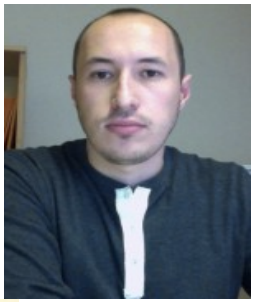
Cooperative functions in safety-critical System-of-Systems scenarios

Safe Cooperating Cyber-Physical Systems
using Wireless Communication | SafeCOP

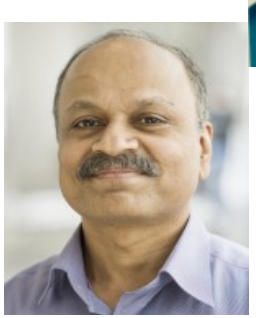
Cooperative functions in safety-critical System-of-Systems scenarios

- Introduction [Hans Hansson, MDH]



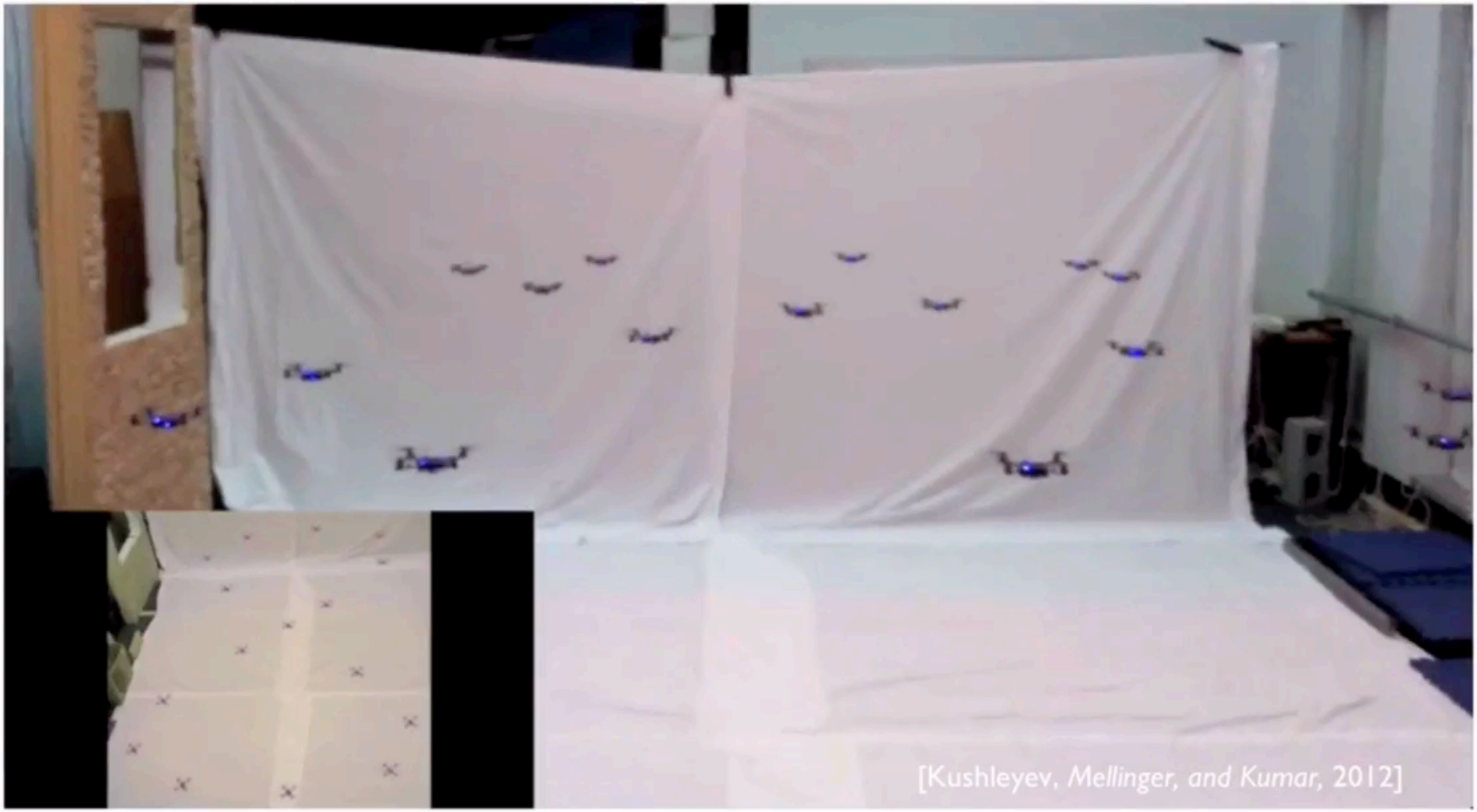
- Facing design and assurance challenges of security-informed safety critical vehicle platoons via FLAR2SAF [Irfan Sljivo, MDH]

