Performing a More Realistic and Complete Safety Analysis by Means of the Six-Variable Model

Nelufar Ulfat-Bunyadi, Denis Hatebur, Maritta Heisel

Motivation

UNIVERSITÄT DUISBURG ESSEN
Open-Minded

- Safety analysis: Hazard Analysis and Risk Assessment (HARA), Fault Tree Analysis (FTA)
- HARA: identify and categorize hazardous events
- Hazardous event: hazard + operational situation
- Hazard: potential source of harm caused by malfunctioning behavior of system
- FTA: identify failure events (within system) that can lead to hazard

Problem: Focus of traditional safety analysis on identifying failure events within system, but hazardous event may also occur due to invalid environmental assumptions

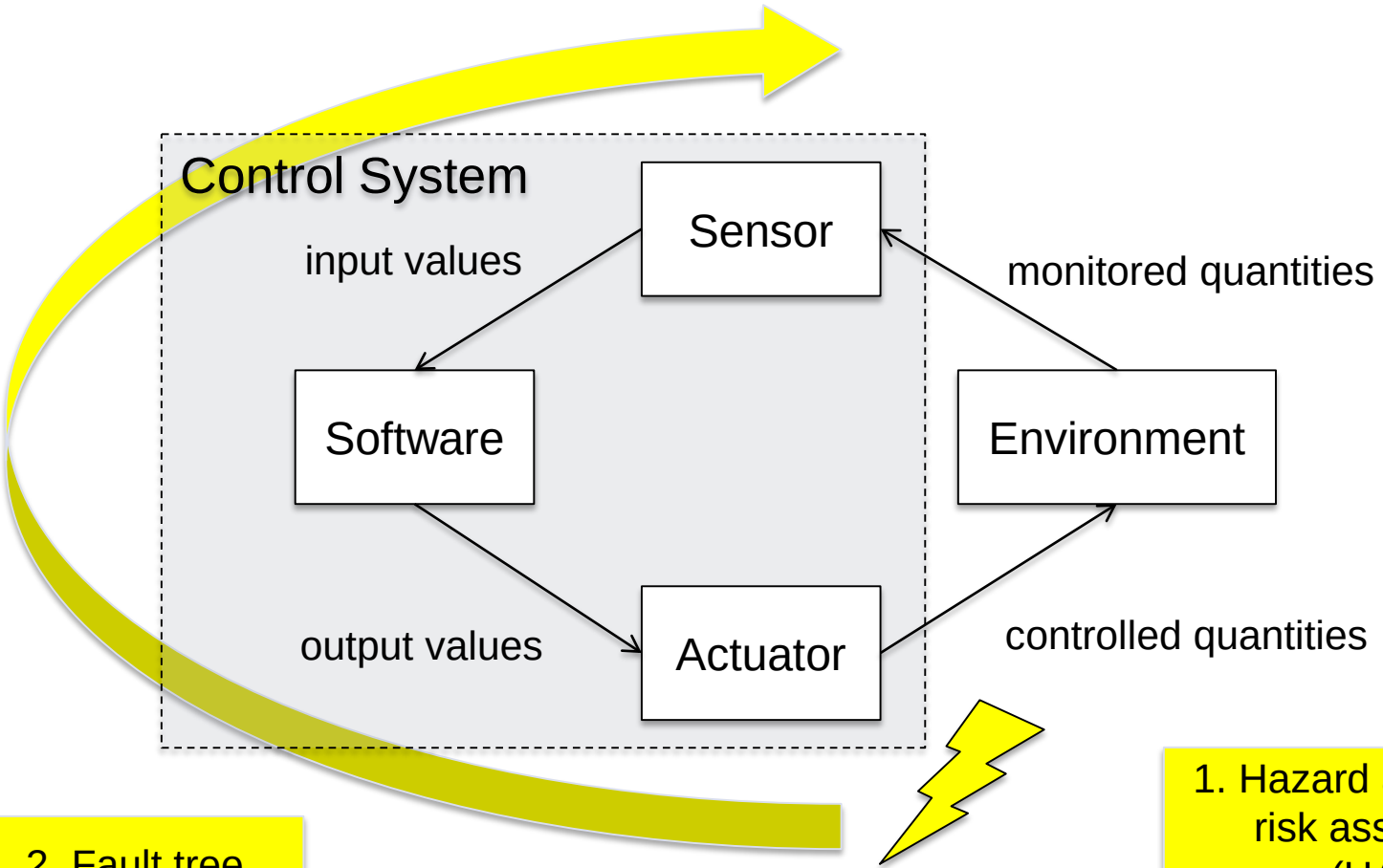
Example:
Autopilot of Lufthansa A320 Flight to Warsaw

UNIVERSITÄT DUISBURG ESSEN
Open-Minded

- Accident:
  Plane ran off the end of the waterlogged runway resulting in injuries and loss of life.
- Requirement:
  Enable reverse thrust iff plane is moving on runway.
- Assumption:
  Plane is moving on runway when wheels are turning.
- Cause:
  Wheels were not turning due to aquaplaning. Autopilot assumed plane is not moving on runway. It did not enable reverse thrust.

