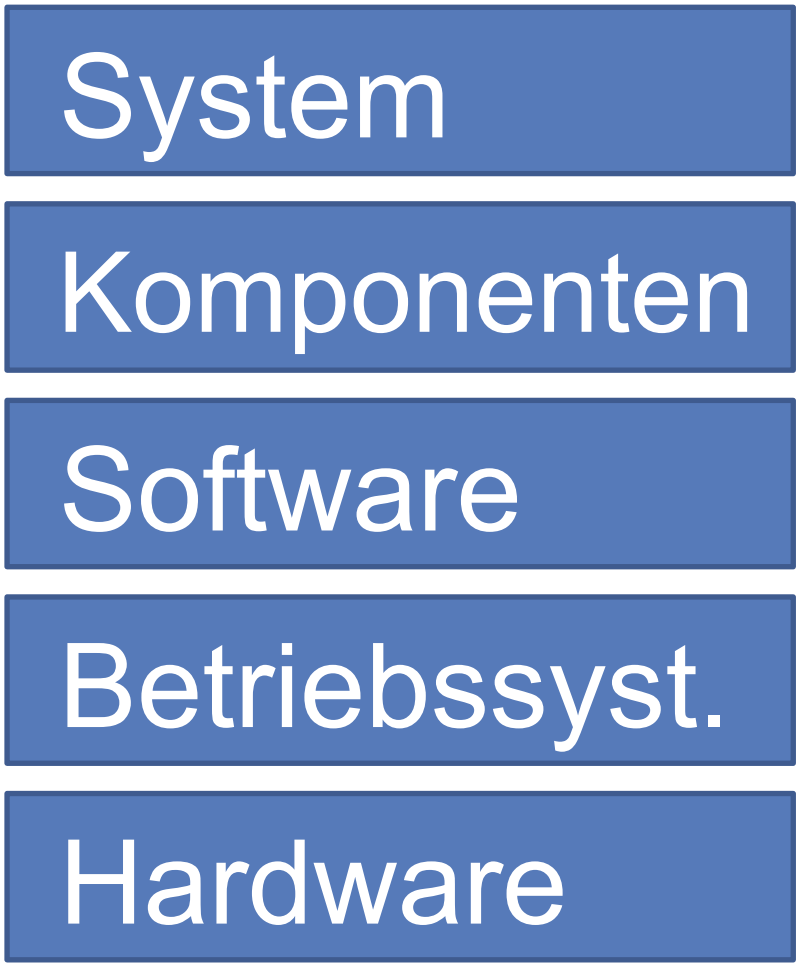
Was bedeutet CIA für Cloud Computing?


Freedom from risk or danger
Sicherheit
Simulatability
Deniability
Confidentiality
Integrity
Availability
Absence of Information Flow
Game Based
Incoercibility
IND-CCA2
UC/c
UC
Indistinguishability from an Ideal Specification



