TECHNISCHE UNIVERSITÄT DRESDEN

«Engineering Principles for Safety and Security of Cyber-Physical Systems»

Prof. Dr. Frank J. Furrer

Hauptseminar Day 1: 22. April 2022
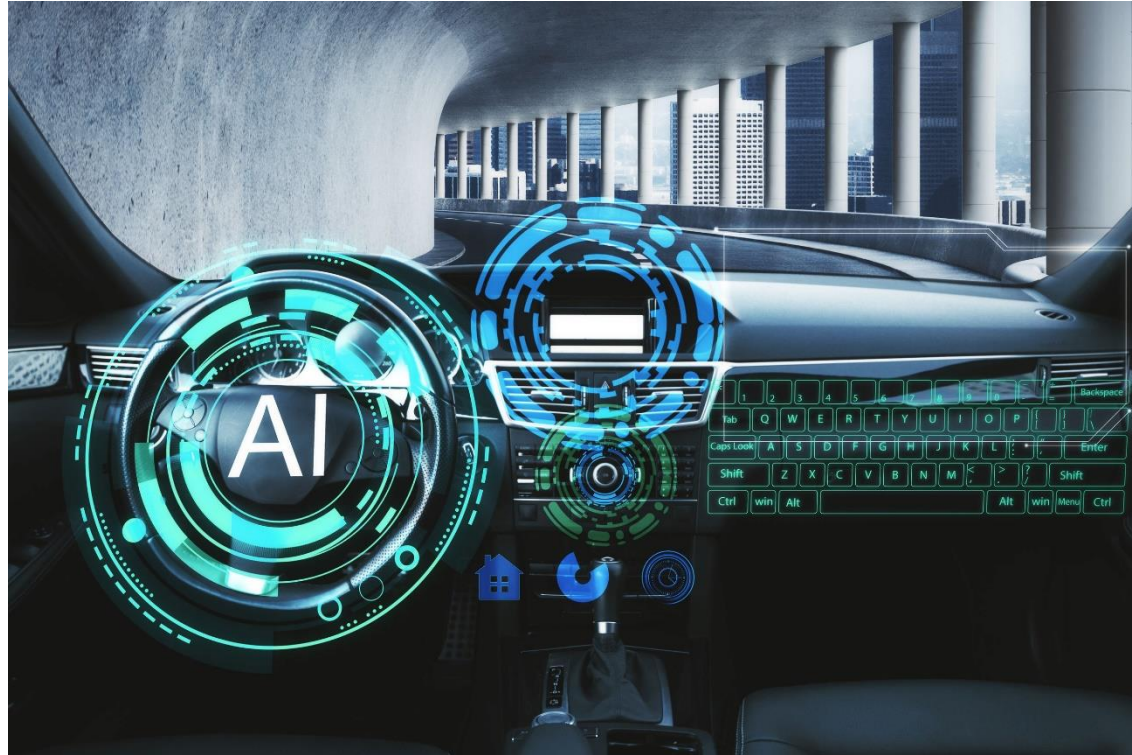
Content

Part 1

- Seminar Objectives
- Explanation of Title
- Setting the Scene
- Technology: Cyber-Physical Systems
- Safety & Security
- Engineering Safety & Security

Part 2

- Doing Research

Part 3

- Principles of a good Paper
- Principles of a convincing Presentation

Part 4

- Work Plan
- Next Steps

Hauptseminar = A course, where a small number of students work intensely and interactively with the teacher to acquire new skills and new knowledge
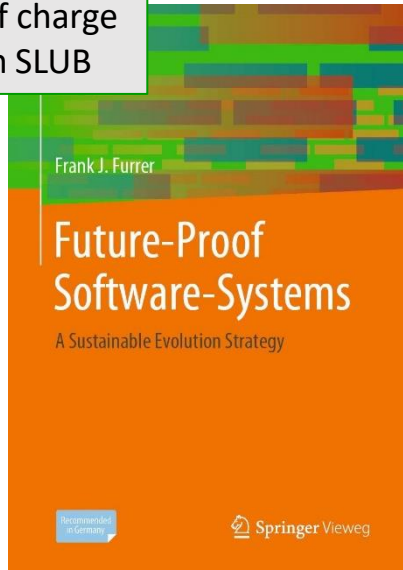
- ask
- challenge
- contribute

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

"Engineering Principles for Safety and Security of Cyber-Physical Systems"

≤ 7

https://www.facultyfocus.com

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

http://worldartsme.com

© HS Prof. Dr. Frank J. Furrer – SS 2022

Your HS-Task:

Downloadable free of charge from SLUB

Frank J. Furrer

Future-Proof Software-Systems

A Sustainable Evolution Strategy

Springer Vieweg

Research and Select
a specific cyber-physical system
safety accident or **security incident**

- Web search: "satellite cyber attacks"
- Web search: "pacemaker cyber attacks"
- Web search: "Tesla truck crash"
- Web search: "water treatment plant cyberattack"
- Web search: "scada cyber attack"
- Web search: "airplane hacking"
- Web search: "hacking cars"
- Web search: "GPS spoofing"
- Web search: "cyber-physical system cyberattack"
- Web search: "industrial plant cyber attack"
- Web search: "drone hacking"
- Web search: "traffic light hacking"
- etc.

Research and decide
which **violation** of which
safety or security **principle**
caused the accident or incident

- Web search: "safety principles in CPS"
- Web search: "security principles in CPS"
- Web search: "engineering principles in CPS"
- Web search: "CPS risk"
- etc.

Write your Storyline

Peer Review

Write a good paper

Prepare a convincing presentation

Seminar Objectives

Learning Outcomes

✓ To do *focused research* in a specific area ("Engineering Safety and Security of Cyber-Physical Systems")

✓ To author a good *scientific paper*

✓ To hold a convincing *presentation*

✓ To experience the *peer-review process*

✓ To benefit from a considerable broadening of the *perspective* in the field of technology, software, and applications

- 3 ECTS Credits
- An assessment (with a grade)

if:

① Full attendance at 3 seminar days

② Helpful peer reviews produced

③ A good presentations delivered

④ Timely delivery of an interesting paper

Required Effort (2 SWS):
~ 90 working hours

Meeting Time-Table

<u>Hauptseminar Day 1 (Introduction)</u>:

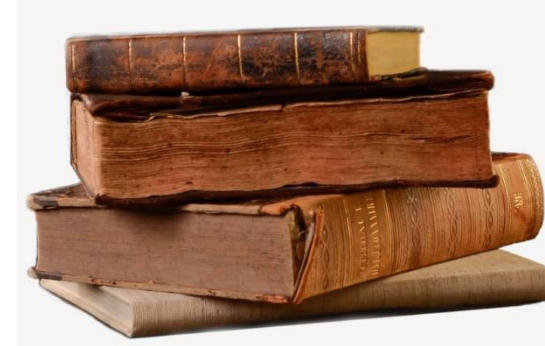Friday, **April 22, 2022** / 09:20 – 10:50 in APB/INF 2101

<u>Hauptseminar Day 2</u>:

Friday, **May 27, 2022** / 09:20 – 10:50 & 11:10 – 12:40 in APB/INF 2101

<u>Hauptseminar Day 3</u>:

Friday, **July 1, 2022** / 09:20 – 10:50 & 11:10 – 12:40 in APB/INF 2101

Mandatory Reading (1)

Introductory Text:

Poul Heegaard, Erwin Schoitsch (Editors): *Combining Safety and Security Engineering for Trustworthy Cyber-Physical Systems*. ERCIM News, Nr. 102, July 2015. Free pdf-Download from: https://ercim-news.ercim.eu/en102/special/combining-safety-and-security-engineering-for-trustworthy-cyber-physical-systems [last accessed 16.03.2022]

Safety and Security Principles:

Frank J. Furrer: **Future-Proof Software-Systems – *A Sustainable Evolution Strategy***. Springer Vieweg Verlag, Wiesbaden, Germany, 2019. ISBN 978-3-658-19937-1

Mandatory Reading (2)
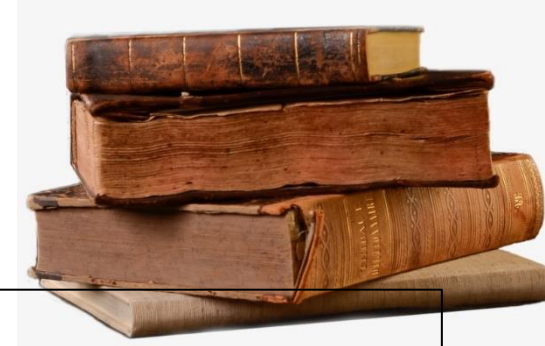
For the topic: *Safety*:

The National Academies Press (NAP), Washington DC, 2012. TRB Special Report 308: *The Safety Challenge and Promise of Automotive Electronics*: Insights from Unintended Acceleration. ISBN 978-0-309-25297-3. Free pdf-Download from: https://www.nap.edu/catalog/13342/trb-special-report-308-the-safety-challenge-and-promise-of-automotive-electronics [last accessed 16.03.2022]

For the topic **Security**:

Robert Radvanovsky, Jacob Brodsky: Handbook of SCADA/Control Systems Security. CRC Press (Taylor & Francis Group), Boca Raton, FL, USA. ISBN 978-1-4665-0227-7. Free pdf-Download from:

http://www.icsdefender.ir/files/scadadefender-ir/books/ICS-SECURITY-NEW/Radvanovsky-%20Robert%20Handbook%20of%20SCADA_control%20systems%20security.pdf [last accessed 16.03.2022]

Please ask questions **<u>anytime</u>** during my lecture

… I value the dialogue !

© HS Prof. Dr. Frank J. Furrer – SS 2022

Prof. h.c. Dr. sc. techn. ETH-Z
Frank J. Furrer

Contact Details:

frank.j.furrer@bluewin.ch
frank.furrer@mailbox.tu-dresden.de

Please check regularly for updates

Hauptseminar Website:

https://st.inf.tu-dresden.de/teaching/hs

http://hoakiauhakseng.blogspot.com

Short individual introduction:

https://www.schulzentrum-stetten-akm.de

Name:

Origin:

Studienrichtung:

[Personal]:

What do you expect from this Hauptseminar?

Prof. Dr. Frank J. Furrer:

| 1974 | WS 13/14 | 1.7.2015 | SS 2022 |

PhD
Federal Institute of Technology, Zurich

Industry Career:
- Industrial Electronics
- Safety & Security Eng.
- Software Architect
- Very large IT Systems
- Consultant for IT-Megasystems

First Lecture at TUD

Appointed **Honorary Professor** TUD

TUD Academic Career:
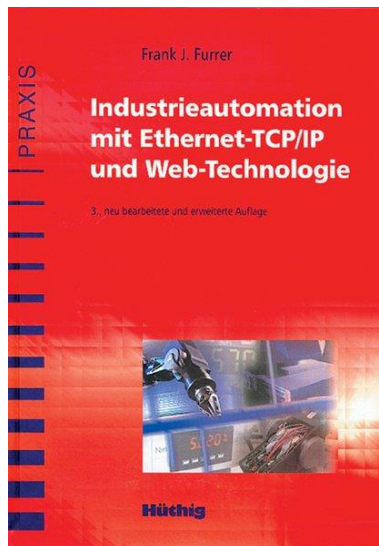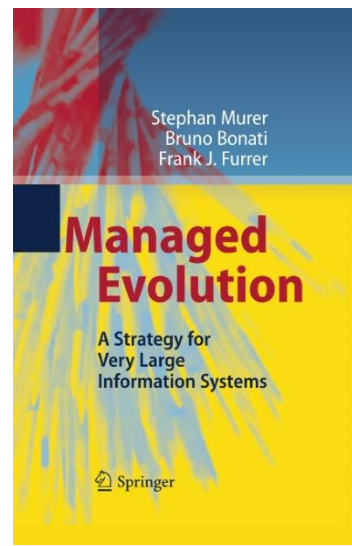- Large SW-System Architecture /CPS / Safety & Security

Lehr- und Handbücher der Ingenieurwissenschaften Band 36
LHI 36
F. J. Furrer
Fehlerkorrigierende Block-Codierung für die Datenübertragung
Springer Basel AG

Frank J. Furrer
PRAXIS
Industrieautomation mit Ethernet-TCP/IP und Web-Technologie
3., neu bearbeitete und erweiterte Auflage
Hüthig

Stephan Murer
Bruno Bonati
Frank J. Furrer
Managed Evolution
A Strategy for Very Large Information Systems
Springer

Frank J. Furrer
Future-Proof Software-Systems
A Sustainable Evolution Strategy
Recommended in Germany
Springer Vieweg

Frank J. Furrer
Safety and Security of Cyber-Physical Systems
Engineering dependable Software using Principle-based Development
Recommended in Germany
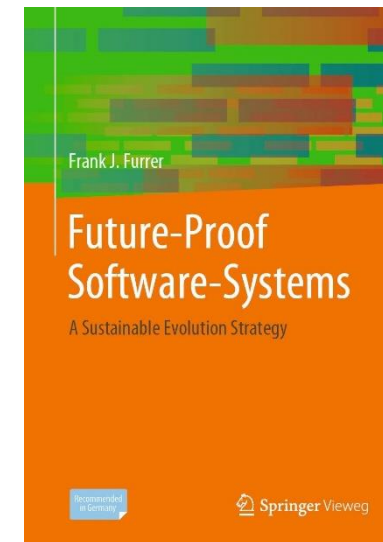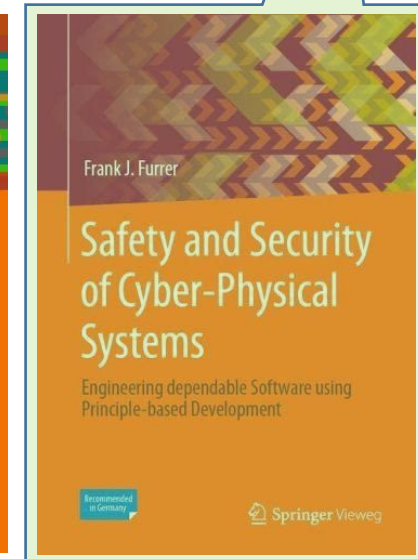Springer Vieweg

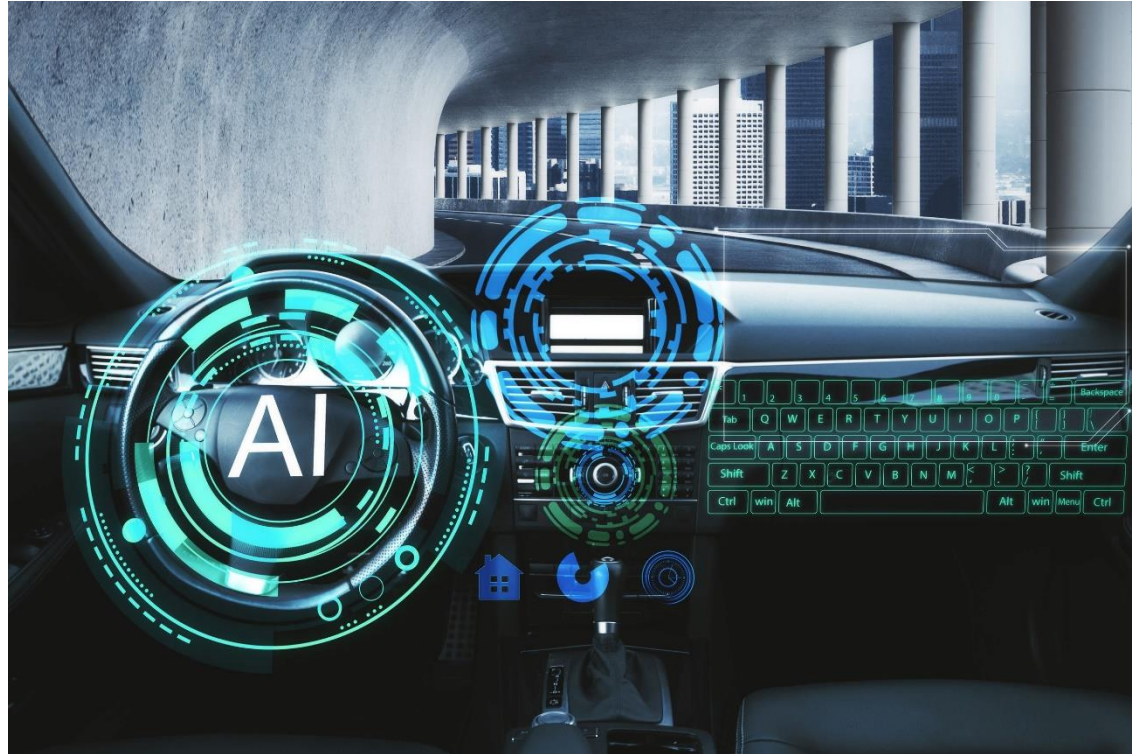1981, reprinted 2013   1/2000   9/2014   10/2019   8/2022

Content

Part 1

- Seminar Objectives
- Explanation of Title
- Setting the Scene
- Technology: Cyber-Physical Systems
- Safety & Security
- Engineering Safety & Security

Part 2

- Doing Research

Part 3

- Principles of a good Paper
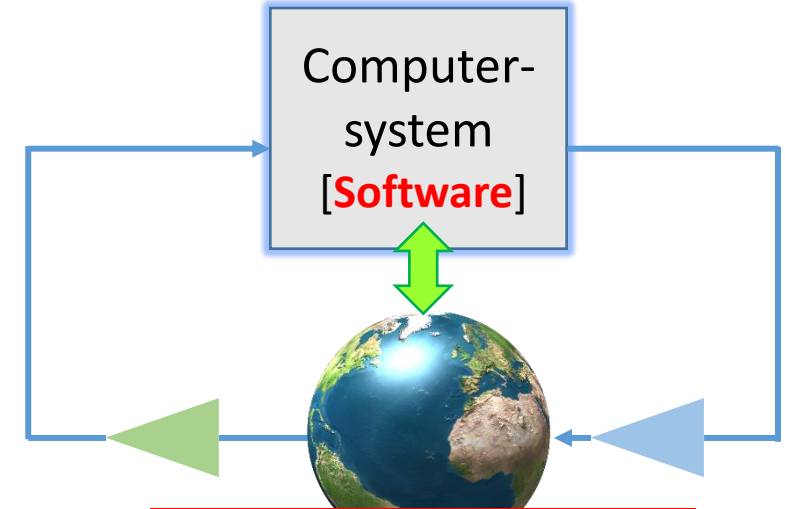- Principles of a convincing Presentation

Part 4

- Work Plan
- Next Steps

Engineering Principles for Safety and Security of Cyber-Physical Systems

A safe and secure CPS is the result of competent and responsible **engineering**
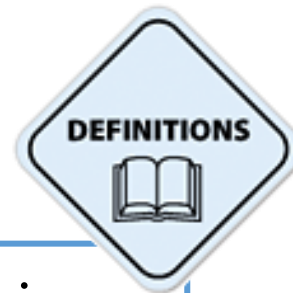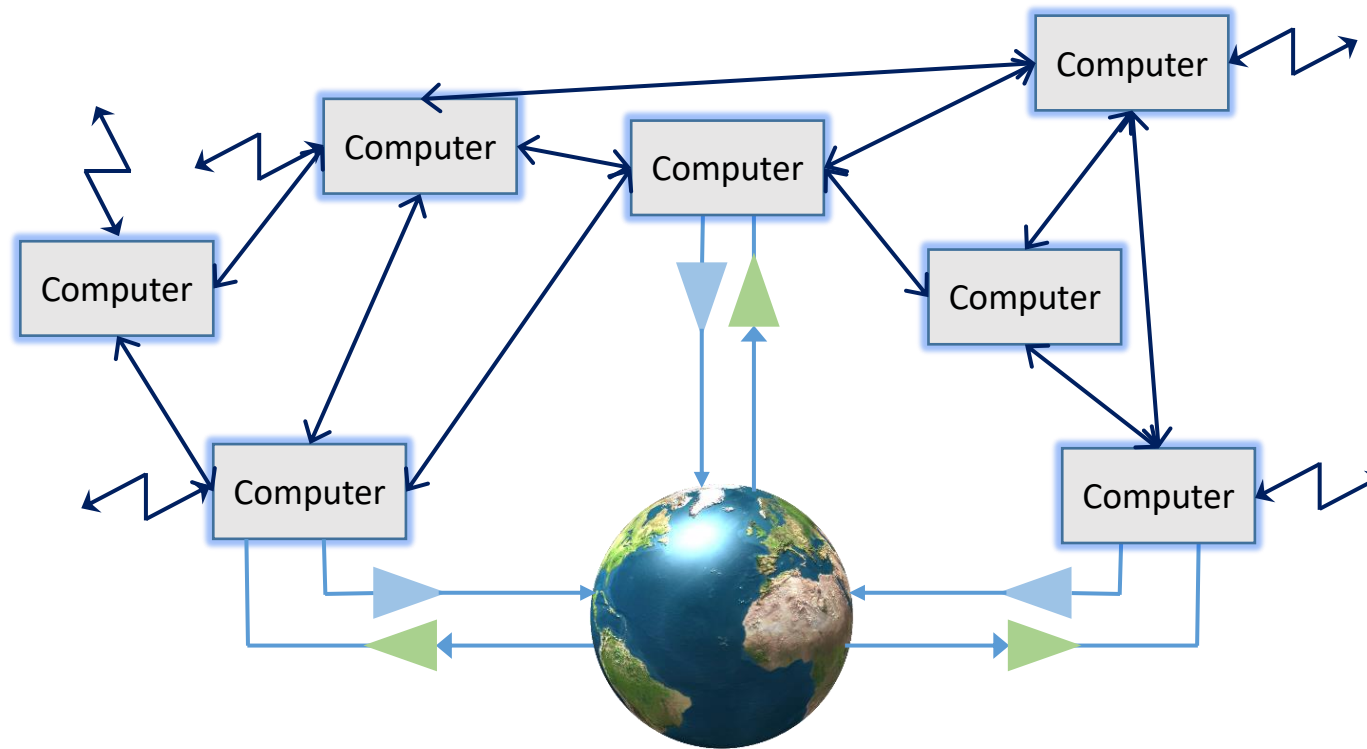
https://www.terreactive.ch