- CO-CPS: A sample XSTAMPP usage in V2I traffic management scenario based on STAMP model [Leonardo Napolitano, RO Technology]



- Panel/Discussion [Sasi Punnekkat, MDH]

Cooperative functions?


[Kushleyev, *Mellinger, and Kumar,* 2012]

Systems-of-systems (SoS)

Characterization by Maier[1]

1. **Operational independence** of the elements. The constituent systems can operate independently in a meaningful way, and are useful in their own right.
2. **Managerial independence** of the elements. The constituent systems not only can operate independently, but they do operate independently even while being part of the SoS. They are acquired separately.
3. **Evolutionary development**. The SoS does not appear fully formed, and functions and purposes are added based on experience.
4. **Emergent behavior**. The principle purposes of the SoS are fulfilled by behaviors that cannot be localized to any individual constituent system.
5. **Geographical distribution**. The constituent systems only exchange information and not substantial quantities of mass or energy.

Maier, M. W. (1996). Architecting Principles for Systems-of-Systems. INCOSE International Symposium, 6(1), 565–573

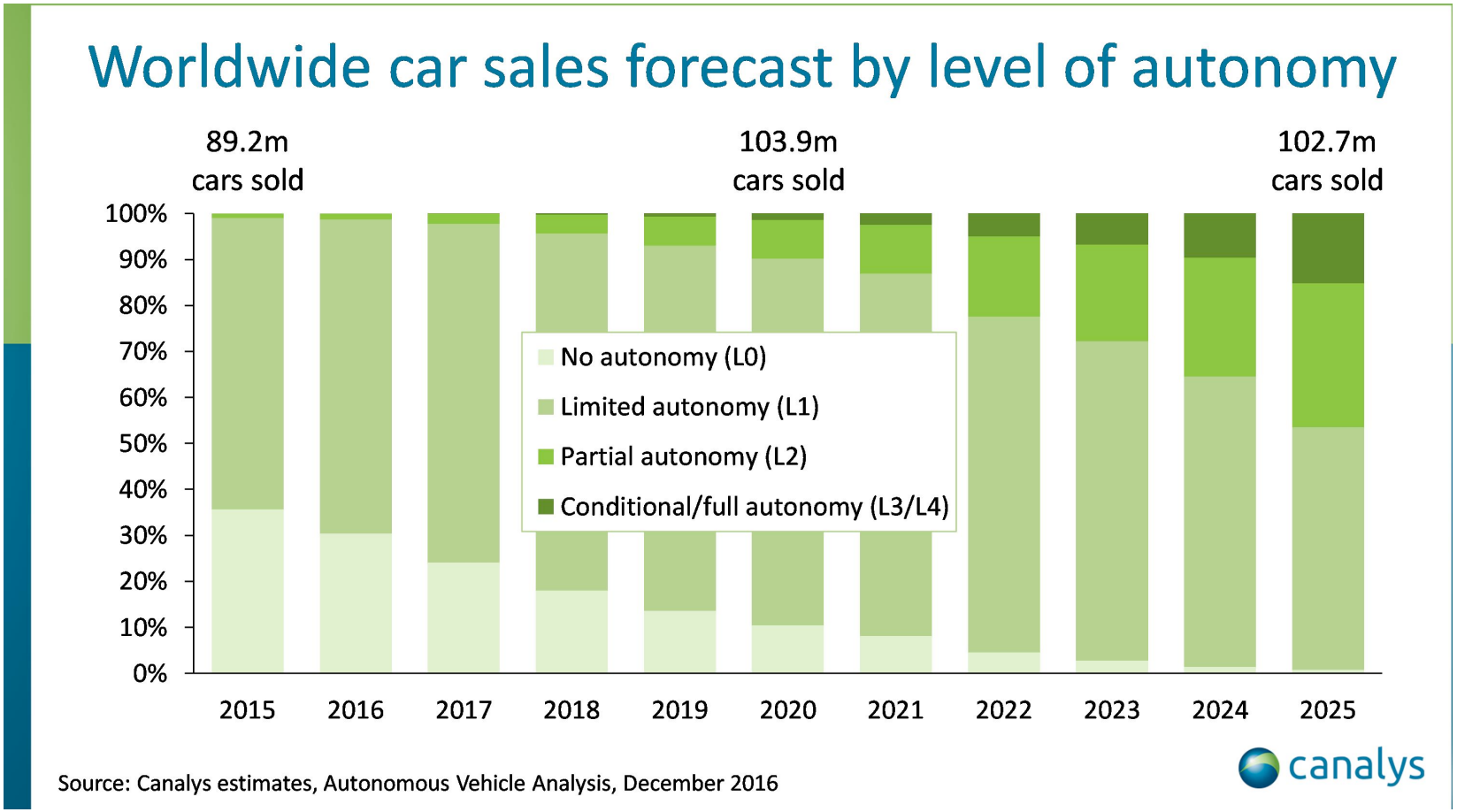
Collaborative robotics

- Market size and growth
  - Industrial robotics market: USD 79.58 Billion by 2022
    - CAGR (Compound Annual Growth Rate) of **11.92%** in 2016-2022.
  - Collaborative robots market: USD 3.3 Billion by 2022
    - CAGR of **60.04%** in 2016-2022
  - Service robotics market: USD 23.90 Billion by 2022
    - CAGR of **15.18%** in 2016-2022.
  - Medical Robotics market: USD 12.80 Billion by 2021
    - CAGR of **21.1%** in 2015-2021.

Sources: www.eurogip.fr/en/eurogip-infos-news?id=4436; www.marketsandmarkets.com/Market-Reports/

