

The Quest for Infrastructures and Engineering Methods enabling Highly Dynamic Autonomous Systems

Georg Macher¹, Konrad Diwold³, Omar Veledar², Eric Armengaud², Kay Römer¹

¹ Institute of Technical Informatics, Graz University of Technology

² AVL List GmbH

³ Pro2Future

EuroSPI 2019

Explanatory Note

Vision in Paper is provided by the research context at
Institute of Technical Informatics

- Graz University of Technology
- AVL List GmbH
- Pro2Future Competence Center

Explanatory Note

Vision in Paper is provided by the research group at
Institute of Technical Informatics

- Graz University of Technology
- AVL List
- Pro2Future

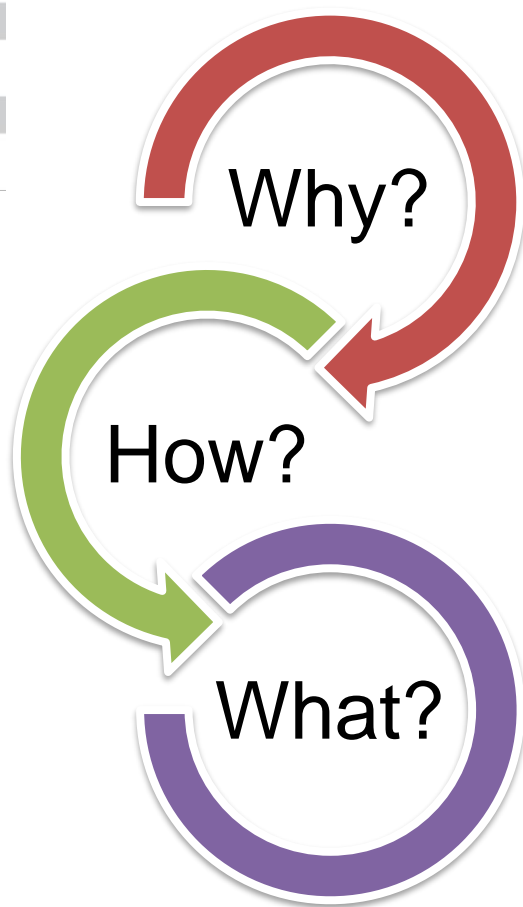


Your perspective on reality may not be wrong.

But that doesn't mean you're the only one
who might have some insight on the truth.



Agenda



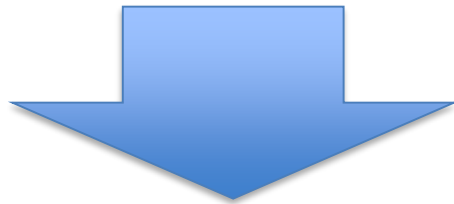
- Why should I care?
- How does this stuff affect me?
- What is the research context?
- What are the future prospects?
- What was this maniac talking about?

Highly Dynamic Autonomous Systems

- Automated Driving Vehicles (ADV)
- Autonomous Robots (AR)

Highly Dynamic Autonomous Systems

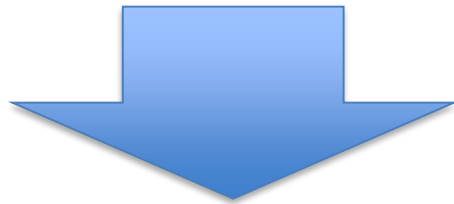
- Automated Driving Vehicles (ADV)
- Autonomous Robots (AR)



- Connected & autonomous things

Highly Dynamic Autonomous Systems

- Automated Driving Vehicles (ADV)
- Autonomous Robots (AR)



- Connected & autonomous things

BRACE YOURSELVES

**THE INTERNET OF THINGS IS
COMING**

Highly Dynamic Autonomous Systems

- Automated Driving Vehicles (ADV)
- Autonomous Robots (AR)



- Connected & autonomous things



- Internet-of-Things

BRACE YOURSELVES



Why should I care?



Maybe because the big players care?



Maybe because the big players care?



SOFTWARE
OFFENSIVE
BAYERN

Altancy
regulatory compliance

n

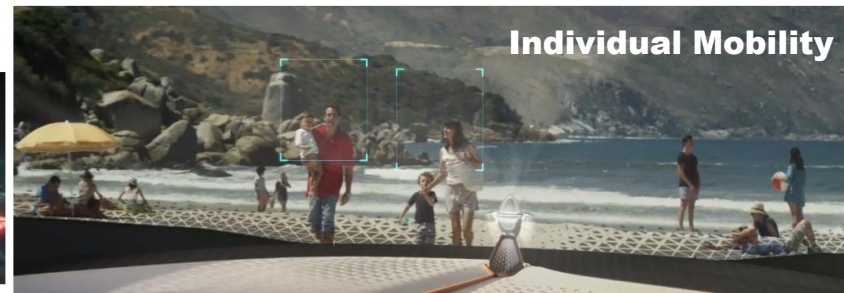
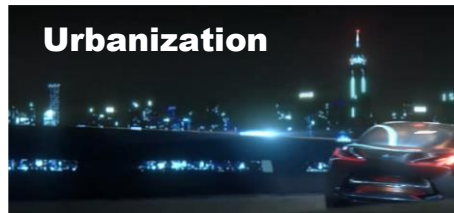
The Automotive (R)Evolution



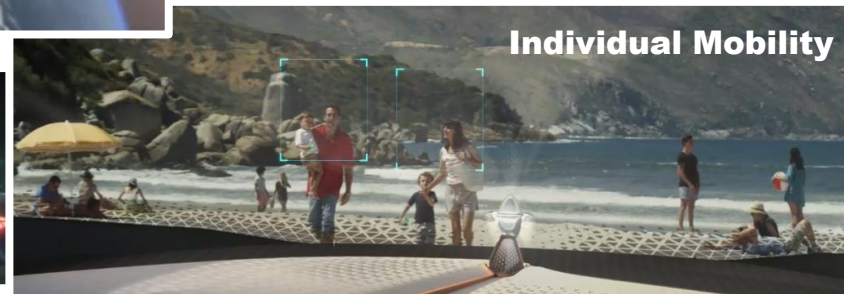
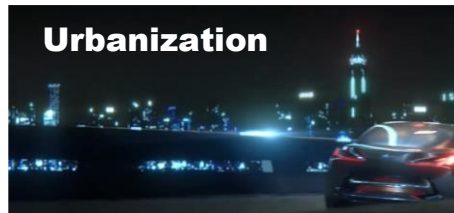
The Automotive (R)Evolution



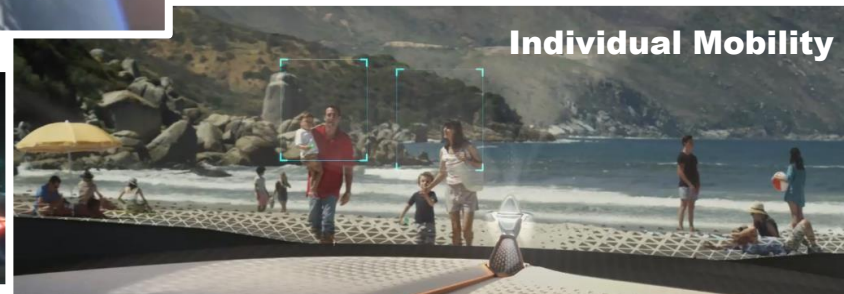
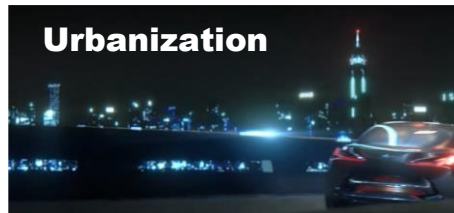
The Automotive (R)Evolution



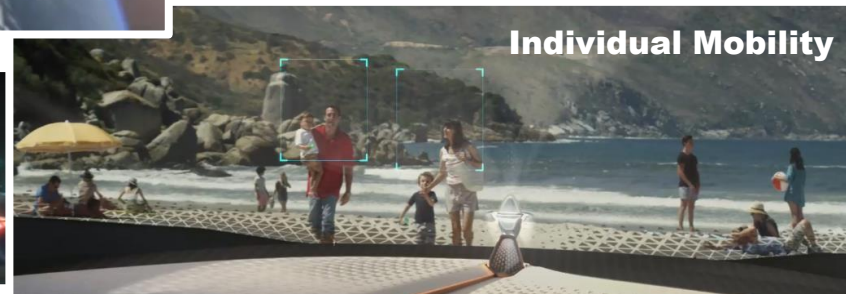
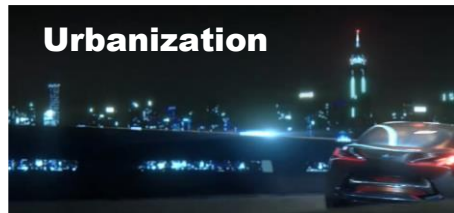
The Automotive (R)Evolution