Definitions + Models

Principles + Patterns

Processes

People

Our Topic

Any **vulnerability** in the CPS may cause a **safety accident**

https://eu.usatoday.com

Any **vulnerability** in the CPS may cause a **Security incident**

Computer-system [**Software**]

Serious Concerns:

Safety   Security

https://www.fosterwallace.com   https://safety.lovetoknow.com

https://www.networkworld.com
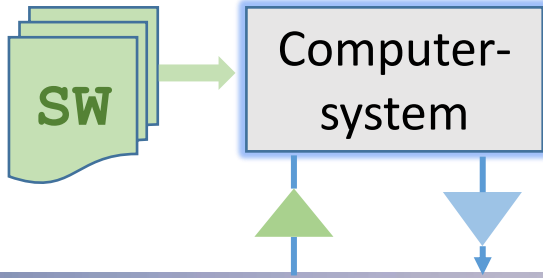
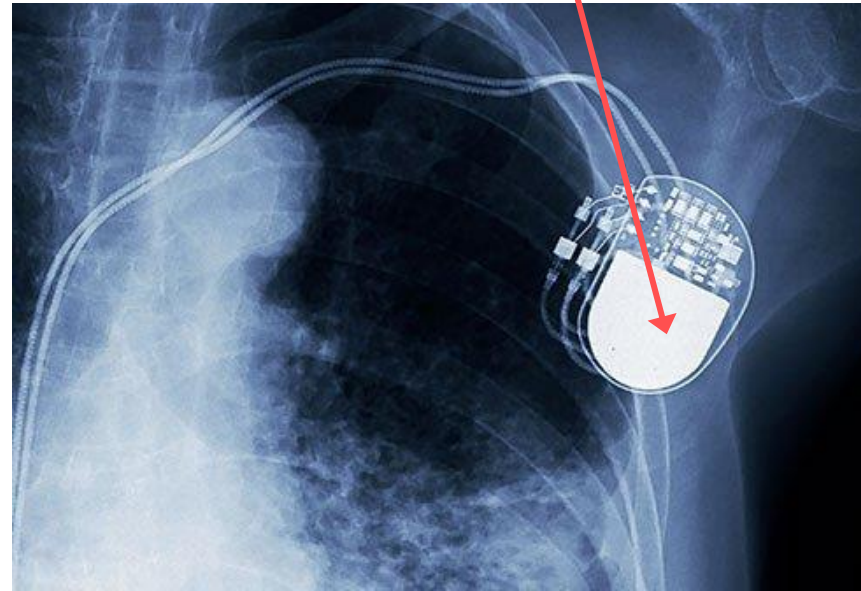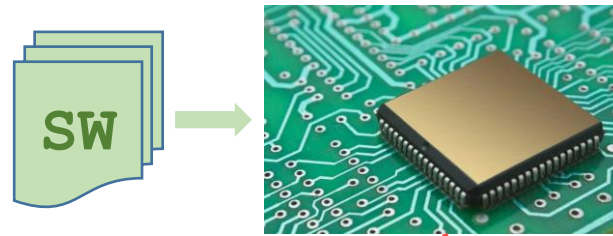22.04.2022   © HS Prof.   14

DEFINITIONS

A **cyber-physical system** (CPS) consists of a collection of computing devices communicating with one another

and interacting with the physical world, through sensors and actuators,

often in a feedback loop

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

Cyber-Physical Systems Examples:

Computer-system

SW

Heart Pacemaker

SW

Unmanned Aerial Vehicle

Freshwater Treatment Plant

SW

Safety

Definition: Safety

Safety is the state of being protected against faults, errors, failures, or any other event that could be considered non-desirable to achieve an acceptable level of risk concerning the loss of property, damage to life, health or society, or harm to the environment.

Product safety refers to the operational safety <u>under normal conditions</u>, i.e. without failures.

Functional safety refers to the safety of the system when it <u>malfunctions</u>.

ISO 26262 [https://www.iso.org/standard/68383.html]

Security

Security is a discipline to protect *information* and *functionality* of systems from threats:

By defining and implementing *security controls,*

To achieve defined *security objectives*, such as confidentiality, integrity, and availability (CIA),

And support the *organizational mission* and processes.

Engineering Principles

Definition: Principle

A principle is a fundamental truth or proposition that serves as the foundation for a system of belief, or behaviour, or for a chain of reasoning.

Oxford Dictionary

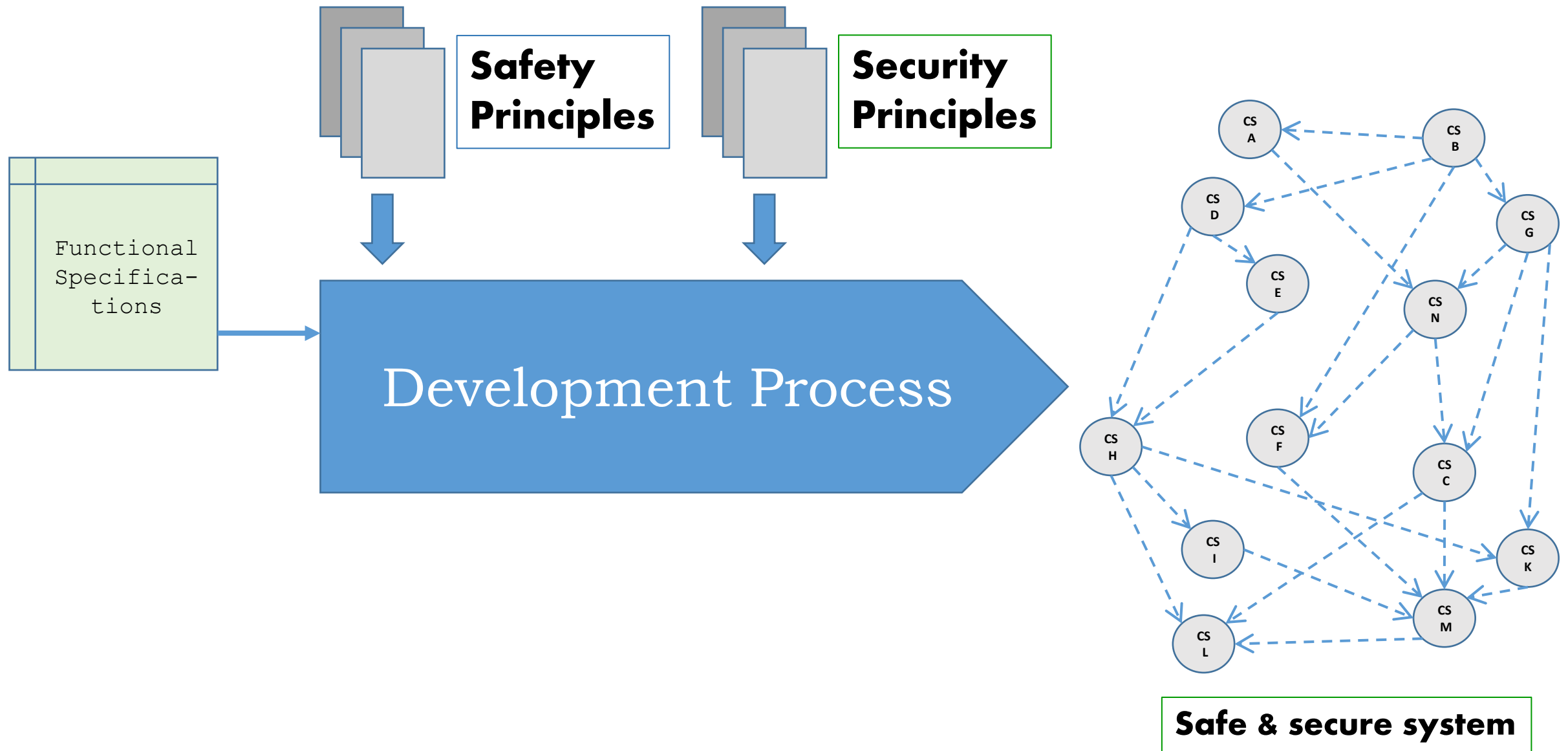Note: An engineering principle must be teachable, actionable, and enforcable.

Treasure Chest

Engineering Principles

distill the proven *knowledge* for systems engineering into precise, actionable, and enforcable *guidance* for the development process
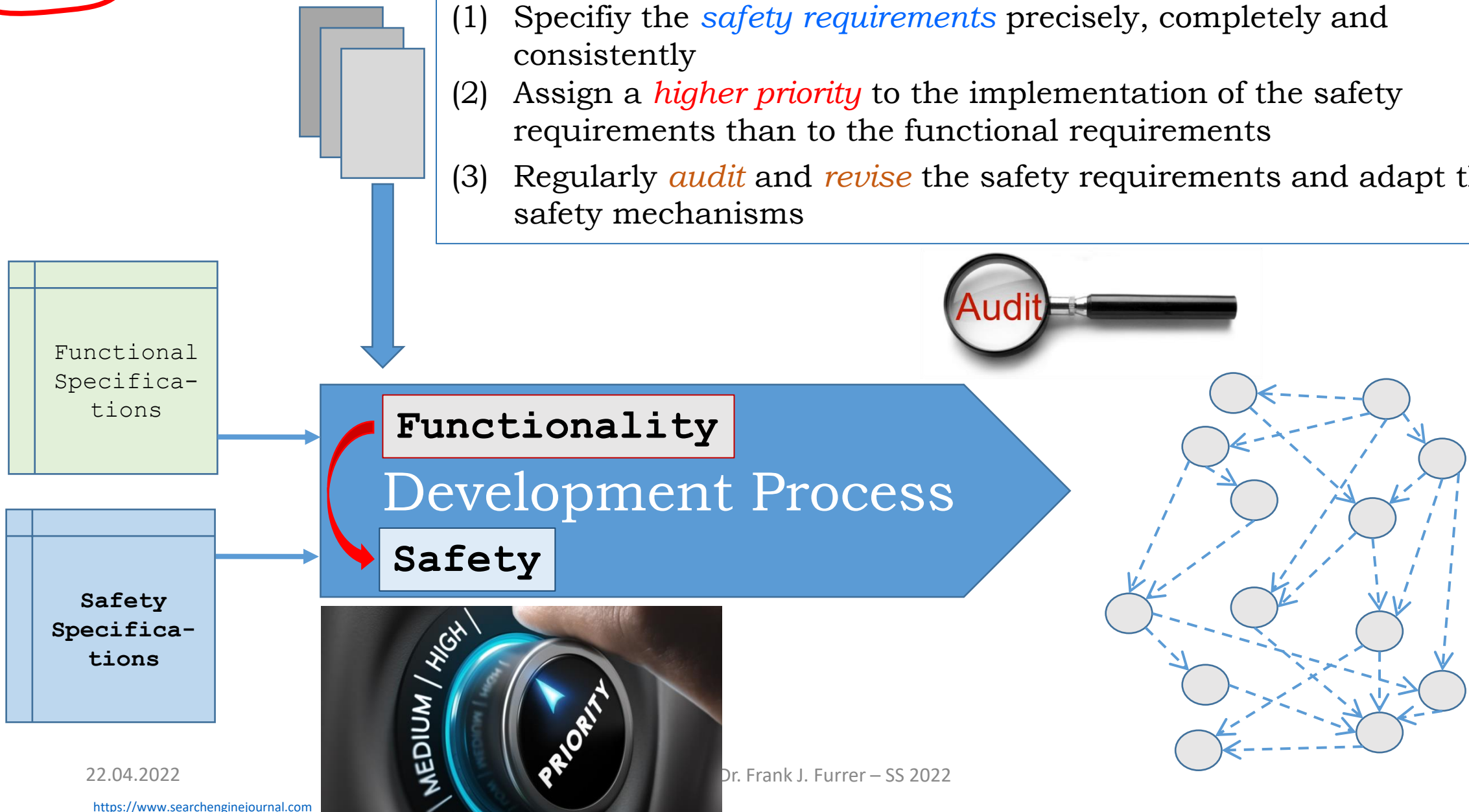
Engineering Principles

https://www.numis.ch/ideen-fuer-geschenke/schatztruhe.php

19

Safety Principles

Security Principles

Functional Specifica-tions

Development Process

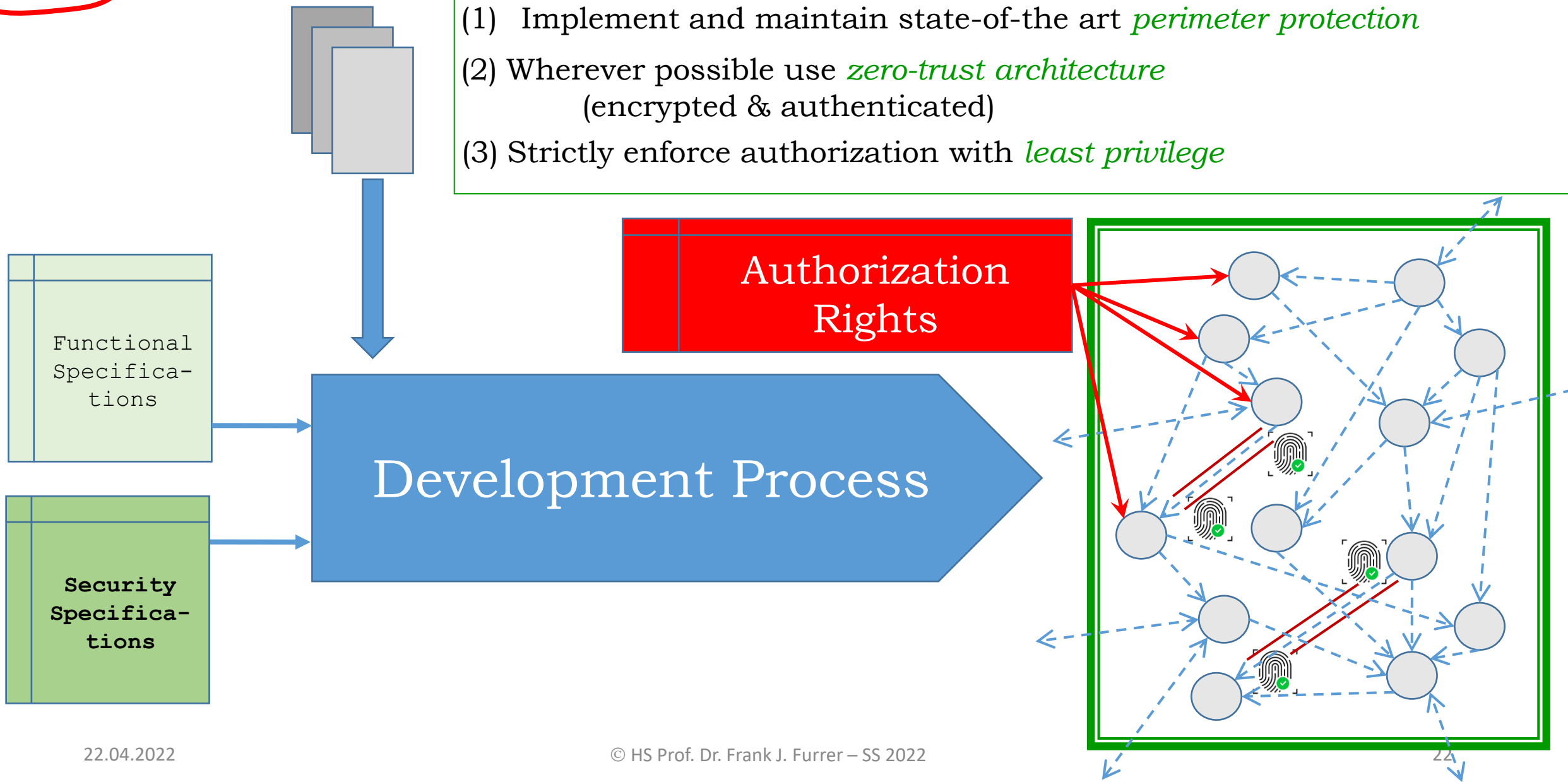**Safe & secure system**

Example: Safety Principle

Safety Principle:
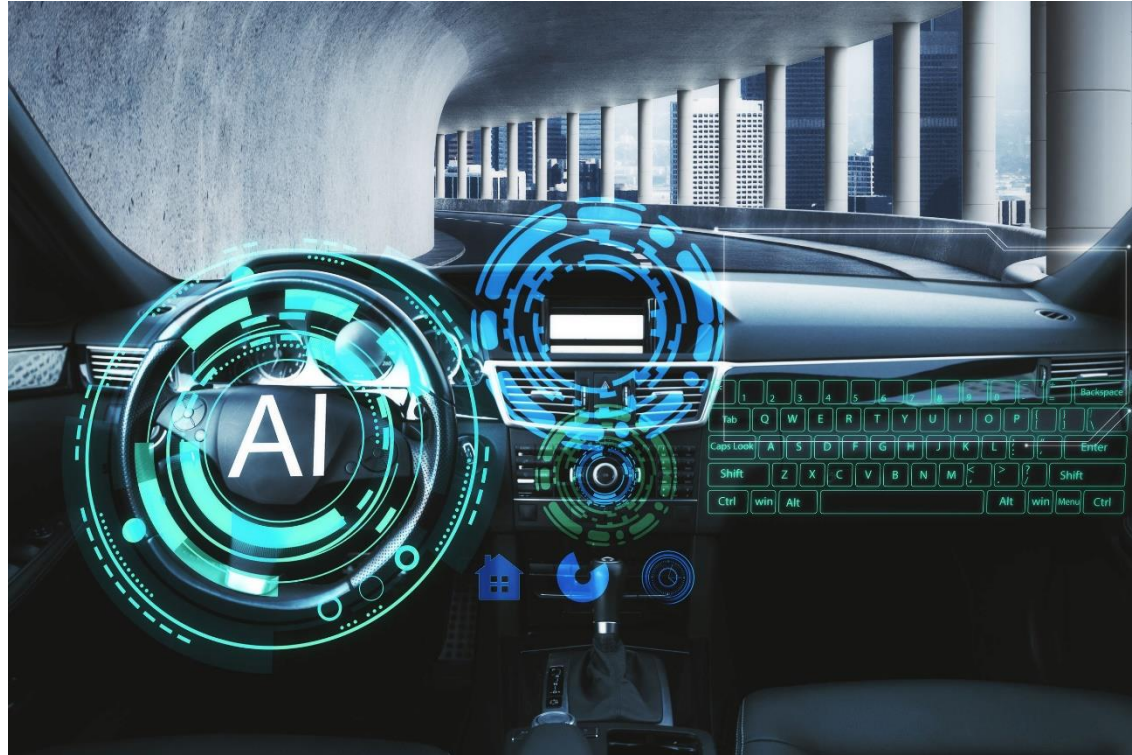
(1) Specifiy the *safety requirements* precisely, completely and consistently

(2) Assign a *higher priority* to the implementation of the safety requirements than to the functional requirements

(3) Regularly *audit* and *revise* the safety requirements and adapt the safety mechanisms

Functional Specifica-tions

Safety Specifica-tions

Functionality

Development Process

Safety

Audit

https://www.johner-institut.de

https://www.searchenginejournal.com

Example: Security Principle

Security Principle:

(1) Implement and maintain state-of-the art *perimeter protection*

(2) Wherever possible use *zero-trust architecture* (encrypted & authenticated)

(3) Strictly enforce authorization with *least privilege*

Functional Specifica-tions

Security Specifica-tions

Development Process

Authorization Rights

Content

Part 1

- Seminar Objectives
- Explanation of Title
- Setting the Scene
- Technology: Cyber-Physical Systems
- Safety & Security
- Engineering Safety & Security

