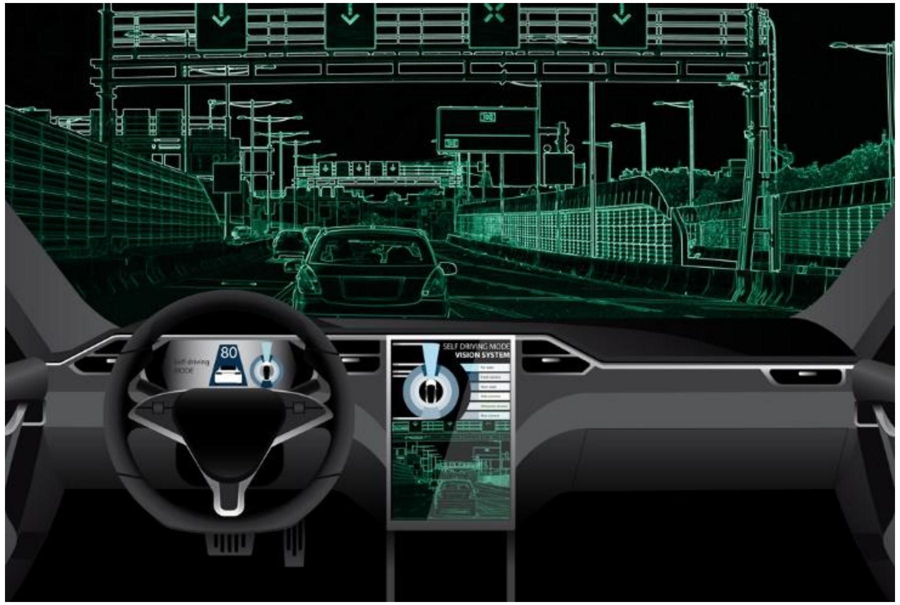
Ringvorlesung WS 2019/20 [Montag, 14.10.2019]

«Engineering Trustworthy Software for Cyber-Physical Systems»

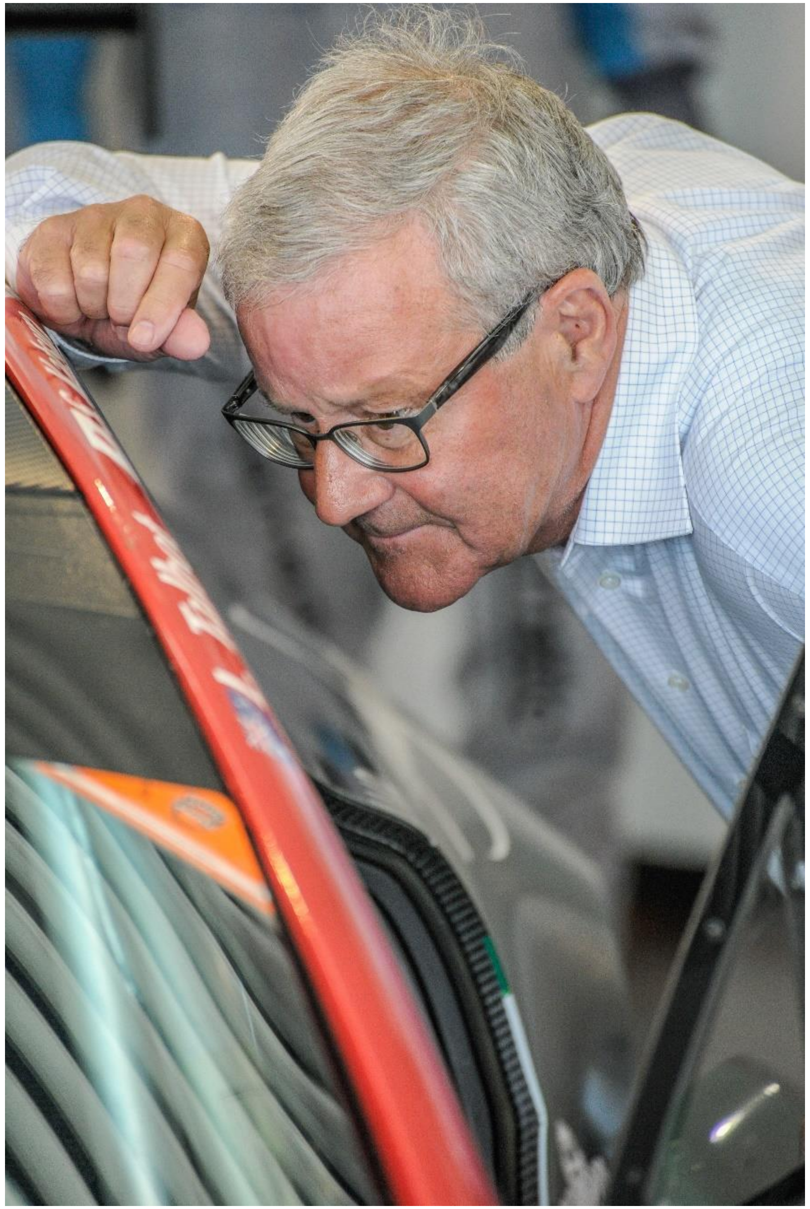
«Entwicklung von verlässlicher Software für Cyber-Physikalische Systeme»

Prof. Dr. Frank J. Furrer



© Shutterstock_746309743

V2.2/08.10.2019

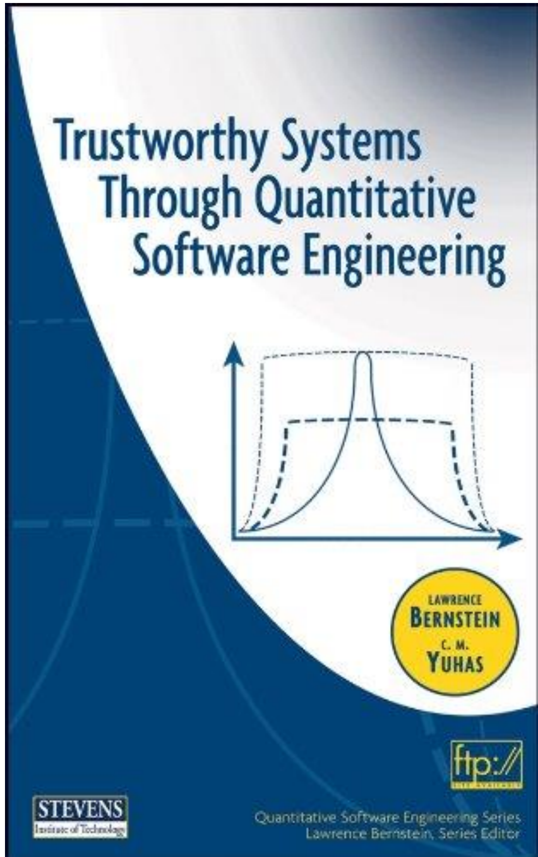


Prof. h.c. Dr. sc. techn. ETH-Z Frank J. Furrer

Contact Details:

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

Literature References introduced during the lecture



Trustworthy Systems Through Quantitative Software Engineering

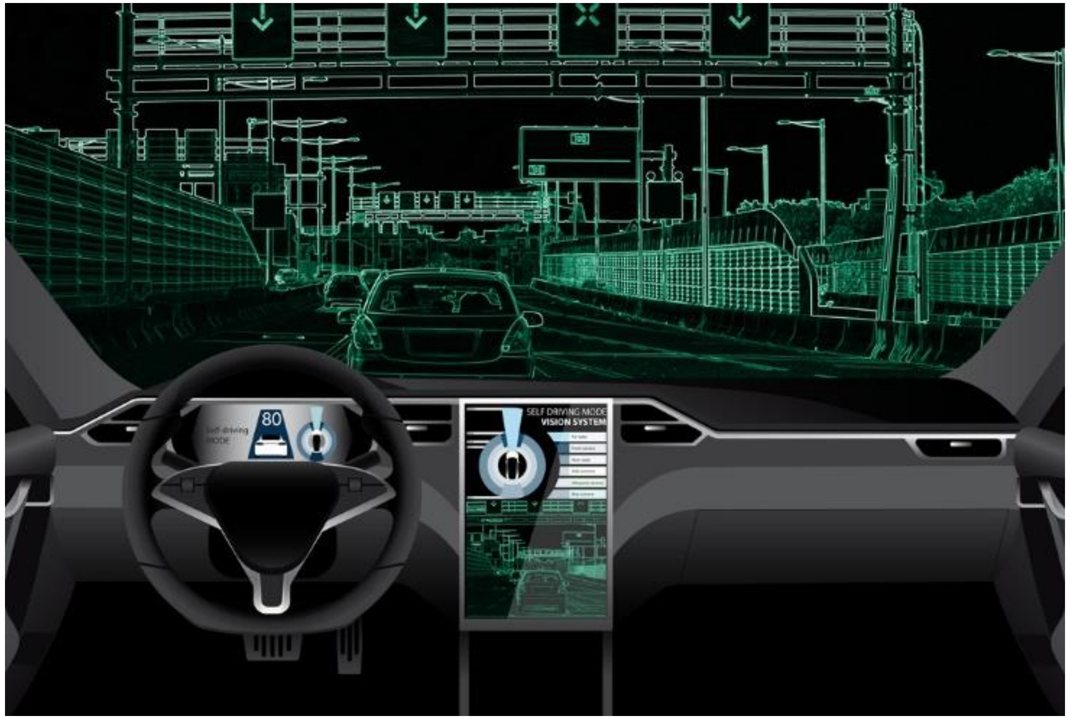
Lawrence Bernstein
C. M. Yuhas

ftp://

STEVENS Institute of Technology

Quantitative Software Engineering Series
Lawrence Bernstein, Series Editor

Engineering Trustworthy Software for Cyber-Physical Systems



Content

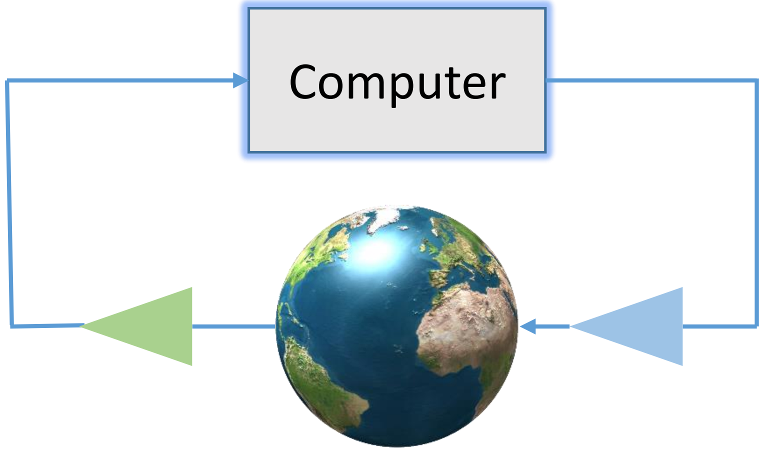
- Introduction
- Technology: Cyber-Physical Systems
- Trustworthiness
- Engineering
- Conclusions

«Engineering Trustworthy Software for Cyber-Physical Systems»

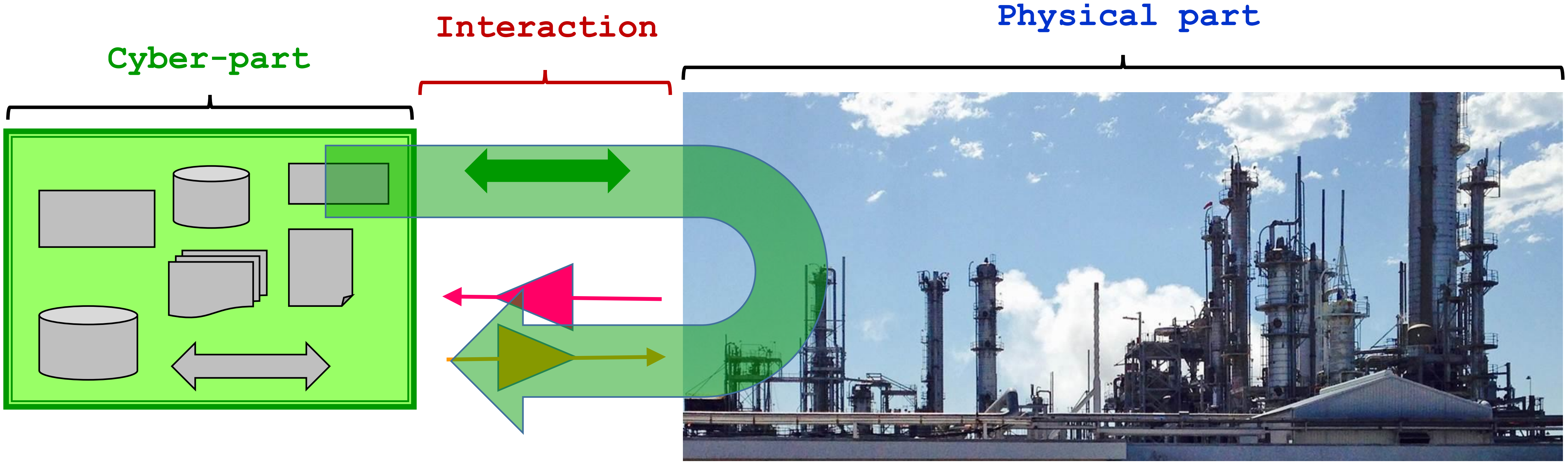
Systems engineering is an interdisciplinary field of engineering and engineering management that focuses on how to design, implement, maintain and manage complex systems over their life cycles
https://en.wikipedia.org/wiki/Systems_engineering

Cyber-physical system with an adequate degree of **security** and **safety** to fulfill the trust expectations of its users

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
R. Alur, 2015



Cyber-Physical System



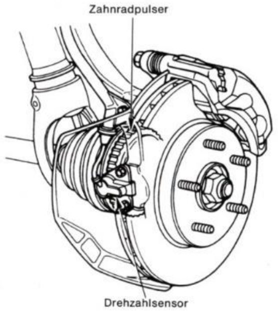
http://www.eternaaddaily.com

Software Control Loop

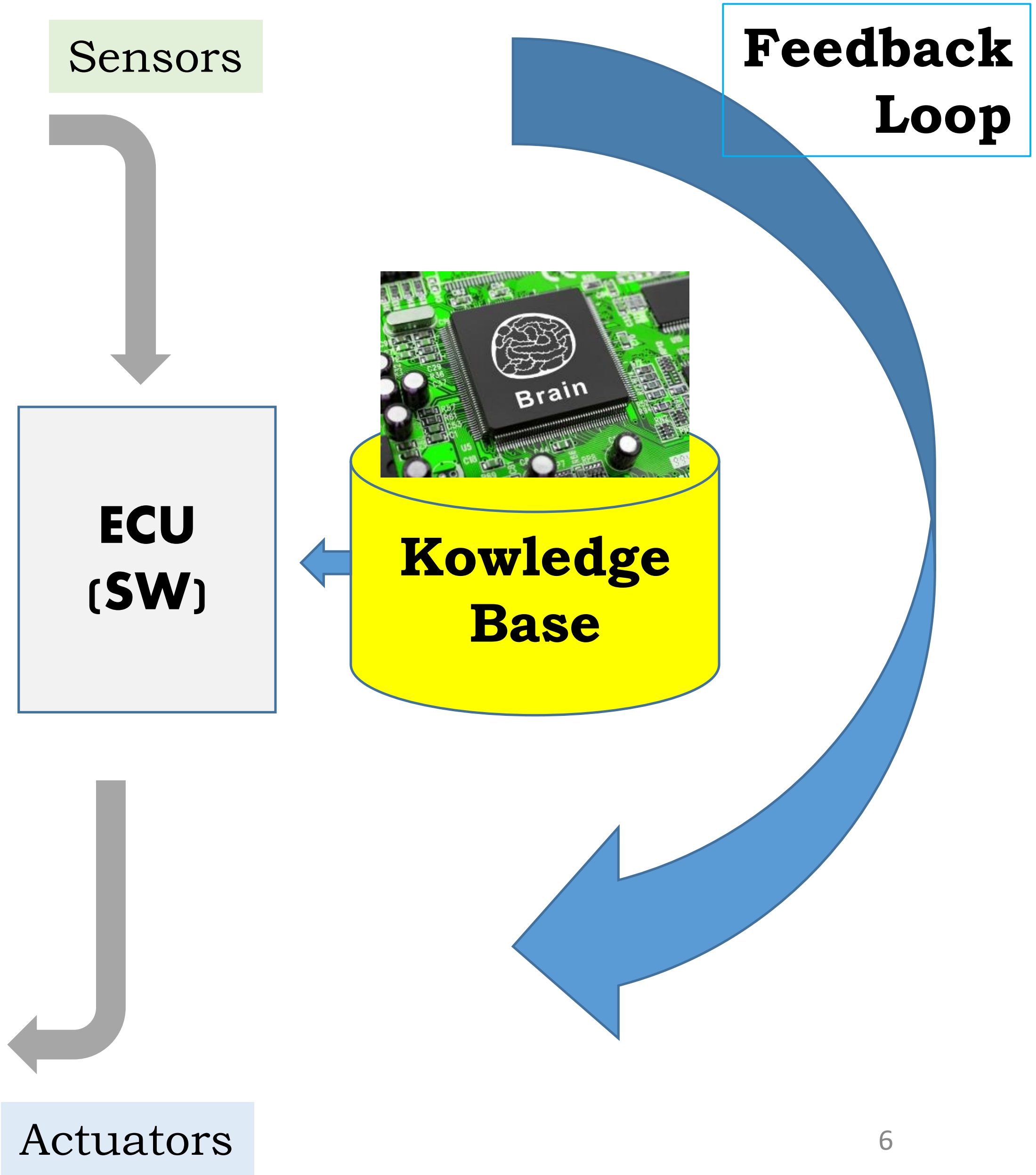
Sensors: Read plant information

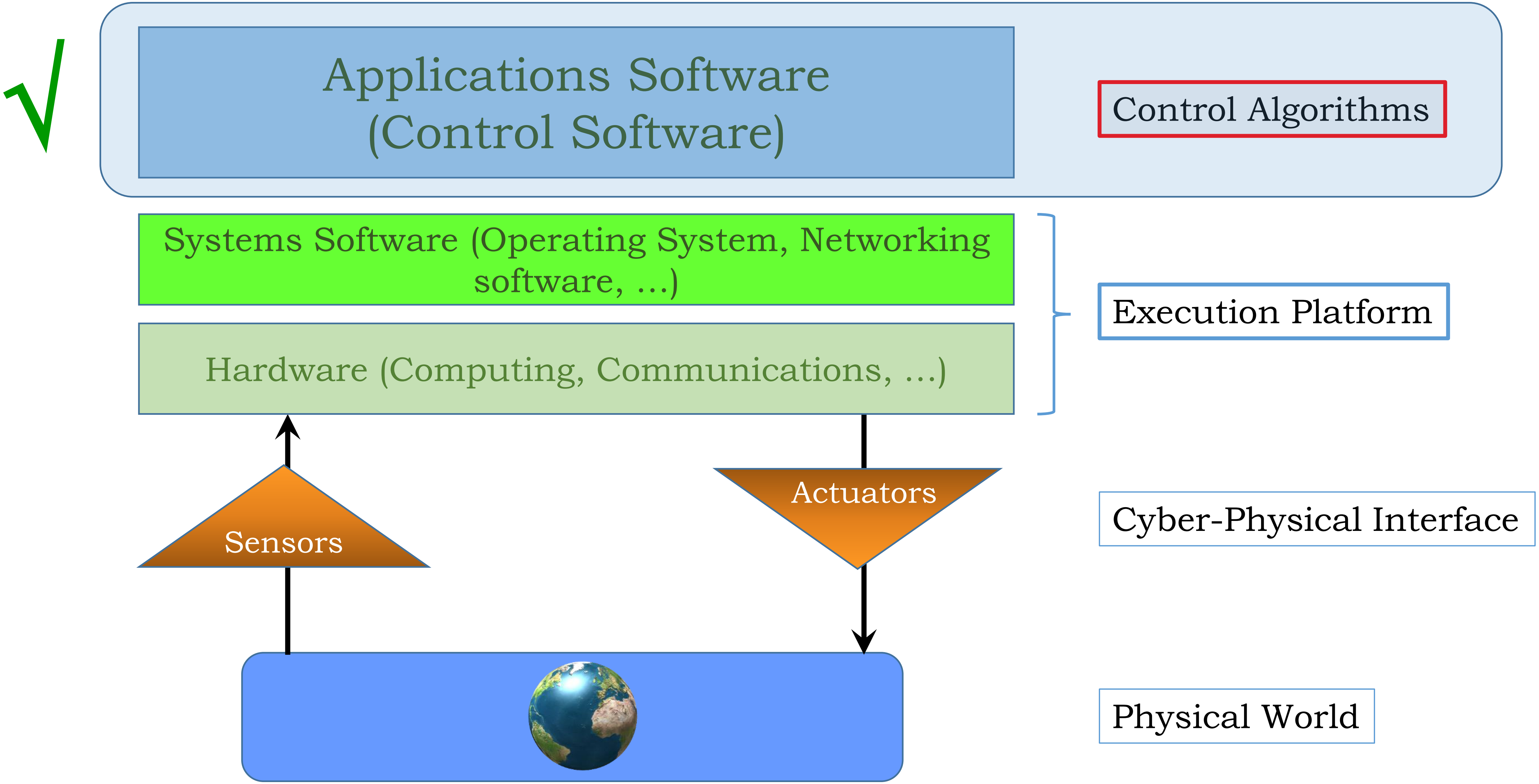
Actuators: Control plant

CPS-Example: **ESC**



http://www.polizeiticker.ch





√

Applications Software (Control Software)

Control Algorithms

Systems Software (Operating System, Networking software, …)

Hardware (Computing, Communications, …)

Execution Platform

Sensors

Actuators

Cyber-Physical Interface

Physical World

Applications Software (Control Software)

Control Algorithms

https://www.schoenesleben.ch

Trustworthy Software

https://marketingland.com

- Functional Properties
- Non-Functional Properties

Safety

Security

Other Properties

- Performance
- User-Friendliness
- Energy-Minimization
- … illities

https://avnetlaw.com

Image credit: istockphoto.com/rscyther5
https://www.ndtv.com

Safety

Security

https://avnetlaw.com

Image credit: istockphoto.com/rscyther5

https://www.ndtv.com

Definition: 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.

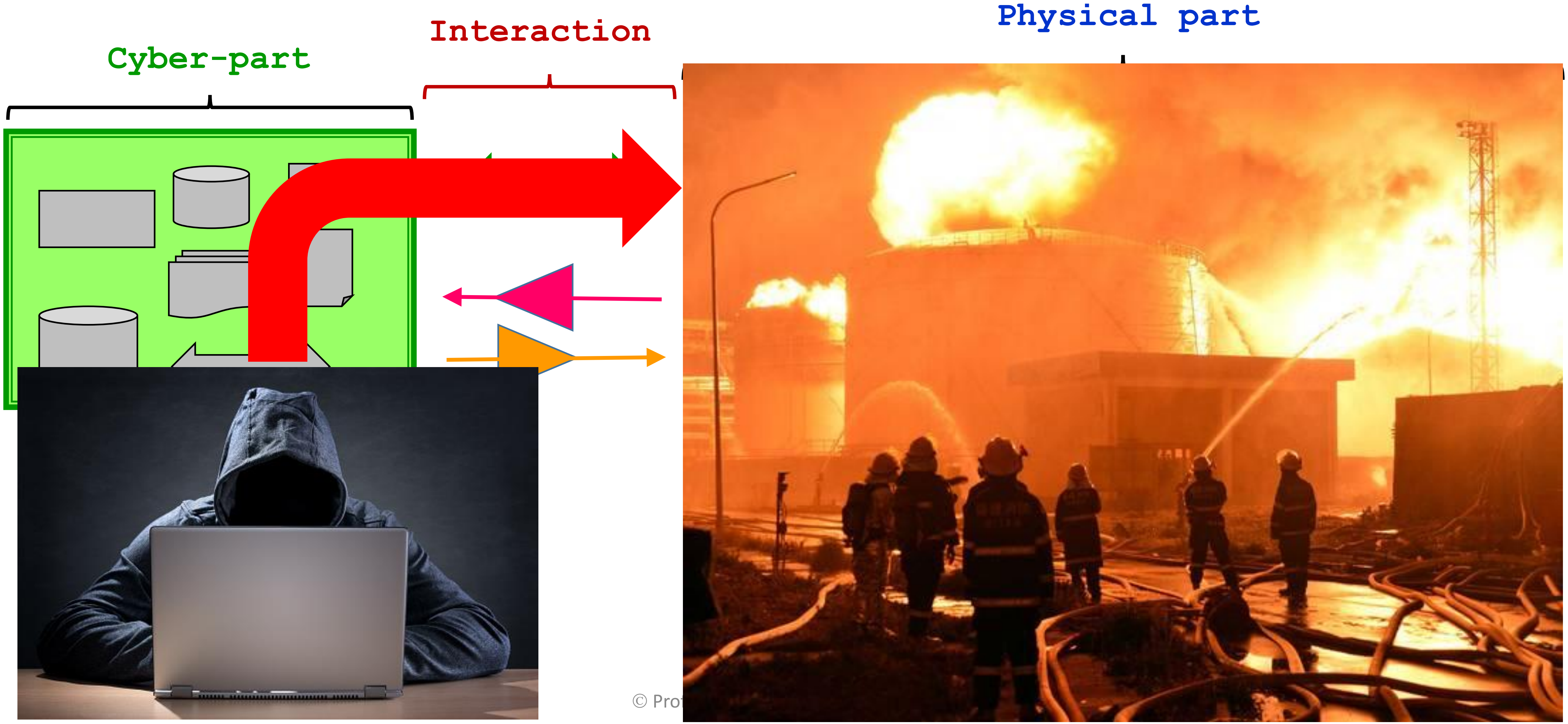
Definition: Information Security

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

Definition: Functional Security

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

CPS-Example: **Security Risk**



http://www.etemaaddaily.com

CPS-Example: Safety Risk

Both planes crashed **nose-down**

What happened?

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

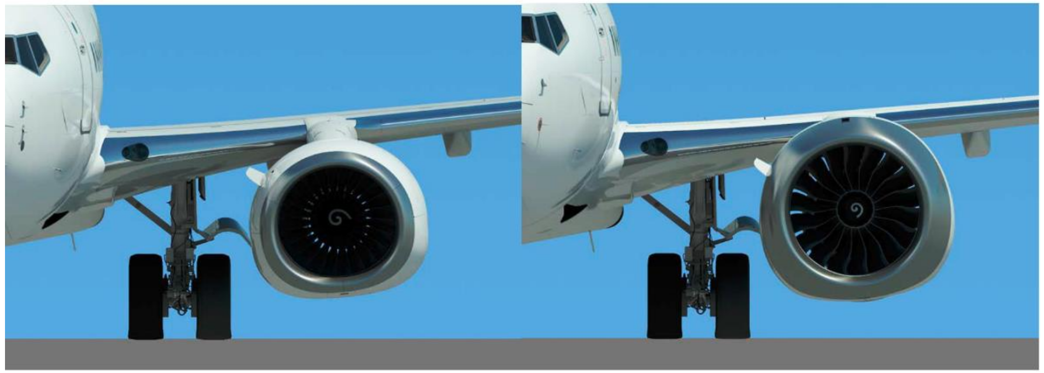
https://www.abc.net.au

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

https://www.aerotelegraph.com

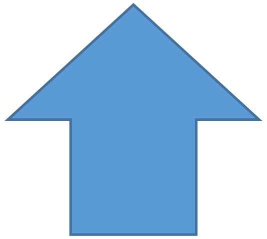
CPS-Example: **Safety Risk**

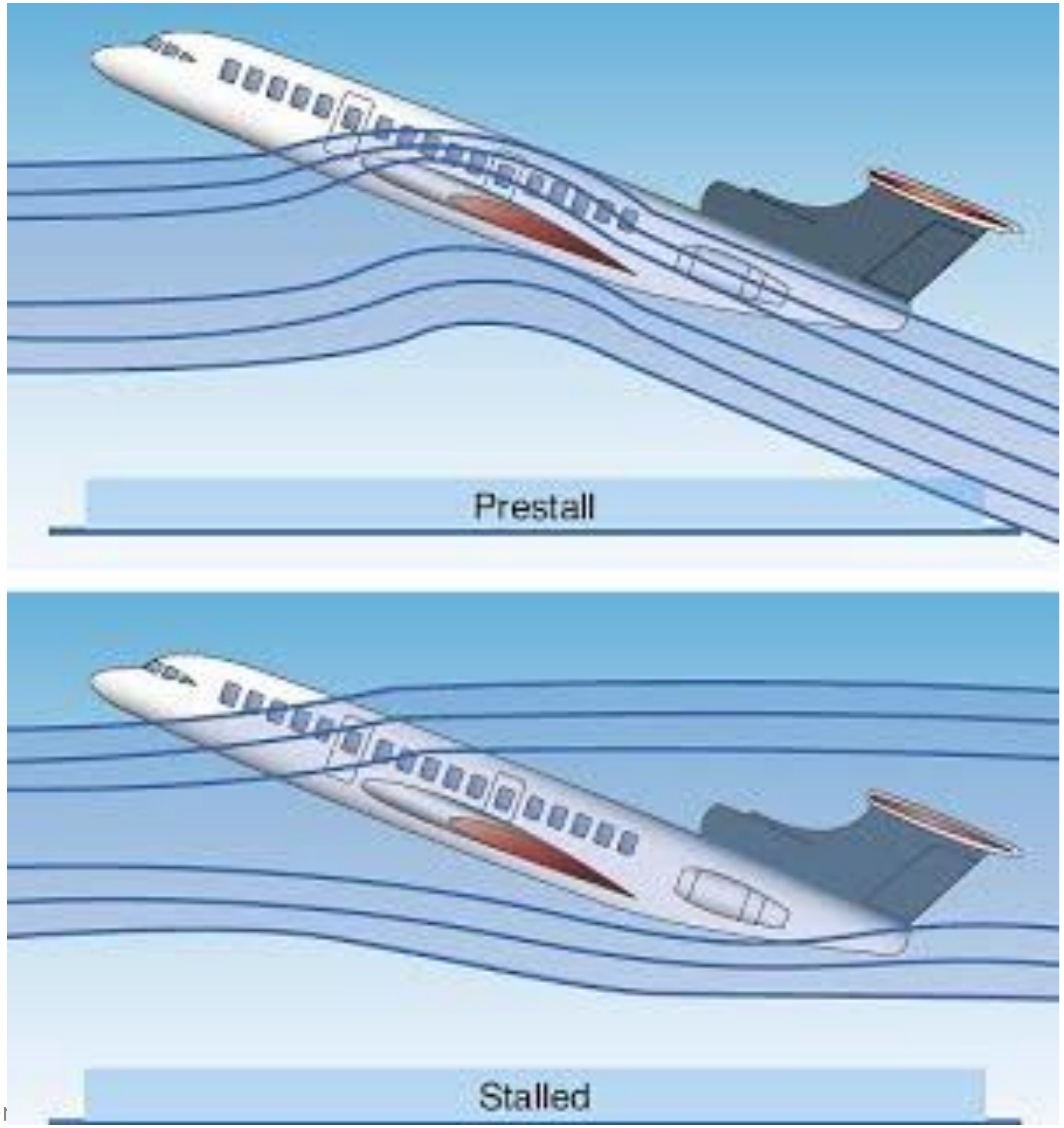
The 737 MAX was equipped with new, more fuel-efficient engines