The Automotive (R)Evolution



The Automotive (R)Evolution



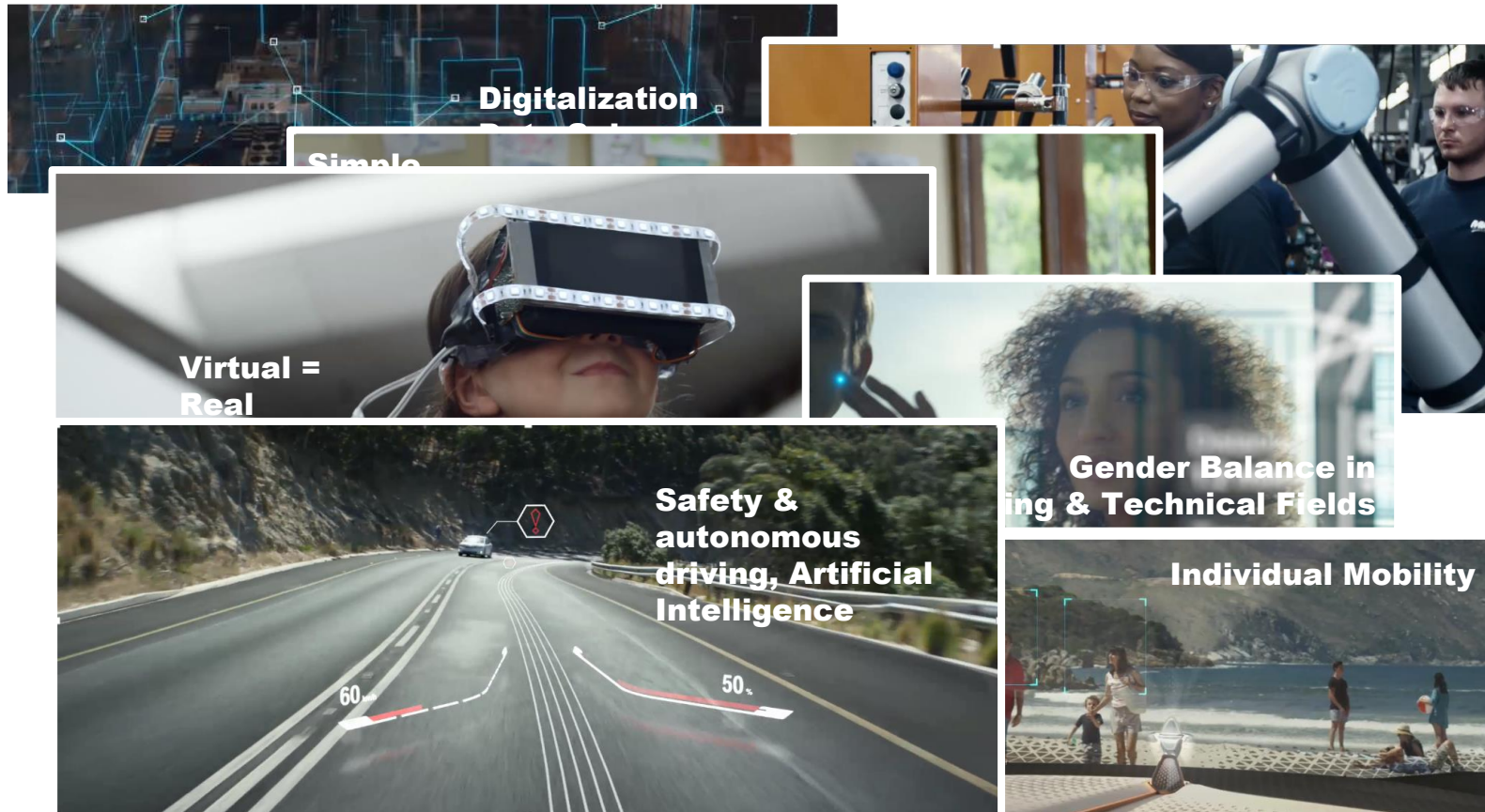
The Automotive (R)Evolution



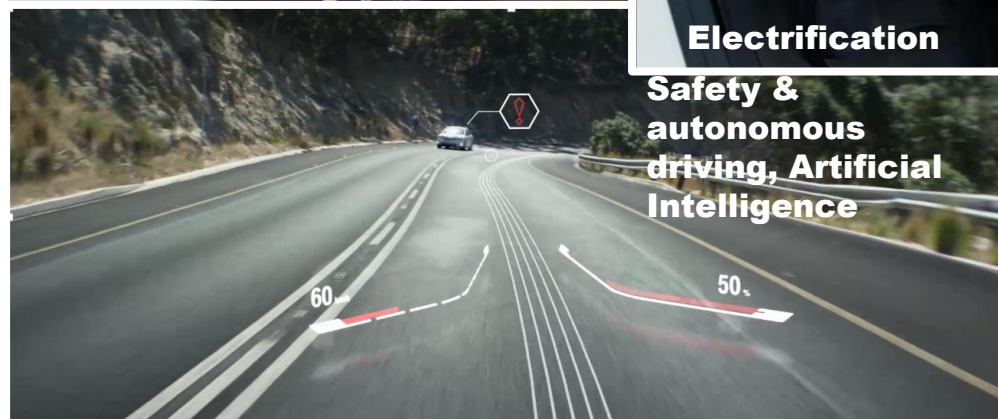
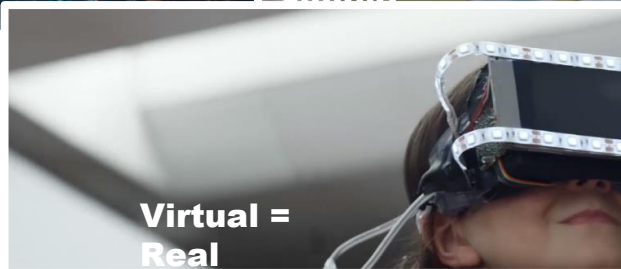
The Automotive (R)Evolution