Part 2

- Doing Research

Part 3

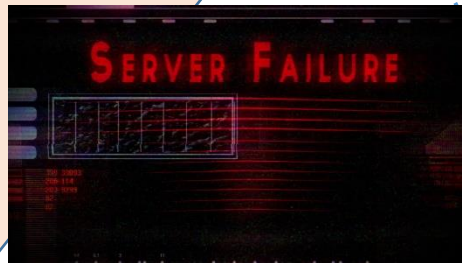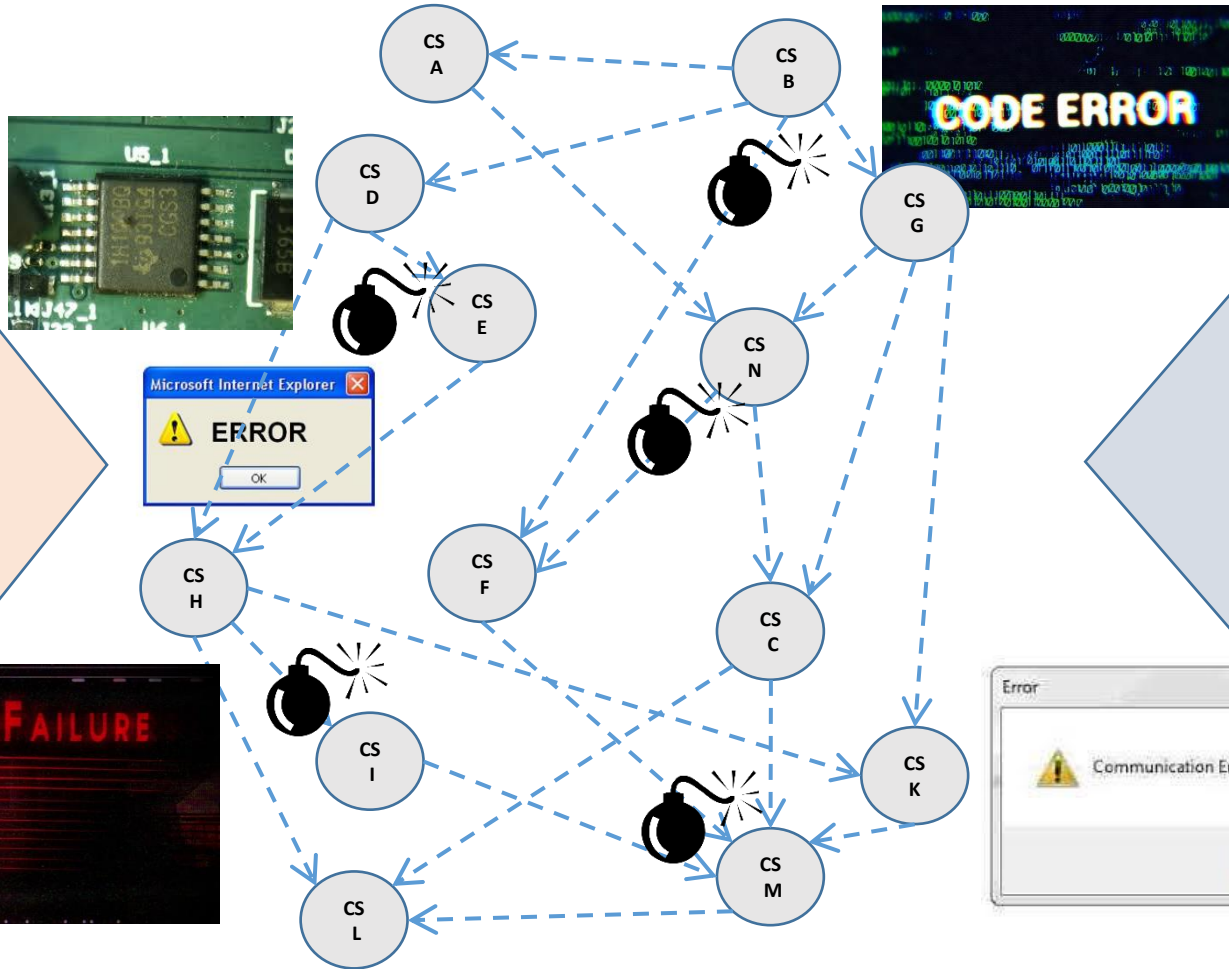- Principles of a good Paper
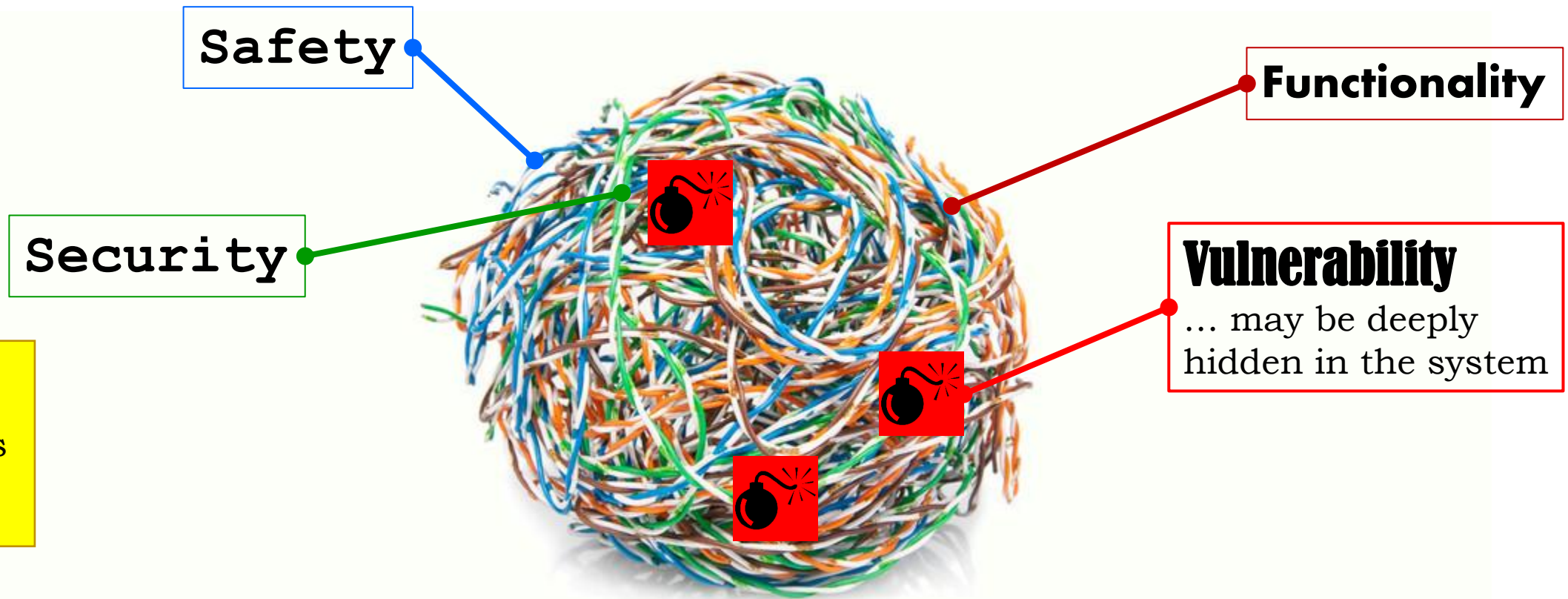- Principles of a convincing Presentation

Part 4

- Work Plan
- Next Steps

http://simpleicon.com/bomb-2.html

Certainty **1**: Cyber-physical systems are highly complex constructs.
They inevitably contain **vulnerabilities**

CS A

CS B

CS D

CS G

CODE ERROR

VIRUS

Certainty **2**:
The cyber-physical
system will
experience **failures**

CS E

CS N

Microsoft Internet Explorer

⚠ ERROR

OK

CS H

CS F

CS C

Certainty **3**:
The cyber-physical
system will be under
threat of cyber-
attacks

SERVER FAILURE

CS I

CS K

CS M

Error

⚠ Communication Error Occured

CS L

Why is safety- and security-engineering so demanding ?

Safety

Security

Functionality

Vulnerability

… may be deeply hidden in the system

Some examples follow

… because functionality, safety, and security are entangled in **complexity** !

https://speakerdeck.com

Example: **Crash Airbus A400M (9. May 2015)** (**Safety** accident)

http://www.reuters.com

Failure of the thrust control of 3 engines shortly after the start
$\Rightarrow$ **Crash**

http://www.ouest-france.fr

A400M: Military Transport Plane

Capacity: 37'000 kg

Range: > 3'000 km
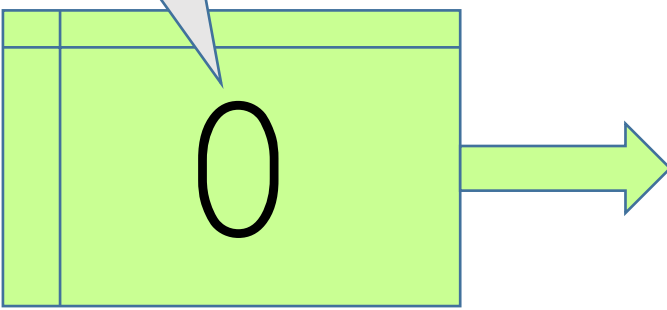
Example: **Crash Airbus A400M (9. May 2015)** (**Safety** accident)

Ground crew software update

Check **completeness** and **integrity** of required data

Start

Control Program

0

Engine Control Data

http://defence-blog.com
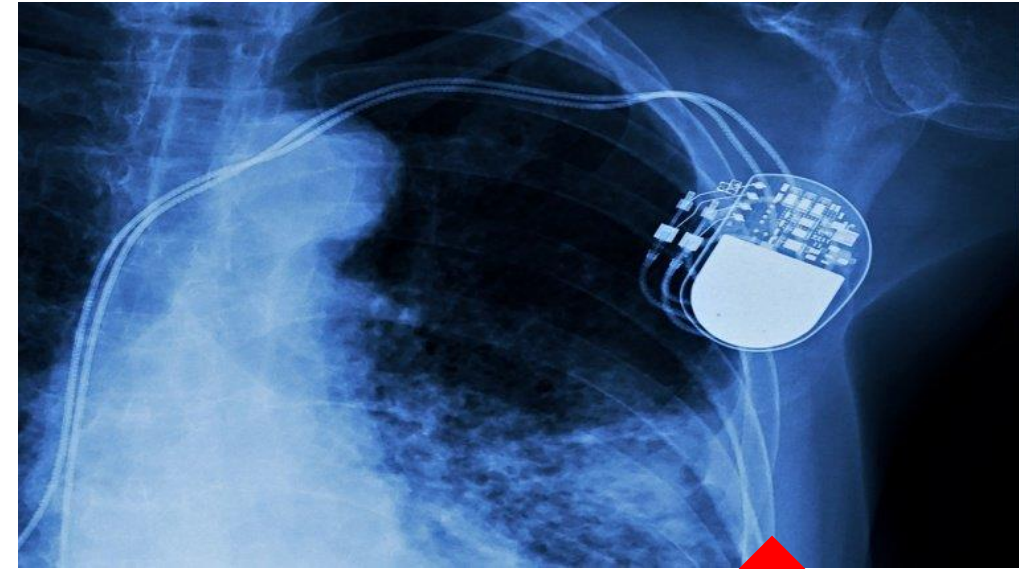
http://www.triumphgroup.com

Example: **Heart Pacemaker Vulnerability**
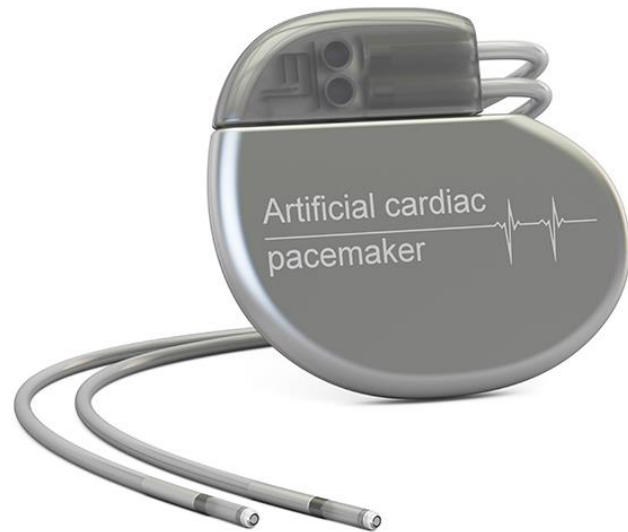
August 30, 2017:

An estimated 465,000 people in the US are getting notices that they should **update the firmware** that runs their life-sustaining pacemakers or risk falling victim to potentially **fatal hacks**

https://arstechnica.com/information-technology/2017/08/465k-patients-need-a-firmware-update-to-prevent-serious-pacemaker-hacks/

https://www.bbc.com/news/technology-34899713

Example: Satellite Attack (**Security** threat)

Viasat communicated on Feb. 28, 2022 that it was "experiencing a partial **network outage**" said to be "impacting internet service for fixed broadband customers in Ukraine and elsewhere on our European KA-SAT network" The outage started on Feb. 24, 2022, the day Russia invaded Ukraine

VIRUS
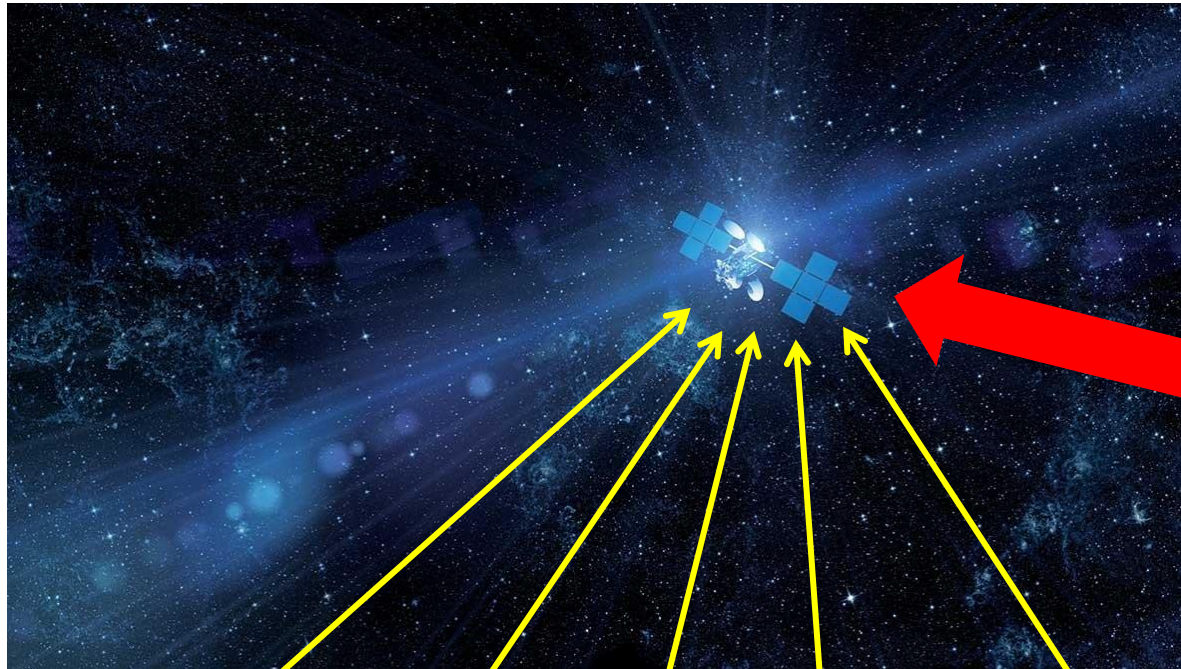
Viasat told Reuters the outage affected **satellite modems** owned by tens of thousands of customers in Europe. Some of those modems are still offline, and bringing them back online is going to be a fairly involved process

© HS

CPS-Example> **Safety Risk**

Toyota "Unintended Acceleration" has killed 89 People

https://www.cbsnews.com / May 25, 2010
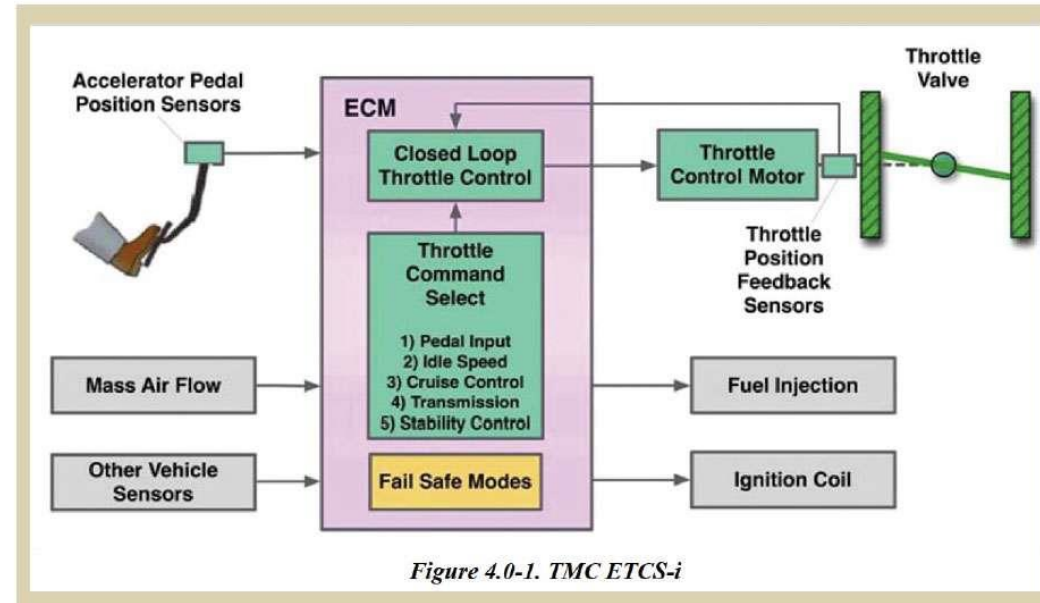

Figure 4.0-1. TMC ETCS-i

Figure 4.0-1 on page 13 of NASA Report shows the ETCS-i.[5]

All of these issues involved unrealistic timing delays in the multiprocessing, asynchronous software control flow. NASA also spent time simulating possible race conditions due to worrisome "recursively nested interrupt masking"

Toyota Is Fined $1.2 Billion for Concealing Safety Defects
March 19, 2014

Example: **Attack on a water treatment plant** (**Safety** accident)

https://www.chemistryworld.com
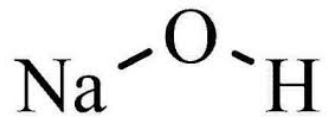
Cyber attack on Florida's water treatment plant: A security wake up call

https://blogs.manageengine.com

On February 5, 2021 a **water treatment plant** operator for the city Oldsmar of about 15,000 on Florida's west coast saw his cursor being moved around on his computer screen, opening various software functions that **control** the water being treated

The cyber-intruder boosted the level of *sodium hydroxide* in the water supply to 100 times higher than normal.
Sodium hydroxide, the main ingredient in liquid drain cleaners, is used to control water acidity and remove metals from drinking water in treatment plants. Sodium hydroxide poisoning can cause burns, vomiting, severe pain and bleeding

Source: https://blogs.manageengine.com/corporate/manageengine/pam360/2021/02/17/cyberattack-on-floridas-water-treatment-plant-what-it-means-to-global-organizations.html

Example: Ukrainian **Power Grid Attack** (**Security** incident)

Malware package:
BLACKENERGY

It was 3:30 p.m. last December 23, 2016 operators Prykarpattyaoblenergo *grid control center* were nearing the end of their shift. But just as one worker was organizing papers at his desk that day, the cursor on his computer suddenly skittered across the screen of its own accord

He watched as it navigated purposefully toward buttons ***controlling the circuit breakers*** at a substation in the region and then clicked on a box to open the breakers and take the substation offline. A dialogue window popped up on screen asking to confirm the action, and the operator stared dumbfounded as the cursor glided to the box and clicked to affirm. Somewhere in a region outside the city he knew that thousands of residents had just lost their lights and heaters

Source:
https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

© HS Prof. Dr. Frank J. Furrer – SS 2022

CPS Example 3:
Boeing 737Max8 Anti-Stall Control

Lion Air Flight 610: On 29 October 2018, the Boeing 737 MAX 8 crashed into the Java Sea 12 minutes after takeoff, killing all 189 passengers and crew

Ethiopian Airlines Flight 302: Six minutes after takeoff, the plane crashed near the town of Bishoftu, Ethiopia, killing all 157 people aboard.

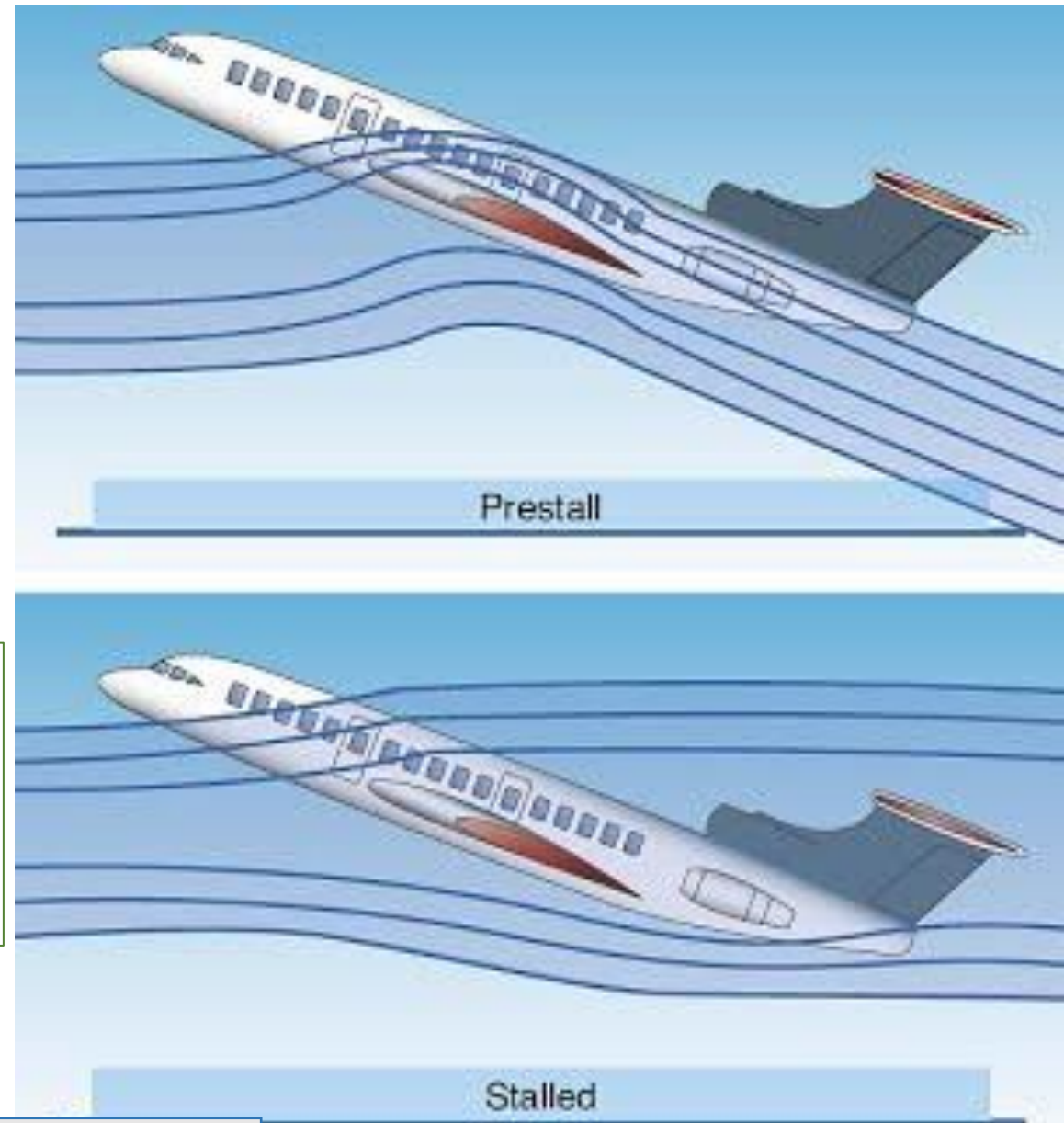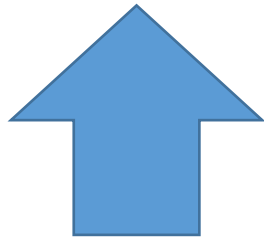Both planes crashed **nose-down**

What happened?

