SIP-adus
Innovation of Automated Driving for Universal Services

SecForCARs
security for connected automated cars

funding by:
Bundesministerium für Bildung und Forschung

Automotive Trust Models
Project SAVE (“Securing Automated Vehicles”)

Frank Kargl, Ulm University, V1.2 2022-10-12

universität ulm

Fraunhofer IEM

Fraunhofer AISEC

Freie Universität Berlin

Hochschule Karlsruhe
University of
Applied Sciences

HKA

SecForCARs
security for connected automated cars

Audi

escrypt
SECURITY. TRUST. SUCCESS.

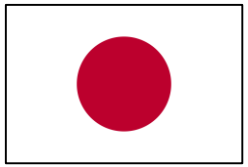
SCHUTZWERK

Technische
Universität
München

funding by:

Bundesministerium
für Bildung
und Forschung

Securing Automated Vehicles (SAVE)
German–Japanese Cooperation



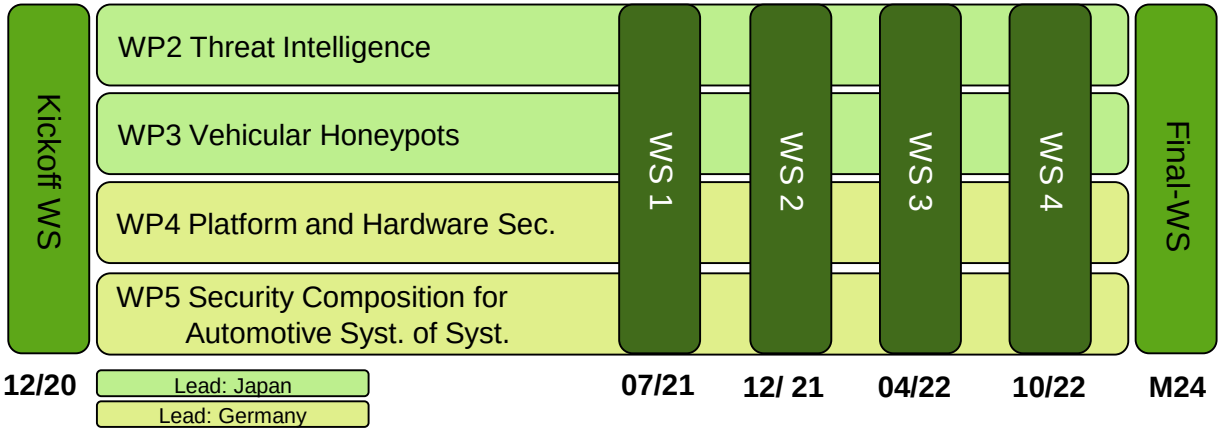
SIP

SecForCARs
security for connected automated cars

YNU YOKOHAMA National University
TOYOTA
NEDO
pwc

infineon
Hochschule Karlsruhe University of Applied Sciences
HKA
escrypt SECURITY. TRUST. SUCCESS.
Freie Universität Berlin
Fraunhofer SIT & IEM
DENSO

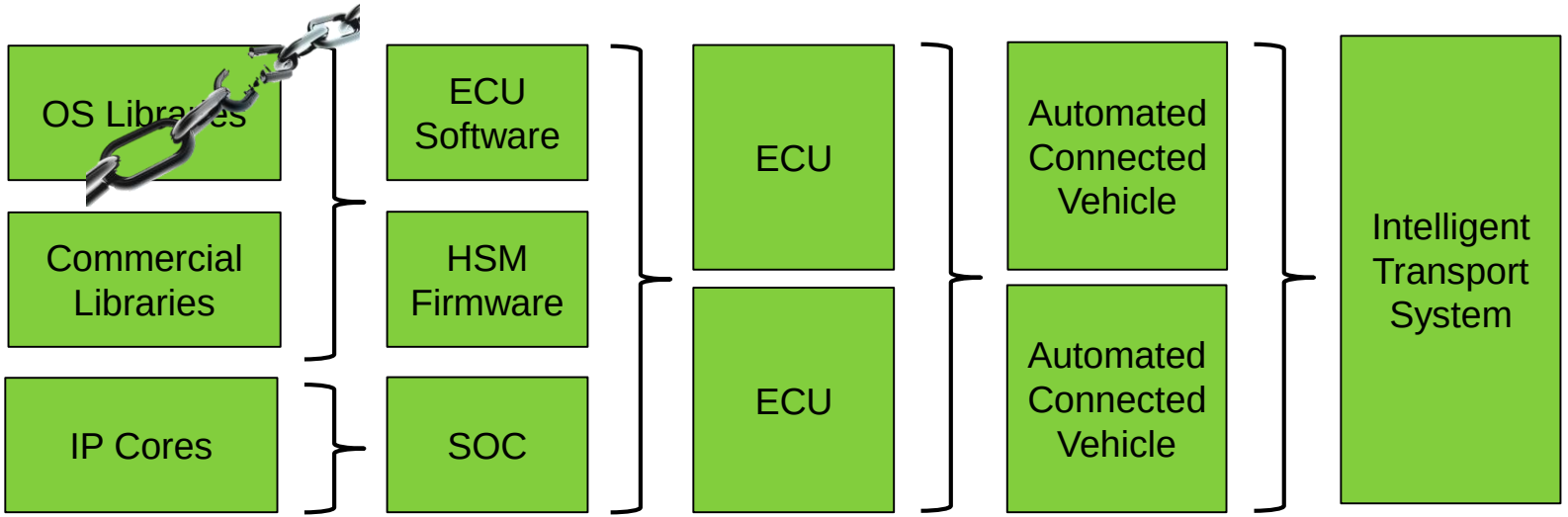
funding by:
Bundesministerium für Bildung und Forschung



