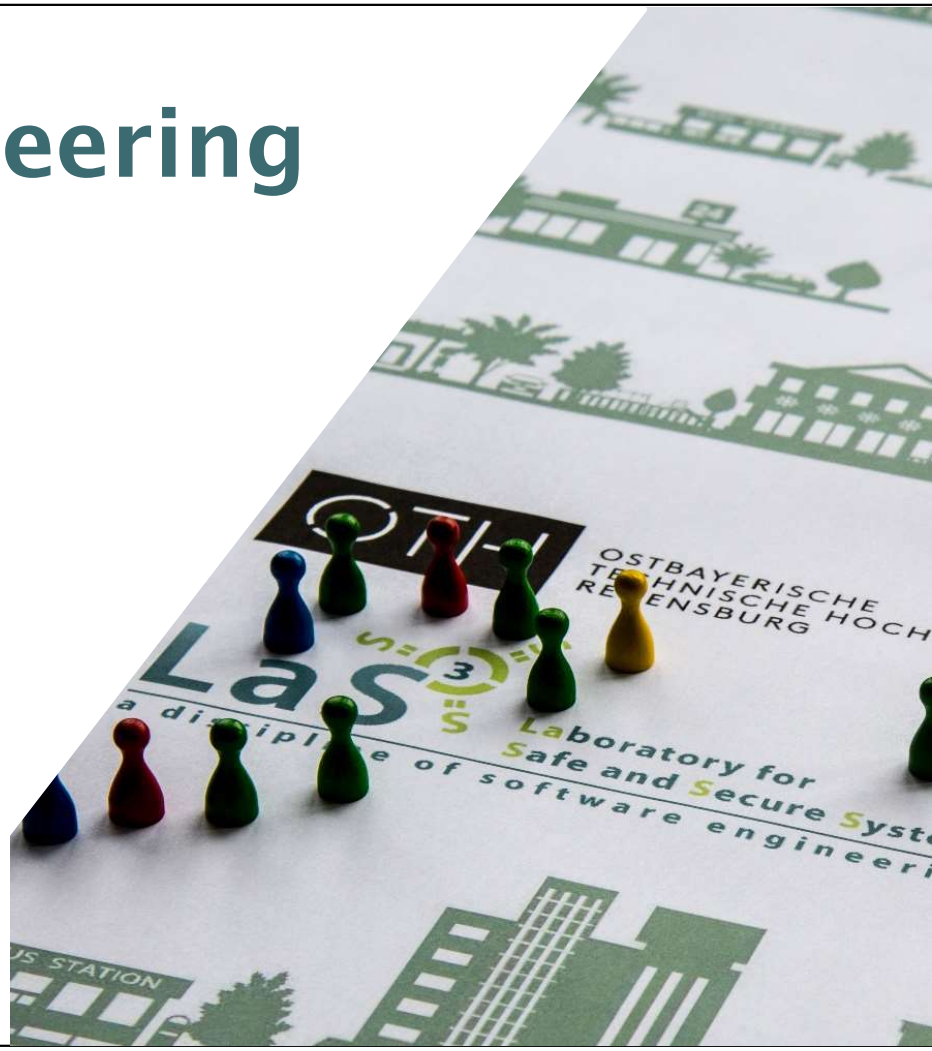
Vorlesung Software Engineering sicherer Systeme

6. Safety und Security

Prof. Dr. Jürgen Mottok



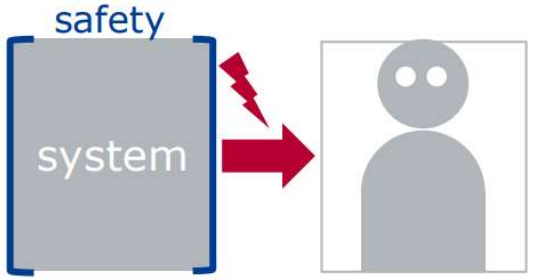
Inhalte der Vorlesung

1. Einführung und Motivation und Definition von Software Engineering
2. Entwicklungsprozesse
3. Requirements Engineering
4. UML
5. Design Pattern
6. **Safety und Security**
    1. Grundlagen
    2. Bedrohungsmodellierung
    3. Funktionale Sicherheit
    4. IT-Sicherheit
7. Software Test

Unterscheidung Safety und Security

(Functional) Safety is an intrinsic property of a system that performs in a way that does not present an unreasonable risk of injury to operators or bystanders.