The 737 MAX was equipped with new, more fuel-efficient engines

https://leehamnews.com

The larger engines augmented the risk of **stalling**

MCAS takes readings from sensors to determine how much the plane's nose is pointing up or down. If the software detects the nose is pointing up at a dangerous angle it has the ability to automatically push the nose down in an attempt to **stop the plane stalling**

https://www.theguardian.com

Airflow
⇓
Lift

Lift
Loss
⇓
Stalling

Prestall

Stalled

https://en.wikipedia.org

Typical CPS

CPS Example 3: Boeing 737Max8 Anti-Stall Control

737 Max 8 Beispielbild

https://www.youtube.com

Dangerous nose-up angle

→ Risk of stalling (= loss of uplift)

Software-Fix:

MCAS takes readings from sensors to determine how much the plane's nose is pointing up or down. If the software detects the nose is pointing up at a dangerous angle it automatically pushes the nose to **stop the plane stalling**
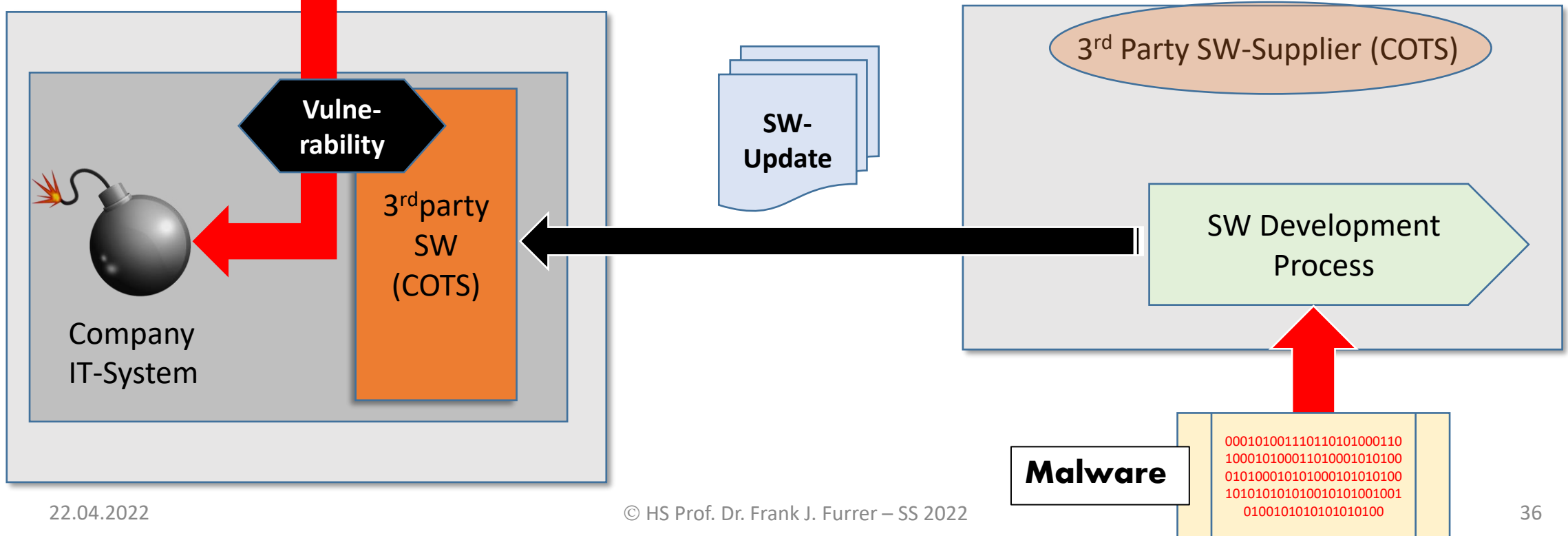
https://www.theguardian.com

… However:

• The pilots were **not** informed about this (new) functionality

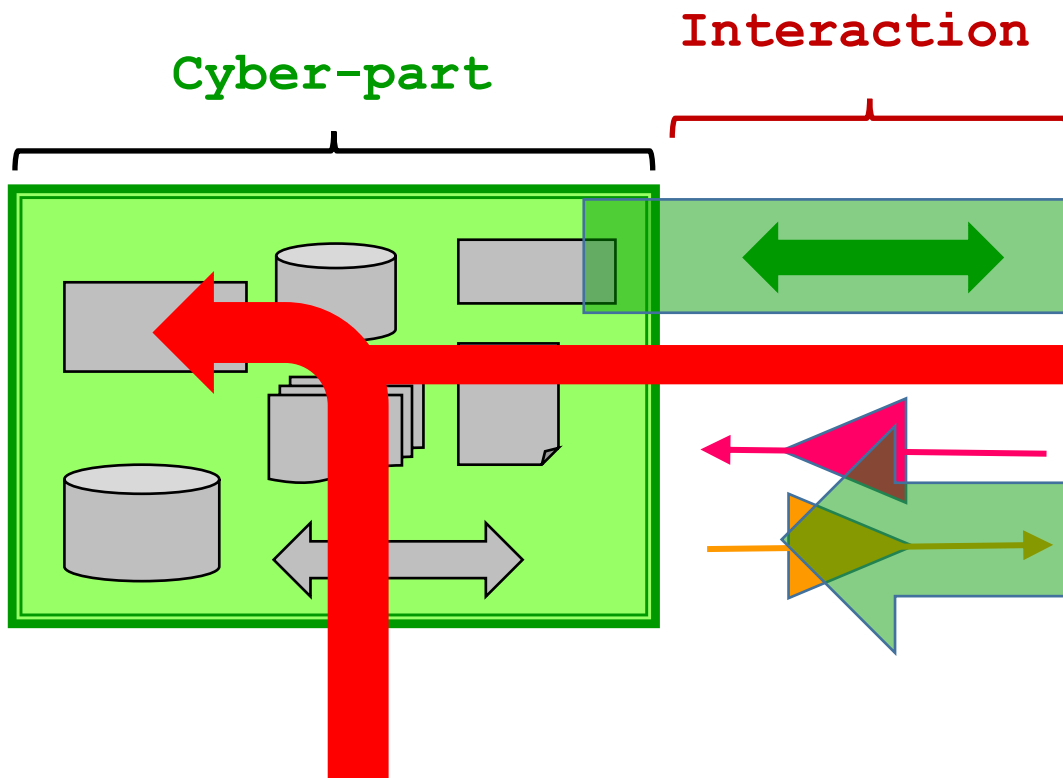• The MCAS (= Software) decisions/actions could **not** be overridden by the pilots

https://news.delta.com

Example: Supply Chain Attack (**Security** threat)

https://www.swisscom.ch

December 13, 2020: Malicious actors are currently exploiting SolarWinds Orion products. The Orion platform is a suite of products to *monitor* the health of IT networks (https://www.solarwinds.com). SolarWinds acknowledged that hackers had inserted malware into its *software update distribution* mechanism. This security incident resulted in malicious code being pushed to more than 16'000 customers (industry & government)

Vulne-rability

3rd Party SW-Supplier (COTS)

SW-Update

3rdparty SW (COTS)

Company IT-System

SW Development Process

Malware

0001010011101101010001010
1000101000110100010101000
0101000101010001010100100
1010101010100101010010010
01001010101010100100

© HS Prof. Dr. Frank J. Furrer – SS 2022

Cyber-Physical System
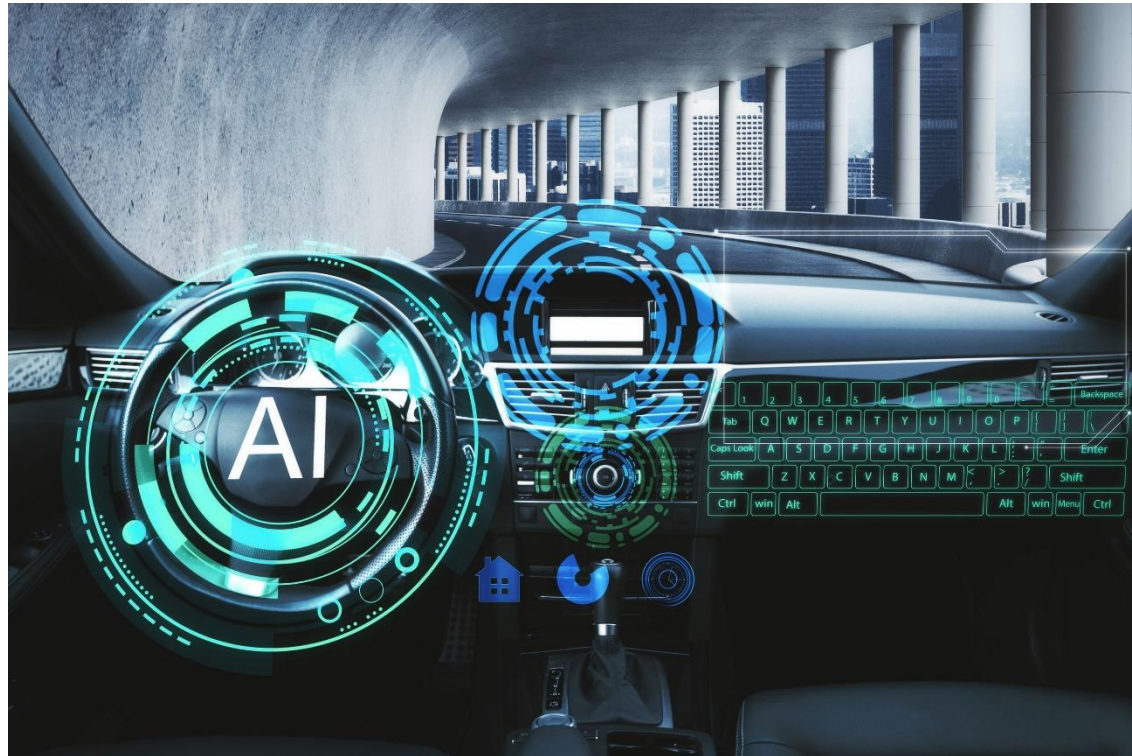
Cyber-part

Interaction

https://www.kevburns.com

Therefore:

It is our undeniable **responsibility** as engineers to build and operate **safe** and **secure** cyber-physical systems

https://etsc.eu

Content

Part 1

- Seminar Objectives

- Explanation of Title

- Setting the Scene

- Technology: Cyber-Physical Systems

- Safety & Security

- Engineering Safety & Security
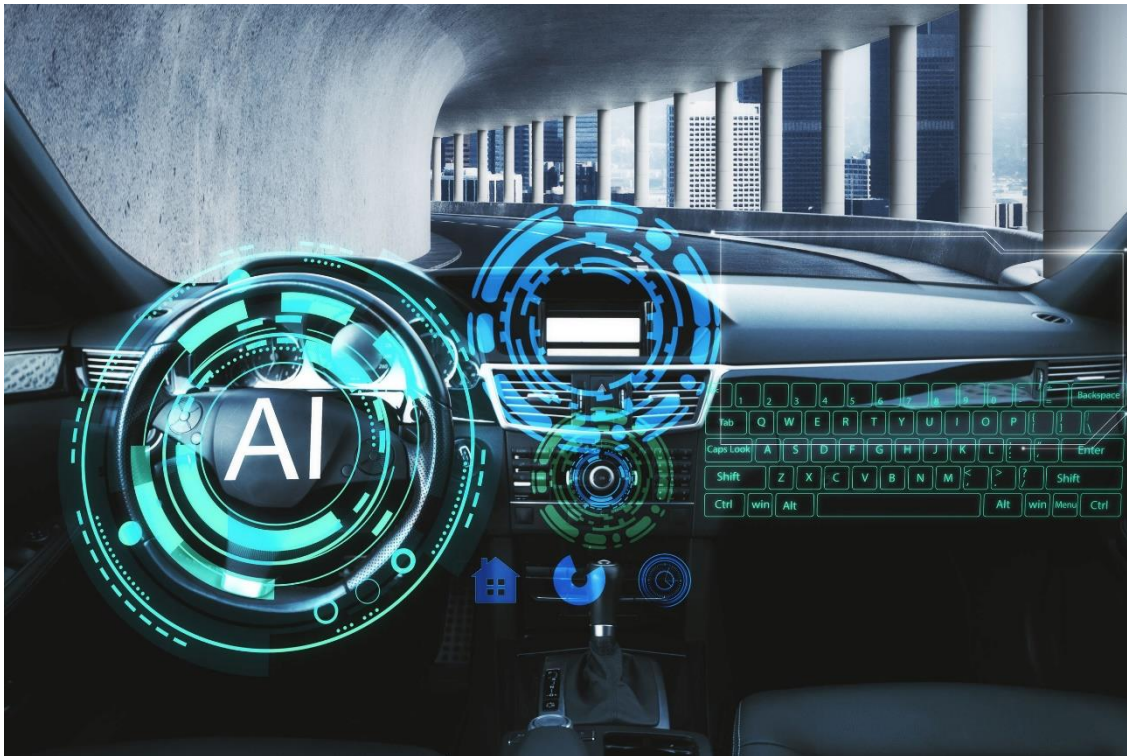
Part 2

- Doing Research

Part 3
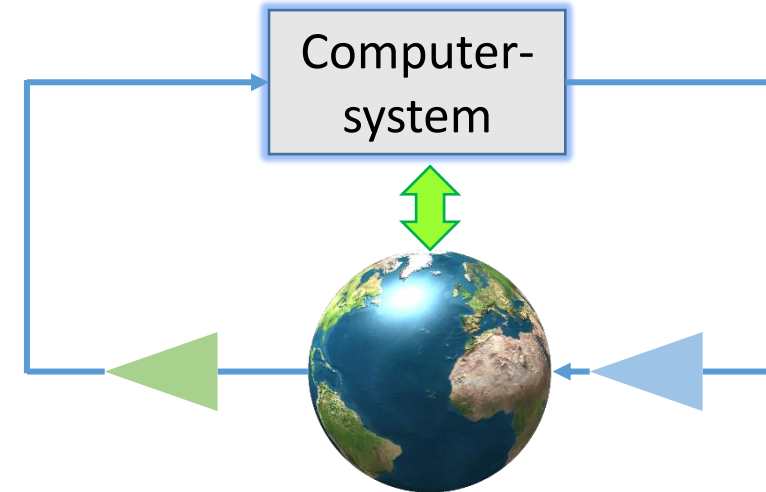
- Principles of a good Paper

- Principles of a convincing Presentation

Part 4

- Work Plan

- Next Steps

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]

Computer-system

Software controls physical systems

Real-world model

Control Computer (ECU)

Actuators

Real-World Model

Software

The model governs the CPS-behaviour

Sensors

Cyber-Part

Physical-Part

Cyber-Physical System

Physical part

Interaction

Cyber-part
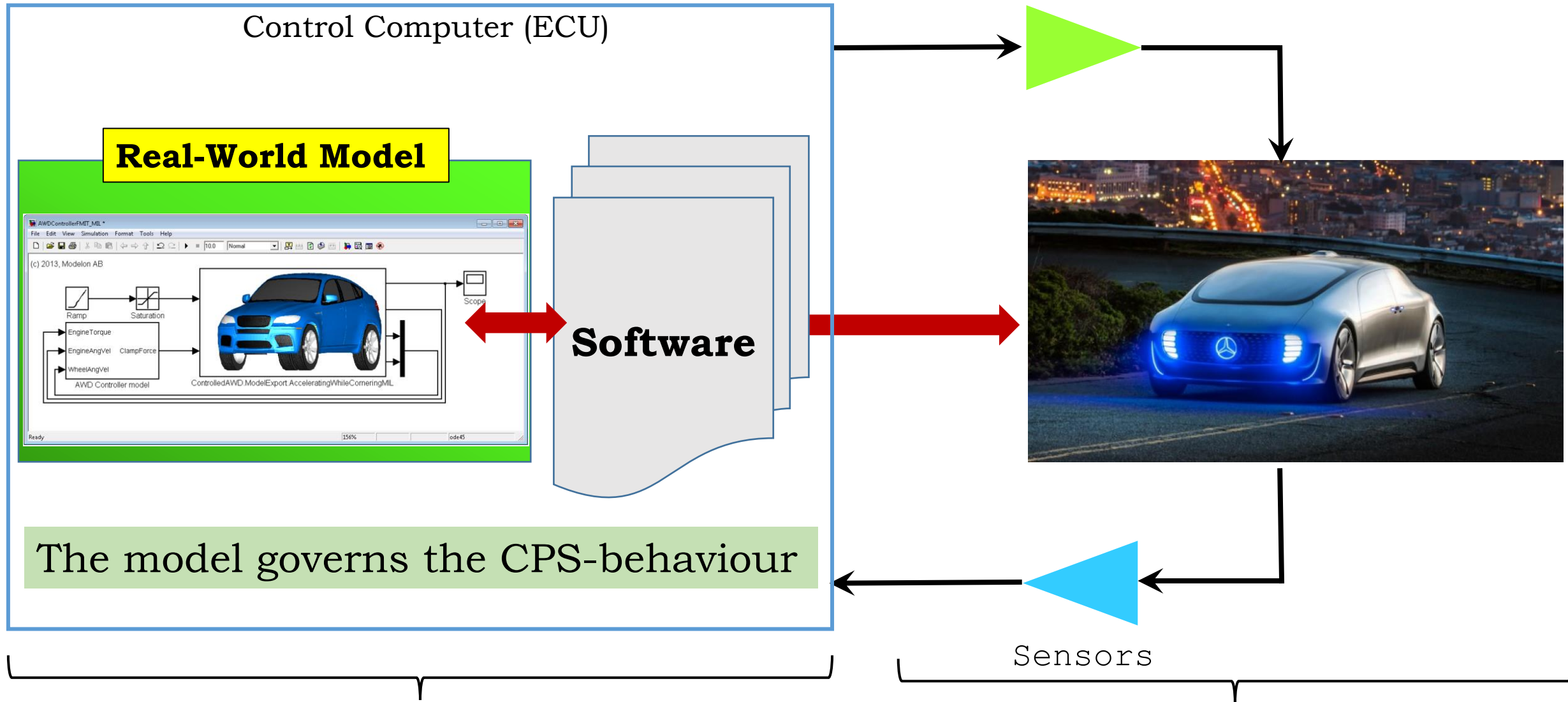
http://www.etemaaddaily.com
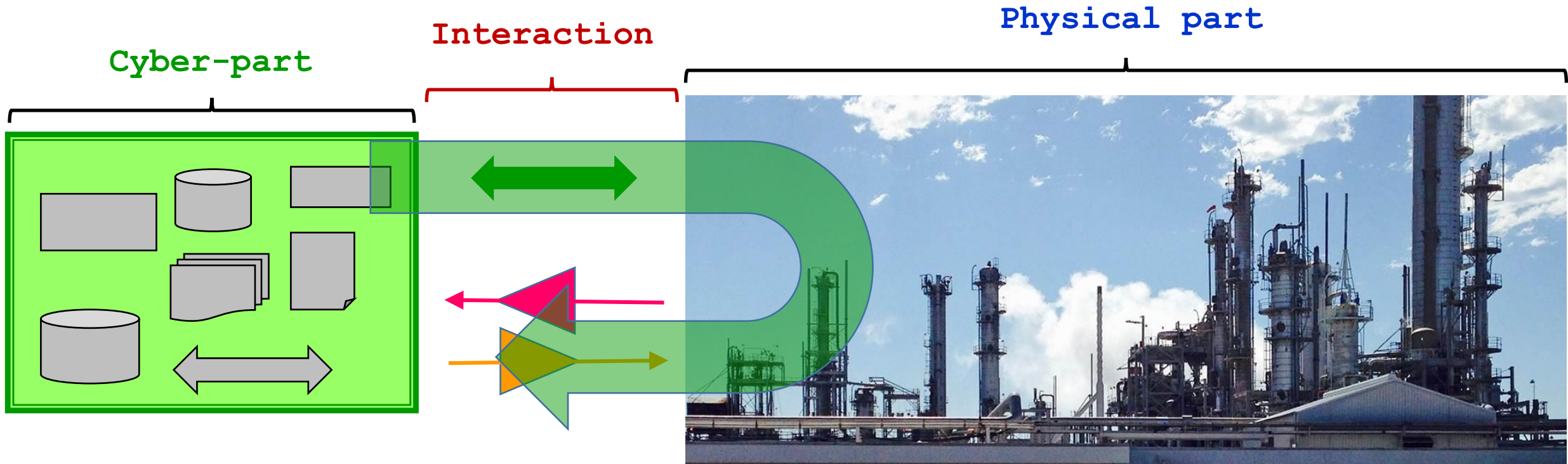
Sensors: Read plant information

Software Control Loop

Physical Plant Parameters:
• Temperatures
• Motor speeds
• Valve positions
• ...

