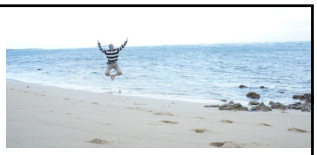
Opportunities, risks and methodologies in a new era of autonomous and "smart" CPSoS

Martin Törngren (*martint@kth.se*), Professor
https://www.kth.se/profile/martint
Mechatronics and Embedded Control Systems,
Machine Design, KTH - Royal Institute of Technology

Innovative Centre for Embedded Systems

1

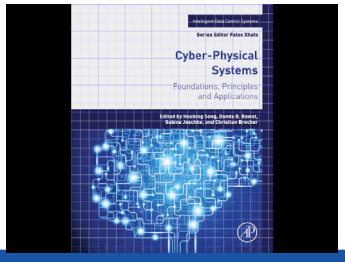
Dr. Who?

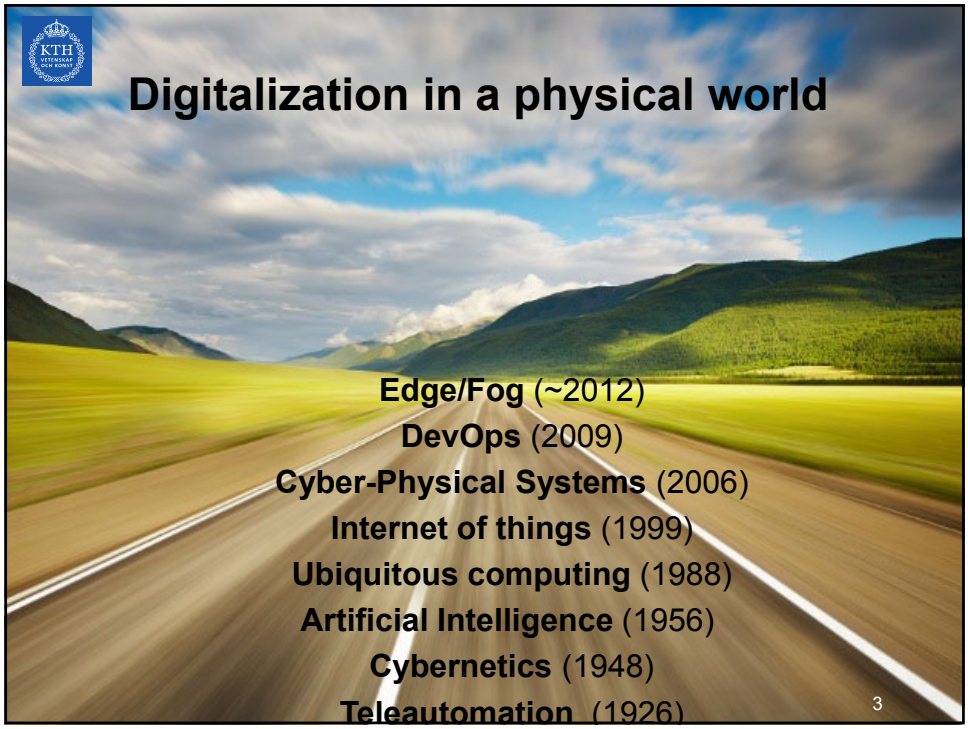


- Prof. at KTH in Embedded Control Systems 2002
- Automated vehicle safety, architecting and MBSE
- Innovation eco-systems: KTH and industry competence network - www.ices.kth.se
- Cyber-Physical Systems

PLATFORMS 4CPS

CyPhERS





Cyber-physical systems (~2006)

Integration of computation, networking and physical processes where CPS range from minuscule (pace makers) to large-scale (e.g. national power-grid).

Not new but with

- Increasing integration across technologies, systems, domains and life-cycle
- Improved and new capabilities
- Business model evolution
- Open society scale deployment

Unprecedented opportunities, societal reliance and risks

Autonomous and smart cyber-physical systems of systems

Scenarios

↓

Automated driving

↓

CPS generalization and challenge perspectives

↓

Reflections for SE

Stockholm central station 2008

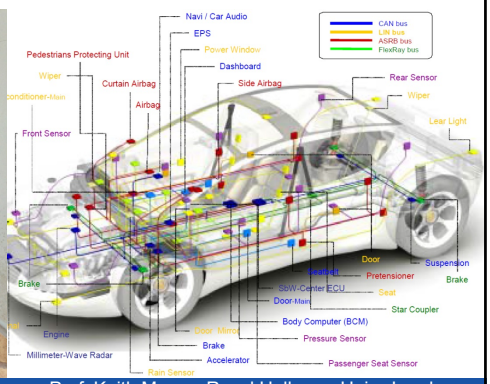
Photo by Michell Zappa, São Paulo, Brazil, CC BY-SA 3.0