- Mit Safety ist die Betriebssicherheit gemeint, also der Schutz von Mensch und Umwelt

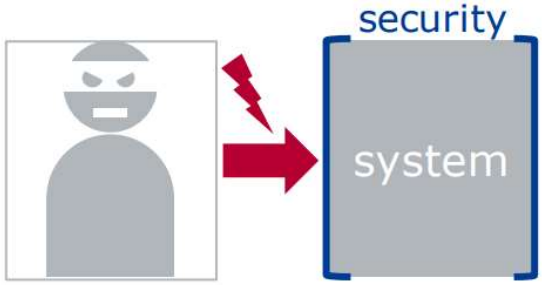


Functional safety System must not cause hazards probably leading to harm of persons

Quelle: Vector Informatik GmbH

Security is an intrinsic property of a system that protects itself against intended abuse by an attacker.

- Security hingegen meint den Schutz der Daten (Informationssicherheit)



Security System must neither be influenced nor abused by any attacker

Quelle: Vector Informatik GmbH

Safety und Security - Grundlagen

Kultur – auch im Normenumfeld als Gelingensbedingung

- **Compare Safety Culture in:**

V.Gebhard, G.M. Rieger, J. Mottok, C. Gießelbach:
Funktionale Sicherheit nach ISO 26262:
Ein Praxisleitfaden zur Umsetzung. dpunkt Verlag, 2012