WP1: WS Organization
WP6: Exchange and Dissemination
WP7: Project Administration

Why Trust Modeling in Automotive SoS?

Due to the complexity of automotive Systems-of-Systems, it is hard to estimate the effects of security vulnerabilities and attacks on all parts of the system.

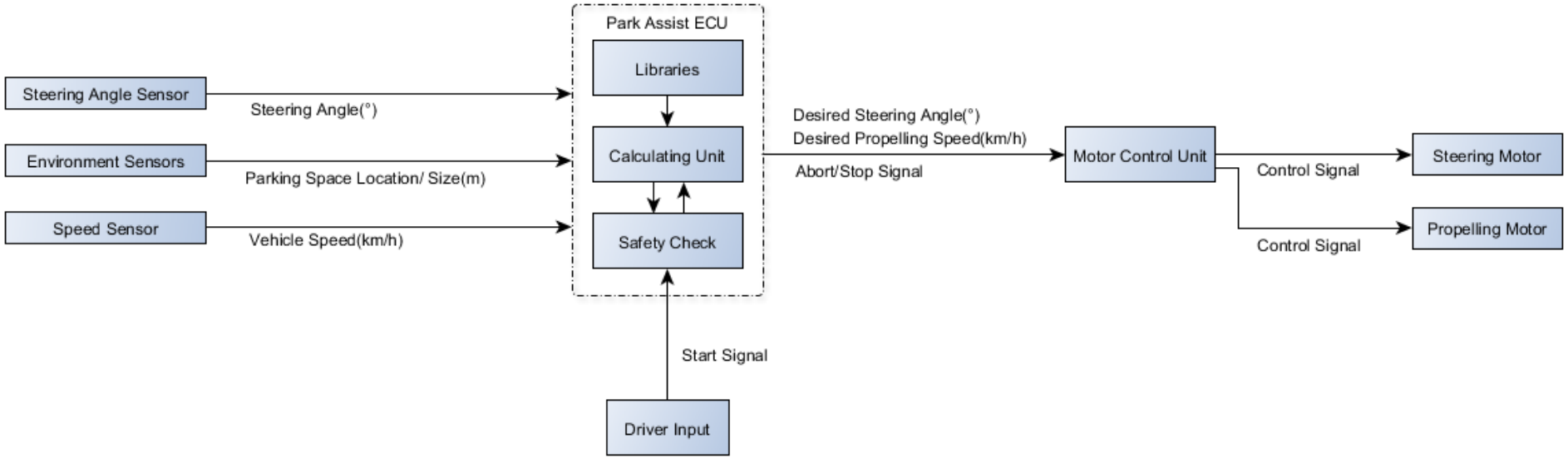


Trust Modeling can Help Solve Security Problems in SoS

- Many trust-related questions exist in automotive security
  - Can ECU X trust the firmware deployed by OTA update?
  - Can manufacturer M trust library L embedded into a binary B of its firmware F?
  - Can ECU X trust data D reported by Sensor S via CAN-bus B?
  - How will an IDS alarm reduce overall trustworthiness of the system?
  - How will knowledge of a new attack affect trustworthiness of the system?
  - And many more

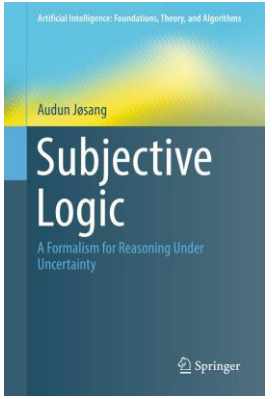
- In SAVE, we work towards a generic trust management framework to model such trust relationships and reason over them to answer simple questions:
  - Can I interact with another entity in a trustworthy way?
  - Can I trust the data that I have received?