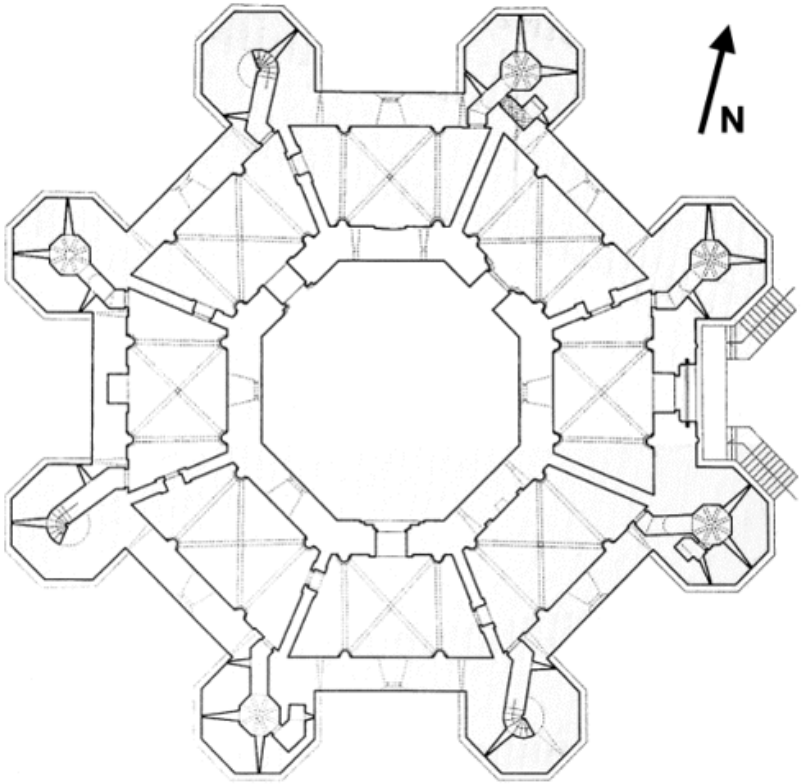
KASTEL

Systemsicherheit



Architekturbasierte Sicherheit

Wir sichern die Anwendung auf Architekturebene



Separation of Duties

Need to know Prinzip

kleine unkorrumpierbare Anker

Aber

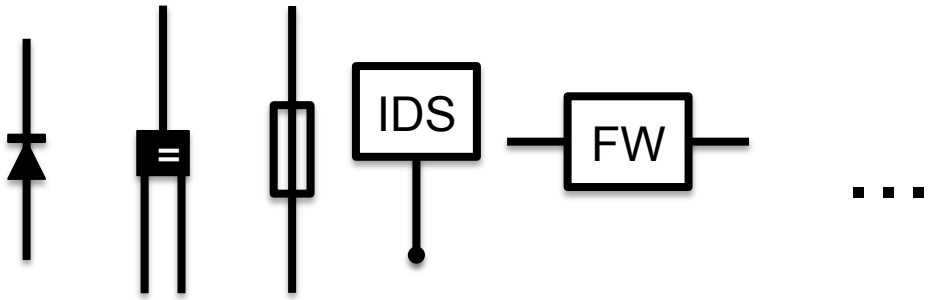
Anwendungsspezifisch

Nicht durch den Kunden prüfbar

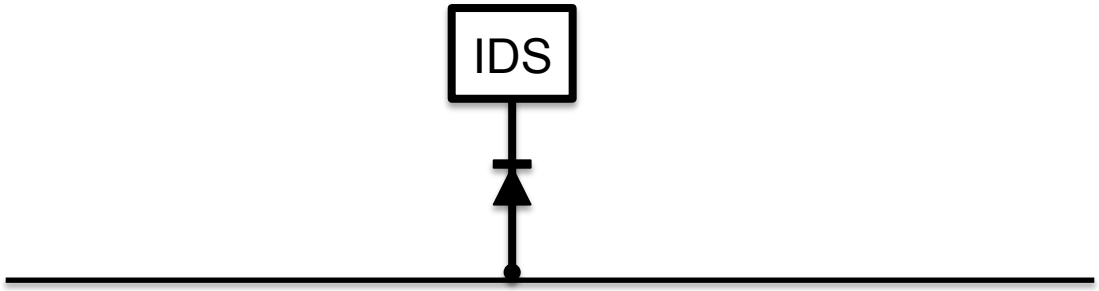
Auditable Security?