https://leehamnews.com

Airflow
⇓
Lift



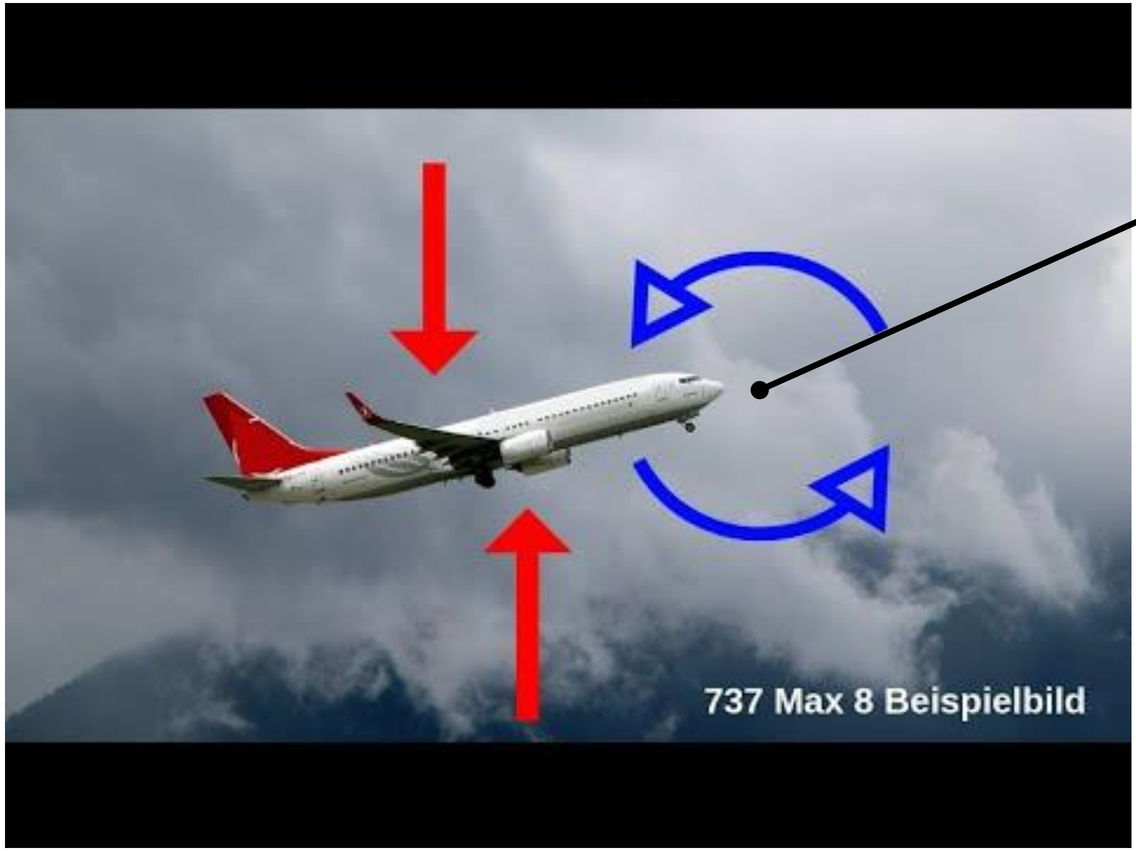


https://en.wikipedia.org

Lift
Loss
⇓
Stalling

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

CPS-Example: **Safety Risk**



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

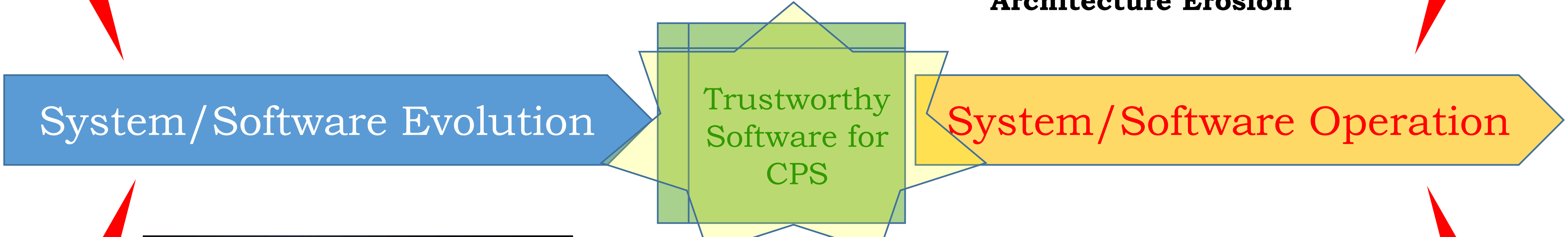
Complexity

Change

Uncertainty

Technical Debt

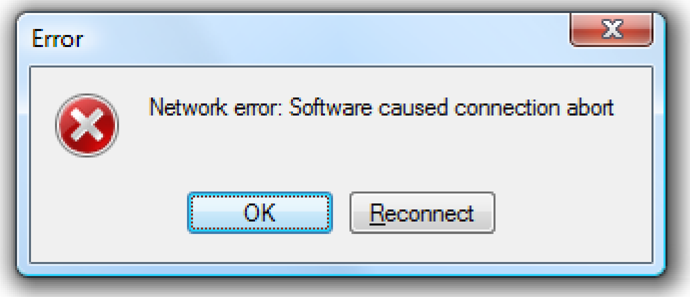
Architecture Erosion



System/Software Evolution

Trustworthy Software for CPS

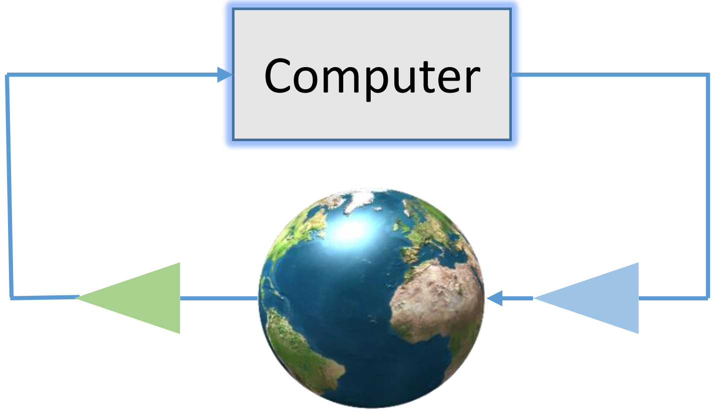
System/Software Operation



Error

Network error: Software caused connection abort

WS19/20: Engineering Trustworthy Software for Cyber-Physical Systems



Fault, Failure

40 players online
Wuty Wuty (WT254): is GO AIR AFK
Test Pilot (TP126C): dk
(EK520) Slamovnik: Whats going on in Miami int'l airport?
Test Pilot (TP126C): dk
(EK520) Slamovnik: Whats going on in Miami int'l airport?
Test Pilot (TP126C): ima
Mickelodeon473(Youtube)(QF459): Oh there it worked
Mickelodeon473(Youtube)(QF459): Test
Mickelodeon473(Youtube)(QF459): Oh there it worked
Mickelodeon473(Youtube)(QF459): Test
Wuty Wuty (WT254): what?
Test Pilot (TP126C): hey
Mickelodeon473(Youtube)(QF459): Hey guys
Wuty Wuty (WT254): yea I know it once did that for me
usNWA Mistakes Were Made: lol
BravoYankee (BY-1015): Mayday Mayday my autopilot has just put me to the ground in a nearby neighborhood
Wuty Wuty (WT254): bye

Attack, Intrusion

Risk

= Inherent **property** of cyber-physical systems

Risk Management

= Decisive part of systems engineering

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

Risk Management =

The identification, analysis, assessment, control,and avoidance, minimization, or elimination of unacceptable risks.

An organization may use risk assumption, risk avoidance, risk retention, risk transfer, or any other strategy (or combination of strategies) in proper management of future events

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

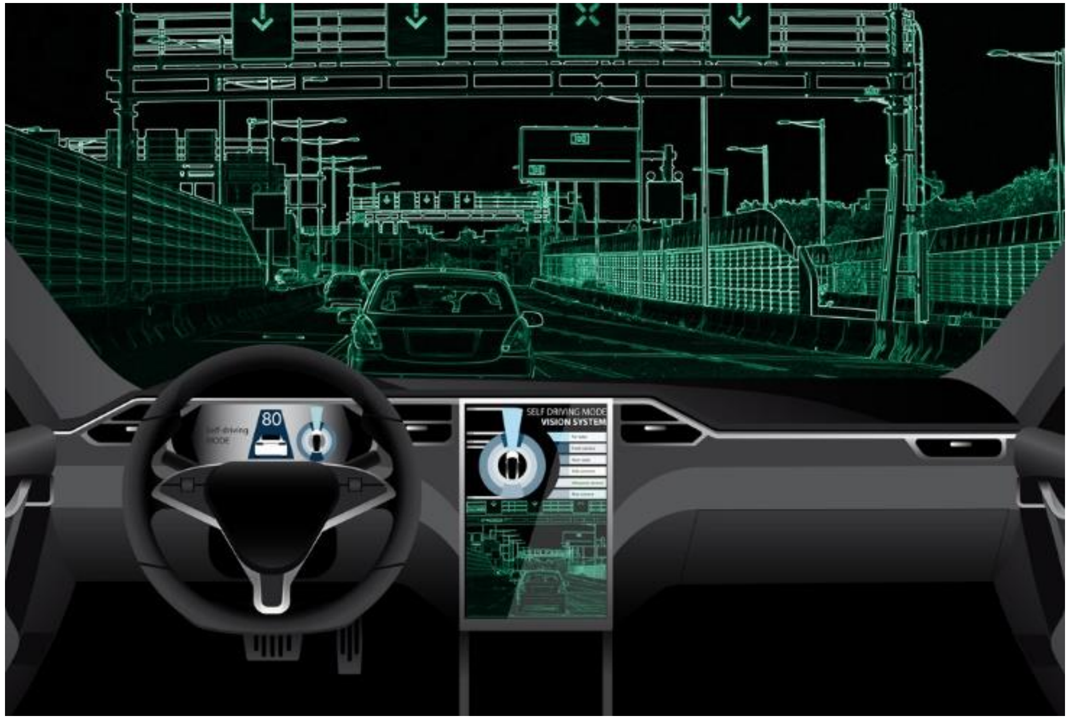
Building **trustworthy** systems = Successful **risk management**

Our responsibility is to

architect, design, implement, and operate

trustworthy, dependable software-systems

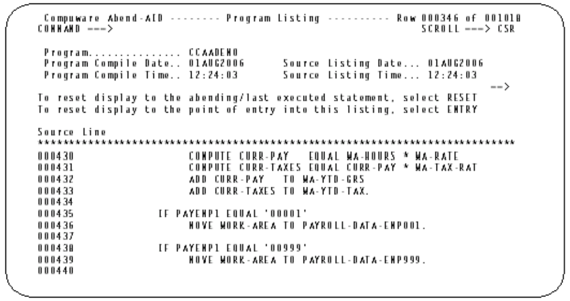
Engineering Trustworthy Software for Cyber-Physical Systems



Content

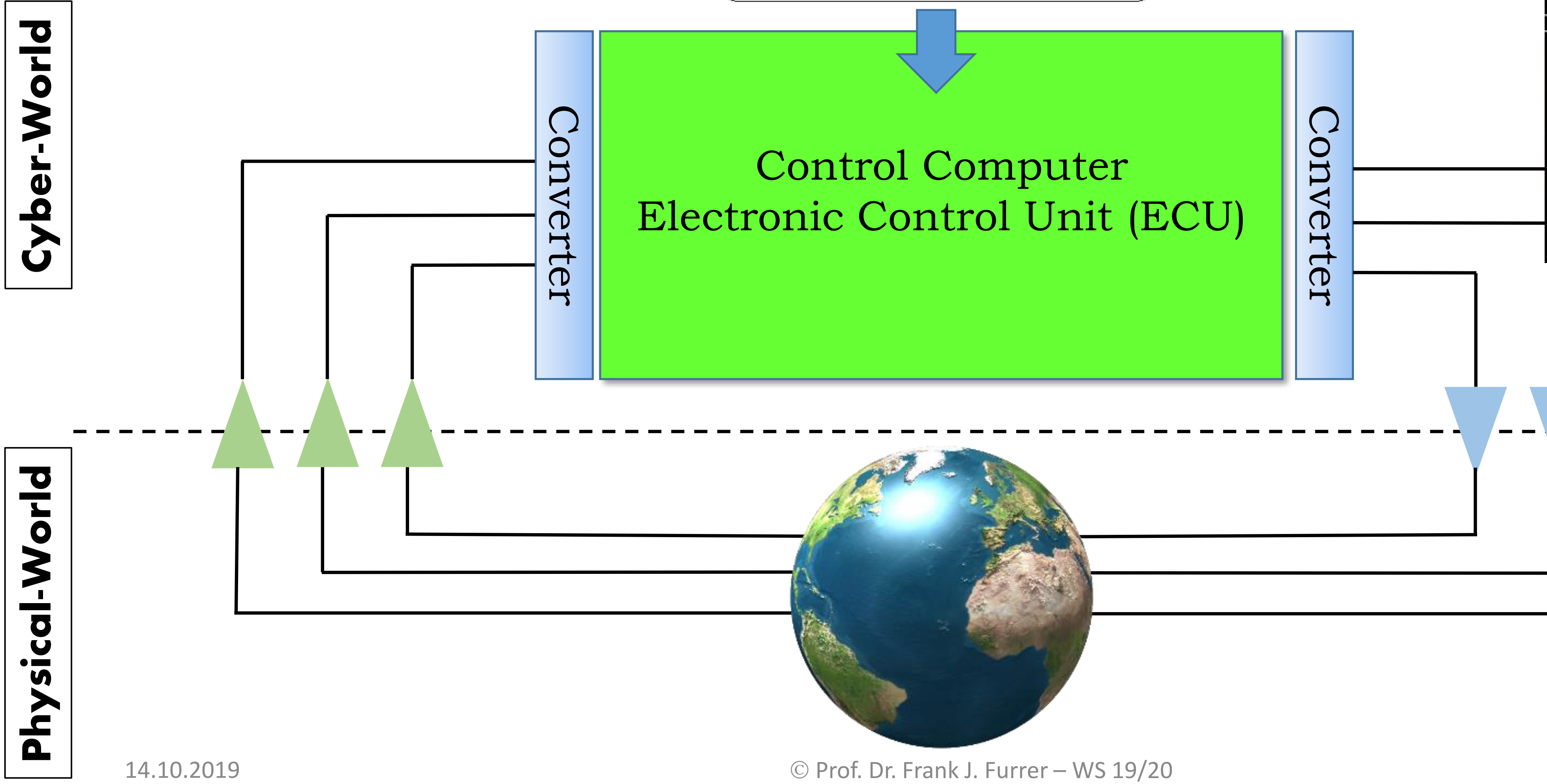
- Introduction
- Technology: Cyber-Physical Systems
- Trustworthiness
- Engineering
- Conclusions

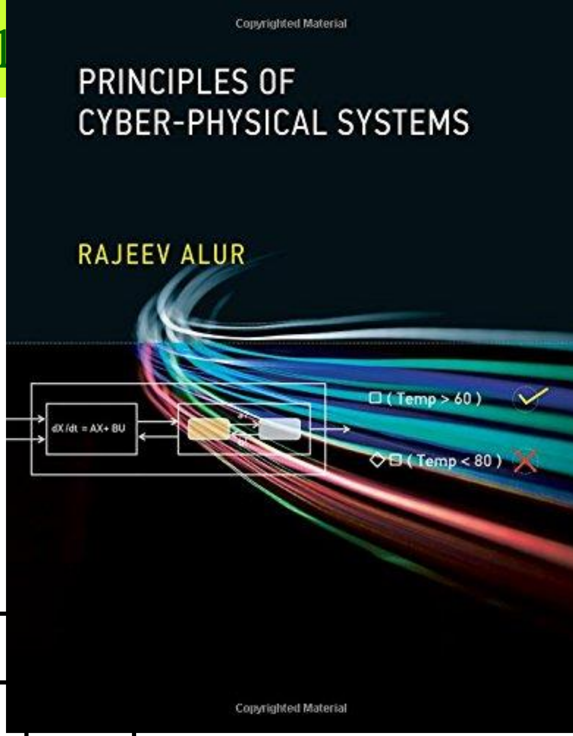
CPS Hardware Architecture



```
 Compuware Abend-AID -------- Program Listing ---------- Row 000346 of 001010
COMMAND --->                                                      SCROLL ---> CSR

 Program............... CCAADEMO
 Program Compile Date.. 01AUG2006      Source Listing Date... 01AUG2006
 Program Compile Time.. 12:24:03       Source Listing Time... 12:24:03
                                                                        -->
To reset display to the abending/last executed statement, select RESET
To reset display to the point of entry into this listing, select ENTRY

Source Line
*************************************************************************
000430                   COMPUTE CURR-PAY   EQUAL WA-HOURS * WA-RATE
000431                   COMPUTE CURR-TAXES EQUAL CURR-PAY * WA-TAX-RAT
000432                   ADD CURR-PAY   TO WA-YTD-GRS
000433                   ADD CURR-TAXES TO WA-YTD-TAX.
000434
000435               IF PAYEMP1 EQUAL '00001'
000436                   MOVE WORK-AREA TO PAYROLL-DATA-EMP001.
000437
000438               IF PAYEMP1 EQUAL '00999'
000439                   MOVE WORK-AREA TO PAYROLL-DATA-EMP999.
000440
```

Software





Copyrighted Material

PRINCIPLES OF CYBER-PHYSICAL SYSTEMS

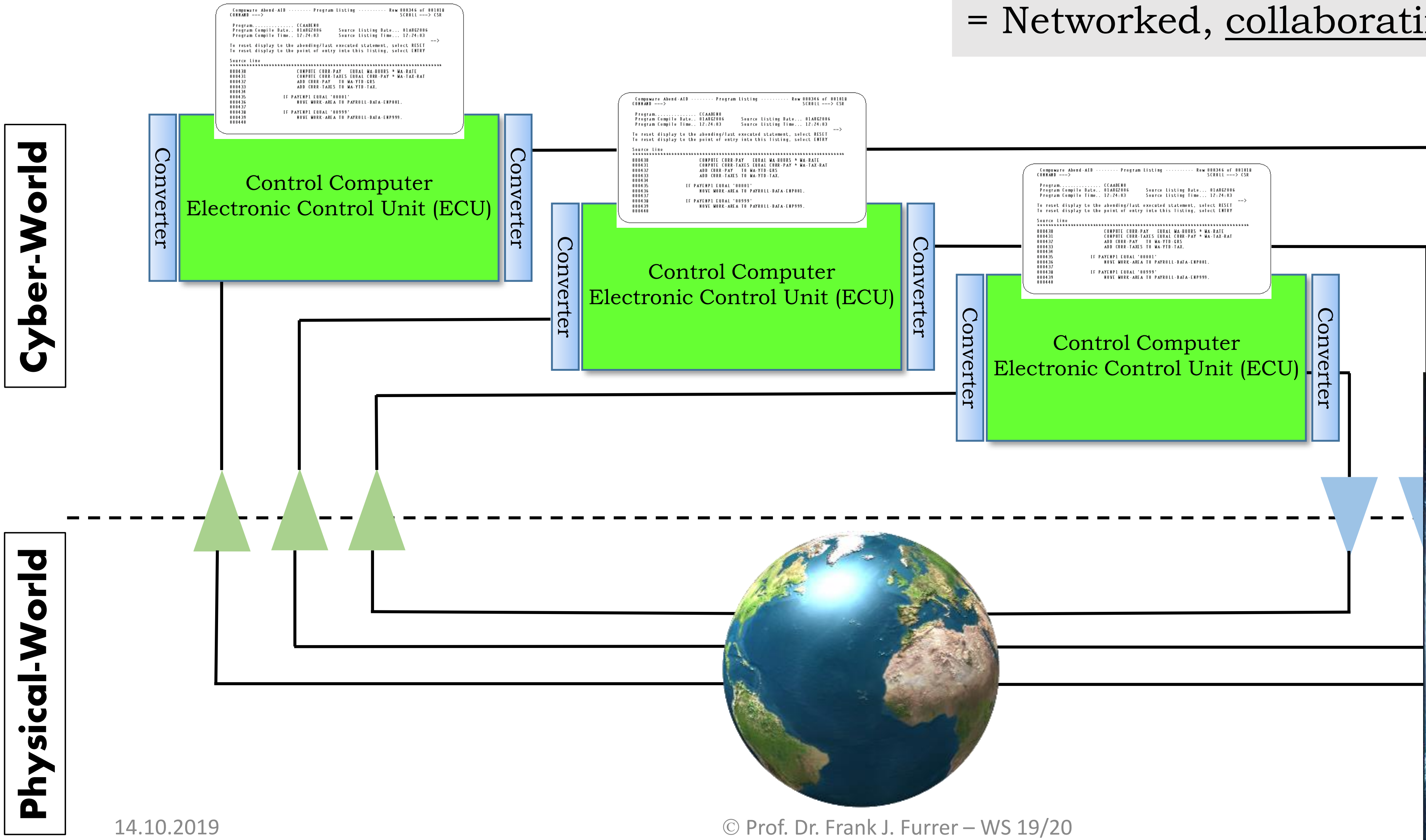
RAJEEV ALUR

Copyrighted Material

CPSoS Hardware Architecture

Cyber-Physical System-of-Systems (**CPSoS**)

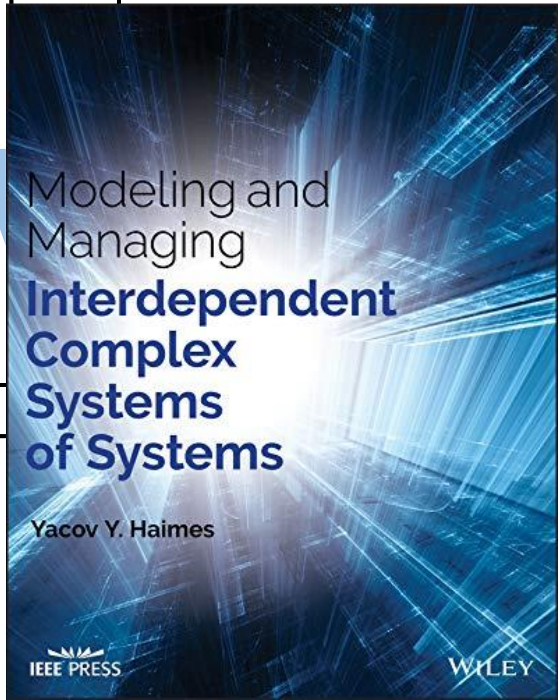
= Networked, collaborating CPS's



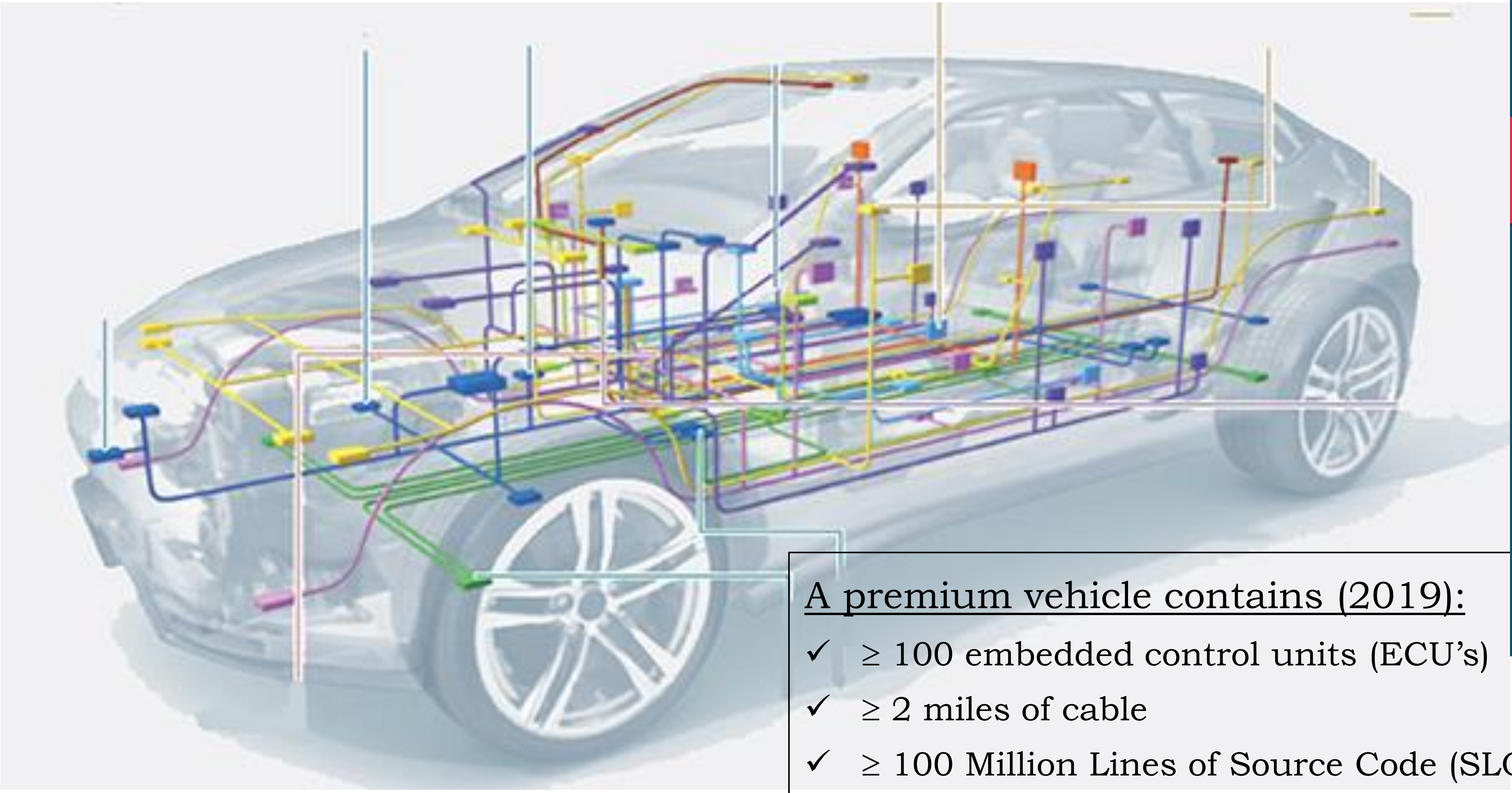
```
 Compuware Abend-AID -------- Program Listing ---------- Row 000346 of 001018
COMMAND --->                                                   SCROLL ---> CSR

 Program............... CCAADEMO
 Program Compile Date.. 01AUG2006      Source Listing Date... 01AUG2006
 Program Compile Time.. 12:24:03       Source Listing Time... 12:24:03
                                                                         -->
To reset display to the abending/last executed statement, select RESET
To reset display to the point of entry into this listing, select ENTRY

Source Line
******************************************************************************
000430                   COMPUTE CURR-PAY   EQUAL WA-HOURS * WA-RATE
000431                   COMPUTE CURR-TAXES EQUAL CURR-PAY * WA-TAX-RAT
000432                   ADD CURR-PAY   TO WA-YTD-GRS
000433                   ADD CURR-TAXES TO WA-YTD-TAX.
000434
000435              IF PAYEMP1 EQUAL '00001'
000436                   MOVE WORK-AREA TO PAYROLL-DATA-EMP001.
000437
000438              IF PAYEMP1 EQUAL '00999'
000439                   MOVE WORK-AREA TO PAYROLL-DATA-EMP999.
000440
```

```
 Compuware Abend-AID -------- Program Listing ---------- Row 000346 of 001018
COMMAND --->                                                   SCROLL ---> CSR

 Program............... CCAADEMO
 Program Compile Date.. 01AUG2006      Source Listing Date... 01AUG2006
 Program Compile Time.. 12:24:03       Source Listing Time... 12:24:03
                                                                         -->
To reset display to the abending/last executed statement, select RESET
To reset display to the point of entry into this listing, select ENTRY

Source Line
******************************************************************************
000430                   COMPUTE CURR-PAY   EQUAL WA-HOURS * WA-RATE
000431                   COMPUTE CURR-TAXES EQUAL CURR-PAY * WA-TAX-RAT
000432                   ADD CURR-PAY   TO WA-YTD-GRS
000433                   ADD CURR-TAXES TO WA-YTD-TAX.
000434
000435              IF PAYEMP1 EQUAL '00001'
000436                   MOVE WORK-AREA TO PAYROLL-DATA-EMP001.
000437
000438              IF PAYEMP1 EQUAL '00999'
000439                   MOVE WORK-AREA TO PAYROLL-DATA-EMP999.
000440
```

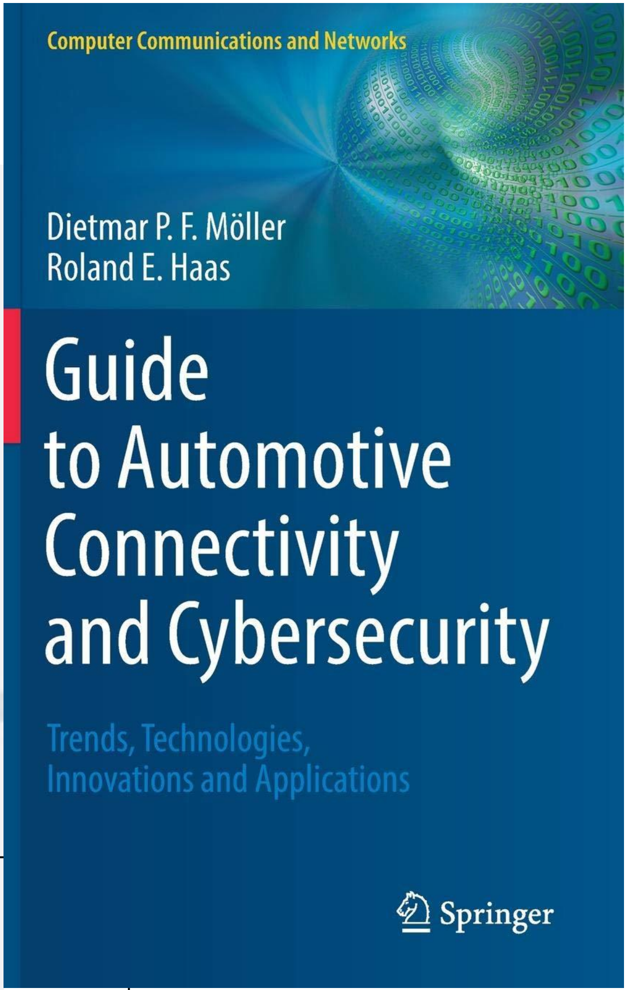
```
 Compuware Abend-AID -------- Program Listing ---------- Row 000346 of 001018
COMMAND --->                                                   SCROLL ---> CSR

 Program............... CCAADEMO
 Program Compile Date.. 01AUG2006      Source Listing Date... 01AUG2006
 Program Compile Time.. 12:24:03       Source Listing Time... 12:24:03
                                                                         -->
To reset display to the abending/last executed statement, select RESET
To reset display to the point of entry into this listing, select ENTRY

Source Line
******************************************************************************
000430                   COMPUTE CURR-PAY   EQUAL WA-HOURS * WA-RATE
000431                   COMPUTE CURR-TAXES EQUAL CURR-PAY * WA-TAX-RAT
000432                   ADD CURR-PAY   TO WA-YTD-GRS
000433                   ADD CURR-TAXES TO WA-YTD-TAX.
000434
000435              IF PAYEMP1 EQUAL '00001'
000436                   MOVE WORK-AREA TO PAYROLL-DATA-EMP001.
000437
000438              IF PAYEMP1 EQUAL '00999'
000439                   MOVE WORK-AREA TO PAYROLL-DATA-EMP999.
000440
```



