Virtual Verification for Autonomous Vehicles – focusing on safety

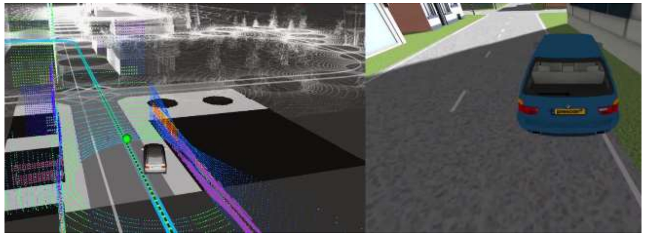
Martin Törngren

- Mechatronics and Embedded Control Systems, **KTH**

Collaborative work with Fredrik Asplund, Naveen Mohan, Masoumeh Parseh, José Gaspar Sánchez, Lars Svensson, Xin Tao, and Xinhai Zhang

KTH (Kungliga Tekniska Högskolan) – Royal Institute of Technology

- Sweden's largest technical University, 1827, Stockholm
  ~ 15000 students
- Architecting and Safety for Autonomous systems
  - Automated driving: Trucks, cars, forestry
  - AD-EYE simulation environment
  - Research concept vehicle



www.ices.kth.se (ICES competence network)

Perspectives to virtual verification – focusing on safety

Context of AVs and V-V challenges