The Automotive (R)Evolution



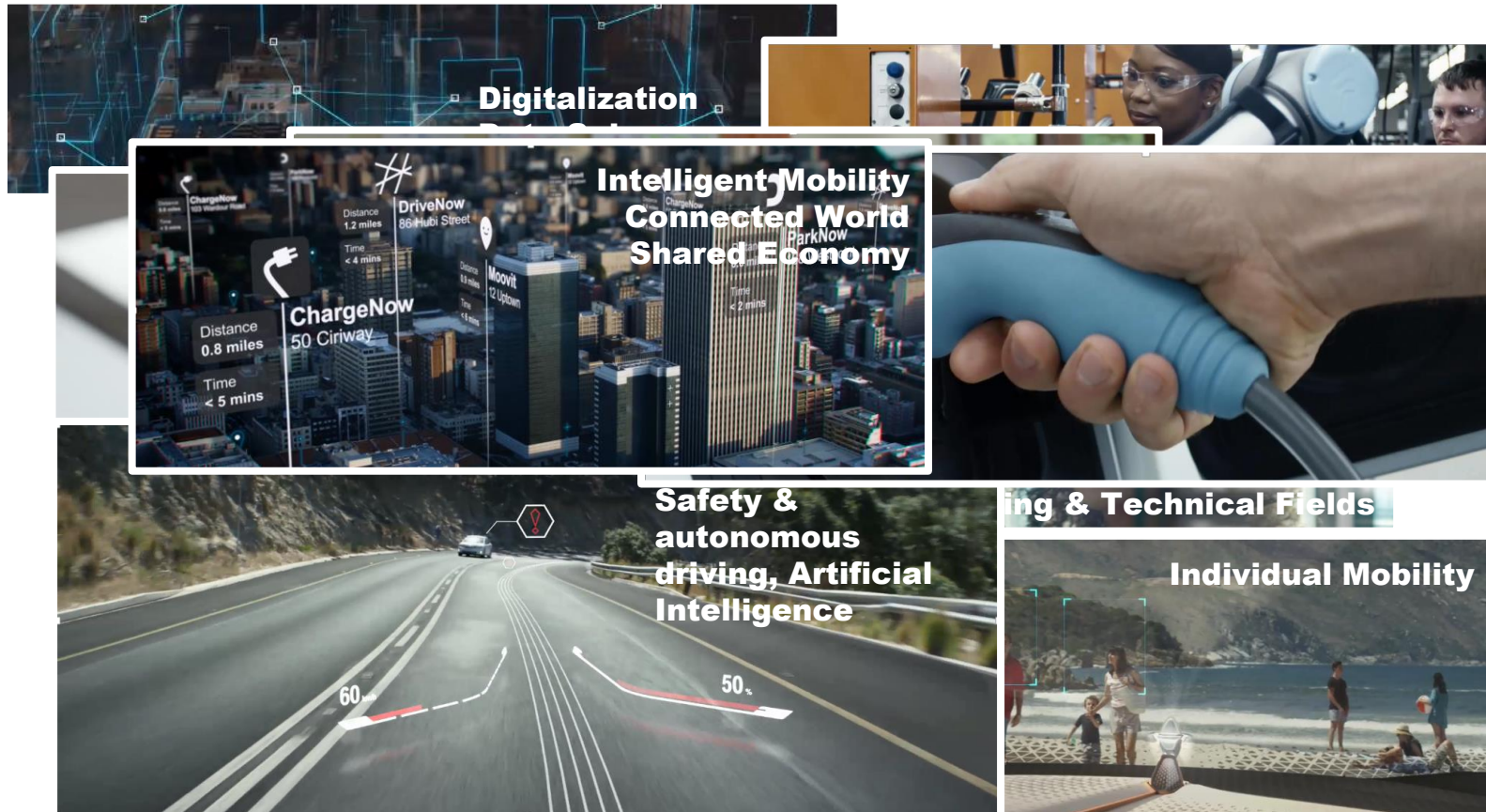
The Automotive (R)Evolution



ing & Technical Fields



The Automotive (R)Evolution



The Automotive (R)Evolution



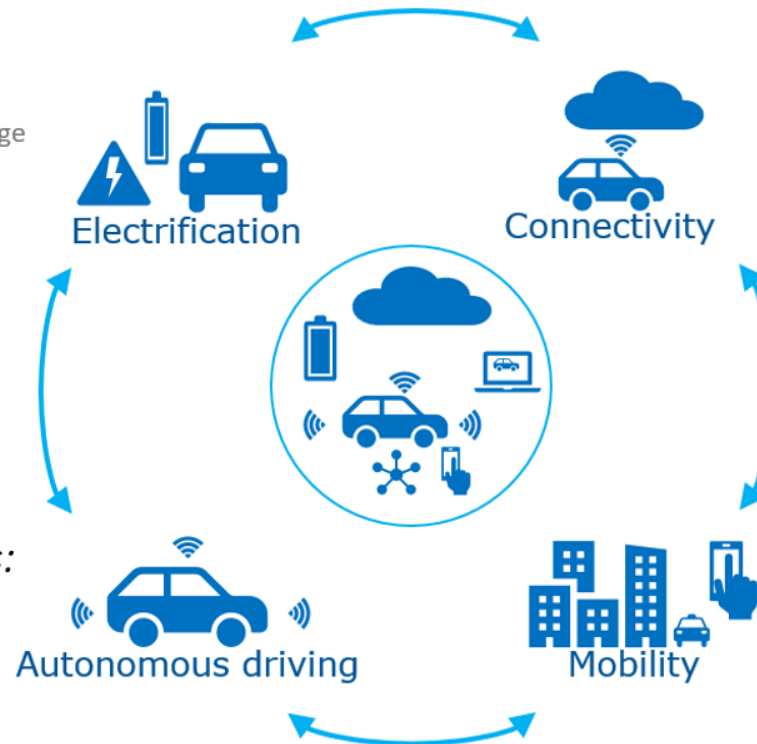
Trends in the Automotive Domain

- CPS → digitalisation
- IoT → connectivity
- Data analytics and AI → knowledge

Technology push:
ICT

Societal challenges:
Legislation

- Reduced pollution
- Reduction of road fatalities
- Increased mobility
- Reduced congestion



Market pull:
evolving consumer needs

- Infotainment & connectivity
- Human-machine interaction
- Customisation
- Mobility as a service

Emergence of data market

85% of executives absolutely or partly agree that the **digital ecosystem will generate higher revenues** than the hardware of the car.

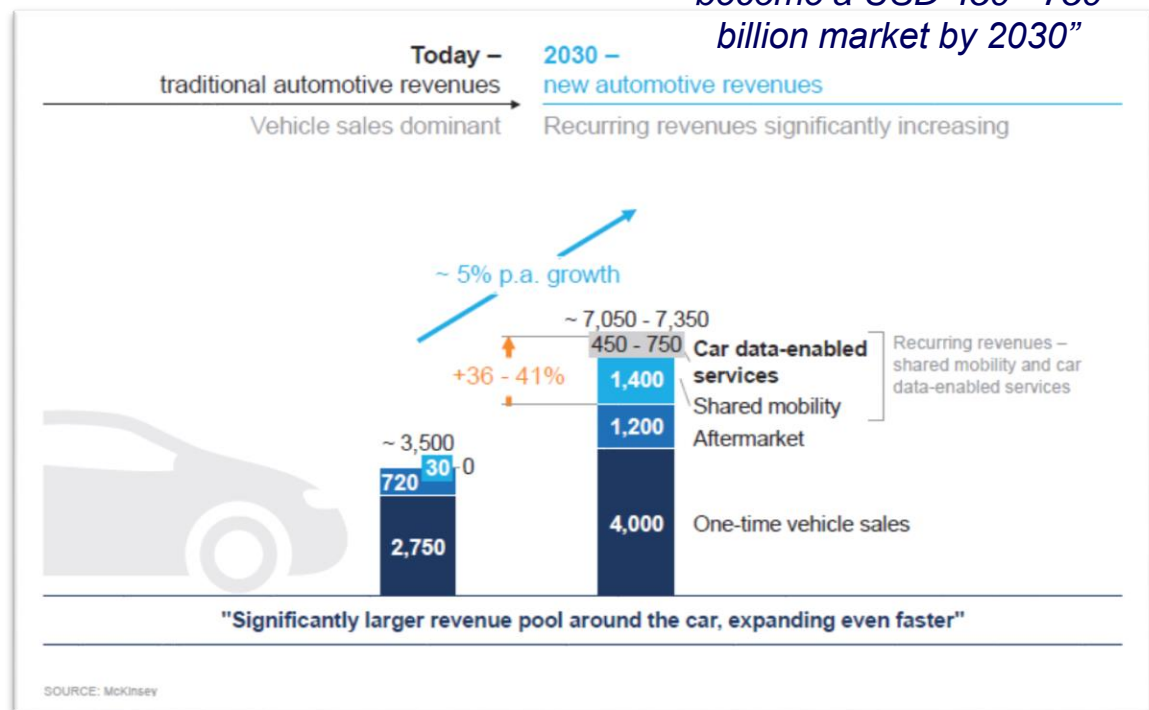
76% absolutely or partly agree that one **connected vehicle generates higher revenue** streams than 10 vehicles which are not connected.

Emergence of data market

85% of executives absolutely or partly agree that the **digital ecosystem will generate higher revenues** than the hardware of the car.

76% absolutely or partly agree that one **connected vehicle generates higher revenue** streams than 10 vehicles which are not connected.