Invalid environmental assumption was cause of hazardous event, not a system failure!

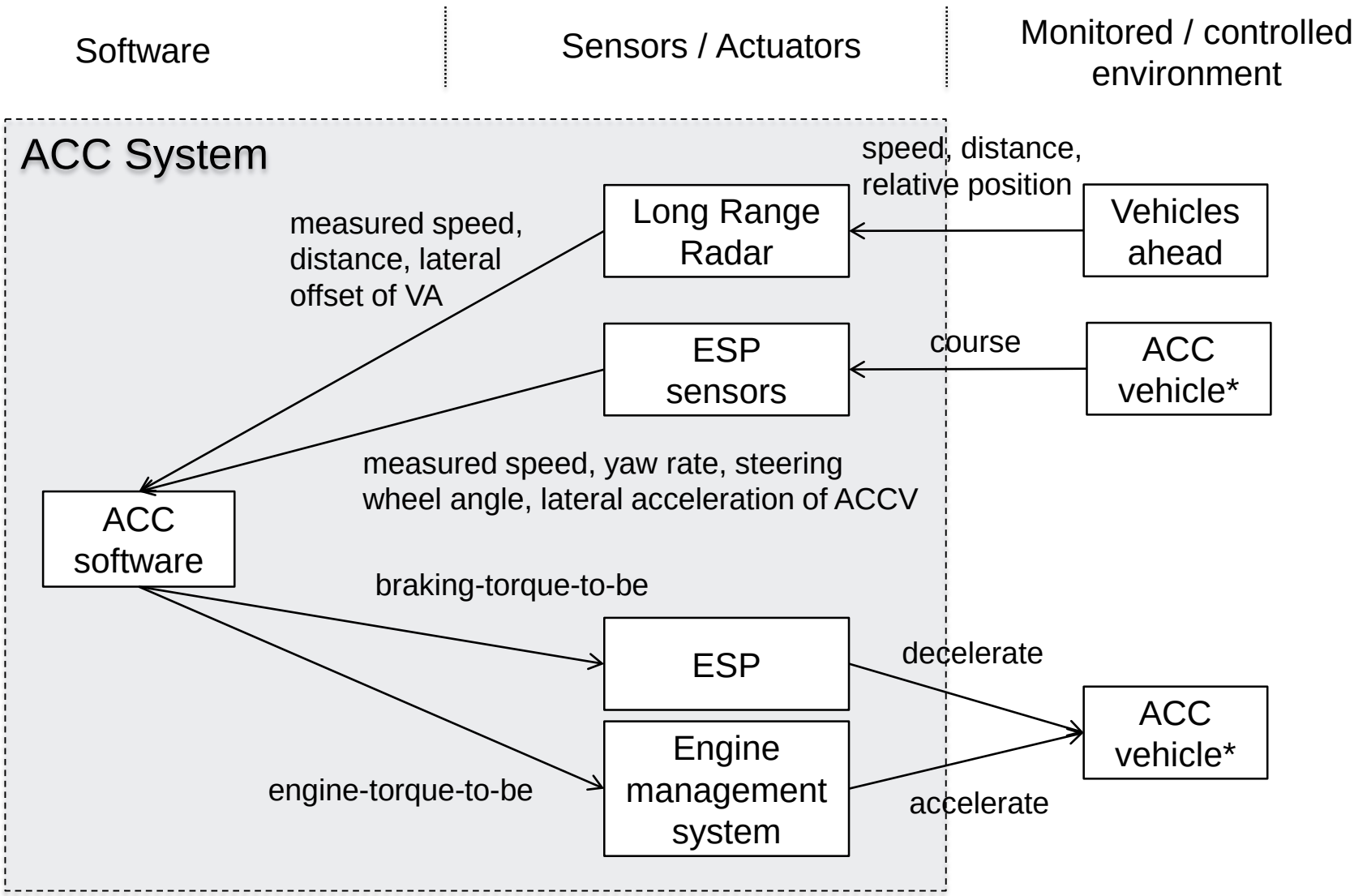
Traditional Safety Analysis



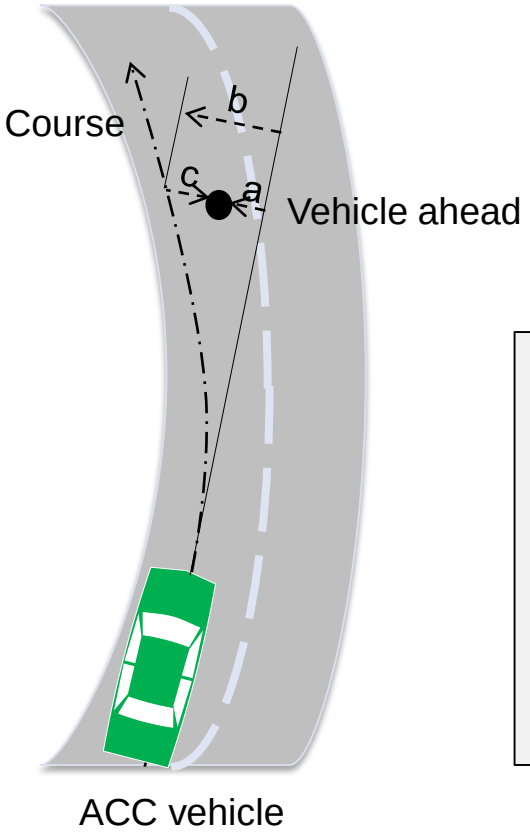
1. Hazard analysis and risk assessment (HARA)

2. Fault tree analysis (FTA)

Traditional Safety Analysis (Example)