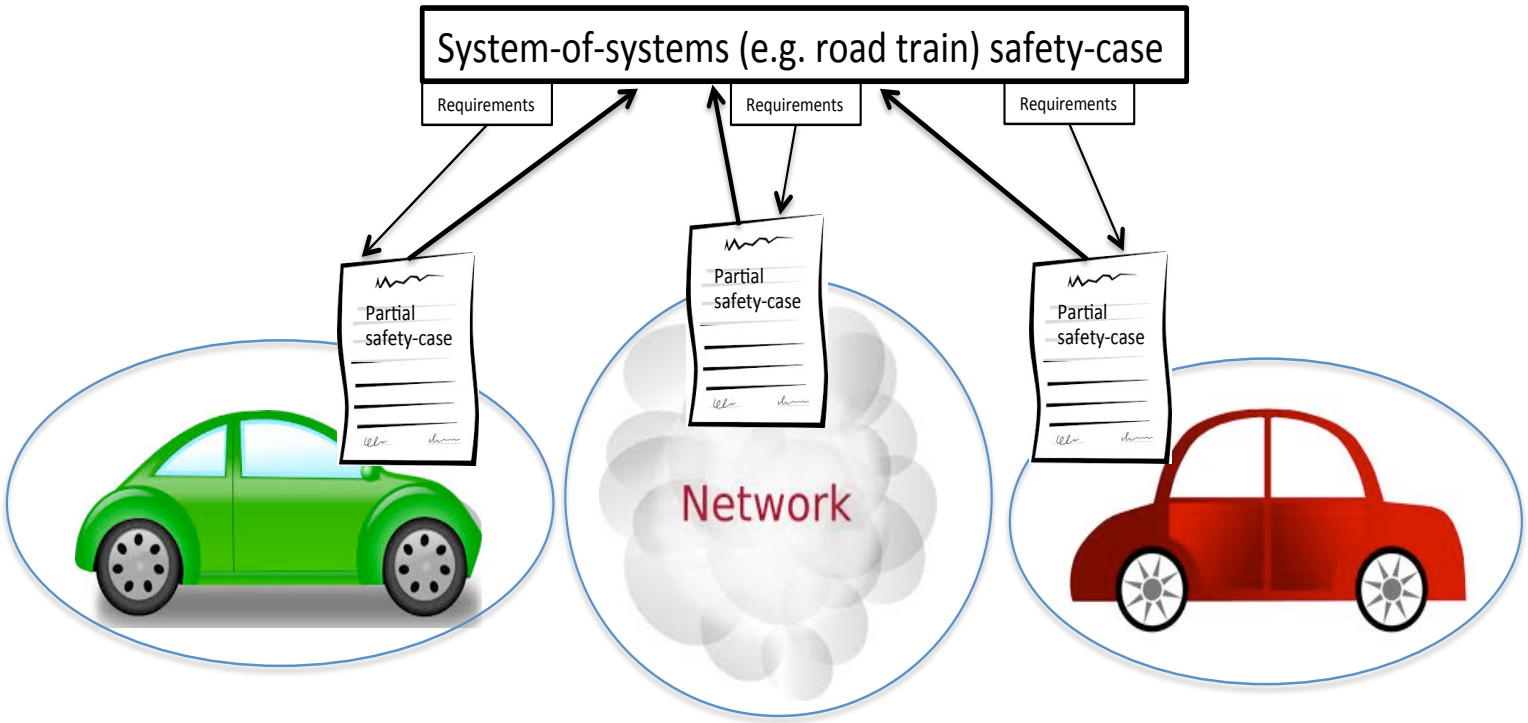
Self-driving cars are here…

- Single vehicle Autonomous Driving (AD) is here.




Platooning
PLATOONING
0:02 / 2:12
HD

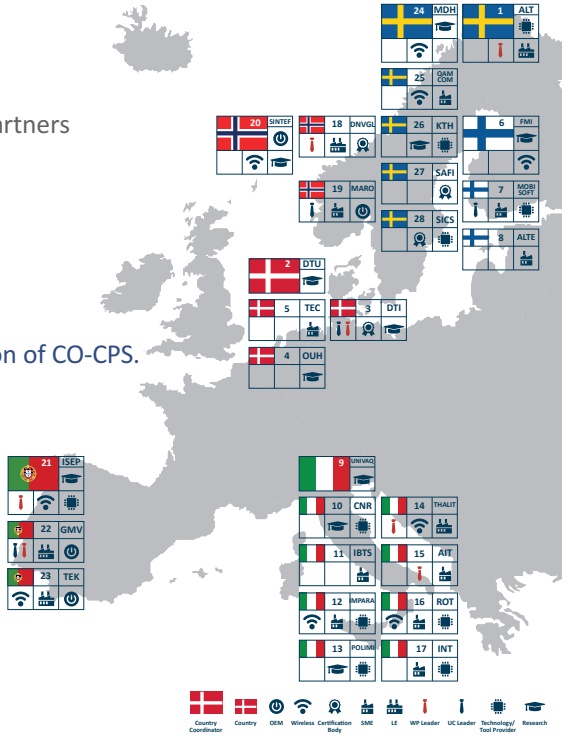
A hierarchical safety-cases



SafeCOP—ECSEL 2016-2019, 28 partners, 5 countries ~11 M€ EU budget, ~1,300 PMs

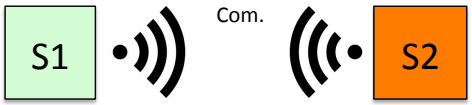
Safe Cooperating Cyber-Physical Systems (CO-CPS) using Wireless Communication

Partners



Objectives

- Develop a safety-assurance framework for CO-CPS.
- Develop a reference platform to support the engineering and certification of CO-CPS.
- Extend the current wireless protocols for safe & secure cooperation.
- Contribute to new standards and regulations.
- Demonstrate the usefulness of SafeCOP concepts in target applications.