The present – new behaviors

More has changed

"Old man's googling"

Proliferation of embedded systems

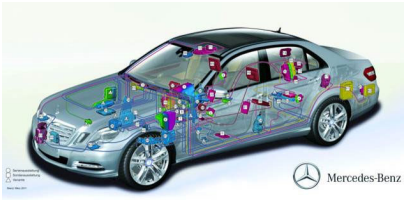


Swedish energy agency

Prof. Keith Mayes, Royal Holloway Univ., London

http://www.energimyndigheten.se/tester/tester-a-o/elmatare-smarta/

Mechanics ➔ Mechatronics



	Susp	Brake	Steer	Wheel	Diff	Trans	Clutch	Eng	Driver
Susp				X					X
Brake				X					X
Steer				X					X
Wheel	X	X	X		X				
Diff				X		X			
Trans					X		X		
Clutch						X		X	X
Eng							X		
Driver		X	X				X		

	Susp	Brake	Steer	Wheel	Diff	Trans	Clutch	Eng	Driver
Susp		P	P	X+P	P	P	P	P	X+P
Brake	P		P	*X*+P	P	P	P	P	*X*+P
Steer	P	P		*X*+P	P	P	P	P	*X*+P
Wheel	X	X	*X*+P		*X*				
Diff	P	P	P	*X*+P		*X*+P	P	P	
Trans	P	P	P	P	*X*+P		*X*+P	P	P
Clutch		P	P		P	*X*+P		*X*+P	P
Eng	P	P	P	P	P	P	*X*+P		P
Driver	P	*X*+P	*X*+P		P	P	*X*+P	P	

Design structure matrices illustrating vehicle components and relations: P – Programmable relations. *X* – Possible change

More has changed

"Old man's googling"

Fortune 500 top list changing more frequently

- Since 2000, more than 50% of the companies have disappeared due to the digitalization wave

http://www.internethistorypodcast.com/2016/07/inventor-of-the-first-digital-camera-steven-sasson/

Leading internet companies (2018, market value)

Rank 2018	Company	Region	Market Value ($B) 5/29/13	5/29/18
1)	Apple	USA	$418	$924
2)	Amazon	USA	121	783
3)	Microsoft	USA	291	753
4)	Google / Alphabet	USA	288	739
5)	Facebook	USA	56	538
6)	Alibaba	China	--	509
7)	Tencent	China	71	483
8)	Netflix	USA	13	152
9)	Ant Financial	China	--	150
10)	eBay + PayPal*	USA	71	133
11)	Booking Holdings	USA	41	100
12)	Salesforce.com	USA	25	94
13)	Baidu	China	34	84
14)	Xiaomi	China	--	75
15)	Uber	USA	--	72
16)	Didi Chuxing	China	--	56
17)	JD.com	China	--	52
18)	Airbnb	USA	--	31
19)	Meituan-Dianping	China	--	30
20)	Toutiao	China	--	30
		Total	$1,429	$5,788

KLEINER PERKINS 2018 INTERNET TRENDS

Source: CapIQ, CB Insights, Wall Street Journal, media reports. *eBay + PayPal combined for comparison purposes though PayPal spun-off of eBay on 7/20/15. Market value data as of 5/29/18. The Wall Street Journey, Recode, TechCrunch, Reuters, and the Information articles detail the latest valuations for Ant Financial (4/18), Xiaomi (5/18), Uber (2/18), Didi Chuxing (12/17), Airbnb (3/17), Meituan-Dianping (10/17), and Toutiao (12/17).