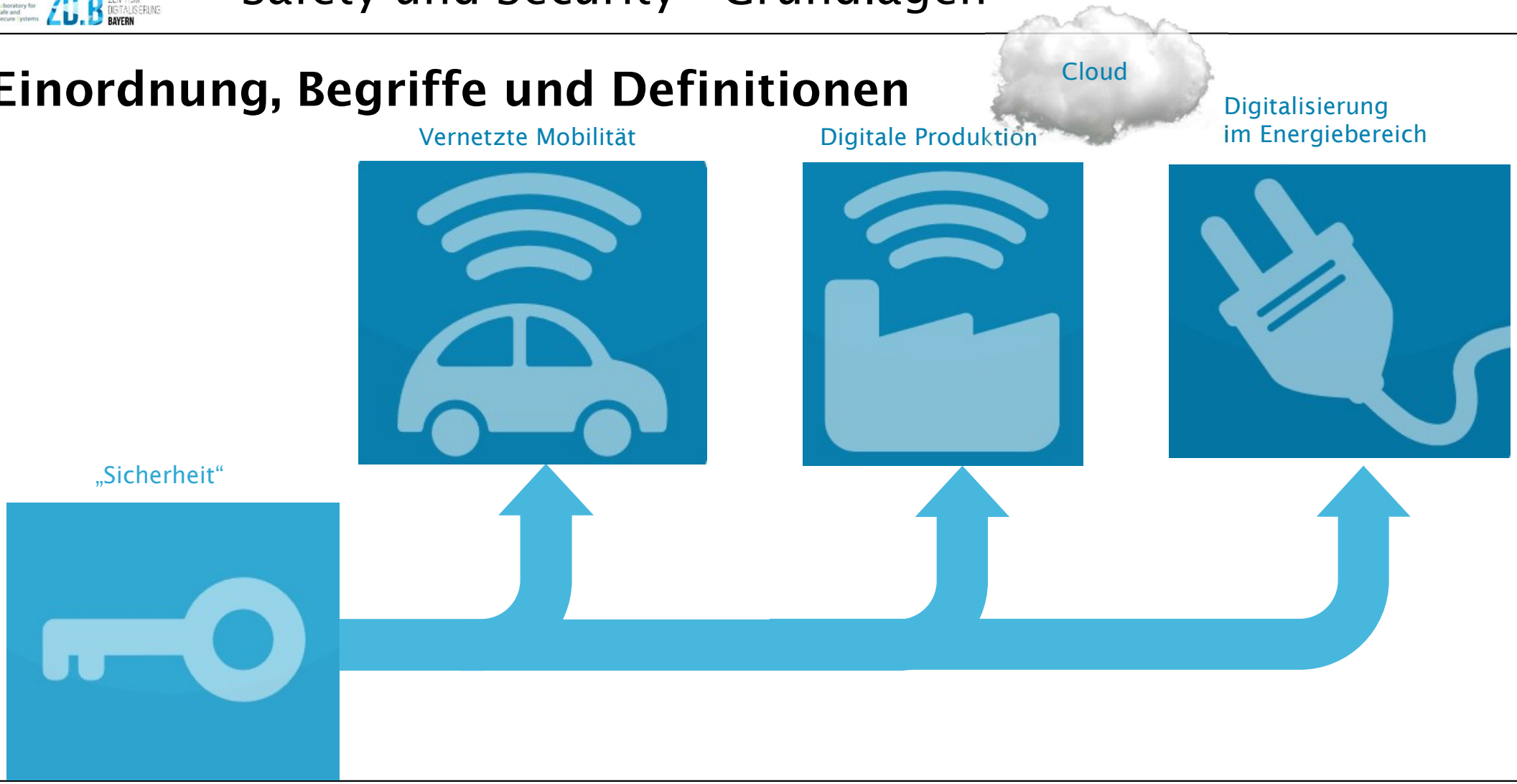
- **Compare Security Culture in:**

Frank Simon, Jürgen Grossmann, Christian Alexander Graf,
Jürgen Mottok, Martin A. Schneider:
Basiswissen **Sicherheitstests**, Aus- und Weiterbildung zum ISTQB® Advanced Level Specialist
– Certified **Security Tester**. dpunkt.verlag, 2019

- **Compare Modeling Culture in:**

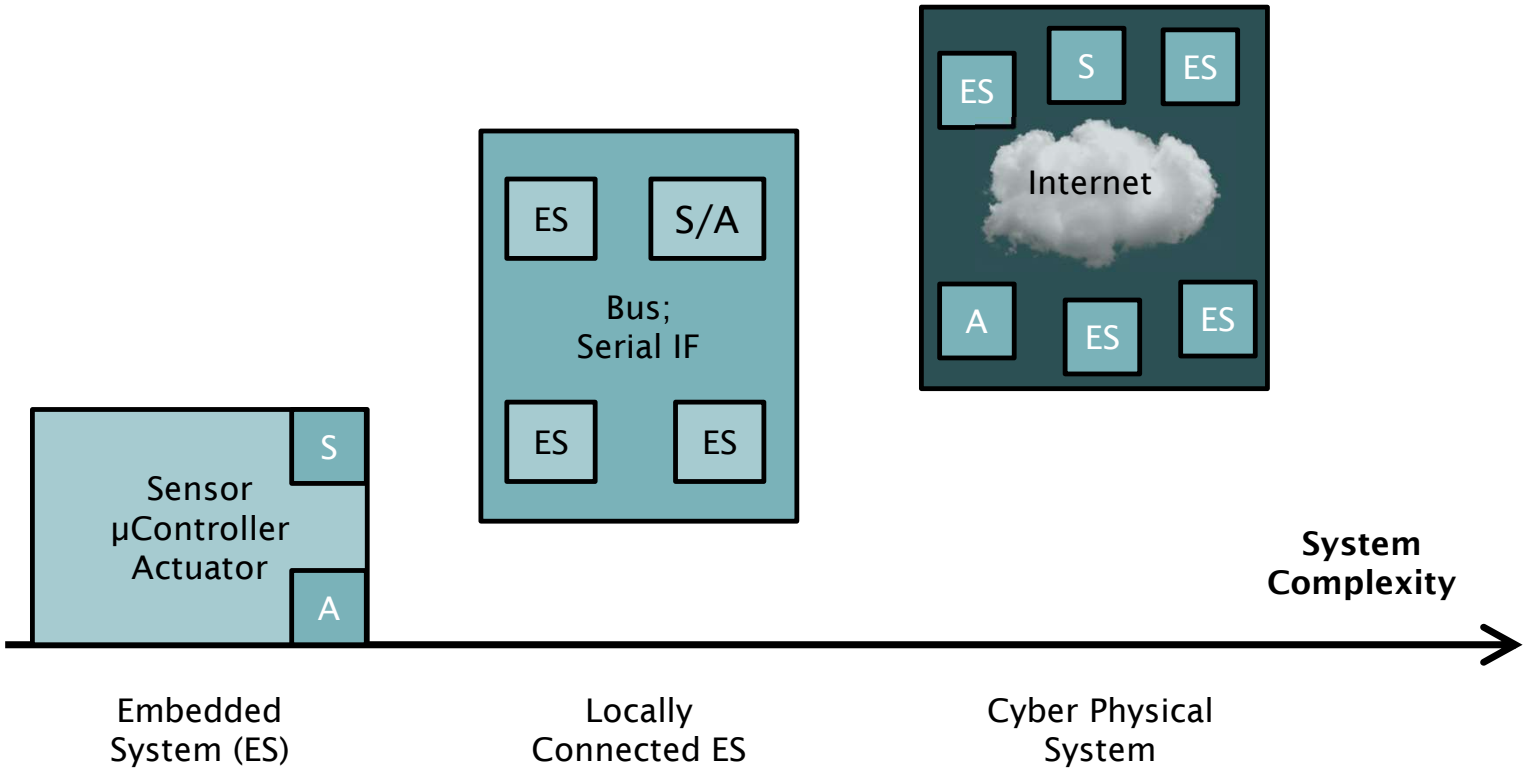
Tim Weilkiens, Alexander Huwaldt, Jürgen Mottok, Stephan Roth, Andreas Willert:
Modellbasierte Softwareentwicklung für eingebettete Systeme verstehen und anwenden. dpunkt Verlag, 2018