“Car-generated data may become a USD 450 - 750 billion market by 2030”

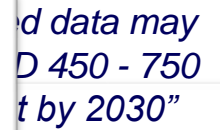


[KPMG, Global Executive Automotive Survey 2017]

[McKinsey, Monetizing Car Data]

85% of executives ab
the **digital ecosystem w**
nues than the hardware o

76% absolutely or partially
connected vehicle gene
streams than 10 vehicles

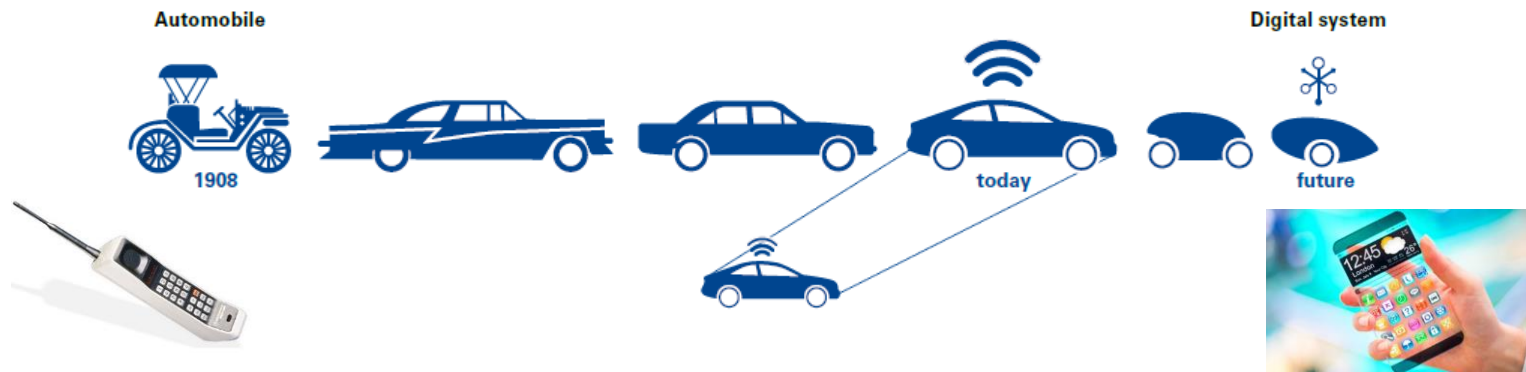


creasing

curing revenues –
ired mobility and car
a-enabled services

ster™

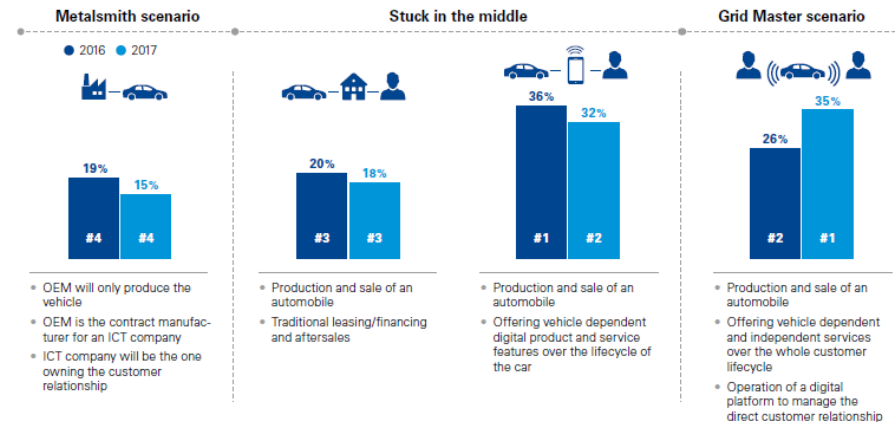
Value creation... and Market (Re)organization



Strong shift of value creation due to digitalization

→ What about the required **competences and skills**?

→ What about the **market organization**?



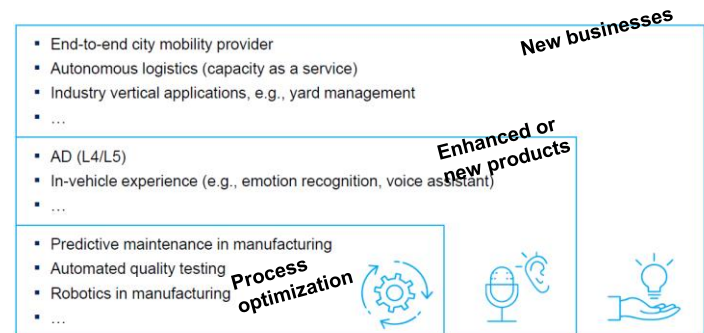
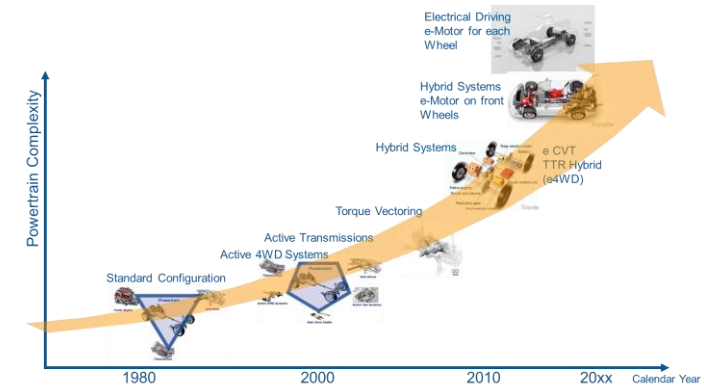
[KPMG, Global Executive Automotive Survey 2017]

ICT as a Key Enabling Technology

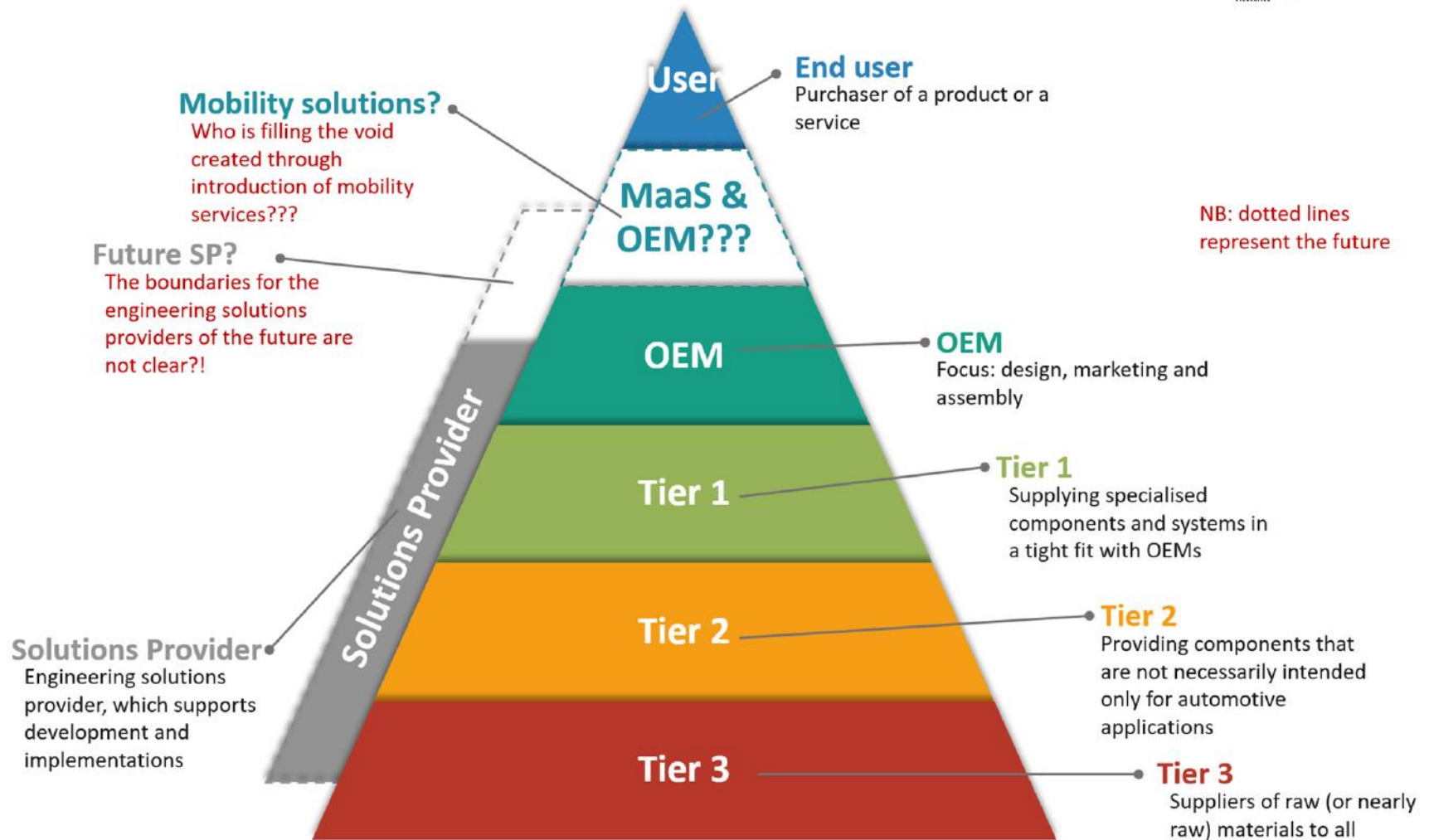
ICT as strong driver for value creation, leading to exponential increase of system complexity