CPSoS Example: Modern Car



https://www.digikey.com



Computer Communications and Networks

Dietmar P. F. Möller
Roland E. Haas

Guide to Automotive Connectivity and Cybersecurity

Trends, Technologies, Innovations and Applications

Springer

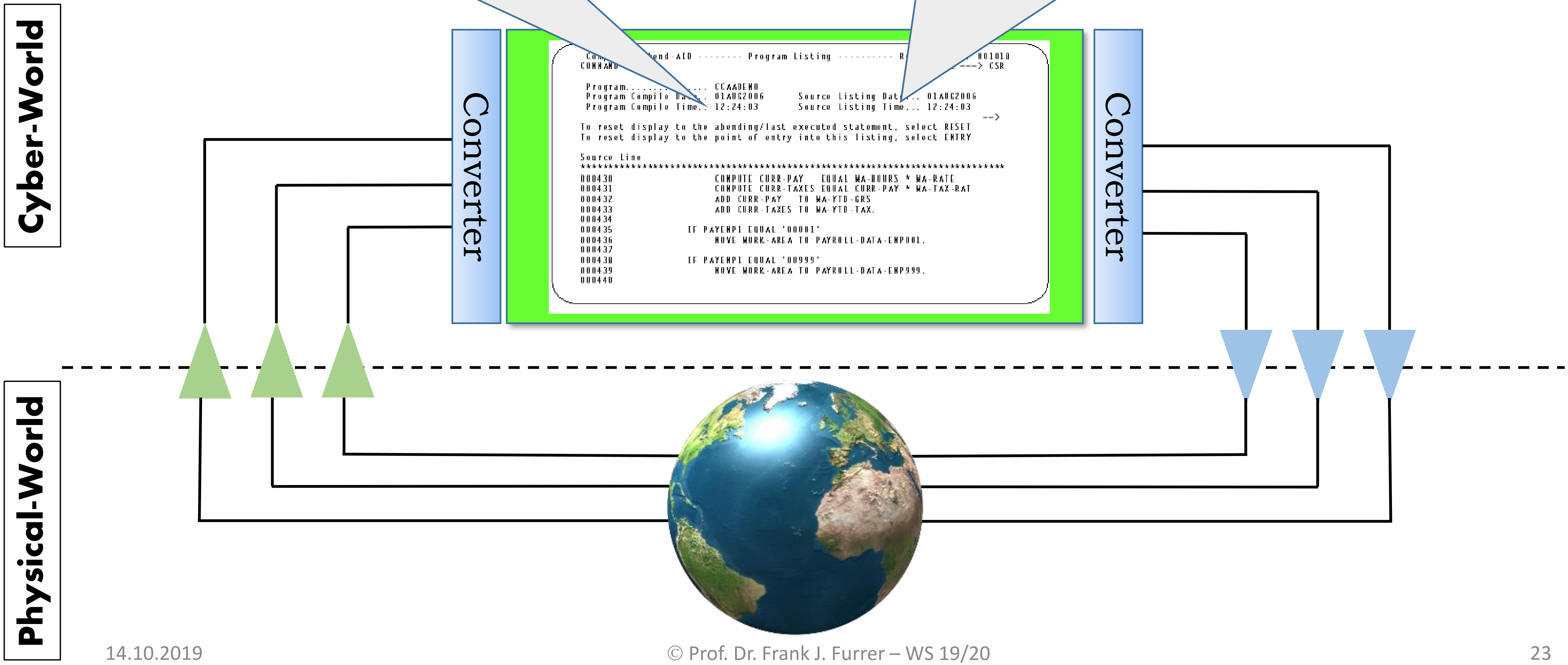
<u>A premium vehicle contains (2019):</u>

- ✓ ≥ 100 embedded control units (ECU's)
- ✓ ≥ 2 miles of cable
- ✓ ≥ 100 Million Lines of Source Code (SLOC's)
- ✓ ≥ 5 in-vehicle networks

WS19/20: Engineering Trustworthy Software for Cyber-Physical Systems

CPS-Trustworthiness
=
Property of the **whole** system

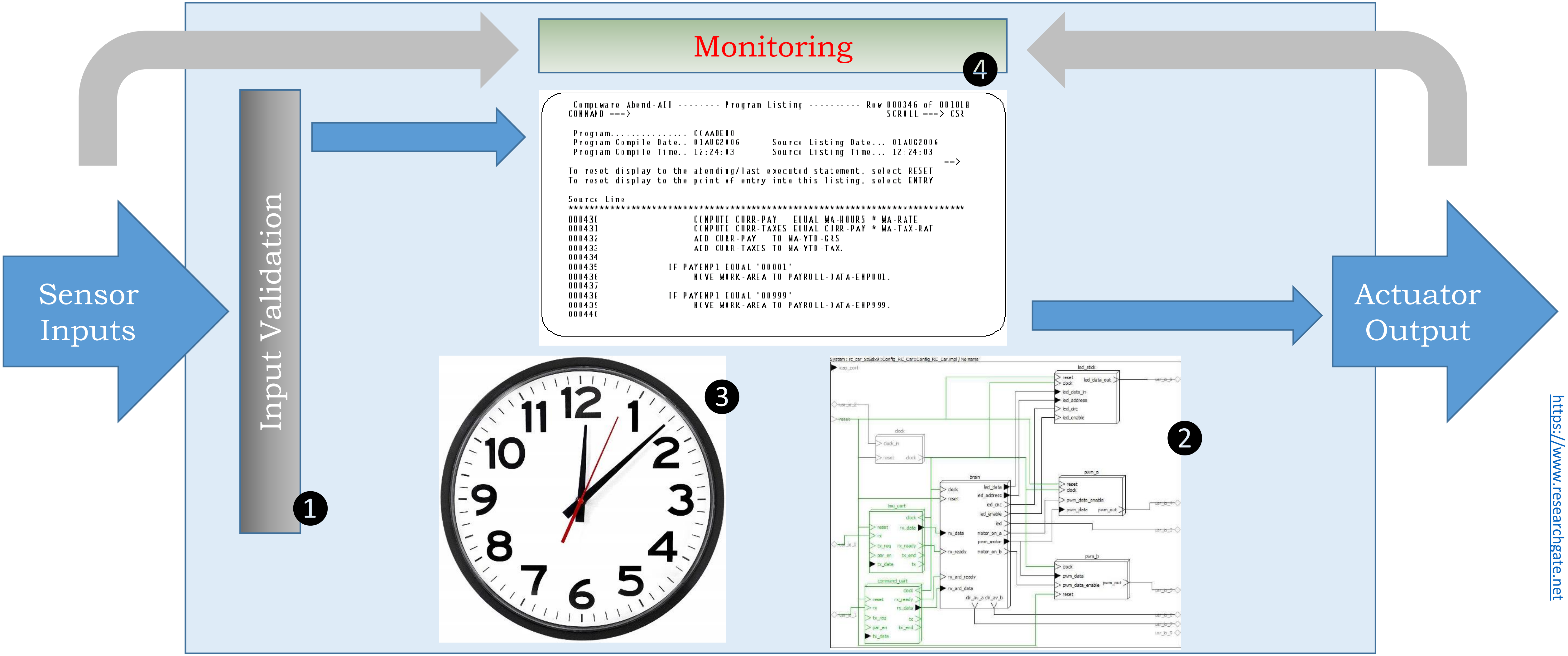
However, most of the **functionality** is implemented in software
⇒ **Trustworthy Software**



```
 Com         bend-AID -------- Program Listing ----------  R              001018
COMMAND                                                          ---> CSR

 Program........      .... CCAADEMO
 Program Compile Da   .. 01AUG2006      Source Listing Dat ... 01AUG2006
 Program Compile Time.. 12:24:03        Source Listing Time... 12:24:03
                                                                        -->
To reset display to the abending/last executed statement, select RESET
To reset display to the point of entry into this listing, select ENTRY

Source Line
*****************************************************************************
000430                   COMPUTE CURR-PAY   EQUAL WA-HOURS * WA-RATE
000431                   COMPUTE CURR-TAXES EQUAL CURR-PAY * WA-TAX-RAT
000432                   ADD CURR-PAY   TO WA-YTD-GRS
000433                   ADD CURR-TAXES TO WA-YTD-TAX.
000434
000435               IF PAYEMP1 EQUAL '00001'
000436                   MOVE WORK-AREA TO PAYROLL-DATA-EMP001.
000437
000438               IF PAYEMP1 EQUAL '00999'
000439                   MOVE WORK-AREA TO PAYROLL-DATA-EMP999.
000440
```

http://frontline.compuware.com

CPS Software Architecture

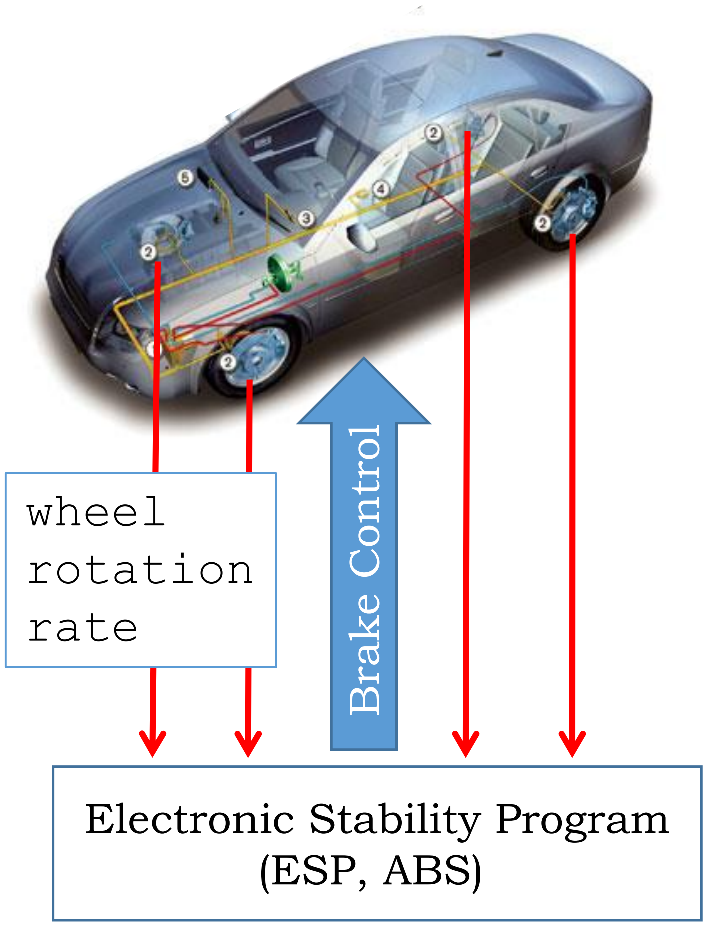


```
 Compuware Abend-AID -------- Program Listing ---------- Row 000346 of 001010
COMMAND ===>                                                  SCROLL ===> CSR

 Program................ CCAADEMO
 Program Compile Date.. 01AUG2006      Source Listing Date... 01AUG2006
 Program Compile Time.. 12:24:03       Source Listing Time... 12:24:03
                                                                        -->
To reset display to the abending/last executed statement, select RESET
To reset display to the point of entry into this listing, select ENTRY

Source Line
******************************************************************************
000430                    COMPUTE CURR-PAY   EQUAL WA-HOURS * WA-RATE
000431                    COMPUTE CURR-TAXES EQUAL CURR-PAY * WA-TAX-RAT
000432                    ADD CURR-PAY   TO WA-YTD-GRS
000433                    ADD CURR-TAXES TO WA-YTD-TAX.
000434
000435                IF PAYEMP1 EQUAL '00001'
000436                    MOVE WORK-AREA TO PAYROLL-DATA-EMP001.
000437
000438                IF PAYEMP1 EQUAL '00999'
000439                    MOVE WORK-AREA TO PAYROLL-DATA-EMP999.
000440
```

https://www.amazon.com

https://www.researchgate.net

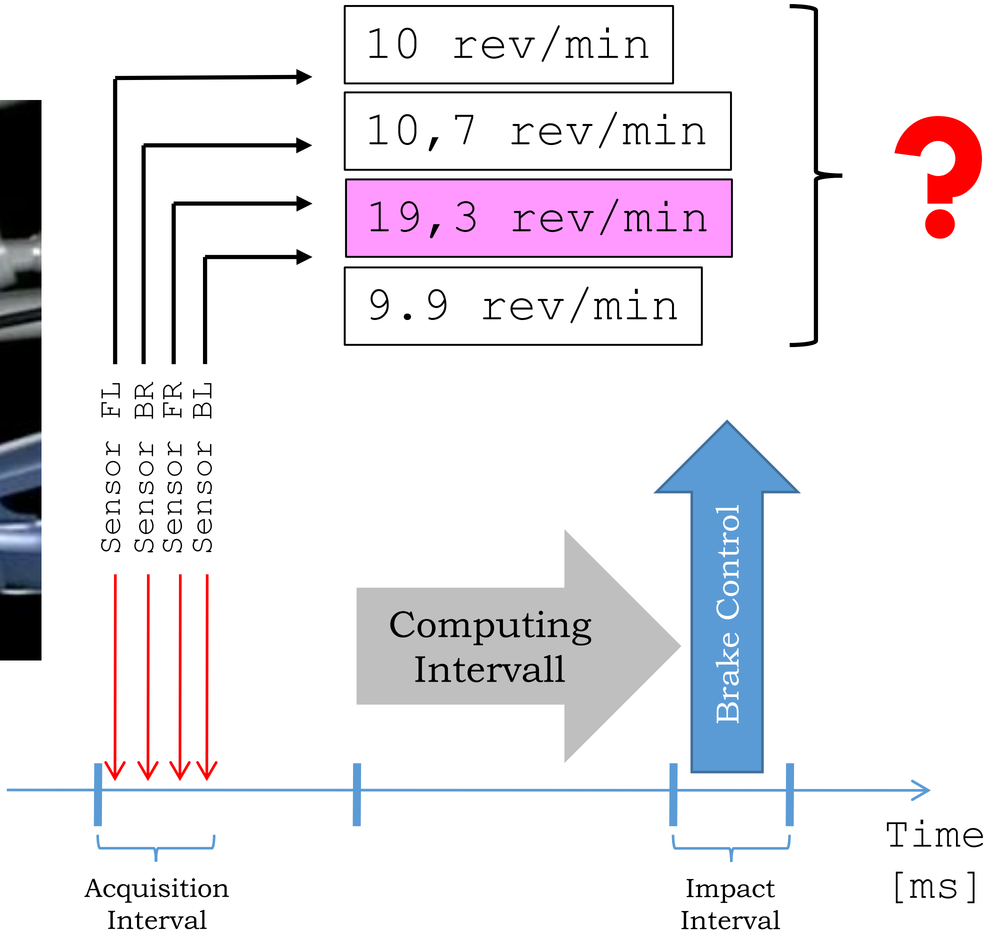
❶ Input Validation

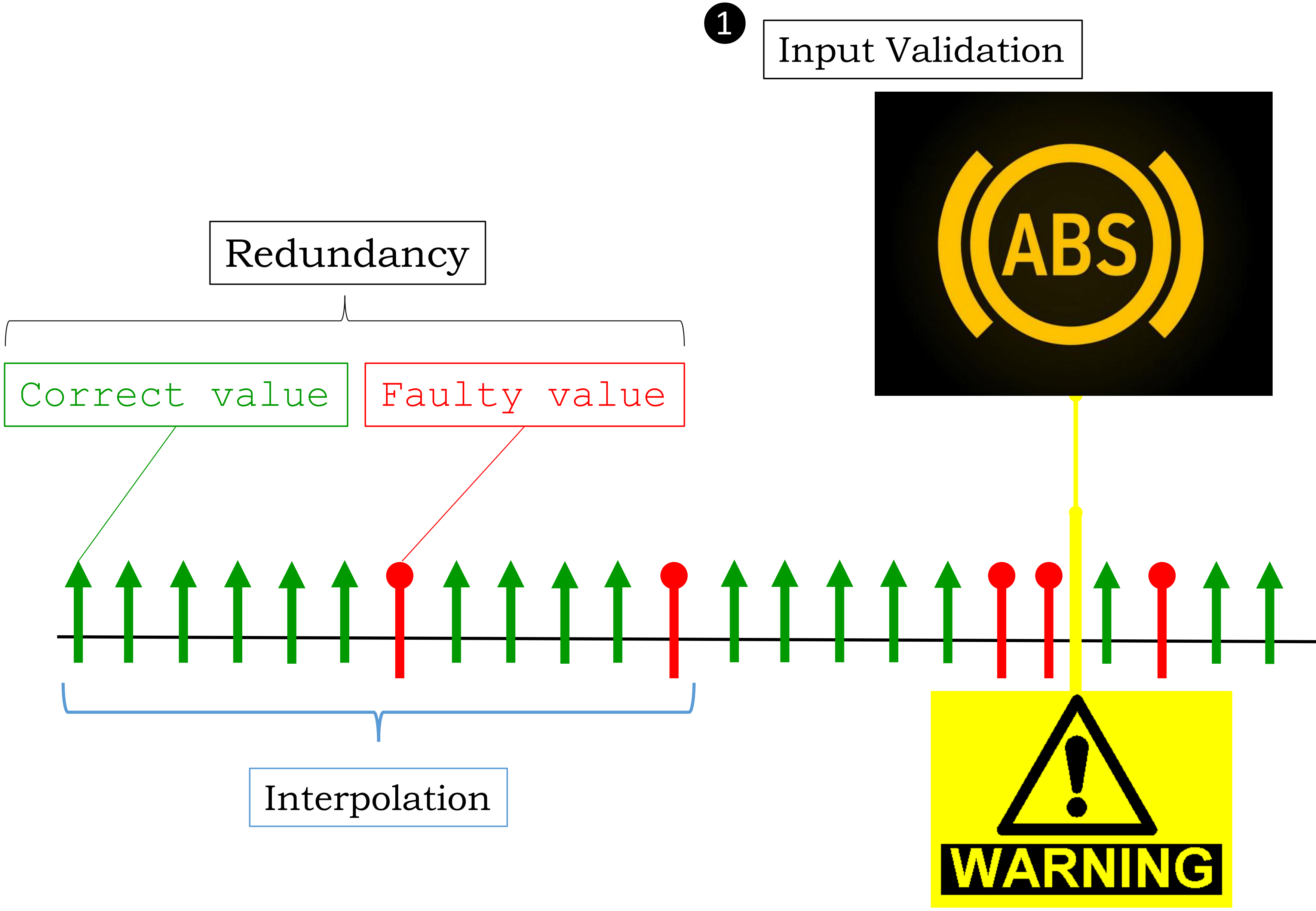


http://www.tomorrowstechnician.com

Wheel rotation speed sensor

http://www.cdxetextbook.com/brakes



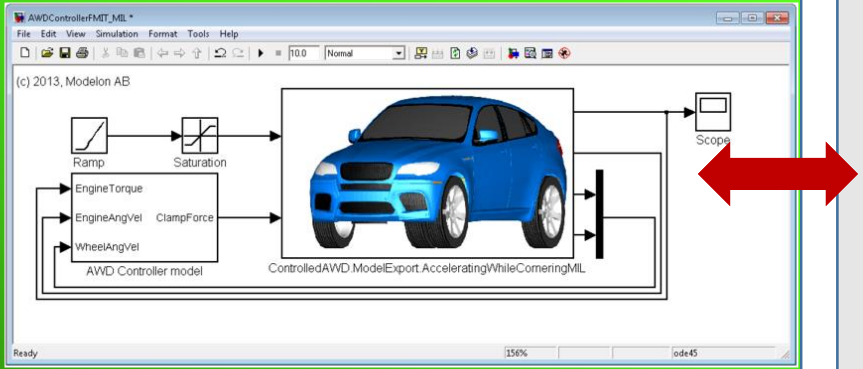


http://www.cdxetextbook.com/brakes

Real-world model ❷

Control Computer (ECU)

Real-World Model



http://www.modelon.com

Software

The model governs the CPS-behaviour

Actuators

http://cdn1.alphr.com

Sensors

Cyber-Part

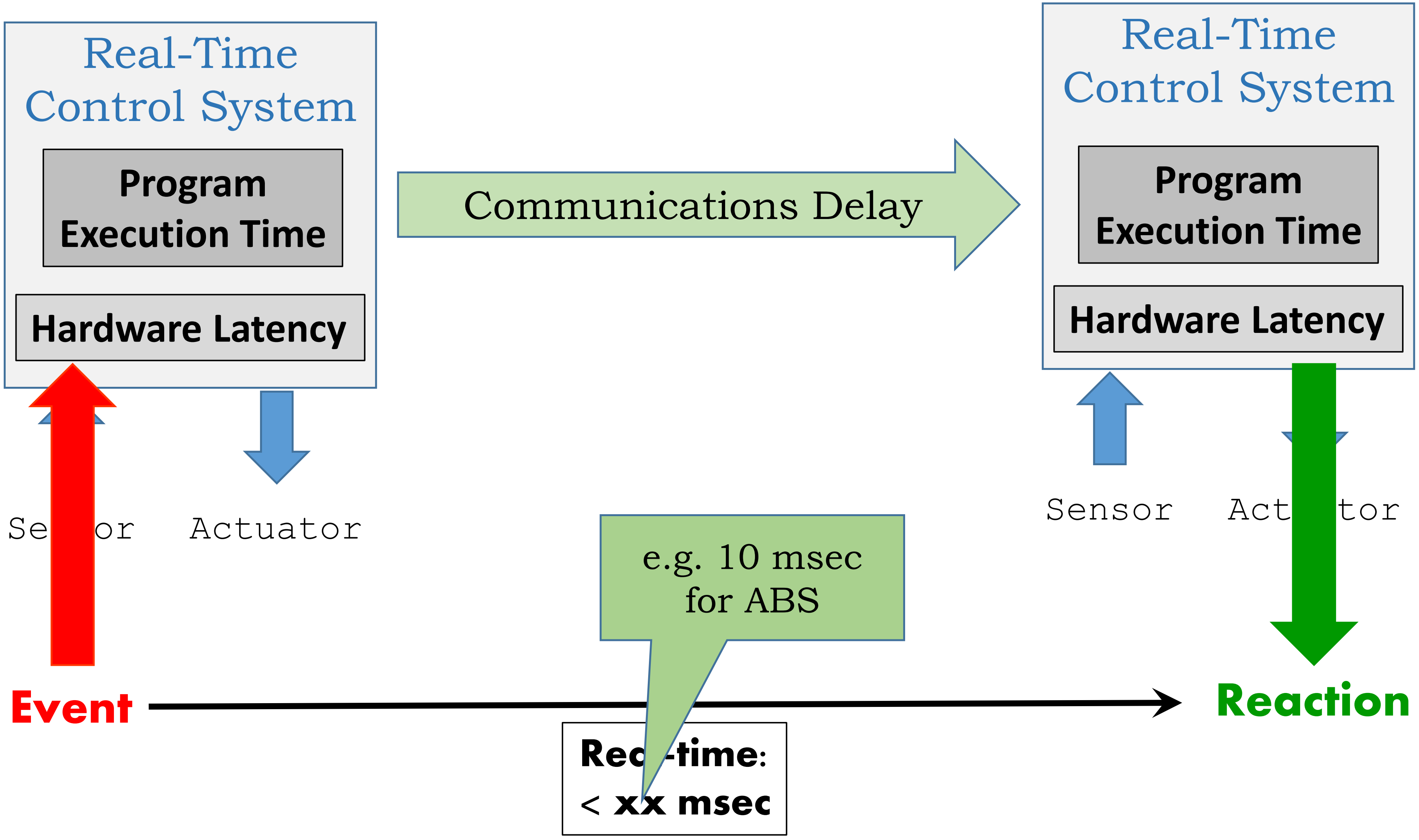
Physical-Part

❸ Time

https://www.amazon.com

- In most cyber-physical systems time is **important**
- The CPS must **react** within a guaranteed time period (= Real Time-Behaviour)
- Failing to react timely may cause **malfunction** of the system
- The software, therefore, must assure **real-time behaviour**

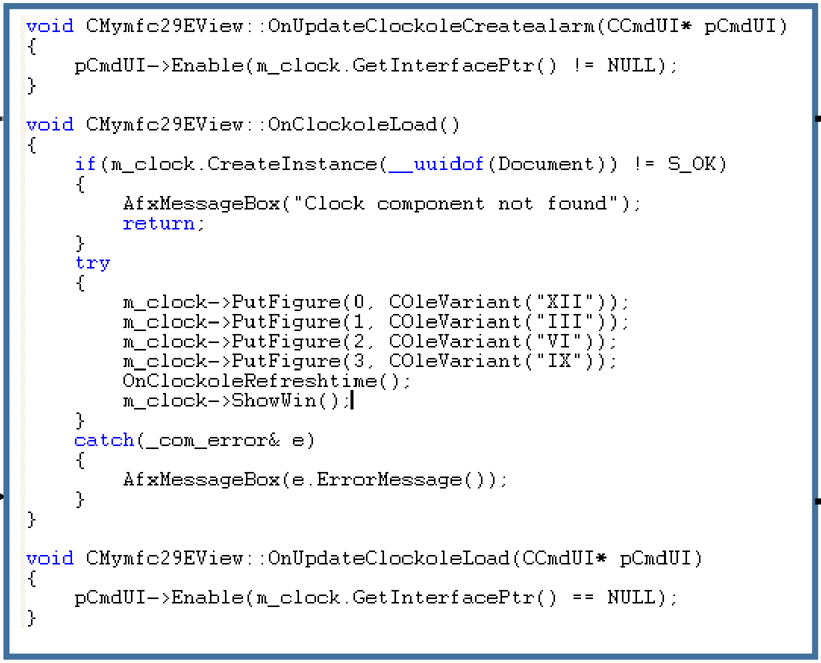
Real-world: Systems-of-Systems



Response Time

Start **Event**
[Receipt of Message]

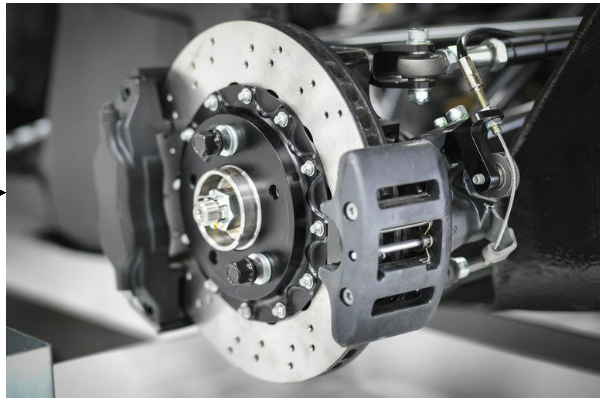
Software Processing



```
void CMymfc29EView::OnUpdateClockoleCreatealarm(CCmdUI* pCmdUI)
{
    pCmdUI->Enable(m_clock.GetInterfacePtr() != NULL);
}

void CMymfc29EView::OnClockoleLoad()
{
    if(m_clock.CreateInstance(__uuidof(Document)) != S_OK)
    {
        AfxMessageBox("Clock component not found");
        return;
    }
    try
    {
        m_clock->PutFigure(0, COleVariant("XII"));
        m_clock->PutFigure(1, COleVariant("III"));
        m_clock->PutFigure(2, COleVariant("VI"));
        m_clock->PutFigure(3, COleVariant("IX"));
        OnClockoleRefreshtime();
        m_clock->ShowWin();
    }
    catch(_com_error& e)
    {
        AfxMessageBox(e.ErrorMessage());
    }
}

void CMymfc29EView::OnUpdateClockoleLoad(CCmdUI* pCmdUI)
{
    pCmdUI->Enable(m_clock.GetInterfacePtr() == NULL);
}
```

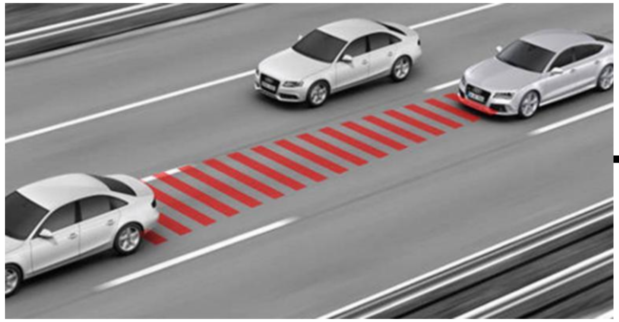
Action

http://www.fahrschule-luckau-dahme.de



https://www.thoughtco.com

Action



https://www.electronicdesign.com

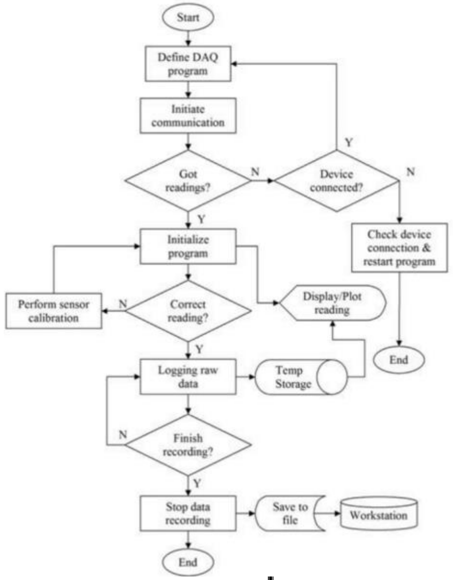
Start **Event**
[Radar Sensor Input]

Worst Case Execution Time (WCET)

WS19/20: Engineering Trustworthy Software for Cyber-Physical Systems

Response Time

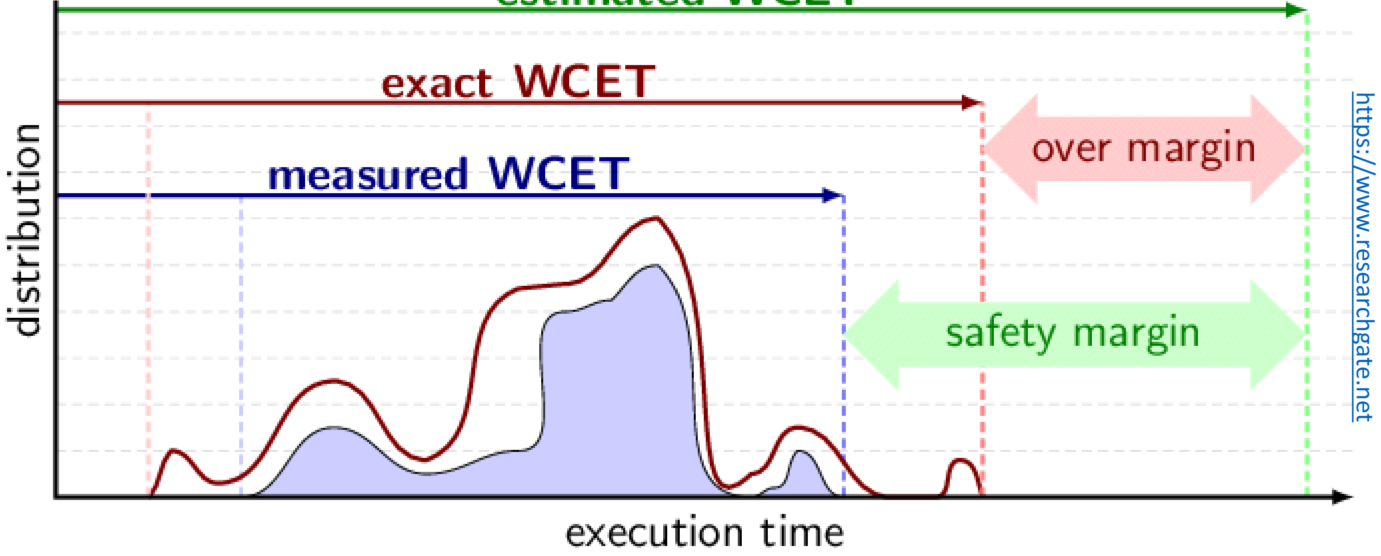
Total elapsed time from an event to the completed, correct action



Worst Case Execution Time (WCET)