218

Digitalized infrastructures

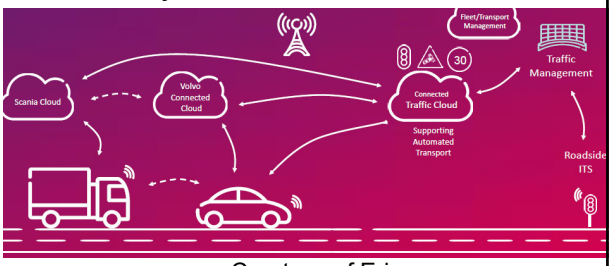
Telecommunication: …3G, 4G, 5G, …

Smart phones/pads

Internet and cloud computing

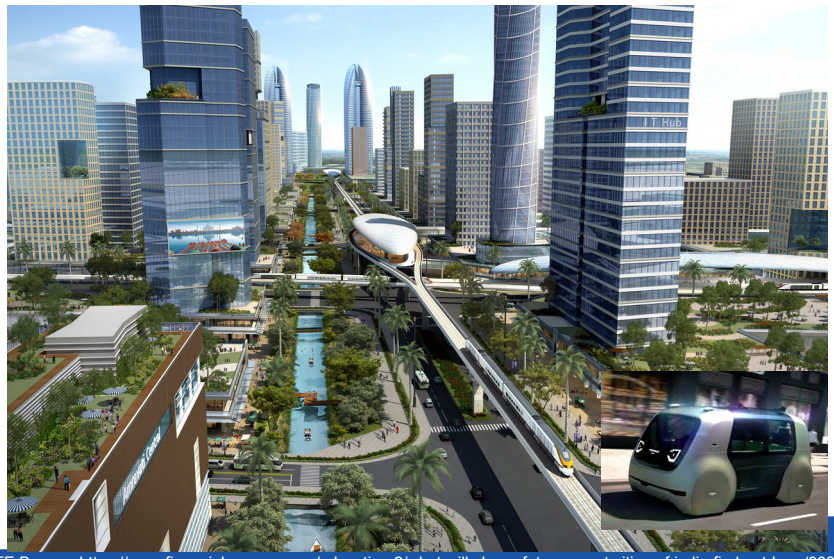
Connected embedded systems

The world as a connected distributed computer system



Courtesy of Ericsson

A future scenario



By FE Bureau: https://www.financialexpress.com/education-2/what-will-shape-future-smart-cities-of-india-find-out-here/968678/

CPS capabilities

Gather, store and process all kinds of data

Awareness and prediction

Plan and make decisions

Affect and create physical systems

Collaborate - exchange information, visualization, AR/VR

➔ Cyber and Physical forming OODA /MAPE-K loops with various time and system perspectives

➔ Reinforced by multiple progressing technological fronts

➔ Unprecedented opportunities and risks!

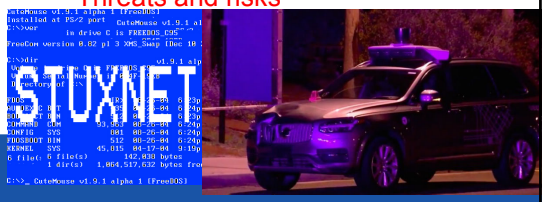
Snapshot of benefits and concerns/risks

How do we consume as much of your time and attention as possible?

… dopamine hits (Sean Parker)

"… the mere prescence of one's own smartphone reduces available cognitive capacity"

Threats and risks



Autonomous and smart cyber-physical systems of systems

Scenarios

↓

Automated driving

↓

CPS generalization and challenge perspectives

↓

Reflections for SE

Perspectives to automated vehicles

Societal aspects, ethics, values

Transportation systems

Legislation, liability, insurance

Life-cycle operation

Automated vehicle(s)

Desired properties

Organizations

Research and science

Context & scenarios (ITS and ODD)