Cooperative Open Cyber-Physical Systems (**CO-CPS**)

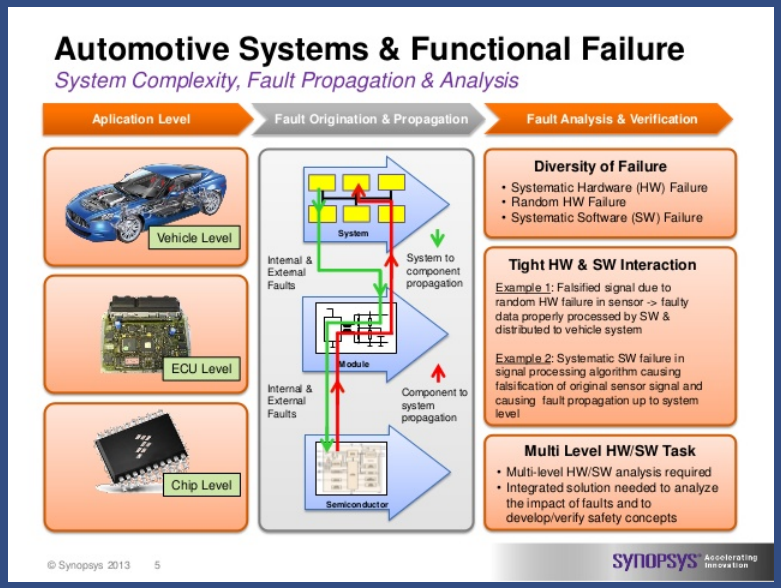
UC1. Cooperative moving of empty hospital beds	UC2. Cooperative bathymetry w/ boat platoons	UC3. Vehicle control loss warning	UC4. Vehicles and roadside units interaction	UC5. V2I cooperation for traffic management
				

Safety-assurance framework for CO-CPS

- **Now**: standards and practice do not address CO-CPS
  - SafeCOP will influence practice and standards
- **Impact & long-term effects**:
  - Enabler for deployment of cooperative functions
  - Enabler for dynamic assurance/certification in general (e.g. for basic AD)
  - Assist in closing the gap between standards and technical development

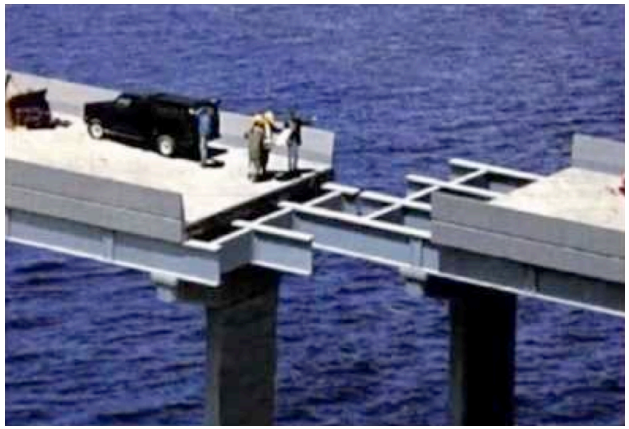
ISO 26262 – “stress testing”