Legislation, standards and metrics

Automated vehicle virtual verification

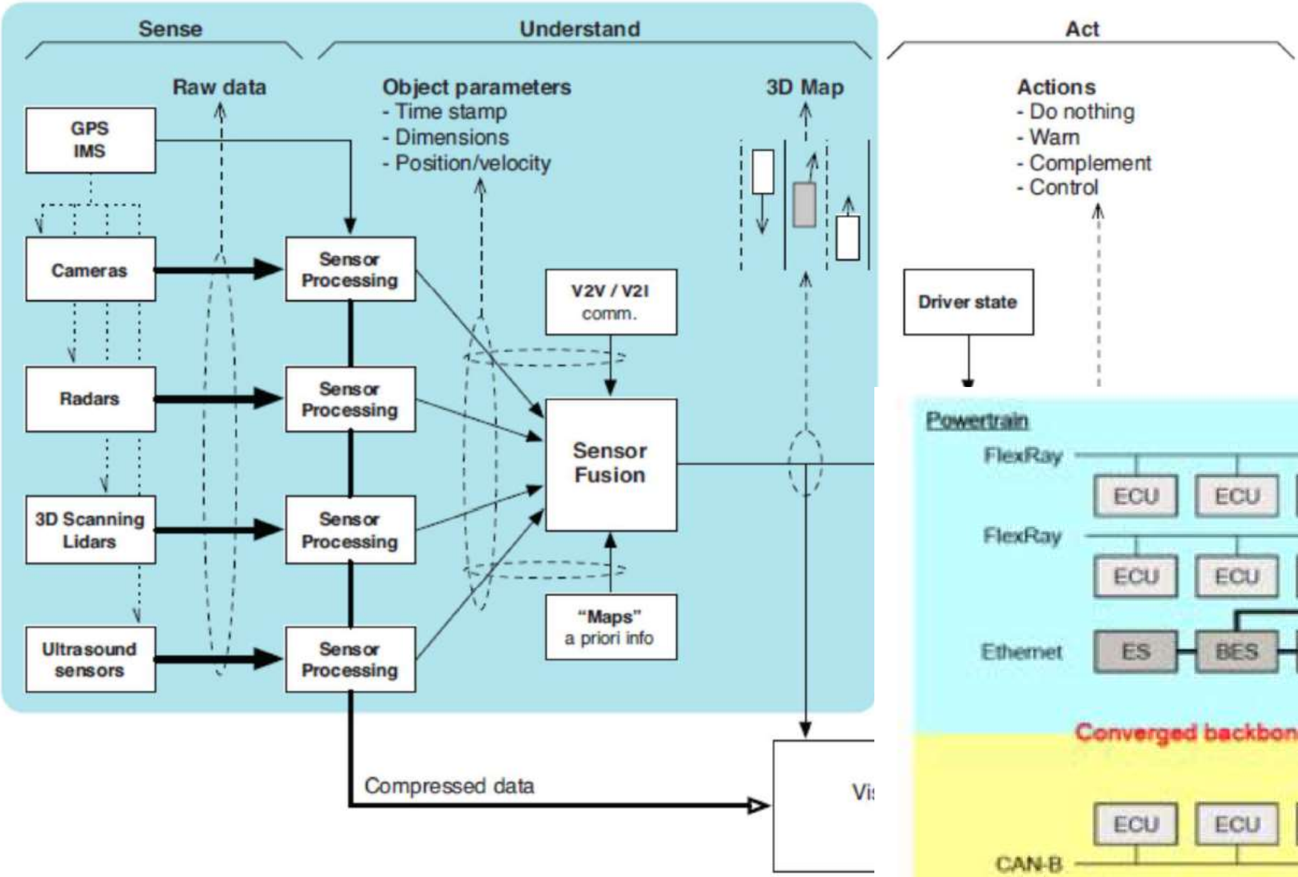
Virtual verification/

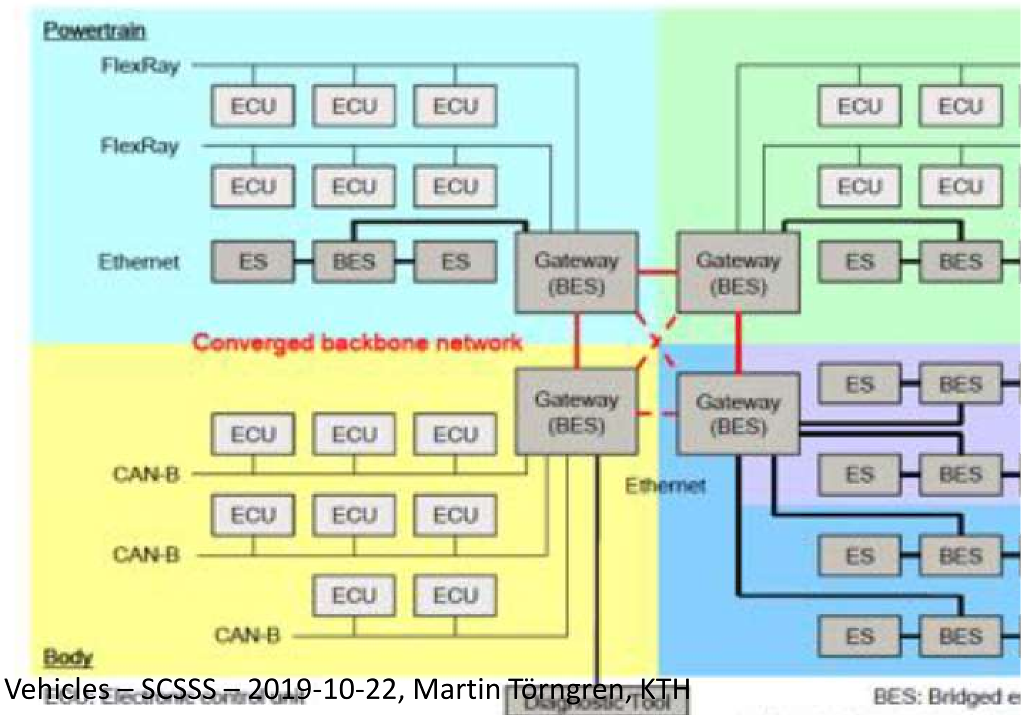
KTH research efforts - AD-EYE

Dealing with inherent dynamic risk

www.youtube.com/watch?v=HjtiiGCe1pE&feature=youtu.be

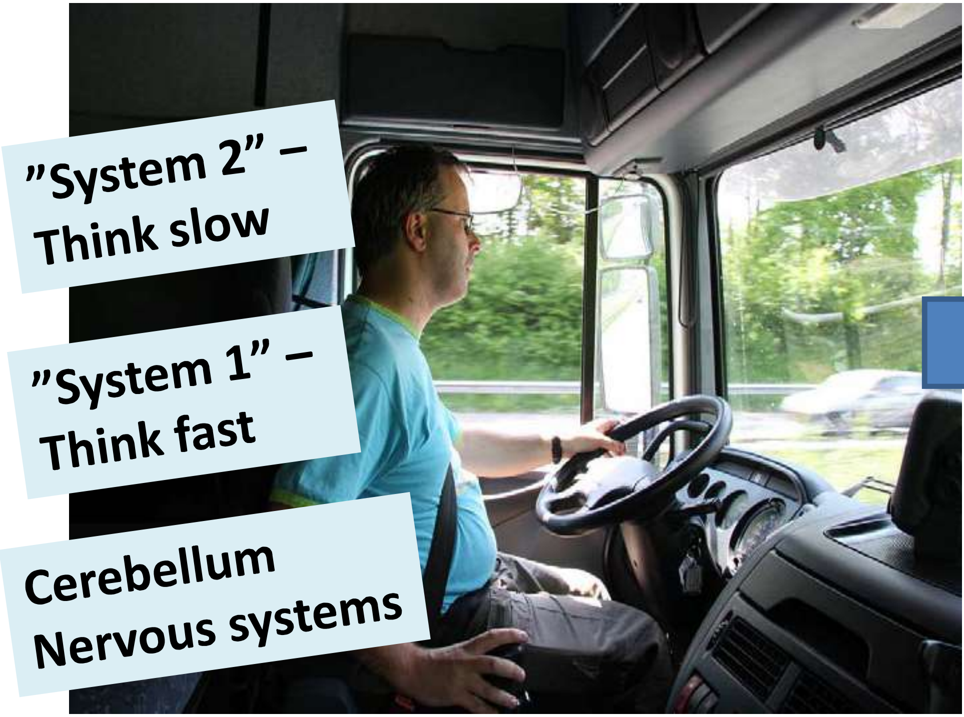
New ground: Unprecedented complexity and corresponding capabilities (1)





New ground – higher level reasoning (2)

ADI – Autonomous Driving Intelligence



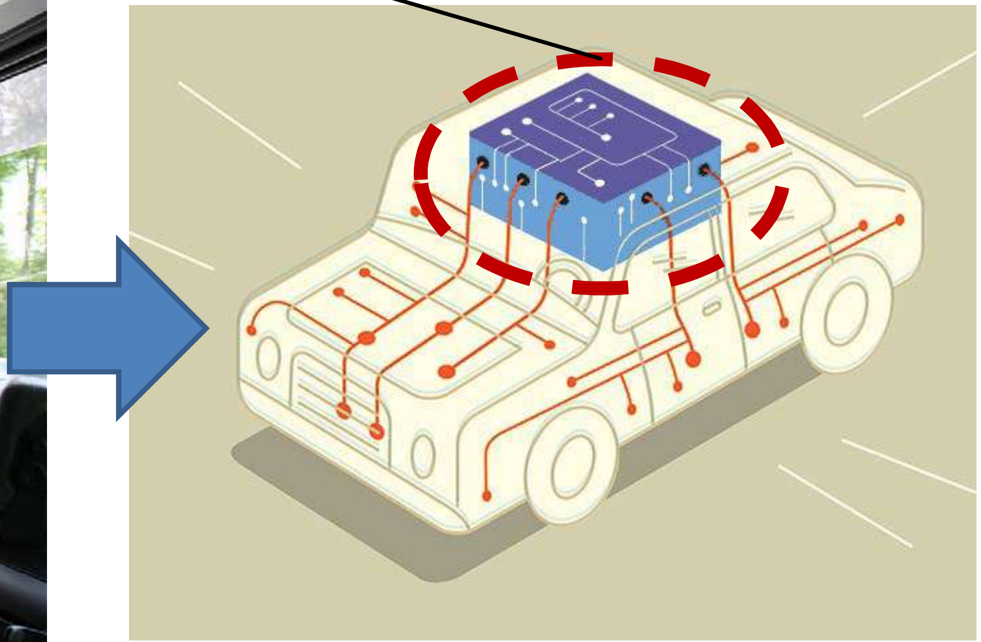


Illustration: Harry Campbell, IEEE Spectrum
http://spectrum.ieee.org/cars-that-think/transportation/self-driving/nxps-bluebox-bids-to-be-the-brains-of-your-car

When is verification "done" for an AV?