Actuators: Control plant

Physical Plant Parameters:
• Flows
• Pressures
• Levels
• ...

42

CPS-Example: **ESC**

Feedback Loop

Sensors

http://www.polizeiticker.ch

ECU (SW)

Kowledge Base
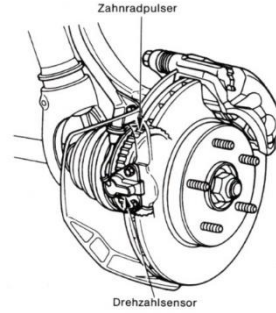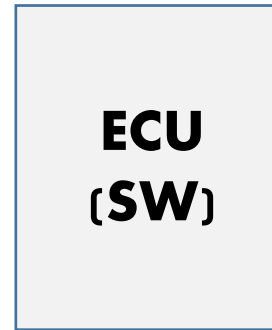
Actuators
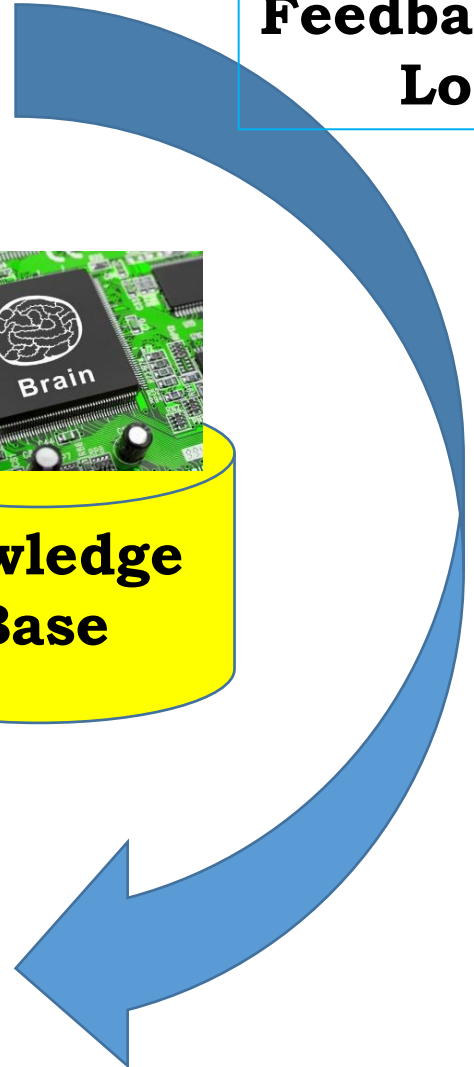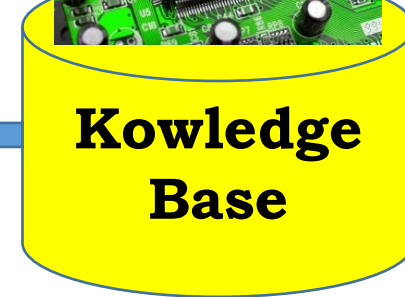
Cyber-Physical Systems-of-Systems (CPSoS)

Constituent System

Computer

Computer

Computer

Computer

Computer

Computer

Computer

Governance **A**

Governance **B**

Governance **C**

1 Adaptive Cruise Control
2 Electronic Brake System MK60E
3 Sensor Cluster
4 Gateway Data Transmitter
5 Force Feedback Accelerator Pedal
6 Door Control Unit
7 Sunroof Control Unit

8 Reversible Seatbelt Pretensioner
9 Seat Control Unit
10 Brakes
11 Closing Velocity Sensor
12 Side Satellites
13 Upfront Sensor
14 Airbag Control Unit

A modern car contains:
- > 100 networked ECU's
- > 100 Million lines of code

A modern car is a **CPSoS** on wheels

https://sites.google.com/a/g.ucla.edu

Danger

«The combination of physical systems with complex computer systems opens up new concerns and threats that are more than the sum of traditional safety engineering and computer security»

Marilyn Wolf & Dimitrios Serpanos

ISBN 978-3-030-25807-8

1st devil of safety and security:
Vulnerabilities

2nd devil of safety and security:
Threats

3rd devil of safety and security:
Failures
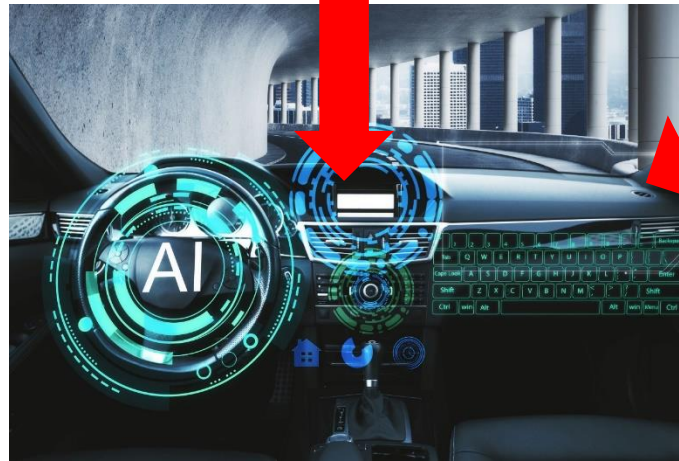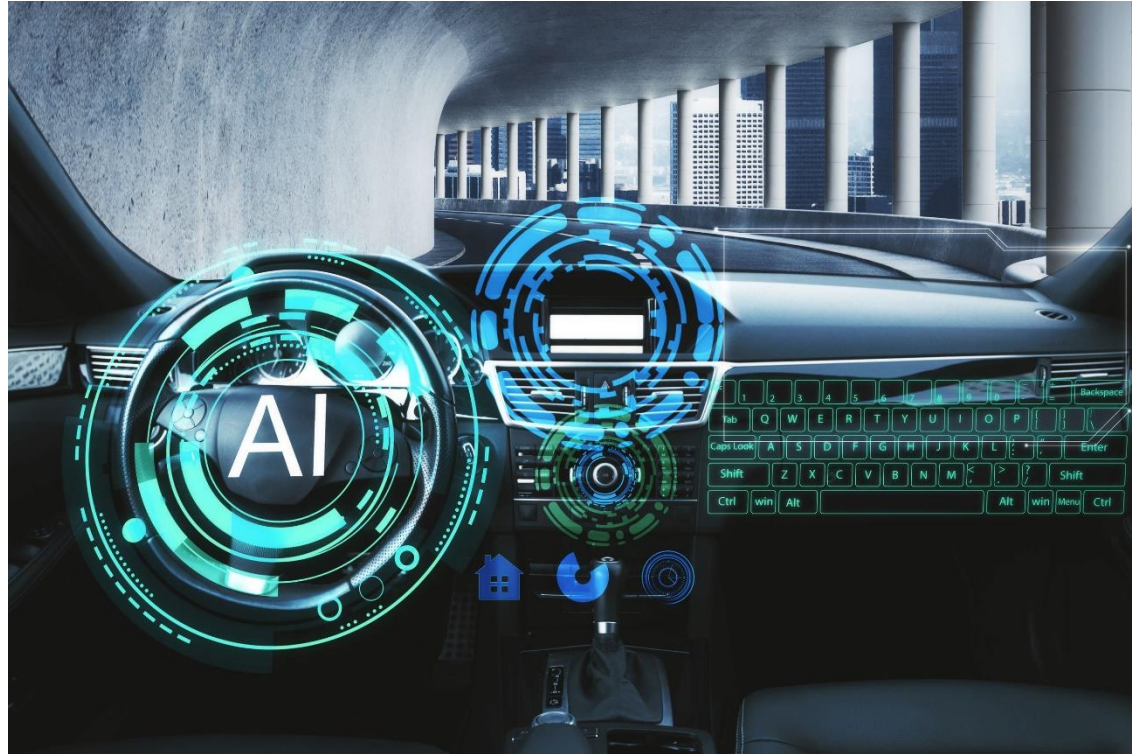
Content

Part 1

- Seminar Objectives
- Explanation of Title
- Setting the Scene
- Technology: Cyber-Physical Systems
- Safety & Security
- Engineering Safety & Security

Part 2

- Doing Research

Part 3

- Principles of a good Paper
- Principles of a convincing Presentation

Part 4

- Work Plan
- Next Steps

http://worldartsme.com

Trustworthy

Trustworthy CPS and CPSoS:

Cyber-physical system or cyber-physical system-of-systems

with an adequate degree of **safety** and **security**

to fulfill the trust expectations of its users

Risk Consideration

Protection from malicious activities

https://www.raymancini.academy

«The system does what it should - and does not what it should not»

Protection from failures, faults, errors, malfunctions

Risk Managment = Decisive Part of Systems Engineering !

http://www.osalp.com.pk

Safety

Safety

Safety is the state of being protected against faults, errors, failures, or any other event that could be considered non-desirable in order to achieve an acceptable level of risk concerning loss of property, damage to life, health or society, or harm to the environment.

Safety is
the sum of all accidents
that did <u>not</u> happen

Fault-tolerance

Graceful degradation

Availability

Fail-safe states

…

Quality of Service
Properties for
SAFETY

https://www.aeteurope.com

Security

Information Security

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

Functional Security

Functional security protects the software-system from **malicious, infiltrated code**, both from the outside and from the inside of the organization

Confidentiality

Integrity

Availability

…

Quality of Service Properties for **SECURITY**

Safety

Security

Traditionally, safety and security were **two different** fields of engineering

Road Vehicles - Fuctional Safety

Cyber-Security Standard

http://tacsafe.net

https://de.coursera.org

https://www.qa-systems.com

https://www.information-age.com

Car Hacking

Aeroplane Hacking

Merging of Safety and Security Engineering!
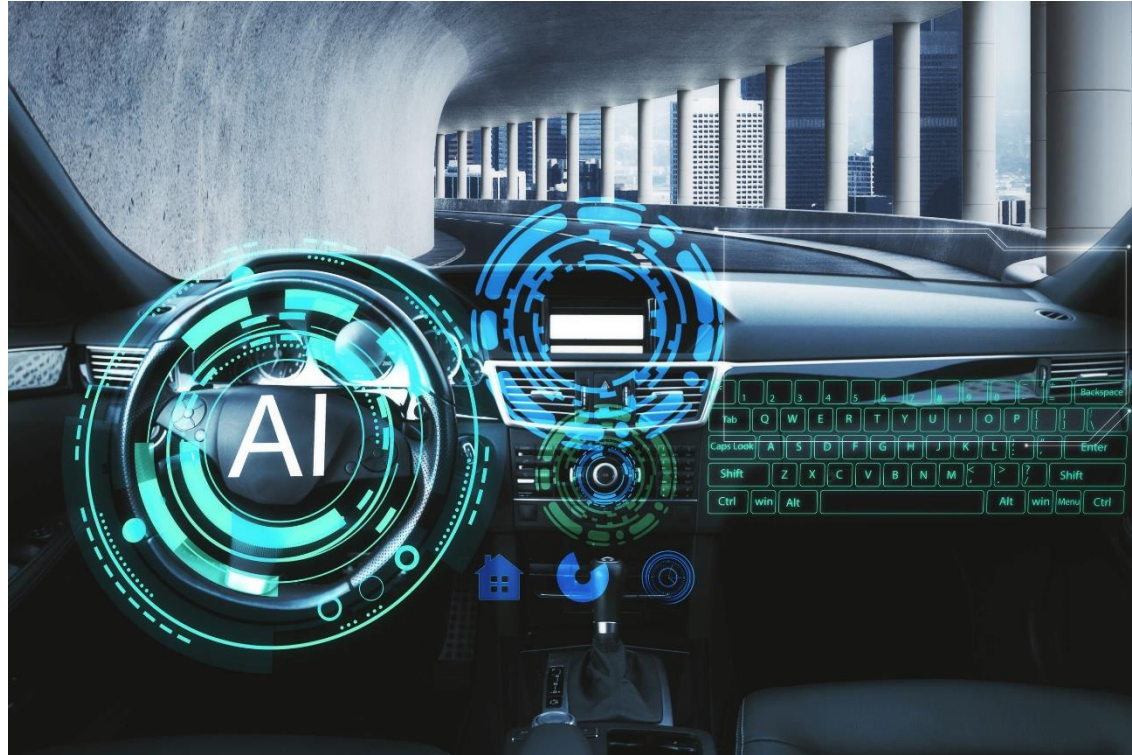
https://koddos.net

In 2016, the two cybersecurity researchers, Charlie Miller and Chris Valasek, remotely compromised a Jeep Cherokee. They were able to disable the car's transmission and brakes, and, while the vehicle was in reverse, take over the steering wheel

https://www.theverge.com/2016/8/2/12353186/car-hack-jeep-cherokee-vulnerability-miller-valasek

In August 2019, an engineer for a cyber-software company said he found serious security and safety flaws with the Boeing 787 jets.

The engineers said a code vulnerability in the jets software can *be hacked through the plane's entertainment system*

https://abc7chicago.com/5452768/

Content

Part 1

- Seminar Objectives
- Explanation of Title
- Setting the Scene
- Technology: Cyber-Physical Systems
- Safety & Security
- Engineering Safety & Security

Part 2

- Doing Research

Part 3

- Principles of a good Paper
- Principles of a convincing Presentation

Part 4

- Work Plan
- Next Steps

Safety and **Security** are the results of competent and responsible engineering

Competence: The ability to do something well
https://dictionary.cambridge.org/dictionary/english/competence

https://kayaconnect.org

A duty or obligation to satisfactorily perform or complete a task that one must fulfill, and which has a consequent penalty for failure
http://www.businessdictionary.com

Systems engineering is an interdisciplinary field of engineering and engineering management that focuses on how to design, implement, maintain and manage complex systems over their life cycles
https://en.wikipedia.org/wiki/Systems_engineering

https://w-dog.net

https://www.charteredengineers.sg
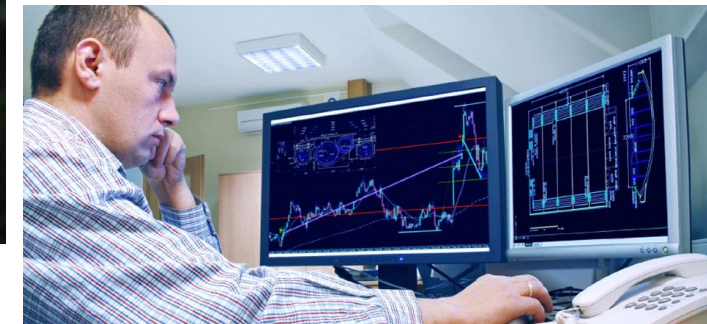
System extension
→ Project

new

TOP PRIORITY

Safety and Security concerns/requirements have _**higher priority**_ than functionality

Reqs

Safety

Functionality

Security

deleted

modified

Risk Management

© HS Prof. Dr. Frank J. Furrer – SS 2022

Safety & **Security**: Central Concept: **Risk**

https://english.khabarhub.com

Safety

Functionality

Security

ACCIDENT

206C69744746C6
20Data Breach
616368865732040

https://def.camp/

Safety is the state of being protected against faults, errors, failures, or any other event that could be considered non-desirable in order to achieve an **acceptable level of risk** concerning loss of property, damage to life, health or society, or harm to the environment.

No technical system can have zero risk

Engineering must reduce the risk to acceptable residual risks

RISK RISK RISK RISK
CONTROLS
Residual Risk

https://marketbusinessnews.com

Security protects the confidentiality, integrity, and availability (CIA) of data and functionality from unauthorized and malicious **accesses** and protects the software-system from **malicious, infiltrated code and data**

Safety & Security: Central Concept: **Risk**

Definition: Risk

A **probability** or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through preemptive action

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

ISBN 978-0-7494-8307-4

Definition: Risk Management

The identification, analysis, assessment, control, and avoidance, minimization, or elimination of <mark>unacceptable risks</mark>

http://www.businessdictionary.com/definition/risk-management.html

Residual Risk

https://de.clipdealer.com

Risk Management = Fundamental function in an CPC-development/evolution

Fundamentals of **Risk Management**
5th Edition

Understanding, evaluating and implementing effective risk management

Paul Hopkin
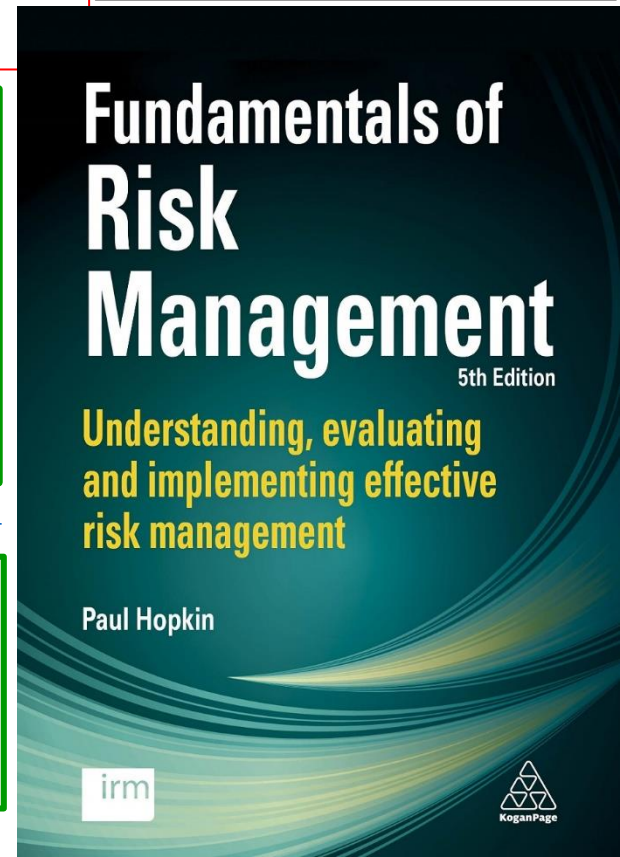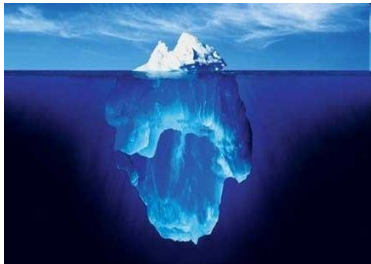
22.04.2022   © HS Prof. Dr. Frank J. Fu

Risk Management Process Essentials

ok

Identifiable Risks

Risk Identification, Recognition, and Description

→

Vulne- rability Detection

→

Risk Assessment [Potential Damage, Probability]

→

Risk Mitigation (Protection, Controls)

Residual Risk Assessment

Threat

inacceptable

Hidden Risks

RESILIENCE

Resilience Engineering

https://mdf.nl

Resilience Engineering
Concepts and Precepts

Edited by
ERIK HOLLNAGEL
DAVID D. WOODS
NANCY LEVESON

https://www.istockphoto.com

https://www.osb-i.com

22.04.2022

© HS Prof. Dr. Frank J. Furrer – SS 2022

ISBN 978-0-7546-4904-5
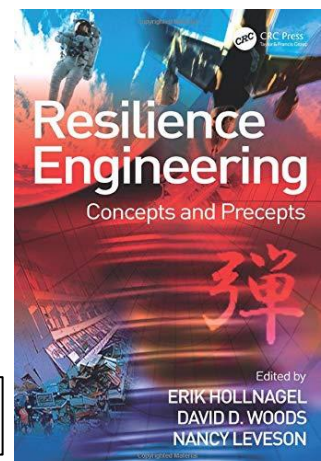
Risk Management Process

The result of the risk management process is a risk assessment and risk control **document**

ISBN 978-1-138-07532-0

Safety Case

Security Concept
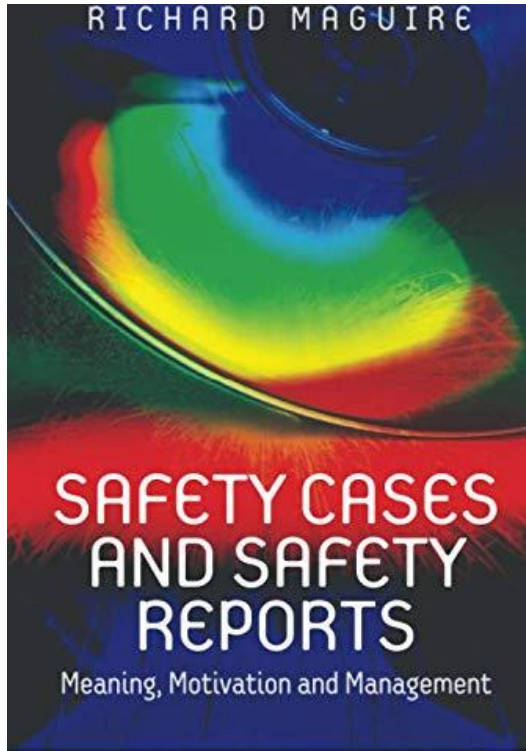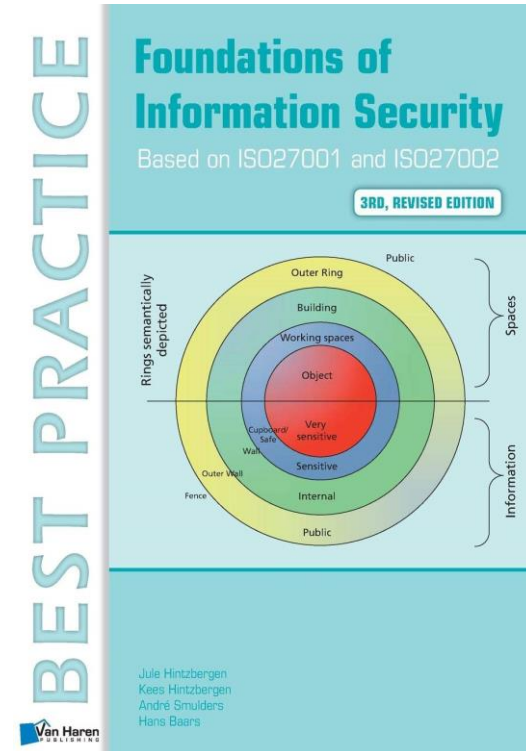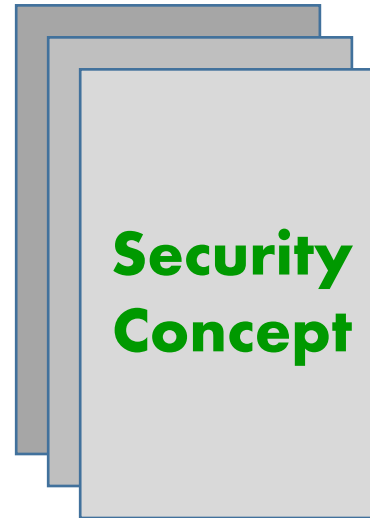
ISBN 978-94-018-0012-9

Content

Part 1

- Seminar Objectives
- Explanation of Title
- Setting the Scene
- Technology: Cyber-Physical Systems
- Safety & Security
- Engineering Safety & Security

Part 2

- Doing Research

Part 3

- Principles of a good Paper
- Principles of a convincing Presentation

Part 4

- Work Plan
- Next Steps

Doing Research

Research is the creative and systematic work

generating new knowledge or better understanding of existing knowledge

Problem or lack of specific knowledge

Paul Johannesson · Erik Perjons

An Introduction to Design Science

Springer

Solution Artefact

?