Certification for Products
in accordance with
ISO 26262



Cooperative CPS are complex

- Unanticipated behaviours makes design-time safety assurance insufficient

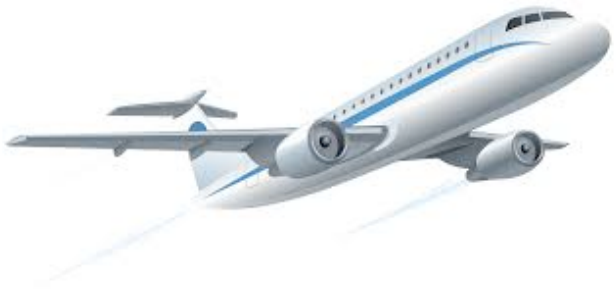


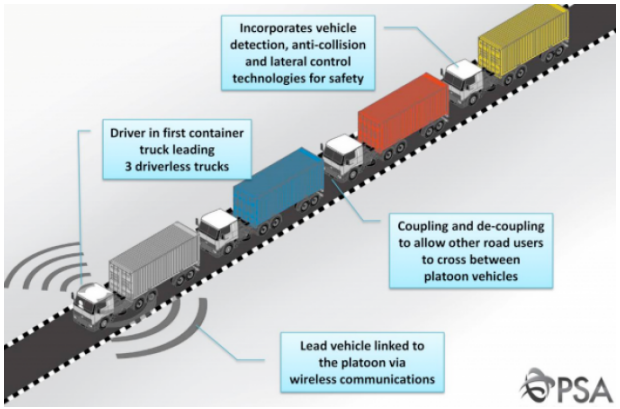
- Run-time assurance required for acceptably safe cooperative functions (or even basic AD)

Autonomy followed by cooperative functions

- Increased customer and societal value
- Challenging from safety and security perspectives
  - Multiple stake-holders responsible for safety-critical functions
  - Dynamic configuration and ”open” interfaces

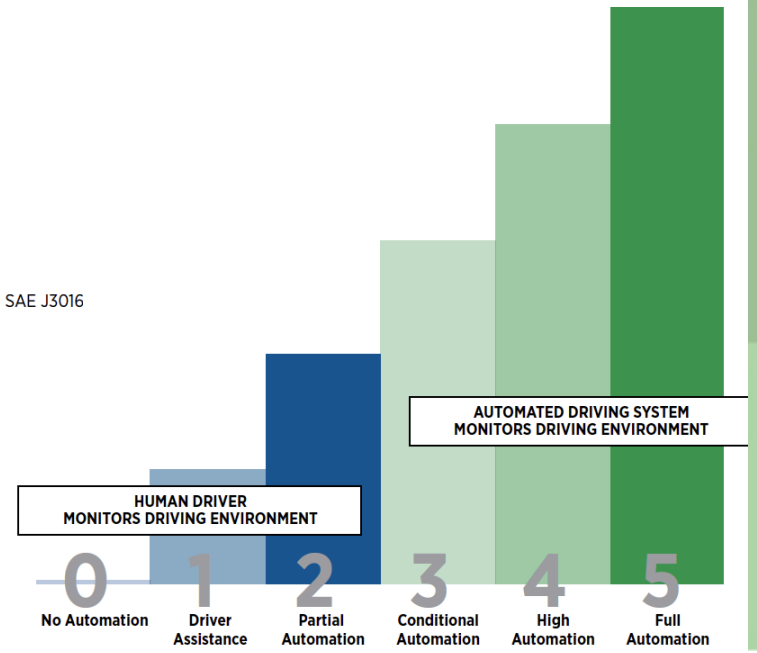
- AD: Required to be Fail-Safe
- CF: Required to be Fail-Operational