"Automated vehicles would have to be driven hundreds of millions of miles and sometimes even hundreds of billions of miles to demonstrate their reliability in terms of fatalities and injuries" (Kalra & Paddock, 2016)

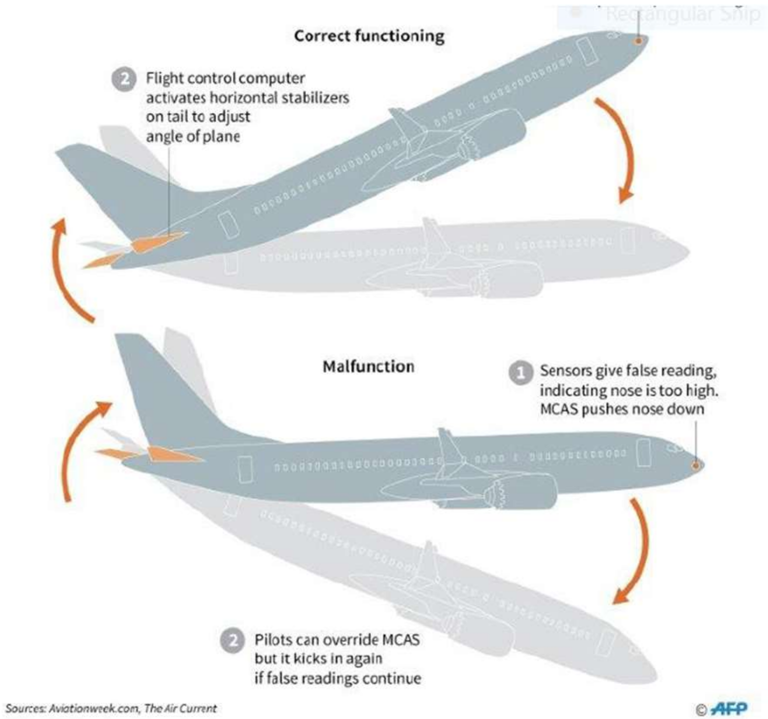
- Quality and coverage of the miles?
- Changing systems, and systems of systems

Safety/Assurance cases for AV's

"… a structured argument, supported by a body of evidence, that provides a compelling, comprehensible and valid case that a system is safe …"

- NASA System Safety Handbook ver. 1 (2014)

Boeing 737 MCAS

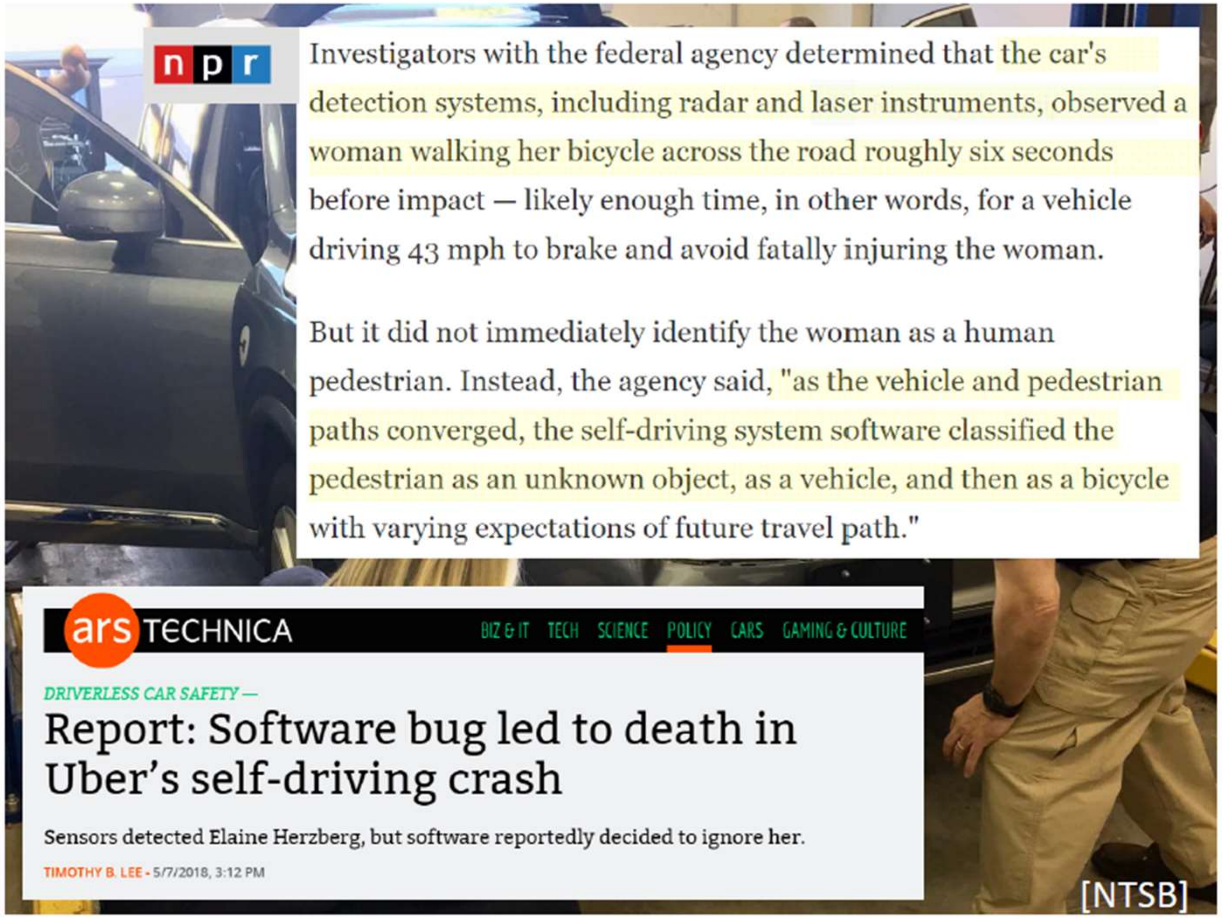


After two flight crashes:

A <u>compelling,</u> <u>comprehensible</u> and <u>valid</u> case?