Identifying vehicles ahead on same lane



a: lateral offset of vehicle ahead

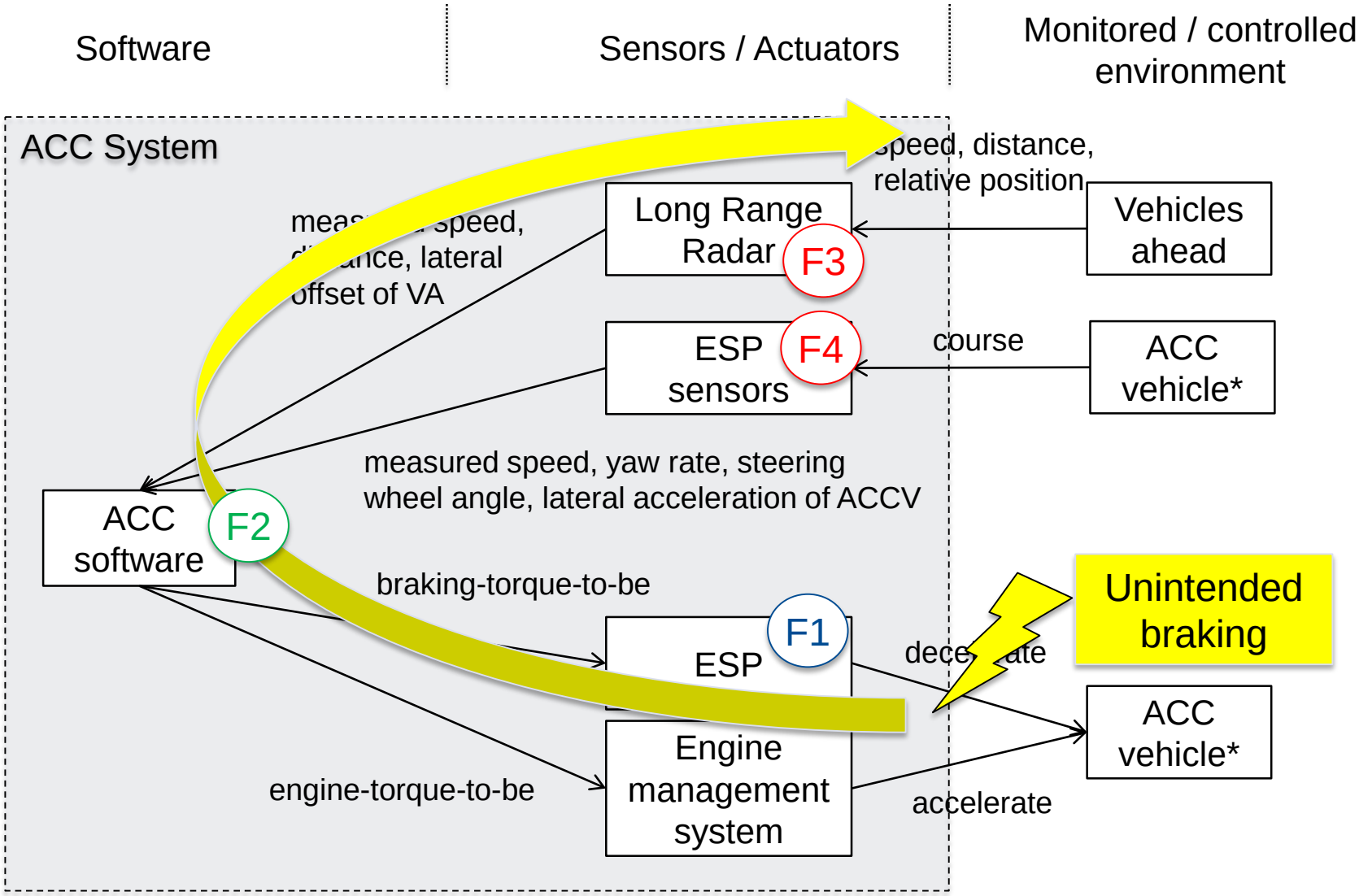
b: course of ACCV

c: relative position of VA