Example Scenario: Parking Assistant



What trust dependencies exist in this scenario?

Subjective Logic Intuition for Binary Domains



(**b**elief,**d**isbelief,**u**ncertainty,b**a**serate)

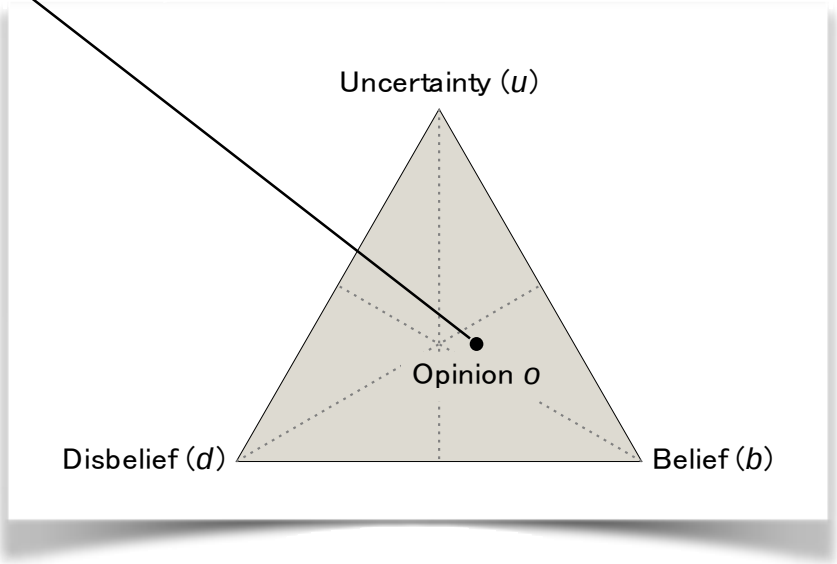
$S \xrightarrow{\omega} x$

S: opinion holder
x: proposition / data value
ω[S;x]: opinion of S on x
b+d+u=1

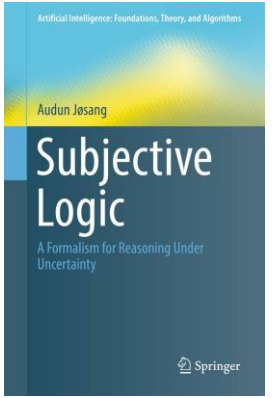
Example:
o = (1,0,0,a) ≙ Boolean True

o = (0,1,0,a) ≙ Boolean False

o = (0,0,1,a) ≙ Total uncertainty