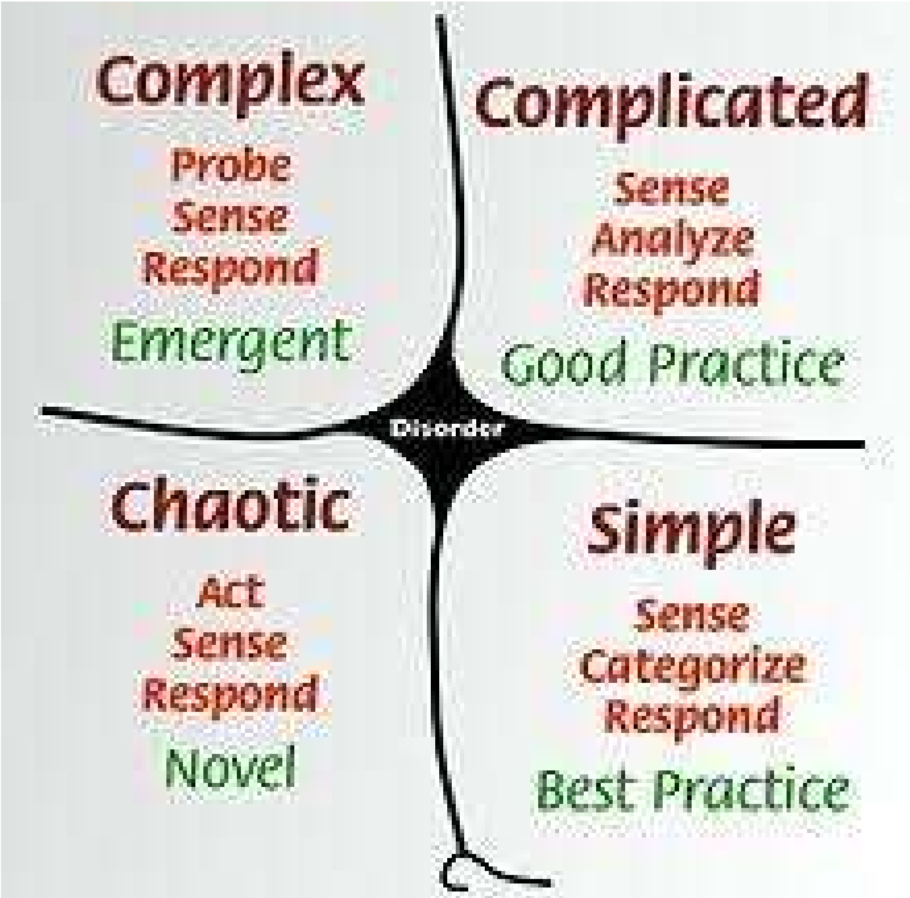
The Maneuvering Characteristics Augmentation System (**MCAS**) flight control law **was designed and certified** for the 737 MAX **to enhance the pitch stability** of the airplane – so that it feels and flies like other 737s (Source: Boeing).

Uber crash March 2018



A <u>compelling</u>, <u>comprehensible</u> and <u>valid</u> case?

Systems engineering insights and needs for new methodologies



Cynefin model

- ➔ complex environments and uncertainty
- ➔ composability - dependencies and side effects

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

Preliminary take aways

- Need for new verification methodologies!
- Scenario reasoning - underpinning the safety case
- Need to turn to design!
  - Architecture, functionalities and SoS providing resilience
  - "Simplicity is complex" (H. Kopetz)
- Unknowns drive updates: a safety life-cycle

Perspectives to virtual verification – focusing on safety

<u>Context of AVs and V-V challenges</u>

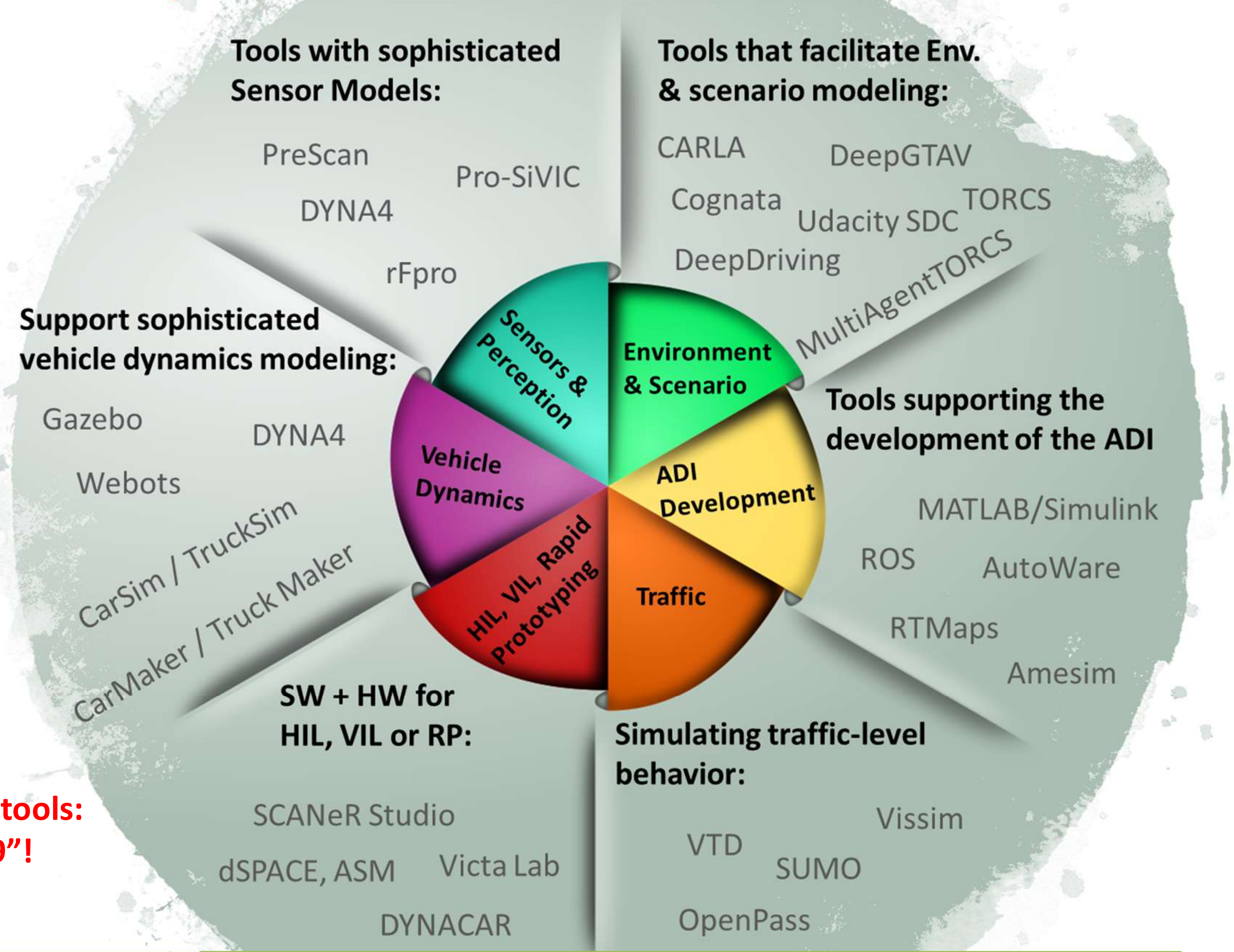
<u>Legislation, standards and metrics</u>