Opportunities for use of ICT in the automotive domain

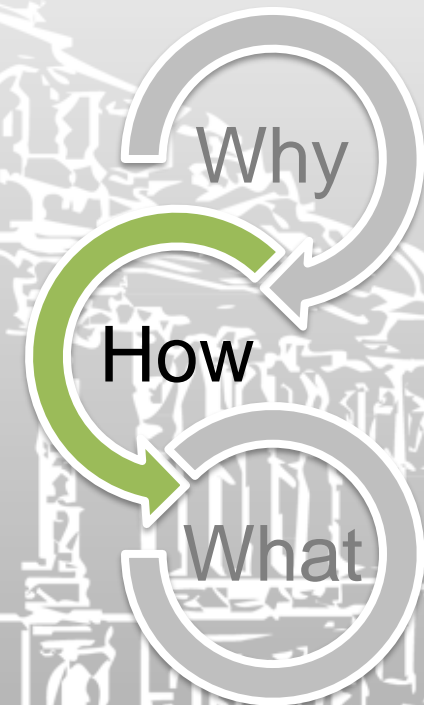
- **Value creation for the end-users** by more intelligent / cognitive / adaptive products
- **Improving development / validation / production efficiency** by more intelligent / cognitive / adaptive development and production environments




New Market Situation



How does this affect me?



Insights from FP9 (Horizon Europe)



Edge 2030 vision

Disclaimer:
This stuff is for internal discussion – nothing decided yet!

The trends

Evolution of **computing architectures** (Heterogeneous, Tensor Processing Units, Quantum processors, ASIC...)
Artificial Intelligence mainstreamed (and powered by big data)
Cyber-security a major concern for any application (and for governments, too)


Long term: synthetic biology, bio-processors, DNA computing

The challenges

No **trust** in Artificial Intelligence and autonomous systems => **ROBOTS STEAL OUR JOBS**
 Too difficult / expensive to develop **dependable, high quality software** => **SW DEVELOPMENT NOT FOR HUMANS**
 No access to **internals of processors** (not built in EU) => **CANNOT GUARANTEE SECURITY**
Energy consumption of computing not sustainable => **BLOCKCHAIN NOT A SILVER BULLET**

e.g. Intel Management Engine or Qualcomm Secure Execution Environment According to one estimate consumes more than 5,0

[Sandro D'Elia, EC, Ecsel Austria conference, April 2018]



Edge 2030 vision

The constraints

Energy / spectrum

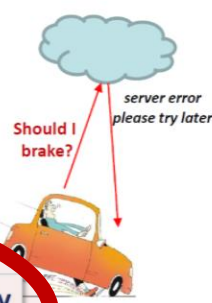

Data transmission is expensive. Mobile data transmission depends on radio spectrum which is a limited resource

Safety / latency / predictability

Autonomous systems cannot rely on cloud-based computing in all situations

Privacy / security

Processing data at the edge, without transmitting and storing it in the cloud, is good for privacy and security (and also for GDPR compliance)

News related to IoT Security



Hackers Remotely
Kill a Jeep on the
Highway—With Me
in It

Wired - 21.07.2015

News related to IoT Security



BBC

Sign in

News

Sport

Reel

Worklife

Travel

Future

NEWS

Home

Video

World

UK

Business

Tech

Science

Stories

Entertainment & Arts

Technology

Twitter CEO and co-founder Jack Dorsey has account hacked



Dave Lee

North America technology reporter

🕒 31 August 2019



🔗 Share

News related to IoT Security



BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

FROM RUSSIA WITH LOVE —

VPNFilter malware infecting 500,000 devices is worse than we thought

Malware tied to Russia can attack connected computers and downgrade HTTPS.

DAN GOODIN - 6/6/2018, 3:00 PM

Twitter CEO and co-founder Jack Dorsey has account hacked



Dave Lee

North America technology reporter

🕒 31 August 2019



🔗 Share

News related to IoT Security

ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

TechRepublic.

SEARCH



Developer Top DaaS providers Security More ▾

Amazon Echo randomly recorded and sent a Portland couple's conversation

A Portland couple claimed that their [Amazon Echo smart speaker recorded a conversation and transmitted it](#) to someone in their contact list—an employee of the couple—in Seattle. The original report is suspect, though [Amazon confirmed to CNET that the incident occurred as described](#).

The model of the Echo Dot photographed in the original report is capable of outputting sound to an external speaker through a 3.5mm audio cable. If a speaker was attached to the Echo Dot, but turned off, the microphone in the Echo Dot unit would still be active, though it would have been impossible for the owners to hear an audio prompt through the speaker. The original report fails to mention this possibility, likewise, the report fails to correctly identify the device as an Amazon Echo.



🕒 31 August 2019



News related to IoT Security

CyberDB
The Cyber Research Databank

ABOUT

DATABASE

PURCHASE

CARS GAMING & CULTURE

5 providers Security More ▾

couple's

ded a conversation and
e-in Seattle. The original
occurred as described.

of outputting sound to an
ed to the Echo Dot, but
ugh it would have been
. The original report fails
ne device as an Amazon

Top 10 Sectors Breached

(Ordered by Number of Identities Exposed)

Rank	Sector	Number of Identities Exposed	Percentage of Identities Exposed
1	Retail	205,446,276	59%
2	Financial	79,465,597	23%
3	Computer Software	35,068,405	10%
4	Healthcare	7,230,517	2%
5	Gov. and Public Sector	7,127,263	2%
6	Social Networking	4,600,000	1%
7	Telecom	2,124,021	.6%
8	Hospitality	1,818,600	.5%
9	Education	1,359,190	.4%
10	Arts and Media	1,082,690	.3%

Source: Symantec



B B

NE

Home

Techr

Tw
has



🕒 31 August 2019



Share

News related to IoT Security

**BUSINESS
NEWS DAILY**
Small Business Solutions & Inspiration

START
Your Business

GROW
Your Business

BUILD
Your Career

LEAD
Your Team

FIND
A Solution



SALES & MARKETING

FINANCES

YOUR TEAM

TECHNOLOGY

SOCIAL MEDIA

SECURITY

B

Product and service reviews are conducted independently by our editorial team, but we sometimes make money when you click on link

N

Home

[Grow Your Business](#) » [Technology](#)

The Security of Connected Medical Devices

Tec

By Adam C. Uzialko, Writer | [May 10, 2019](#) 07:00 am EST

0 0 0

**Tv
ha**



31

- The **healthcare industry is very vulnerable to cyberattack.**
- The most **common types of threats are ransomware, malware, data breaches, DDoS** and cryptojacking.
- Patient care and safety, data loss, and damage to a healthcare provider's reputation are among the consequences of networks being attacked.
- To stop cyberattacks on medical devices, you need to monitor and segment devices, keep software updated, and implement a response plan to an attack.



News related to IoT Security

BUSINESS

Uber confirms that massic global data breach impacted 2.7 million UK customers and drivers

Posted 30th November

THOUGHT LEADERSHIP

Ride-hailing service Uber has confirmed that as many as 2.7 million people in the UK were impacted by a 2016 hacking incident that the company hid from regulators for over a year.

Tec

By Adam C. Uzialko, Writer | May 10, 2019 07:00 am EST

f 0 t 0 in 0

Tv
ha

- The healthcare industry is very vulnerable to cyberattack.
- The most common types of threats are ransomware, malware, data breaches, DDoS and cryptojacking.
- Patient care and safety, data loss, and damage to a healthcare provider's reputation are among the consequences of networks being attacked.
- To stop cyberattacks on medical devices, you need to monitor and segment devices, keep software updated, and implement a response plan to an attack.



31

News related to IoT Security

BUSINESS

Uber confirms that massic global data breach impacted 2.7 million UK customers and drivers

[MORE](#)
[AUDIO](#)
FBI

AUDIO


[Twitter](#)

[Facebook](#)

[Email](#)

Te Inside the FBI: Internet-Connected Toys Pose Security Risks

Tv
ha

- The most **common types of threats** are ransomware, malware, data breaches, DDoS and cryptojacking.
- Patient care and safety, data loss, and damage to a healthcare provider's reputation are among the consequences of networks being attacked.
- To stop cyberattacks on medical devices, you need to monitor and segment devices, keep software updated, and implement a response plan to an attack.



