Towards an era of smart life-cycle connected cyber-physical systems – SE implications or …

… When is an automated vehicle (AV) ready to go?

Martin Törngren, Mechatronics,

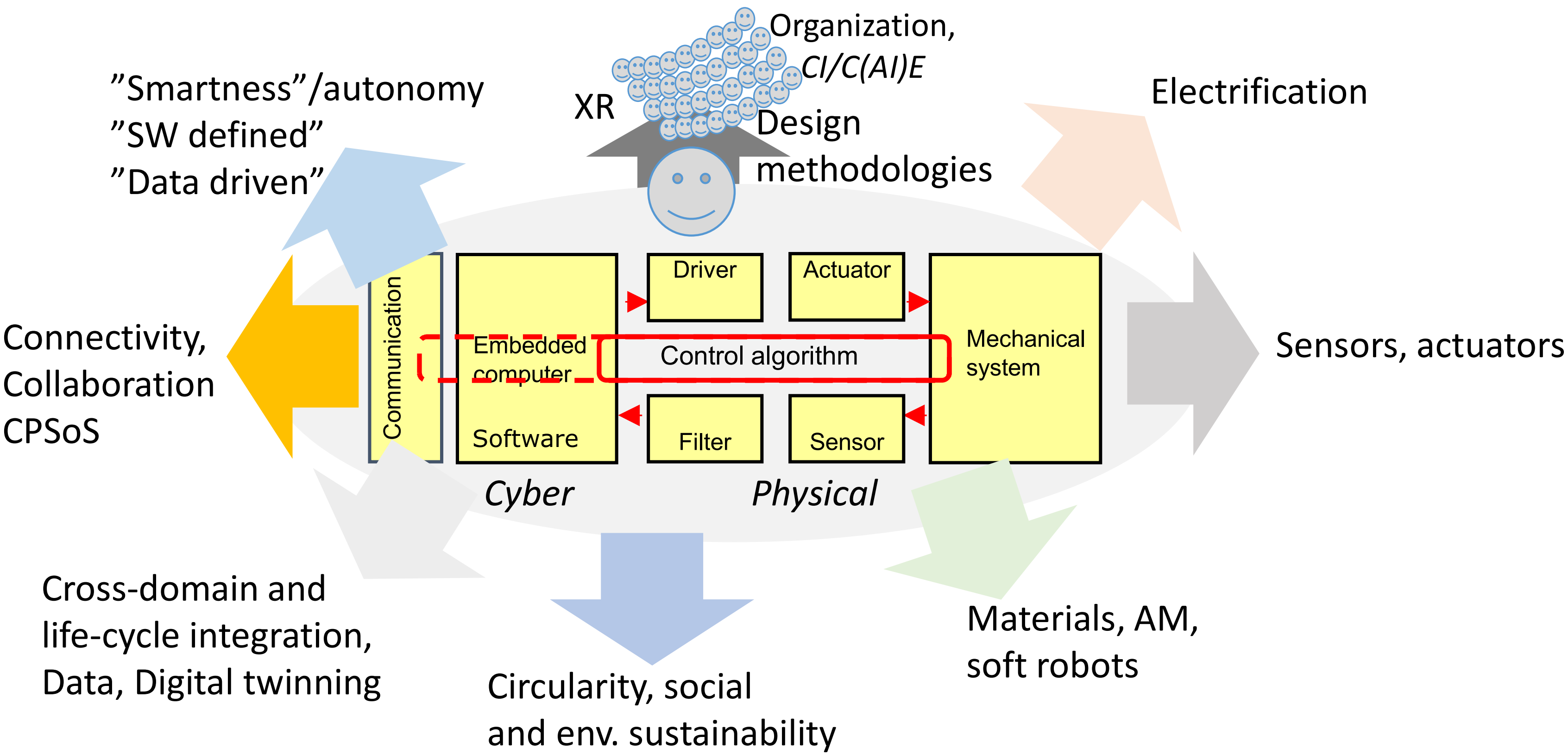
KTH Royal Institute of Technology, Stockholm

PERCy

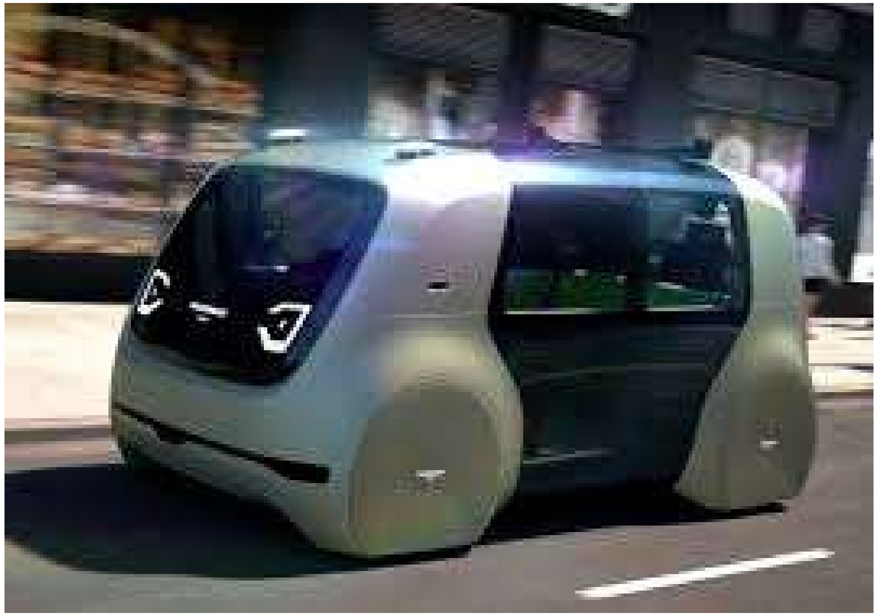
WASP bridge

AD-EYE

Zooming in ➔ Mechatronics and trends



When is an automated vehicle (AV) ready to go?