Automated vehicle virtual verification

<u>Virtual verification/</u>

<u>KTH research efforts - AD-EYE</u>

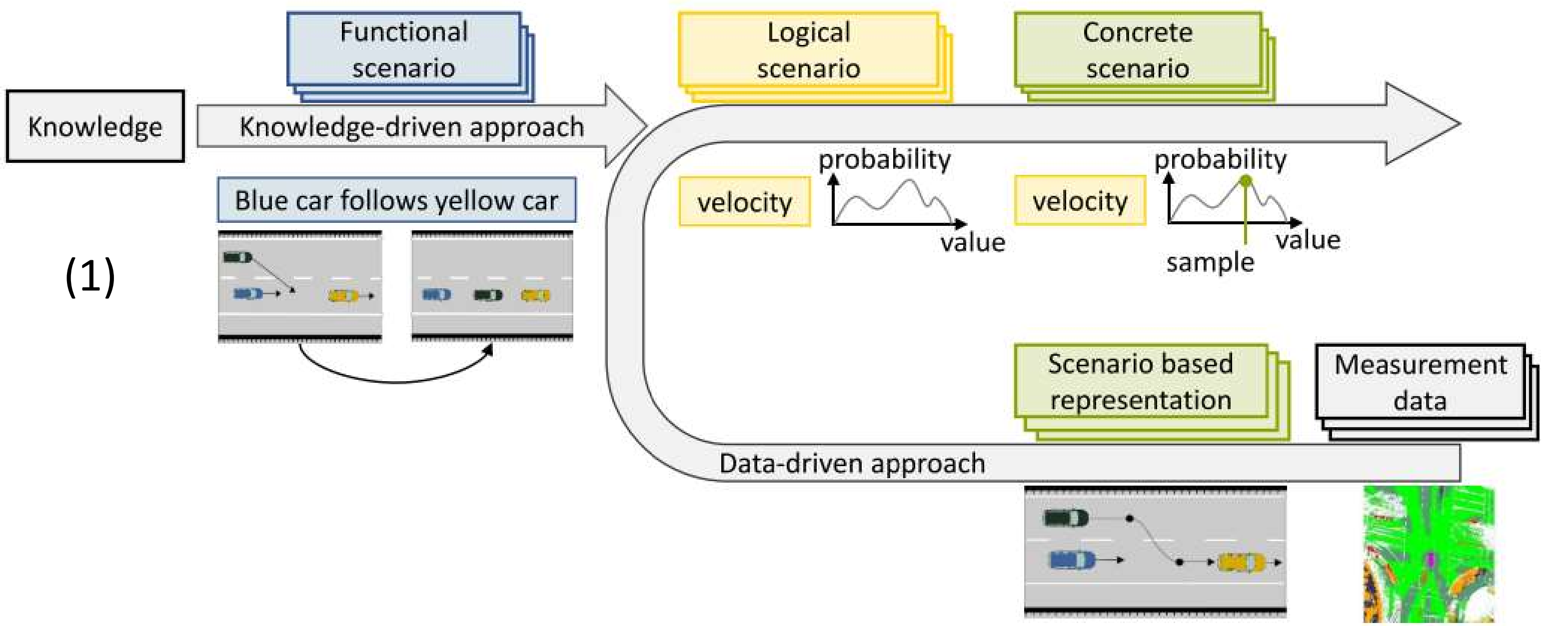
Modeling and simulation tools



KTH survey on Modeling & sim. tools: Dated: "Jan. 2019"!

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

Snapshots: state of the art on scenarios



Taxonomies, Catalogues, Schemas, Languages, Formats,

…

(2)

```
spot = OrientedPoint on visible curb
badAngle = Uniform(1.0, -1.0) * (10, 20) deg
Car left of spot by 0.5, \
    facing badAngle relative to roadDirection
```

(1): Menzel et al. (2019): From Functional to Logical Scenarios: Detailing a Keyword-Based Scenario Description …
(2): Fremont et al. (2018): Scenic: Language-Based Scene Generation

Hazardous events and standards

Source	Cause of hazardous event	Within scope of
System	E/E System failures	ISO 26262 series
	Performance limitations or insufficient situational awareness, with or without reasonably foreseeable misuse	ISO/PAS 21448
	Reasonably foreseeable misuse, incorrect HMI (e.g. user confusion, user overload)	ISO/PAS 21448 ISO 26262 series European statement of principal on the design of human-machine-interface
	Hazards caused by the system technology	Specific standards
External factor	successful attack exploiting vehicle security vulnerabilities	ISO 21434[a] or SAE J3061
	Impact from active Infrastructure and/or vehicle to vehicle communication, external devices and cloud services.	ISO 20077 series; ISO 26262 series
	Impact from car surroundings (other users, "passive" infrastructure, environmental conditions: weather, Electro-Magnetic Interference…)	ISO/PAS 21448 ISO 26262 series

[a] Under preparation. Stage at the time of publication: ISO/SAE CD 21434

Source: Overview of safety-relevant topics addressed by different ISO standards (Source: ISO 21448)

Approaches to scenarios (intermediate summary from ongoing KTH study)

Tasks\"Drivers":	Data	Models	Knowledge
"Gathering/ Identifying	Real-world data, databases (accidents)	Simulation Exploration/ synthesis tools	Brainstorming Structured analysis (e.g. safety analysis) Checklists
Refinement	Analysis and synthesis tools ⟷		Manual refinement
Representation	XML, Open drive, Open scenario, Scenario description languages, …		

Further state of the art observations (from ongoing KTH study)

- Scope of scenarios (environment/internal; event types)
  - External factors: environment, ODD, uncertainties, ...
  - Internal factors: Functionalities, data, and technology performance limitations/uncertainty; faults/failure modes
- Strive for higher levels of abstraction and automation
- Scenario + model expressiveness vs. Tractability
- Other and combined factors
  - Interactions, emergence
  - Metrics (risks, robustness, sensitivity)

Lessons learnt in model-based systems engineering

- **Learning from models by focusing on specific properties**
  - Accurate enough modeling for predictions, enquiry, training
  - Models (e.g. scenarios) for synthesis
  - Simplicity, Tractability, Accuracy, Precision, Robustness, Generality
  - Choice of formalisms and abstractions (viewpoints to tools)
- **Models become complex systems in their own right**
  - Model management: rationale, assumptions, versions, …
  - Models have components and architectures
  - Attention to federated modeling, dependencies, concurrent usage and dependability

Solomon Wolf Golomb on Modeling

Don’t apply a model until you understand the **simplifying assumptions** on which it is based and can test their applicability.