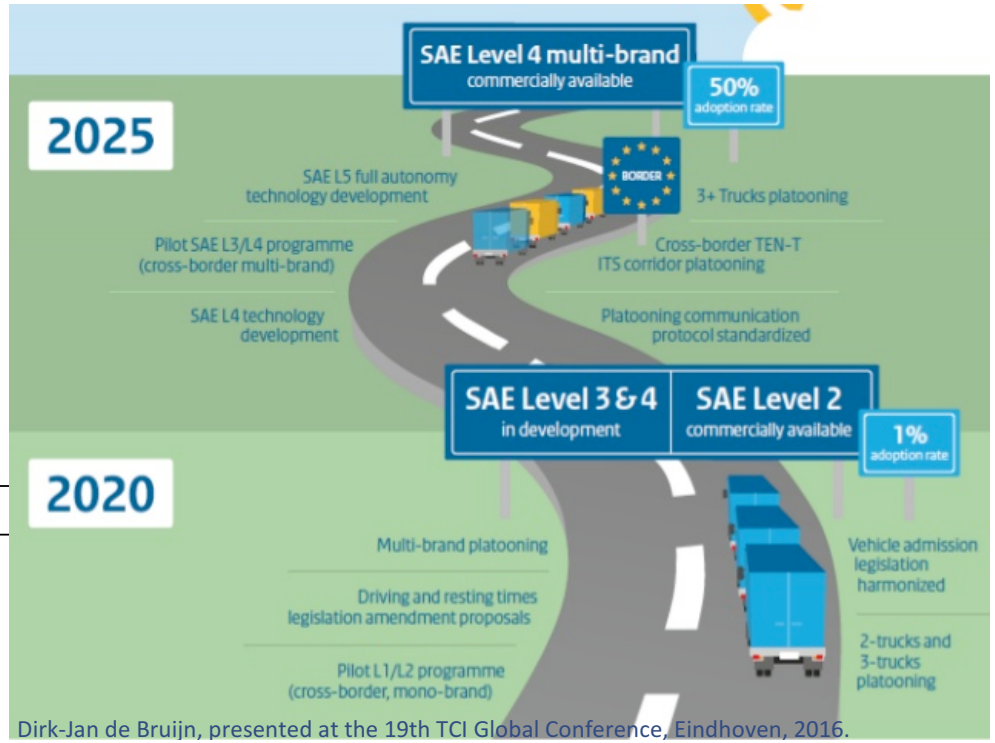




Why increased importance?

- Cooperative functions in AD is still a few years into the future.
- On-going experiments with and standardization of e.g. cross-vendor platooning has started
- Safety-assurance/certification largely open problem



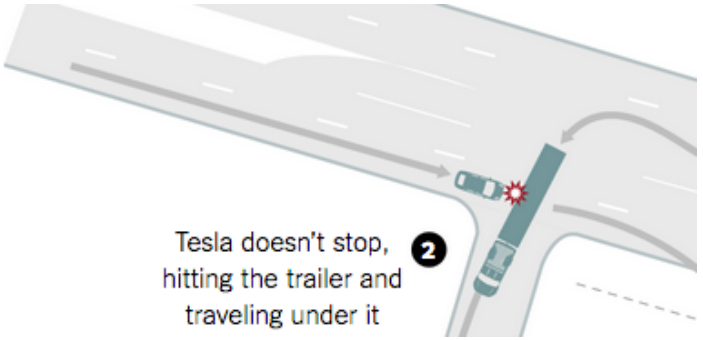


Dirk-Jan de Bruijn, presented at the 19th TCI Global Conference, Eindhoven, 2016.

Key Co-CPS challenge

- Safety-assurance is a potential show-stopper
  - solutions are lacking (and/or are not commonly accepted or supported by standards)

Fatal Tesla Model S Crash While In Autopilot Triggers NHTSA Investigation



Safety is not enough!

- Security is receiving increased attention and public awareness/pressure.

The four main roadblocks holding up self-driving cars

New Scientist

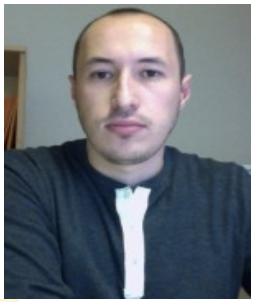
PROBLEM 3

SECURITY

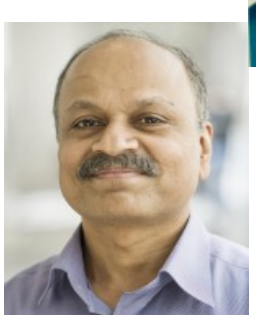
It's one thing for a virus to cause your phone or laptop to crash, but if the same fate befalls a driverless car, the consequences will be much more dramatic.

Cooperative functions in safety-critical System-of-Systems scenarios

- Introduction [Hans Hansson, MDH]



- Facing design and assurance challenges of security-informed safety critical vehicle platoons via FLAR2SAF [Irfan Sljivo, MDH]
- CO-CPS: A sample XSTAMPP usage in V2I traffic management scenario based on STAMP model [Leonardo Napolitano, RO Technology]



- Panel/Discussion [Sasi Punnekkat, MDH]