Technology, methodology, standards

Human machine

Levels of automated driving

Sources: Evercore ISI, SAE International

Autonomy: Basic functions

Observation

Localization

Object detection & classification

Planning and generation

Control

Vehicle dynamics

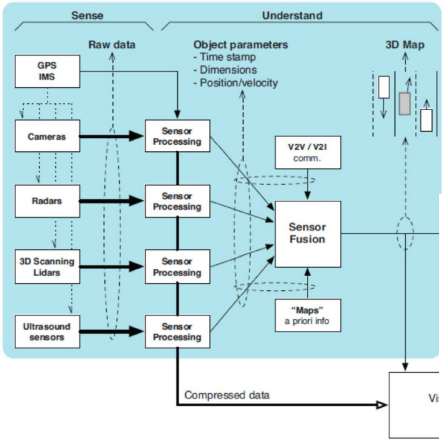
Energy management

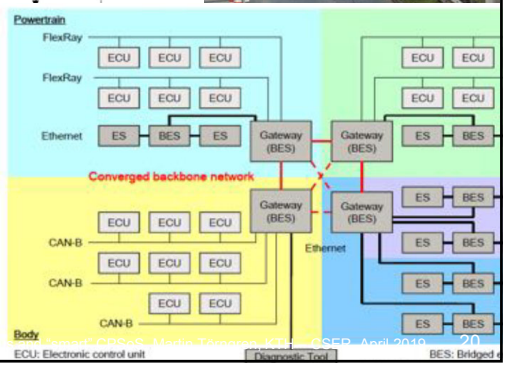
Steering

Propulsion

Braking

Unprecedented capabilities and complexity

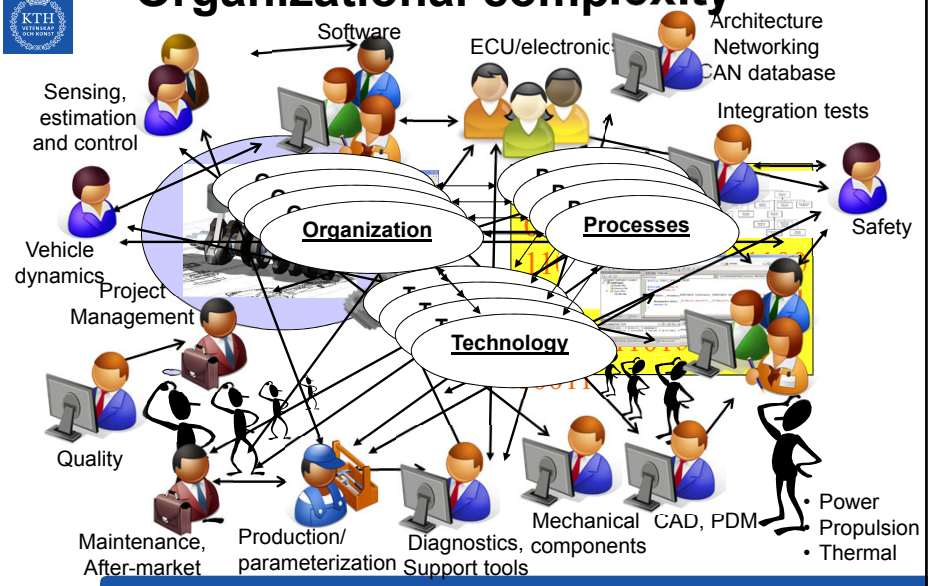




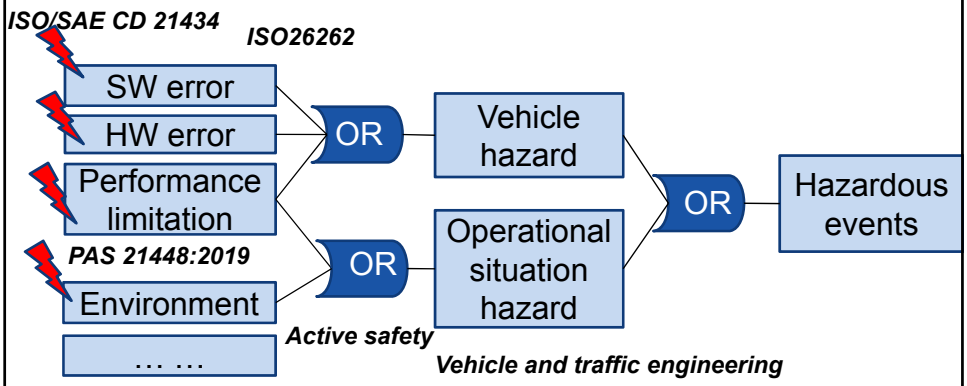
How to assess risk and understand intentions of other actors?

Example – Automated vehicle testing - highway merging
https://www.youtube.com/watch?v=HjtiiGCe1pE&feature=youtu.be

Organizational complexity



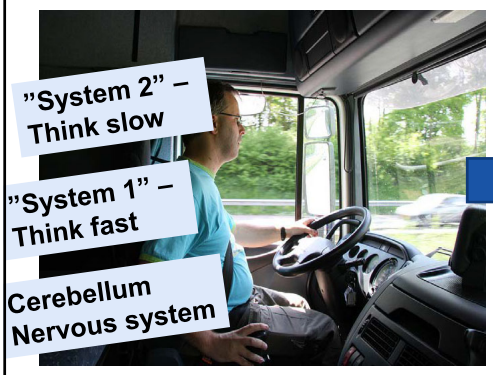
Things that can go wrong - hazardous events



Predictability? Decomposition?
Fragmentation: techniques, standards and communities
Safety engineering methods and standards seriously lagging!

Breaking new ground – generalized knowledge

ADI – "Autonomous Driving Intelligence"



By Veronica538 (Own work)
[CC BY-SA 3.0 (http://creativecommons.org/licenses/by-sa/3.0) or GFDL (http://www.gnu.org/copyleft/fdl.html)], via Wikimedia Commons