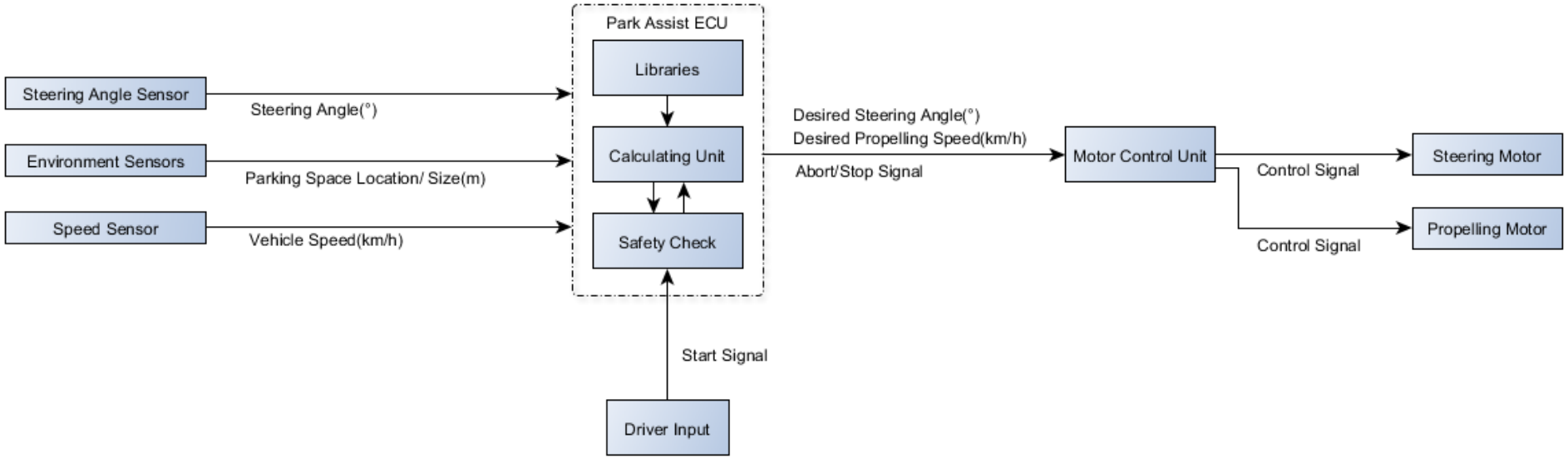


Subjective Logic Reasoning



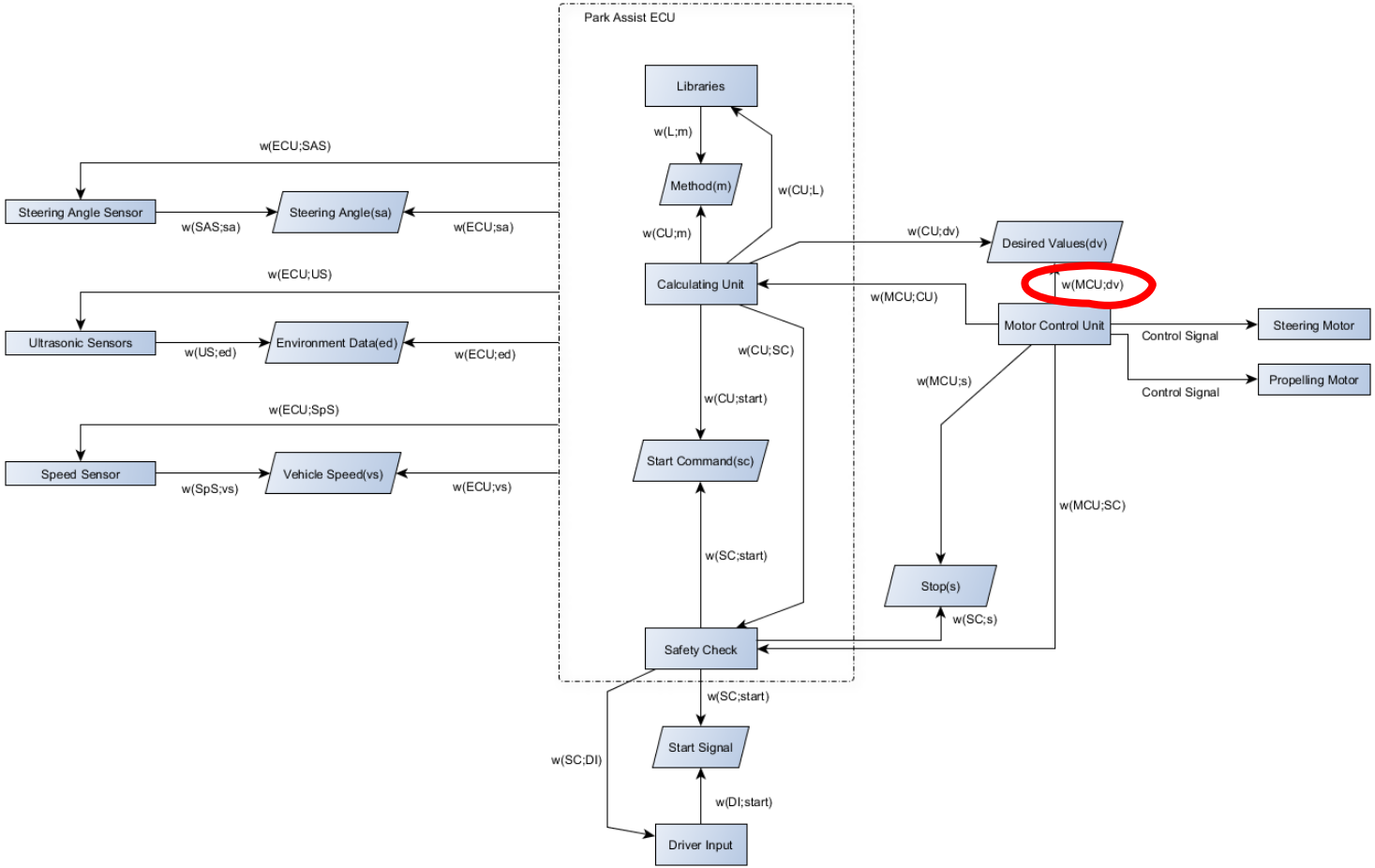
- Rich set of operators:
  - Trust discounting: transitive trust resolution
  - Fusion operators
    - BCF: Belief Constraint Fusion (equivalent to Dempster's Rule)
    - CBF: Cumulative Belief Fusion ("sum the evidence")
    - ABF: Averaging Belief Fusion ("average the evidence")
    - WBF: Weighted Belief Fusion ("confidence-weighted average")
    - CCF: Consensus & Compromise Fusion ("conflict → vagueness")