Distinguish at all times between the model and the real world. You will never strike oil by drilling through the map!

”Mathematical Models: Uses and Limitations” – Solomon Wolf Golomb, April 70:

”Essentially all models are wrong, some are useful”, Box and Draper, 1987
“Essentially, all system implementations are wrong, but some are useful.” Lee and Sirjani!

Perspectives to virtual verification – focusing on safety

Context of AVs and V-V challenges

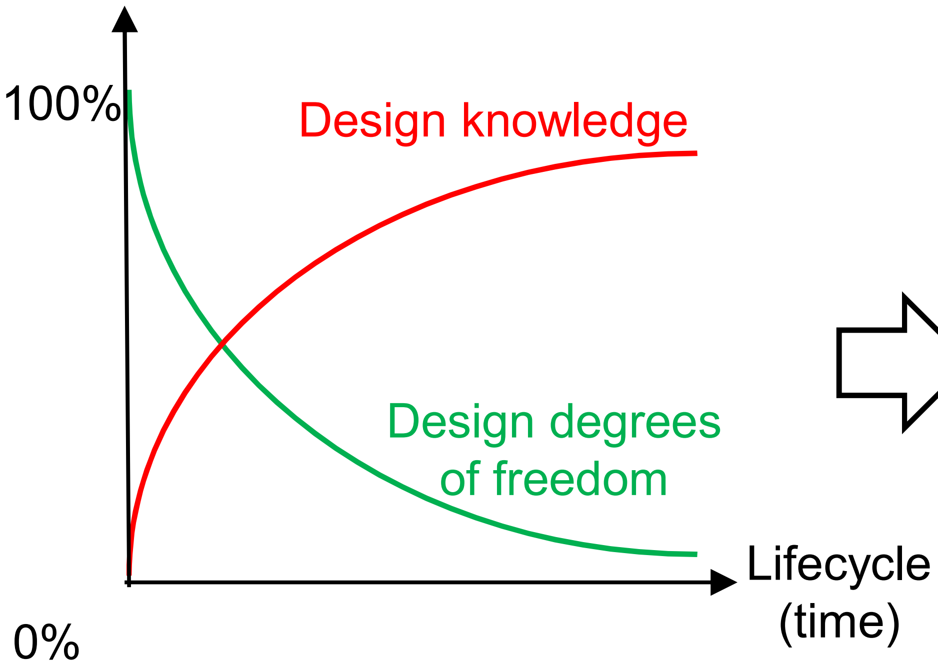
Legislation, standards and metrics

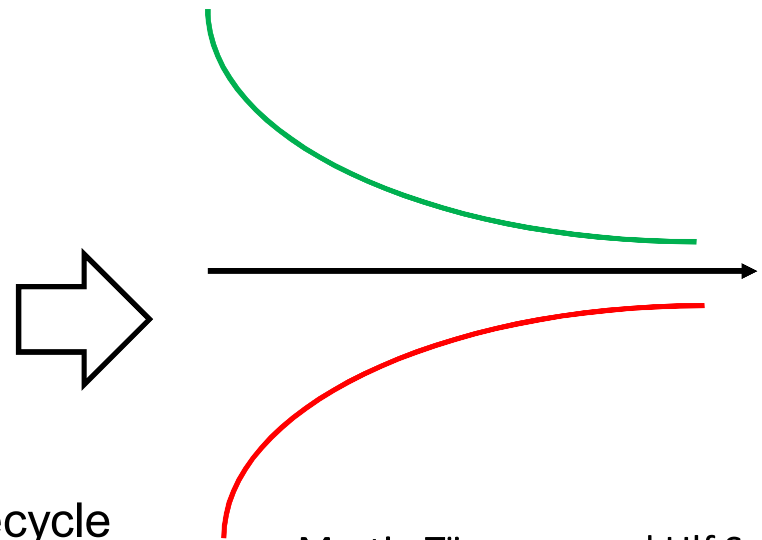