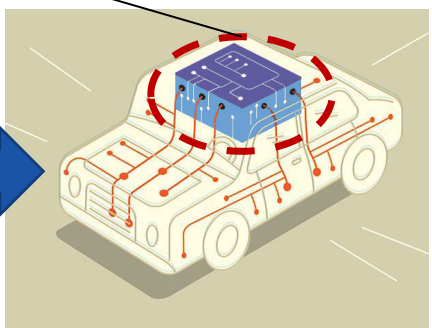


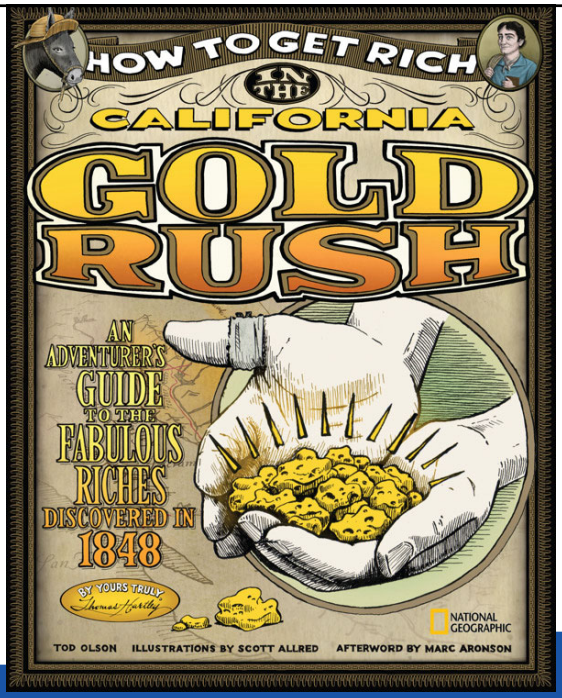
Illustration: Harry Campbell, IEEE Spectrum
http://spectrum.ieee.org/cars-that-think/transportation/self-driving/nxps-bluebox-bids-to-be-the-brains-of-your-car

What drives AV development?

Business MIT Tech Review:
- **Can We Put a Price on Autonomous Driving?**

- Transport services: ~ Trillions of dollars!
- Traffic accidents: 100's of billions of dollars
- Traffic efficiency, productivity and public health: - II -

The beginning of wisdom is to call things by their proper name – attributed to Confucius



Today: Billions poured in to get to the Trillions!

Key question: When will the Gold emerge?

1849 – Gold rush

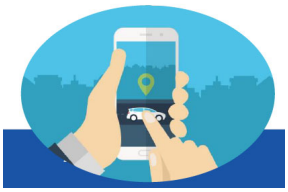
What is the impact of the gold-rush?

”All digging” – doing the same thing!

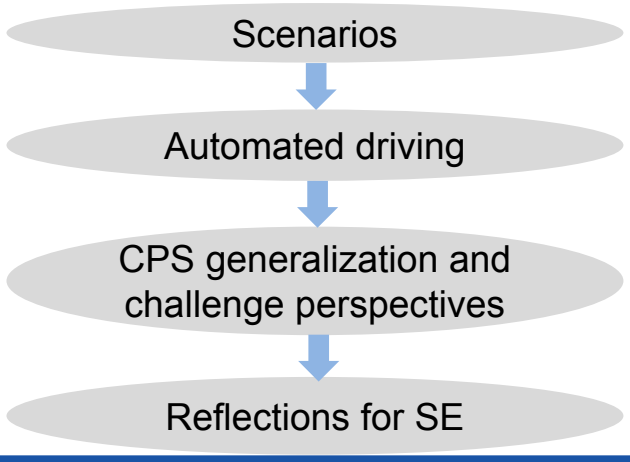
- Enormous parallel investments to brake new ground and hit the market!
- Fight for competence
- New Constellations but very little of broad collaborations
- Risks

CPS melting pot



Autonomous and smart cyber-physical systems of systems



Cyber-physical systems (~2006)

Integration of computation, networking and physical processes where CPS range from minuscule (pace makers) to large-scale (e.g. national power-grid).

Same trends across domains

- Increasing level of integration and capabilities
- Business model evolution
- Open society scale deployment

Unprecedented opportunities, societal reliance and risks

Several parallel gold rushes!

Automated driving/
transportation services

1200 IoT platforms

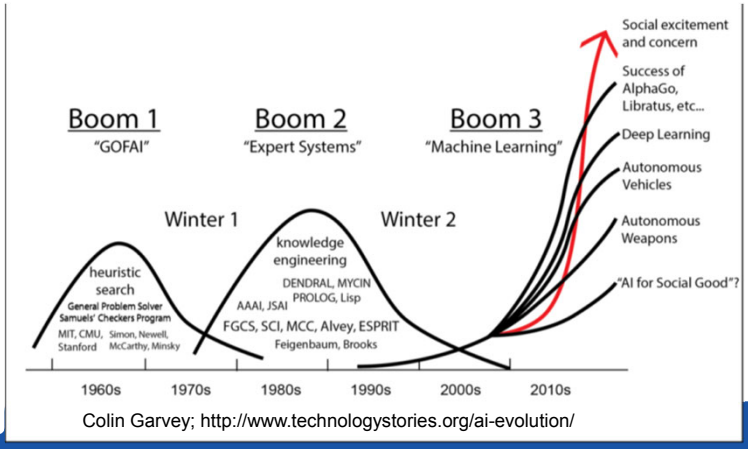
Strong market forces!
Partly unregulated areas!
Is trust a key priority?

