ARCHER project perspectives, and reflections from the "Software certification consortium meeting"

Martin Törngren, KTH, Stockholm, Sweden

Funding acknowledged from Vinnova and ECSEL/H2020

Assurance cases and managing risk

Assurance cases: a documented body of evidence that provides a convincing and valid argument that a system is adequately dependable …

Assurance cases - applied to one or more trustworthiness properties

Risk – severity of outcome and probability:

- Risk reduction measures design-time
- Risk assessment and management run-time

Assurance case

- Why are these all hazards and hazardous situations?
- Why are these causes of hazardous situations?
- Why are these risk control adequate for risk reduction?
- Why are these risk controls implemented properly?

Software certification consortium meeting, Annapolis, May 10-11, 2018

FUNDAMENTALS OF EFFECTIVE ASSURANCE CASES

- What does it mean?
- Philosophy
- Best practices,
- Who should do it?
- Standards and formalisms
  - Structured assurance case meta-model; SACM2.0
- Role and practices of assessors, e.g. FAA and FDA

Fundamentals of effective assurance cases (SW certification consortium meeting)

Keys and challenges

- 1000's of years of engineering, vs. 100 years for SW
  - Culture? Lack of accountability and accreditation
- Methodology and mindset
  - Bias; critical thinking vs. doing the paperwork right?!
  - Balancing cost and rigor, incentivize "rigor"
  - Multidomain expertise; collaboration and humility is key
- Handling masses of heterogeneous distributed data

Fundamentals of effective assurance cases (SW certification consortium meeting)

- Panel debates – and their claims:
  - "Goal/claim de(composition) is well addressed in the current safety assurance case practice"
  - "This house believes that attempting to quantify confidence does more harm than good"

Voting at the panel provide a sounding No (or at least – not without significant challenges), and Yes, to the two claims respectively

Three challenges

1. **Multidisciplinary, evolutionary, distributed …**
   - Cyber-physical systems, heterogeneity – knowledge, data, systems …

   Efforts: Data and organizational structure/integration

2. **Formulating, designing and validating assurance cases**
   - a mix of quantitative and qualitative arguments/evidences

   Partly feasible: +reuse/patterns, - validation of risk reduction

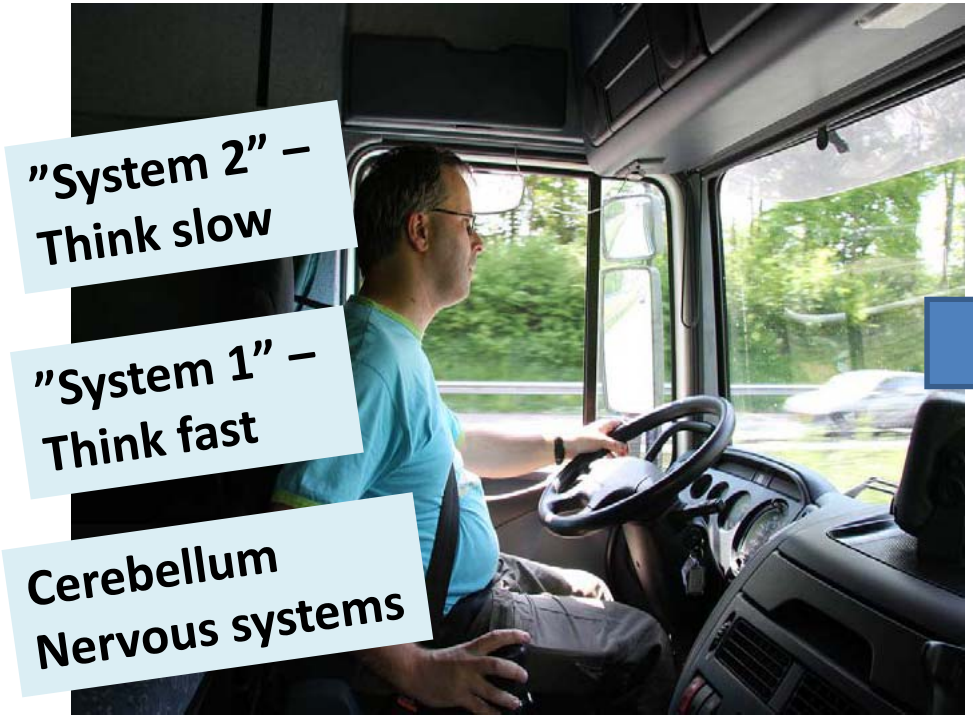
3. **Safety assurance in the era of smart CPS**
   - Open world, uncertainty, safety of intended functionality
   - What makes a useful safety case for automated vehicles?