Einordnung, Begriffe und Definitionen



Einordnung, Begriffe und Definitionen

Von eingebetteten Systemen zum Cyber Physical System (CPS)



Vernetzte Mobilität

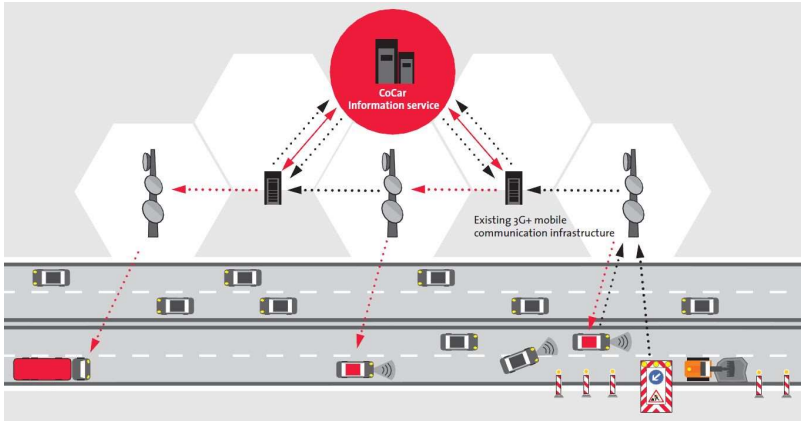
Digitalisierung im Energiebereich

Digitale Produktion

Einordnung, Begriffe und Definitionen

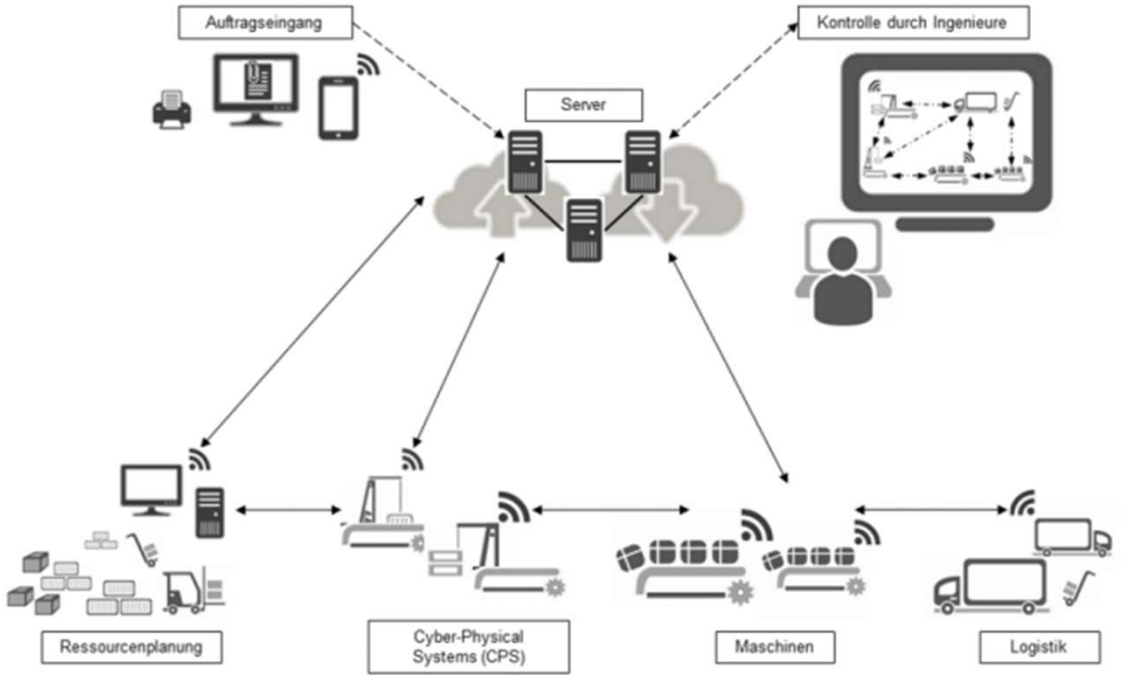
Cyber Physical System (CPS) überall

Vernetzte Mobilität (Car2Car, Car2X)