Herbert Simon on industrial revolutions: (the steam engine and the computer)

- Technological revolutions are slow
- The first revolution (involving steam engines) took 150 years to change society – with 6 generations as a tentative time constant
- There is no single technology - behind of revolution – rather a web of technologies!
  - Computers, internet, connectivity, AI, …
- We shape technological revolutions!!
  - Social impact becomes tangible in the 2nd half

Amara's law

We tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run



Colin Garvey; http://www.technologystories.org/ai-evolution/

CyPhERS Cyber-Physical European Roadmap & Strategy

Technological **Organizational/Business** **Societal**

Push

Software
Networking
Wireless com.
Sensors and actuators
Packaging/integration
Computing technology
Software platforms
Control methods
Tools
…

Values/properties

Society

Science & Technology

Organizations

Pull

Energy

Transportation

Healthcare

Competitive production

Comfort

Entertainment

Technological **Organizational/Business** **Societal**

Push

Software
Networking
Wireless com.
Sensors and actuators
Packaging/integration
Computing technology
Software platforms
Control methods
Tools
…

Values/properties

Science & Technology
Complexity
Trustworthiness

Society
Sustainability

Organizations
Competence

Pull

Energy

Transportation

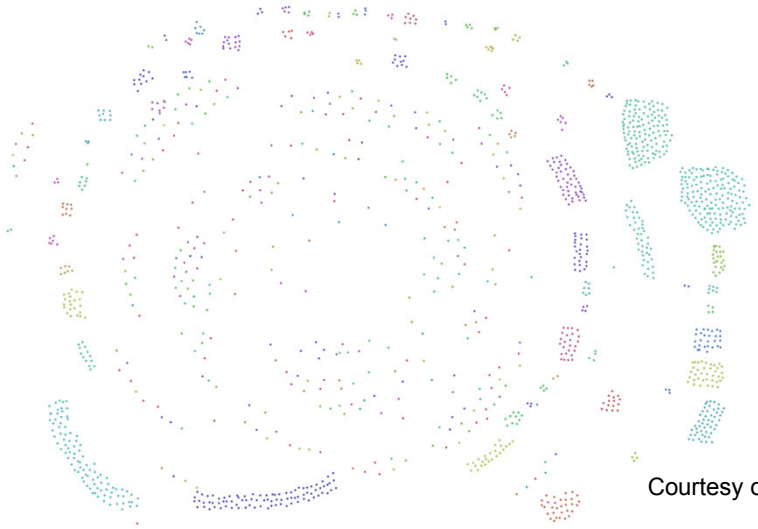
Healthcare

Competitive production

Comfort

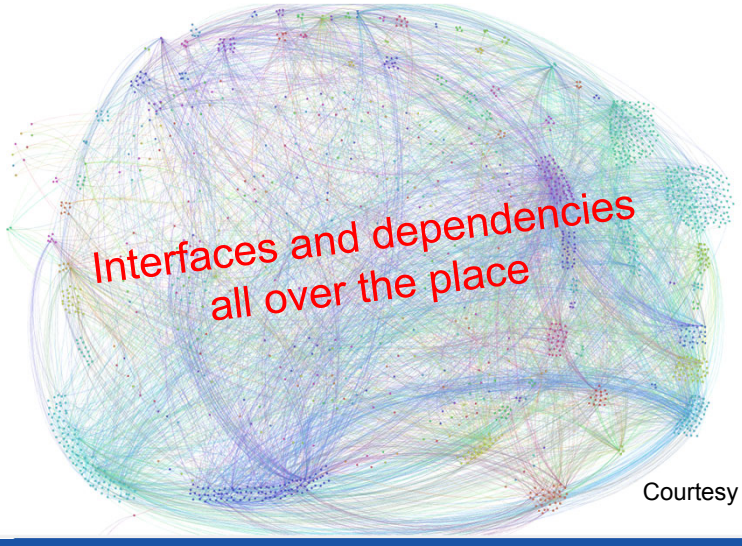
Entertainment

1500 logical nodes – example Scania production vehicle, 2013



Courtesy of Scania

14000 connections – same Scania production vehicle example, 2013



Courtesy of Scania

A key CPS challenge: Combinations of deterministic models are non-determinstic

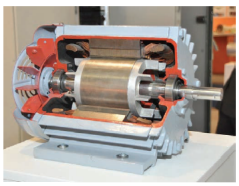


Image: Wikimedia Commons

```
void initTimer(void) {
    SysTickPeriodSet(SysCtlClockGet() / 1000);
    SysTickEnable();
    SysTickIntEnable();
}
volatile uint timer_count = 0;
void ISR(void) {
    if(timer_count != 0) {
        timer_count--;
    }
}
int main(void) {
    SysTickIntRegister(&ISR);
    ... // other init
    timer_count = 2000;
    initTimer();
    while(timer_count != 0) {
        ... code to run for 2 seconds
    }
    ... // other code
}
```