Initial Problem → Explicate Problem → Define Requirements → Design & Develop Artefact → Demonstrate Artefact → Evaluate Artefact → Research Result

Existing Knowledge Base

Research Question(s)

An Introduction to
Design Science

Paul Johannesson · Erik Perjons

Springer

https://www.eurobitume.eu

Key Concept:
Research Questions

Research Question(s)

A research question is a question that a study or research project aims to answer. This question often addresses an issue or a problem, which, through analysis and interpretation of data, is answered in the study's result

https://research.com/research/how-to-write-a-research-question

The research question(s) is the <u>starting point</u> of your work.

Its quality determines the <u>success</u> of your efforts.

RESEARCH.COM:
How to Write a Research Question - Types, Steps, and Examples
May 4, 2021. Free access:
https://research.com/research/how-to-write-a-research-question

Research Question(s)

Initial Problem → Explicate Problem → Define Requirements → Design & Develop Artefact → ~~Demonstrate Artefact~~ → Evaluate Artefact → Research Result

Existing Knowledge Base

F1: Choose a documented **safety accident** involving a cyber-physical system

F2: Choose a documented **security incident** involving a cyber-physical system

Formulate your Research Question(s)
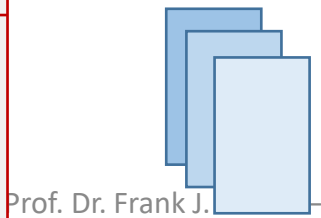
PEER REVIEW

https://de.123rf.com

https://www.wallpaperflare.com

https://sciblogs.co.nz

Prof. Dr. Frank J. ___ – SS 2022

64

http://de.123rf.com

Content

Part 1

- Seminar Objectives

- Explanation of Title

- Setting the Scene

- Technology: Cyber-Physical Systems

- Safety & Security

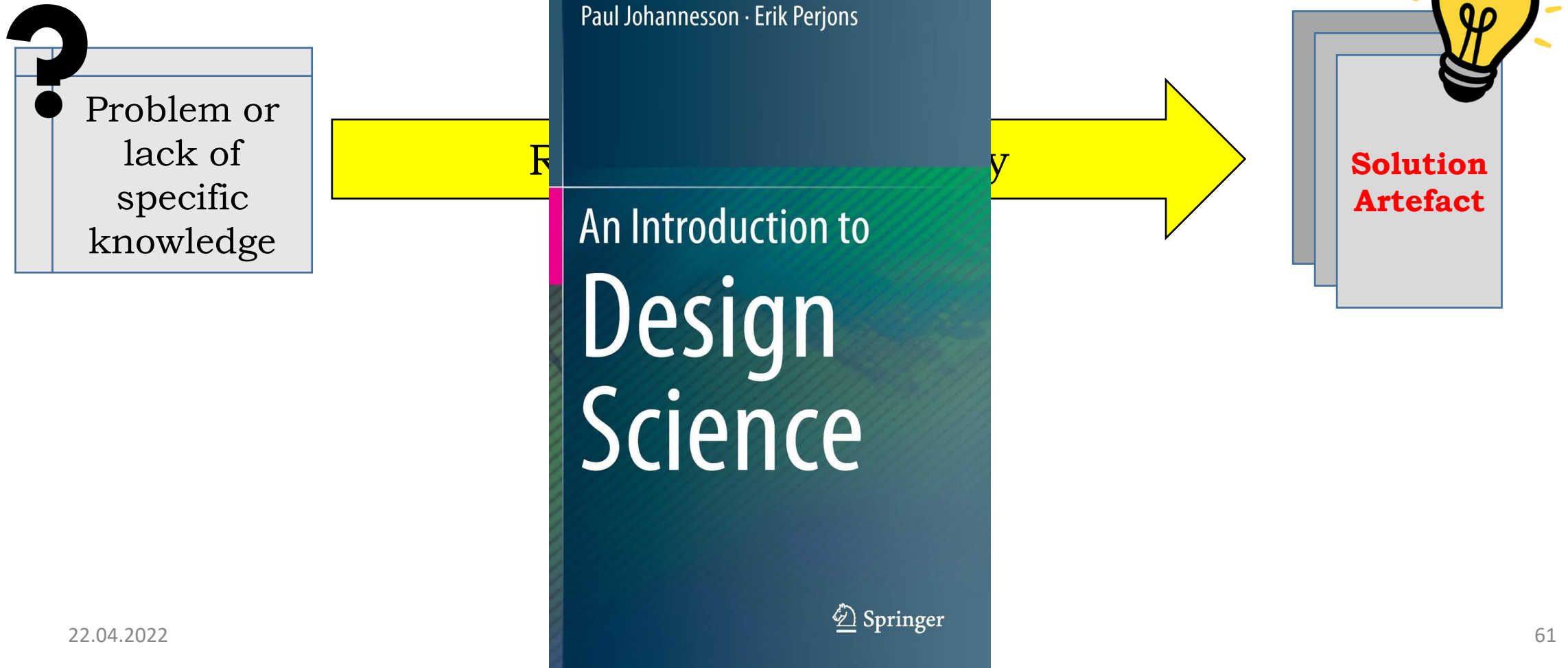- Engineering Safety & Security

Part 2

- Doing Research

Part 3

- Principles of a good Paper
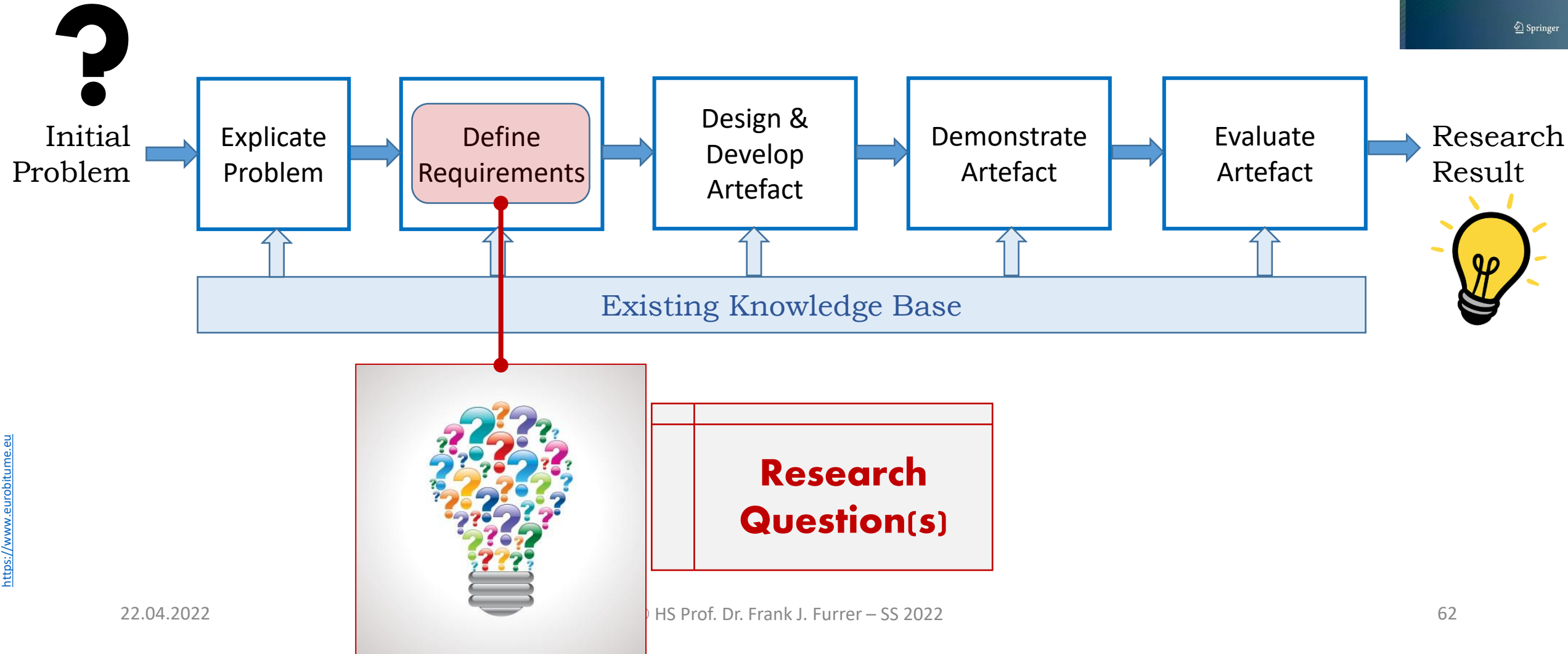
- Principles of a convincing Presentation

Part 4

- Work Plan

- Next Steps

© HS Prof. Dr. Frank J. Furrer – SS 2022

A good paper has:

http://www.florian-ultra.de

- A *valuable* message that will be *remembered*

- A *pleasurable* experience while reading it

http://gibloemfontein.sites.caxton.co.za
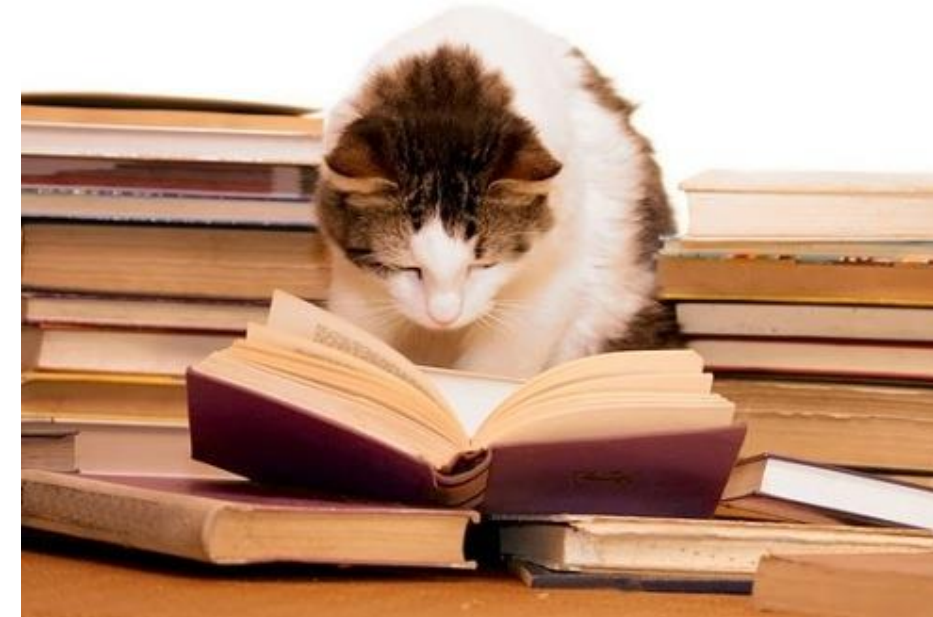
Key element = An interesting, consistent and complete **storyline**

Storyline = Logical, seamless sequence of ideas

The reader must be **_guided_** gently and pleasurably through your written material

- Logical and no breaks

- Understandable terminology

- **NO** unnecessary concepts

- Short and concise

- Good language

https://img.clipartfest.com

The **storyline** is a **document** which is written and reviewed *before* the first word of the paper is written

http://peccoud.org

REJECTED

A **weak** storyline is a sure reason for:

1. Annoying your reader
2. Get a rejection
3. Loose your reputation

Hauptseminar SS-2022
Prof. Dr. Frank J. Furrer
Engineering Principles for Safety and Security of Cyber-Physical Systems
Template for the Storyline
Name: _____
Version: _____
Date: _____

Available on the HS-Website

	Logical Step in Storyline	Remarks
1)	Paper Author:	
1)	Paper Title:	
1)	Paper Vision:	
1)	Paper Mission:	
1)	Literature/References used: [1] [2] [3] [4] [5] [6] Frank J. Furrer: Future-Proof Software-Systems: A Sustainable Evolution Strategy. Springer Vieweg Verlag, Wiesbaden, Germany, 2019. ISBN 978-3-658-19937-1.	Use the IEEE-notation for references (see [6]) Note: Ref [6] can be downloaded for free from SLUB as pdf
1)	Idea/Concept: Message: Bridge to next idea/concept:	

… or graphical storyline (Next slides)

Graphical Storyline Check

Key message:

«THORIUM
– The Green Energy Source of the Future»

The world needs a new, safe, and clean **band-energy** source

Consequences and Dangers of Uranium-Technology

- Radioactive waste
- Nuclear accidents
- Plutonium (weapons)

The world needs to **abandon** Uranium-Technology

Need for a new, clean and safe energy generation technology

- environment
- zero accident potential
- Large scale affordability

Which potential energy sources are promising?

Survey and assessment of energy generation technologies

- «green energy»
- Nature protection
- Long-term sustainability

Logical line of thought

Self-study

Graphical Storyline Check 2/3

Solution: Thorium!

Decision & justification for Thorium reactors

- «green energy» (CO_2, …)
- Practically no waste
- Unlimited supply

Put into **context**

Previous work & State of the art

- US Oak Ridge reactor
- Theory
- Current work

Which my role?

My contribution

- SoA description
- Assessment of promises
- Recommendations

Tutorial – because the technology is little known

Theory of Thorium Reactors (Th^{90} Nuclear Chain reaction)

- Some nuclear theory
- Breeder function
- Fuel chain

Th^{90} **technology** overview

Implementation of Thorium Reactors (Th^{90} breeders)

- Reactor types
- LFTR

Self-study

Graphical Storyline Check 3/3

Why is Th^{90} safe?

Safety, environmental assessment and long-term sustainability

- Emergency mechanisms
- Waste analysis
- Plutonium burner

What did we learn from this paper?

Findings & Recommendations

- Continue research
- Build CH-expertise (ETH)
- Generate confidence (Public)

What is the deduction from this paper?

Conclusions: Main points and future work

- «Message»
- Lessons
- Reason for further work

References

- Best possible
- Easily available
- To the point

Acknowledgments

- Fair
- Truthful
- Complete

Architecture of the Storyline

Storyline

Context

Vision

Mission

Focus

Material/body

Message

My contribution
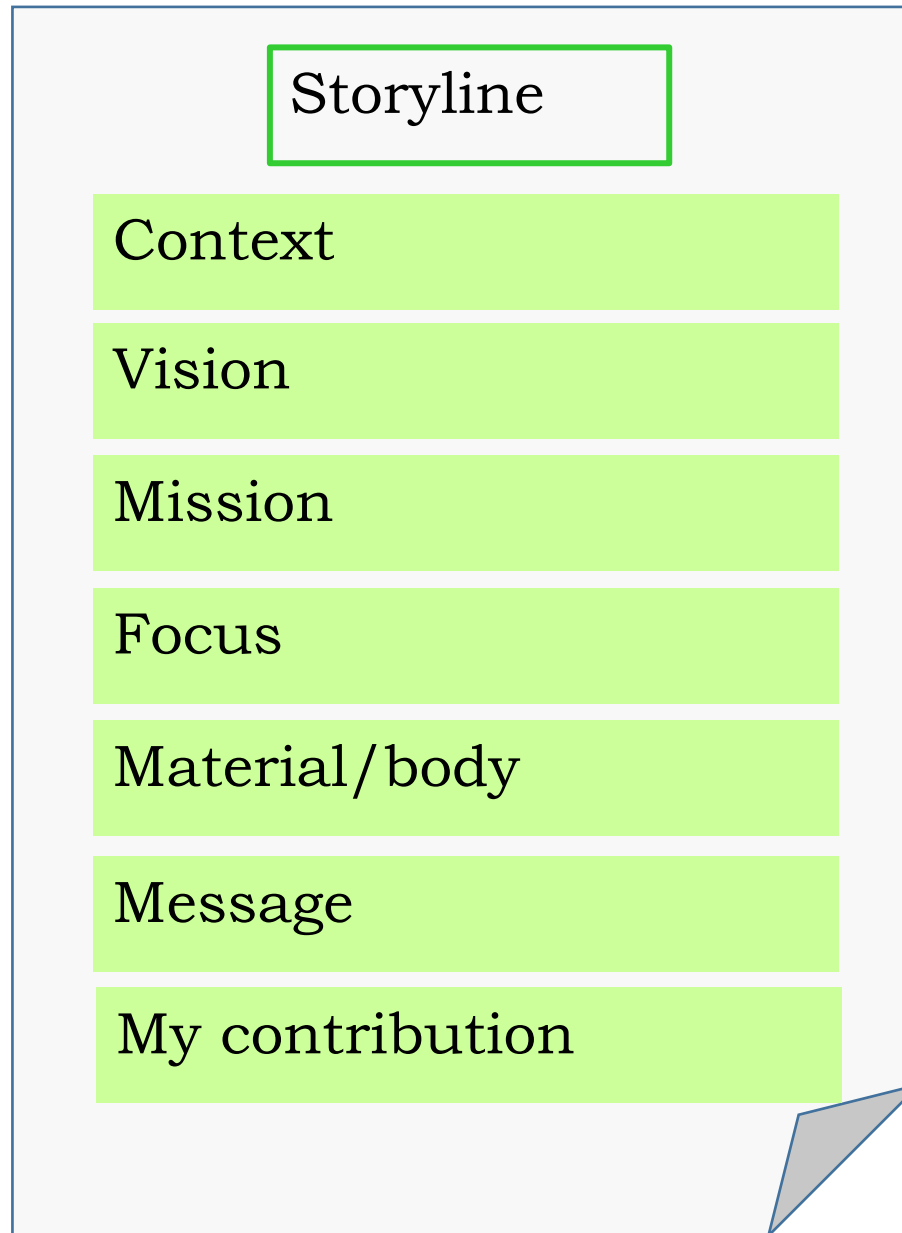
Self-study

Full **Storyline** Example

http://en.wikipedia.org/wiki/Traffic

Example:

Modern individual traffic

Self-study

Storyline:

Context

Vision

Mission

Focus

Material/body

Message

My contribution

CONTEXT

Individual traffic using trucks and private cars forms an important element of our economy and of our individual life-style.

In the last decades the amount of traffic has increased considerably.

The results are daily congestions and higher accident rates.

They cause significant damage to the economy and to our individual mobility.

http://en.wikipedia.org/wiki/Traffic

<u>Example:</u>

Modern individual traffic

Self-study

Storyline:

Context

Vision

Mission

Focus

Material/body

Message

My contribution

http://en.wikipedia.org/wiki/Traffic

What we want to **achieve**

„… how do we see an improved world"

(State [Utopia])

What we want to **do**

„… how do we improve the world"

(Action [Way to …])

Self-study

Storyline:

Context

Vision

Mission

Focus

Material/body

Message

My contribution

http://en.wikipedia.org/wiki/Traffic
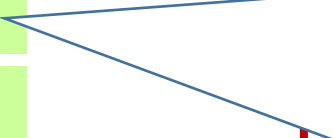
VISION

The vision is to keep traffic fluid, efficient and with low rates of accidents.

One promising approach is to support – or even replace – the drivers by electronic driving assistance systems.

Clear and comprehensive statement of the long-term goal
⇒ **Vision Statement**

Self-study

Storyline:

Context

Vision

Mission

Focus

Material/body

Message

My contribution

MISSION

This paper demonstrates the feasibility and implementation of one important electronic driving assistance system.

We present and discuss the sensor-based collision-avoidance systems.

Many such systems are under development - some of them can even be found in modern production cars.

Our target audience are graduate students in mechanical, electronics and computer science

Precise statement of the work
⇒ **Mission Statement**

Self-study

Storyline:

Context

Vision

Mission

Focus

Material/body

Message

My contribution

http://en.wikipedia.org/wiki/Traffic

FOCUS

Sensor-based collision-avoidance systems are a wide field of research.

It encompasses sensor-, software-, image processing- and safety engineering.

We focus on one specific system: The system developped by Mercedes-Benz which can be found in most of their current production cars.

We explain its architecture, functionality, features and limitations.