Architekturbasierte Sicherheit

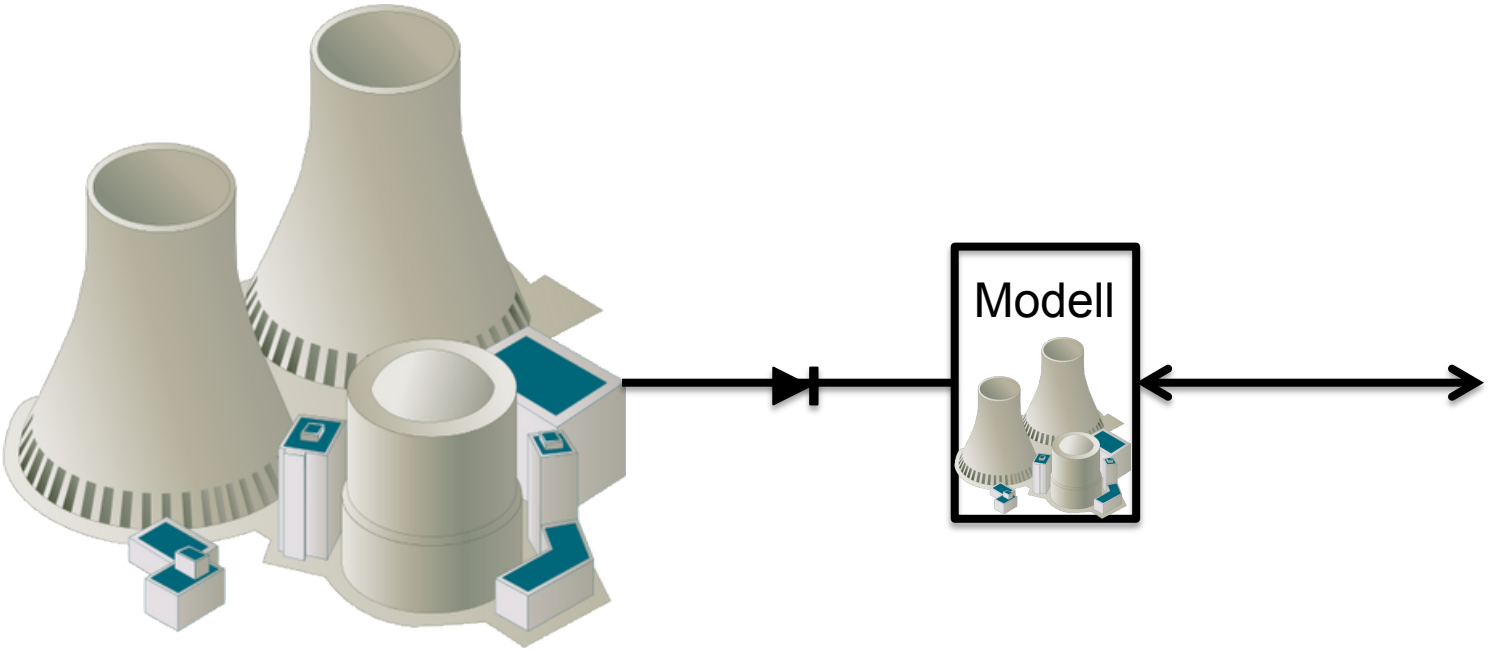
Grundprinzip:
Zerteilen in Module mit Separation of Duties und need to know.



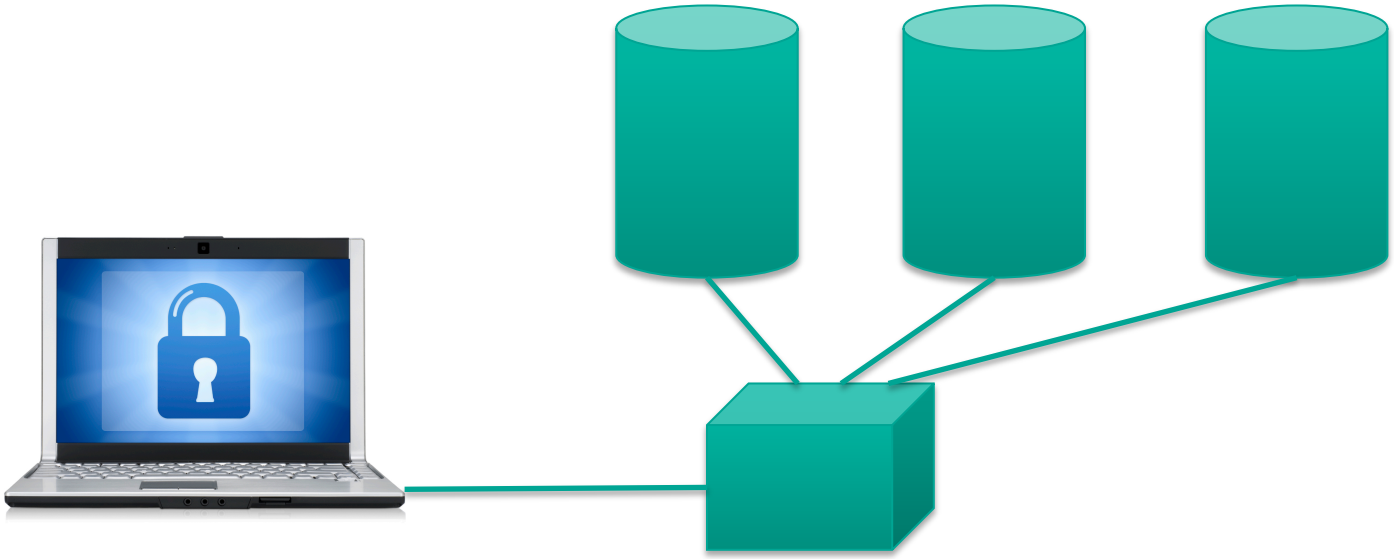
Modellierung wie MPC, aber realistische Korruption von Maschinen



