Controllability-aware Threat Analysis and Risk Assessment for L3 Automated Driving Systems

Jukka Laitinen, VTT

Contents

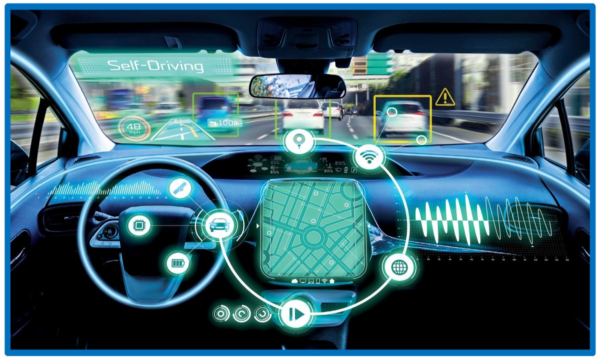
- Motivation for cyber security work in L3Pilot
- Threat analysis and risk assessment modified model proposed*
- Results
- Discussion

+ anonymized input from L3PIlot OEMs

* [Publication IV 2019] A. Bolovinou, U. Atmaca, A-T. Sheik, O. Rehman, G. Wallraf, A. Amditis, **TARA+: Controllability-aware Threat Analysis and Risk Assessment for L3 Automated Driving Systems.**

Motivation

[Attack profile per SAE J3016]



System resilience

C o n t r o l l a b i l i t y

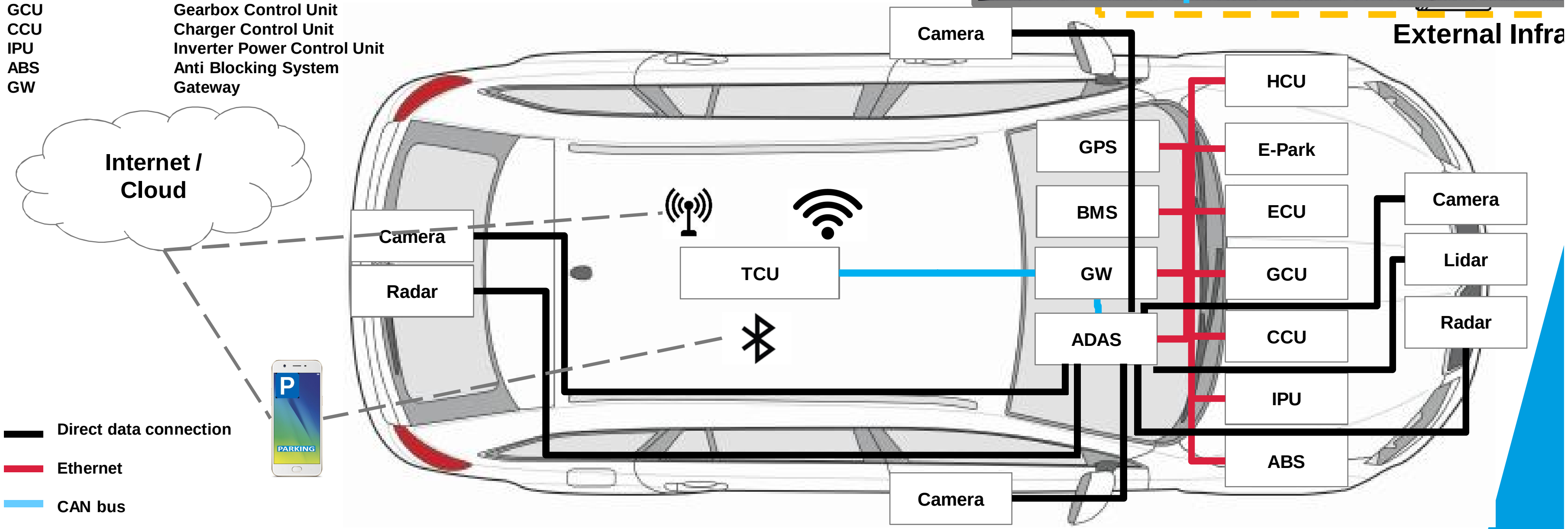
[ISO 26262]