Example Scenario: Parking Assistant

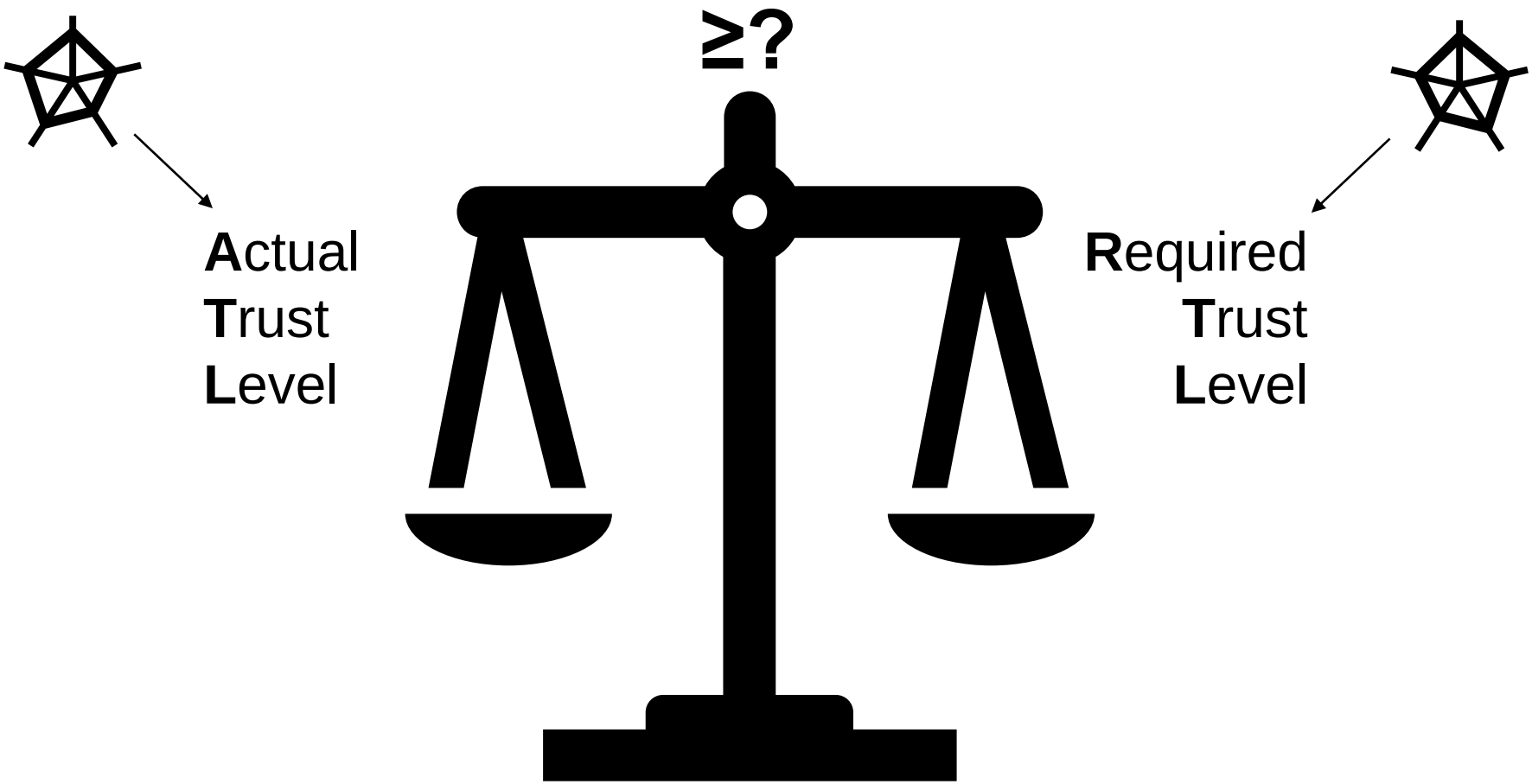


Can MCU trust Desired Values from Park Assist ECU?

