Submitted by the experts
from CLEPA and OICA

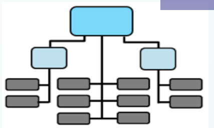
Informal document **GRVA-06-08rev1**
6th GRVA, 3-4 March 2020
Agenda item 4

Explanations for the suggested amendments to GRVA-05-05-Rev.1

Explanation for 48 months transition time

1

Vehicle type for cyber security regulation = Essential aspects of the E/E architecture and external interfaces with respect to cyber security.



2

One E/E architecture can be built into multiple carlines

3

It takes up to 4-6 years for the entire development of an E/E architecture

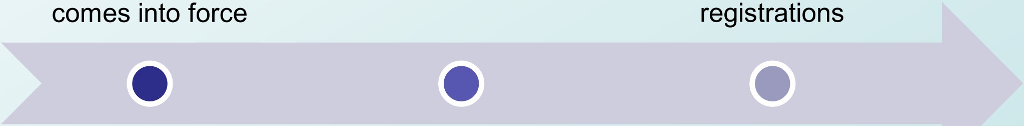
For CS, the development involves contracting suppliers with a certified CSMS to ensure CS throughout the supply chain.

4

Type approval procedure and timeline in the EU

Various system type approvals e.g. steering, braking, in the future cyber security etc.

Whole vehicle type approval



Jan 2021
UN CS regulation comes into force

July 2022
In the EU, CS mandatory for new whole vehicle types

July 2024, CS mandatory for first registrations

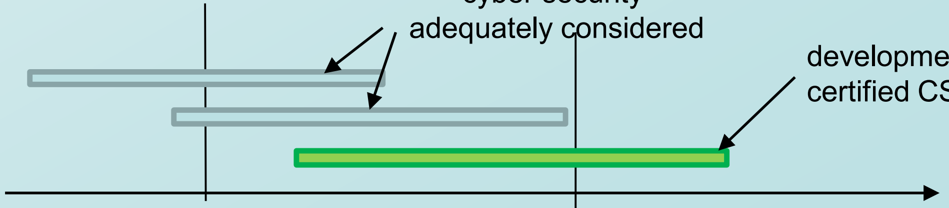
5

Hard points for existing architectures for formal and technical reasons:

7.3.1. Existing architectures have not been developed under a certified CSMS.

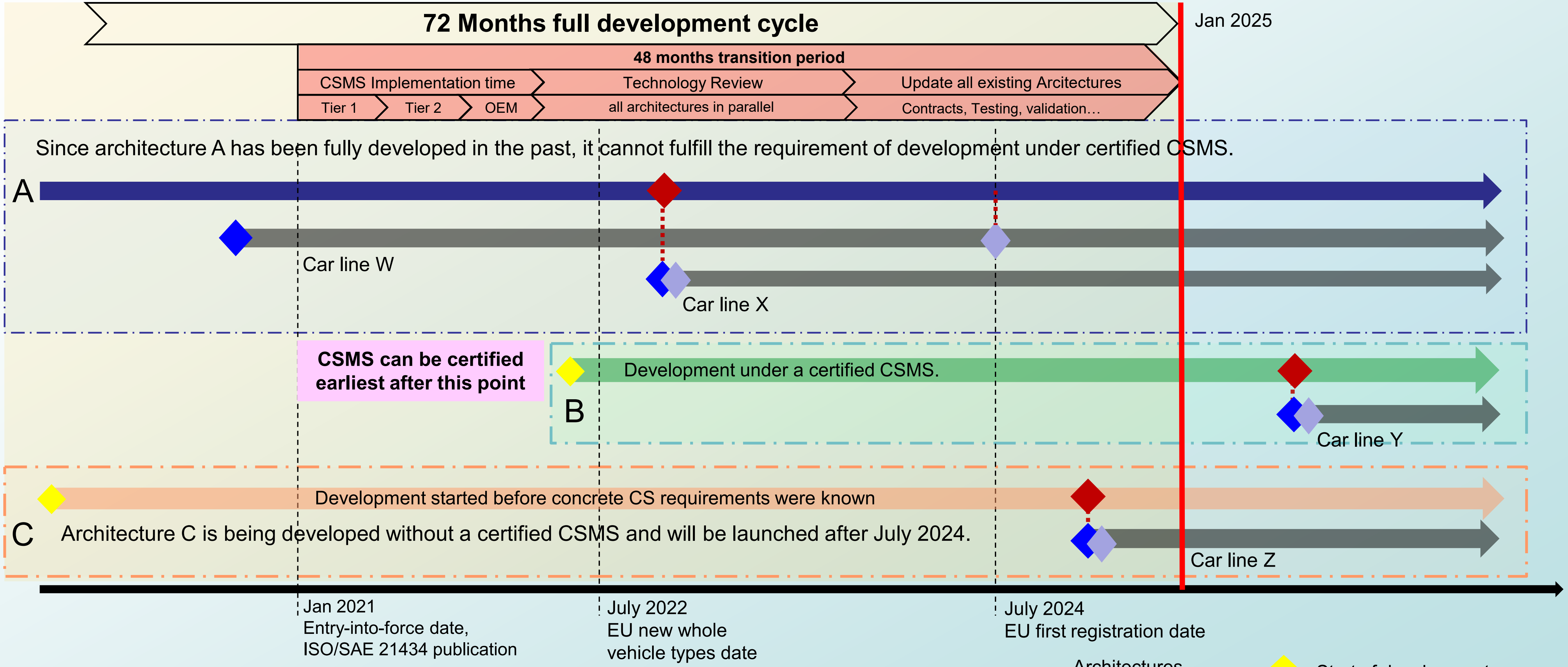
7.3.4. Existing architectures cannot be retroactively brought in compliance with Annex 5.