Longest possible time for the execution of the software action

https://www.amazon.de

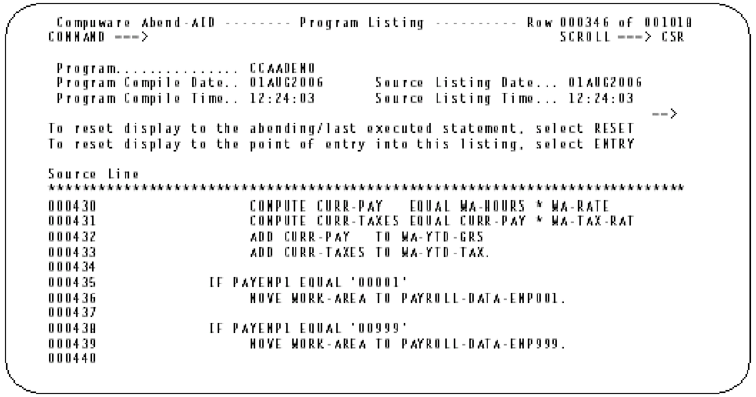


https://www.researchgate.net

⇒ Critical Parameters in Real-Time Cyber-Physical Systems

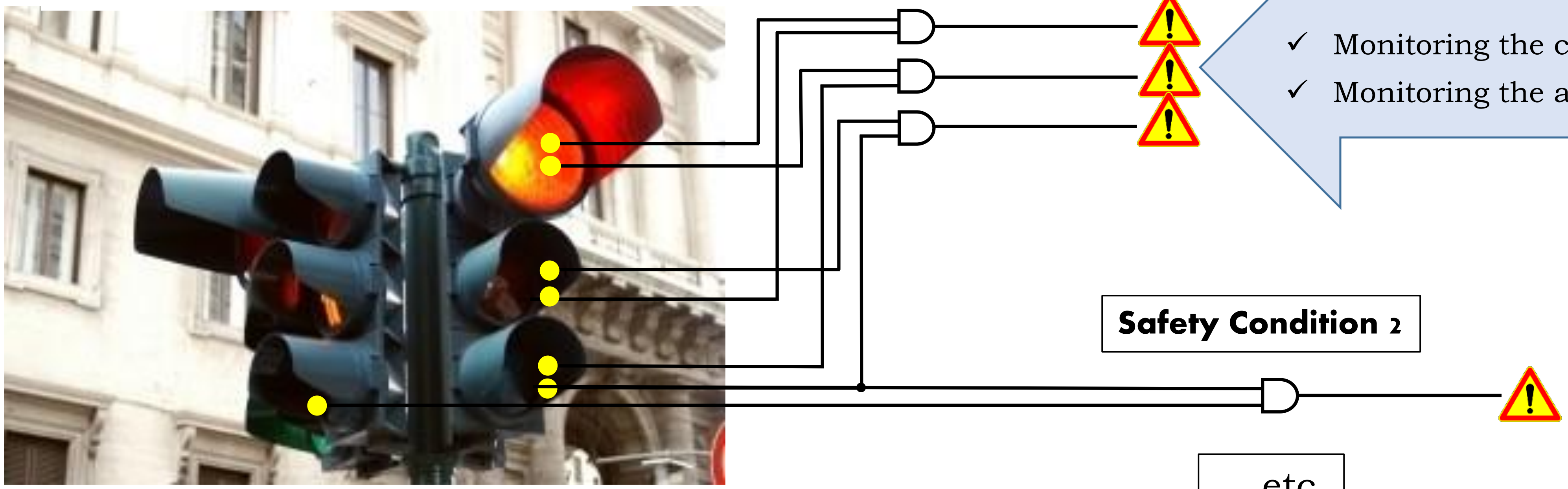
❹ Monitoring

Monitoring



```
 Compuware Abend-AID -------- Program Listing ---------- Row 000346 of 001010
COMMAND ===>                                                   SCROLL ===> CSR

 Program............... CCAADEMO
 Program Compile Date.. 01AUG2006       Source Listing Date... 01AUG2006
 Program Compile Time.. 12:24:03        Source Listing Time... 12:24:03
                                                                        -->
To reset display to the abending/last executed statement, select RESET
To reset display to the point of entry into this listing, select ENTRY

Source Line
******************************************************************************
000430                  COMPUTE CURR-PAY   EQUAL WA-HOURS * WA-RATE
000431                  COMPUTE CURR-TAXES EQUAL CURR-PAY * WA-TAX-RAT
000432                  ADD CURR-PAY   TO WA-YTD-GRS
000433                  ADD CURR-TAXES TO WA-YTD-TAX.
000434
000435              IF PAYEMP1 EQUAL '00001'
000436                  MOVE WORK-AREA TO PAYROLL-DATA-EMP001.
000437
000438              IF PAYEMP1 EQUAL '00999'
000439                  MOVE WORK-AREA TO PAYROLL-DATA-EMP999.
000440
```

An **IT system monitor** is a hardware and/or software component used to detect **anomalies** in the operation



Safety Condition 1

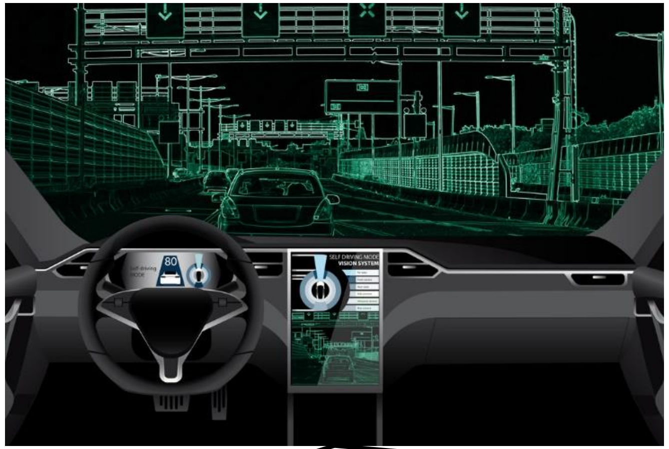
Safety Condition 2

- ✓ Monitoring the control variables in **SW**
- ✓ Monitoring the actual **hardware** signals

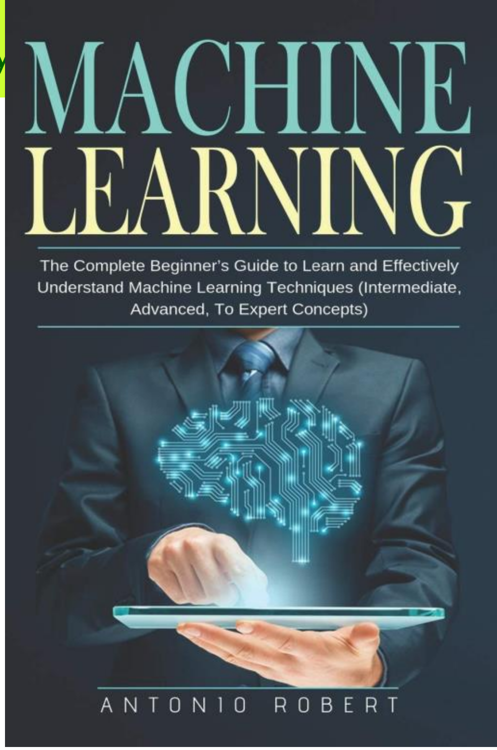
… etc.

https://www.bussgeldkatalog.org

Algorithmic/
Autonomic CPS



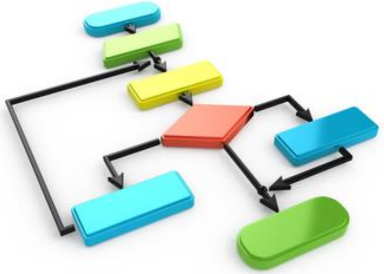
Cyber-Physical System


MACHINE
LEARNING
The Complete Beginner's Guide to Learn and Effectively Understand Machine Learning Techniques (Intermediate, Advanced, To Expert Concepts)
ANTONIO ROBERT

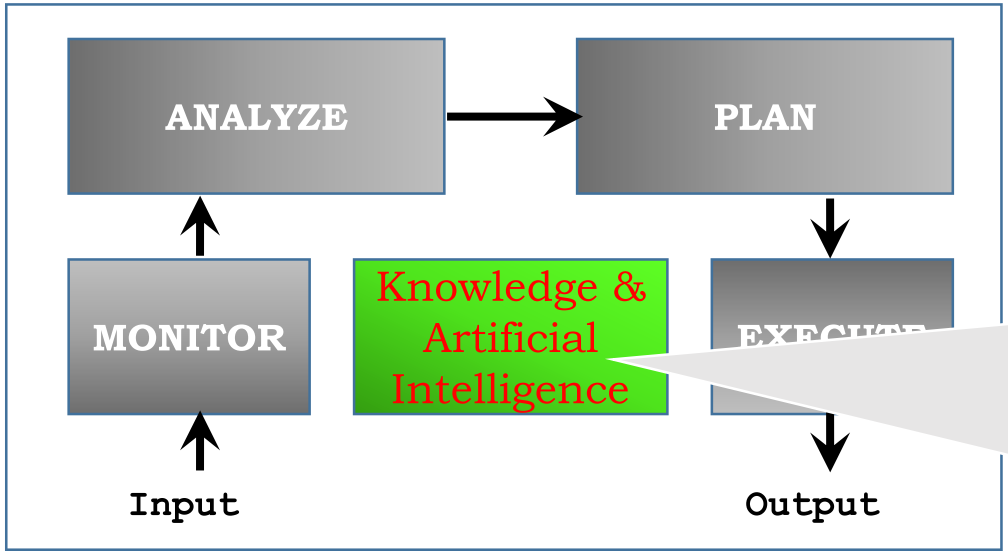
Algorithmic Computing

Autonomic Computing

http://www.bobology.com



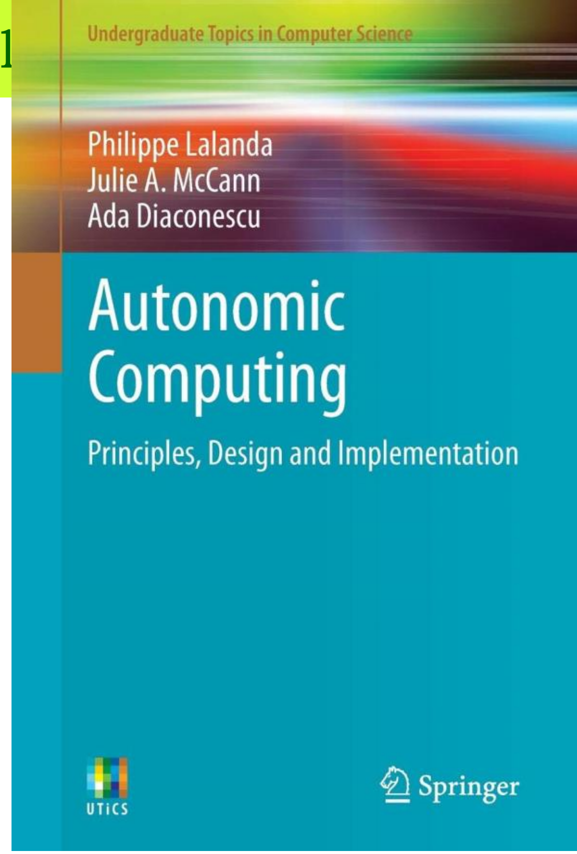
The «programmer» must think of all *possible* cases and decisions *beforehand*



Machine Learning

Machine reasoning

Machine Decisions



Undergraduate Topics in Computer Science

Philippe Lalanda
Julie A. McCann
Ada Diaconescu

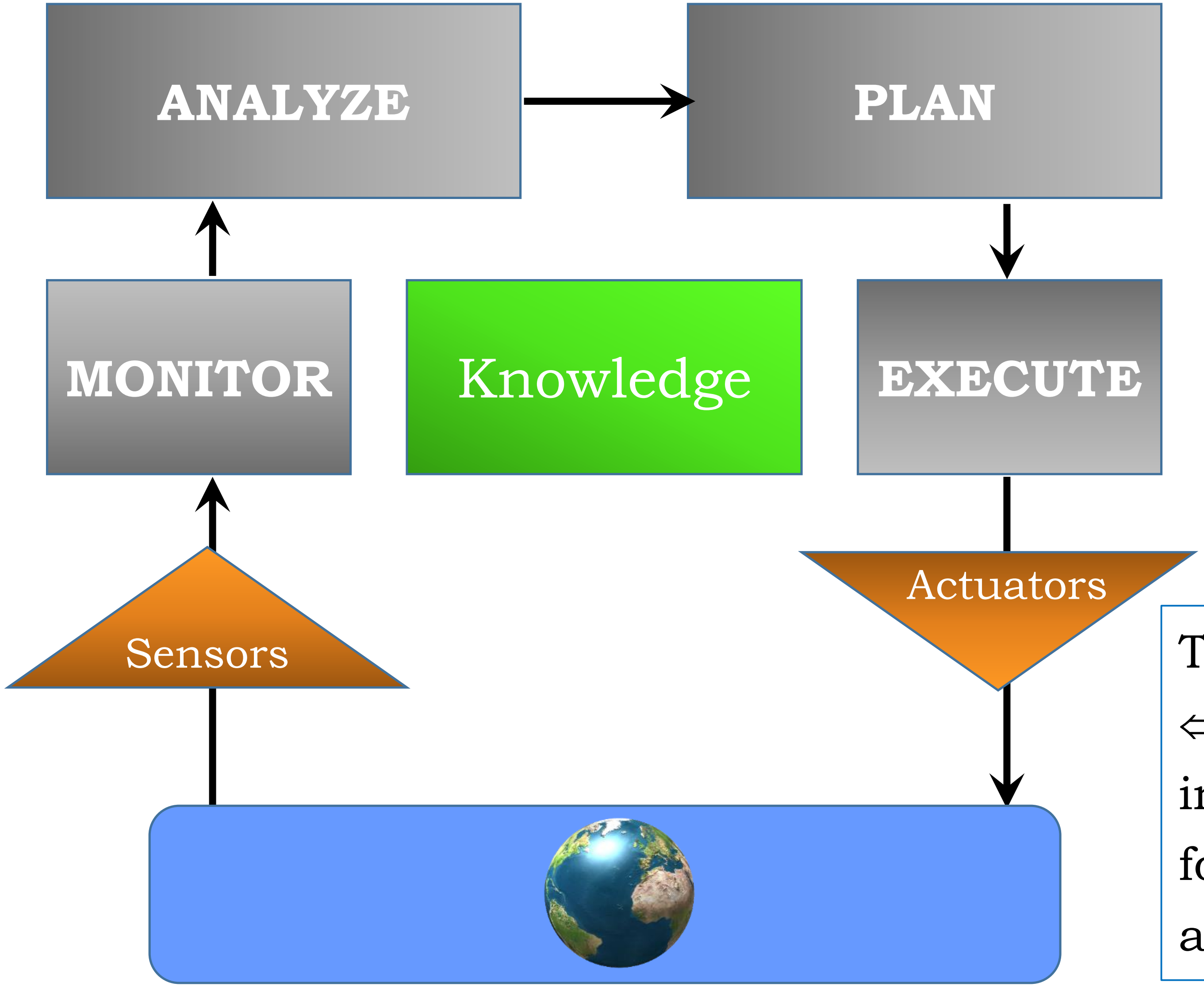
Autonomic Computing

Principles, Design and Implementation

UTICS

Springer

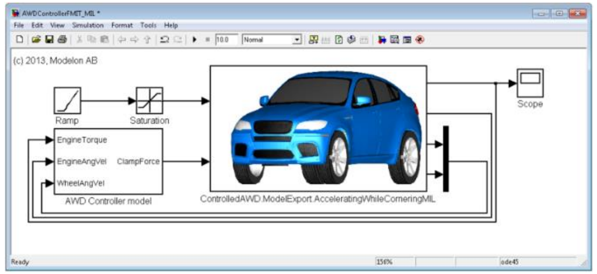
CPS [Reference] Software Architecture



The MAPE-K [**M**onitor-**A**nalyze-**P**lan-**E**xecute ⇐ **K**nowledge] reference architecture was introduced by IBM scientists and forms the foundation of many systems ◊ especially autonomic systems

Anatomy of a CPS

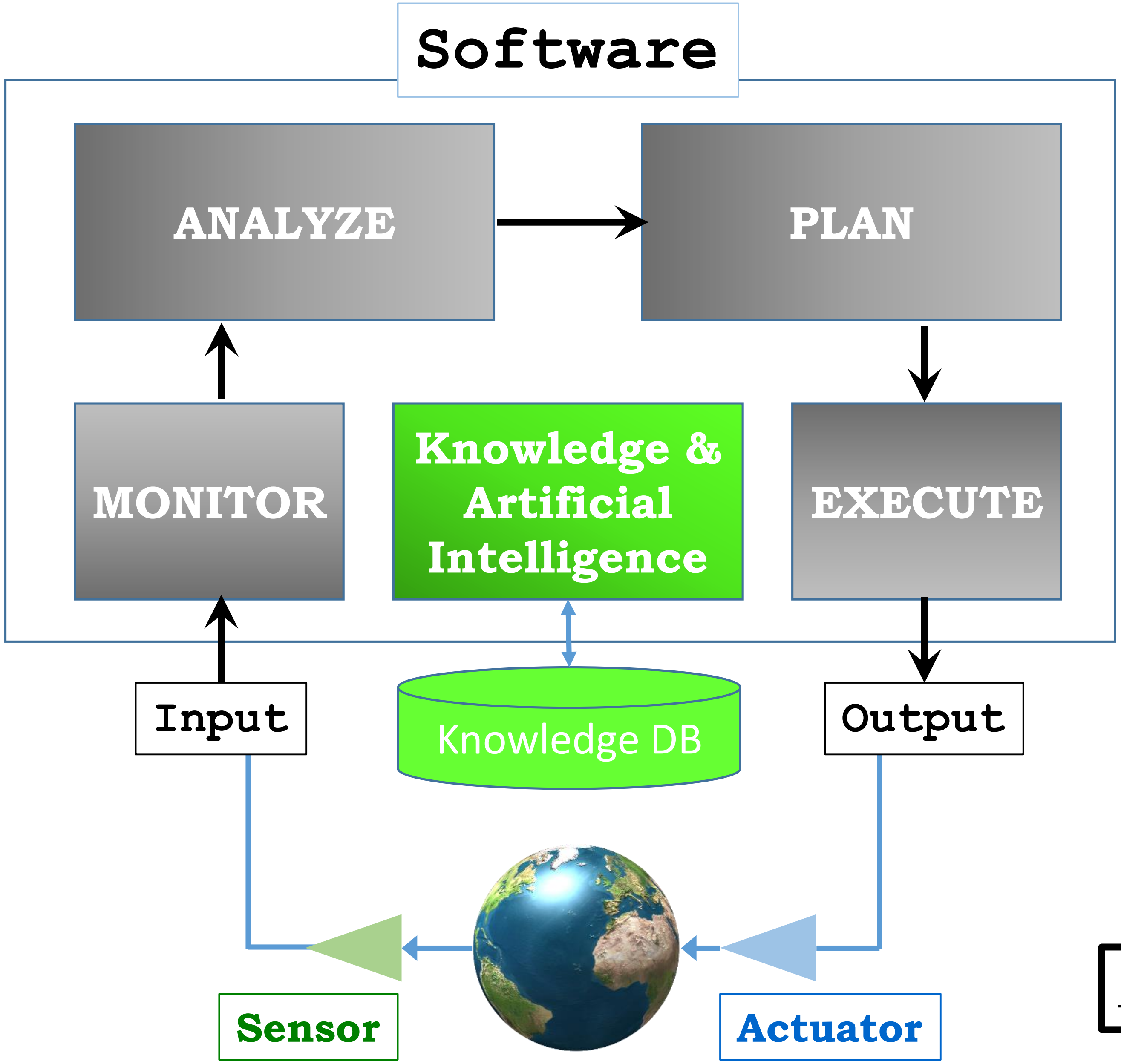
Real-World Model

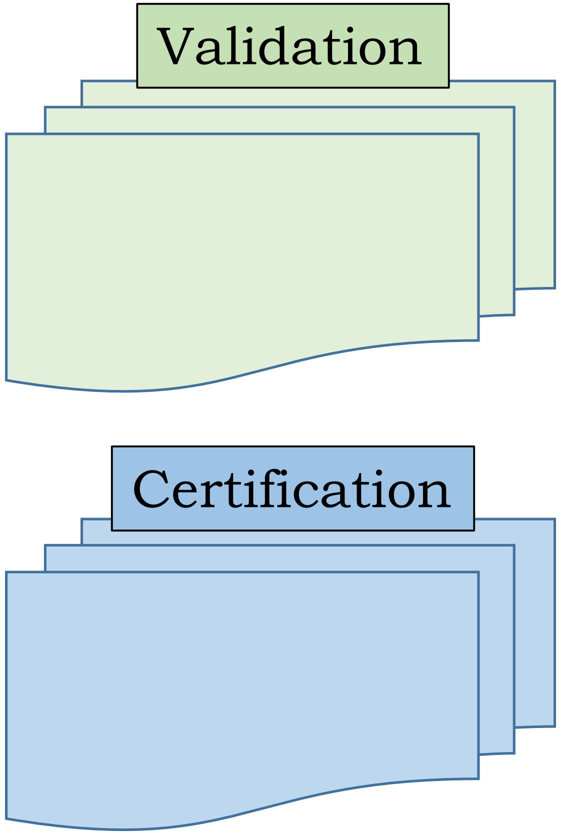


http://www.modelon.com

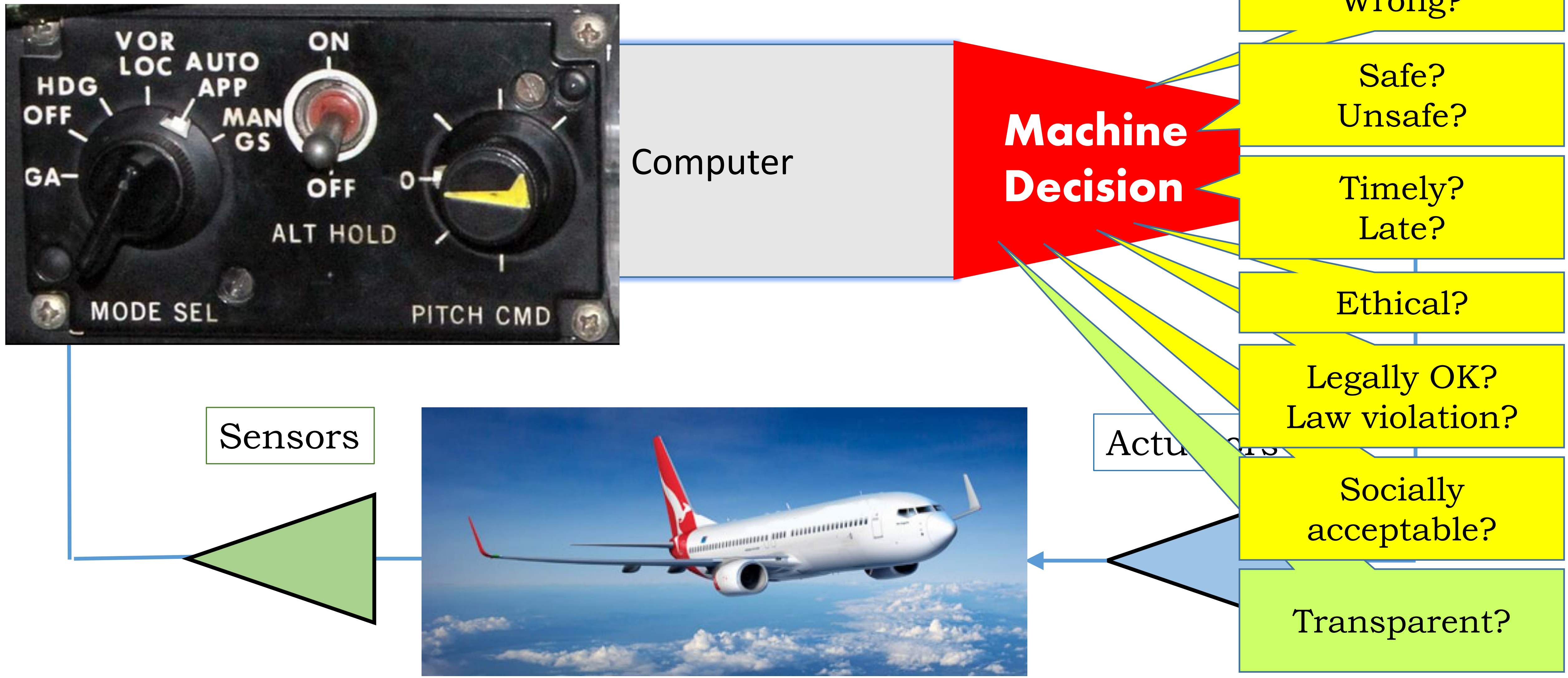
Requirements
- Functional
- Quality properties

Specifications
- Functional
- Quality properties





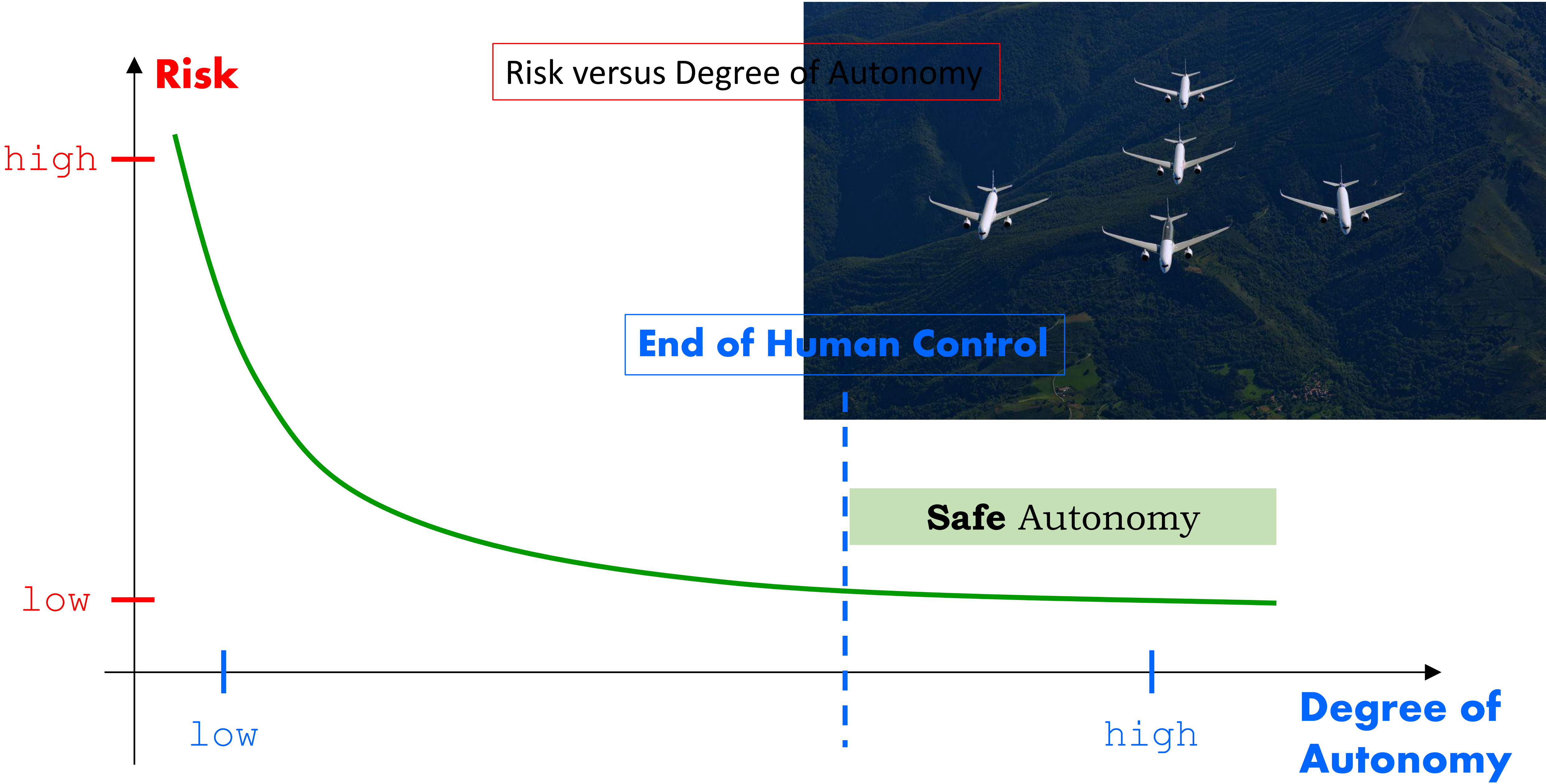
Decision Taking by Machines (i.e. Software)

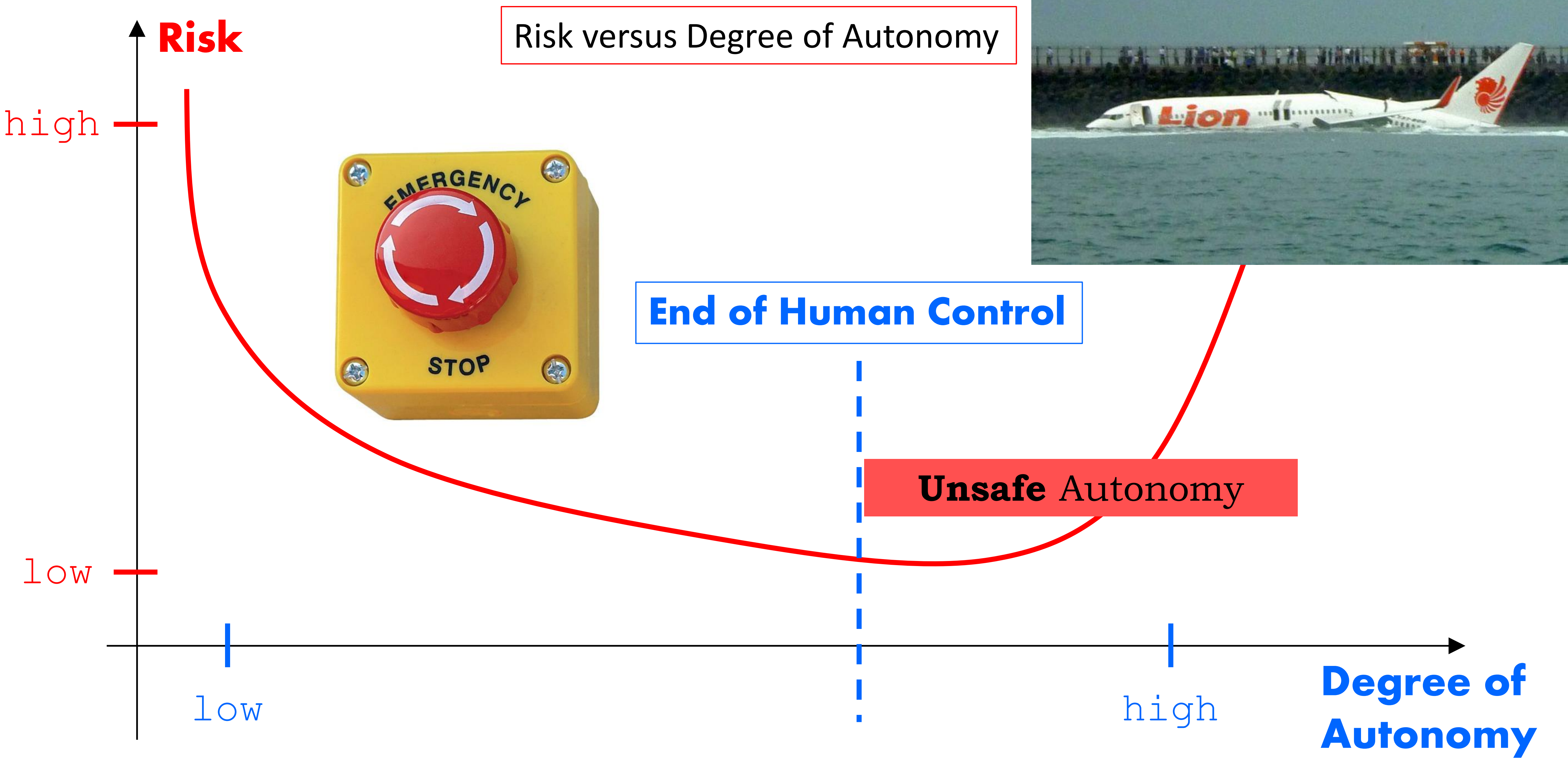


https://www.aitrends.com

http://www.yalescientific.org

Risk versus Degree of Autonomy





Risk versus Degree of Autonomy

Risk

high

low

End of Human Control

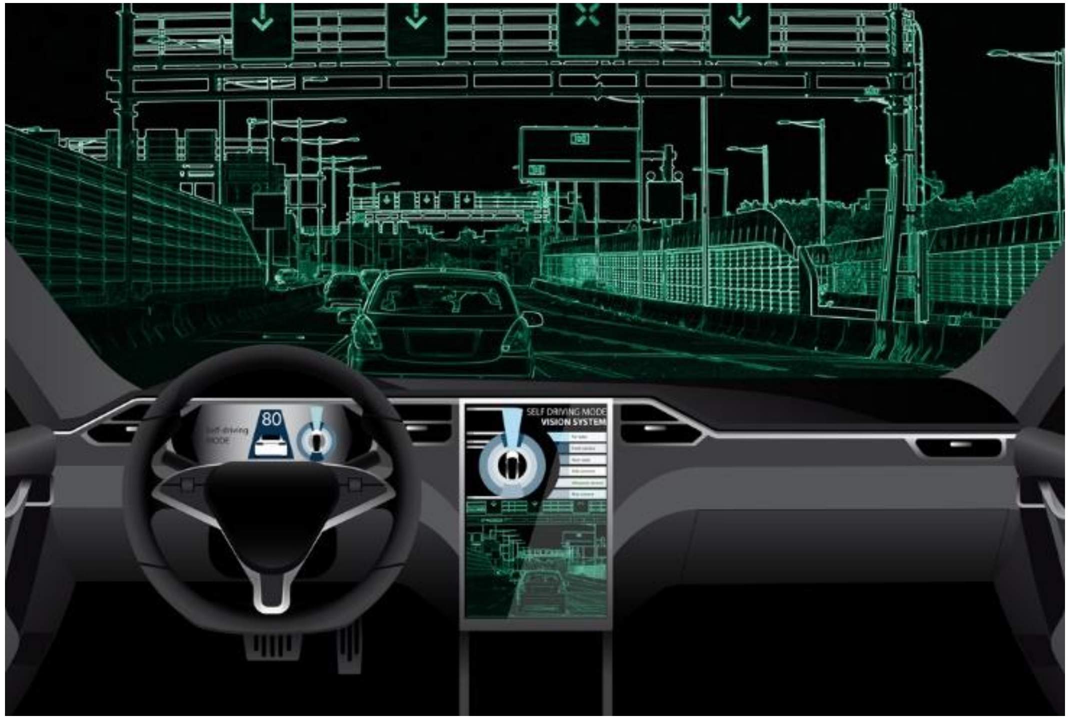
Unsafe Autonomy

low

high

Degree of Autonomy

Engineering Trustworthy Software for Cyber-Physical Systems



Content

- Introduction
- Technology: Cyber-Physical Systems
- Trustworthiness
- Engineering
- Conclusions

http://worldartsme.com

Trustworthy Software for Cyber-Physical System (CPS) :

= Cyber-physical system
with an adequate degree of security and safety
to fulfill the trust expectations of its users

Risk Consideration

Protection from malicious activities

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

Protection from failures, faults, errors, malfunctions

https://www.raymancini.academy

Risk Managment = Decisive Part of Systems Engineering !