Converting the Scenario into a Subjective Trust Network



How to use the Subjective Trust Network?



Sources for Initial Opinions

- Where do initial opinions originate from?
  - Misbehavior Detection Systems
  - Intrusion Detection Systems
  - Reputation Management Systems
  - Trusted Execution Environments & Remote Attestation
  - Code Reviews of Software, Static Code Analysis
  - Risk & Safety Analysis Processes & Certification
  - Honeypots and Threat Intelligence

  - Basically, all security & safety processes and mechanisms can contribute to the trust model
  - The trust model unifies and integrates all security-related information in a quantifiable and analyzable way

Where can Trust Models be Useful?

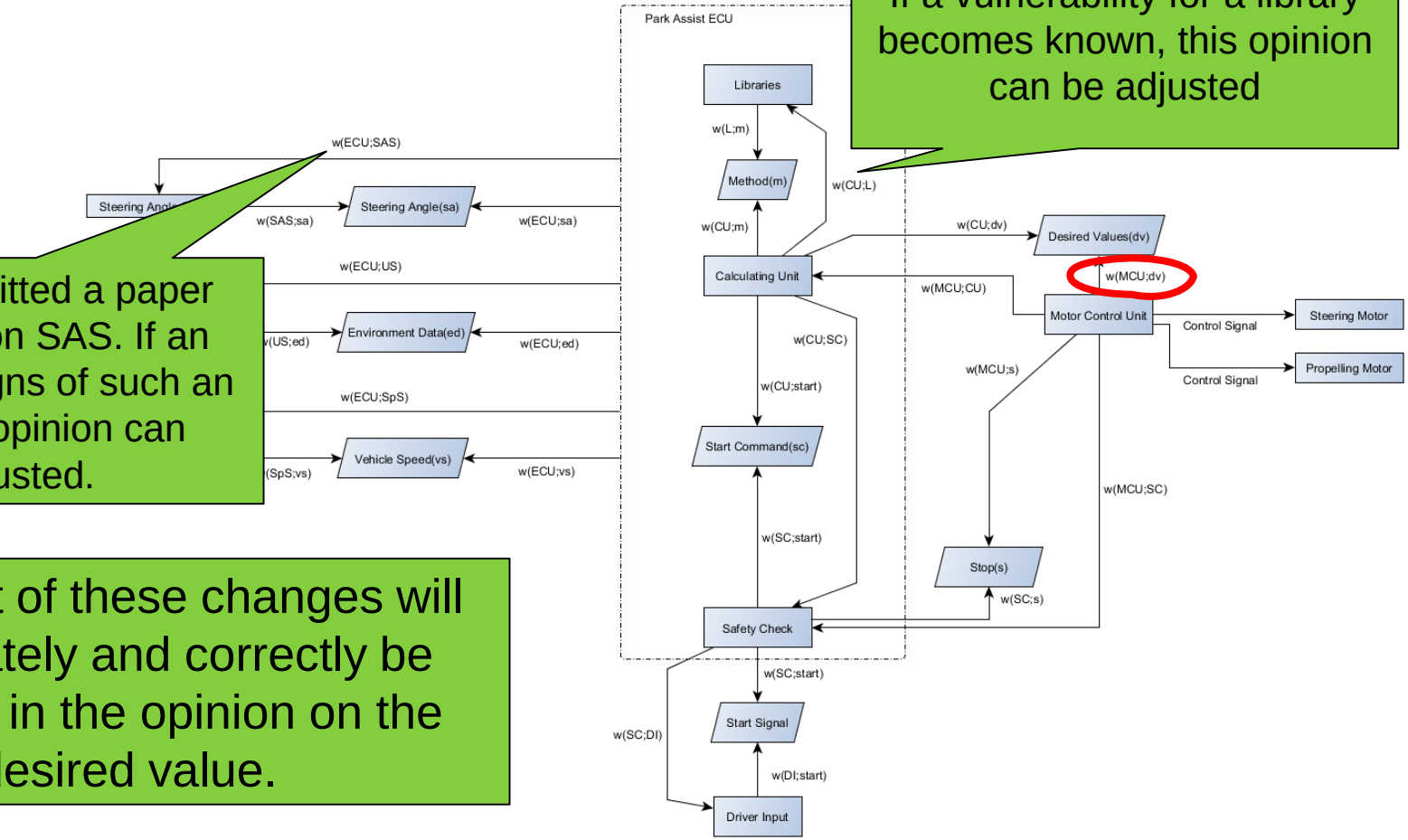
- At design time:
  - Make risk assessment more precise
  - Evaluate effect of attack found in penetration test on overall system
  - Evaluate effect of security mechanisms in the trust model
- At run time:
  - Vehicles in cooperative system can assess trustworthiness of data and decide to rely on it or not
    (depending on how safety critical application is)
  - An in-vehicle IDS that detects an attack can rely on the trust model to assess the effect on different parts of the system or it can evaluate how effective countermeasure would be

