Summary of Lecture 08.01.2020

http://englishskills.se

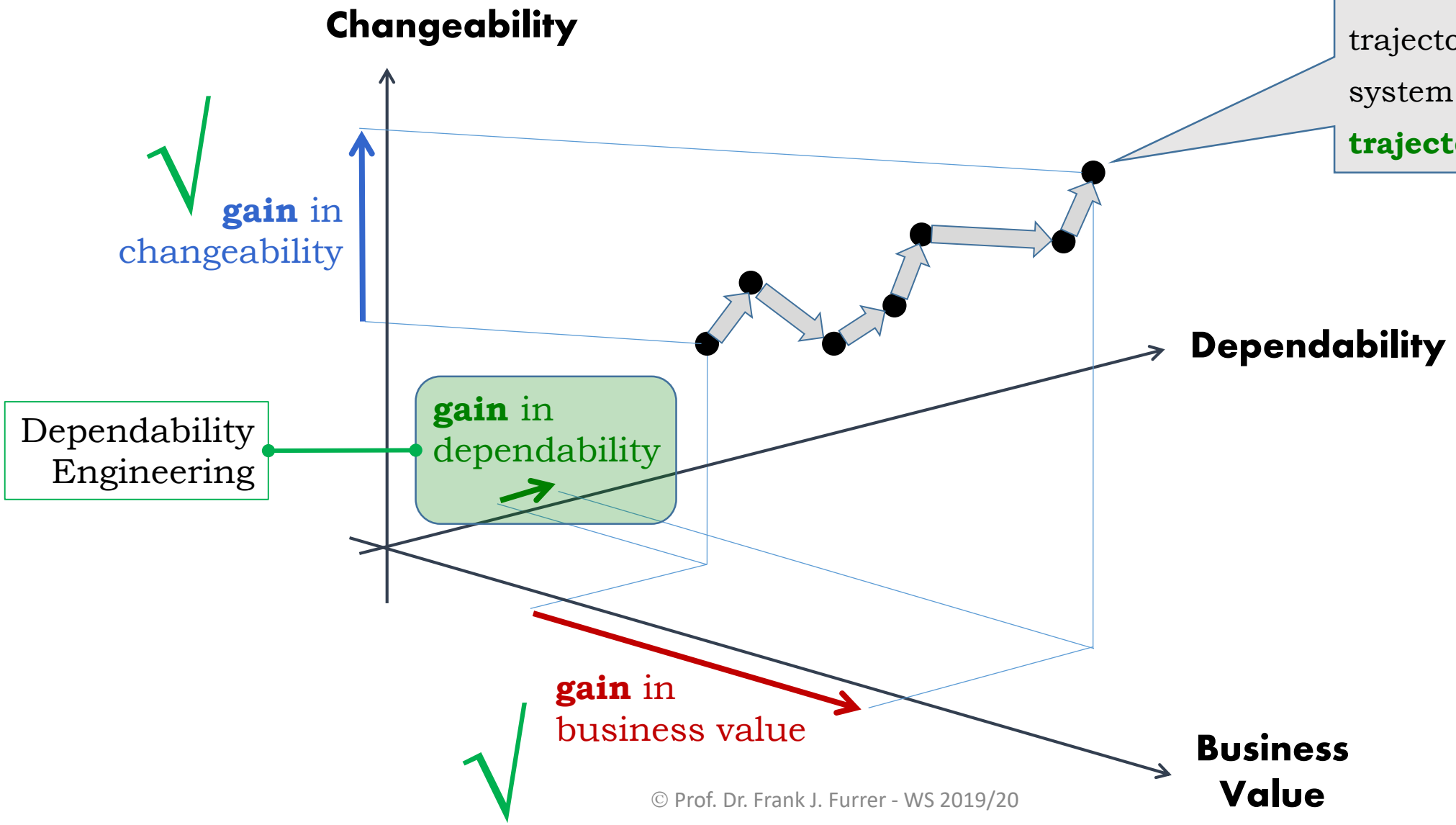
... Very condensed summary of the 08.01.2020 lecture

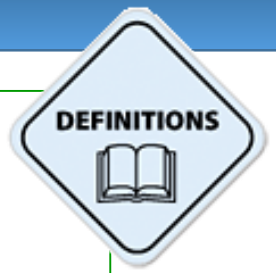
https://de.fotolia.com

Summary 08.01.2020

Evolution Trajectory = Sequence of Projects

A sequence of projects builds a transformation trajectory of the IT system (= the **evolution trajectory**)





Architecting for Dependability:

Defining and implementing an **IT-structure** providing the optimum defense against incidents, based on a *risk management methodology* and on proven *dependability architecture/ design principles*

https://www.npmjs.com

Dependability Engineer:

Responsible for the resilience engineering *process* in a company

	Dependability Principles & Patterns

Summary 08.01.2020

Dependability

Resilience

Resilience Principles:
Valid for **all** Systems

- R1: Policies
- R2: Vertical Architectures
- R3: Fault Containment Regions
- R4: Single Points of Failure
- R5: Multiple Lines of Defense
- R6: Fail-Safe States
- R7: Graceful Degradation
- R8: Dependable Foundation (Infrastructure)
- R9: Monitoring

Domain-specific Properties

Safety

http://pb-attorneys.com

Security

… etc.

Summary 08.01.2020

R1: Policies

Policy =
The set of *basic principles* and *associated guidelines*, formulated and enforced by the governing body of an organization, to direct and limit its actions in pursuit of ***long-term goals***

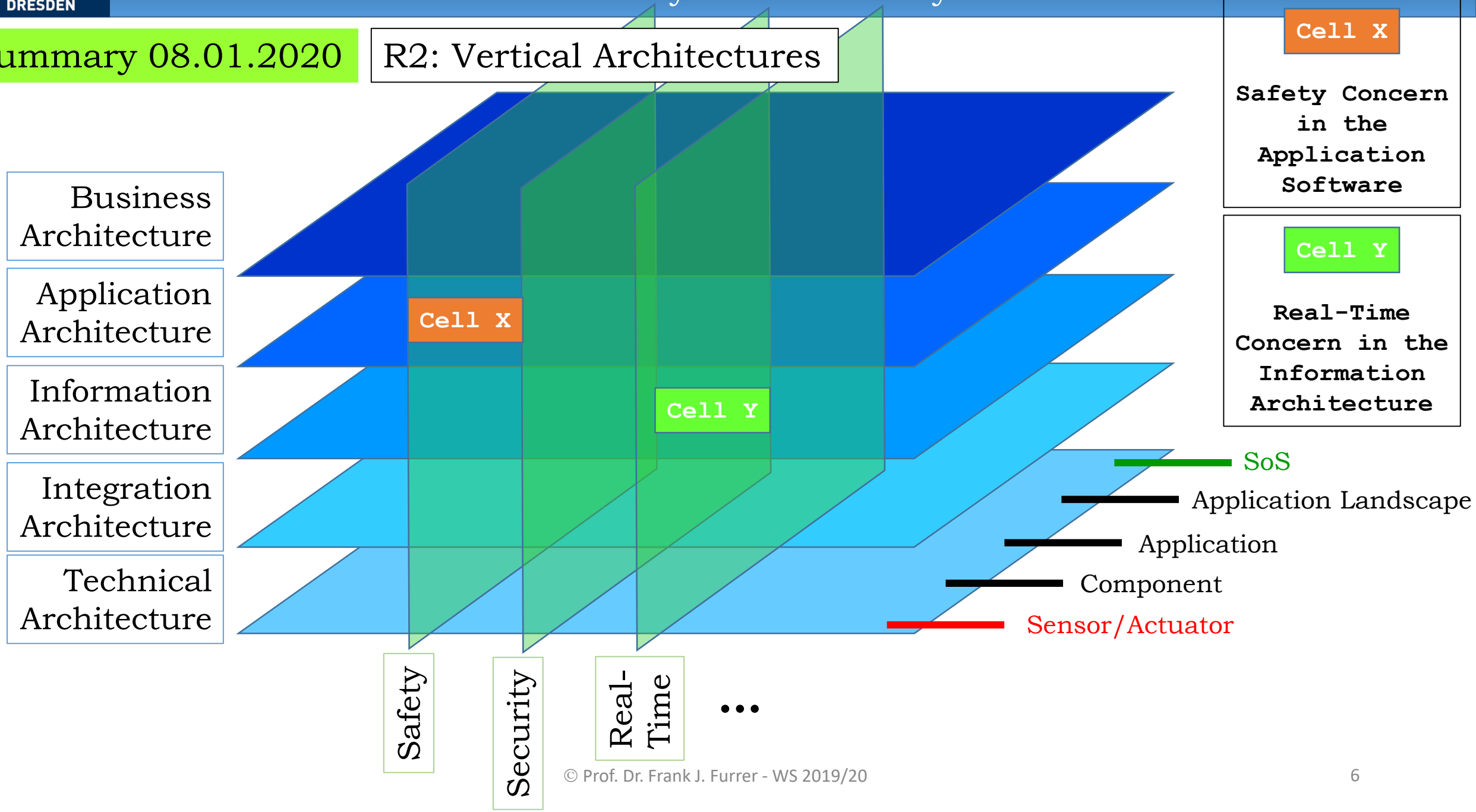
http://www.businessdictionary.com/definition/policy.html