A trustworthy system is the result of competent and responsible **engineering**

http://worldartsme.com

Definition: Trustworthy Cyber-Physical System and Cyber-Physical System-of-Systems

Cyber-physical system (CPS) or cyber-physical system-of-systems (CPSoS) with an adequate degree of security and safety to fulfill the trust expectations of its users

Security

Safety

https://www.ndtv.com

https://avnetlaw.com

User trust **expectations**

Examples

e-banking system:

- *security* (= defense against hackers)
- *integrity* (= don't digitally lose my money)
- *confidentiality* (= "it's my business")
- *availability* (= 24 h/7 days).

Car:

- *safety* (= no accidents)
- *security* (= no hostile influence)
- *reliability* (= no engine failures on the motorway)
- *conformance* to all laws and regulations

Trustworthiness expectations
=
Application domain

Security

https://www.ndtv.com

- Confidentiality
- Integrity
- Availability
- Multiple lines of defence
- Secure infrastructure
- etc.

Safety

https://avnetlaw.com

- Fault-Tolerance
- No single point of failure
- Graceful degradation
- Fault containment
- Diagnosability
- etc.

The set of **Security** & **Safety** properties depends on the *criticality* of the application

https://www.123rf.com

… some more examples of **un**trustworthy systems

Untrustworthy System **1: Crash Airbus A400M (9. Mai 2015)**

http://www.reuters.com

A400M: Military Transport Plane

Capacity: 37’000 kg

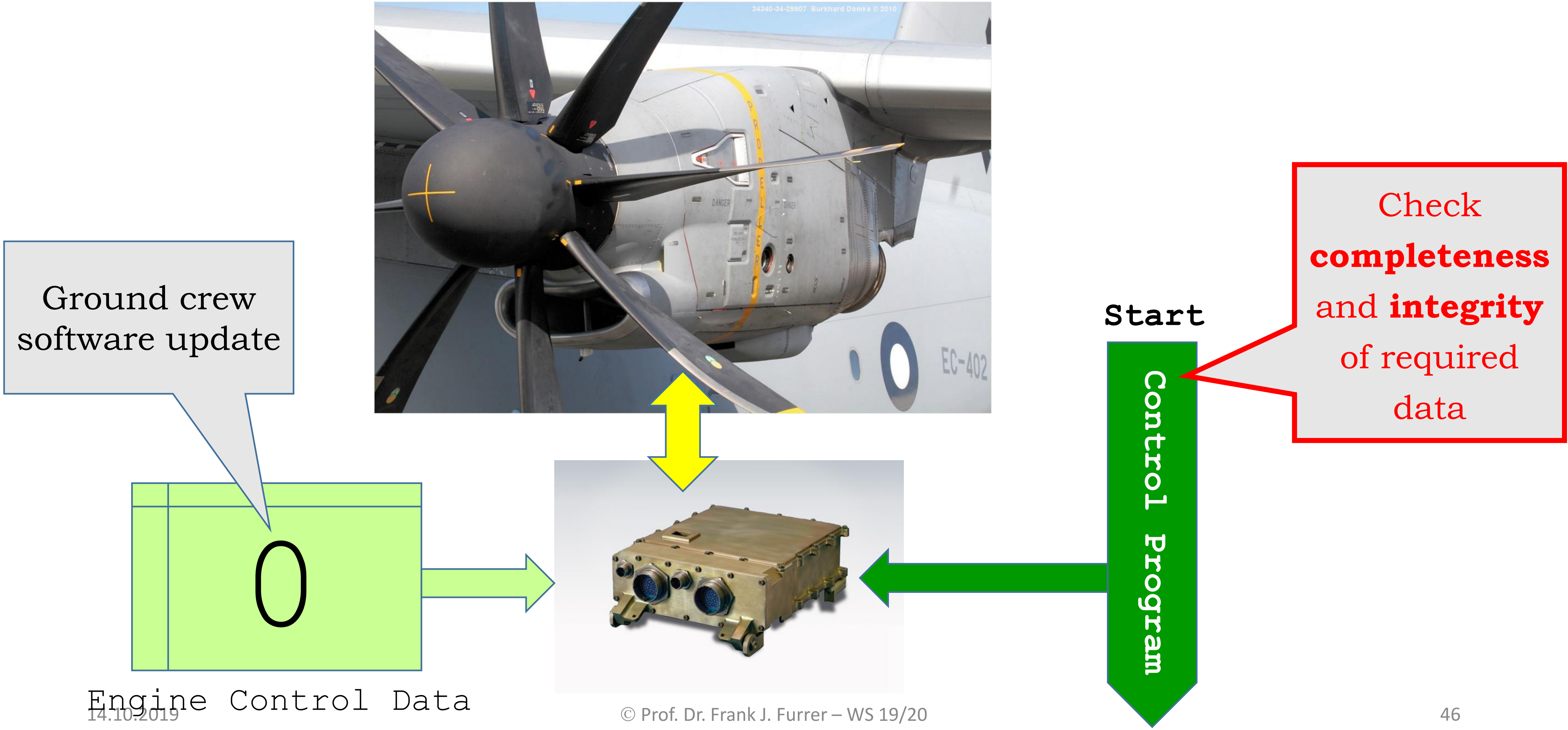
Range: > 3’000 km

Failure of the thrust control of 3 engines shortly after the start

⇒ **Crash**

http://www.ouest-france.fr

Untrustworthy System **1: Crash Airbus A400M (9. Mai 2015)**


Ground crew software update
0
Engine Control Data
Start
Control Program
Check **completeness** and **integrity** of required data
34340-34-29907 Burkhard Domke © 2010
EC-402

http://defence-blog.com

http://www.triumphgroup.com

Untrustworthy System **2**: **US$ 951 Million cyber-theft**

In February 2016, instructions to **steal US$ 951 million** from the central bank of Bangladesh, were issued via the SWIFT network

Five transactions issued by hackers, worth $101 million, succeeded

The Federal Reserve Bank of NY blocked the remaining thirty transactions, amounting to $850 million

Untrustworthy System **3**: **Unwanted acceleration of Toyota cars**

http://businessethicscases.blogspot.ch

The unwanted acceleration of Toyota and Lexus cars caused **89 traffic deaths** and **52 injured** from 2000 to 2010

Untrustworthy System **3**: **Unwanted acceleration of Toyota cars**

http://www.autoevolution.com

Toyota claimed in the beginning that the ***doormat*** was the source of the acceleration

Independent research demonstrated a ***software-problem*** in the throttle control

19. March 2014: Toyota pays a US-fine of 1.2 Billion US$

Untrustworthy System **4**: **Automated Trading Big Loss**

http://bilder1.n-tv.de

Knight Capital:

Computer-Trader
= high-frequency automated computer-trading

[10'000 Trades/sec
Holding: Milliseconds]

Computer-traded Loss on 1.8.2012 (NYSE): **440 Million US$**
(in 20 minutes)

Untrustworthy System **4**: **Automated Trading Big Loss**

http://www.nj.com

On 1.8.2012 at 9:30
the computers generated
(without human activity)
millions of ***faulty trades***

At 9:58 Knight Capital had lost **440 Millionen US$**

https://www.mytechlogy.com

Reason: **Programming mistake** in the high-frequency automated trading algorithm after a software-update

Untrustworthy System **5**: **Blockchain Code Exploit**

http://www.extremetech.com

A **blockchain** is a cryptographic, anonymous public ledger of all cryptocurrency transactions that have ever been executed in a community.

The blockchain-technology is the base for nearly all **FinTech** ventures.

http://www.bitcoinisle.com

http://fortune.com

Anyone who invested Ether into the ***DAO fund*** received a particular number of DAO tokens, which enabled them to vote on the projects that the DAO will fund. By the end of May, the DAO had raised more than **US$150 million** worth of Ether from investors.

http://www.bitcoinisle.com

http://www.coindesk.com

Untrustworthy System **6**: **Cryptocurrency Exchange Hacks**

https://cryptoeddy.com

A brief History of Crypto Exchanges Hacks
Total loss to date (Jul 11 – Sep 18):
$1,542,620,000.-
Source: https://discover.ledger.com/hackstimeline/

+ Wallet hacking
+ Mining hacking

Untrustworthy System **7**: **US Clinton e-Mail Hack**

https://www.theatlantic.com

In March 2016, the personal Gmail account of John Podesta, the chairman of Hillary Clinton's 2016 U.S. presidential campaign, was compromised in a data breach, and a collection of his **e-mails**, many of which were work-related, were stolen https://en.wikipedia.org/wiki/Podesta_emails

The e-mails were subsequently published by WikiLeaks.

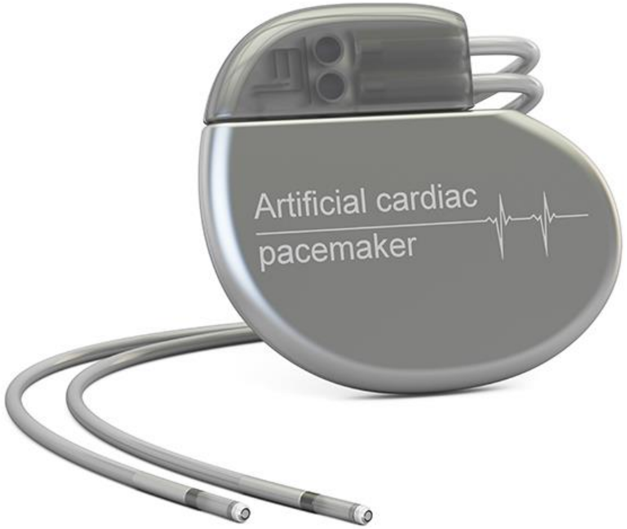
https://www.theatlantic.com:

"Conservatives will see corruption and liberals will see corporatism and expedience, but the exchanges simply expose the candidate who's been there all along"

The leaks certainly damaged Hilary Clinton's campaign and possibly decided the outcome

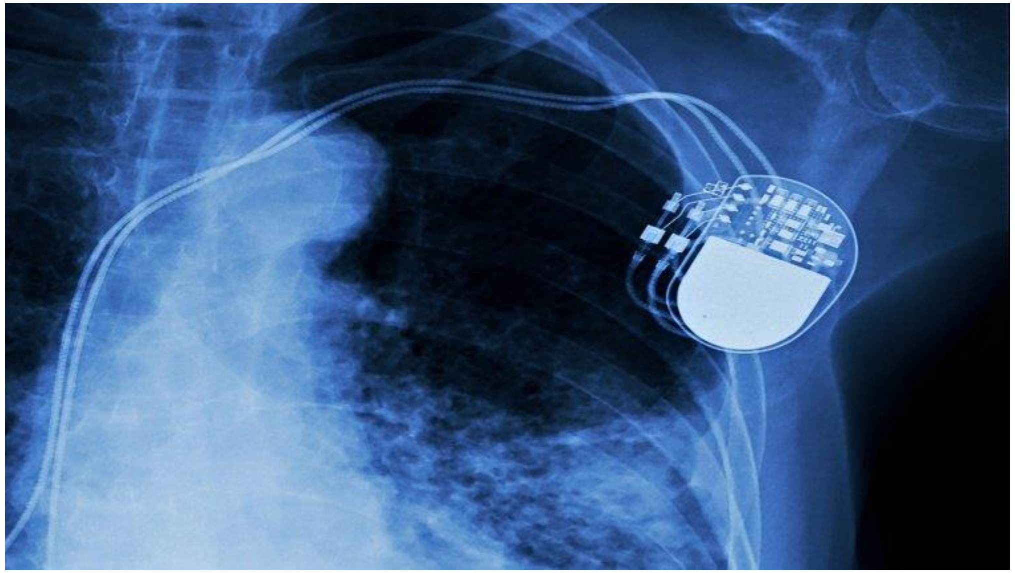
Untrustworthy System **8**: **Heart Pacemaker Vulnerability**

https://www.cisomag.com/wp-content/uploads/2017/08/Pacemaker.jpg



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://www.hackread.com/pacemaker-ecosystem-security-flaws-leave-vulnerable-hackers/

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

Untrustworthy System **9**: EQUIFAX Hacking

http://cdn.mos.cms.futurecdn.net

7. September 2017:

Data of 143 million Americans exposed in hack of credit reporting agency Equifax

https://www.washingtonpost.com

Hackers gained access to *sensitive personal data* — Social Security numbers, birth dates, home addresses, credit histories — for up to 143 million Americans, a major cybersecurity breach at a firm that serves as one of the three major clearinghouses for Americans' ***credit histories***

https://www.hackread.com

Untrustworthy System **10**: CAPITOL ONE Hacking

A hacker gained access to 100 million Capital One credit card applications and accounts

By Rob McLean, CNN Business
Updated 2117 GMT (0517 HKT) July 30, 2019

JOHANNES EISELE/AFP/AFP/GETTY IMAGES

https://edition.cnn.com

Paige Thompson is accused of breaking into a Capital One server and gaining access to 140,000 Social Security numbers, 1 million Canadian Social Insurance numbers and 80,000 bank account numbers, in addition to an undisclosed number of people's names, addresses, credit scores, credit limits, balances, and other information, according to the bank and the US Department of Justice

Untrustworthy System **11**: **IoT**

https://media.scmagazineuk.com

Looking at the **Internet of Things**, the market consistently fails to produce reasonably secure and trustworthy devices. This is especially true for smart home and consumer devices such as Internet routers, door locks, light bulbs and TVs. Manufacturers seem to have little economic incentive to implement secure software development processes or at least follow Security-by-Design principles. **This means that billions of severely insecure IoT devices will continue to proliferate the Internet** making it far too easy for criminals to exploit those vulnerable devices.

https://www.stiftung-nv.de/de/publikation/internet-insecure-things

Untrustworthy System **12**: **Water Supply Plant**

30.3.2016: Hackers Infiltrate Water Plant, Modify Chemical Levels

https://d.ibtimes.co.uk

Hackers infiltrated the control system at a *water treatment plant* and managed to *manipulate the level of chemicals* being used at the facility

The fallout from the hack was not as bad as it could have been. The water company reversed chemical and flow changes before any customers became ill

https://www.wateronline.com/doc/hackers-infiltrate-water-plant-modify-chemical-levels-0001

What is **common** to all these examples ?

https://www.decisivedge.com

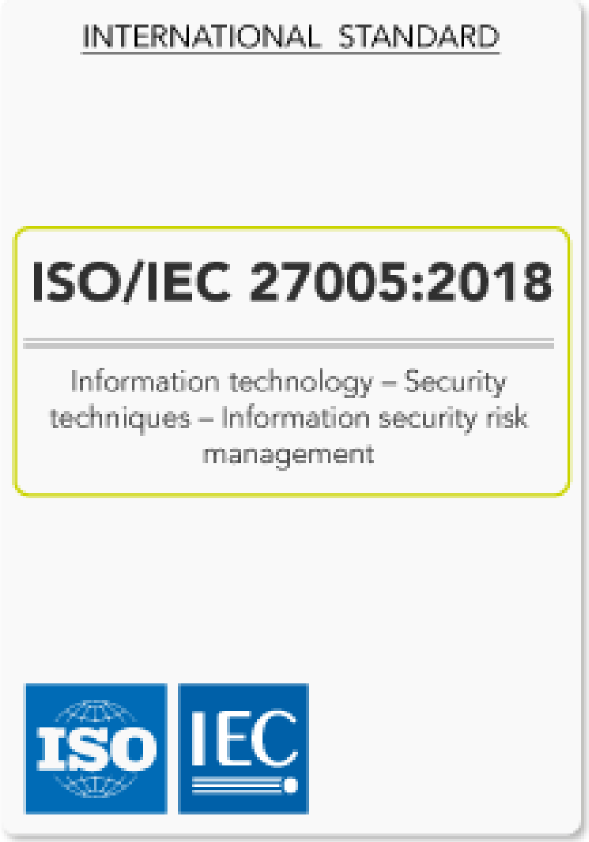
Software Fault

https://www.afcea.org

Software Vulnerability

What is **needed** to build and evolve trustworthy software ?

https://marketingland.com



INTERNATIONAL STANDARD

ISO/IEC 27005:2018

Information technology – Security techniques – Information security risk management

ISO IEC

A unambiguous and enforcable **specification** of trust

A reliable, provable **development process**

Conclusion

Everybody working in the software-industry

Our responsibility is to

architect, design, implement, and operate

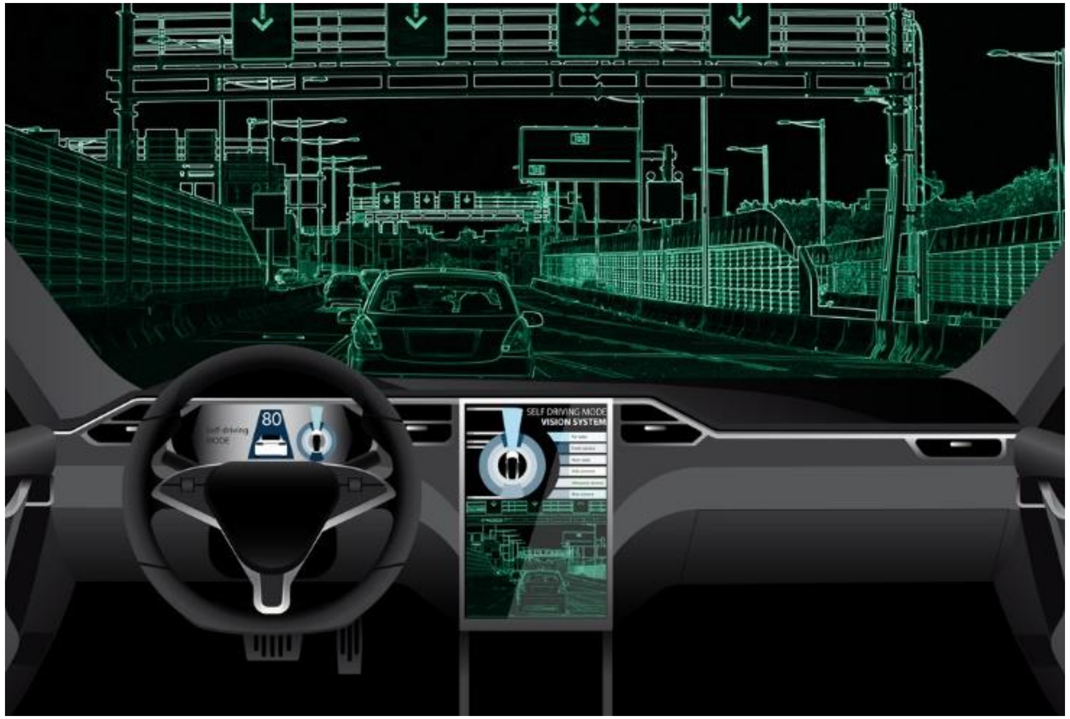
trustworthy, dependable software-systems

- especially cyber-physical systems

Vulnerable & risky

High damage potential

Engineering Trustworthy Software for Cyber-Physical Systems



Content

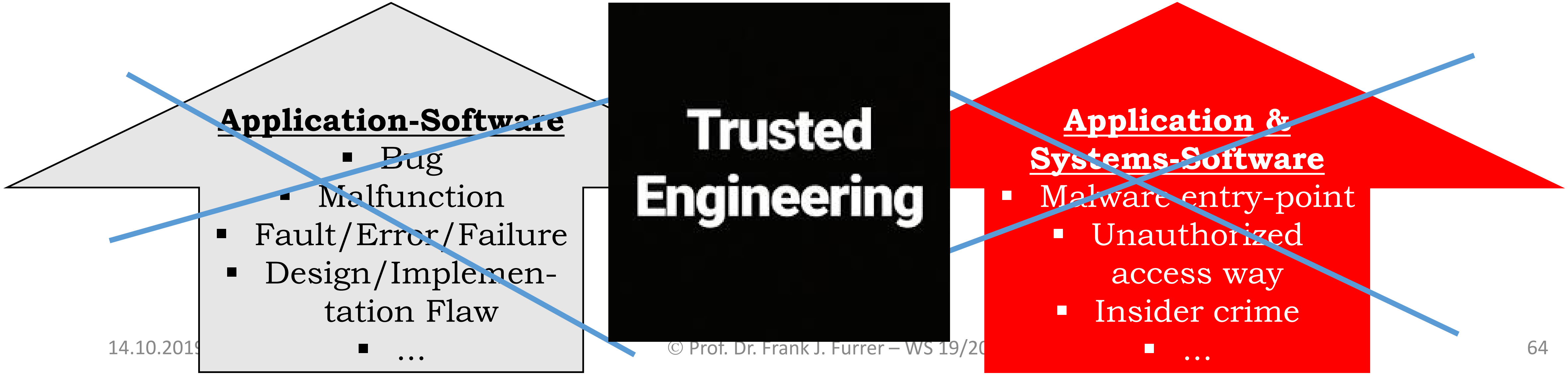
- Introduction
- Technology: Cyber-Physical Systems
- Trustworthiness
- **Engineering**
- Conclusions

https://www.decisivedge.com

https://www.afcea.org

Software Fault

Software Vulnerability



~~Application-Software~~

- ~~Bug~~
- ~~Malfunction~~
- ~~Fault/Error/Failure~~
- ~~Design/Implementation Flaw~~
- ~~…~~

~~Application & Systems-Software~~

- ~~Malware entry-point~~
- ~~Unauthorized access way~~
- ~~Insider crime~~
- ~~…~~

Building **trustworthy** systems = Successful **risk management**

Trustworthy Engineering Process

https://www.vasont.com

New system or system extension

Requirements & Specifications

Trustworthy Engineering Process

Trustworthy System

https://keyw.com

The **trustworthy engineering process** is a methodical series of steps that engineers use in creating functional products and processes following strict, proven principles for **assuring the relevant, non-functional system properties**

https://pngio.com

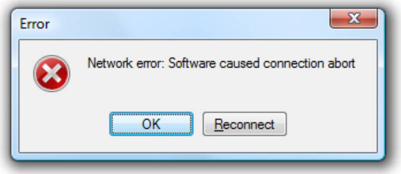
System/Software Evolution

Functionality

Quality Properties (…illities)
Security, Safety, Availability, Integrity, …

Subprocesses

Risk Management Process


Error

Network error: Software caused connection abort

No technical system can be operated with zero risk

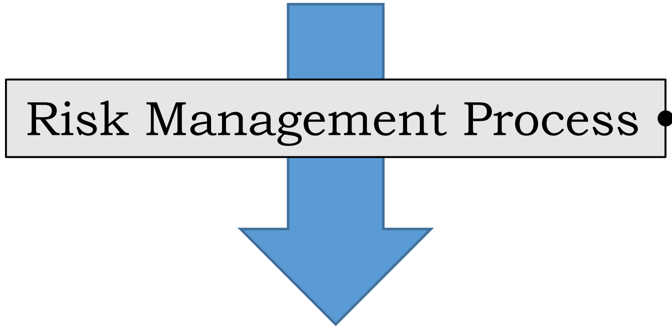
- A residual risk always remains

https://www.pinterest.ch

Acceptable Residual Risk

All technical systems are subject to many risks

«If you are on-line, you will be attacked. It is only a question of when»

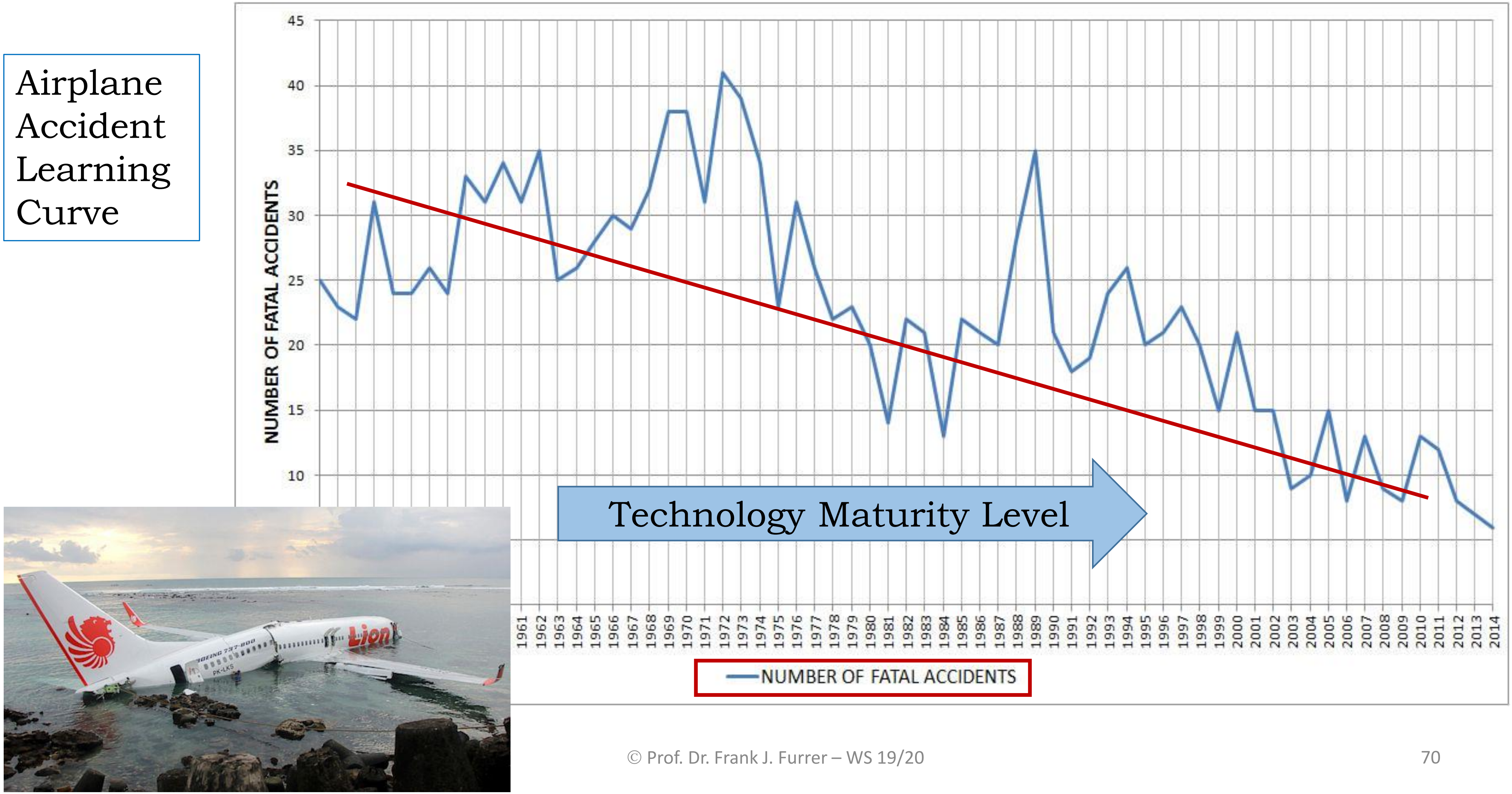

Risk Management Process

The **risk management process** assures that risks are reduced to acceptable residual risks

Acceptable Residual Risk

However carefully you build and operate your technical systems – there always remains a last bit of risk – the **residual risk**.
The residual risk must be **acceptable**!