Technically?
Socio-technically?
What about upgrades and emergence?

Physical vs. Software vs. Data systems

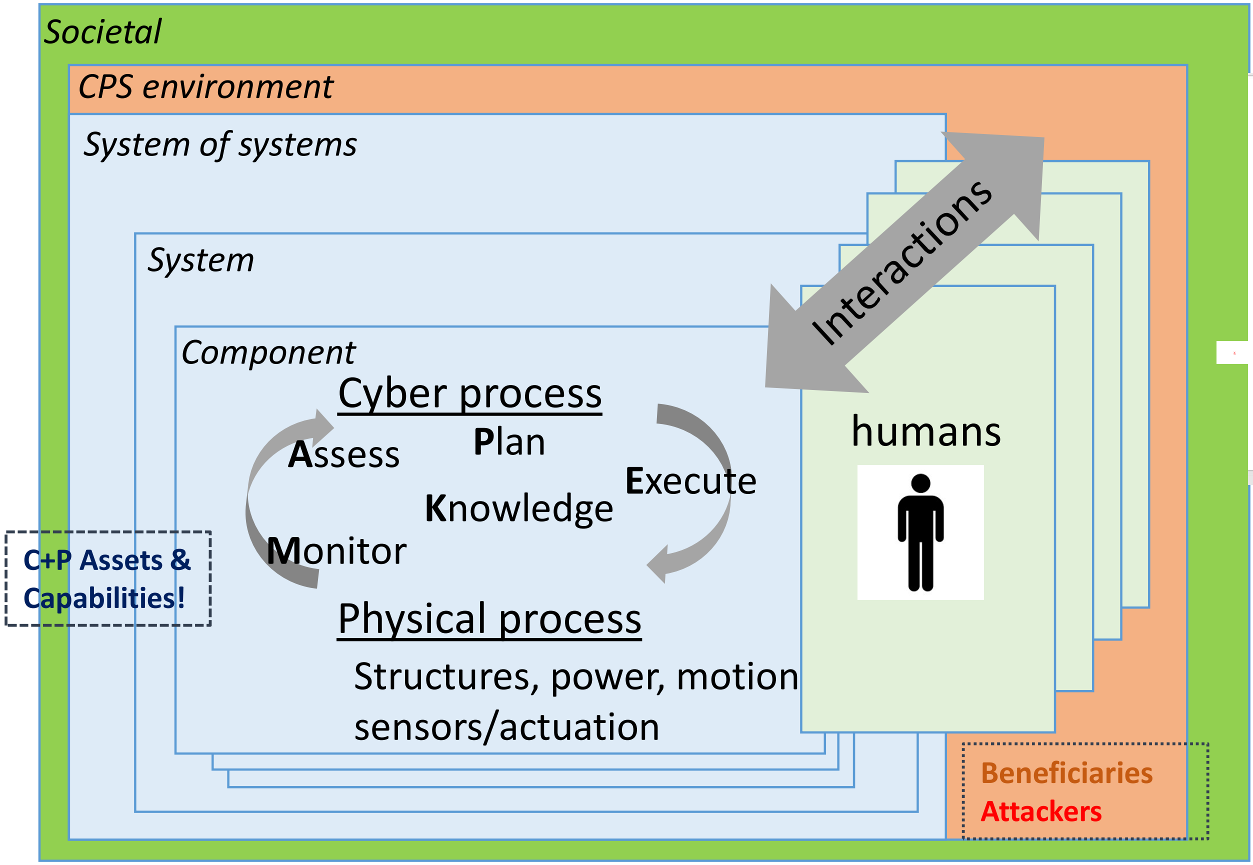
	Physical systems	Software	Data
Phenomena and effects	Multiple coupled physical phenomena, ”slow transfer”	State space; bugs; connectivity; variability ”fast transfer”	Super-human performance; Brittleness
Abstractions, synthesis, and platforms	Approximations, analog, no single “platform technology”	Digital / discretization ”platform” foundations; Abstracted physical props!	Learning based models
Extra-functional properties	Established cost models	Dependencies all-over, hard to estimate life-cycle cost	SW under the hood Data quality, availability; and accessibility

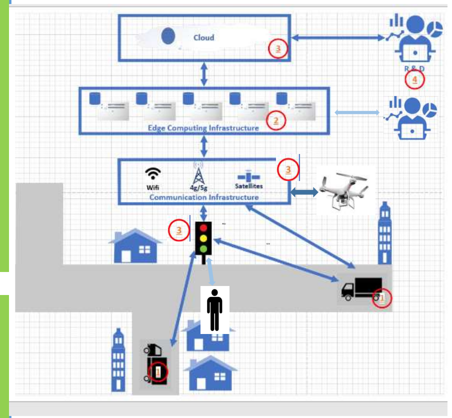
Combined … and in systems at different levels → CPS capabilities

Cyber-physical systems have far-reaching implications. Hipeac Vision 2021. https://doi.org/10.5281/zenodo.4710500