Good policies guide the course of a company
in all relevant areas
towards sustainable success

Good policies are a great help for the people implementing company objectives, especially ***infrastructure projects***

Summary 08.01.2020

R2: Vertical Architectures



Summary 08.01.2020

R2: Vertical Architectures

Cell X = **Safety Concern in the Application Software**

Architecture Framework Cells =

Allow assignment, structuring, and separating of the functionality and of the quality properties of IT-systems to enable partitioning and life-cycle management.

⇒ **Formulation of Powerful Set of Architecture Principles**,

e.g.:

NEVER implement security functionality in the applications software

… but only allow calls to the security functionality

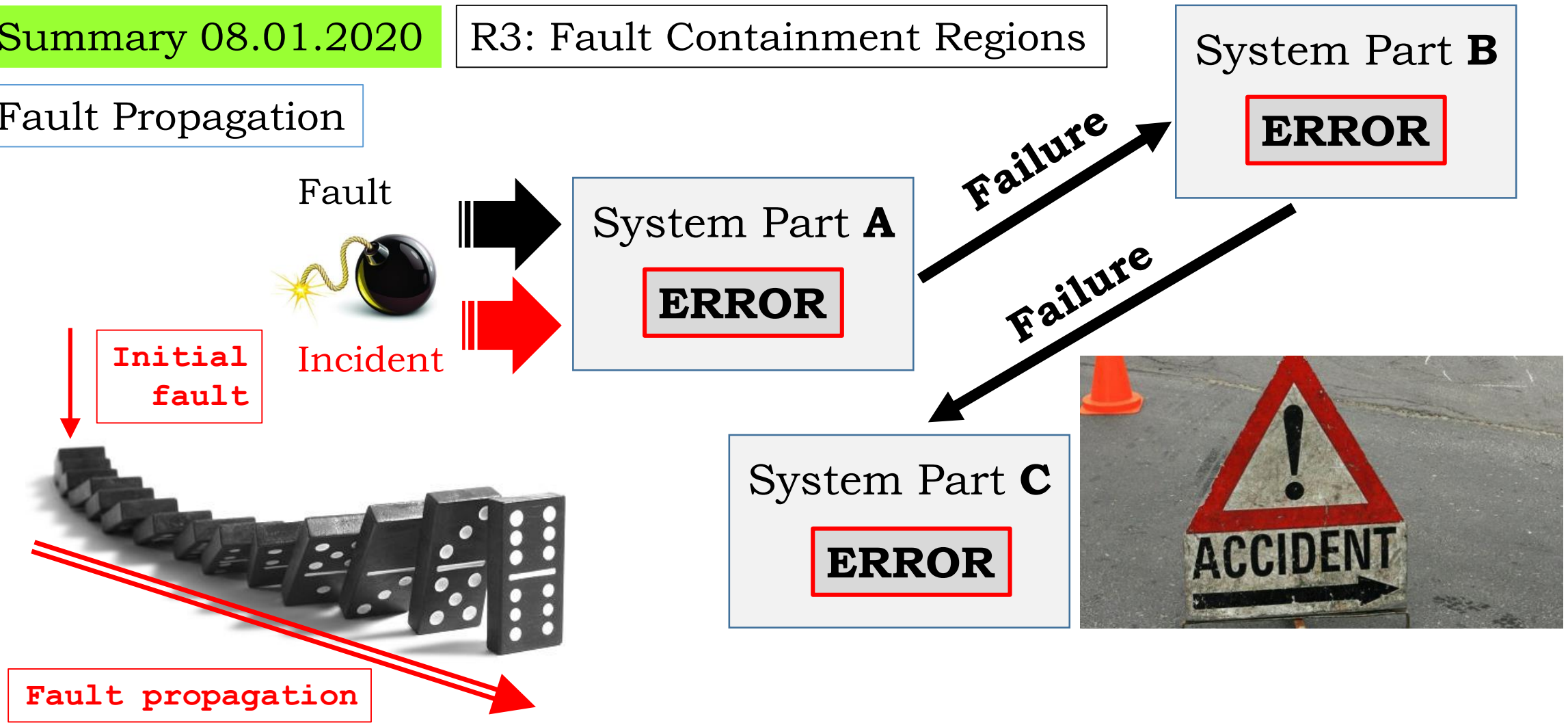
https://www.npmjs.com

«Canon of Orthogonality»