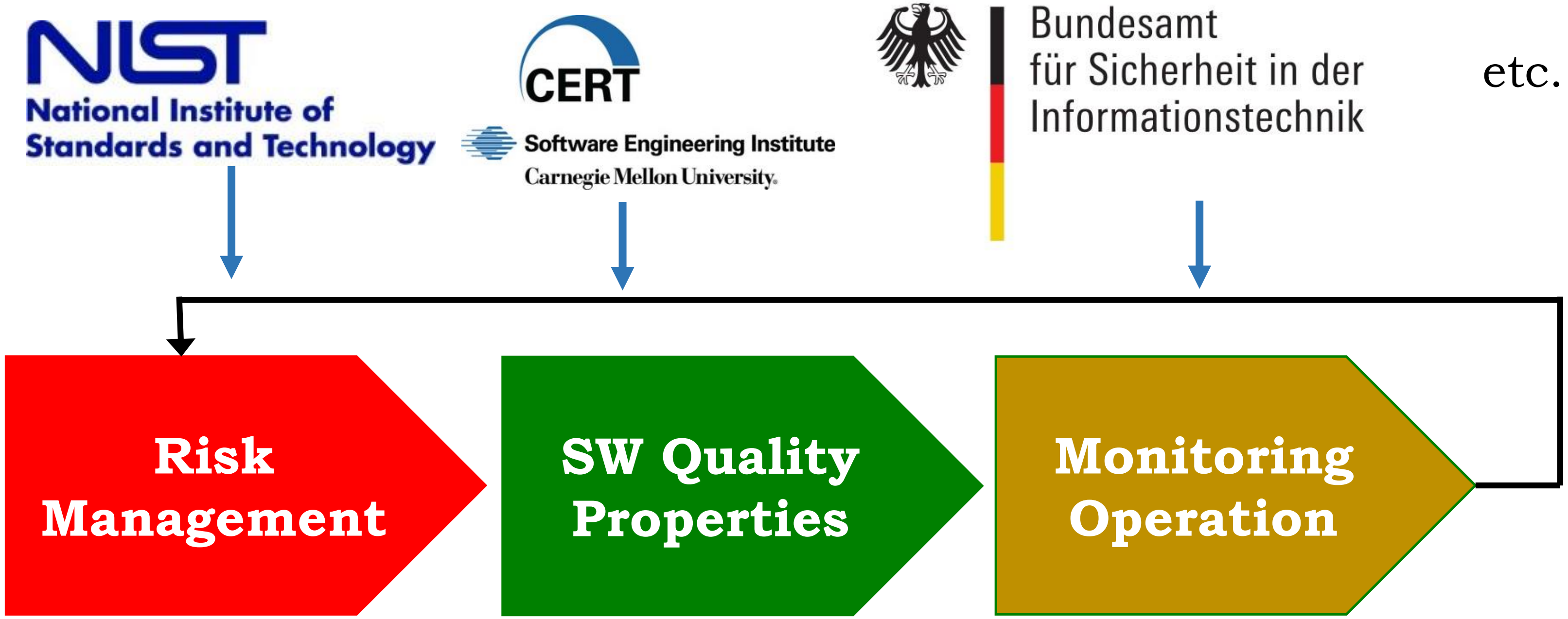
Airplane Accident Learning Curve



Source: http://www.planecrashinfo.com/cause.htm [16.1.2017]

$$\text{«}\underbrace{\textbf{Engineering}}\textbf{ Trustworthy Software for Cyber-Physical Systems»}$$

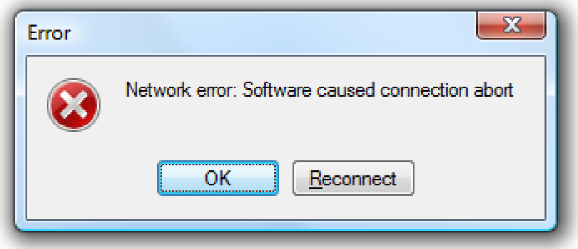
Systems engineering is an interdisciplinary field of engineering and engineering management that focuses on how to design, implement, maintain and manage complex systems over their life cycles
https://en.wikipedia.org/wiki/Systems_engineering


NIST
National Institute of Standards and Technology
CERT
Software Engineering Institute
Carnegie Mellon University
Bundesamt für Sicherheit in der Informationstechnik
etc.
Risk Management
SW Quality Properties
Monitoring Operation

Engineering for Trustworthiness

Technical Debt

Architecture Erosion



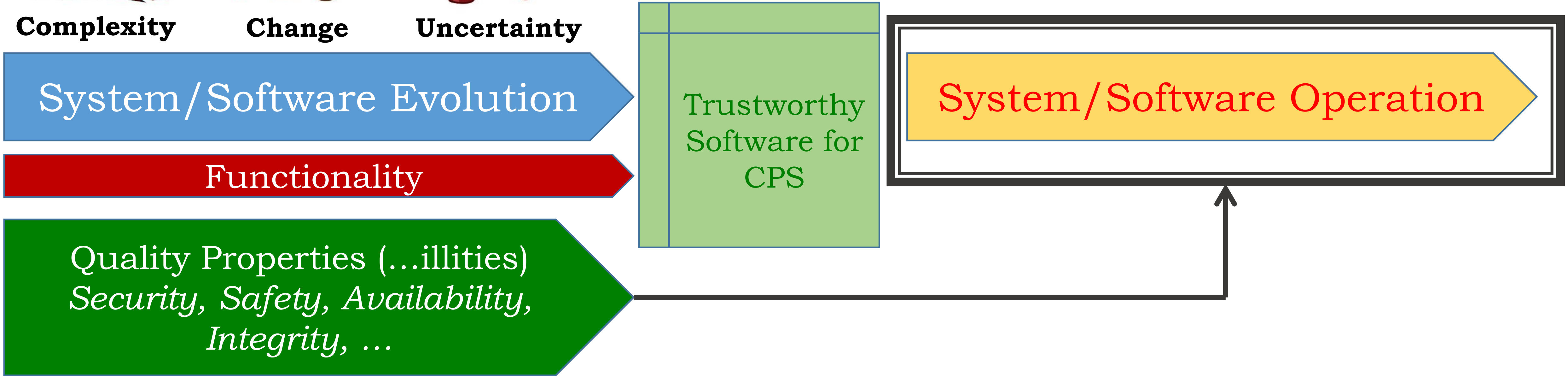
Error

Network error: Software caused connection abort

Complexity

Change

Uncertainty



System/Software Evolution

Functionality

Quality Properties (…illities)
Security, Safety, Availability, Integrity, …

Trustworthy Software for CPS

System/Software Operation

Trustworthy Software for CPS

http://clipartmag.com

System/Software Evolution

Functionality

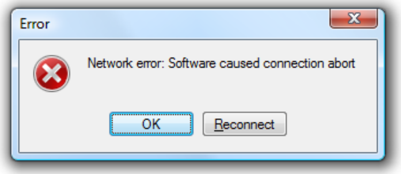
Quality Properties (…illities)
Security, Safety, Availability, Integrity, …

- ✓ For trustworthy software the **…illities** (security, safety, availability, integrity, …) have priority over functionality
- ✓ Sufficient effort and the **best resources** must be invested into the … illities throughout the full life-cycle of the software

Risk Management Process

✓ Acceptable Residual **Security** Risk

✓ Acceptable Residual **Safety** Risk

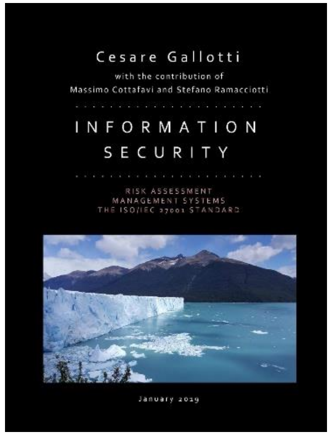

Error

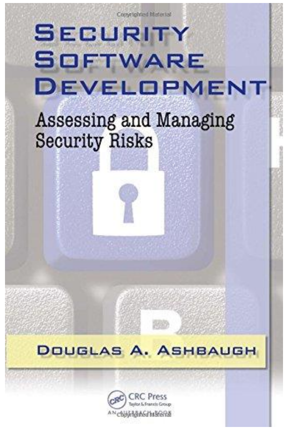
Network error: Software caused connection abort

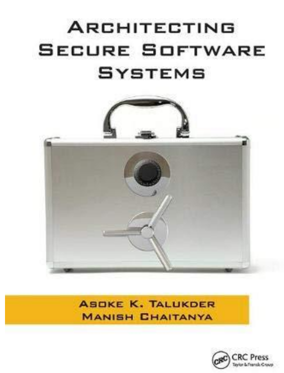
Risk Management Process

Acceptable Residual Risk

WS19/20: Engineering Trustworthy Software for Cyber-Physical Systems


Cesare Gallotti
with the contribution of Massimo Cottafavi and Stefano Ramacciotti
INFORMATION SECURITY
RISK ASSESSMENT MANAGEMENT SYSTEMS THE ISO/IEC 27001 STANDARD
January 2019


SECURITY SOFTWARE DEVELOPMENT
Assessing and Managing Security Risks
DOUGLAS A. ASHBAUGH
CRC Press



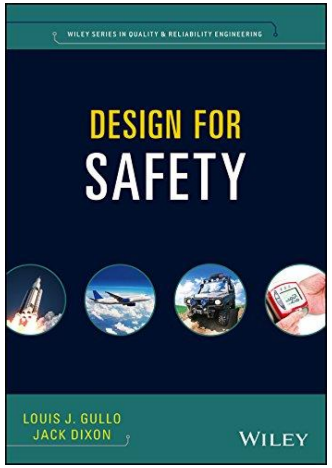
Unfortunately,
The Risk Management Processes
for **Security** and for **Safety**
are <u>very different and incompatible</u>

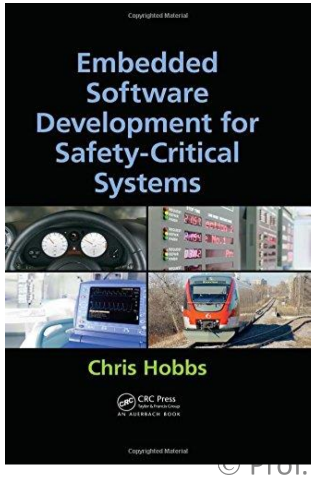
Security Risk Management Process

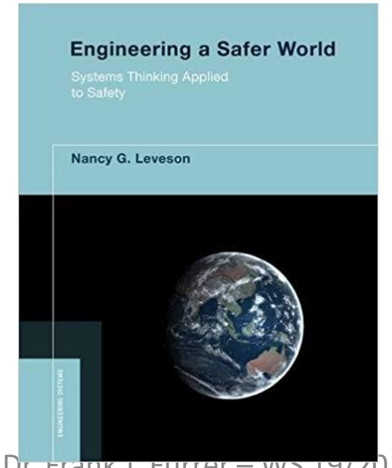
Safety Risk Management Process

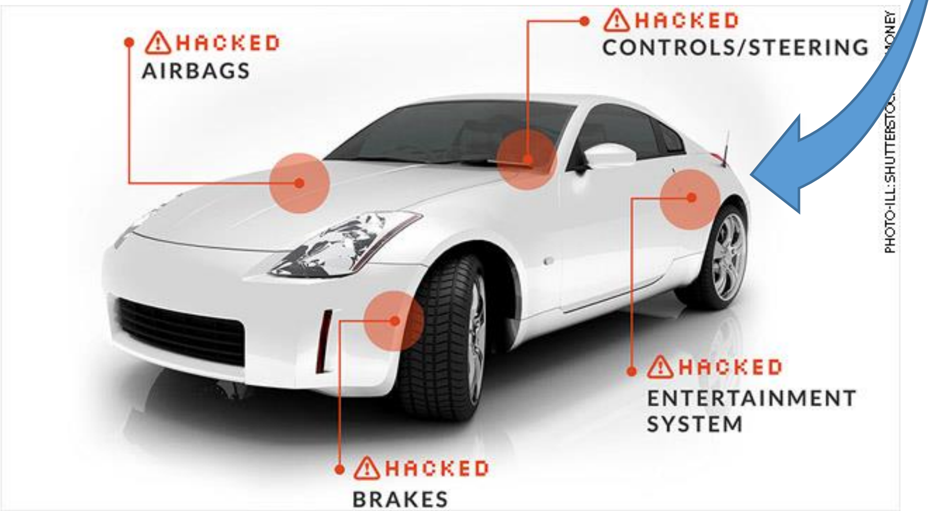
Acceptable Residual Security Risk

Acceptable Residual Safety Risk

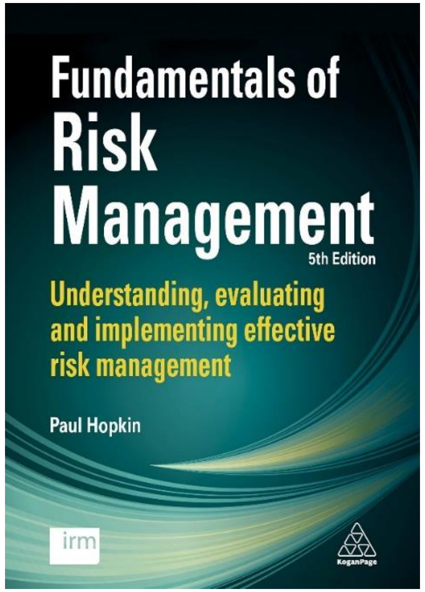


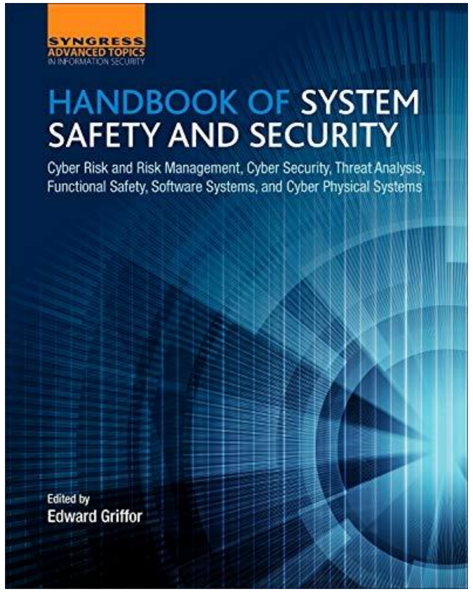


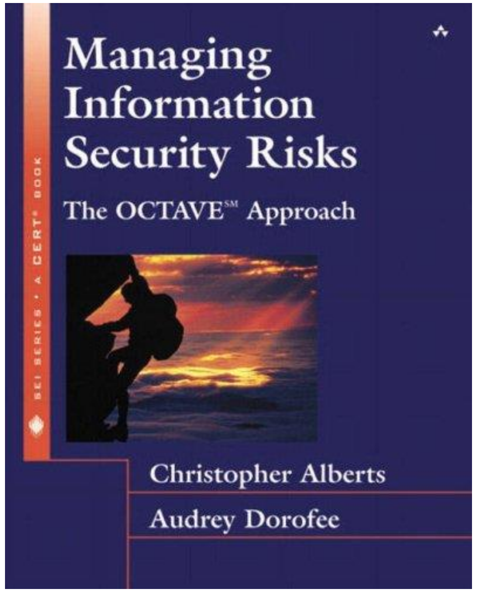




https://money.cnn.com/2014/06/01/technology/security/car-hack/index.html


Fundamentals of Risk Management
5th Edition
Understanding, evaluating and implementing effective risk management
Paul Hopkin


SYNGRESS ADVANCED TOPICS IN INFORMATION SECURITY
HANDBOOK OF SYSTEM SAFETY AND SECURITY
Cyber Risk and Risk Management, Cyber Security, Threat Analysis, Functional Safety, Software Systems, and Cyber Physical Systems
Edited by
Edward Griffor

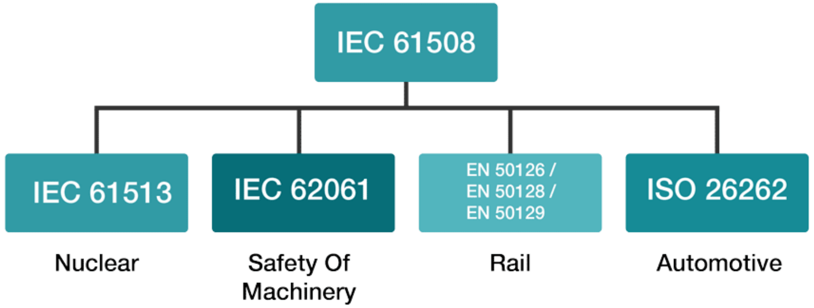

Managing Information Security Risks
The OCTAVE℠ Approach
Christopher Alberts
Audrey Dorofee

A significant number of risk management **methodologies** exist

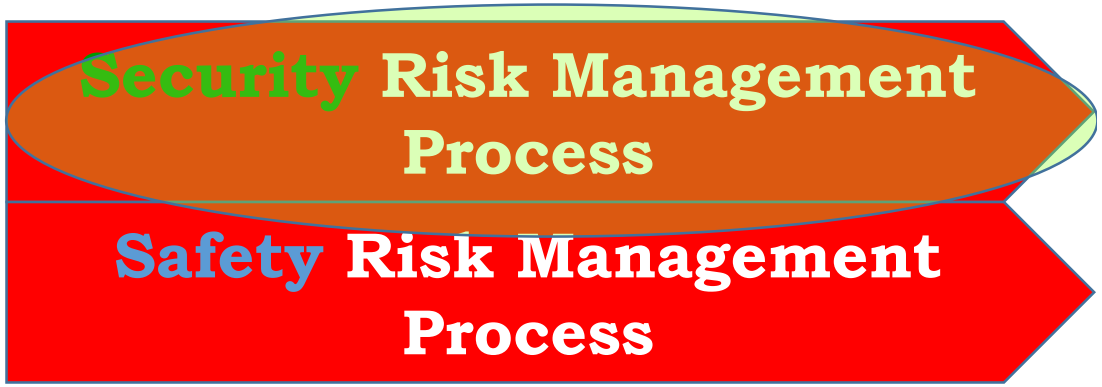
Many industries are based on risk management **standards**

Companies have their own set of methodologies & standards

ISO 26262
Road Vehicles - Fuctional Safety



ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization
https://www.iso.org/standard/54534.html

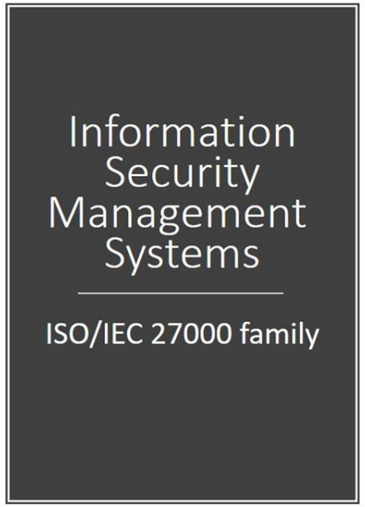


Security Risk Management Process

Safety Risk Management Process

ISO 27000 is a large **family** of standards

… and is growing
(⇒ application-specific security standards)



Information Security Management Systems

ISO/IEC 27000 family

ISO 27000

Edition <kes>

Heinrich Kersten
Gerhard Klett
Jürgen Reuter
Klaus-Werner Schröder

IT-Sicherheitsmanagement nach der neuen ISO 27001

ISMS, Risiken, Kennziffern, Controls

<kes>

Springer Vieweg

https://www.isocertificateonline.in/revision-of-isms-standard-iso-iec-27000

1 of 7

The ISO27k Standards

List contributed and maintained by Gary Hinson

#	Standard	Published	Title	Notes
1	ISO/IEC 27000	2018	Information security management systems — **Overview and vocabulary**	Overview/introduction to the ISO27k standards as a whole plus a glossary of terms; **FREE!**
2	ISO/IEC 27001	2013	Information security management systems — **Requirements**	Formally specifies an ISMS against which thousands of organizations have been certified compliant
3	ISO/IEC 27002	2013	Code of practice for **information security controls**	A reasonably comprehensive suite of information security control objectives and generally-accepted good practice security controls
4	ISO/IEC 27003	2017	Information security management system **implementation guidance**	Sound advice on implementing ISO27k, expanding section-by-section on the main body of ISO/IEC 27001
5	ISO/IEC 27004	2016	Information security management — **Measurement**	Much improved second version, with useful advice on security metrics
6	ISO/IEC 27005	2018	Information security **risk management**	Discusses information risk management principles in general terms without specifying or mandating particular methods. *Major revision in progress*

2 of 7

The ISO27k Standards

List contributed and maintained by Gary Hinson

7	ISO/IEC 27006	2015	Requirements for bodies providing audit and **certification** of information security management systems	Formal guidance for the certification bodies, with several grammatical errors – needs revision
8	ISO/IEC 27007	2017	Guidelines for information security **management systems auditing**	Auditing the *management system* elements of the ISMS
9	ISO/IEC TR 27008	2011	Guidelines for auditors on **information security controls**	Auditing the *information security* elements of the ISMS
10	ISO/IEC 27009	2016	**Sector-specific** application of ISO/IEC 27001 – requirements	Guidance for those developing new ISO27k standards (*i.e.* ISO/IEC JTC1/SC27 – an internal committee standing document really)
11	ISO/IEC 27010	2015	Information security management for **inter-sector and inter-organisational communications**	Sharing information on information security between industry sectors and/or nations, particularly those affecting "critical infrastructure"
12	ISO/IEC 27011	2016	Information security management guidelines for **telecommunications** organizations based on ISO/IEC 27002	Information security controls for the telecoms industry; also called "ITU-T Recommendation x.1051"
13	ISO/IEC 27013	2015	Guidance on the **integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1**	Combining ISO27k/ISMS with IT Service Management/ITIL
14	ISO/IEC 27014	2013	**Governance** of information security	Governance in the context of information security; will also be called "ITU-T Recommendation X.1054"
16	ISO/IEC TR 27016	2014	Information security management – Organizational **economics**	Economic theory applied to information security

3 of 7

The ISO27k Standards

List contributed and maintained by Gary Hinson

17	ISO/IEC 27017	2015	Code of practice for information security controls for **cloud computing** services based on ISO/IEC 27002	Information security controls for cloud computing
18	ISO/IEC 27018	2014	Code of practice for controls to protect **personally identifiable information** processed in public **cloud** computing services	Privacy controls for cloud computing
19	ISO/IEC TR 27019	2017	Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the **energy industry**	Information security for ICS/SCADA/embedded systems (not just used in the energy industry!), *excluding* the nuclear industry
20	ISO/IEC 27021	2017	**Competence** requirements for information security management professionals	Guidance on the skills and knowledge necessary to work in this field
21	ISO/IEC 27023	2015	Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002	Belated advice for those updating their ISMSs from the 2005 to 2013 versions
22	ISO/IEC 27030	DRAFT	Guidelines for security and privacy in **I**nternet **o**f **T**hings (**IoT**)	A standard about the information risk, security and privacy aspects of IoT
23	ISO/IEC 27031	2011	Guidelines for **information and communications technology readiness for business continuity**	Continuity (*i.e.* resilience, incident management and disaster recovery) for ICT, supporting general business continuity
24	ISO/IEC 27032	2012	Guidelines for cybersecurity	Ignore the vague title: this standard actually concerns **Internet security**

4 of 7

The ISO27k Standards

List contributed and maintained by Gary Hinson

25	ISO/IEC 27033	-1 2015	**Network security** overview and concepts	Various aspects of network security, updating and replacing ISO/IEC 18028
26		-2 2012	Guidelines for the design and implementation of network security	
27		-3 2010	Reference networking scenarios - threats, design techniques and control issues	
28		-4 2014	Securing communications between networks using security gateways	
29		-5 2013	Securing communications across networks using Virtual Private Networks (VPNs)	
30		-6 2016	Securing wireless IP network access	
31	ISO/IEC 27034	-1 2011	**Application security** — Overview and concepts	Multi-part application security standard Promotes the concept of a reusable library of information security control functions, formally specified, designed and tested
32		-2 2015	Organization normative framework	
33		-3 2018	Application security management process	
34		-4 DRAFT	Application security validation	
35		-5 2017	Protocols and application security control data structure	
36		-5-1 2018	Protocols and application security control data structure, XML schemas	

5 of 7

The ISO27k Standards

List contributed and maintained by Gary Hinson

37		-6 2016	Case studies	
38		-7 2018	Application security assurance prediction framework	
39	ISO/IEC 27035	-1 2016	Information security incident management — Principles of **incident management**	Replaced ISO TR 18044 Actually concerns incidents affecting IT systems and networks, specifically
40		-2 2016	— Guidelines to plan and prepare for incident response	
41		-3 DRAFT	— Guidelines for incident response operations??	Part 3 drafting restarted – due out in 2019 or 2020
42	ISO/IEC 27036	-1 2014	Information security for **supplier relationships** – Overview and concepts (**FREE!**)	Information security aspects of ICT outsourcing and services
43		-2 2014	— Common requirements	
44		-3 2013	— Guidelines for ICT supply chain security	
45		-4 2016	— Guidelines for security of cloud services	
46	ISO/IEC 27037	2012	Guidelines for identification, collection, acquisition, and preservation of **digital evidence**	One of several IT forensics standards
47	ISO/IEC 27038	2014	Specification for digital **redaction**	Redaction of digital documents
48	ISO/IEC 27039	2015	Selection, deployment and operations of **intrusion detection and prevention** systems (IDPS)	IDS/IPS

6 of 7

The ISO27k Standards

List contributed and maintained by Gary Hinson

49	ISO/IEC 27040	2015	**Storage** security	IT security for stored data
50	ISO/IEC 27041	2015	Guidelines on assuring suitability and adequacy of incident **investigative methods**	Assurance of the integrity of forensic evidence is absolutely vital
51	ISO/IEC 27042	2015	Guidelines for the **analysis and interpretation of digital evidence**	IT forensics analytical methods
52	ISO/IEC 27043	2015	**Incident investigation** principles and processes	The basic principles of eForensics
53	ISO/IEC 27050	-1 2016	**Electronic discovery** – overview and concepts	More eForensics advice
54		-2 2018	Guidance for governance and management of electronic discovery	Advice on treating the risks relating to eForensics
55		-3 2017	Code of practice for electronic discovery	A *how-to-do-it* guide to eDiscovery
56		-4 DRAFT	ICT readiness for electronic discovery	Guidance on eDiscovery technology (tools, systems and processes)
57	ISO/IEC 27070	DRAFT	Security requirements for establishing virtualized roots of trust	Concerns **trusted cloud computing**
58	ISO/IEC 27099	DRAFT	**Public key infrastructure** - practices and policy framework	Infosec management requirements for Certification Authorities
59	ISO/IEC 27100	DRAFT	**Cybersecurity** – overview and concepts	Perhaps this standard will clarify, once and for all, what ‘cybersecurity’ actually is. Perhaps not.
60	ISO/IEC 27101	DRAFT	**Cybersecurity** framework development guidelines	Given the above, we can barely guess what this might turn out to be

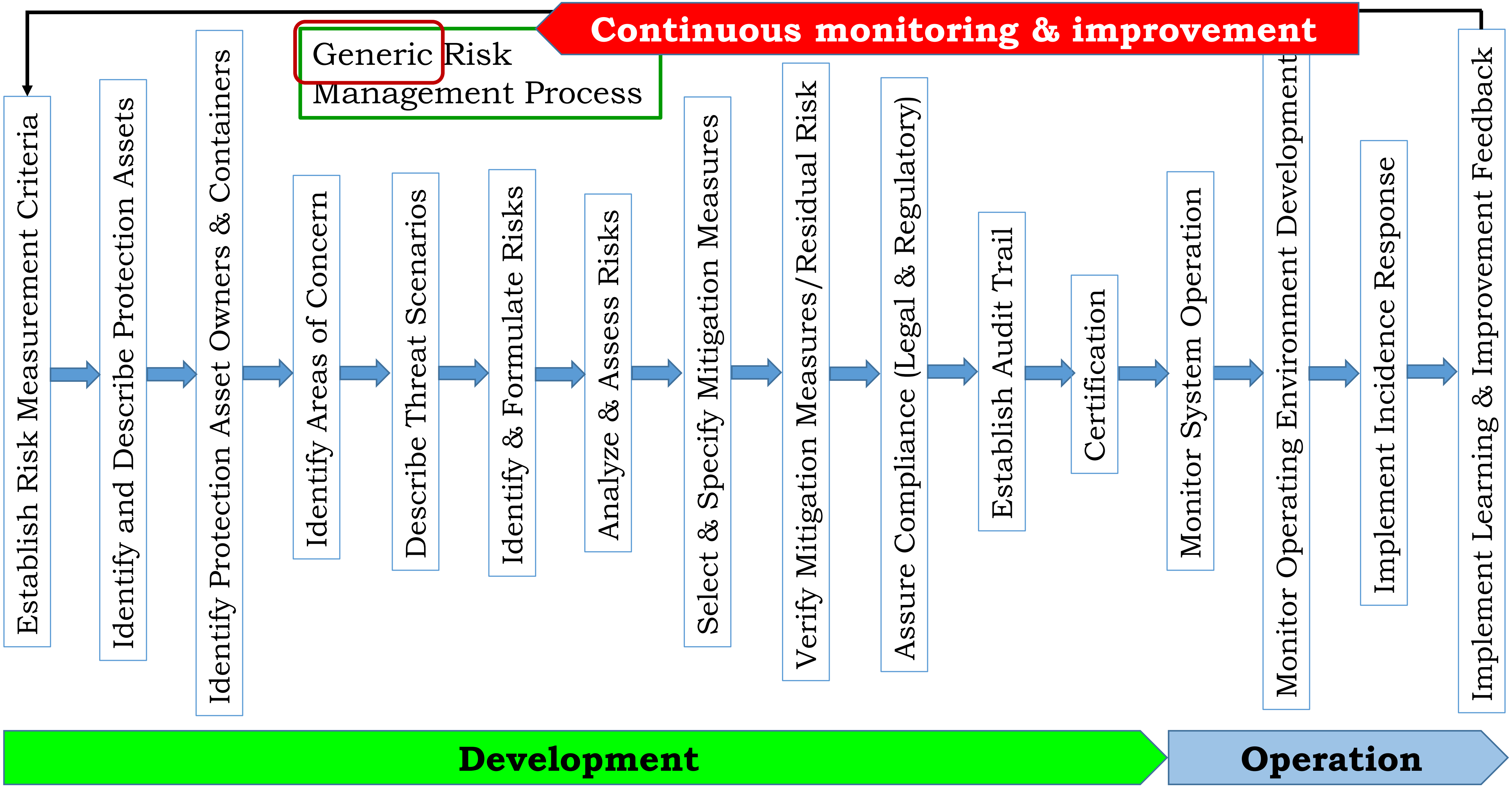
7 of 7

The ISO27k Standards

List contributed and maintained by Gary Hinson

61	ISO/IEC 27102	DRAFT	Information security management guidelines for **cyber insurance**	Advice on obtaining insurance to reduce the costs of cyber incidents
62	ISO/IEC TR 27103	2018	**Cybersecurity** and ISO and IEC standards	Explains how ISO27k and other ISO and IEC standards relate to 'cybersecurity' (without actually defining the term!)
63	ISO/IEC 27550	DRAFT	Privacy engineering	How to address privacy throughout the lifecycle of IT systems
64	ISO/IEC 27551	DRAFT	Requirements for attribute-based unlinkable entity authentication	Seems more like an authentication standard than ISO27k … scope creep?
65	ISO/IEC 27552	DRAFT	Extension to ISO/IEC 27001 and to ISO/IEC 27002 for privacy management — Requirements and guidelines	Explains extensions to an ISO27k ISMS for privacy management
66	ISO/IEC 27553	DRAFT	Security requirements for authentication using biometrics on mobile devices	High-level requirements attempting to standardize the use of biometrics on mobile devices
67	ISO/IEC 27554	DRAFT	Application of ISO 31000 for assessment of identity management-related risk	About applying the ISO 31000 risk management process to identity management
68	ISO/IEC 27555	DRAFT	Establishing a PII deletion concept in organizations	A conceptual framework, of all things, for deleting personal information
69	ISO 27799	2016	Health informatics — Information security management in **health** using ISO/IEC 27002	Infosec management advice for the health industry

Generic Risk Management Process



Continuous monitoring & improvement

Establish Risk Measurement Criteria

Identify and Describe Protection Assets

Identify Protection Asset Owners & Containers

Identify Areas of Concern

Describe Threat Scenarios

Identify & Formulate Risks

Analyze & Assess Risks

Select & Specify Mitigation Measures

Verify Mitigation Measures/Residual Risk

Assure Compliance (Legal & Regulatory)

Establish Audit Trail

Certification

Monitor System Operation

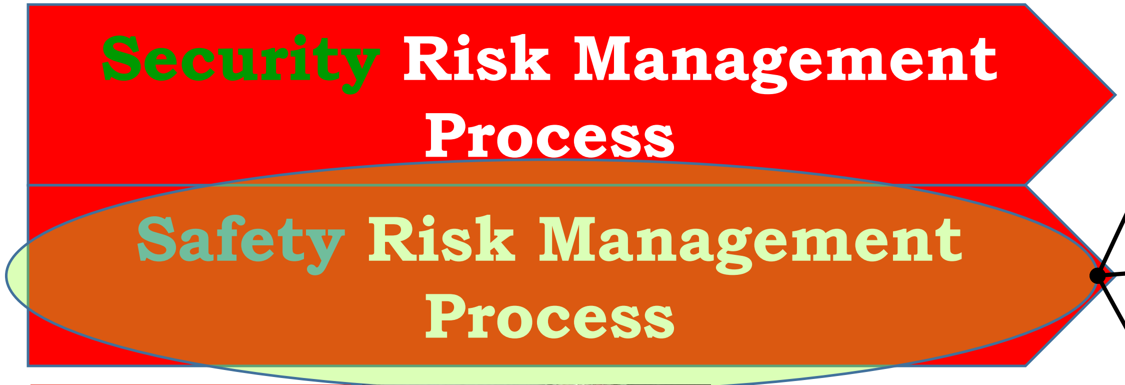
Monitor Operating Environment Development