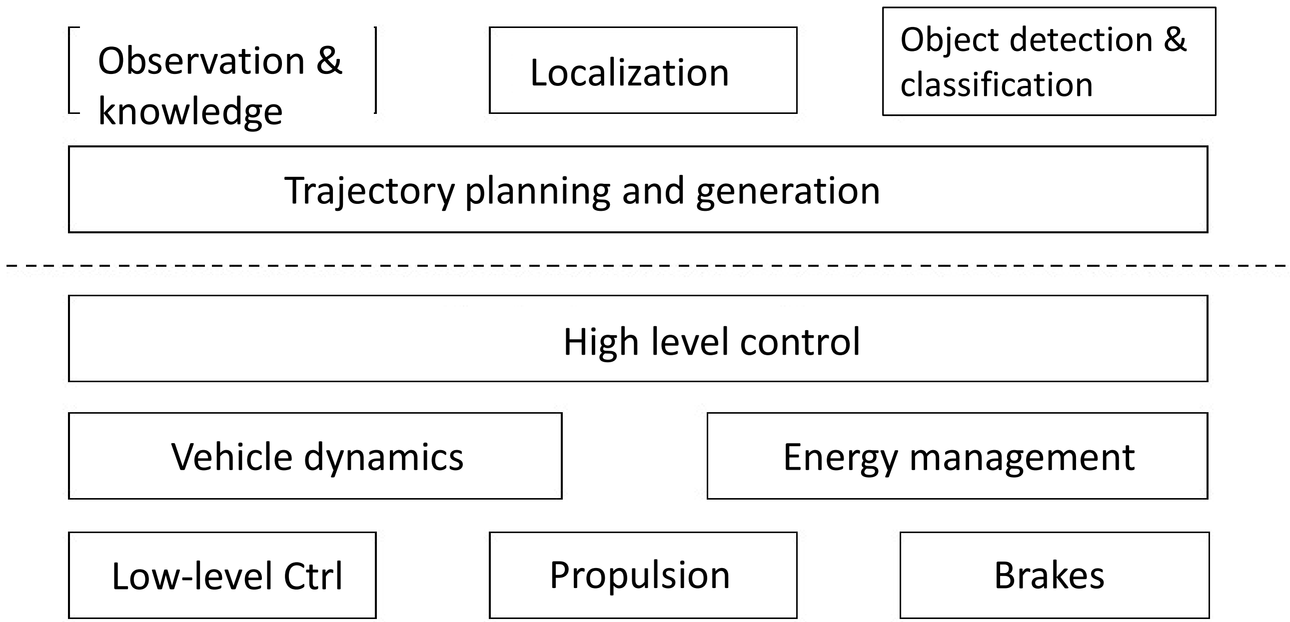
Cyber-physical systems

Public perception
Regulations, standards
Societal effects

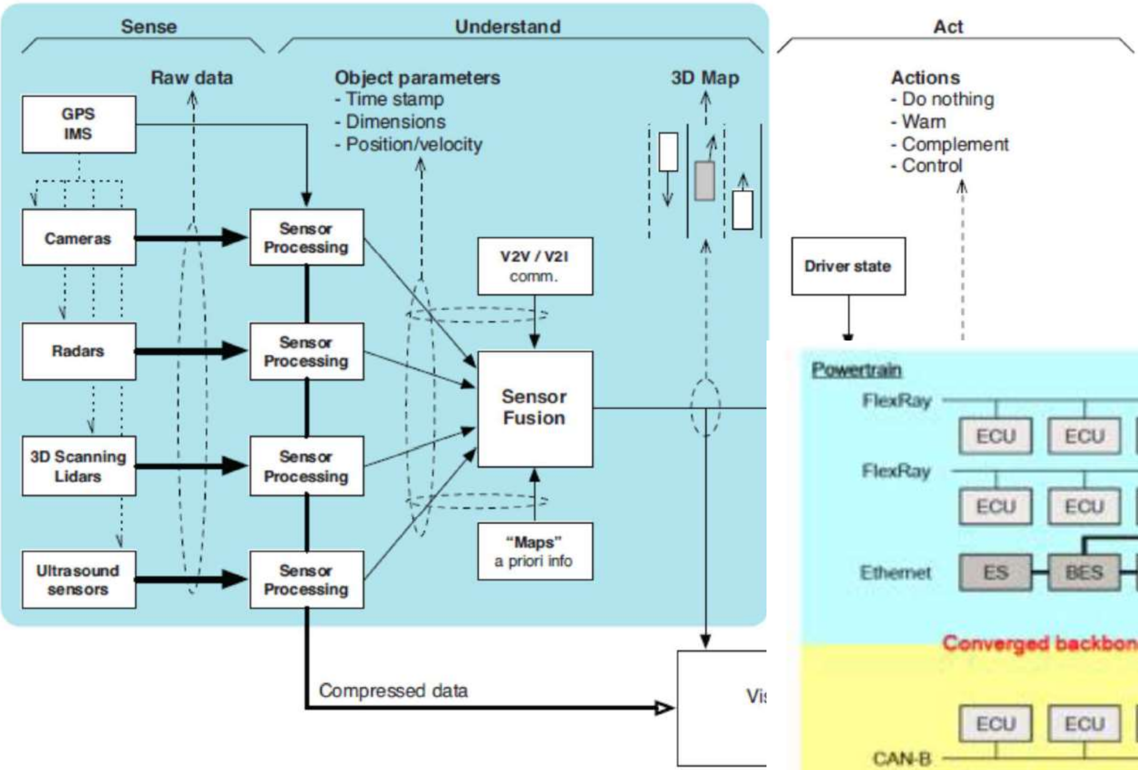


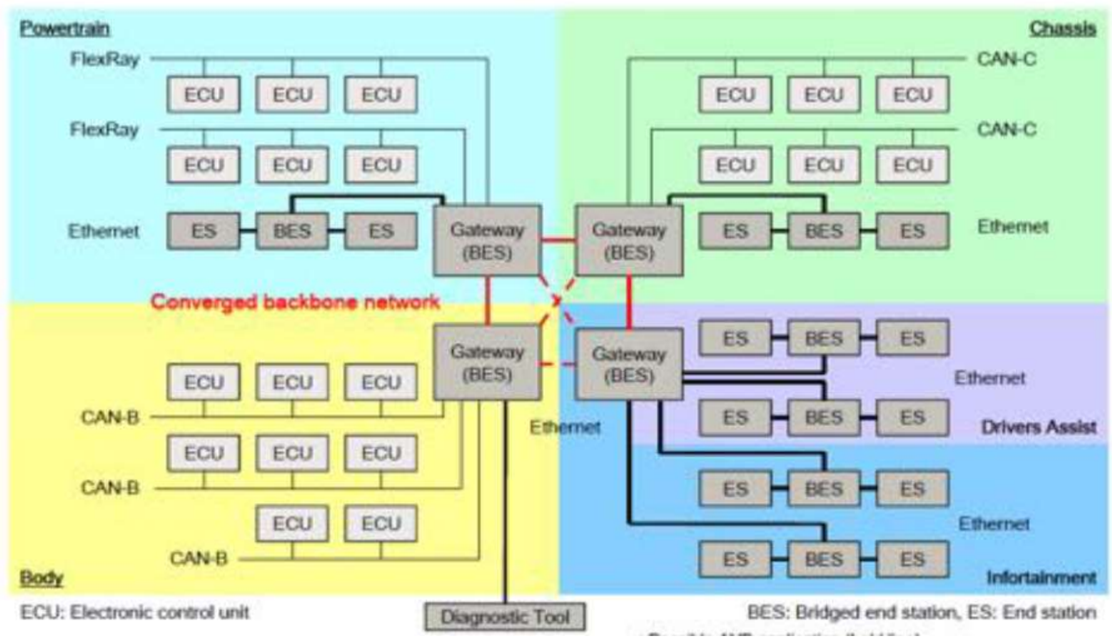


Autonomy: Basic functions

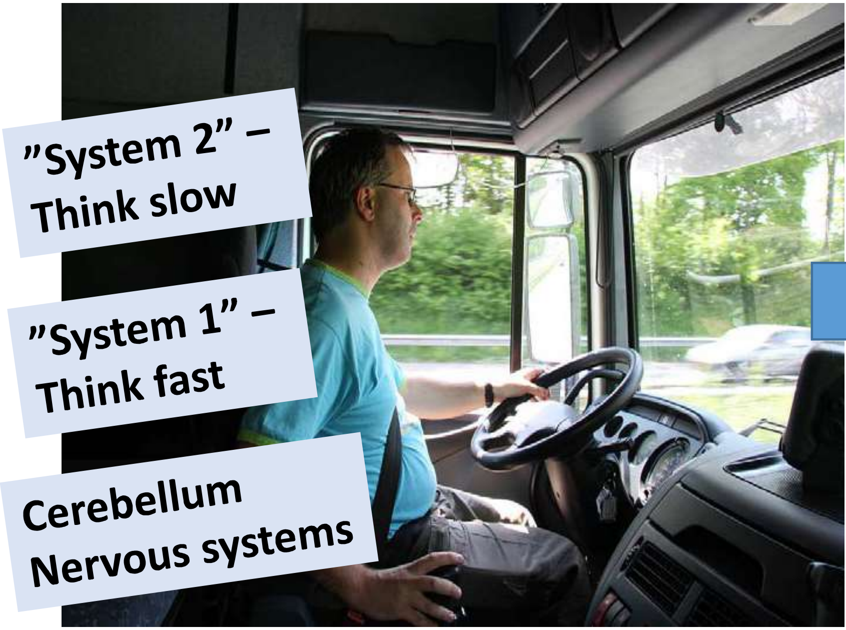