Summary 08.01.2020

R3: Fault Containment Regions

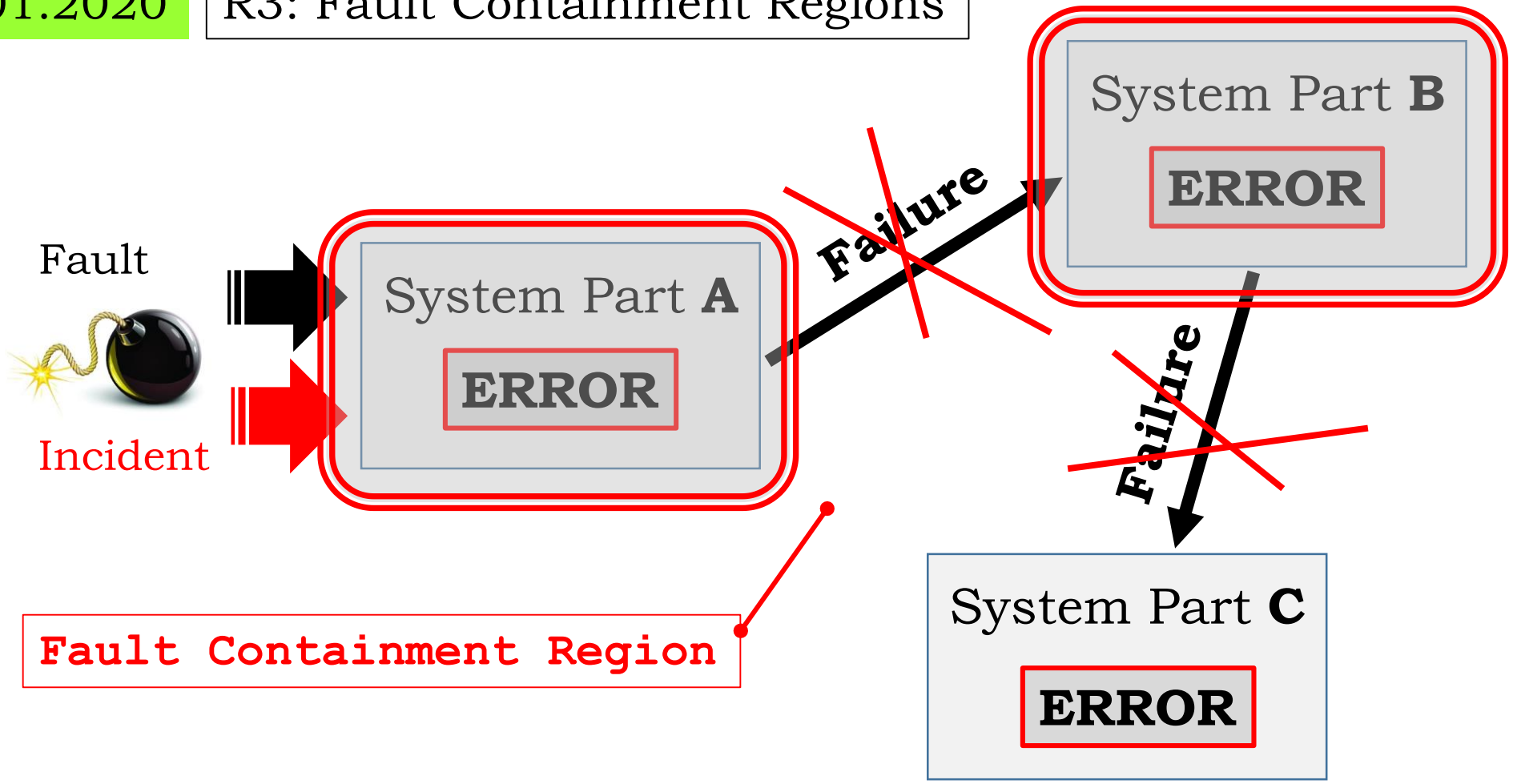
Fault Propagation



The consequences of a *fault* – the ensuing *error* – can **propagate** either by an erroneous message or by an erroneous output action of the faulty part

Summary 08.01.2020

R3: Fault Containment Regions

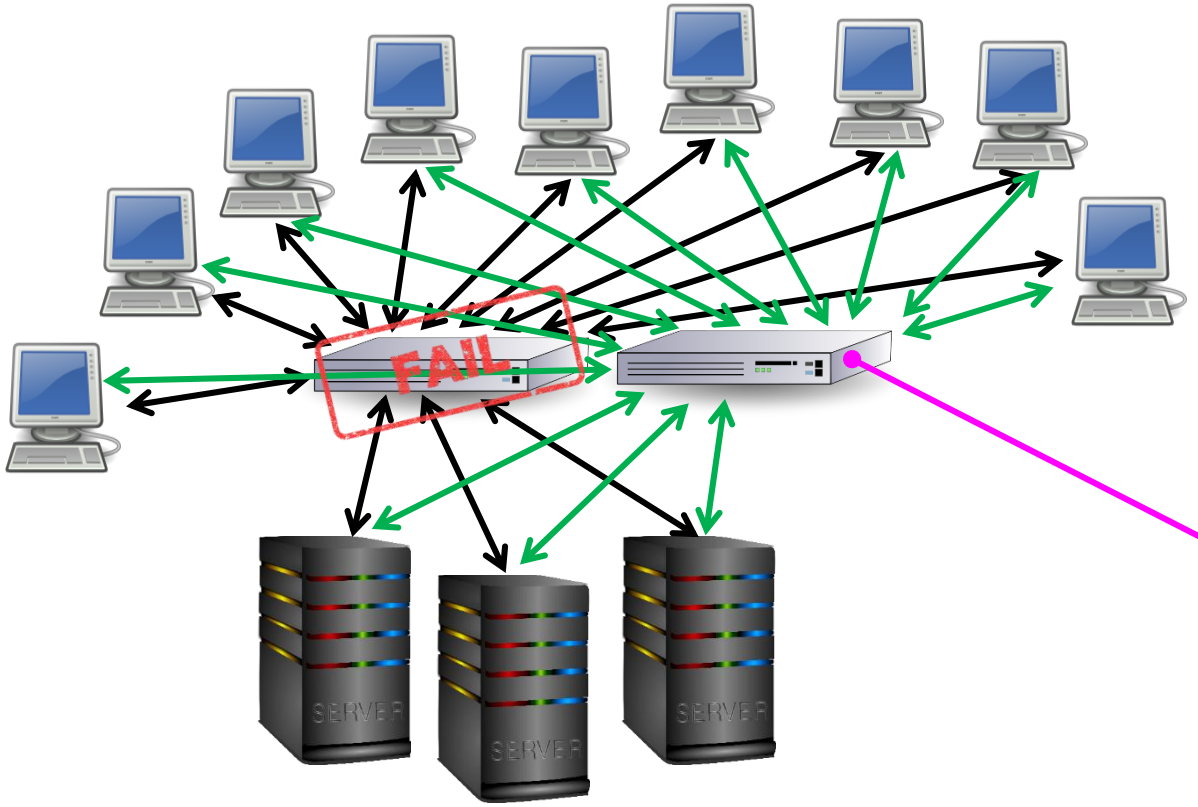


Build **error** propagation boundaries around each system part

Summary 08.01.2020

R4: Single Points of Failure

A single point of failure (SPOF)
is a part of a system that,
if it *fails*,
will stop the *entire* system from working

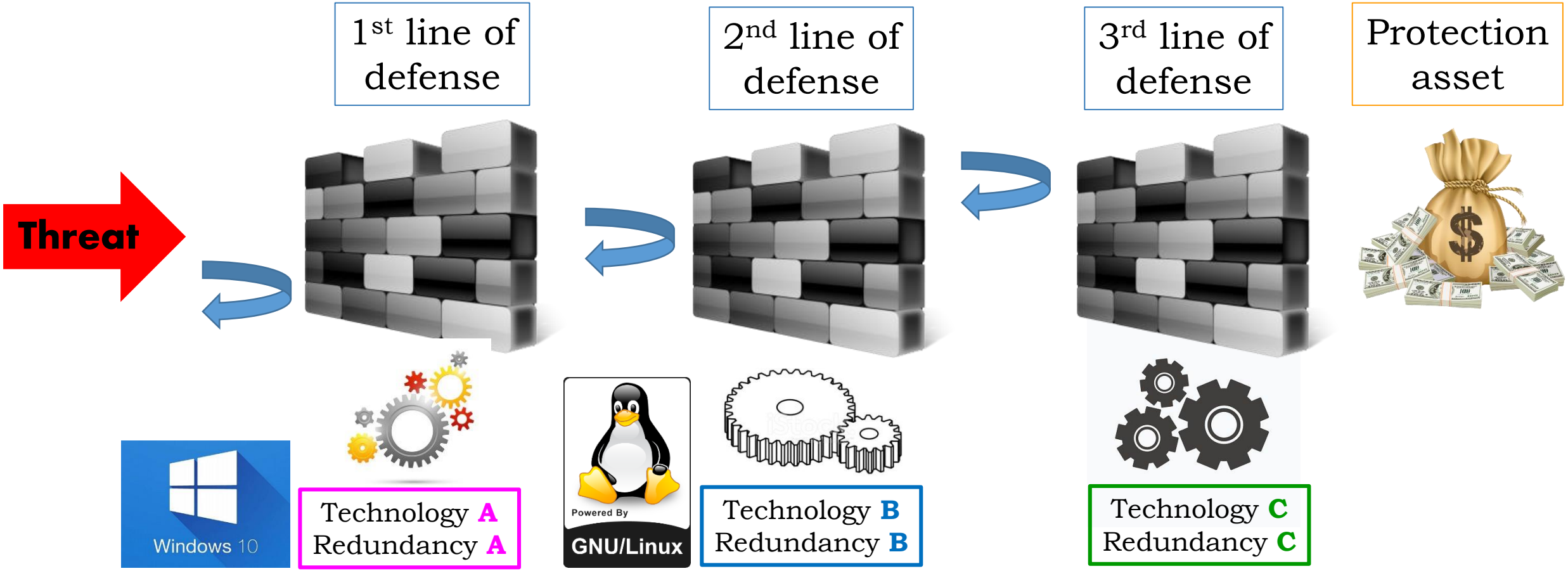


Redundancy eliminates SPOF

Summary 08.01.2020

R5: Multiple Lines of Defense

Multiple lines of defense represents the use of *multiple* computer techniques to help mitigate the risk of one component of the defense being compromised or circumvented