Self-study

Storyline:

Context

Vision

Mission

Focus

Material/body

Message

My contribution

http://en.wikipedia.org/wiki/Traffic

Restrict, restrict, restrict !

Organize, organize, organize !

Avoid <u>all</u> unnecessary concepts.

Establish a clear state-of-the-art, of prior work and of relevant references

Self-study

Storyline:

Context

Vision

Mission

Focus

Material/body

Message

My contribution

http://en.wikipedia.org/wiki/Traffic

This paper has demonstrated the great value of collision-avoidance systems.

Such systems could greatly be improved by using real-time environmental information.

Therefore, research should continue into dependable car-to-car and car-to-infrastructure communications

Self-study

Storyline:

Context

Vision

Mission

Focus

Material/body

Message

My contribution

My contribution was to explain the current collision avoidance system in the form of a tutorial for engineering students
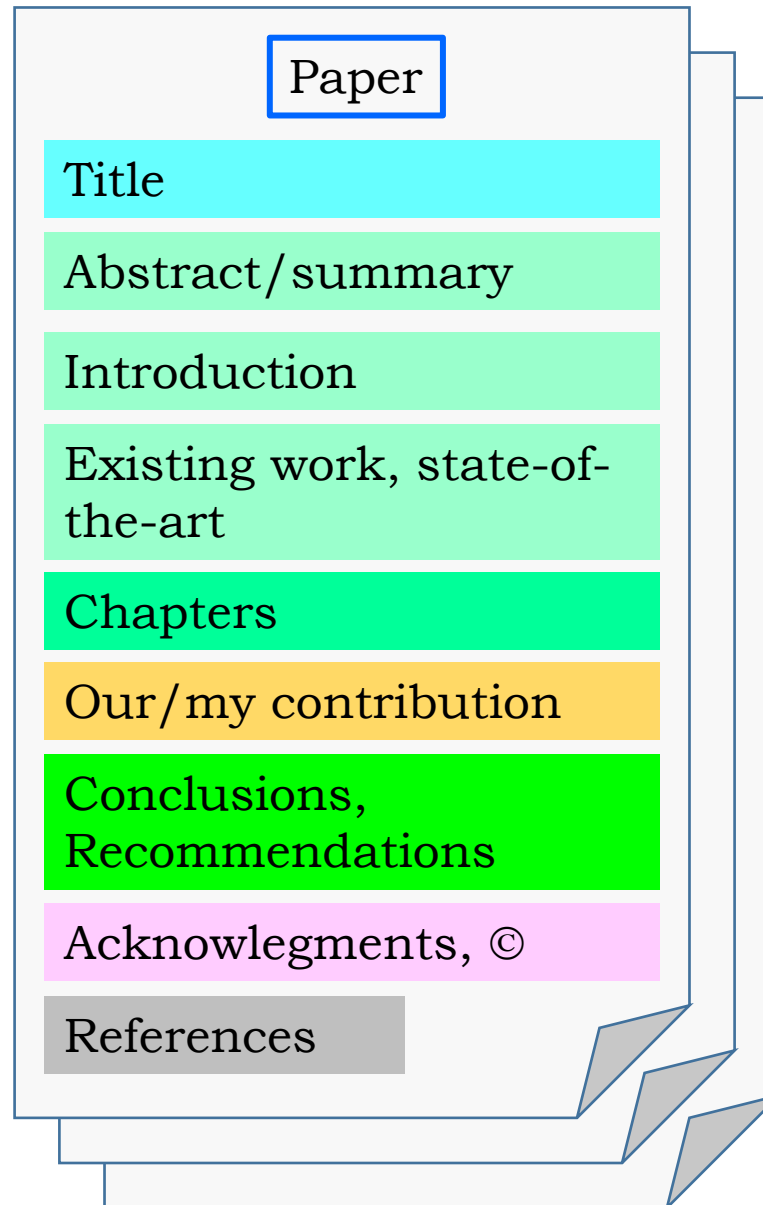
In addition I have shown the impact of the system on the avoidance of accidents

«I, my, …»
«**It** has been shown …»

Architecture of the Paper

Paper

Title

Abstract/summary

Introduction

Existing work, state-of-the-art

Chapters

Our/my contribution

Conclusions, Recommendations

Acknowlegments, ©

References

Hauptseminar SS-2022
Prof. Dr. Frank J. Furrer
Engineering Principles for Safety and Security of Cyber-Physical Systems

Template for the Storyline

Name: _____
Version: _____
Date: _____

Logical Step in Storyline	Remarks
Paper Author:	
Paper Title:	
Paper Vision:	
Paper Mission:	
Literature/References used: [1] [2] [3] [4] [5]	Use the IEEE-notation for references (see [6])
[6] Frank J. Furrer: Future-Proof Software-Systems: A Sustainable Evolution Strategy. Springer Vieweg Verlag, Wiesbaden, Germany, 2019. ISBN 978-3-658-19937-1.	Note: Ref [6] can be downloaded for free from SLUB as pdf
Idea/Concept: Message: Bridge to next idea/concept:	

√

Start authoring the paper only **after** you have finished the storyline to your **full** satisfaction

Paper

| Title |
| Abstract/summary |
| Introduction |
| Existing work, state-of-the-art |
| Chapters |
| Our/my contribution |
| Conclusions, Recommendations |
| Acknowlegments, © |
| References |
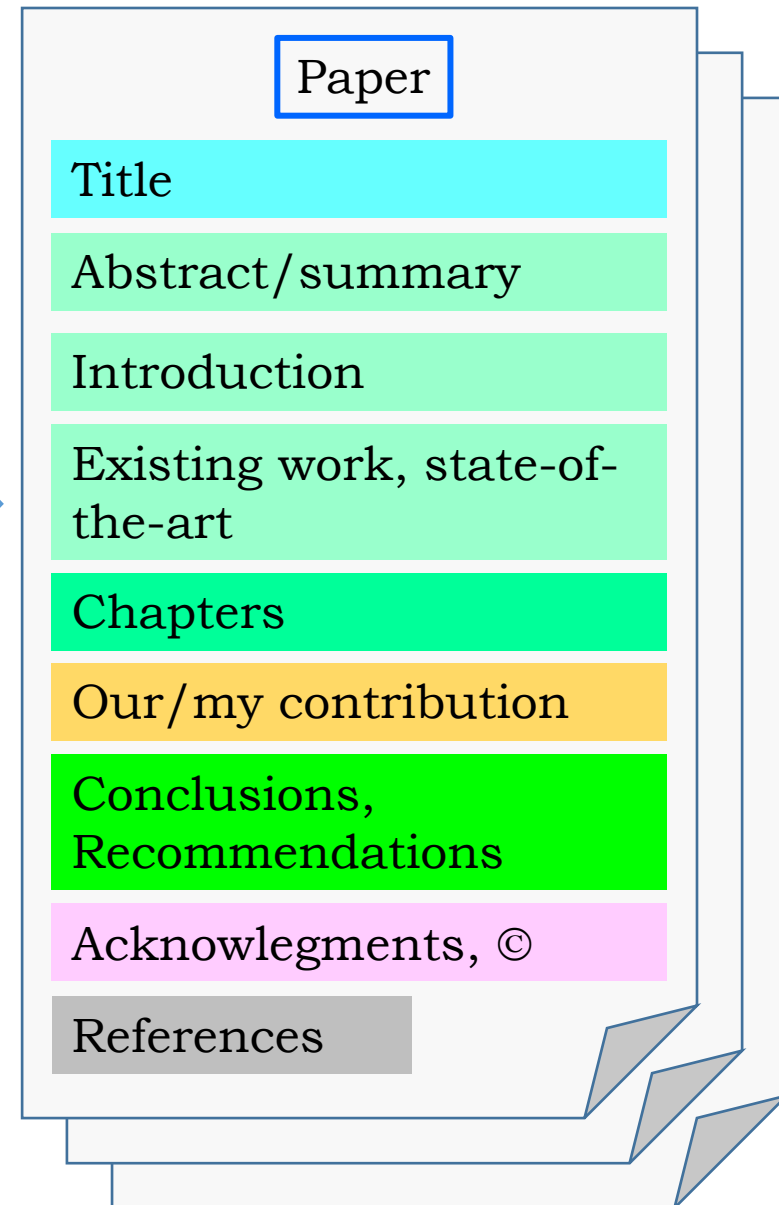
Importance of a promising title

Paper

| Title |
| Abstract/Summary |
| Introduction |
| Existing work, state-of-the-art |
| Chapters |
| Our/my contribution |
| Conclusions, Recommendations |
| Acknowlegments, © |
| References |

Reader Attention:

Circle Size = Attraction for the potential reader

Title

Abstract

Paper

http://blogs.nature.com
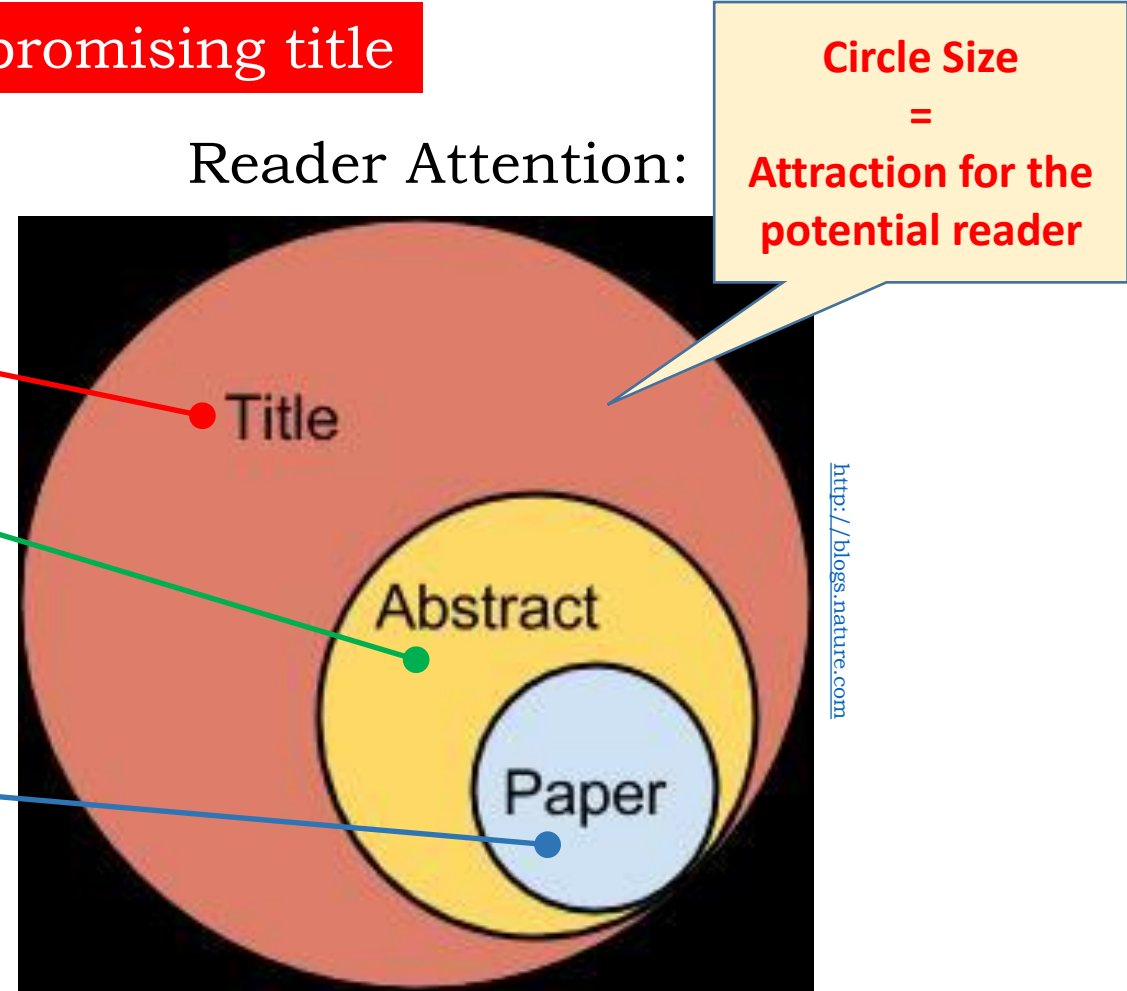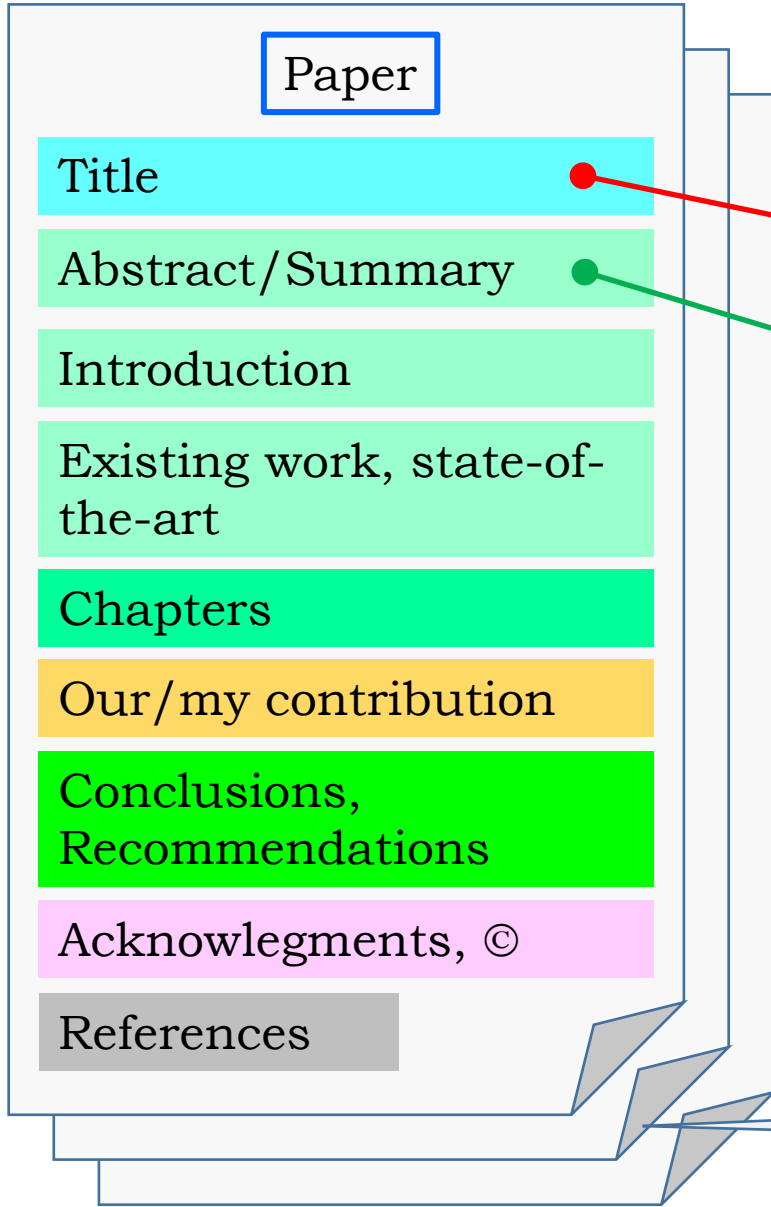
Typical structure of a good paper

Additional Topics of a good Paper:

- correct
- precise
- clear
- brief
- ethical
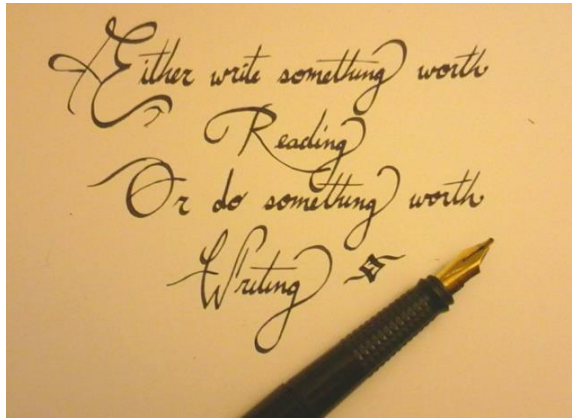
Style

Language

Versioning

Plagiarism

Term „Human" [Definition]:

We are bilaterally, symmetrical, sexually differentiated bipeds located on one of the outer spirals of the Milky Way, capable of recognising the prime numbers ...

[NASA Deep Space Probe]

Plagiarism is a serious Offence !

… and can fairly easily be detected ☹

Correct Language is mandatory !

Correct Language is mandatory !

Language

Use a spell checker!
https://www.grammarly.com
http://www.whitesmoke.com/
etc.

http://www.prsproof.net
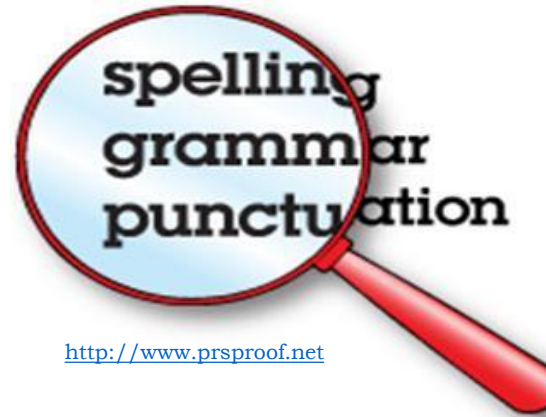
Versioning

Version all your documents!

Version	Date	Author(s)	Changes
0.1	13.2.17	Frank J. Furrer	Initial Draft
0.2	9.4.17	Hans Muster	Review + Additions

File Name:
HS17Paper_HansMuster_V03_20170410

Plagiarism is a serious Offence !

Plagiarism:
the act of presenting another's work or ideas as your own.
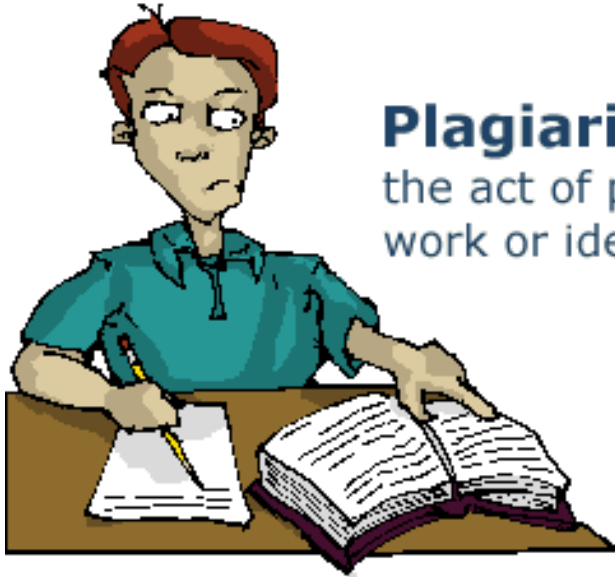
Intended Plagiarism
• **Willfully** done!

Unintended Plagiarism
• **Carelessly** done!

• Completely list **all** your references

• Carefully give credit to other authors

• Mark citations

• Add copyright notice (© xyz)

• Respect commercial rights

CUT & PASTE

Attention: Powerful Plagiarism **Checkers** exist, e.g.:
https://www.grammarly.com
https://www.quetext.com/
https://plagiarismdetector.net/
https://www.scribbr.com/plagiarism-checker/
https://copyleaks.com/plagiarism-checker
… etc.

Content

Part 1

- Seminar Objectives

- Explanation of Title

- Setting the Scene

- Technology: Cyber-Physical Systems

- Safety & Security

- Engineering Safety & Security

http://dailygrail.com

Part 2

- Doing Research

Part 3

- Principles of a good Paper

- Principles of a convincing Presentation

Part 4

- Work Plan

- Next Steps

What is the **difference** between a good paper and a convincing presentation?

… same basic principles

+

Less material

Pictures/Illustrations

Animations

Personal style

More expressiveness

FOCUS

https://violentmetaphors.files.wordpress.com

https://sarahzaki.files.wordpress.com

https://mbckonsult.com

http://www.wfs.org

Paper ⇔ Presentation ?