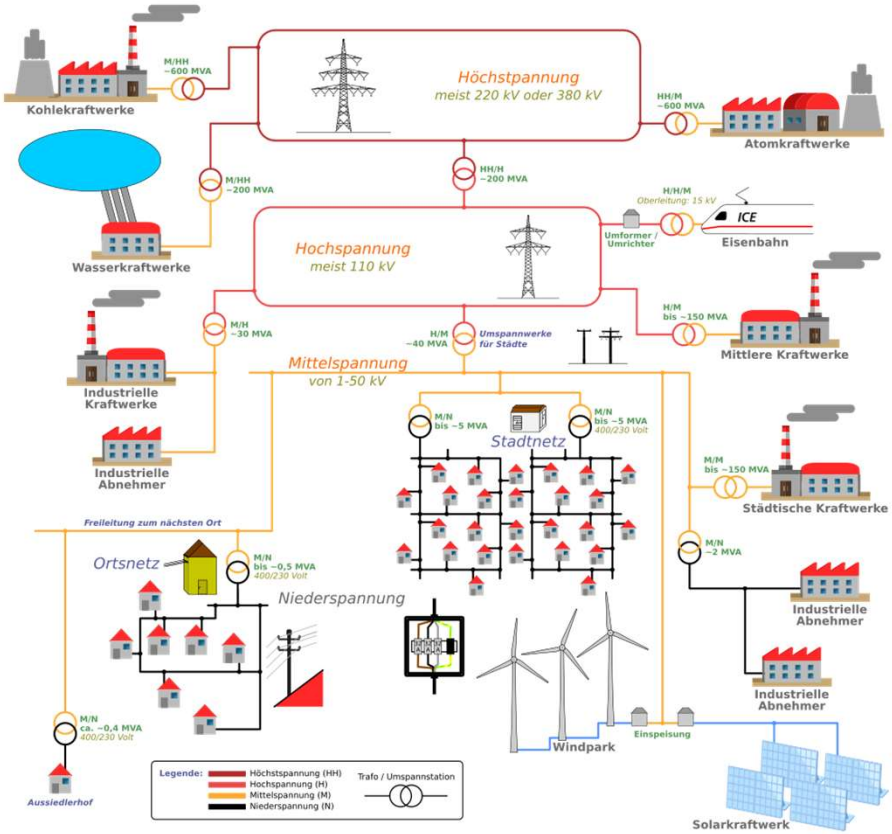
http://amicale-citroen.de/wp-content/uploads/2011/08/2011.cocar-01.jpg