- Attack surface analysis for L3Pilot Urban | Highway | Parking – Chauffer AD systems
- **System resilience rough assessment** based on OEMs questionnaires
- **System resilience modeling** inside TARA framework
  - ß missing from SAE J3061, bears relationship with ISO26262
- High-level recommendations for OEMs before piloting on public roads

Reference Architecture for Threat Analysis

Legend

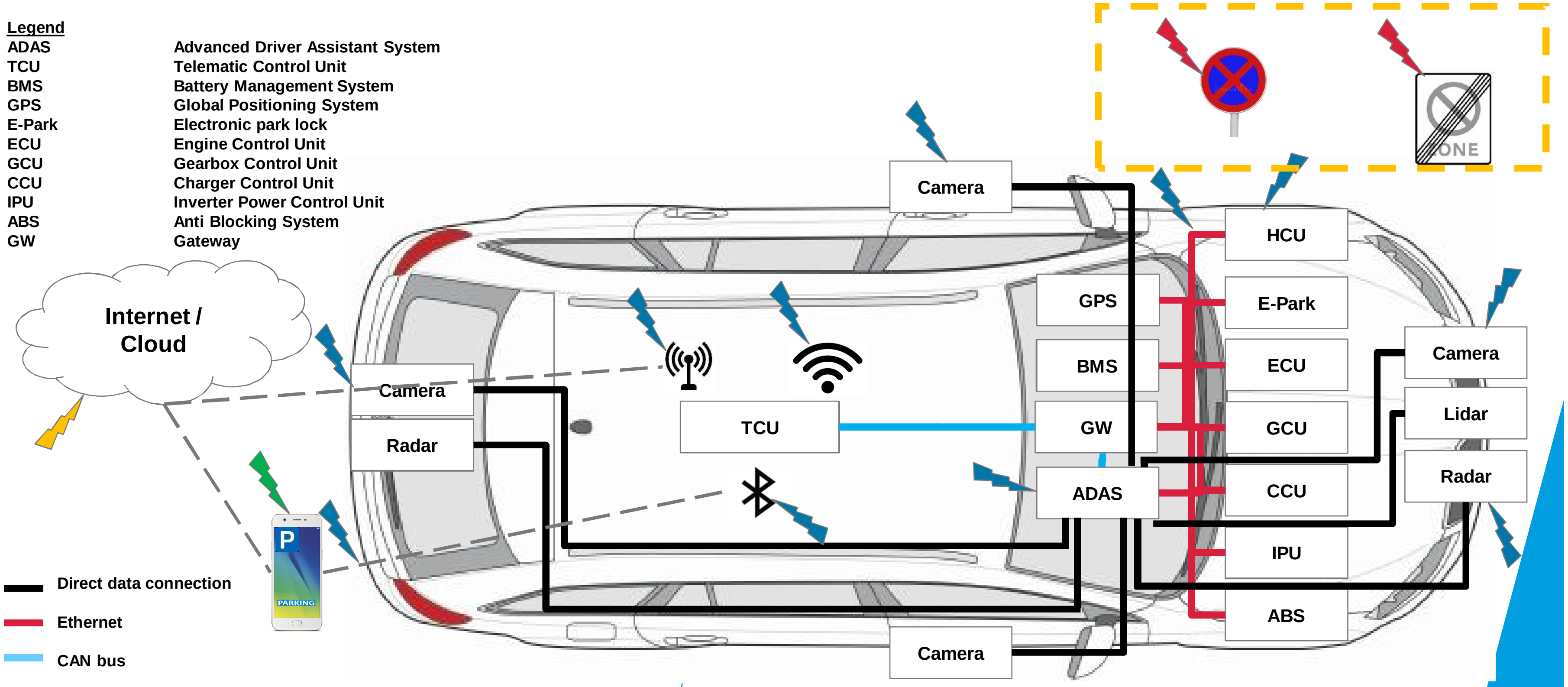
ADAS	Advanced Driver Assistant System
TCU	Telematic Control Unit
BMS	Battery Management System
GPS	Global Positioning System
E-Park	Electronic park lock
ECU	Engine Control Unit
GCU	Gearbox Control Unit
CCU	Charger Control Unit
IPU	Inverter Power Control Unit
ABS	Anti Blocking System
GW	Gateway