Illustrations/pictures

Animations

Personal style

- emotion
- feeling
- provocation

http://www.thanod.com
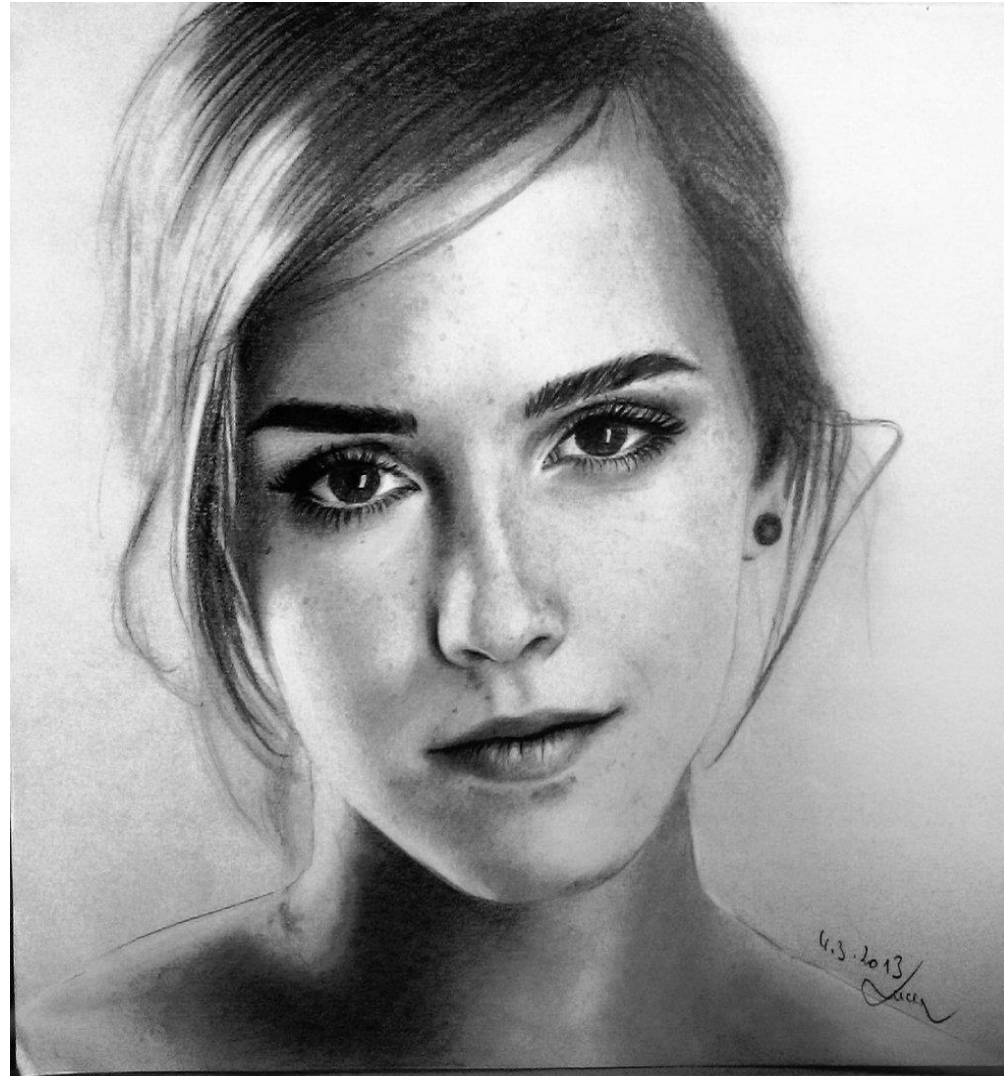
Paper ⇔ Presentation ?

Illustrations/pictures

Animations

Personal style

Cloud Definitions:

Software as a **S**ervice

Platform as a **S**ervice

Infrastructure as a **S**ervice

SaaS

PaaS

IaaS
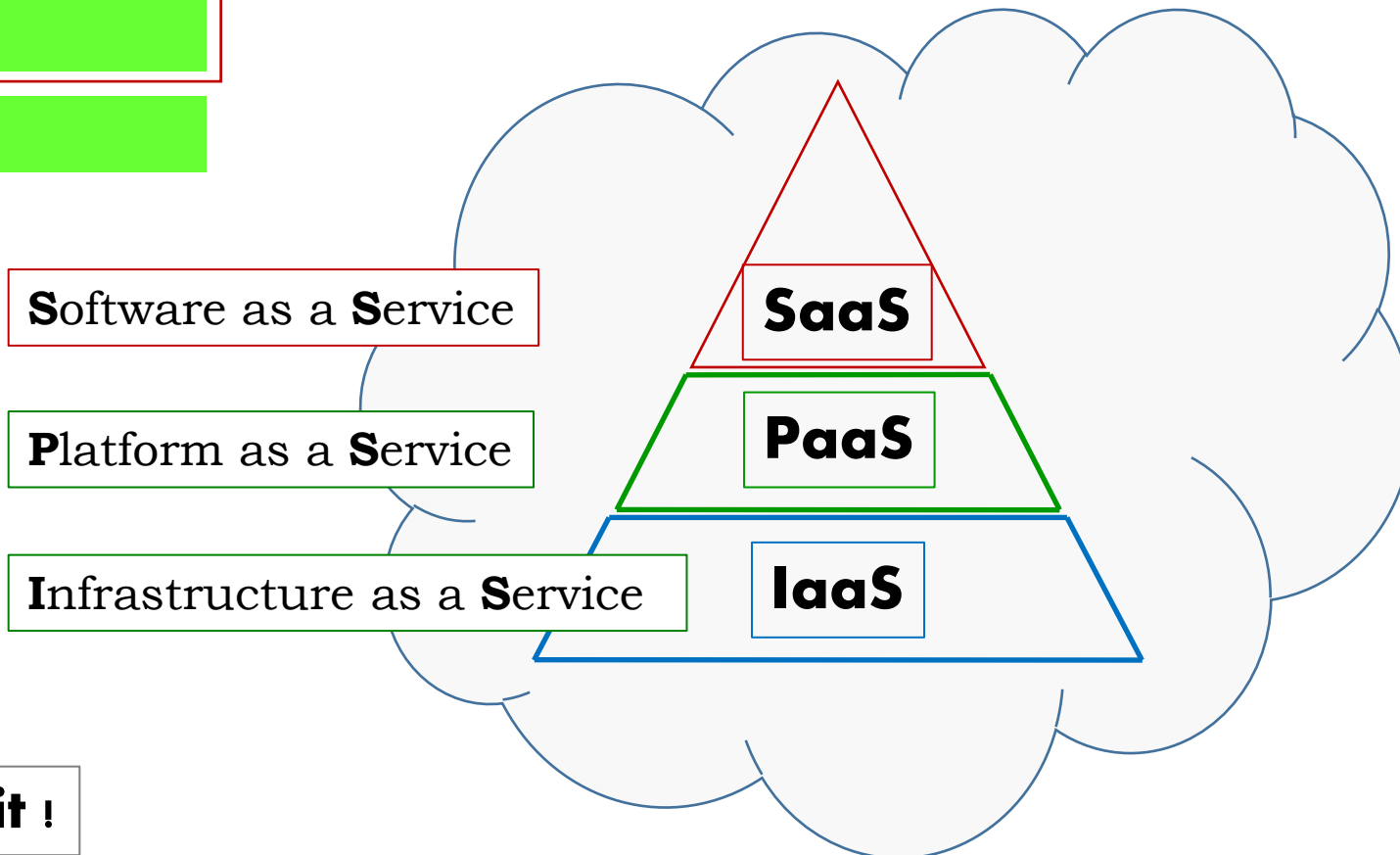
Don't overdo it !

Paper ⇔ Presentation ?

Illustrations/pictures

Animations

Personal style

- relate to your audience
- be highly present
- be strongly engaged

http://dailygrail.com

Additional Principles

https://prezentio.com

Time to Make Good-looking Slides

Principle 1: Understand your audience

Principle 2: Clear key message

Principle 3: Organized slide format

Specific principle 1: **Understand** your audience

Background ?

Prior Knowledge ?

Expectations ?

Reason for attendance ?

http://www.englishandculture.com

Tailor your presentation
to the background and needs
of your audience

Specific principle 2: **Key Message**

What is your message ?

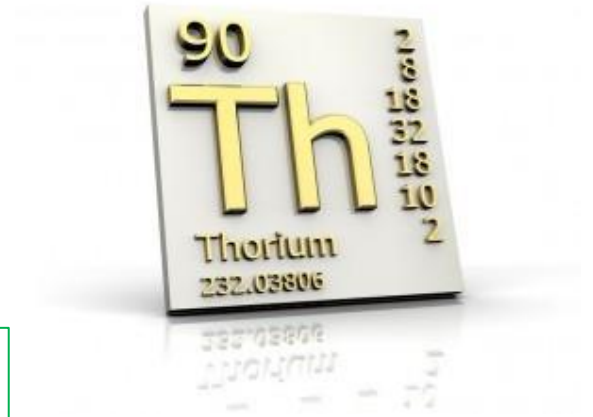Why is it important ?

What does it mean to your audience ?

What do you want them to remember ?

http://www.florian-ultra.de

The key message is the continuous **focus** of your presentation

Example: Thorium Nuclear Energy

Audience: YOU!

- *Background*: mathematical-physical-engineering education
- *Prior knowledge*: basic nuclear physics
- *Expectations*: Possible solution to world's energy problem?
- *Reason for attendance*: Critical assessment, gain of knowledge

Characterization of the Audience

Key message:

«THORIUM – The Green Energy Source of the Future»

Richard Martin: **Superfuel –** *Thorium, the green energy source of the future*.

Palgrave McMillan Publishers, New York, USA, 2012. ISBN 978-0-230-11647-4

Very promising message (and excellent title)

Slide Structure: Orientation

Institution

Topic

Slide design

The audience must feel well with the slide design

Date

Author, ©, event
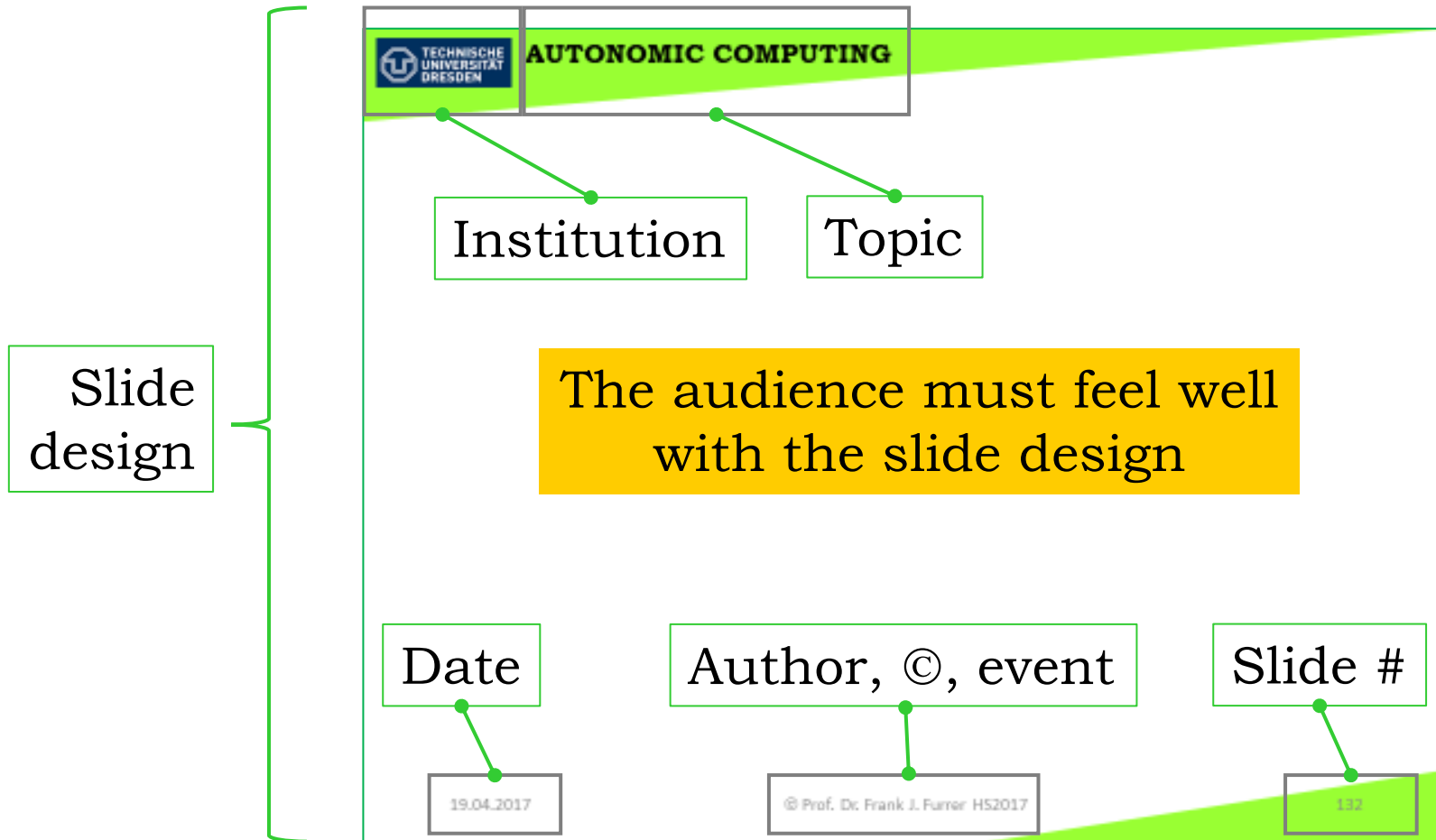
Slide #

Elements of a bad presentation:

- Small (< 22 pt) or unreadable fonts

- Too dense slides
- Few illustrations, pictures
- Excessive animations
- (Extensive) use of bullet point lists
- Unclear message, bad storyline
- Introduction of superfluous concepts
- … and some more

Garr Reynolds: **Presentation ZEN** – *Simple Ideas on Presentation Design and Delivery.*

New Riders Publishing, Berkeley CA, USA, 2008. ISBN 978-0-321-52565-9

ISBN 978-0-3218-1198-1
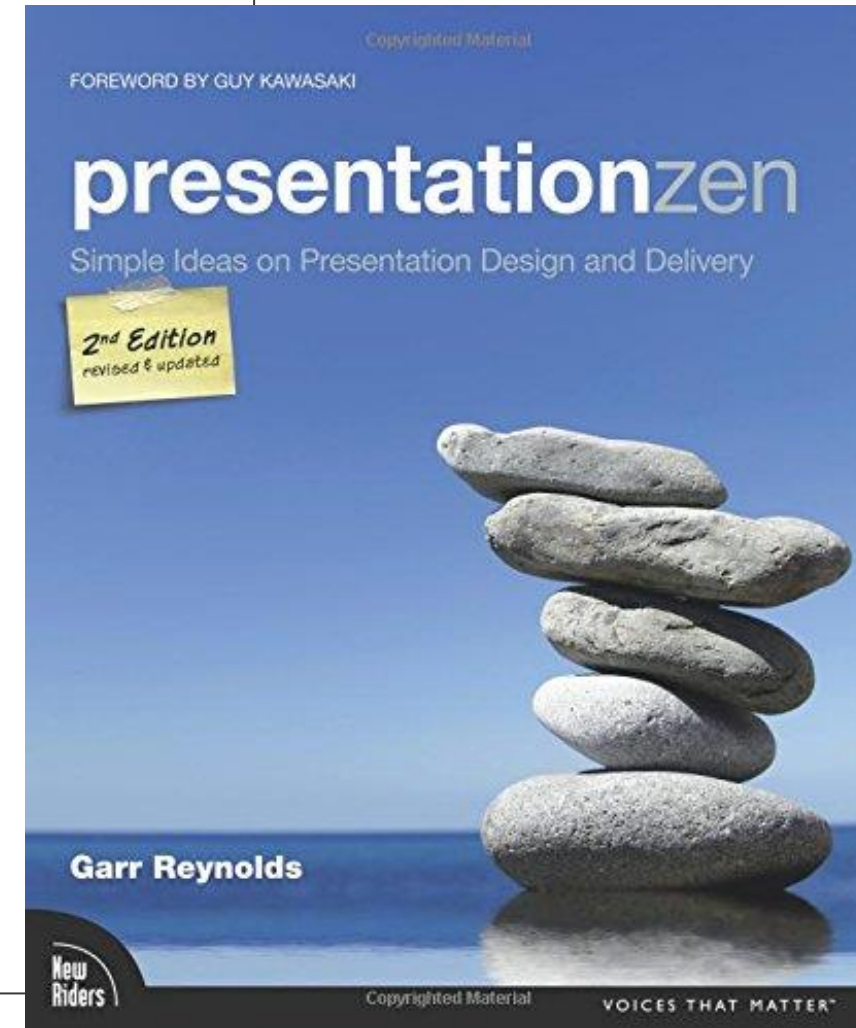
What is the sure **death** of a good presentation ?

Time overrun !

http://www.wfs.org

https://www.istockphoto.com

Summary

The Recipe for a good presentation:

1. *Understand* your audience

2. Have a clear and meaningful *message*

3. Follow a logical, consistent *storyline*

4. Use animated, well-designed *slides*

5. Invest your *personality*

6. Don't *overrun* time

https://openclipart.org

Content

https://carwad.net

Part 1

- Seminar Objectives

- Explanation of Title

- Setting the Scene

- Technology: Cyber-Physical Systems

- Safety & Security

- Engineering Safety & Security

Part 2

- Doing Research

Part 3

- Principles of a good Paper

- Principles of a convincing Presentation

Part 4

- Work Plan

- Next Steps

1. Read the lecture flyer
2. Understand the workplan
3. Careful self-study of the **Day 1 Presentation** of Prof. Dr. F.J.Furrer
4. Prepare a short introduction of yourself to the other participants
5. Prepare your questions related to the course material and workflow

HS Day 1 [April 22, 2022]

Peer Review

FEED BACK

1. Choose a CPS accident or incident
2. Formulate **Research Question(s)**
3. Deliver **storyline**
4. Deliver 1st presentation

HS Day 2 [May 27, 2022]

Peer Review

FEED BACK

1. Deliver Draft of **paper**
2. Deliver pre-final **presentation**

HS Day 3 [July 1, 2022]

1. Deliver final **paper**
2. Deliver final **presentation**

Receive assessment, grade and credits

HS SS22 Workplan (1/2)

Activity	Date/Deadline	Remarks
Hauptseminar Day 1 Meeting	**Friday, April 22, 2022: 09:20 – 10:50 (2. DS), Room APB/INF 2101**	• Introduction of the participants • **Introductory Lecture** by Prof. Dr. Frank J. Furrer • Confirmation of **contact information** (= List of participants) • Discussion of Workplan • Q/A • Commitment of Participants
Prof. Furrer selects 2 **peer reviewers** for each participant Note: **All** papers will also be reviewed by F.J. Furrer (as 3rd peer reviewer)	Thursday, April 28, 2022	Notification of participants by e-Mail
Read the **mandatory literature**	Monday, May 3, 2022	See lecture flyer and Day 1 meeting slides
1. Deliver **your choice** of cyber-physical system accident or incident (Literature & Web research) 2. Concise description, reference(s), justification of choice of your accident or incident 3. Deliver your **research question(s)**	Friday, May 6, 2022	e-mail your choice to: • Your peer reviewers • frank.j.furrer@bluewin.ch Note: only one topic (either F1 or F2 topic)
Feedback from Reviewers	Wednesday, May 11, 2022	By e-mail from: • Your peer reviewers • frank.j.furrer@bluewin.ch
Deliver your **storyline** to your peer reviewers & F.J.Furrer	Monday, May 16, 2022	**Use Storyline-Template from HS-Website or graphical representation from Day 1 lecture** e-mail your storyline to: • Your peer reviewers • frank.j.furrer@bluewin.ch

HS SS22 Workplan (2/2)

Storyline-Feedback from Reviewers & F.J. Furrer	Friday, May 20, 2022	By e-mail from: • Your peer reviewers • frank.j.furrer@bluewin.ch
Hauptseminar Day 2 Meeting	**Friday, May 27, 2022: 09:20 – 10:50/11:10 - 12:40 (2. + 3. DS), Room APB/INF 2101**	• Participants presentations • Peer discussions, Feedback on style & content
Deliver the **draft of your paper** to your peer reviewers (No storyline update required)	Monday, June 13, 2022	e-mail your paper to: • Your peer reviewers • frank.j.furrer@bluewin.ch
Feedback to paper from Reviewers & F.J. Furrer	Friday, June 17, 2022	By e-mail from: • Your peer reviewers • frank.j.furrer@bluewin.ch
Hauptseminar Day 3 Meeting	**Friday, July 1, 2022: 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
Deliver **final** version of your **paper** (WORD or pdf) Deliver **final** version of your **presentation** (ppt or pdf)	**Latest**: Friday, July 15, 2022	e-mail your final paper to: • frank.j.furrer@bluewin.ch • cc: your peer reviewers
Receive assessment, grade and credits (by e-Mail)	Latest: Friday, July 22, 2022	

http://hqwallbase.pw/82449-a-step-forward/

Content

Part 1

- Setting the Scene

- Explanation of Title

- Seminar Objectives

- Technology: Cyber-Physical Systems

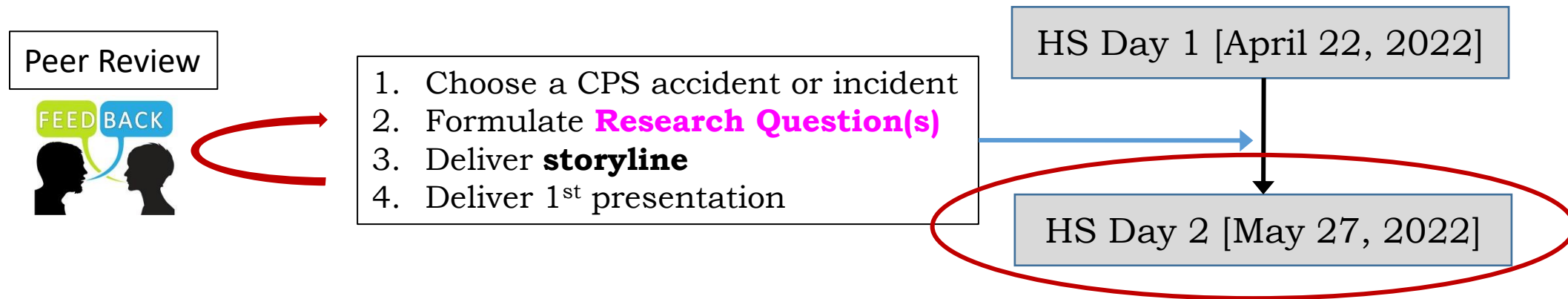- Safety & Security

- Engineering Safety & Security

Part 2

- Principles of a good Paper

- Principles of a convincing Presentation

Part 3

- Work Plan

- Next Steps

Peer Review

FEED BACK

1. Choose a CPS accident or incident
2. Formulate **Research Question(s)**
3. Deliver **storyline**
4. Deliver 1st presentation

HS Day 1 [April 22, 2022]

HS Day 2 [May 27, 2022]

Commitment

Who wants definitely to participate in the full Hauptseminar ?

© HS Prof. Dr. Frank J. Furrer – SS 2022

https://www.techannel.de