The 48 months transition period will allow OEMs to incorporate certified CSMS processes (possible only after the regulation comes into force) in the development of their E/E architectures. Also, suppliers need time to incorporate CS processes.


cyber security adequately considered
development under certified CSMS
Entry-into-force date
48 months after entry-into-force date

Update: Explanation for 48 months transition time

CLEPA
European Association of Automotive Suppliers


72 Months full development cycle
Jan 2025
48 months transition period
CSMS Implementation time
Technology Review
Update all existing Arcitectures
Tier 1
Tier 2
OEM
all architectures in parallel
Contracts, Testing, validation…
Since architecture A has been fully developed in the past, it cannot fulfill the requirement of development under certified CSMS.
A
Car line W
Car line X
CSMS can be certified earliest after this point
Development under a certified CSMS.
B
Car line Y
Development started before concrete CS requirements were known
C
Architecture C is being developed without a certified CSMS and will be launched after July 2024.
Car line Z
Jan 2021
Entry-into-force date,
ISO/SAE 21434 publication
July 2022
EU new whole
vehicle types date
July 2024
EU first registration date

Justification for the 48 months transition period

- Manufacturers need to adapt their internal processes
- Review and perform risk assessment for **all existing architectures** and bring them in line with requirements of 7.3.4.
- Update contracts with suppliers. The suppliers in turn need to contact tier-2 suppliers.
- In order to fulfill the supply chain requirement of the regulation, the suppliers need to be certified for cyber security.
- 48 months is representative for the timeframe required for change management of existing architectures not for new developments.