New ground: Unprecedented complexity





Human intelligence as a reference for automated CPS? Breaking new grounds



ADI – Autonomous Driving Intelligence

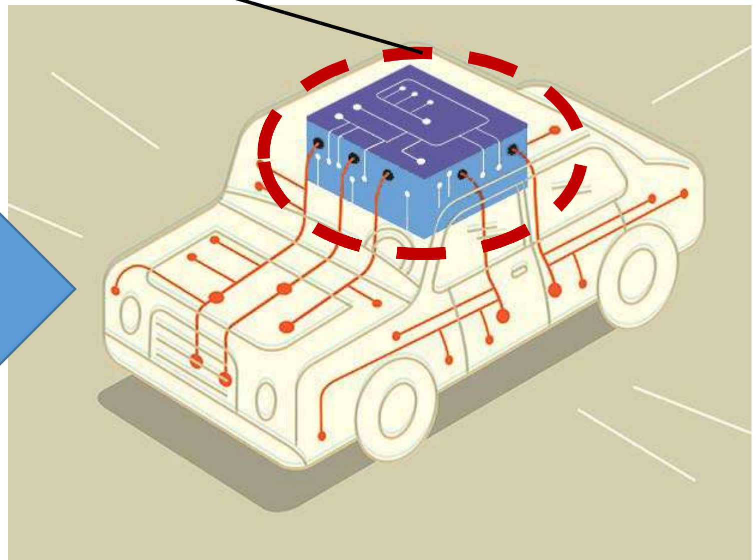
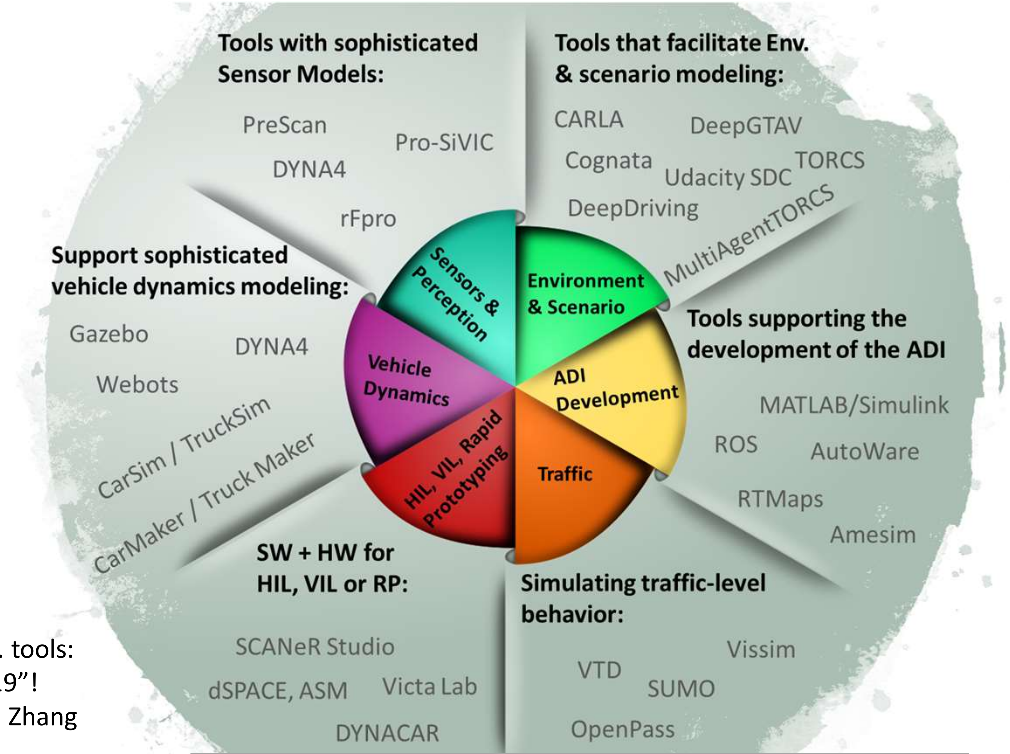