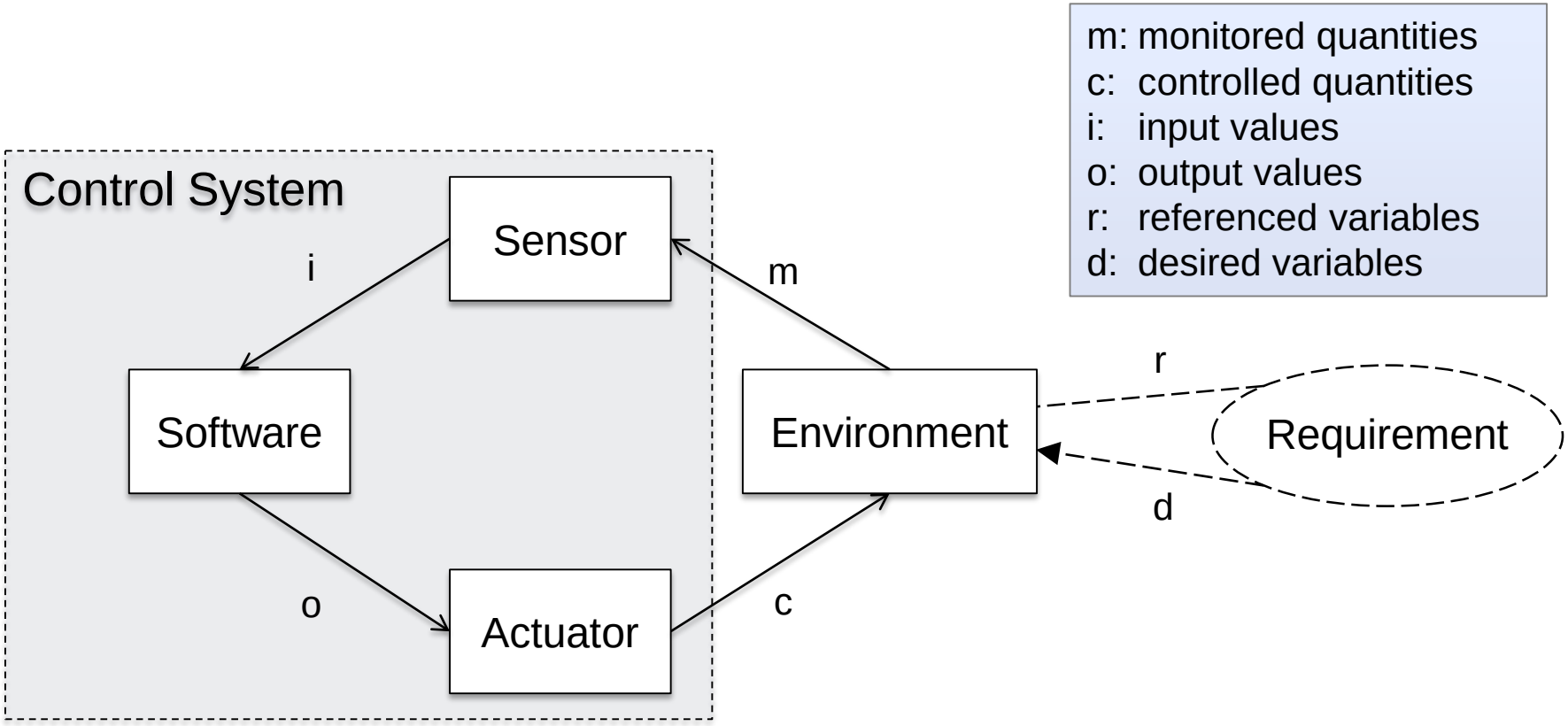
1) a measured by LRR sensor
2) b predicted by ACC based on ESP sensor data
3) c calculated by ACC, c = b – a