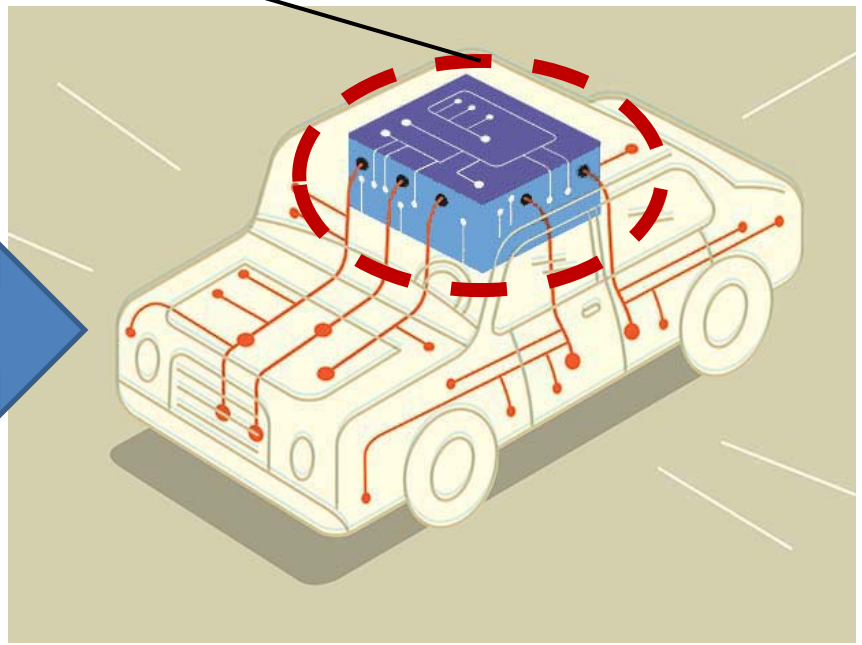
   Breaking new ground

Breaking new ground (1)
– no longer a closed world assumption

Breaking new ground (2) – 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

Breaking new ground (3) – unprecedented complexity in "everyone's hands"