31



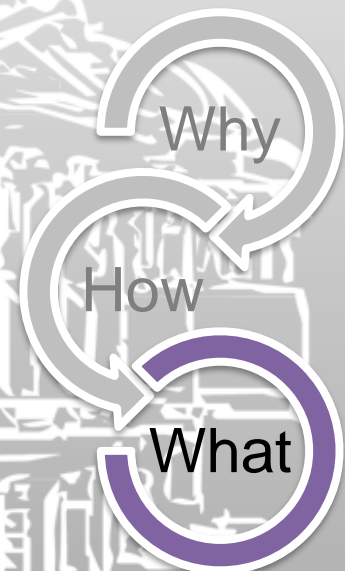
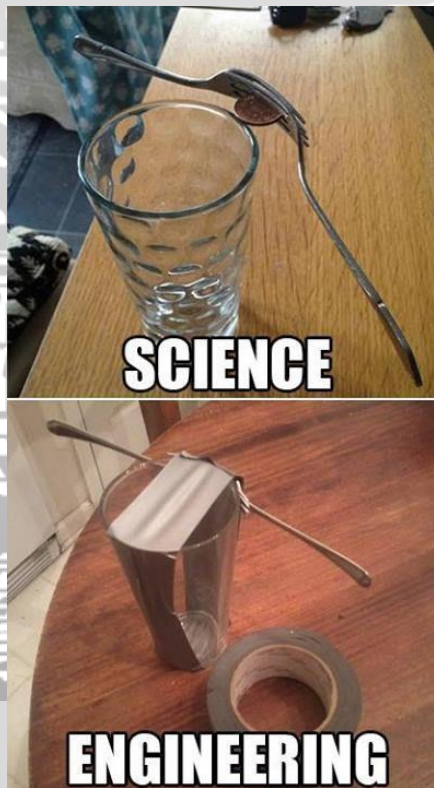




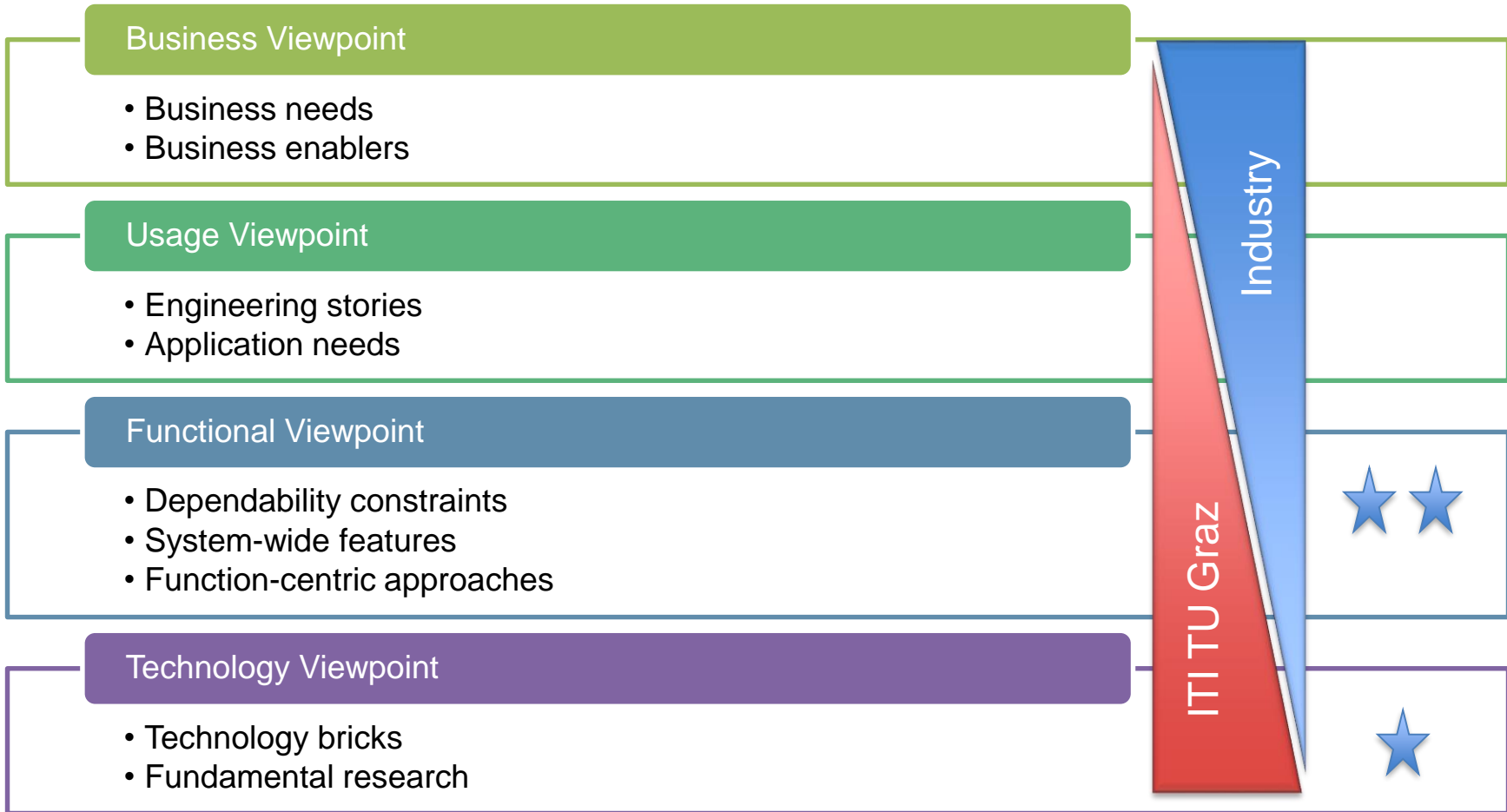
So What!?

What is the research context?

What are the future prospects?

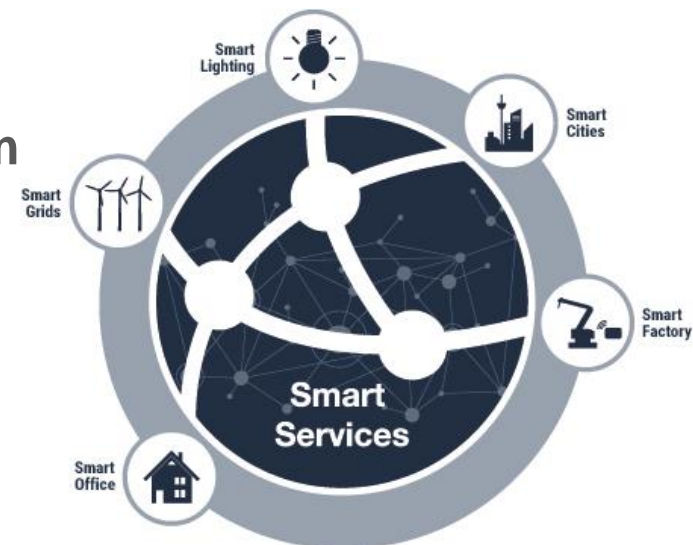


Industrial Cooperation – I3 Viewpoint



ITI Research Groups

- Embedded Automotive Systems
 - Real-Time Operating Systems
 - Multi-Core Architectures
- Hardware/Software Co-Design
 - Semiconductor HW/SW co-design
 - Power awareness
- Industrial Informatics
 - **Safety & security of industrial system**
 - **Resilience in IIoT**
- Networked Embedded Systems
 - Low-power wireless networking
- Smart Services
 - Service oriented architectures



Pro²Future Competence Centre on Products and Production Systems of the Future

<http://www.pro2future.at>

Focus: Development of industrial ICT systems, to facilitate cognitive products and production systems.