Reference: Konrad Reif (Hrsg.): Fahrstabilisierungssysteme und Fahrerassistenzsysteme, Bosch Fachinformation Automobil, Vieweg+Teubner Verlag, 1. Auflage, 2010.

Traditional Safety Analysis (Example)

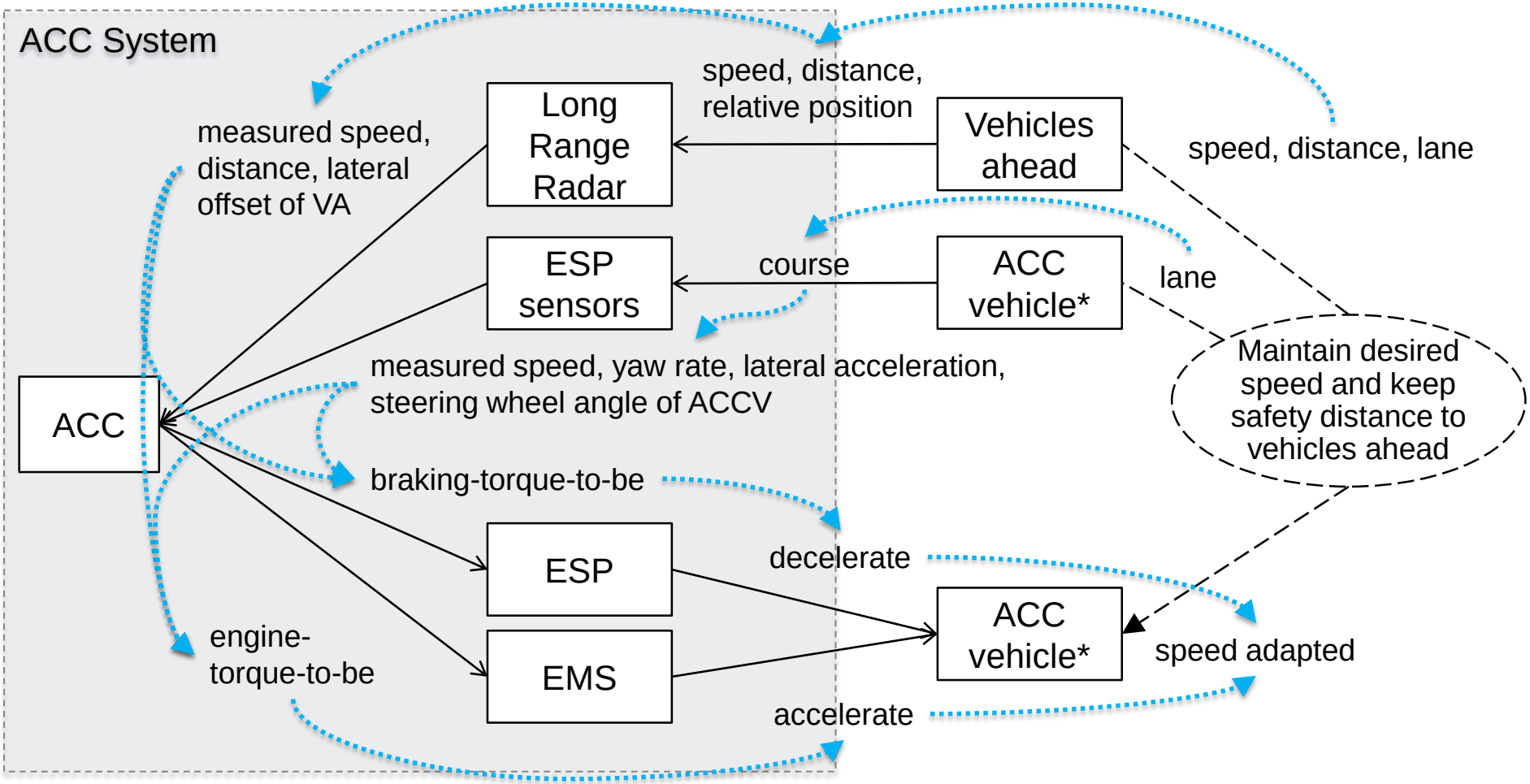