Attack Surface

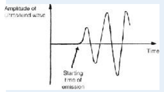
Legend

ADAS	Advanced Driver Assistant System
TCU	Telematic Control Unit
BMS	Battery Management System
GPS	Global Positioning System
E-Park	Electronic park lock
ECU	Engine Control Unit
GCU	Gearbox Control Unit
CCU	Charger Control Unit
IPU	Inverter Power Control Unit
ABS	Anti Blocking System
GW	Gateway



Attack Surfaces analysis - extract

(New columns)

Attack Surface	Relevant Attack Methods	Expertise (knowledge) Required	Equipment Required	Window of Opportunity Required	Controllability Considerations	Application –Specific Considerations
Range Sensors (radar, ultrasonic, LiDAR) 	Spoofing, Tampering (provide false sensor data); Denial of Service **(blind or jam from a distance)**	Proficient (range sensor operation principles)	Light transceivers/ Pulse generator (optional)	Small (very specific, e.g. for Lidars depends on the Lidar pulse frequency)	Sensor fusion should be used for sensors' conflict detection. The attack affects perception (i.e. system intended functionality per ISO/PAS 14446) without causing malfunctioning of the sensor. Redundancy in sensors makes it controllable.	Easier to setup in the urban use case where distance between the vehicles and the roadside and velocities applying are lower.With a static roadside setup multiple cars in the range can be targeted. Effects can be very critical especially in the urban case since presence or distance of detected objects are modified.
Road structural element (e.g. traffic sign, lanes) 	Tampering **(modifying static or dynamic road traffic sign e.g. adding new fake road signs or lanes)**	Layman or proficient in the execution; Proficient in the conception	Physical road surface or traffic sign modification Interfering with road displays' visual content.	Unlimited	Very difficult to be detected since HD maps of the environment not usually available while dynamic localization and matching is a runtime intensive process.	Easy to execute for the attacker since it can be performed independently of the vehicle presence. Affects vehicle self-localization ability and may also result in false positives for objects detected based on visual artefacts (e.g a 3-D object drawing on the road surface).

L3Pilot Driving Automation

The proposed modified model: TARA+ (new features for HAD)

input

- Guidelines for risk assessment are provided in J3061
  - >However, link to a specific automation level is missing
- Security issues do not create new safety hazards (unsafe states) but alter the likelihoods of existing states
  - >There is clearly a need to jointly address functional safety and security
- New applications may be developed in future supporting higher automation levels