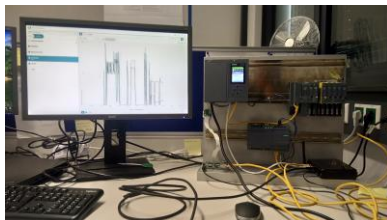
Structure: 5 Research-groups (Areas) at 3 locations (Graz, Steyr und Linz)

Area 1 (Persuasive Computing), Area 2 (Robotics), Area 3 (Analytics), Area 4.1 (Cognitive Products), Area 4.2 (Cognitive Production Systems)

Area 4.1 Cognitive Products

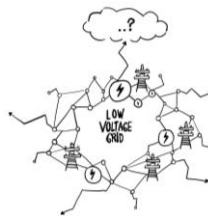
Lead: Kay Römer; Manager: Konrad Diwold; Nr. of Researcher: 4

Area Focus: Dependable Sensor-, ICT-, and Software solutions for cognitive products



Intelligent fail-safe concepts

SIEMENS



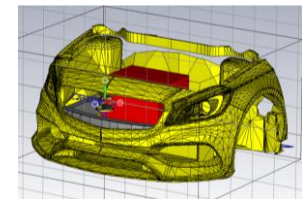
Dependable smart grid communication

SIEMENS



Data-driven process optimization

AVL



Wireless in-car communication

AVL

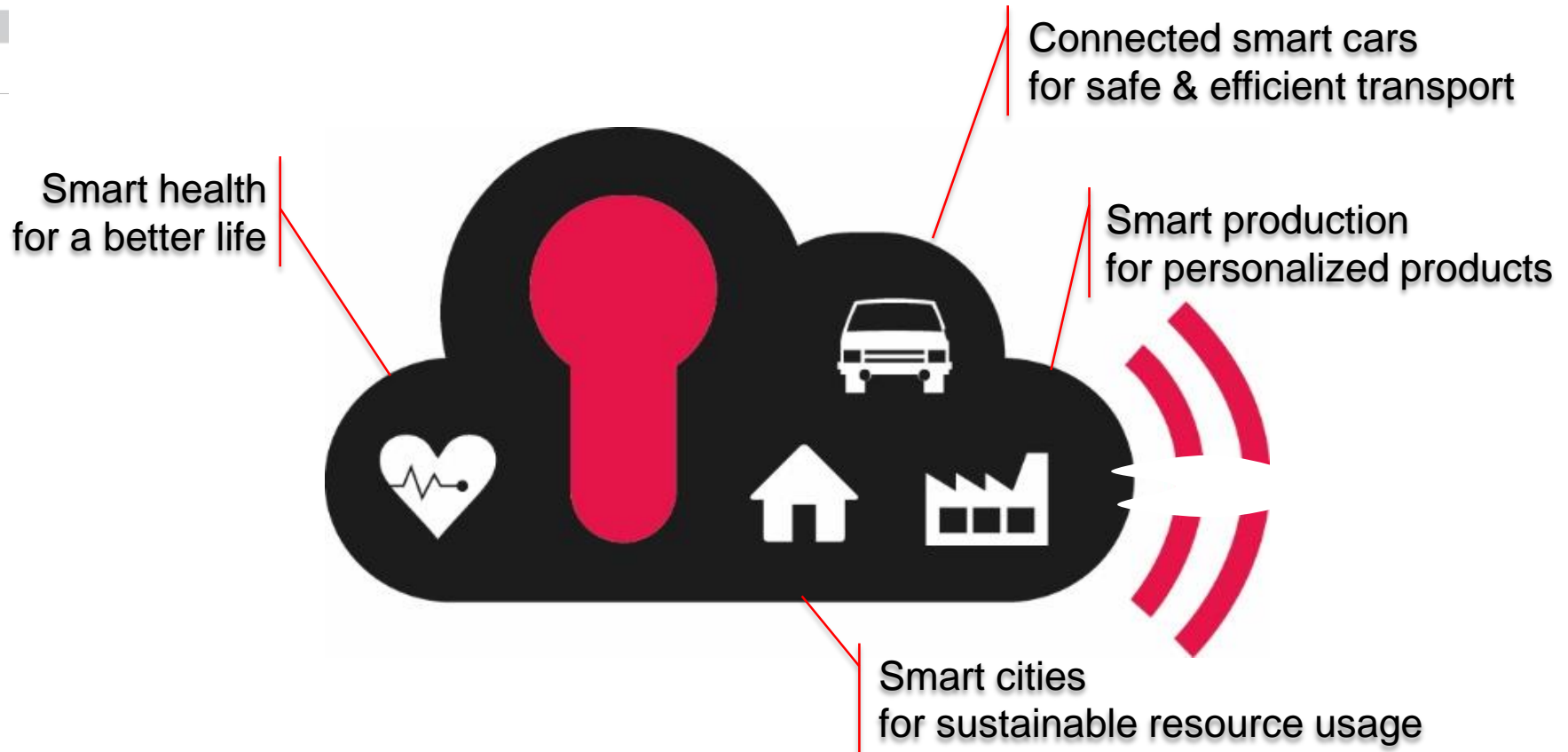
Dependable Things Research Center
@ TU Graz

<http://dependablethings.tugraz.at>



DEPENDABLE INTERNET OF THINGS

Critical Applications

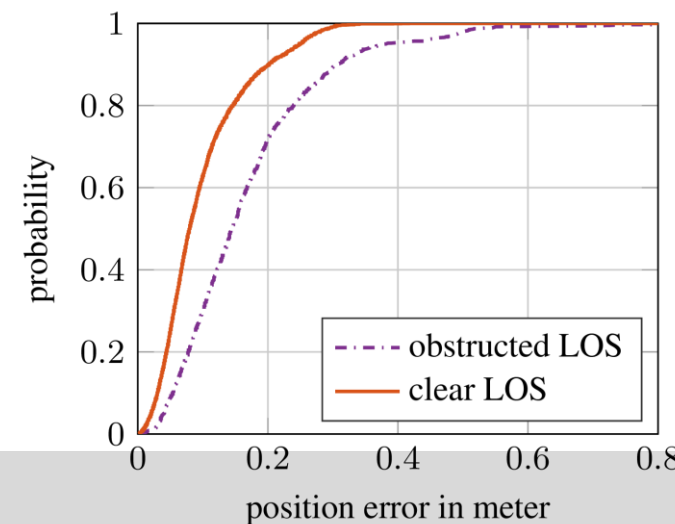
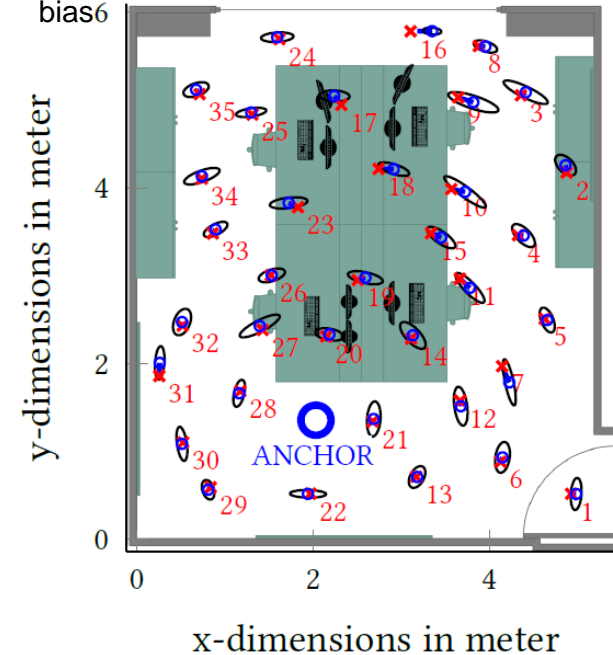


Indoor Localization

Evaluating the performance of the single-anchor localization system in typical office environment