Illustration: Harry Campbell, IEEE Spectrum
http://spectrum.ieee.org/cars-that-think/transportation/self-driving/nxps-bluebox-bids-to-be-the-brains-of-your-car

Automated vehicle modeling & simulation tools



Co-simulation	FMI, HLA, DDS, ModelCONNECT, AD-EYE

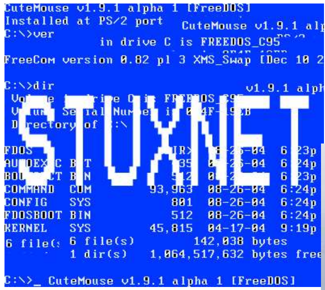
KTH survey on
Modeling & sim. tools:
Dated: ”Jan. 2019”!
Courtesy: Xinhai Zhang

When are we done with V&V efforts?

Challenges in building, operating and maintaining (collaborative) CPS

- **The world of software and bugs**
  - Industry average code ~ 15– 50 errors /KLOC
  - Safety critical systems may reach 0.1 error/KLOC at very high cost
- **Deep learning: breakthroughs but brittleness**
  - Prediction machines with domain specific super-human capability but without explainability and contextualization beyond training data
- **Cyber-security threats and attacks**
  - Dynamic threat landscape; imbalance
- **Complexity**
  - Billions of transistors, LOC's and 100's of billions of (DL) parameters
- **Automation surprises and pitfalls**

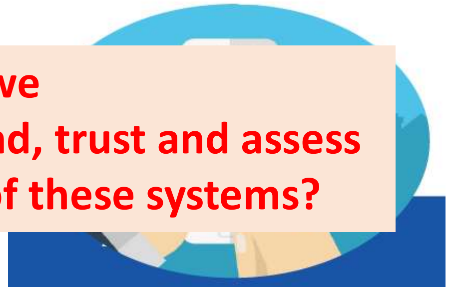
Societal reliance on CPS



Human-centered Cyber-physical systems?

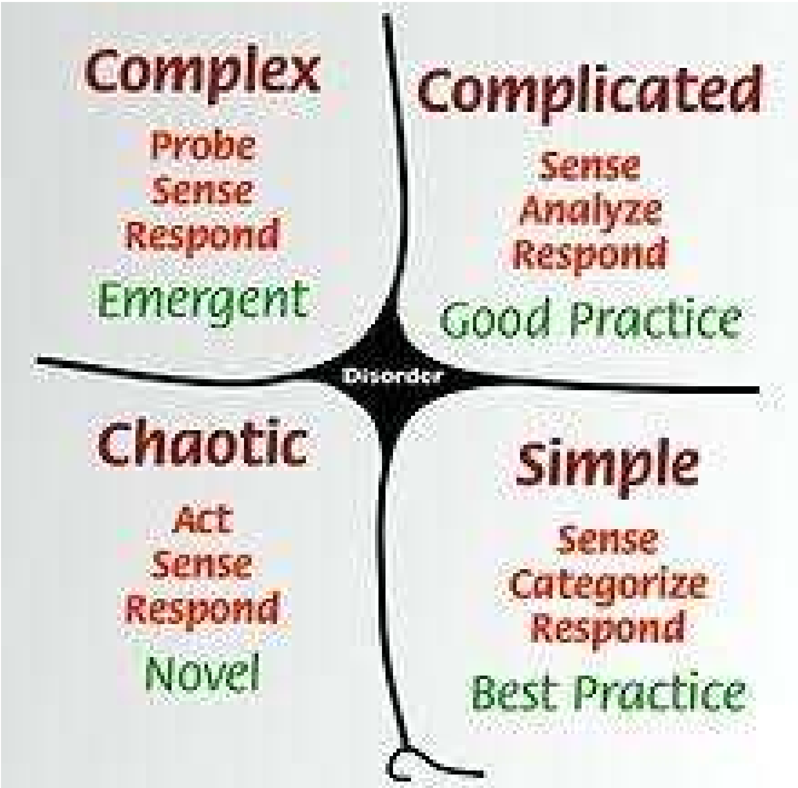
Arthur C. Clarke:

Any sufficiently advanced technology is indistinguishable from magic



How can we
Understand, trust and assess
the risks of these systems?