Automated vehicle virtual verification

Virtual verification/

KTH research efforts - AD-EYE

Managing an increasing cone of uncertainty

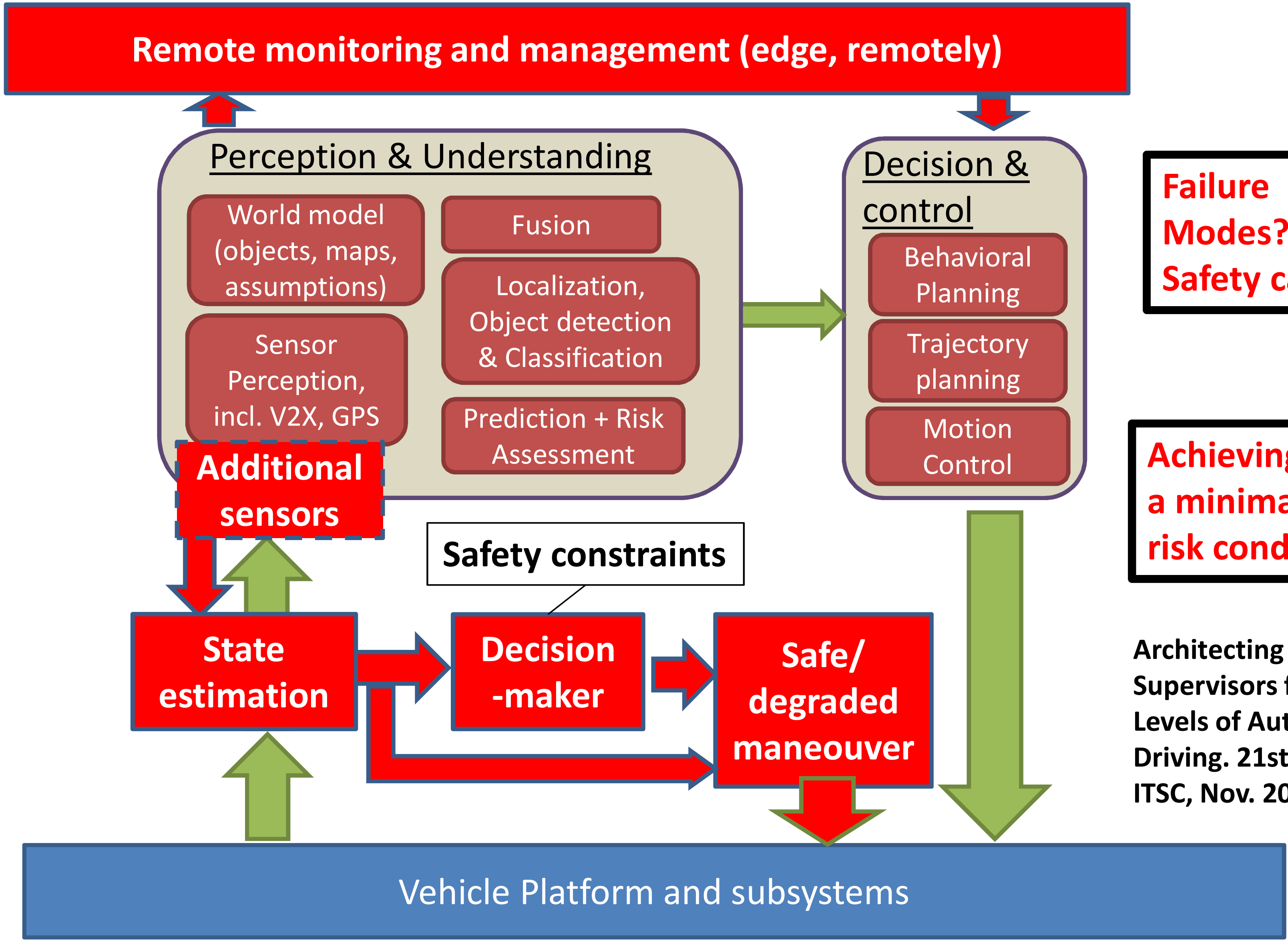




Martin Törngren and Ulf Sellgren. Complexity Challenges in Development of Cyber-Physical Systems. In Principles of Modeling (Springer, July 2018)

- **Uncertainties in system and environment**
- **Resilience; fault-tolerance; survivability**
- **Operational risk management at system and SoS level**

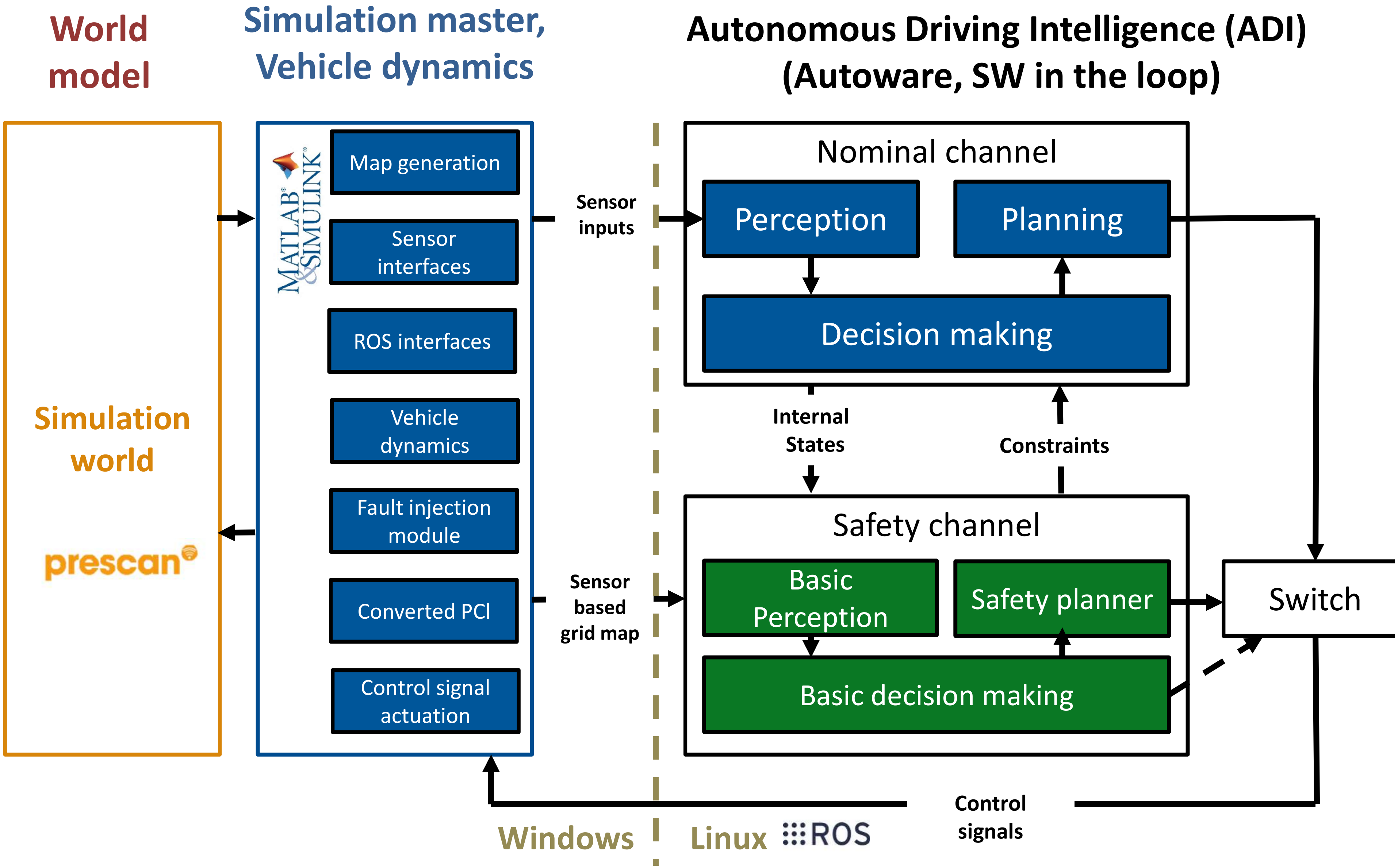
Automous safety supervisor architectures