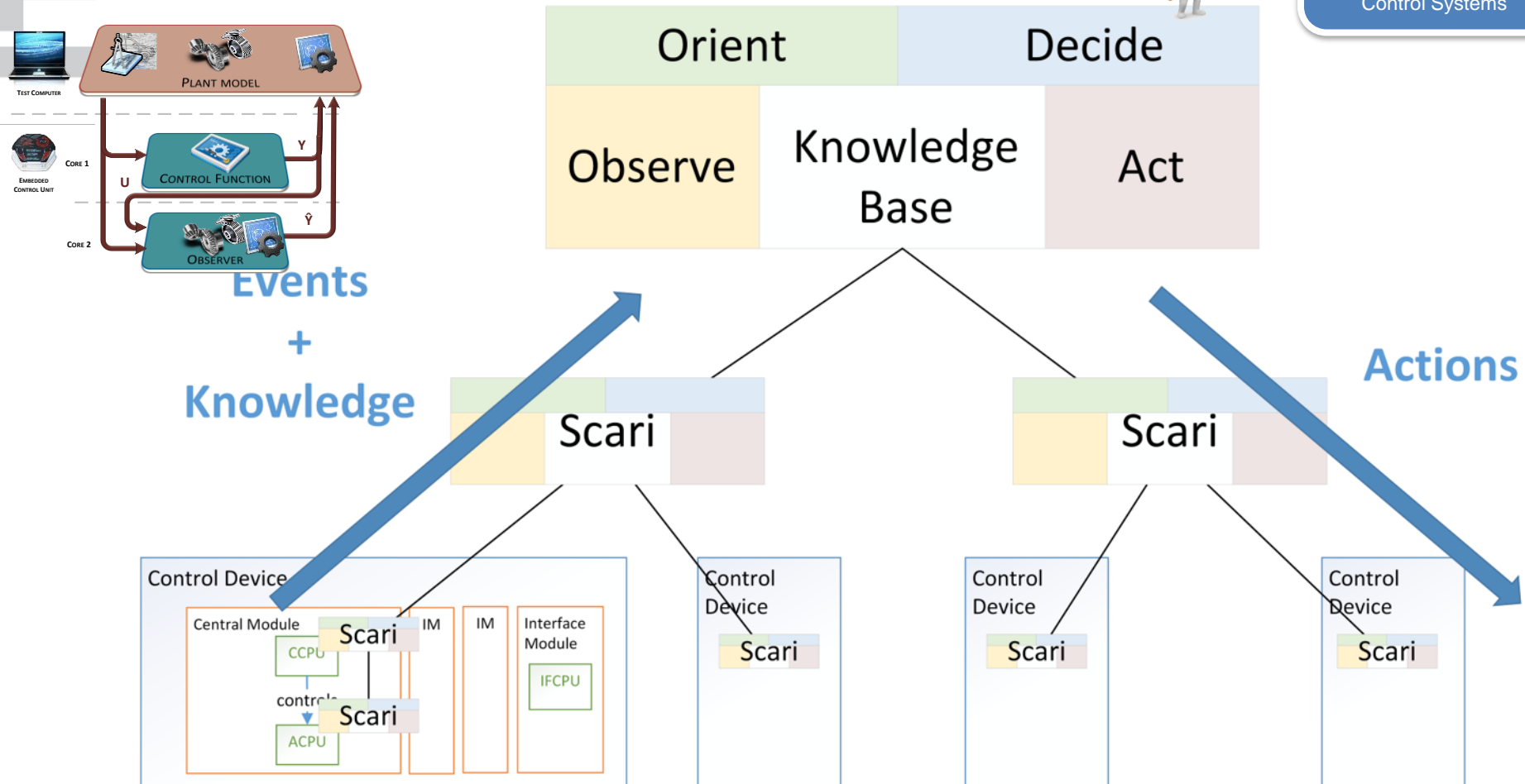
- Accuracy:
 - Clear line-of-sight:
median < 8cm, 90% error < 20cm
 - Obstructed line-of-sight:
median < 14cm, 90% error < 30cm
- Dynamic scenario:
 - 24 hour run with 3 tags and up to 15 people in the room
 - Average error:
< 34cm, 90% error < 79cm

Error ellipses showing position bias6



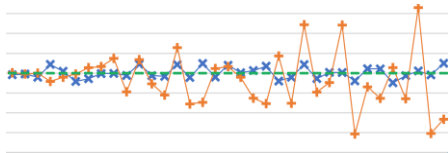
Multi-Layer Resilience Architectures for SCADA Systems

EuroSPI17: Iber et al.
The Potential of Self-Adaptive Software Systems in Industrial Control Systems

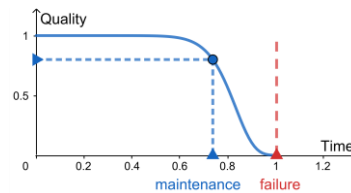


Uncertainty Propagation in IoT

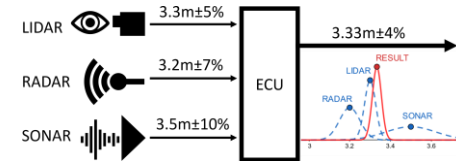
Quality Evaluation



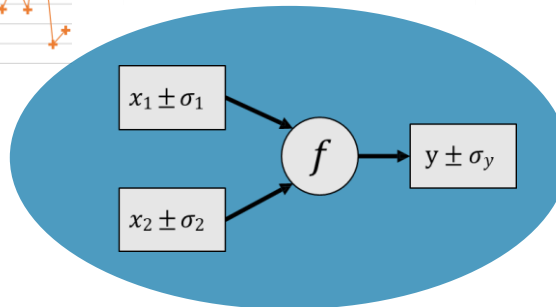
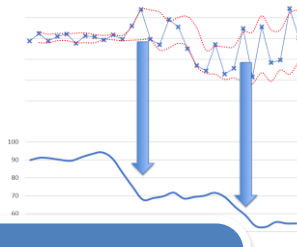
Predictive Maintenance



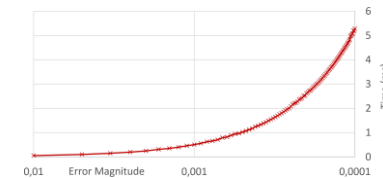
Sensor Fusion



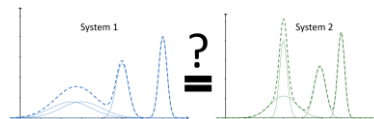
Graceful Degradation



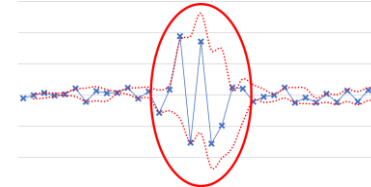
Approximate Computing



Sensor Fingerprinting



Fault Detection



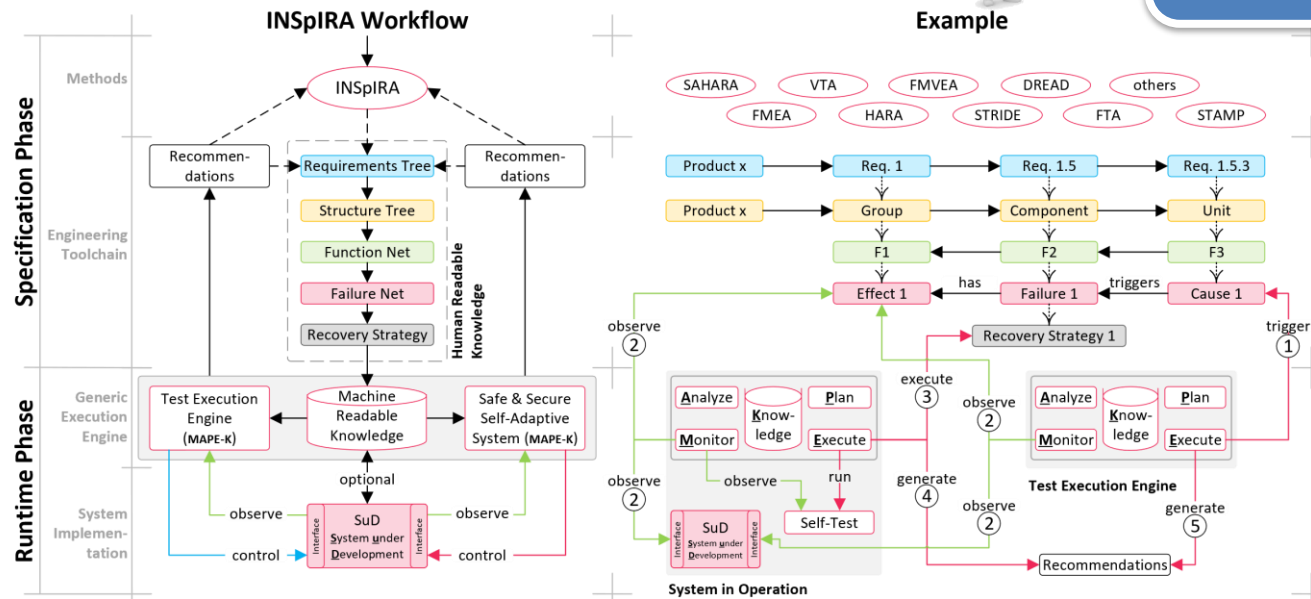
EuroSPI18: Krisper et al.
Use-Cases for Uncertainty
Propagation in Distributed
Control Systems



Runtime Executable Dependability Properties



EuroSPI18: Dobaj et al.
Towards Executable
Dependability Properties



EuroSPI17: Macher et al.
Towards Engineering of
Cooperative Automotive
Cyber-Physical Systems

*Science... never solves a problem without creating
ten more.*

George Bernard Shaw (1856 – 1950)

Science... never solves a problem without creating ten more.

George Bernard Shaw (1856 – 1950)

The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it

Mark Weiser 1991

Is there anything worn under the kilt?



Is there anything worn under the kilt?



No, nothing is worn.
Everything is in perfect
order.