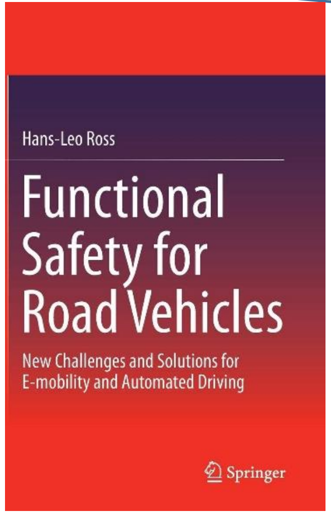
Implement Incidence Response

Implement Learning & Improvement Feedback

Development

Operation


Security Risk Management Process
Safety Risk Management Process



Hans-Leo Ross

Functional Safety for Road Vehicles

New Challenges and Solutions for E-mobility and Automated Driving

Springer

Vera Gebhardt · Gerhard M. Rieger · Jürgen Mottok · Christian Gießelbach

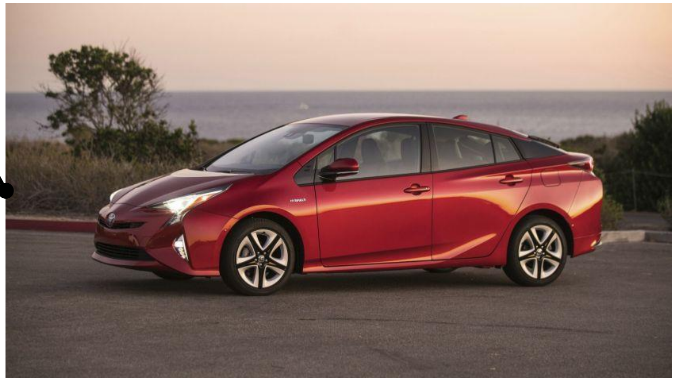
Funktionale Sicherheit nach ISO 26262

Ein Praxisleitfaden zur Umsetzung

dpunkt.verlag

https://blog.trainman.in

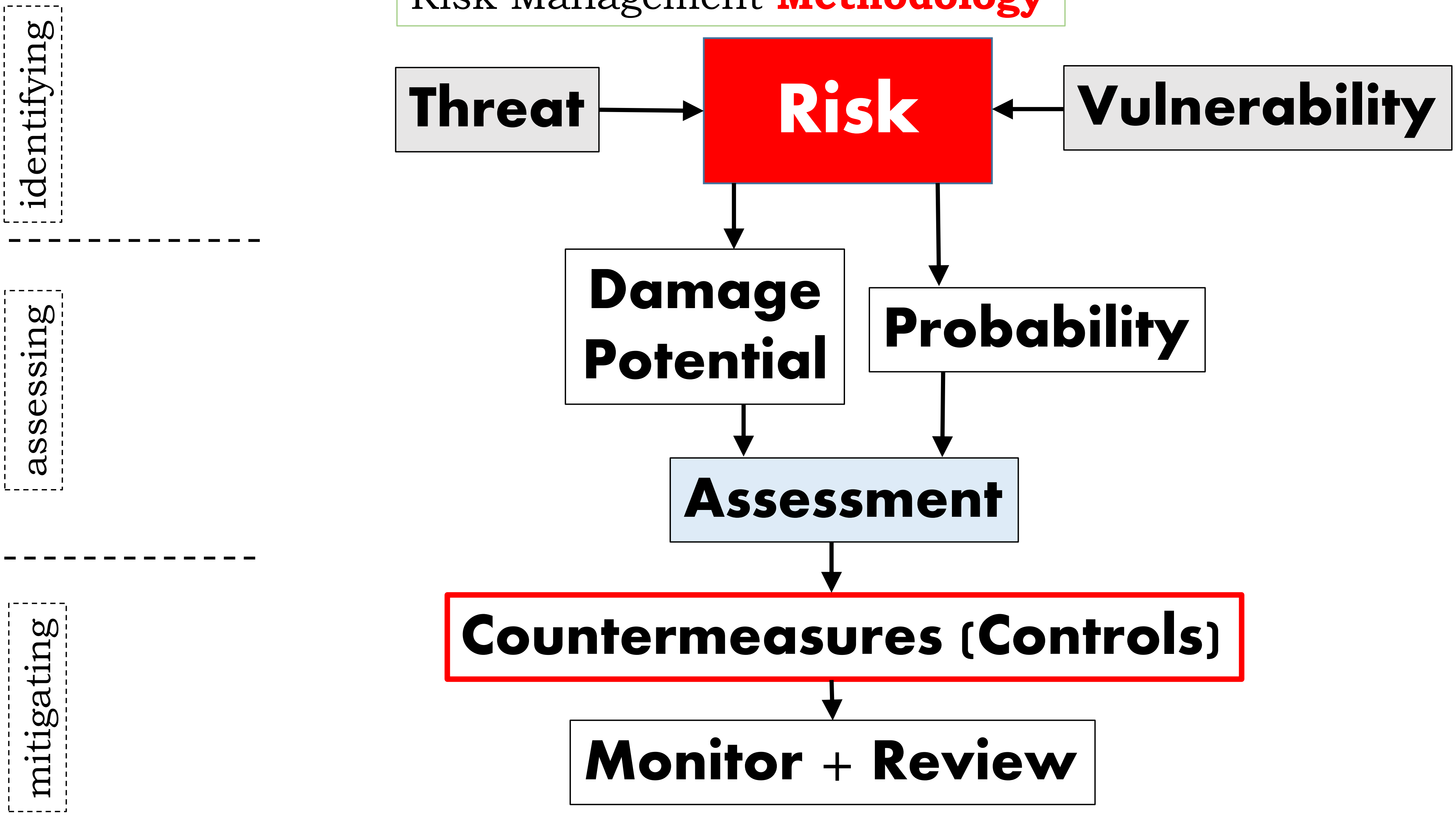
https://www.scienceabc.com



https://www.latimes.com

Risk Management Methodology

Risk Management **Methodology**



Risk Management **Methodology**

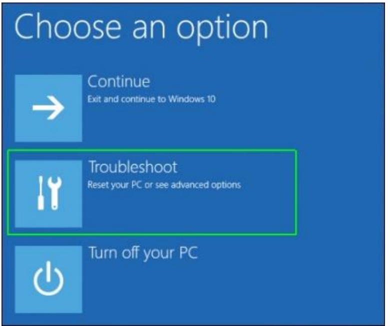
Threat

External **Impact** on our System

Vulnerability

Internal **Weakness** of our System

Network error: Connection refused



Choose an option

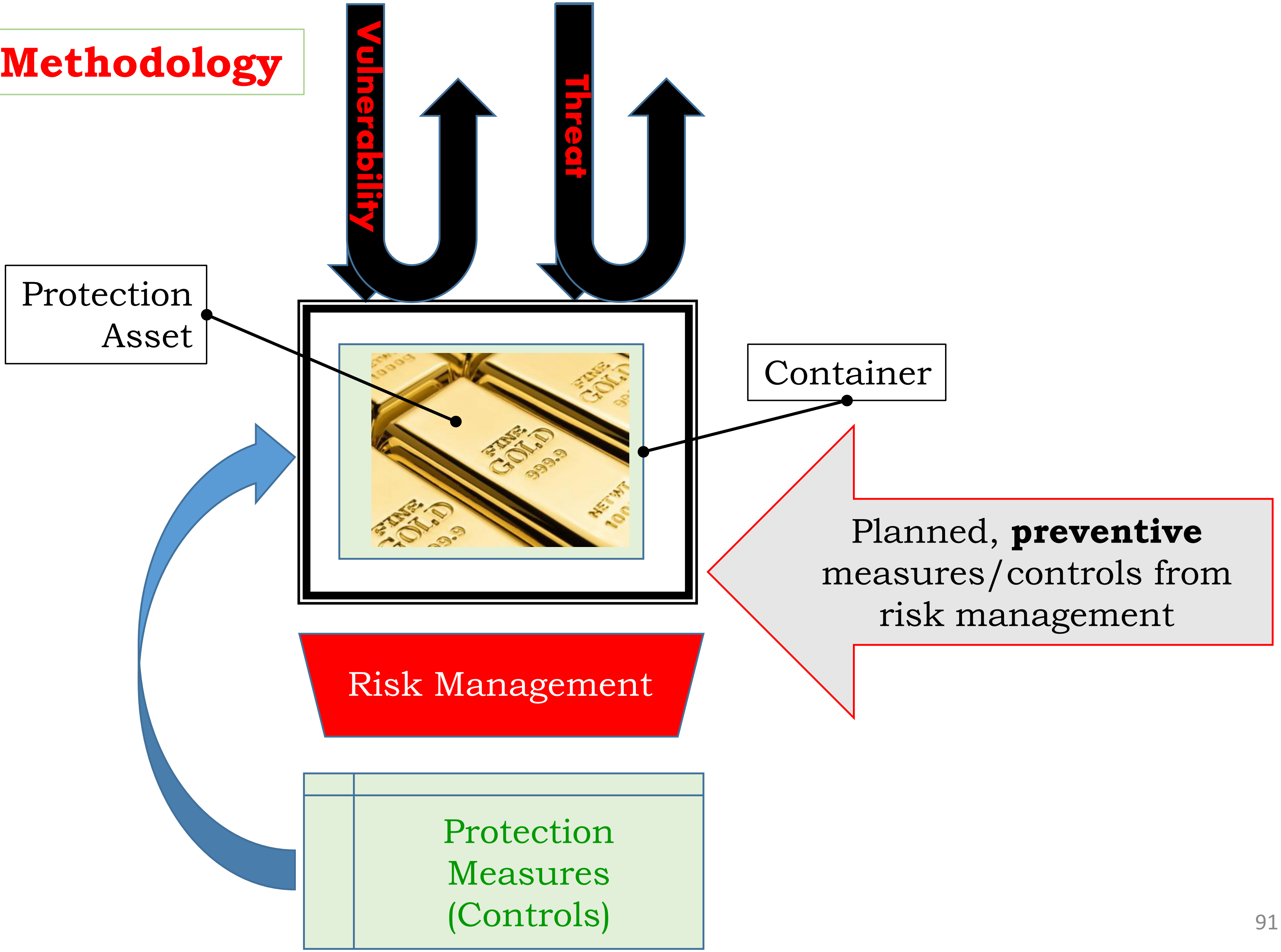
Continue
Exit and continue to Windows 10

Troubleshoot
Reset your PC or see advanced options

Turn off your PC

https://www.youtube.com https://www.netzwelt.de https://www.internetworld.de
https://www.midamericaengine.com http://windowsbulletin.com https://cyware.com https://www.wondershare.com
https://www.darkreading.com

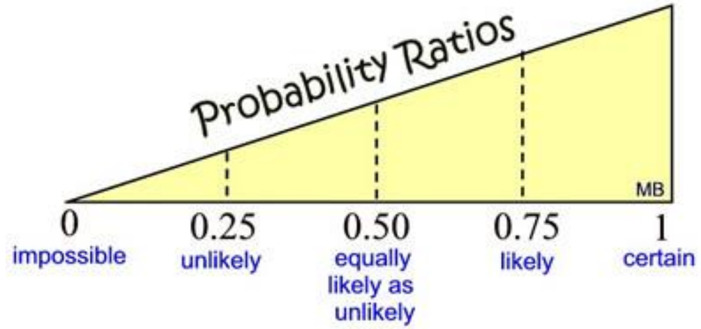
Risk Management **Methodology**


Vulnerability
Threat
Protection Asset
Container
Planned, **preventive** measures/controls from risk management
Risk Management
Protection Measures (Controls)

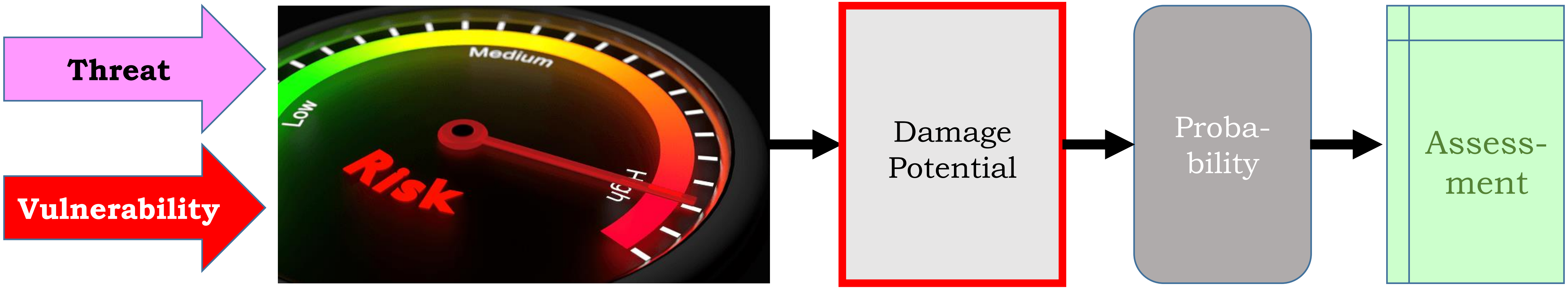
Risk Assessment

How dangerous is the risk?

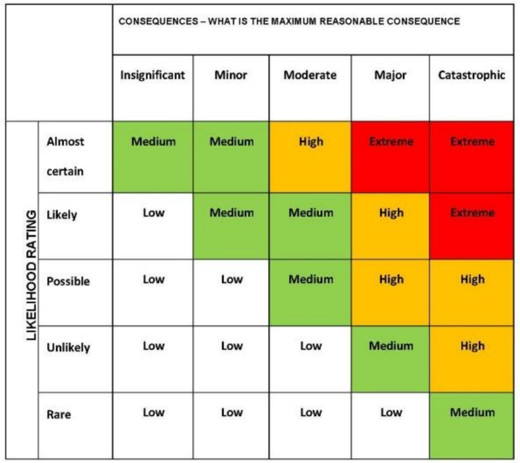
How likely is the risk?



https://mathbitsnotebook.com



https://www.telegraph.co.uk



		CONSEQUENCES – WHAT IS THE MAXIMUM REASONABLE CONSEQUENCE				
		Insignificant	Minor	Moderate	Major	Catastrophic
LIKELIHOOD RATING	Almost certain	Medium	Medium	High	Extreme	Extreme
	Likely	Low	Medium	Medium	High	Extreme
	Possible	Low	Low	Medium	High	High
	Unlikely	Low	Low	Low	Medium	High
	Rare	Low	Low	Low	Low	Medium

https://www.guidelinesforgirlguides.org.au

Risk Management **Methodology**

Threat	**Vulnerability**	**Risk**	**Damage Potential**	**Probability**	**Assessment**
Threat 1	Vulnerability A	Risk R_1	5 (medium)	low	***severe***
Threat 2	Vulnerability B	Risk R_2	1 (very low)	high	***medium***
Threat 3	Vulnerability A	Risk R_3	8 (very high)	very high	***severe***
Threat 4	Vulnerability C	Risk R_4	1	very low	***low***
…	…		…	…	***high***
Malware infusion	Windows Operating System	Information hacking	8 (very high)	high	***high***

Example

Risk Assessment Table

Risk Management **Methodology**

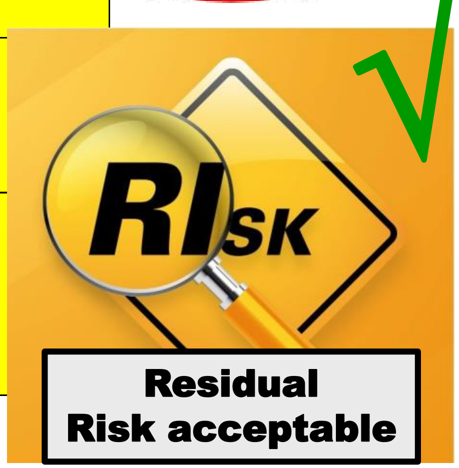
Risk	**Assessment**	**Countermeasures (Controls)**	**Monitoring & Reviewing**
Risk R_1	***severe***	• Countermeasure C_1 • Countermeasure C_2 • …	Method M_4 Periodicity: monthly
Risk R_2	***medium***	• Countermeasure C_7 • Countermeasure C_{13} • …	Method M_{18} Periodicity: monthly
Risk R_3	***severe***	• Countermeasure C_9 • Countermeasure C_{21} • …	Method M_{33} Periodicity: weekly
Risk R_4	***low***	• Countermeasure C_{31} • Countermeasure C_{16} • …	Method M_{19} Periodicity: daily
	high	• Countermeasure C_{15} • Countermeasure C_{33} • …	Method M_{21} Periodicity: yearly
Information hacking	***high***	• *Anti-Virus SW (updated)* • *Intrusion detection SW* • *Regular scans* • *Encrypted data storage*	Full scan Periodicity: daily Updates Periodicity: immediate

Example

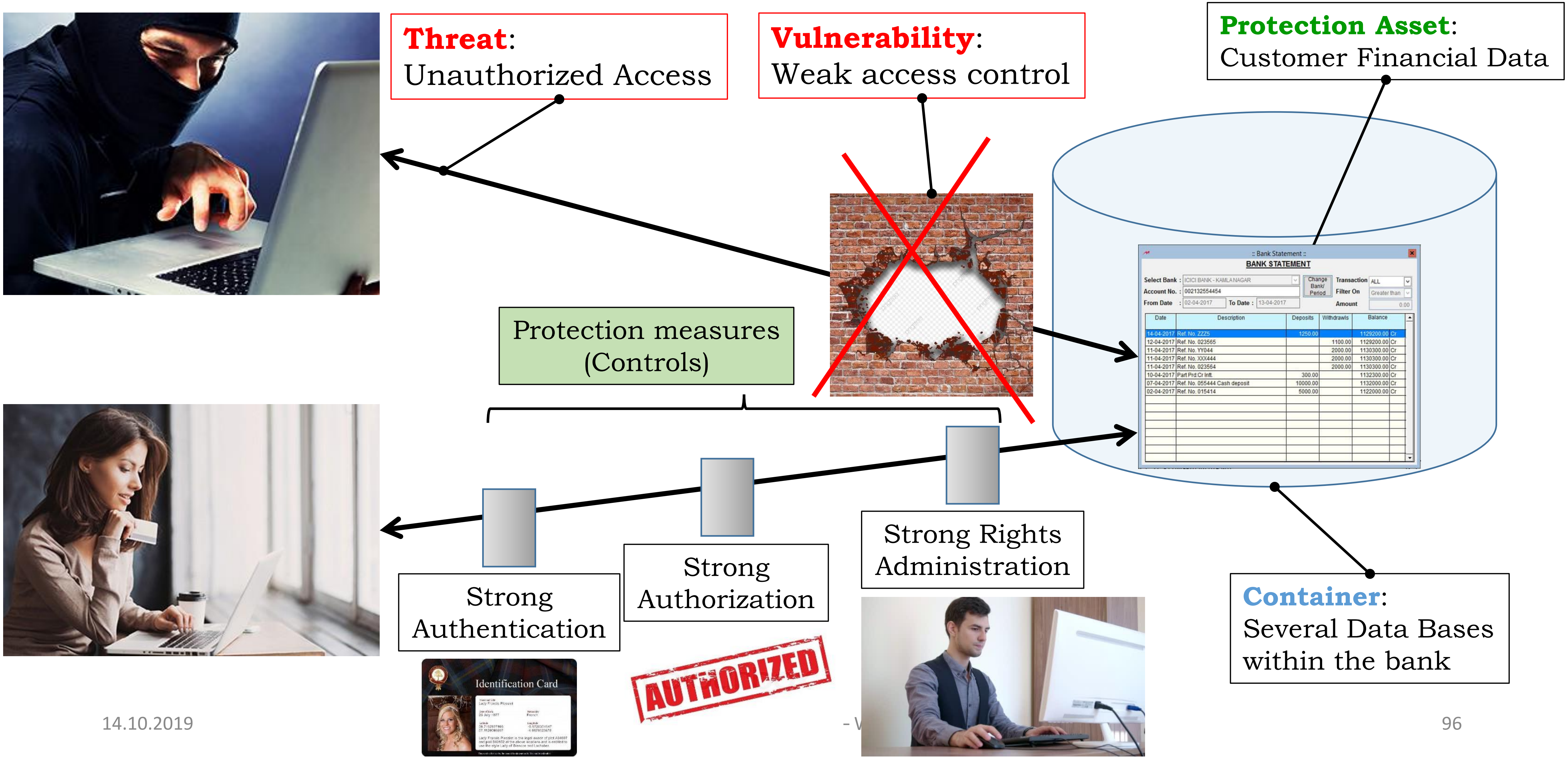
Risk Management **Methodology**

Risk	Assessment	Countermeasures (Controls)	Monitoring & Reviewing	Residual Risk
Risk R_1	***severe***	• Countermeasure C_1 • Countermeasure C_2 • …	Method M_4 Periodicity: monthly	low
Risk R_2	***medium***	• Countermeasure C_7 • Countermeasure C_{13} • …	Method M_{13} Periodicity: monthly	low
Risk R_3	***severe***	• Countermeasure C_9 • Countermeasure C_{21} • Countermeasure C_{30}	Method M_{33} Periodicity: weekly	low
Risk R_4	***low***	• Countermeasure C_{31} • Countermeasure C_{16} • …	Method M_{19} Periodicity: daily	low
	high	• Countermeasure C_{15} • Countermeasure C_{33} • …	Method M_{21} Periodicity: yearly	low
Information hacking	***high***	• *Anti-Virus SW (updated)* • *Intrusion detection SW* • *Regular scans* • *Encrypted data storage*	Full scan Periodicity: daily Updates Periodicity: immediate	low

low



Risk Management Methodology Example: Customer Bank Data Protection



Threat: Unauthorized Access

Vulnerability: Weak access control

Protection Asset: Customer Financial Data

Protection measures (Controls)

Strong Authentication

Strong Authorization

Strong Rights Administration

Container: Several Data Bases within the bank

:: Bank Statement ::

BANK STATEMENT

Select Bank : ICICI BANK - KAMLA NAGAR

Account No. : 002132554454

From Date : 02-04-2017 To Date : 13-04-2017

Change Bank/ Period

Transaction ALL

Filter On Greater than

Amount 0.00

Date	Description	Deposits	Withdrawls	Balance	
14-04-2017	Ref. No. ZZZ5	1250.00		1129200.00	Cr
12-04-2017	Ref. No. 023565		1100.00	1129200.00	Cr
11-04-2017	Ref. No. YY044		2000.00	1130300.00	Cr
11-04-2017	Ref. No. XXX444		2000.00	1130300.00	Cr
11-04-2017	Ref. No. 023564		2000.00	1130300.00	Cr
10-04-2017	Part Prd:Cr Intt.	300.00		1132300.00	Cr
07-04-2017	Ref. No. 055444 Cash deposit	10000.00		1132000.00	Cr
02-04-2017	Ref. No. 015414	5000.00		1122000.00	Cr

https://www.medscape.com

https://www.sunflowerbank.com

https://de.pngtree.com

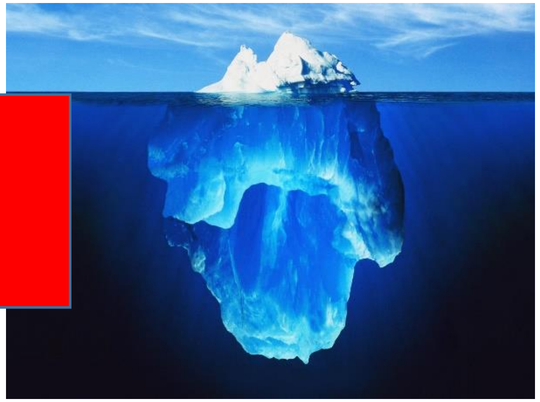
https://www.margcompusoft.com

https://www.fool.com

http://inadinaofset.com

Identified (known) Risks

Hidden (unknown) Risks



http://onthejob.45things.com

- ✓ Mitigation
- ✓ Protection

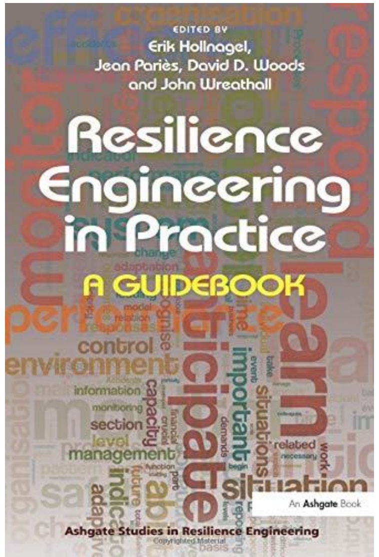
- ✓ Generic Protection Measures

Risk Management Process

Examples:

- ✓ No single points of failure
- ✓ Multiple lines of defense
- ✓ Safe state
- ✓ Graceful degradation
- ✓ …

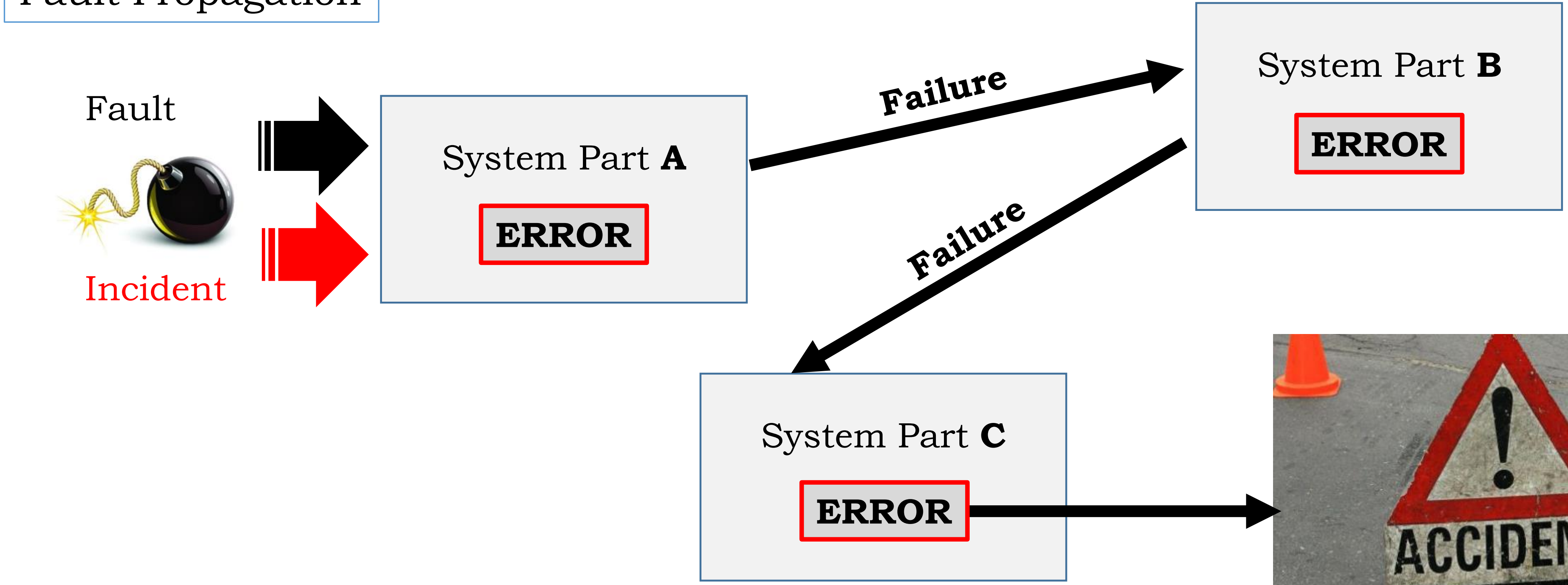
⇒ **Resilience Engineering**



https://www.123rf.com

Unknown Risks: Generic Protection Measures – Fault Containment

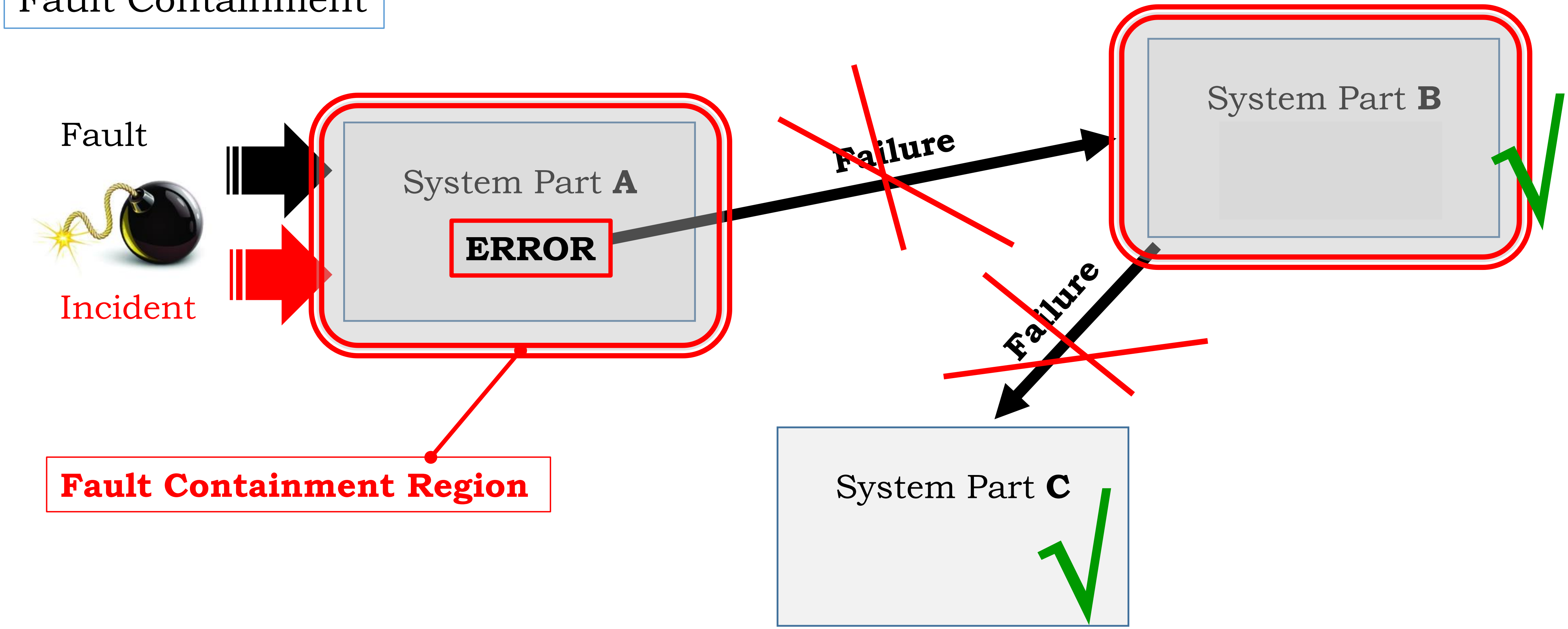
Fault Propagation



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

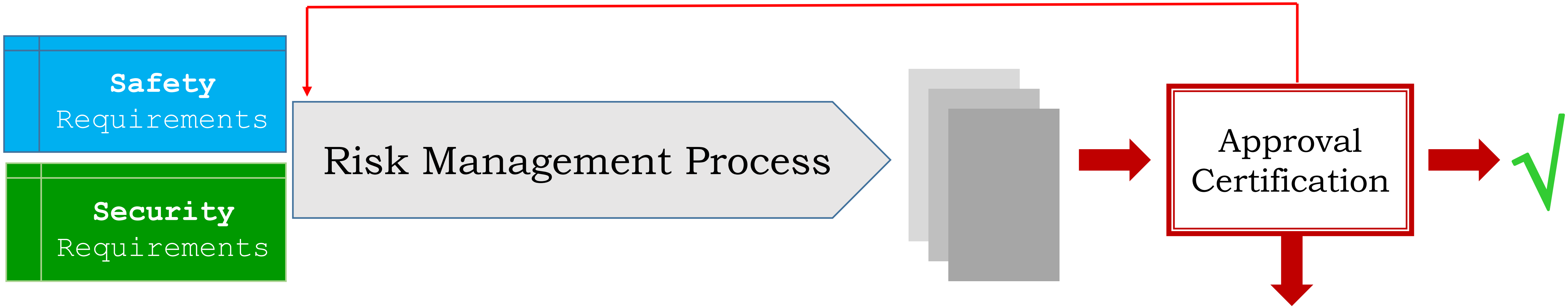
Unknown Risks: Generic Protection Measures – Fault Containment