The Six-Variable Model

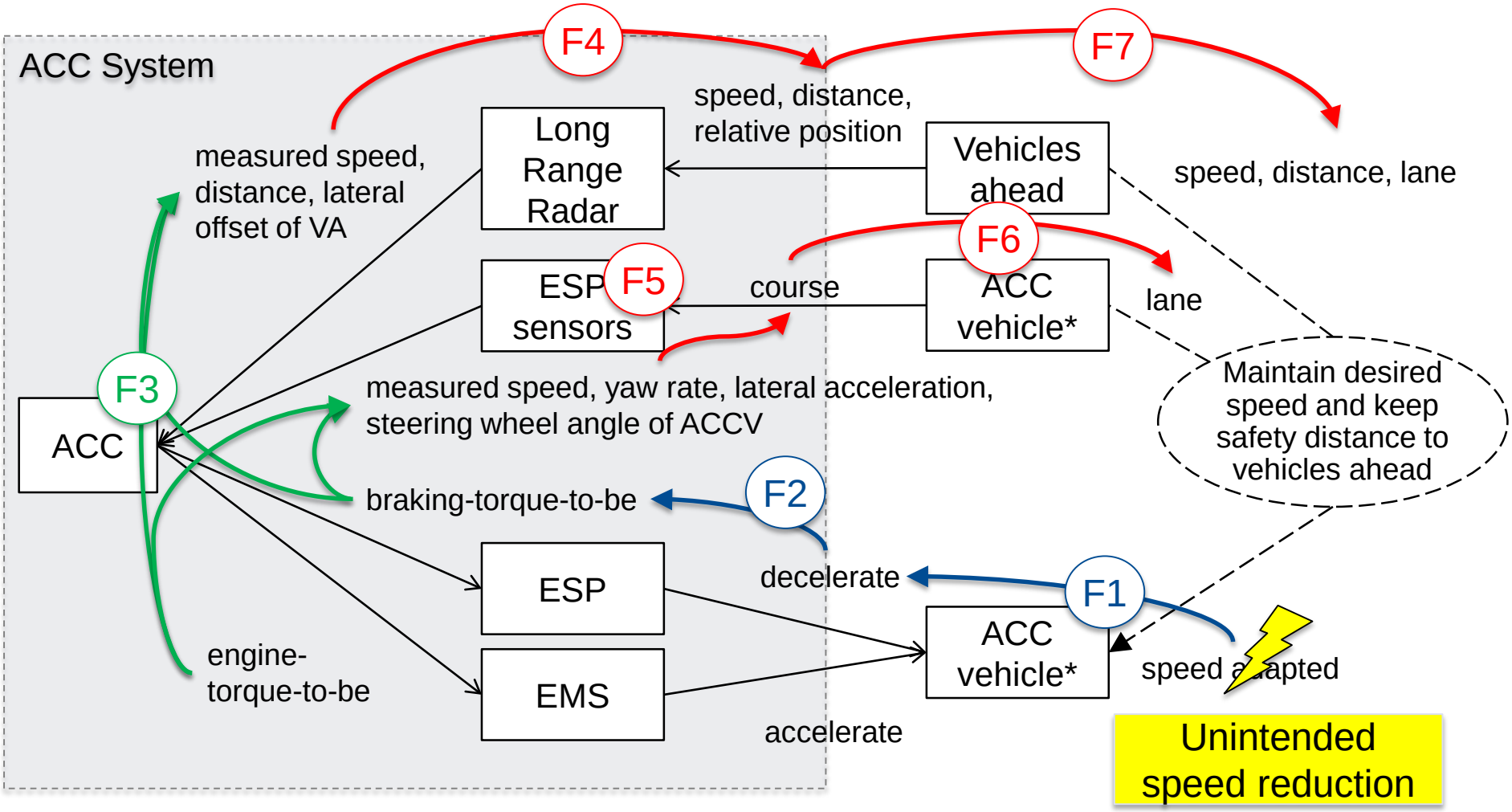


Reference: N. Ulfat-Bunyadi, R. Meis, M. Heisel: The Six-Variable Model - Context Modelling Enabling Systematic Reuse of Control Software. Proc. of ICSOFT-PT 2016, pp. 15-26.