ADI – Autonomous Driving Intelligence

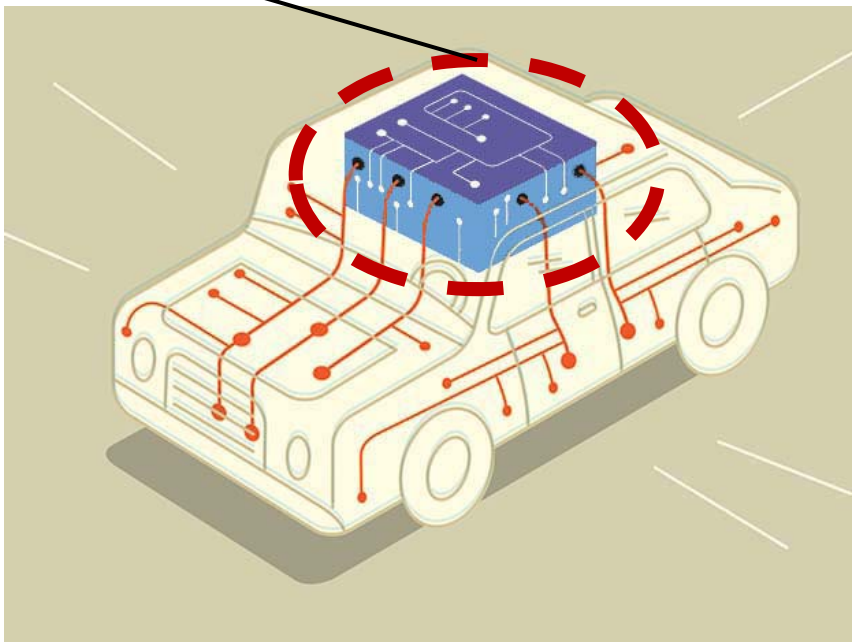
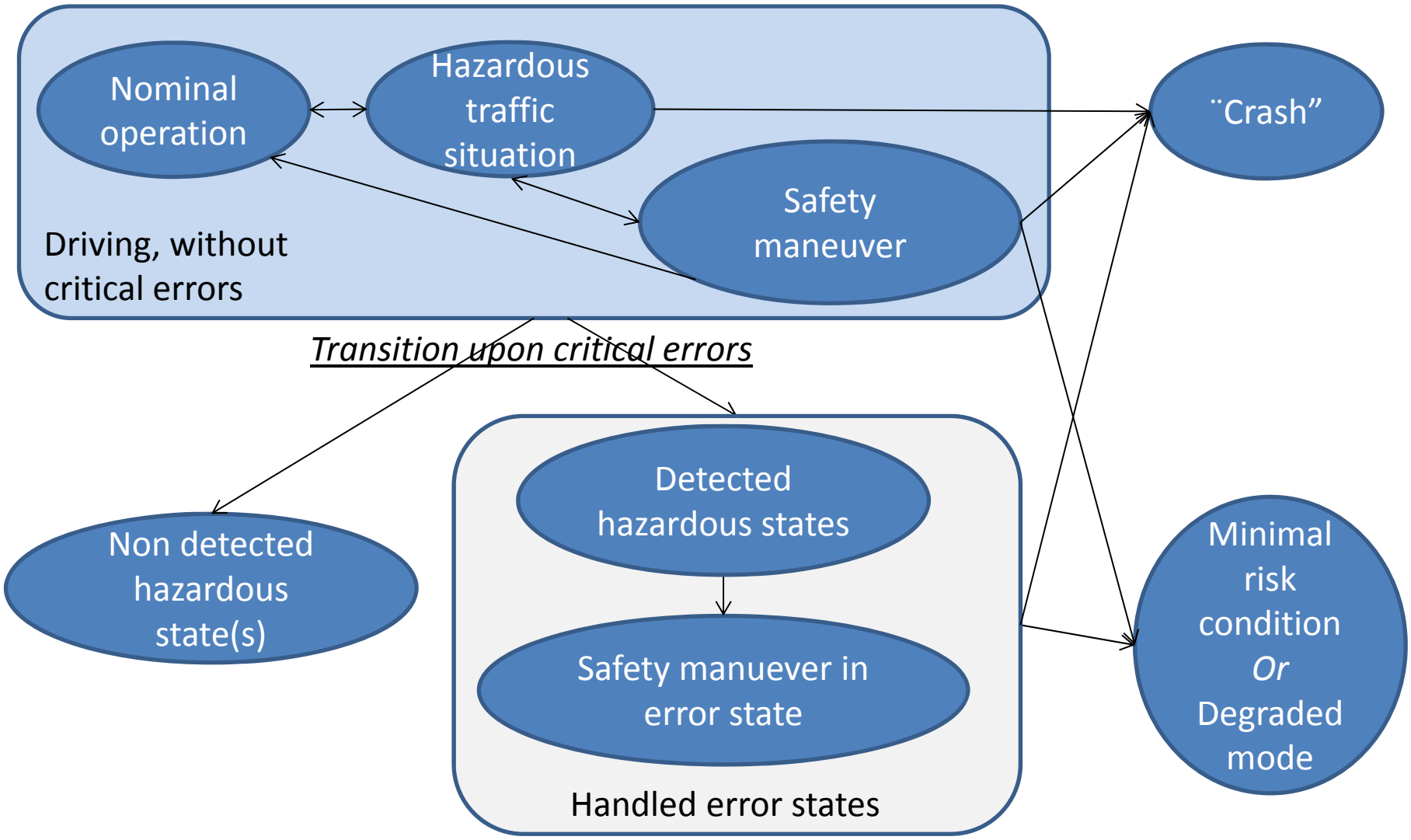


Illustration: Harry Campbell, IEEE Spectrum
http://spectrum.ieee.org/cars-that-think/transportation/self-driving/nxps-bluebox-bids-to-be-the-brains-of-your-car

Hazards and errors to consider



Archer/Prystine research project

- High levels of automation for heavy trucks
- Focus topics:
  - Dynamic risk management
    - Metrics, control approaches
  - Architecting and architectures
    - Safety supervisors, methodology
  - Verification and validation
    - Scenario languages and coverage
  - Variability
- Prystine: a larger EU-project addressing fault-operational concepts for perception and

ARCHER: www.kth.se/en/itm/inst/mmk/avdelningar/mda/mekatronik/systemarkitektur/archer-1.596547