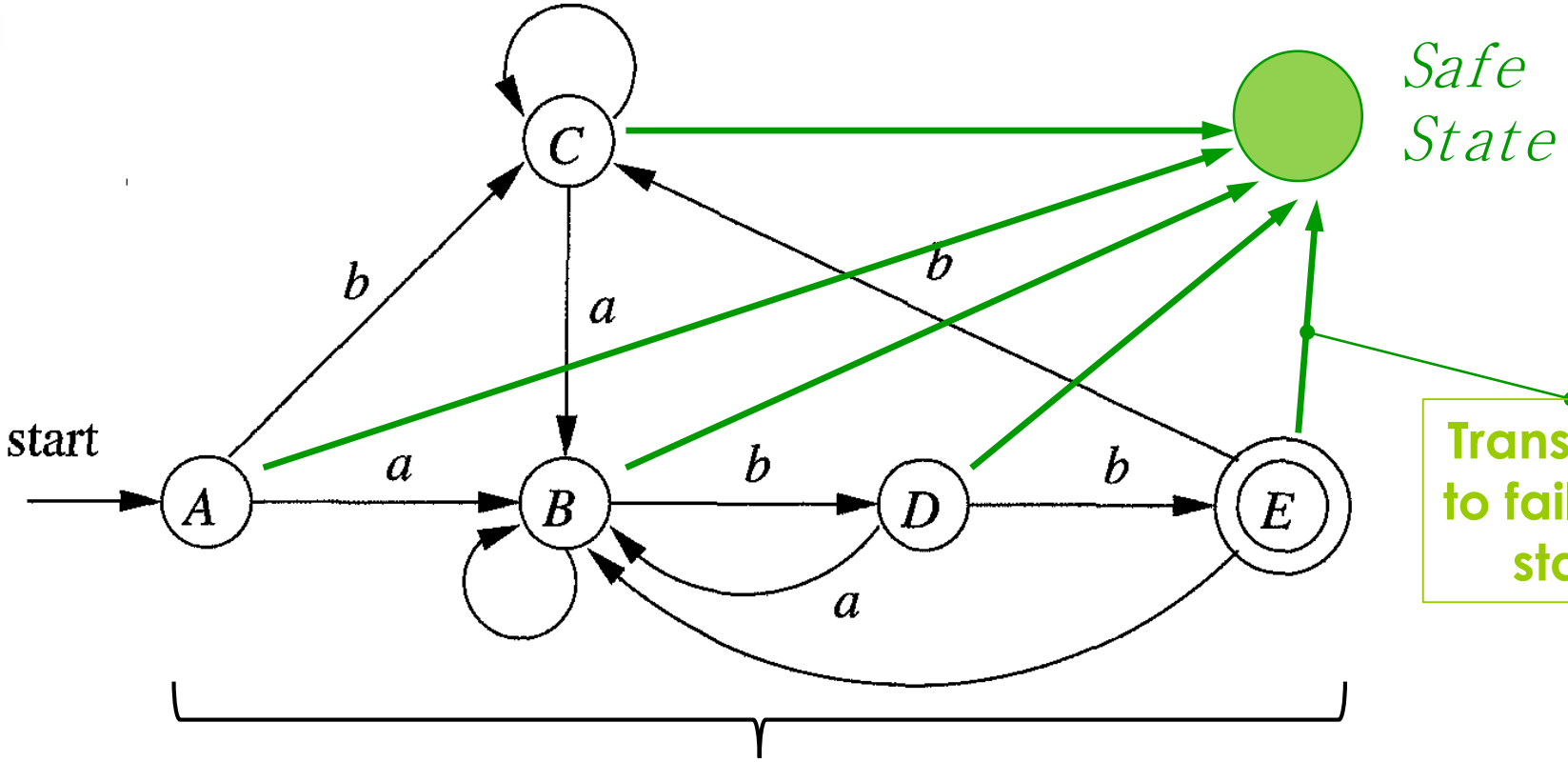
Summary 08.01.2020

R6: Fail-Safe States

https://media.licdn.com

Fail-safe means that a system will not endanger lives or property when it fails.

It will go into a *fail-safe state* and stop working.



Safe State

Which is a safe state?

How can we find a safe state?

Transitions to fail-safe state

Difficult Engineering Task

https://img.clipartxtras.com

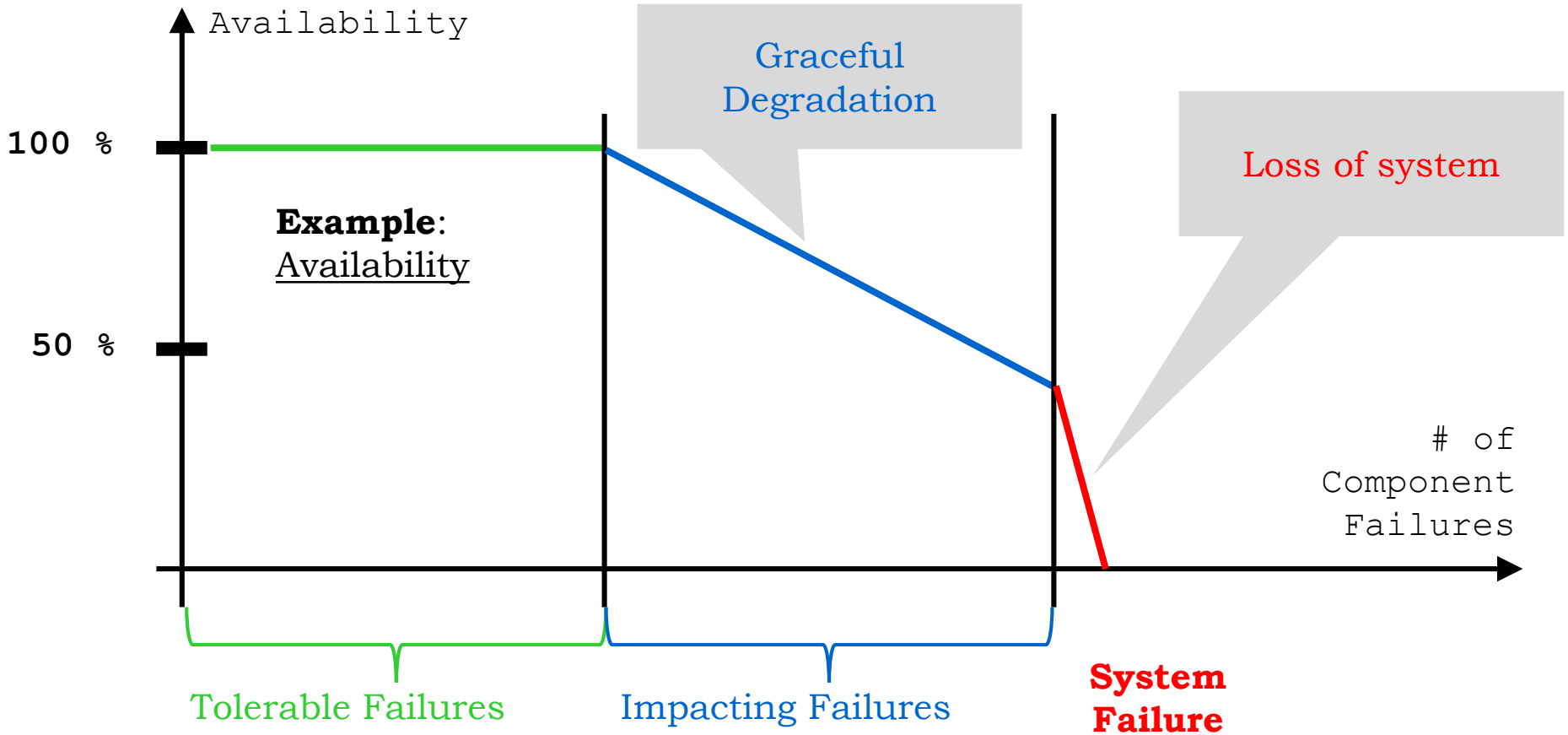
Summary 08.01.2020

R7: Graceful Degradation

DEFINITIONS

Graceful Degradation:

Property of a system to continue operation at some reduced level of **functionality**, **performance** or **dependability** after one or several of its components failed



Fault tolerance: Providing functionality or service that are consistent with its specification in spite of *faults*

⇒ **Redundancy**

Summary 08.01.2020

R8: Dependable Infrastructure

DEFINITIONS

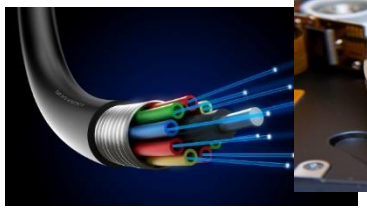
Resilience Infrastructure:
Set of proven resilience technologies and services supporting the dependability properties (availability, security, performance, …) of software systems

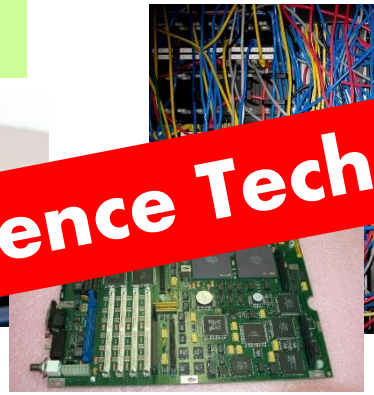
APPLICATIONS ⇒ Resilience Principles

Execution Infrastructure: ***System Software***

⇒ Resilience Technologies

Execution Infrastructure: ***System Hardware***



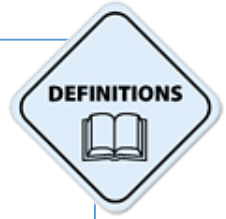


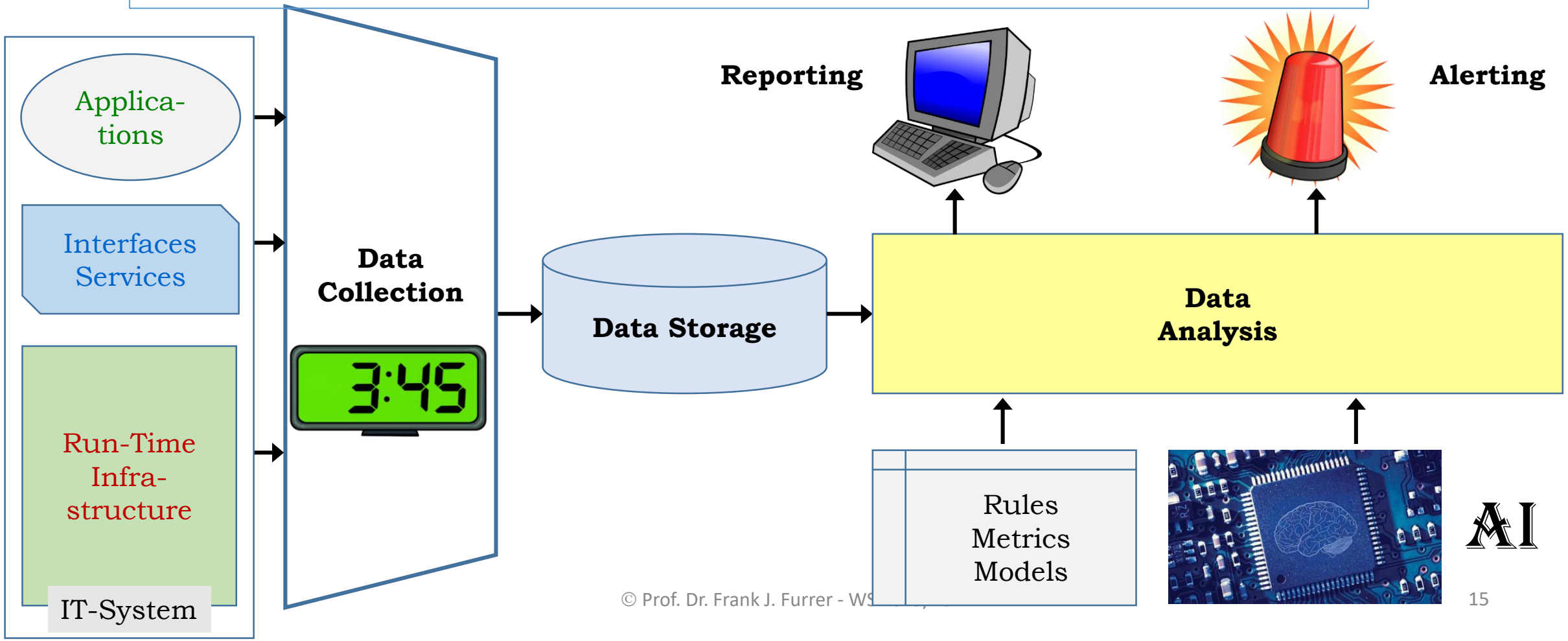
⇒ Resilience Technologies

Summary 08.01.2020

R9: Monitoring

An **IT system monitor** is a hardware and software component used to measure **run-time parameters and behavior**, such as resource consumption, performance, interfaces, applications, etc. in a computer system – reporting and alerting **anomalies**





Summary 08.01.2020

R9: Monitoring

What should be monitored ?

Technical Information

- **Network:** `Operational Parameters`
- **Infrastructure:** `Operational Parameters`
- **Interfaces/Services: Timing,** `Syntax & Semantics`
- **Configuration:** `Changes`

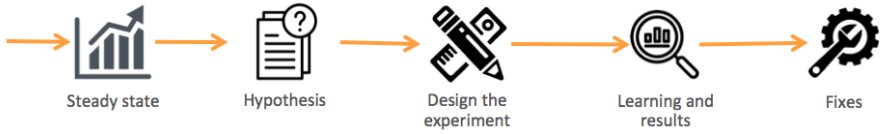
Business Information

- **Business KPI's:** `Statistics`
- **Applications:** `Operational Parameters`
- **Service Level Agreements:** `Operational Parameters`
- **Dependability Properties:** `Activity` & `Parameters`