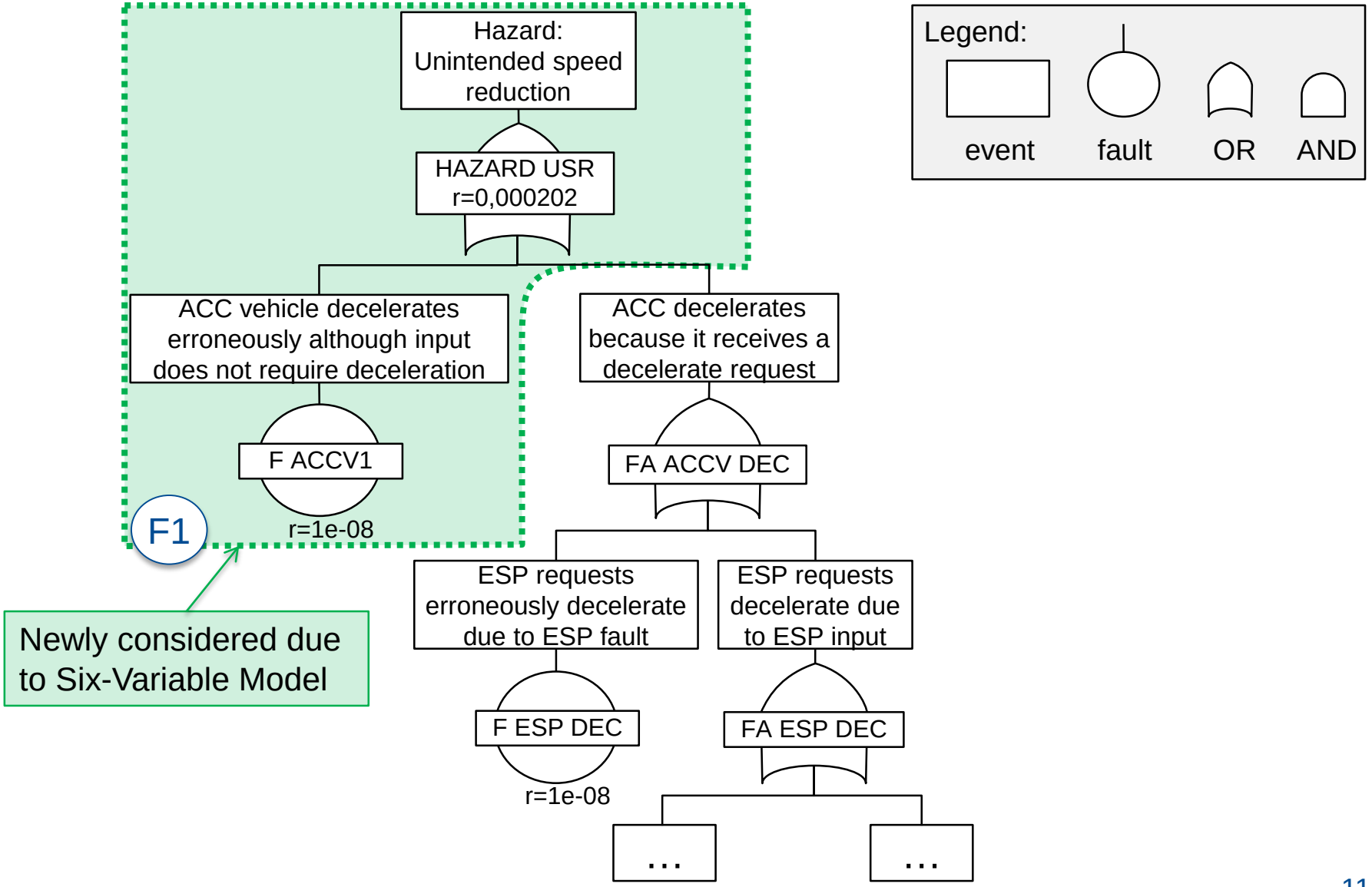
Safety Analysis based on Six-Variable Model