Needs and tools when going into the "complex domain"

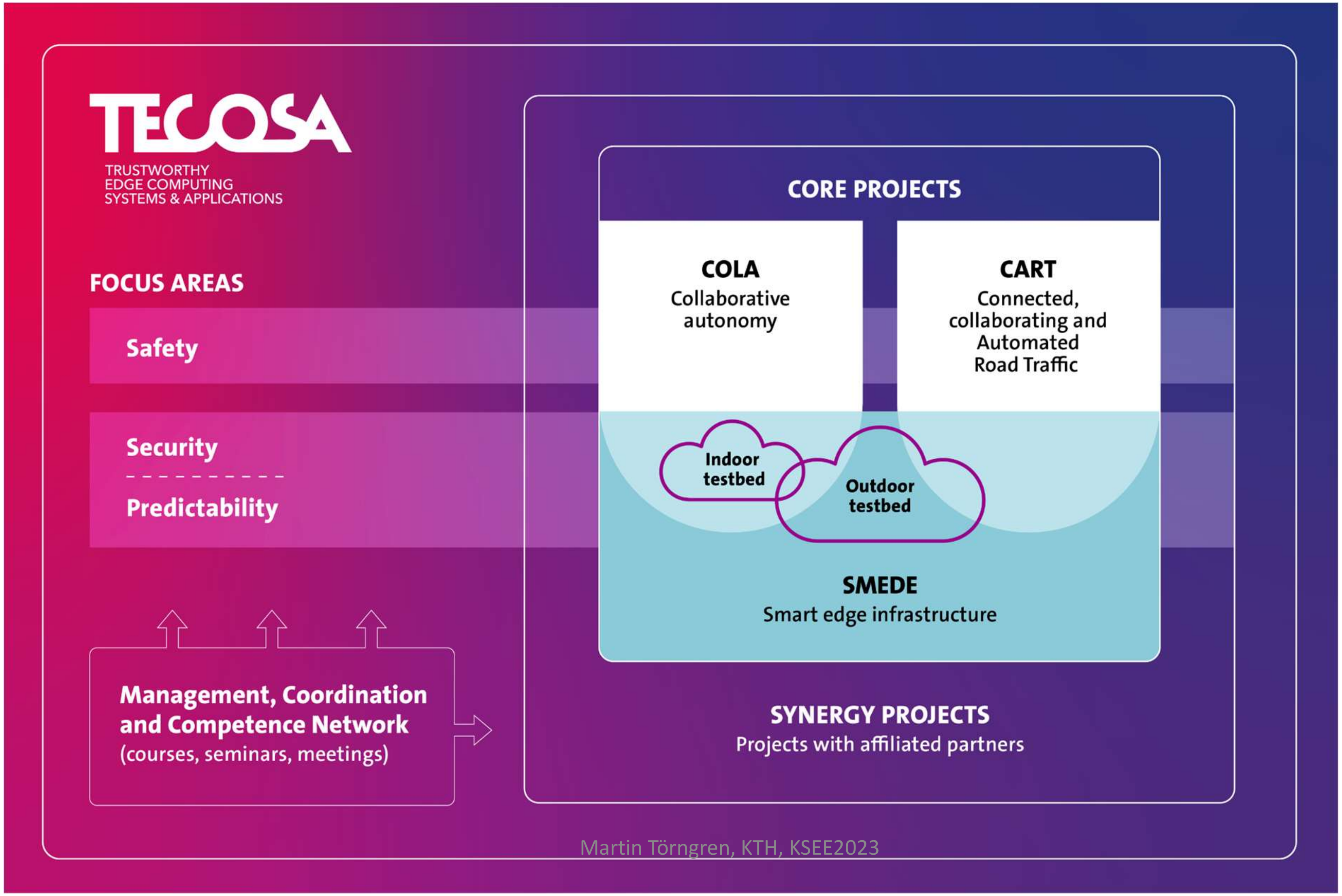


Cynefin model (Snowden, 1999)

- Learning and developing new methodologies and architectures
    - Sharing of data, incidents, failures, …
    - Testbeds and controlled experiments!
- New sociotechnical frameworks, legislation, and agreeing on risks
- New innovation eco-systems
- Forums for debate!

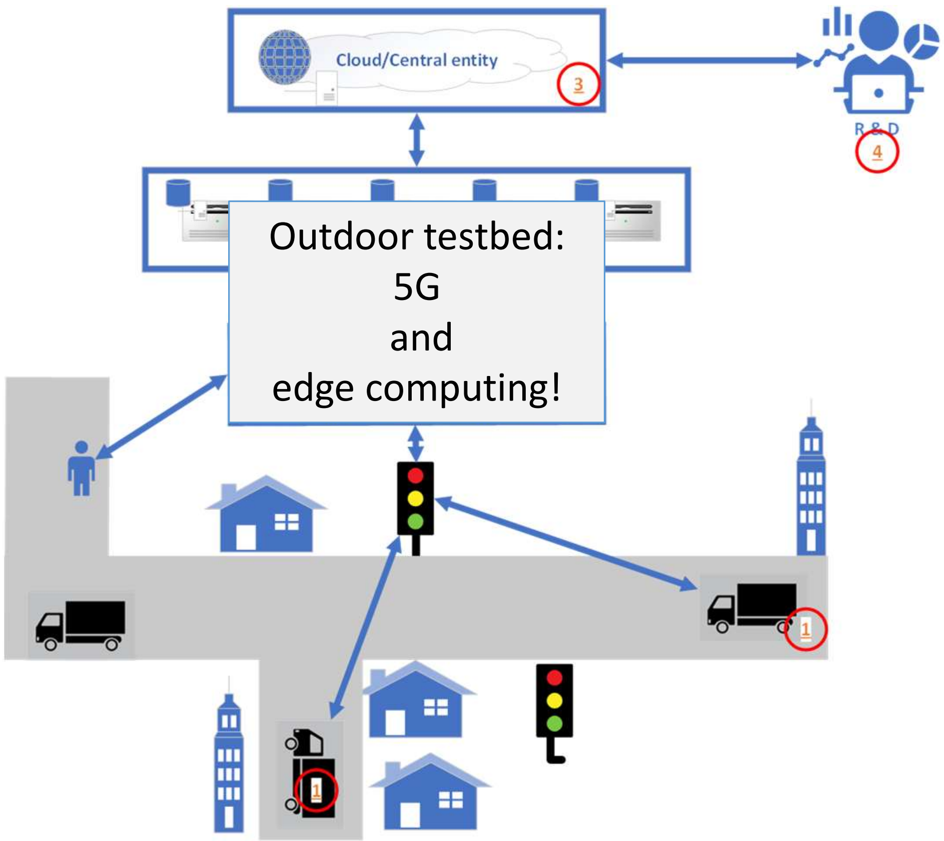
Tech-driven vs. Societal involvement
Cautionary vs. Innovation principles