Example for Usage

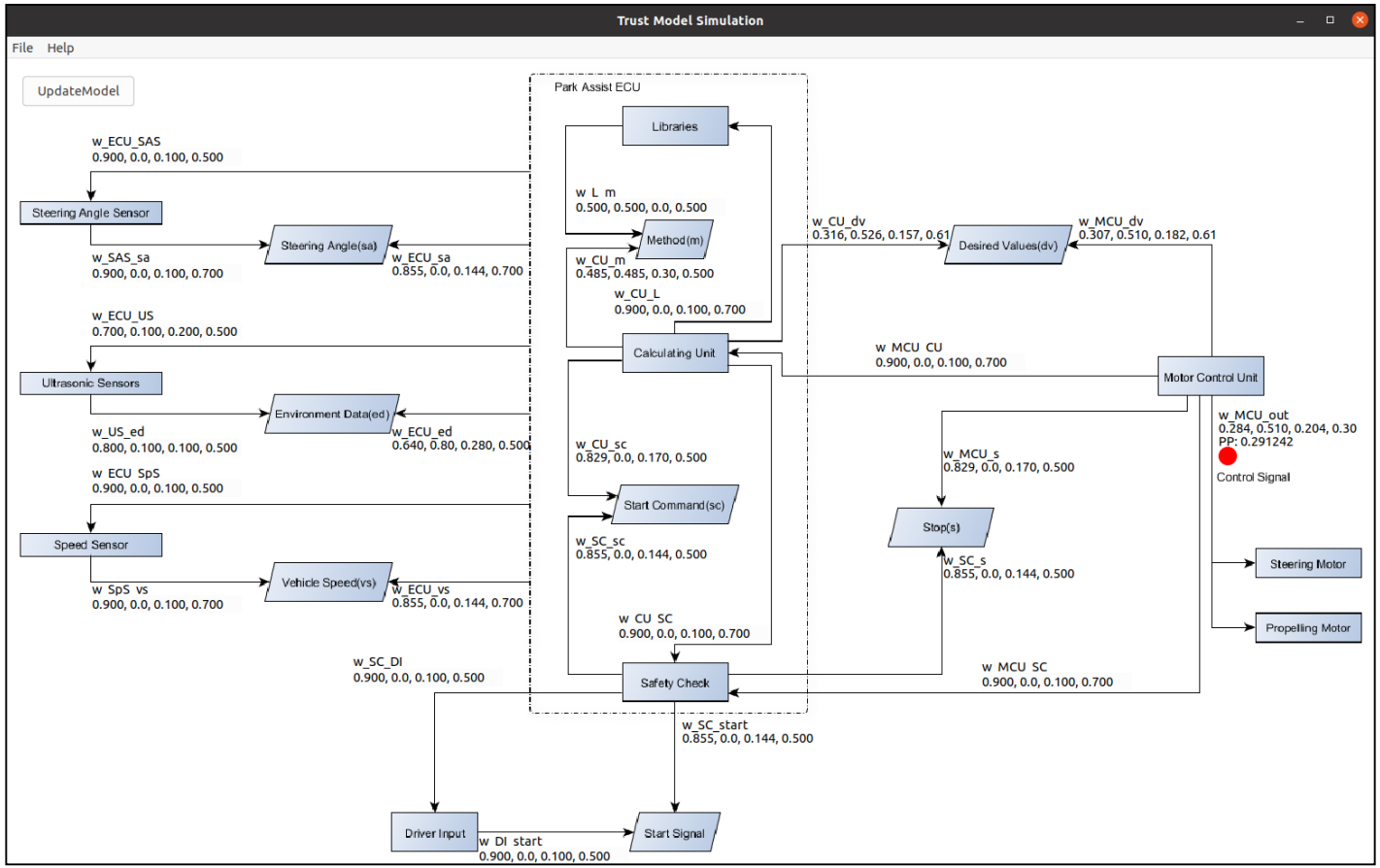
We just submitted a paper with attacks on SAS. If an IDS detects signs of such an attack, this opinion can be adjusted.