Summary 08.01.2020

Chaos-Engineering

https://hub.packtpub.com



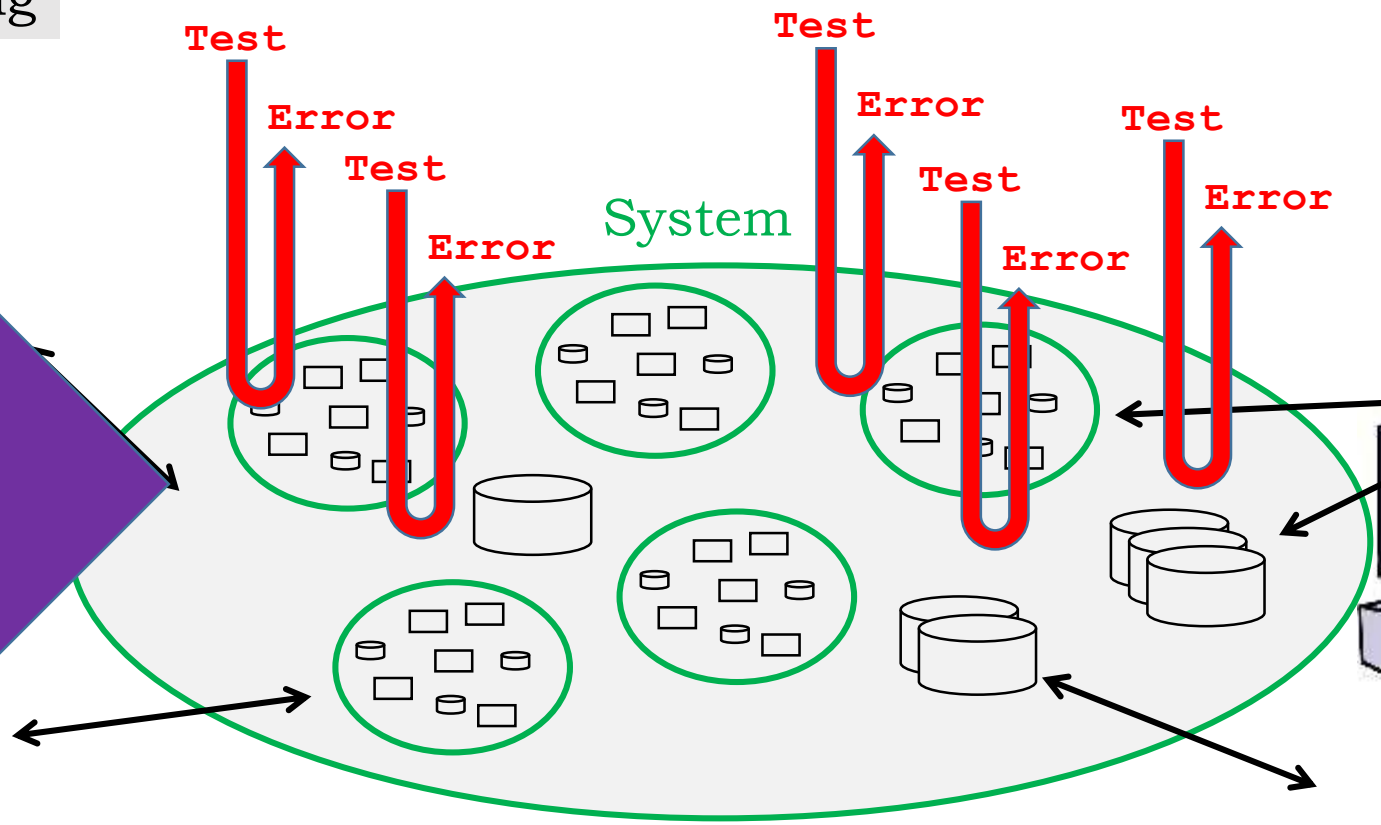
New methodology:
CHAOS-Engineering

Testing only shows the **presence** of errors
- never the **absence** of errors!

https://clipartstation.com

System Weakness

CHAOS
Engineering
Experiments



https://www.advanced-systemcare.org

Summary 08.01.2020

Dependability

Resilience

- ✓ SECURITY
- ✓ SAFETY
- ✓ Real-Time Capability

ain-specific properties

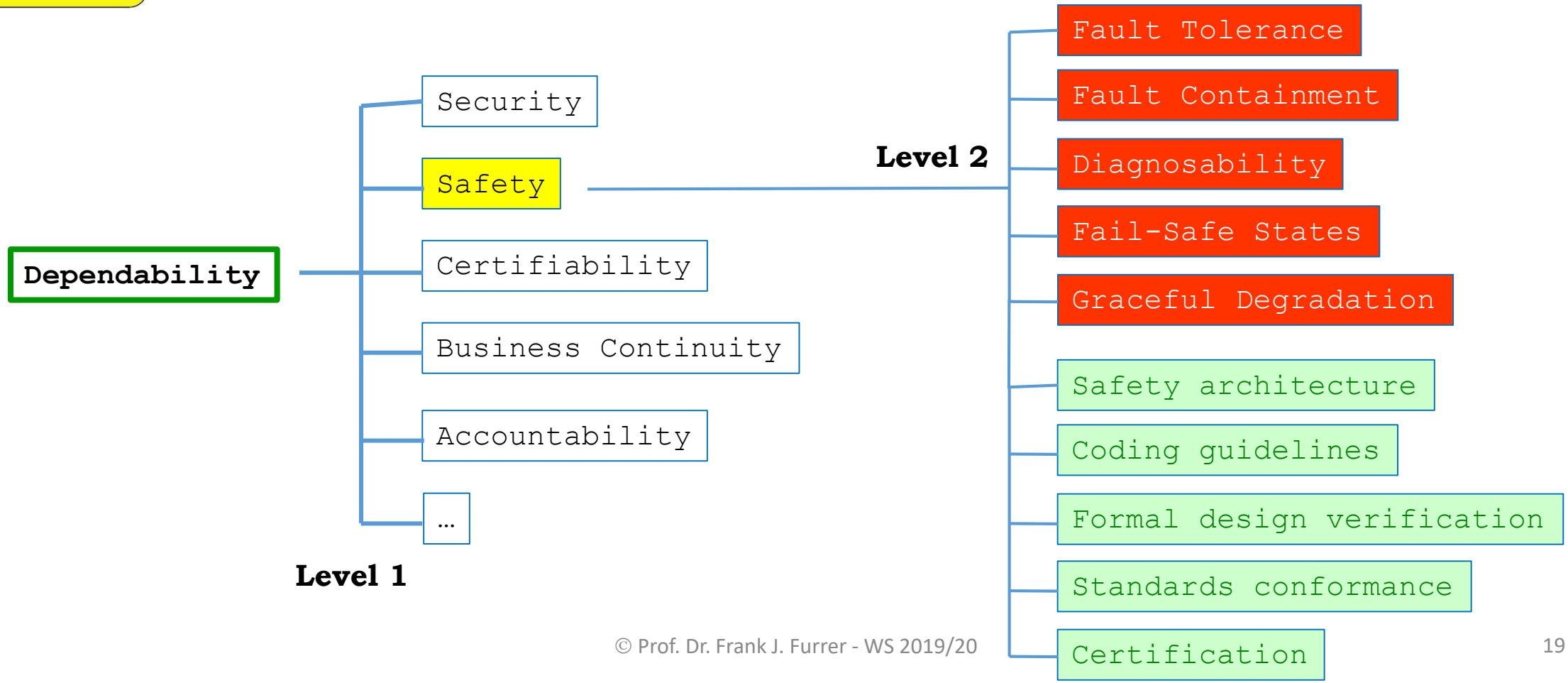
9 **general** resilience principles √

Principles for **specific** dependability properties

Summary 08.01.2020

Safety

Safety is the state of being **protected**
against *failure*, *damage*, *error*, *accidents*, *harm*, or any other event
that could be considered non-desirable
in order to achieve an **acceptable level of risk**



Summary 08.01.2020

Security

Information **Security** protects the
confidentiality, **integrity** and **availability** (CIA)
of computer system **data** and **functionality**
from *unauthorized and malicious accesses*

Level 1

- **Dependability**
  - Security
  - Safety
  - Certifiability
  - Business Continuity
  - Accountability
  - …

Level 2

- Security
  - Confidentiality
  - Integrity
  - Availability
  - Business Continuity
  - Physical Security
  - Isolation

https://png.pngtree.com

Specific Taxonomy = **Domain-dependent**

Summary 08.01.2020

Security

https://vstracking.com

Information Security: The CIA-Triad

C: **Confidentiality**
Allows only *authorized users* to access sensitive information and functionality.

I: **Integrity**
The information and functionality in the system is *correct* and *consistent* at any time (as specified by the rightful owner).

A: **Availability**
Percentage of time a computer system's information and functionality is *ready* for the intended use.

