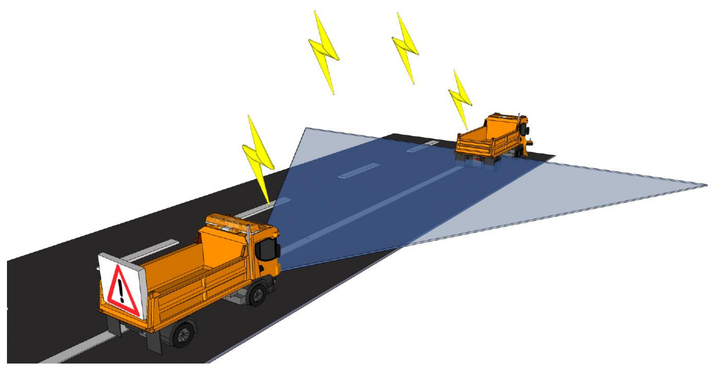
Safety Analysis based on Systems Theory applied to an Unmanned Protective Vehicle

Gerrit Bagschik, Torben Stolte, Markus Maurer
Technische Universität Braunschweig | Institute of Control Engineering
bagschik@ifr.ing.tu-bs.de, stolte@ifr.ing.tu-bs.de, maurer@ifr.ing.tu-bs.de

Unmanned protective vehicle

- Level 4 Automation on public roads
- Reduced environment and speed
- Application of ISO 26262 development process
- Four operating modes:
  - Manual mode
  - Safe halt
  - Follow mode
  - Coupled mode



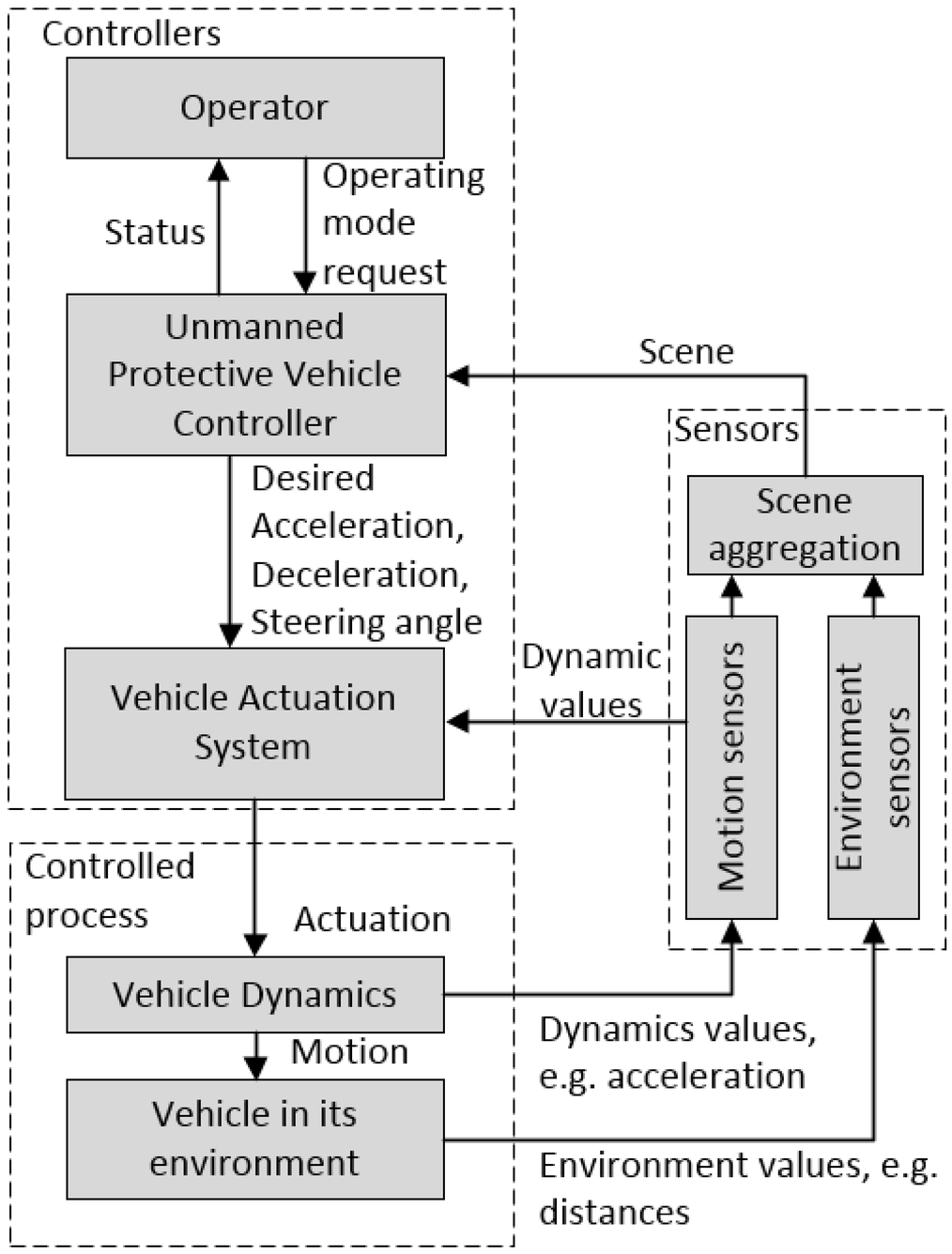
Accidents & Hazards

- A-1 AFA collides with moving traffic during unmanned operation.
- A-2 AFA collides with leading vehicle.
- A-3 AFA collides with solid obstacle on hard shoulder.
- A-4 AFA collides with vulnerable obstacle on hard shoulder.
- A-5 AFA collides with embankment.
- A-6 AFA collides with moving traffic during manual operation.

- H-1 AFA leaves hard shoulder to the left / right.
- H-2 AFA drives too close to leading vehicle.
- H-3 AFA does not react to path-blocking object.
- H-4 AFA performs unintended braking / steering / acceleration.
- H-5 AFA stops on on- / off-ramp.
- H-6 AFA operates in follow mode on on- / off-ramps.
- H-7 AFA operates unmanned at forbidden weather conditions.
- H-8 AFA operates unmanned on too narrow hard shoulder.

Control structure

- Top-level structure with cascaded control loop
  - *Fast* (inner) control loop for vehicle dynamics (20 ms)
  - *Slow* (outer) control loop for vehicle in environment (100ms)



Chosen context variables

- Operating mode
  - Manual mode, follow mode, coupled mode, safe halt
- Vehicle dynamic state
  - stopped, driving (10 km/h), driving (60 km/h)
- Environment
  - Highway/rural, hard-shoulder, on/off-ramp
- Obstacle present
  - yes (solid), yes (vulnerable), no
- Total context 108, revised 36
- Operating mode changes with additional 72 contexts

Discussion

- Control actions need to be assessed by extension of Thomas* for contextual information
- E.g. *Steering* or *Acceleration* can only be hazardous in a certain context which describes the environment
- Previous contribution** shows 108 environment scenes by nearly binary discretization
- Valid abstraction in complex environments is necessary to assess control actions

* J.Thomas, “Extending and automating a systems-theoretic hazard analysis for requirements generation and analysis”, PhD thesis, 2013

**G. Bagschik, A. Reschka, T. Stolte, and M. Maurer, “Identification of Potential Hazardous Events for an Unmanned Protective Vehicle,”
in 2016 IEEE Intelligent Vehicles Symposium Proceedings, accepted to appear

Technische Universität Braunschweig

Institut für Regelungstechnik