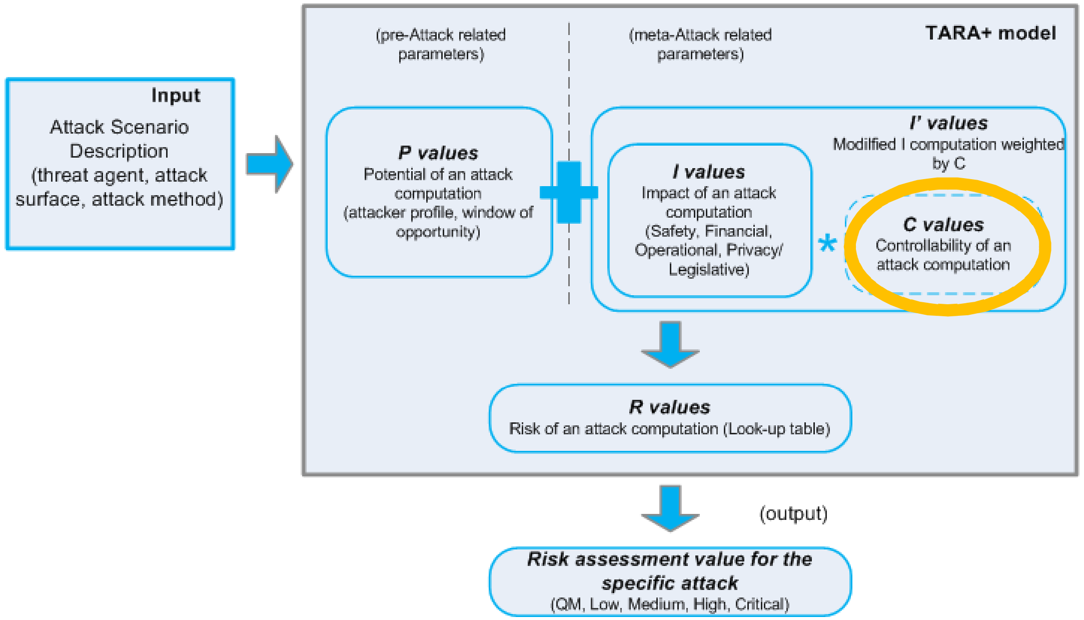
The model

- Definition of controllability levels w.r.t. AD system based on the principles of system availability and safety integrity upon occurrence of a hazard (ISO26262)
- Formation of controllability as system / driver shared property (controllability takes into account levels of automation linking with SAE J3016)
- Integration in TARA by modifying attack's impact factor

ü Promotes synergy amongst AD systems taxonomy (SAE J3016), Automotive security (SAE J3061) and Functional safety (ISO 26262)

The model: logical overview

- Definition of controllability levels w.r.t. AD system based on the principles of system availability and safety integrity upon occurrence of a hazard
- Formation of controllability (C) as system / driver shared property (controllability takes into account levels of automation linking with SAE J3016)
- Integration in TARA by modifying attack's impact factor



L3Pilot Driving Automation

The model: Proposed new controllability factor (1/2)

(SHARED) **Controllability** scheme for AD L3 Systems Under Attack

Driver-based Controllability (C^D)	**Class**	**System-based Controllability (C^S)**	**Class**
Controllable in general *(e.g., driver shuts down infotainment module in case of unexpected radio volume increase)*	$C0^D$	**Attack can be detected** by the system and system goes into **fail-operational mode** *(sufficient vehicle level redundancy to continue full operation; no reliance on the driver).*	$C0^S$
Simply controllable *(e.g., brake to slow down/stop the vehicle in case of blocked steering column when parking the vehicle)*	$C1^D$	**Attack can be detected** by the system and system goes into **fail-silent** ***mode*** *(the system recognizes that it is receiving the wrong information due to a fault).*	$C1^S$
Normally controllable *(e.g., in case of failure of Lane Keeping Assist function; system issues a take over request and driver responds timely)*	$C2^D$	**Attack can be detected** by the system and system goes into **fail-safe mode** *(**relying on the driver** – applicable to L3 and lower).*	$C2^S$
Difficult to control or uncontrollable *(system issues a take-over-request but driver is unable to timely respond; e.g. during a lane change)*	$C3^D$	**Attack can be detected** by the system and system goes into **fail-safe mode** by performing a Minimum Risk Maneuver to bring the vehicle in minimum risk condition *(no reliance on the driver).*	$C3^S$
Genuinely uncontrollable with possible effects on other traffic participants	$C4^D$	Attack cannot be detected by the system and its effect is genuinely uncontrollable with possible effects on other traffic participants.	$C4^S$

If driver is involved, **controllability** based on **system and** on **driver** (per iso 26262) comes into play,

otherwise system-based controllability defines the controllability value (based on **fail proof system design** approach)

Modified impact value

$$MI = \begin{cases} I * 2 * \left({C^D}/{C_{MAX}} * {C^S}/{C_{MAX}} \right), & if\ C^S \epsilon \{C1, C2\} \\ I * \left({C^S}/{C_{MAX}} \right), & otherwise \end{cases}$$

The model: TARA+ look-up tables (attack profile, impact profile)

Expertise	Knowledge of the target	Equipment required	Window of opportunity
E0 (Layman)	K0 (Public info)	Eq0 (Standard)	W0 (Unlimited)
E1 (Proficient)	K1 (Restricted info)	Eq1 (Specialized)	W1 (Large)
E2 (Expert)	K2 (Sensitive info)	Eq2 (Bespoke)	W2 (Medium)
E3 (Mult.experts)	K3 (Critical info)	Eq3 (Mult.bespoke)	W3 (Small)