Fault Containment



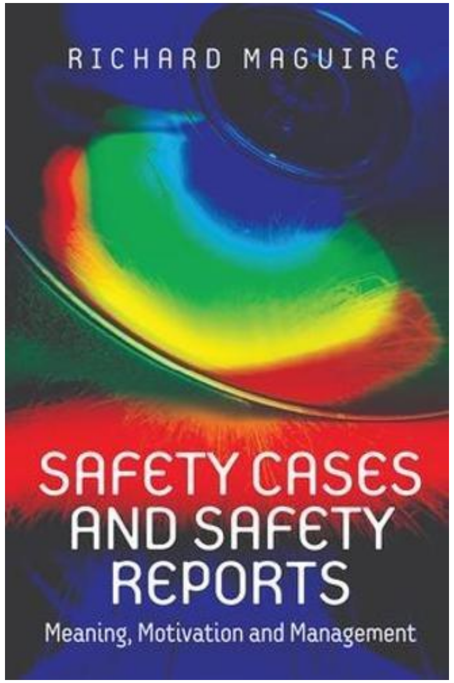
Build **error** propagation boundaries around each system part

Certification: Formal Approval by a legally accredited Authority



Risk Management Report [Safety Case]

https://www.witn.com

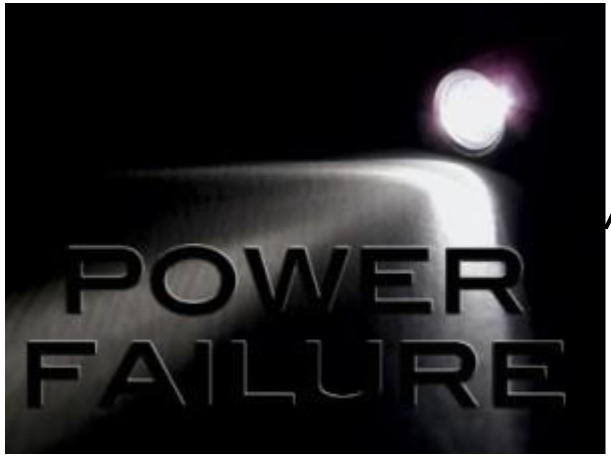

RICHARD MAGUIRE
SAFETY CASES AND SAFETY REPORTS
Meaning, Motivation and Management

Richard Maguire: **Safety Cases and Safety Reports – Meaning, Motivation and Management**
Taylor & Francis Ltd (CRC Press), USA, 2017
ISBN 978-1-138075320

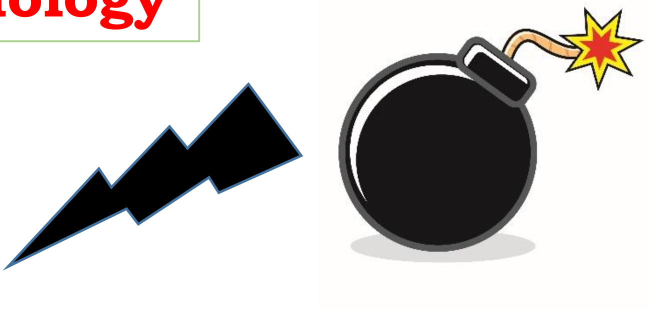
Risk Management **Methodology**

http://marygreeley.com

http://www.datacenterdynamics.com



http://www.bounceenergy.com



Incident Handling

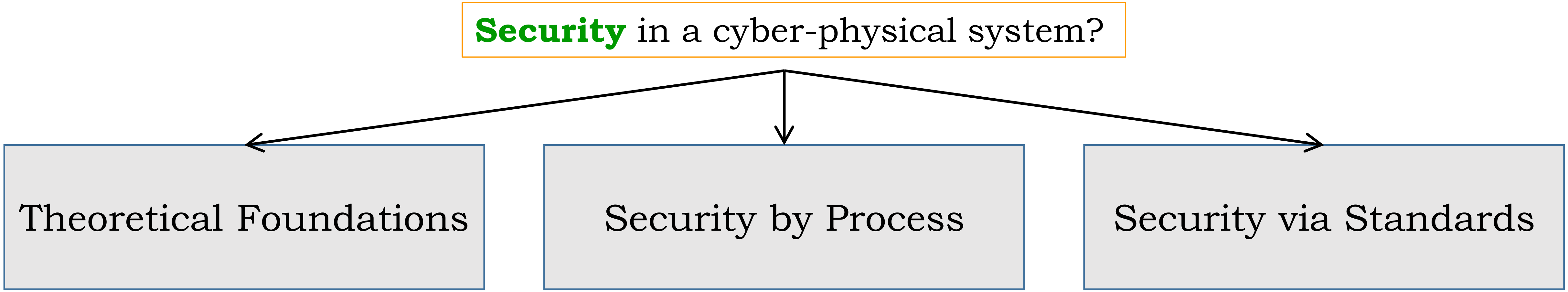
Immediate Response

- preplanned
- automated

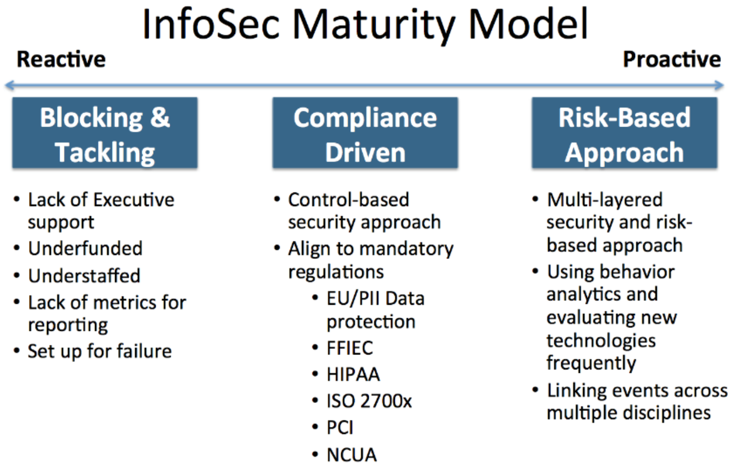
Analysis & Consequences

Last line of defense

Any way you build your system – it will be attacked
⇒ Incident


Security in a cyber-physical system?

- Theoretical Foundations
- Security by Process
- Security via Standards


InfoSec Maturity Model

Reactive — Proactive

Blocking & Tackling

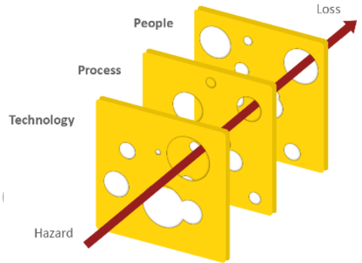
- Lack of Executive support
- Underfunded
- Understaffed
- Lack of metrics for reporting
- Set up for failure

Compliance Driven

- Control-based security approach
- Align to mandatory regulations
  - EU/PII Data protection
  - FFIEC
  - HIPAA
  - ISO 2700x
  - PCI
  - NCUA

Risk-Based Approach

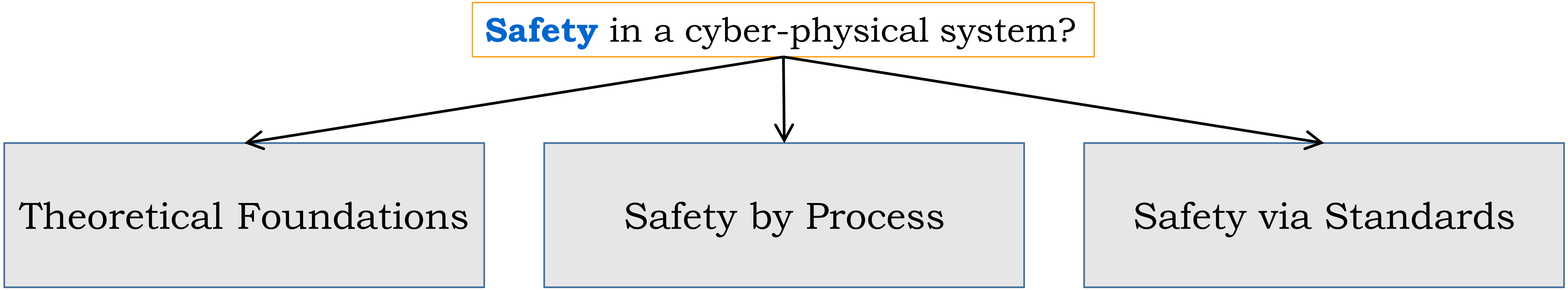
- Multi-layered security and risk-based approach
- Using behavior analytics and evaluating new technologies frequently
- Linking events across multiple disciplines



tumsasedgars/
stockadobe

https://krebsonsecurity.com

https://securityandpeople.com



Safety in a cyber-physical system?

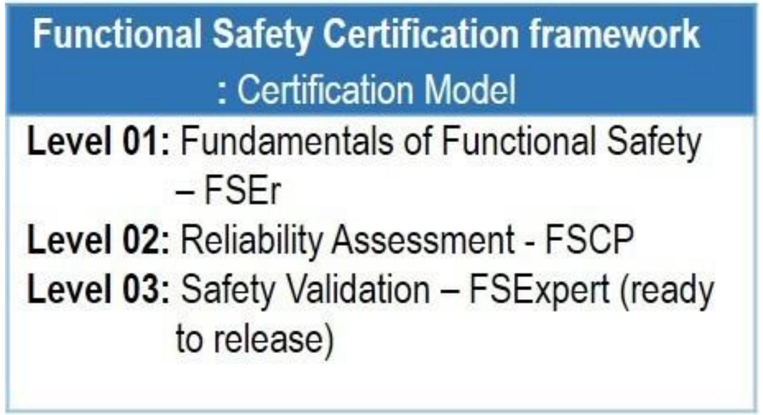
Theoretical Foundations

Safety by Process

Safety via Standards

http://safetyml.com/

https://www.tuv-sud.in

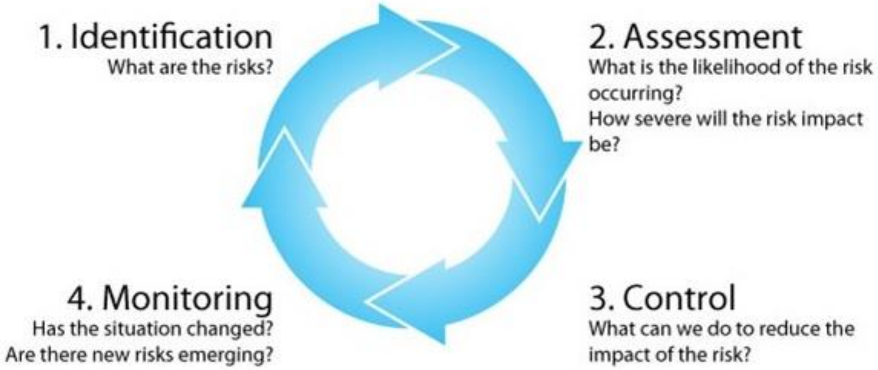


Functional Safety Certification framework : Certification Model

Level 01: Fundamentals of Functional Safety – FSEr

Level 02: Reliability Assessment - FSCP

Level 03: Safety Validation – FSExpert (ready to release)

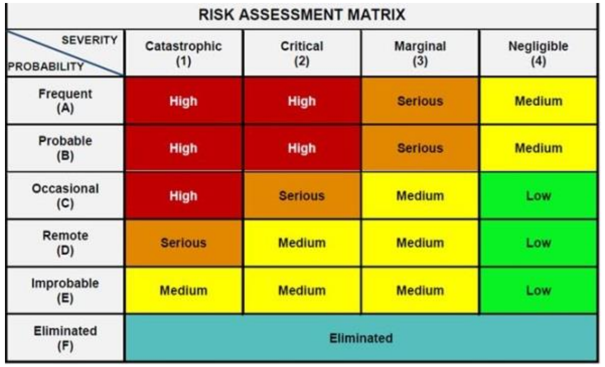


1. Identification
What are the risks?

2. Assessment
What is the likelihood of the risk occurring?
How severe will the risk impact be?

3. Control
What can we do to reduce the impact of the risk?

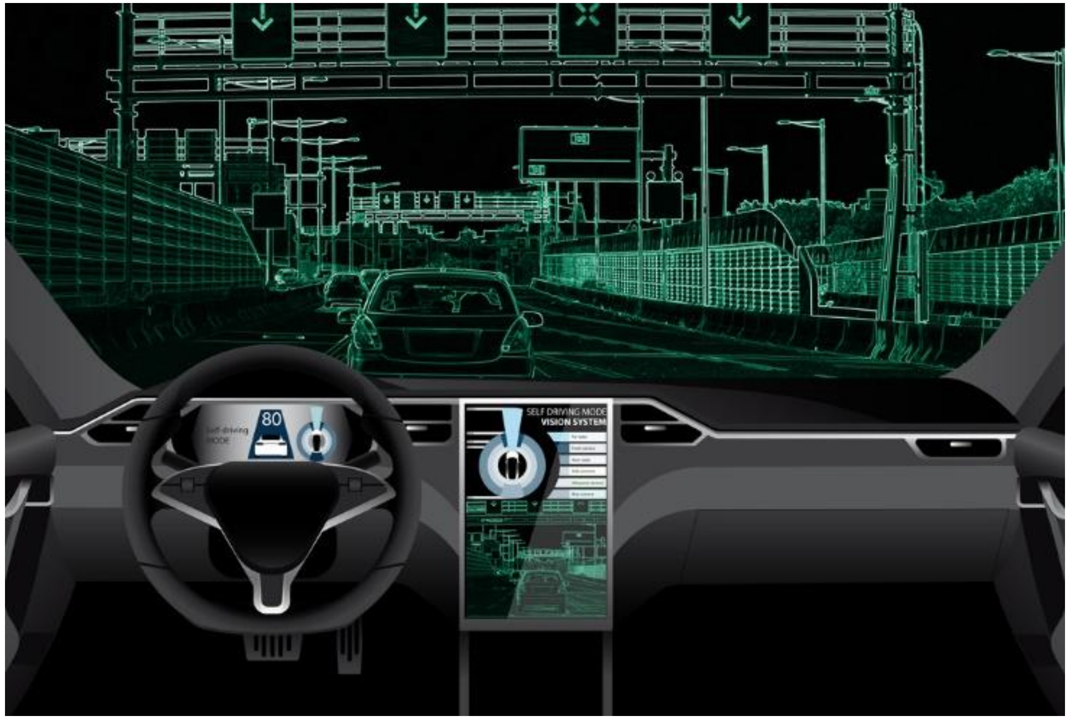
4. Monitoring
Has the situation changed?
Are there new risks emerging?



RISK ASSESSMENT MATRIX

SEVERITY / PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

Engineering Trustworthy Software for Cyber-Physical Systems



Content

- Introduction
- Technology: Cyber-Physical Systems
- Trustworthiness
- Engineering
- Conclusions

TECHNISCHE UNIVERSITÄT DRESDEN

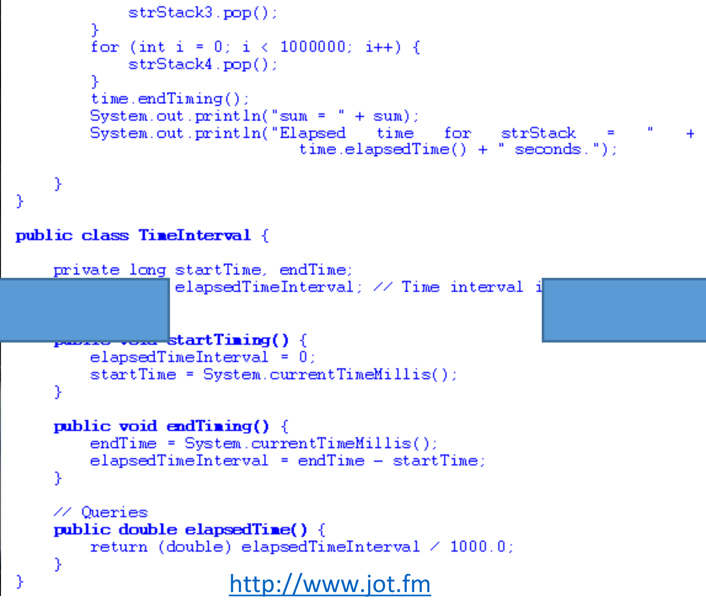
WS19/20: Engineering Trustworthy Software for Cyber-Physical Systems

Cyber-Physical Systems are real-world systems controlled by **software**

SW-errors, faults, vulnerabilities and omissions ⇒ **Risk**

We must build and operate **trustworthy software**

https://www.independent.co.uk



```
            strStack3.pop();
        }
        for (int i = 0; i < 1000000; i++) {
            strStack4.pop();
        }
        time.endTiming();
        System.out.println("sum = " + sum);
        System.out.println("Elapsed   time   for   strStack   =   "   +
                                time.elapsedTime() + " seconds.");

    }
}

public class TimeInterval {

    private long startTime, endTime;
                 elapsedTimeInterval; // Time interval i


    public void startTiming() {
        elapsedTimeInterval = 0;
        startTime = System.currentTimeMillis();
    }

    public void endTiming() {
        endTime = System.currentTimeMillis();
        elapsedTimeInterval = endTime - startTime;
    }

    // Queries
    public double elapsedTime() {
        return (double) elapsedTimeInterval / 1000.0;
    }
}
```

http://www.jot.fm

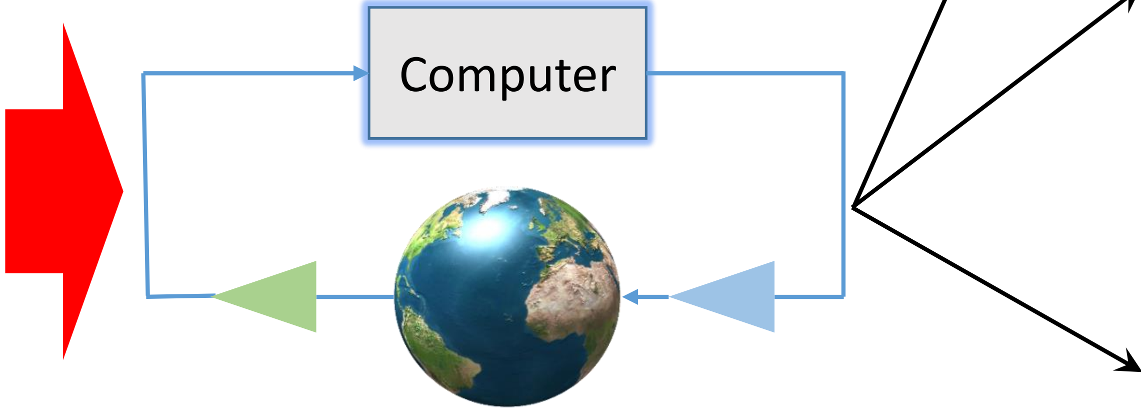
https://keyw.com

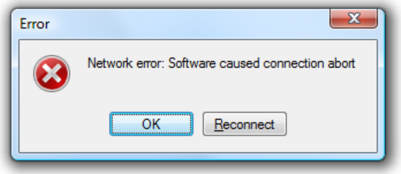
https://en.wikipedia.org

https://www.enisa.europa.eu

Trustworthy Software:
Key Concept = **Risk**

Threats & Vulnerabilities ⇒ Risks

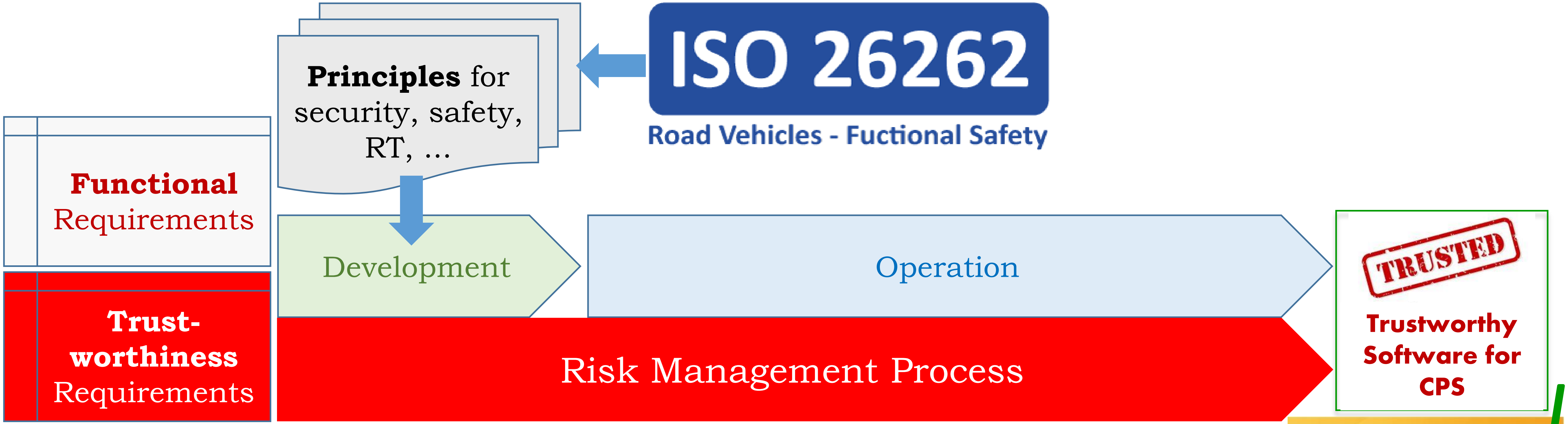



Error

Network error: Software caused connection abort

Key objective of trustworthy systems:

Build and operate the system with a quantified, **acceptable residual risk**


Principles for security, safety, RT, …
ISO 26262
Road Vehicles - Fuctional Safety
Functional Requirements
Trust-worthiness Requirements
Development
Operation
Risk Management Process
TRUSTED
Trustworthy Software for CPS

Identified (known) Risks

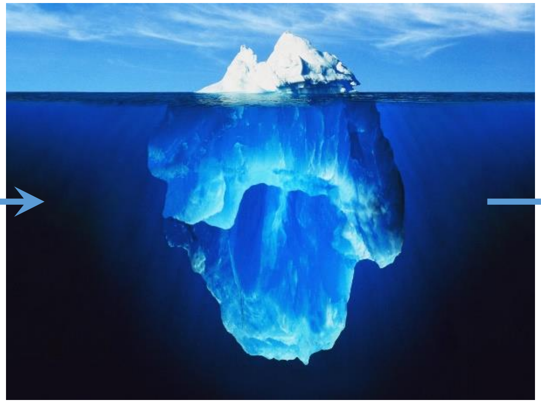
Threat analysis
Vulnerability analysis

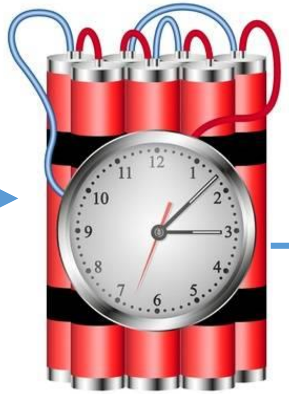
https://www.pinclipart.com

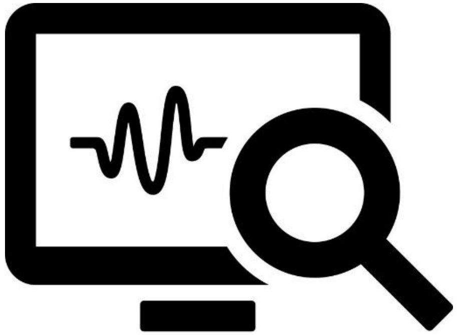
Specific protection Measures (Controls)

Residual Risk acceptable

Hidden (unknown) Risks



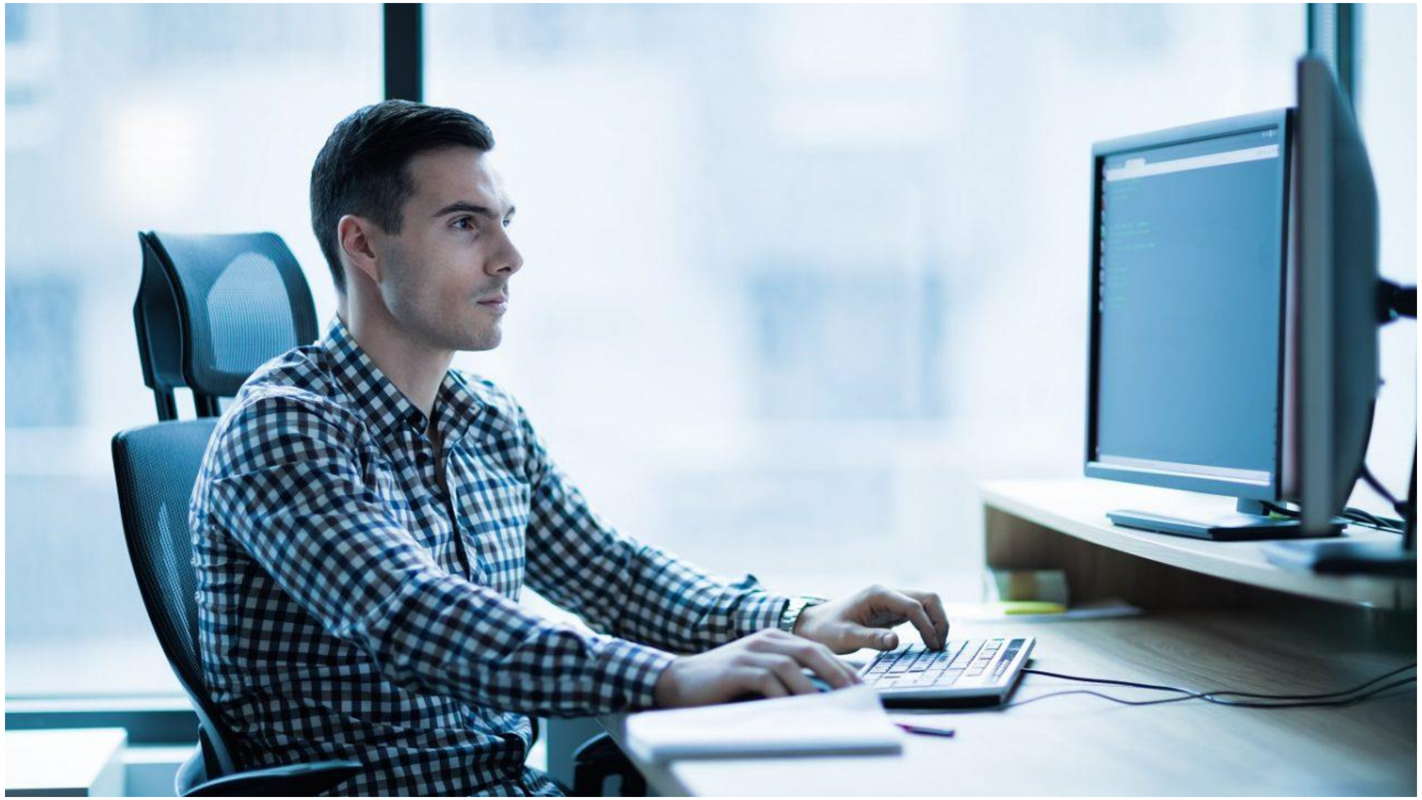




Operational Monitoring

Generic protection Measures (Controls)

http://onthejob.45things.com
https://www.123rf.com



https://www.talentlens.co.uk

Trustworthy systems are the result of knowledgeable, responsible engineering

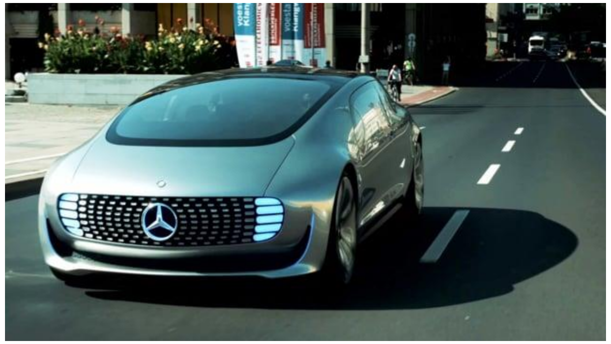
http://www.clker.com

Two interesting professions:

❖ Safety Engineer

❖ Security Engineer

https://www.aviationcv.com



https://vimeo.com

http://www.mikrozol.com

https://www.ness.com

https://www.businessinsider.com

The **safest** airplane cockpit crew is:

https://www.chsmith.com

- A Computer (Autopilot)

The Computer flies the Plane

https://pilotpatrick.com

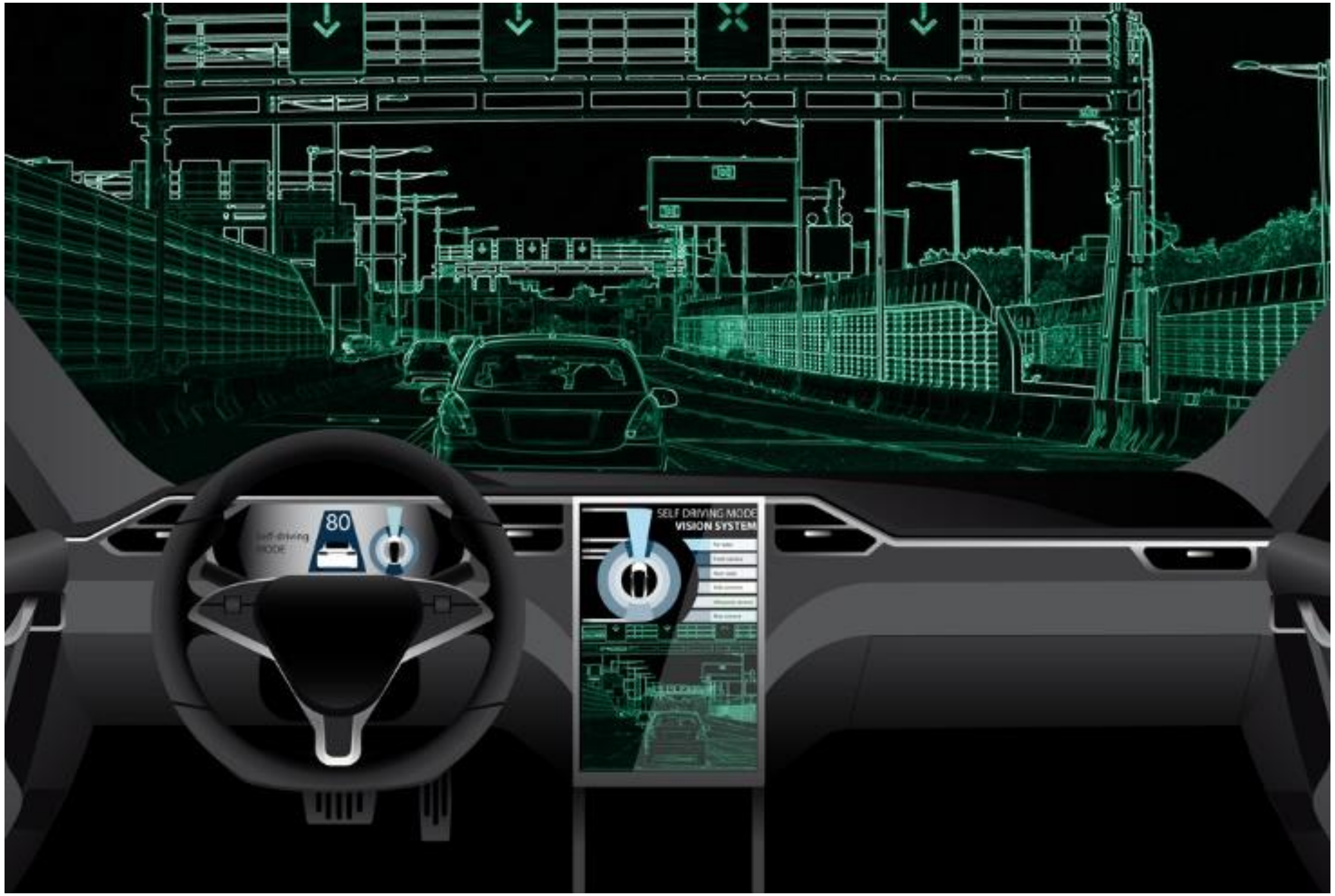
- A Pilot

The Pilot feeds the Dog

https://www.bustle.com

- A Dog

The Dog bites the Pilot if he touches the Computer



Fused sensor vision of a self-driving car

Thank you – Questions please?