TECoSA - Trustworthy Edge Computing Systems and Applications



Welcome Sept 1st to KTH!

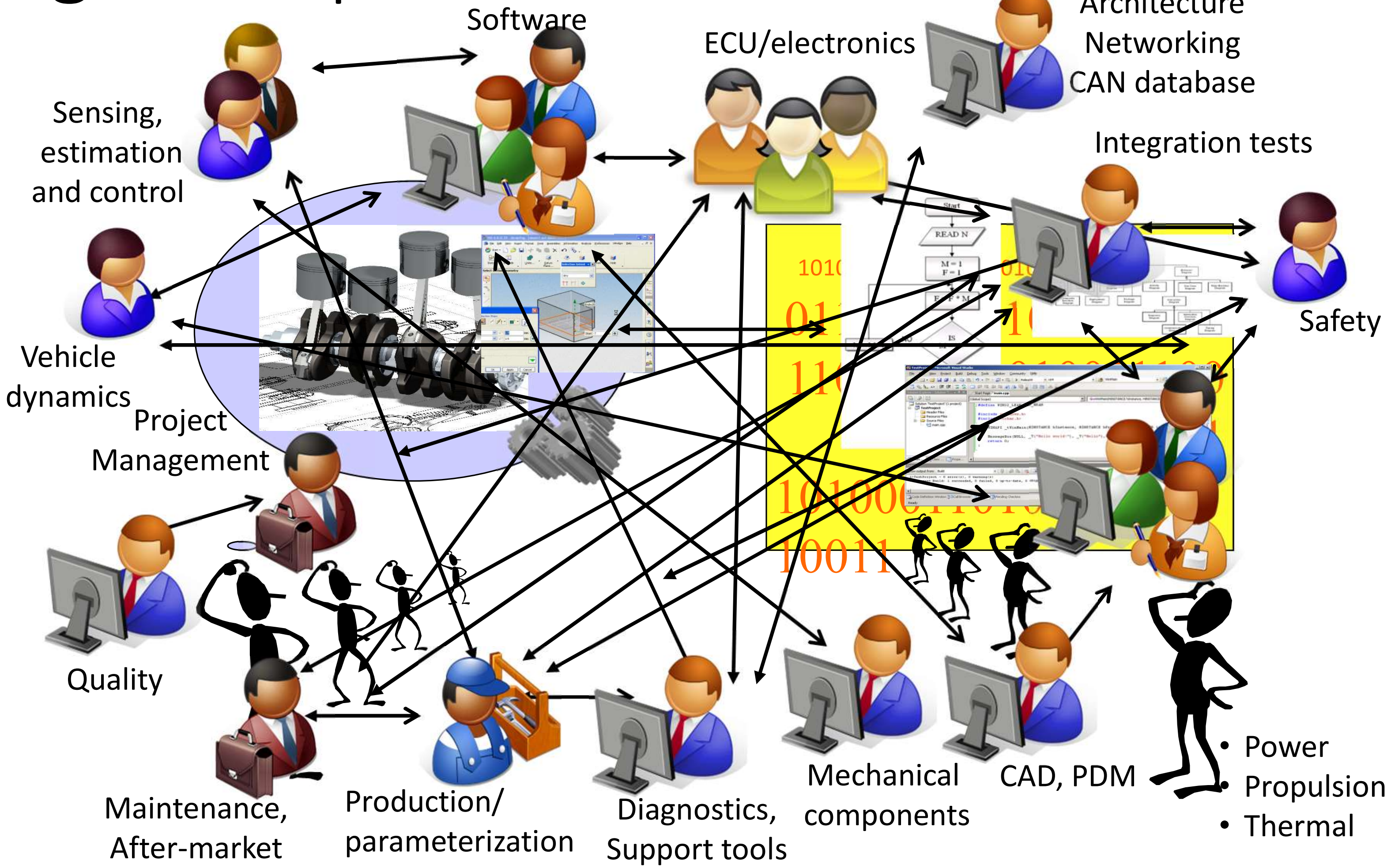
One flagship demonstrator: collaborative awareness and risk mitigation in road traffic