Summary 08.01.2020 **Security**

DEFINITIONS

Information security protects the confidentiality, integrity and availability of computer system data and functionality from unauthorized and malicious accesses

Security Methodology

❶ Identify

Protection Assets

- …
- Customer Data
- …

❷ Assess

Threats & Dangers

- …
- Unauthorized Access
- …

❸ Engineer & Implement

Protection Means

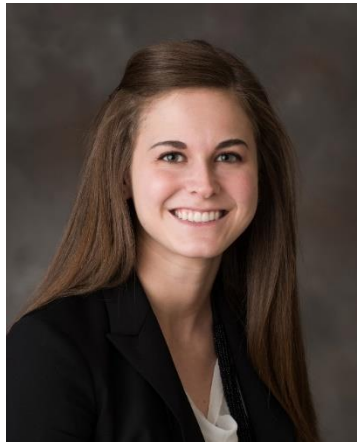
- Authentication
- Authorization
- Access Control
- …

Summary 08.01.2020

Security

Confidentiality

http://engineering.unl.edu



Rightful User

Forbidden User

Protection Means

Protection Assets

- …
- Customer Data
- …

❶ Authentication
❷ Authorization
❸ Access Control

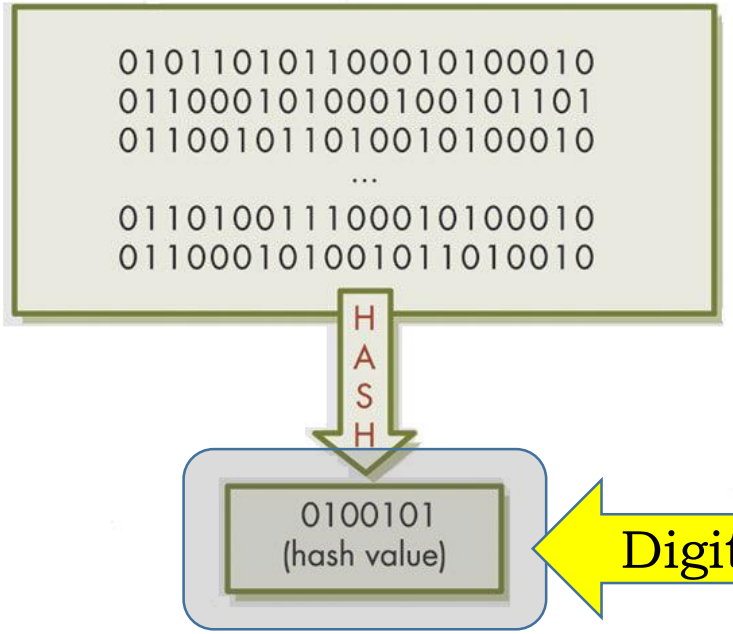
Summary 08.01.2020

Security

Information Integrity

http://www.nelbaliproperty.com

Long-Time Information **Integrity**: Hashing & Digital Signatures



Digital Signature

Document ID
Time Stamp
Hash Value

Check # signature

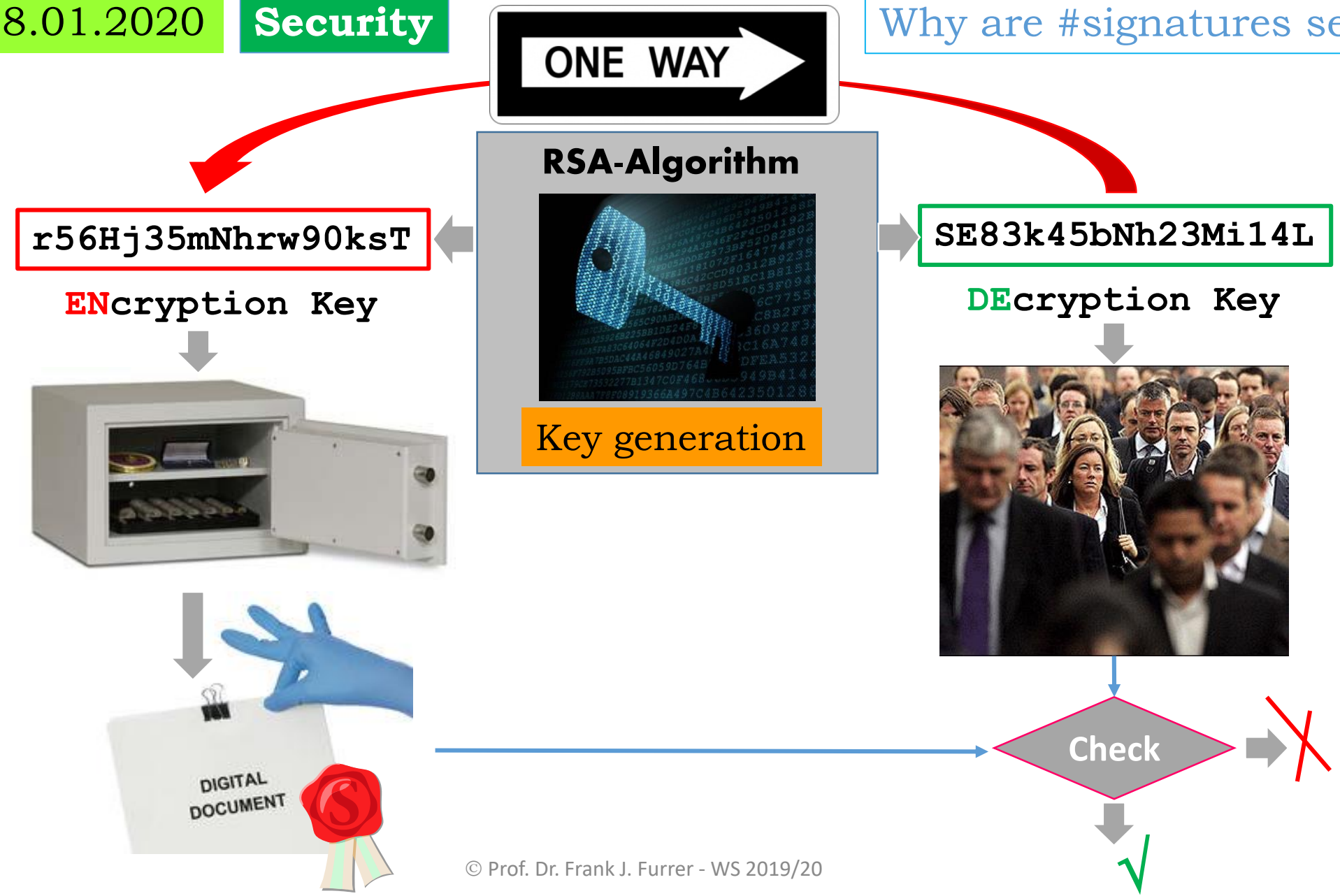
http://de.dreamstime.com

http://www.3gforensics.co.uk

Summary 08.01.2020

Security

Why are #signatures secure?



Announcements

Summary 08.01.2020

Oral Exam

Participants can receive a grade via an **oral exam**
(3 credits ECTS)

http://ipc.sze.hu

Exam Dates:

Monday, 17-Feb-2020 / 09:00 – 17:30

Thursday, 18-Feb-2020 / 09:00 – 13:30

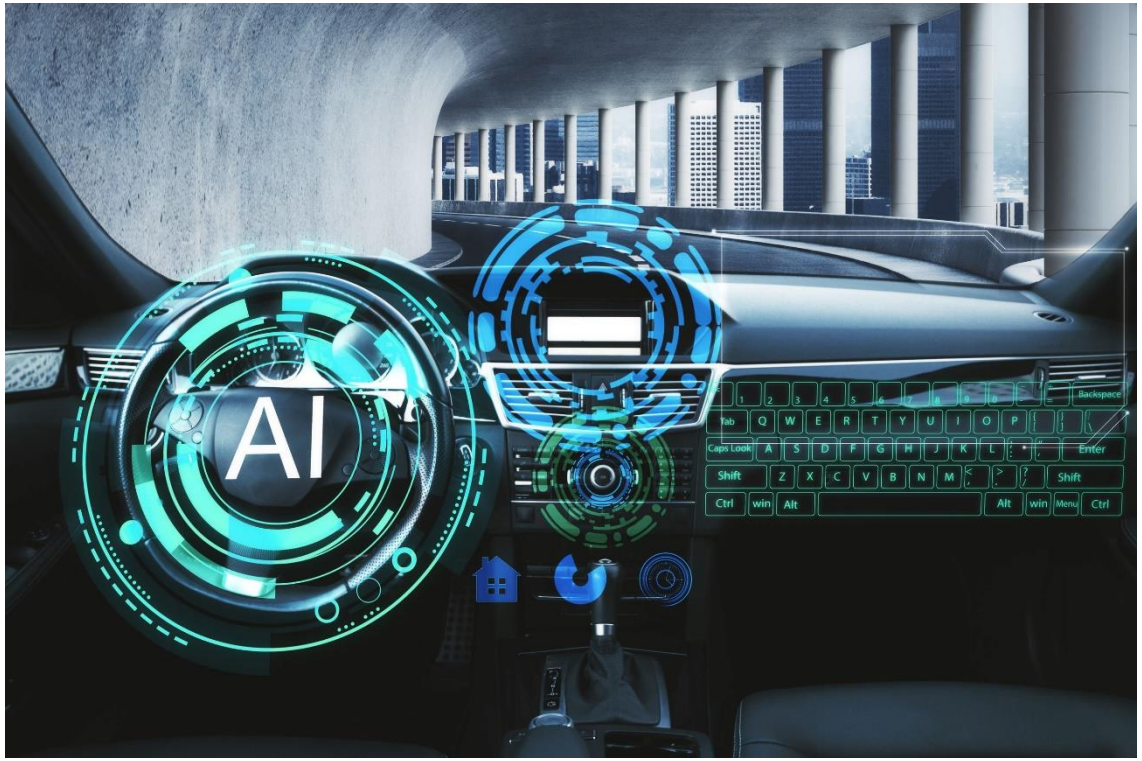
Please agree the date/time with: **Sebastian Goetz**,
Lehrstuhl für Softwaretechnologie

Note: Because I am living in Switzerland, my availability in Dresden is limited

http://constitutional-change.com

Hauptseminar SS 2020:
«Engineering Safety and Security for Cyber-Physical Systems»

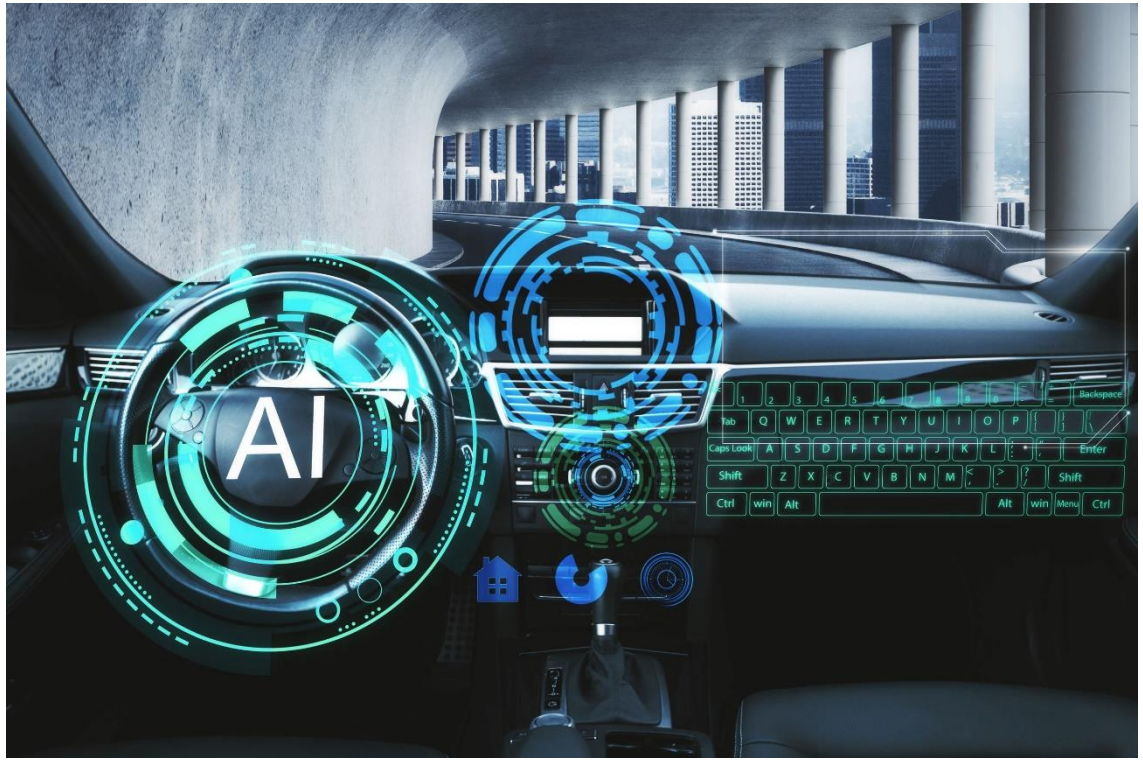
Prof. Dr. Frank J. Furrer

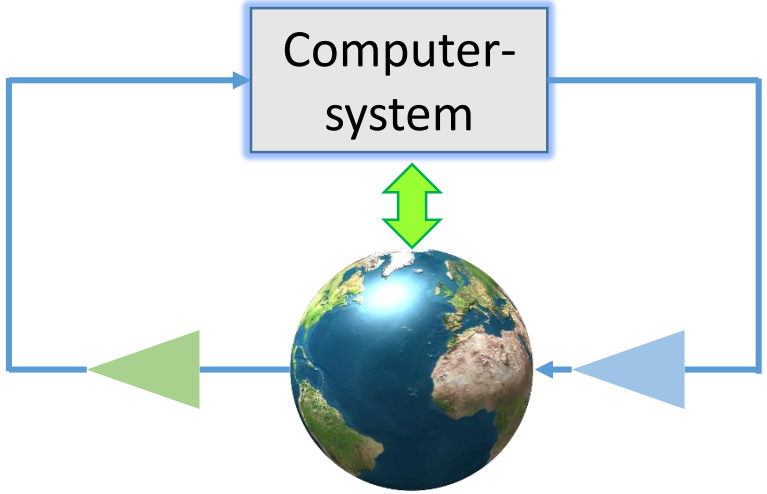


Kick-Off Meeting 27. April 2020

A **cyber-physical system** (CPS) consists of a collection of computing devices communicating with one another and interacting with the physical world, often in a feedback loop

Rajeev Alur, 2015 [ISBN 978-0-262-02911-7]





Serious Concerns:

Safety

https://www.fosterwallace.com

Security

https://safety.lovetoknow.com

https://www.facultyfocus.com

https://de.wikipedia.org/wiki/Seminar

Hauptseminar = A course, where a small number of students work intensely and interactively with the teacher to acquire new skills and/or new knowledge

http://worldartsme.com

- ask
- challenge
- contribute

- write a good paper
- hold a convincing presentation
- learn peer-reviewing

"Engineering Safety and Security for Cyber-Physical Systems"

≤ 7

Time-Table

Hauptseminar Kick-Off Meeting	**Monday, April 27, 2020: 09:20 – 10:50 (2. DS)** **Room APB/INF 2101**	Introductory Lecture by Prof. Frank J. Furrer

1st Seminar Day	**Monday, May 25, 2020: 09:20 – 10:50/11:10 - 12:40 (2. + 3. DS)** **Room APB/INF 2101**	• Participants presentations • Peer discussions, Feedback on style & content

2nd Seminar Day	**Monday, July 6, 2020: 09:20 – 10:50/11:10 - 12:40 (2. + 3. DS)** **Room APB/INF 2101**	• 2nd participants presentation • Peer discussions, Feedback on style and content

Future-Proof Software-Systems: Summary 08.01.2020

Our journey:

«Software everywhere» √ → Systems & Software Engineering √ → Three devils of Systems Engineering √

Three devils of Systems Engineering → Future-Proof Software-Systems √ → Technial Debt Architecture Erosion √ → Managed Evolution Strategy √ → Architecture √ → Architecting for Changeability √ → Special Topics √ → Architecting for Dependability **PART A** √ → The Future-Proof Software-Systems Engineer → Architecting for Dependability **PART B**