If a vulnerability for a library becomes known, this opinion can be adjusted

The effect of these changes will immediately and correctly be reflected in the opinion on the desired value.



Currently Finalizing A Prototype to Allow Detailed Experiments



SecForCARs
security for connected automated cars

SecForCARs has produced many interesting results!

https://www.secforcars.de/

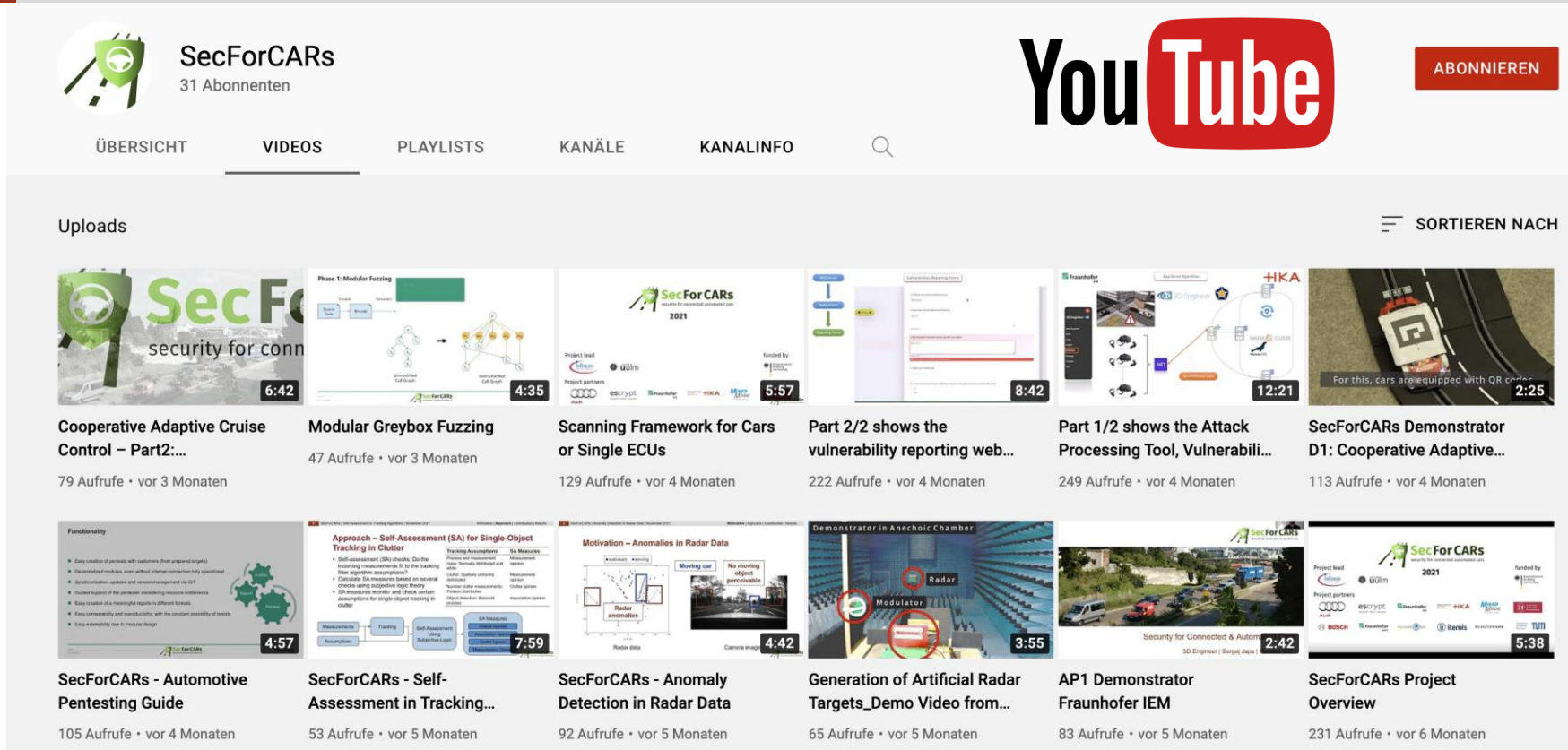
YouTube

Channel “SecForCARs”

LinkedIn

“SecForCARs Project”

@secforcars



Many videos on our YouTube Channel
https://www.youtube.com/channel/UCGwcmqMzUUrfftdyRLQEKiA/

Q&A