Digitale Produktion



Safety und Security - Grundlagen

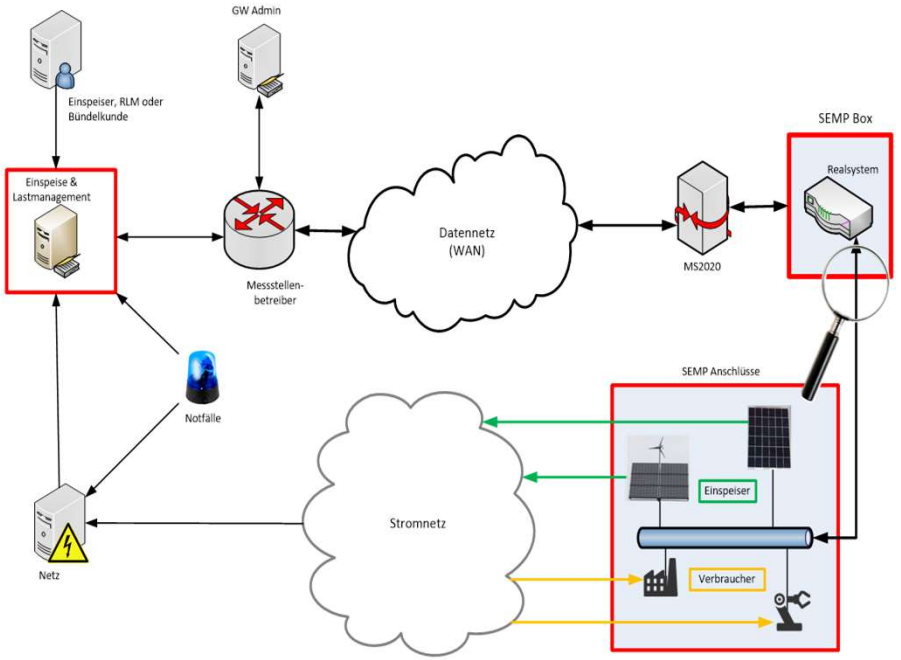
Einordnung, Begriffe und Definitionen



Quelle: https://de.wikipedia.org/wiki/Stromnetz

Cyber Physical System (CPS) überall

Digitalisierung im Energiebereich
Smart Energy Management Program
Projekt des LaS³



Einordnung, Begriffe und Definitionen

Sichere und zuverlässige dezentrale Systeme

Die vier Bedeutungen der Sicherheit

Funktionale Sicherheit (Functional Safety)

- Übereinstimmung der realisierten Ist-Funktionalität der Komponenten mit der Soll-Funktionalität (funktionstreue d.h. **Sicherheit vor Fehlern**)

IT-Sicherheit, Informationssicherheit (IT Security)

- Eigenschaft eines funktionssicheren Systems, nur solche Systemzustände anzunehmen, die zu keiner **unautorisierten Informationsveränderung oder -gewinnung** führen (**Sicherheit vor Angriffen**).

Datensicherheit (Protection)

- Eigenschaft eines funktionssicheren Systems, nur solche Systemzustände anzunehmen, die zu keinem **unautorisierten Zugriff auf Systemressourcen** und insbesondere auf Daten führen (auch Maßnahmen zur Datensicherung, Backup).

Datenschutz (Privacy)

- Fähigkeit einer natürlichen Person, die **Weitergabe von Informationen**, die sie persönlich betreffen, zu **kontrollieren** (Bundesdatenschutzgesetz).
  ⇨ Technologiefolgen-Abschätzung
  ⇨ Ethische Fragen und gesellschaftliche Akzeptanz


Claudia Eckert, IT-Sicherheit, Oldenbourg, 2006.

Einordnung, Begriffe und Definitionen

Sichere und **zuverlässige** dezentrale Systeme

Zuverlässigkeit (Reliability)

Die Zuverlässigkeit eines technischen Produkts oder Systems ist eine Eigenschaft (Verhaltensmerkmal),

die angibt, wie verlässlich eine dem Produkt oder System zugewiesene Funktion in einem Zeitintervall erfüllt wird.

Josef Börcsök, Funktionale Sicherheit, Hüthig Verlag, 2006.

Einordnung, Begriffe und Definitionen

Sichere und zuverlässige **dezentrale Systeme**

Dezentrales System (verteiltes System)

Verteiltes System
Ansammlung unabhängiger Computer, die dem Benutzer wie ein einzelnes kohärentes System erscheint.

Ein verteiltes System ist ein System, in dem sich HW- od. SW-Komponenten auf vernetzten Computern befinden und nur über den Austausch von „Nachrichten“ kommunizieren und ihre Aktionen koordinieren:

- Nebenläufigkeit der Programmausführung
- Keine globale Uhr -> es gibt kein globales Konzept einer genauen Uhr (da Kommunikation ausschließlich über das Senden von Nachrichten erfolgt), aber Uhrensynchonisation
- Unabhängige Ausfälle -> jede Komponente des Systems kann unabhängig von den anderen ausfallen, während die anderen weiterhin funktionieren (und womöglich lange od. überhaupt nie etwas davon merken).

Ziel ist die gemeinsame Nutzung von Ressourcen (HW u. SW).


George Coulouris, Verteilte Systeme, Addison-Wesley, 2002.

Einordnung, Begriffe und Definitionen

Sichere und zuverlässige **dezentrale Systeme**

Dezentrales System (verteiltes System)

Dezentrale Algorithmen

- Kein Computer hat vollständige Informationen über den Systemstatus.
- Computer entscheiden nur aufgrund lokaler Information.
- Der Ausfall eines Computers schädigt nicht den Algorithmus.
  ⇨ Vortrag Fehlertoleranz
- Es wird nicht implizit angenommen, dass es eine globale Uhr gibt.

George Coulouris, Verteilte Systeme, Addison-Wesley, 2002.

Fragen?

OSTBAYERISCHE TECHNISCHE HOCHSCHULE REGENSBURG
Laboratory for Safe and Secure Systems
ZENTRUM DIGITALISIERUNG. BAYERN