Ferndiagnose eines Kraftwerks

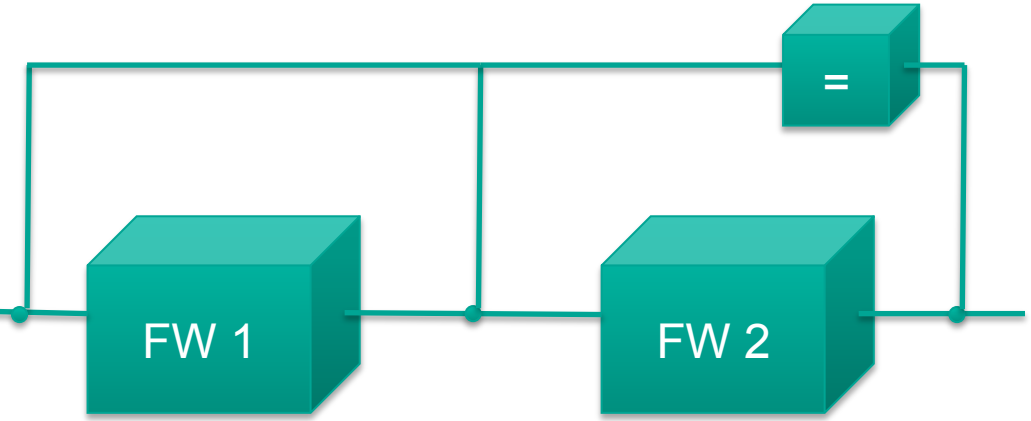


Aufteilen einer Datenbank



Nicht die Einträge, sondern die Zusammenhänge werden geschützt

Einer Firewall misstrauen



Ist beweisbar mindestens so sicher wie die unkorrumpierte Firewall

Vorteile

- Geeignet für komplexe Systeme (aber anwedungsspezifisch)
- Übertragbar auf Softwaremodule, Integrierbar in bestehende Systeme
- Gemeinsame Abstraktionsebene mit der Softwaretechnik => bessere Einbindung in den Entwicklungsprozess (durchgängige Entwicklung)
- Zerteilen in einfache Module: Komplexität wird beherrschbar. Die Systemsicherheit lässt sich auf die Sicherheit der Module zurückführen.
- **Verständlich, überzeugend und mathematisch fundiert**


W 10X
10X
NOVEX
HOLLAND


W 10X
10X
NOVEX
HOLLAND

System of Systems

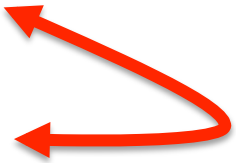
System

Komponenten

Software

Betriebssyst.

Hardware



Ein Problem für die Zukunft:

Emergente Effekte

Unvollständige Spezifikation...