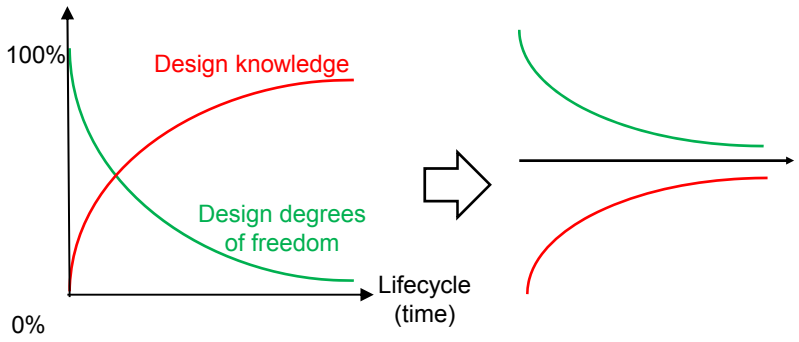
$$\dot{\mathbf{x}}(t) = \dot{\mathbf{x}}(0) + \frac{1}{M}\int_0^t \mathbf{F}(\tau)d\tau$$

No notion of timing at the SW level

Courtesy, Edward Lee, UC Berkeley

Challenge further aggravated by non-predictable multicore platforms

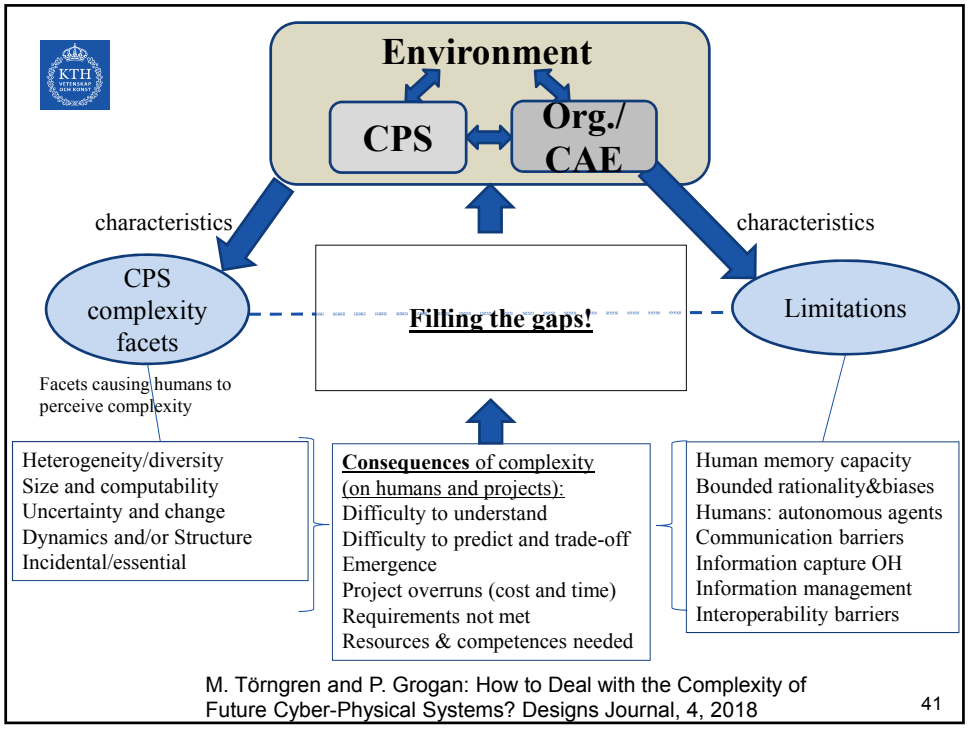
An increasing cone of uncertainty



- **Uncertainties in system and environment, risks and threats**
- **Robustness/resilience becomes even more important**