Attack Potential **Po** calculation

$$Po = E + K + Eq + W$$

Severity	Operational	Financial	Privacy/Legislative
S0	O0	F0	P0
S1	O1	F1	P1
S2	O2	F2	P2
S3	O3	F3	P3
S4	O4	F4	P4

Impact calculation, **MI**

$$I = 3 * S + F + 2 * O + P$$

$$MI = \begin{cases} I * 2 * \left(C^D/C_{MAX} * C^S/C_{MAX}\right), & if\ C^S \epsilon \{C1, C2\} \\ I * \left(C^S/C_{MAX}\right), & otherwise \end{cases}$$

L3Pilot Driving Automation

The model: Risk Rating

Risk value ranking (R*)		Attack potential (P)				
		P0	P1	P2	P3	P4
Modified Impact value (MI)	MI0	QM	QM	QM	QM	Low
	MI1	QM	Low	Low	Low	Medium
	MI2	QM	Low	Medium	Medium	High
	MI3	QM	Low	Medium	High	High
	MI4	Low	Med.	High	High	Critical

TARA+ Risk Levels based on Impact and Potential of an attack

Results

Attack Scenario	Attack Surface	Description	Po (Attack Potential)		Po / Probability Ranking	System / Driver Controllability Factors		Impact Factors		Impact Value / Modified Impact Value		R* Ranking
Remote Attack on Vehicle TCU (Highway)	Vehicle Wi-Fi	Inject fake commands on CAN bus via attacking TCU via exploiting vehicle Wi-Fi hotspot.	E2 Eq2	K1 W1	6 / Pr3 (Possible)	$C3^D$	$C2^S$	S4 F4	O4 P3	27	20.25 (MI3 - HIGH)	HIGH
Lidar sensor spoofing (Highway Traffic Jam)	Lidar	Spoof the vehicle's lidar by optical means by generating signals that make objects disappear from the scene.	E1 Eq2	K1 W3	7 / Pr2 (Unlikely)	$C2^D$	$C2^S$	S4 F3	O4 P0	23	11.5 (MI2 - MEDIUM)	MEDIUM
Road infrastructure attack (Urban)	Static road sign	Modify zebra crossing sign on the road surface creating the artifact of objects in front.	E0 Eq0	K0 W0	0 / Pr4 (Very Possible)	-	$C4^S$	S3 F1	O3 P0	16	16 (MI2 - MEDIUM)	HIGH

Low driver controllability level BUT high system controllability level

High Modified Impact instead of Critical due t controllability assumption

Recommendations produced … [extract from D4.2]

System resilience
Controllability

[ISO 26262]

- […]
- Make sure that cyber security design takes into account aspects of the entire vehicle lifecycle (attacks by a malicious mechanic or during an OTA update are considered probable).
- Promote OBDII standard evolution to integrate security requirements, since physical attacks can no longer be ignored.
- Increase awareness among your users about ADF functions by visualizing what the sensors perceive and by using periodic messages on the TCU. Overall, observability of an attack leads to higher controllability.
- Make sure all the critical ECU components are physically separated from the rest of the system.
- Prevent eavesdropping of wireline and wireless communication.
- Prevent tampering with wireline and wireless communication.
- Secure sensor-based perception by allowing for sensor redundancy and by developing Intrusion Detection Systems specifically for dynamic sensor data spoofing (taking into account the recent literature on adversarial machine learning).

Conclusions

- Security threats do not create new safety hazards (unsafe states) but alter the likelihoods of existing states

  à Security, the new safety requirement

  (new ISO/SAE CD 21434 collaboration)

- Risk assessment for multiple attack scenarios – future work
- A novel controllability definition and classification was proposed that handles both the AD system and the driver in a joint scheme

  à Still, other road users are missing from “controllability” definition

  à Quantification of system withstand is a life-cycle process (new system updates vs new forms of attacks)

Thank you for your kind attention.

This project has received funding from the European Union's Horizon 2020
research and innovation programme under grant agreement No 723051.