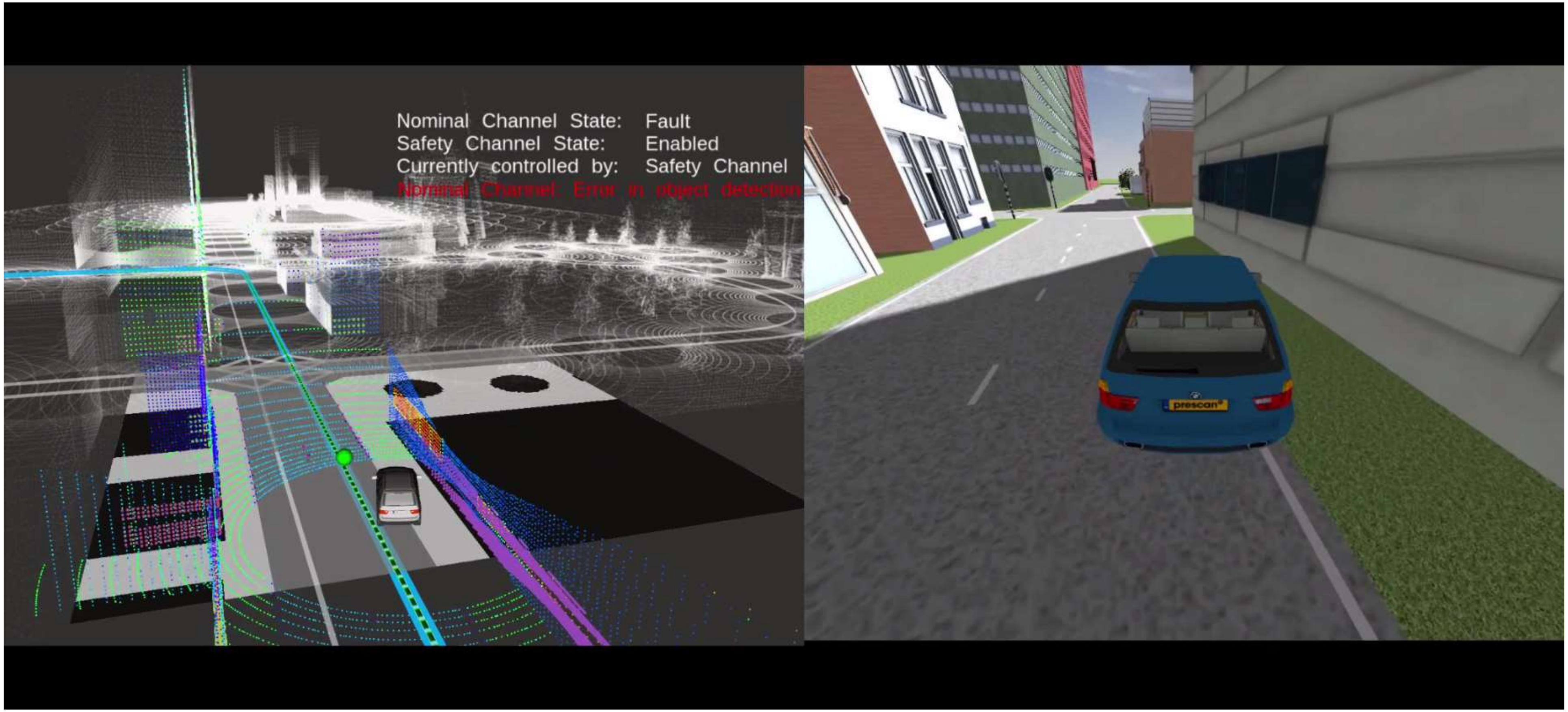
Failure Modes? Safety case?

Achieving a minimal risk condition

Architecting Safety Supervisors for High Levels of Automated Driving. 21st IEEE ITSC, Nov. 2018


World model
Simulation master, Vehicle dynamics
Autonomous Driving Intelligence (ADI) (Autoware, SW in the loop)
Simulation world
prescan
MATLAB & SIMULINK
Map generation
Sensor interfaces
ROS interfaces
Vehicle dynamics
Fault injection module
Converted PCI
Control signal actuation
Sensor inputs
Sensor based grid map
Nominal channel
Perception
Planning
Decision making
Internal States
Constraints
Safety channel
Basic Perception
Safety planner
Basic decision making
Switch
Control signals
Windows
Linux
ROS

AD-Eye simulations – a taster



AD-EYE: read more here: https://tiny.cc/adeye

Take aways

- Need for new methodologies
  - Abstraction levels; Model and method combinations
  - Reasoning about scenarios – crucial for the safety case
  - Uncertainty drives updates: a safety life-cycle
  - Architecting at vehicle and system of system level
    - Resilience; ”Simplicity is complex”
- KTH work on automated safety supervisor architectures and their evaluation
  - AD-Eye simulation environment: **https://tiny.cc/adeye**

References and further reading

- Naveen Mohan and Martin Törngren. **A practical simulation toolchain for the early verification of Functional Safety Concepts**. Accepted for SAE World Congress, 2019.
- 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; Lohstroh, M.; Derler, P.; Sirjani, M., Eds.; 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 Transportation Systems, Nov. 2018.
- Lars Svensson et al. **Safe Stop Trajectory Planning for Highly Automated Vehicles**. IEEE Int. Vehicles Symposium, 2018
- Naveen Mohan et al. **ATRIUM - Architecting Under Uncertainty**: For ISO 26262 compliance. IEEE SysCon 2017.
- Naveen Mohan et al. **A Method towards the Systematic Architecting of Functionally Safe Automated Driving**, Leveraging Diagnostic Specifications for FSC design. SAE Automotive World Congress,2017
- Sagar Behere and Martin Törngren. **A functional reference architecture for autonomous driving**. J. of Information and Software Technology, 2016. Elsevier.
- Xinhai Zhang et al. **Architecture Exploration for Distributed Embedded Systems**: A Gap Analysis in Automotive Domain. 12th IEEE Int. Symposium on Industrial Embedded Systems.