The "Cyber Physical" tension

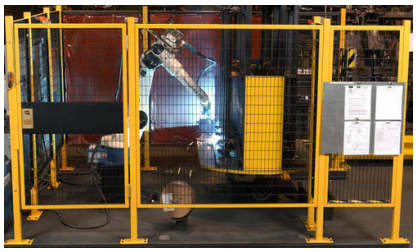
Dimension	„Cyber Domain"	„Physical Domain"
Example Disciplines	Logistics	Aeronautics
Typical Life Cycle	< 2-3 Year	> 10-30 Years
Business Model	Dynamic Value Network	Static Supply Chain
Development Approach	Continuous Delivery	Implement-Commission-Operate –Decommission
Dependability Focus	Security	Safety (and certification)
Platform Approach	Max. virtualization/Cloud	Min. virtualization/RTOS
Example Technologies	Big Data, Online Learning	Control Synthesis

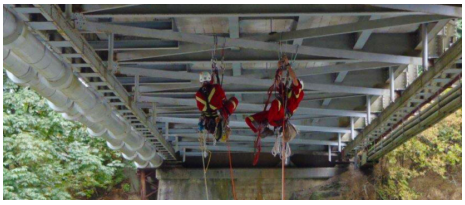


M. Törngren and P. Grogan: How to Deal with the Complexity of Future Cyber-Physical Systems? Designs Journal, 4, 2018

41

Automation and trust: Beyond dirty, dull and dangerous





Failure modes, explainability, understandability, ethics/values
Safety, security, reliability and privacy
The Automation paradox

Automation and trust – what is changing?

Adding "*Dear" and "Difficult*" to Dirty, Dull and Dangerous

Prediction machines (sensors, data, algorithms, compute)

Human AI/robot collaboration, intent

Failure modes, explainability, understandability, ethics/values

The Automation paradox – more relevant than ever

- The better autonomy, the less training, and the more difficult situations to handle when the automation fails
- Call for safety engineering!

Safety, security, reliability and privacy

Systems engineering insights and needs for new methodologies

The Cynefin model

➔ complex environments and uncertainty

➔ composability - dependencies and side effects

Current level 3 testing for AD/AVs

Current tests in the automotive are not well controlled!

Aerospace:

- Simulation, formal methods and rigorous processes.
- Minimizing testing to mitigate risks – Controlled experiments
- **But … safety requires continuous efforts!!!**

Safety case for level 3 testing

- An AV testing platform with safety driver
- Non fruitful blames: victim, technology, safety driver
- To be expected: Pedestrian on road; Failures; Solo human drop-out
- The better autonomy the more difficult situations!

Sources: Aerospace practice; OSS.5-2019, Safecomp 2018

Sustainability

Meeting the needs of the present without compromising the future

Environmental, economical and social:

- Climate warming
- 91% of the world's population live in places where air quality exceeds WHO guideline limits
- Overspending of natural resoures

A case for circular economy!

- Beyond the *take-make-dispose* industrial model
- Important role and opportunities for systems engineering/ST/DT!!

CPS melting pot, requiring multidisciplinary engineering and science!



Robotics and Artificial intelligence
Embedded, edge, cloud and HPC
Software engineering
Mechanical engineering
Systems engineering
Safety, security and dependability

Education and training challenges

Need for educational renewal!

Need for life-long learning!

Low status of education is a problem!

Digitalization in a physical world - Reflections for SE

Virtually all systems will be of CPS nature in a CPSoS context!

Complexity, emergence, resilience, awareness of risks!

Human-CPS – Automation/AI and trustworthiness!

SE, ST and **DT** more important than ever!

Human centered design – requires new approaches!

Sustainability and circular economy!

Promoting teaching, life-long learning and CDIO!

Selected references

Martin Törngren and Paul T. Grogan. **How to Deal with the Complexity of Future Cyber-Physical Systems?**, Journal of Designs, Vol. 2, No. 4, 2018

Martin Törngren and Ulf Sellgren. Complexity Challenges in Development of Cyber-Physical Systems. In Principles of Modeling; M. Lohstroh et al – editors; Springer, 2018; Vol. 10760, Lecture Notes in Computer Science, July 2018

Martin Törngren et al. **Architecting Safety Supervisors for High Levels of Automated Driving**. 21st IEEE Int. Conf. on Intelligent Transp. Systems, Nov. 2018.

Future directions of Systems engineering, Hillary Sillitto, KTH/ICES workshop 2018-03-13:
http://www.ices.kth.se/events.aspx?pid=3&evtKeyId=dc4eb9edb56c49b6b34acc2ee04f3fc5

Platform4CPS recommendations:
www.platforms4cps.eu/fileadmin/user_upload/E-Book_-_Platforms4CPS_Key_Outcomes_and_Recommendations.pdf

German agenda CPS:
http://www.cyphers.eu/sites/default/files/acatech_STUDIE_agendaCPS_eng_ANSICHT.pdf

CPS foundations, principles and applications:
http://www.sciencedirect.com/science/book/9780128038017