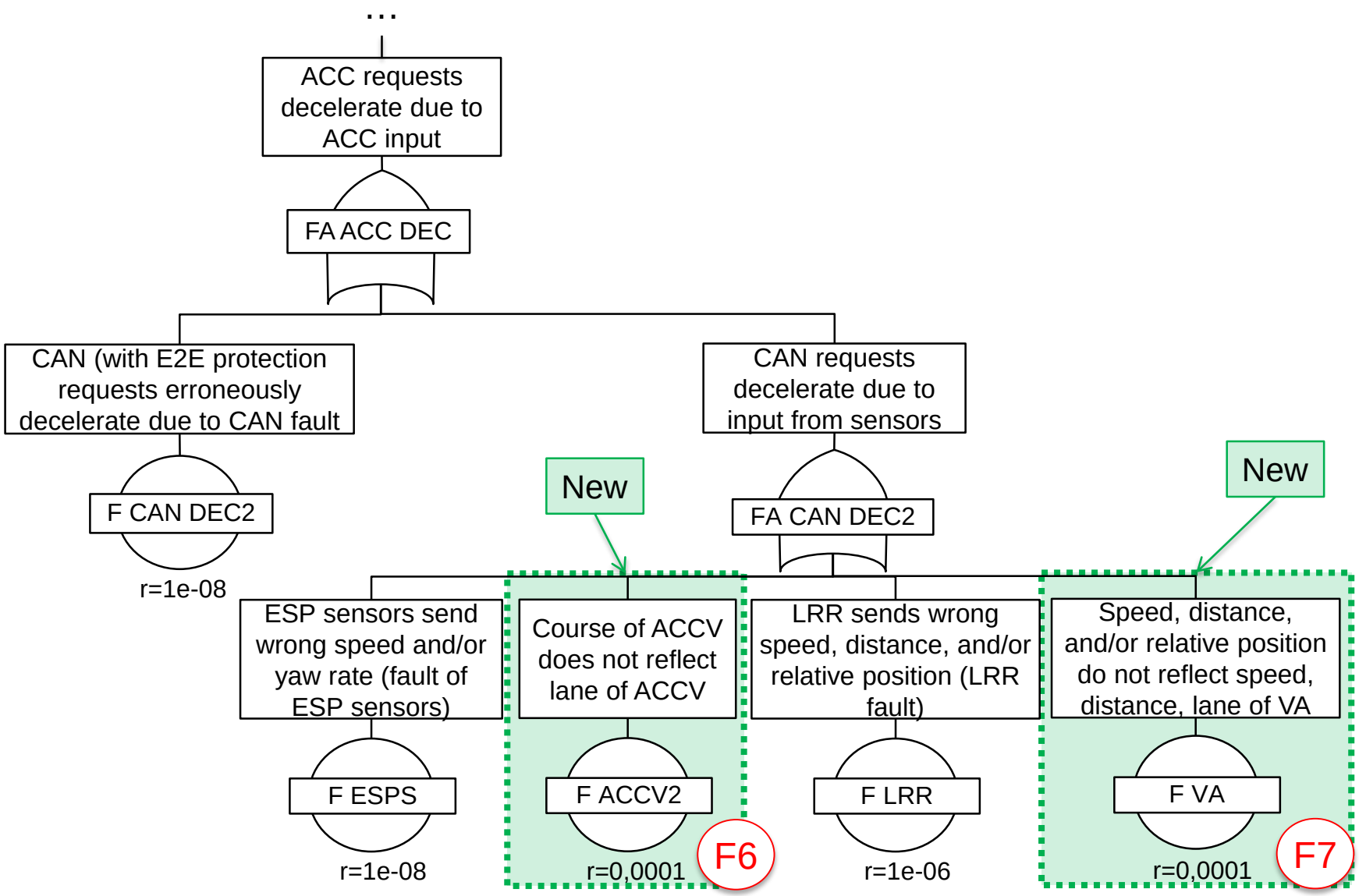
Safety Analysis based on Six-Variable Model



Resulting Fault Tree (Excerpt: Upper Part)



Resulting Fault Tree (Excerpt: Lower Part)



Benefit of Our Method

UNIVERSITÄT DUISBURG ESSEN
Open-Minded

- Consideration of environmental assumptions results in higher overall failure rate, but this is more realistic
  - Environmental assumptions can also turn invalid
- Safety analysis is more complete:
  - Identification of system failures as possible cause
  - Identification of invalid assumptions as possible cause
- Too strong assumptions can be weakened or abandoned by changing system design
  - Adding sensors/actuators
  - Using other sensors/actuators

Future Work

UNIVERSITÄT DUISBURG ESSEN
Open-Minded

- Extend STPA (Systems-Theoretic Process Analysis) with Six-Variable Model and compare the two methods
  - Safety as control problem: “hazards occur when component failures, external disturbances, and/or dysfunctional interactions among system components are not adequately handled”
  - Preventing hazards means designing control structure that enforces constraints
- Method for definition of safety requirements and safety cases based on the Six-Variable Model

UNIVERSITÄT
DUISBURG
ESSEN

Open-Minded

Thanks for your attention ☺

Questions?