KTH campus, Stockholm

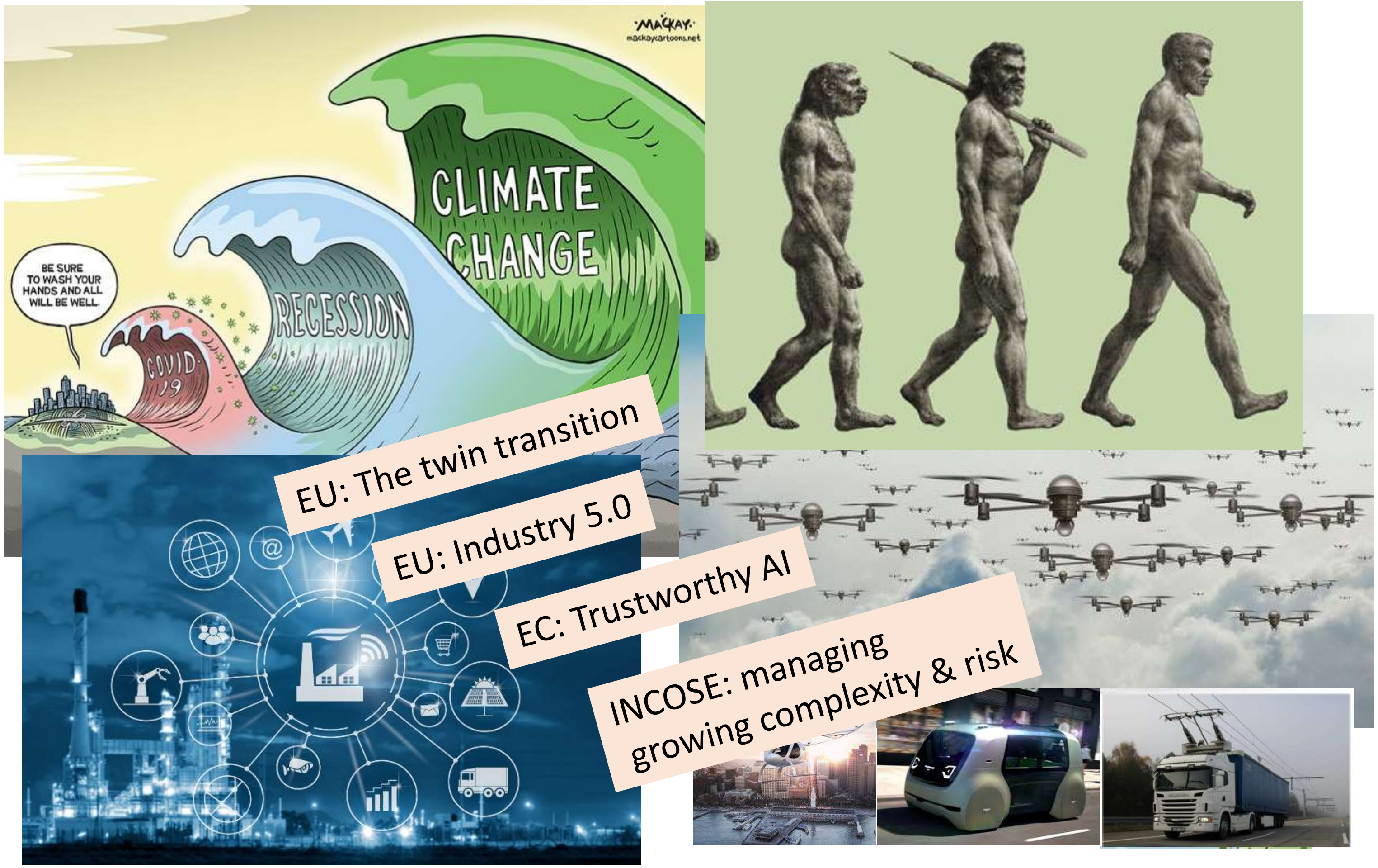
TECoSA
TRUSTWORTHY EDGE COMPUTING SYSTEMS & APPLICATIONS

Integration pasta



https://doi.org/10.1016/j.mechatronics.2013.11.013

Zooming out again



EU: The twin transition

EU: Industry 5.0

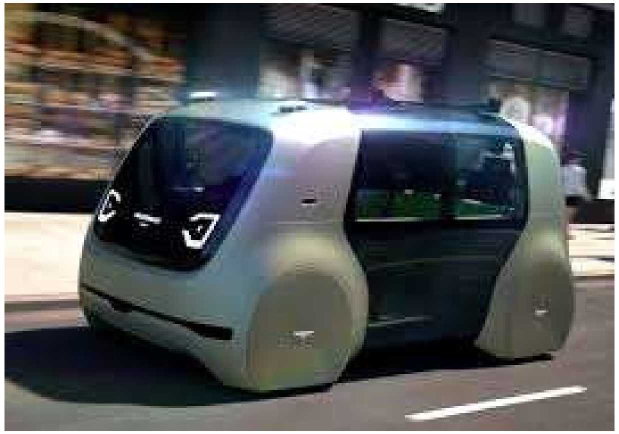
EC: Trustworthy AI

INCOSE: managing growing complexity & risk

Implications for (systems) engineering?

- Know your domain – Cynevin, and apply appropriate tools
- Apply systems thinking and SE principles but strengthening
  - Human-CPS interactions and concerns (all stakeholders)
  - Embrace but balance complexity
  - Key properties: Transparency, resilience, monitoring, human oversight, multiple aspects of trustworthiness and their trade-offs
  - Reconcile/integrate and balance perspectives on SW/Data as part of CPS
  - Architect to prepare for upgrading and circularity
- Need to address educational renewal and life-long learning
- Competence networks

So, when is an automated vehicle (AV) ready to go?



Positive risk balance (requires understanding residual risk) or the ALARP principle

Enablers
- Run-time risk monitoring (vehicle, edge, cloud)
- Complexity reduction, control and management
- Operational safety and performance
- New methodologies

Open question how to assess ”the common sense” for higher levels of automation

Contact: martint@kth.se - https://www.kth.se/profile/martint/