Architectures

🟦 A

🟩 B

🟧 C

⬛ Vehicle types

◆ Start of development

◆ CS system approval mandatory

◆ European WVTA

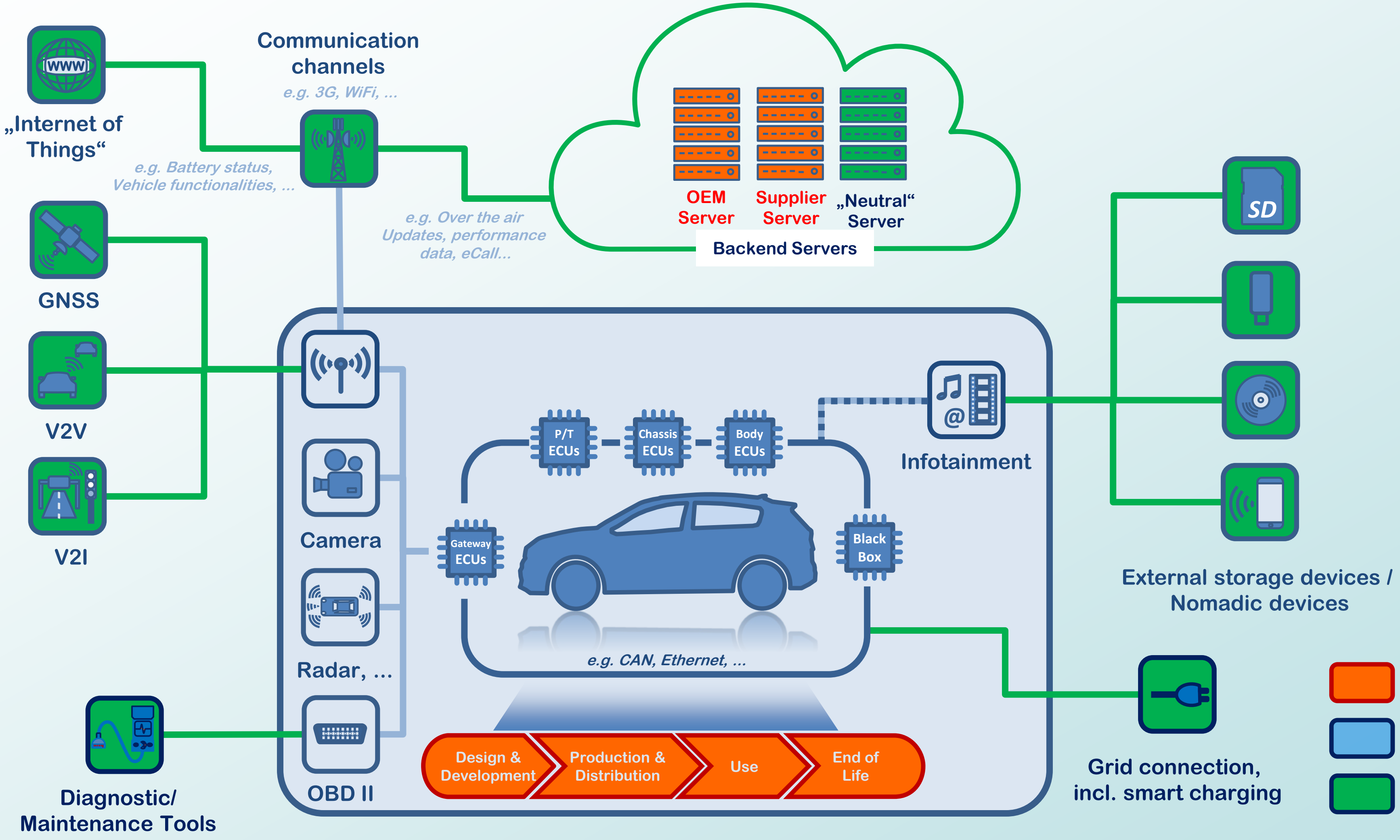
◆ System Type approval

Comments on mitigation tables in Annex 5

- Current mitigation tables are **incomplete, outdated, and need regular updates** when new vulnerabilities and mitigations are identified.
  - ✓ Exemplary gaps: repair shop tools, production tools etc.
- Mitigations beyond the vehicle type would stretch the vehicle type scope beyond manageable limits: +backend, +internet, +production tools, +smartphones…
- According to the 1958 Agreement, vehicle **type only concerns “wheeled vehicles”** themselves. The mitigation tables include mitigations that are not intended for the vehicle type (e.g. backend server mitigations) and are mixing the responsibilities of ISMS (Information Security Management System) and CSMS (Cyber Security Management System).
- It does not make sense to maintain a list of fixed mitigations when the vulnerabilities and attacks keep evolving.

Proposal how to proceed with Annex 5 B & C

Example of reference Model “Vehicle and its Eco-System“

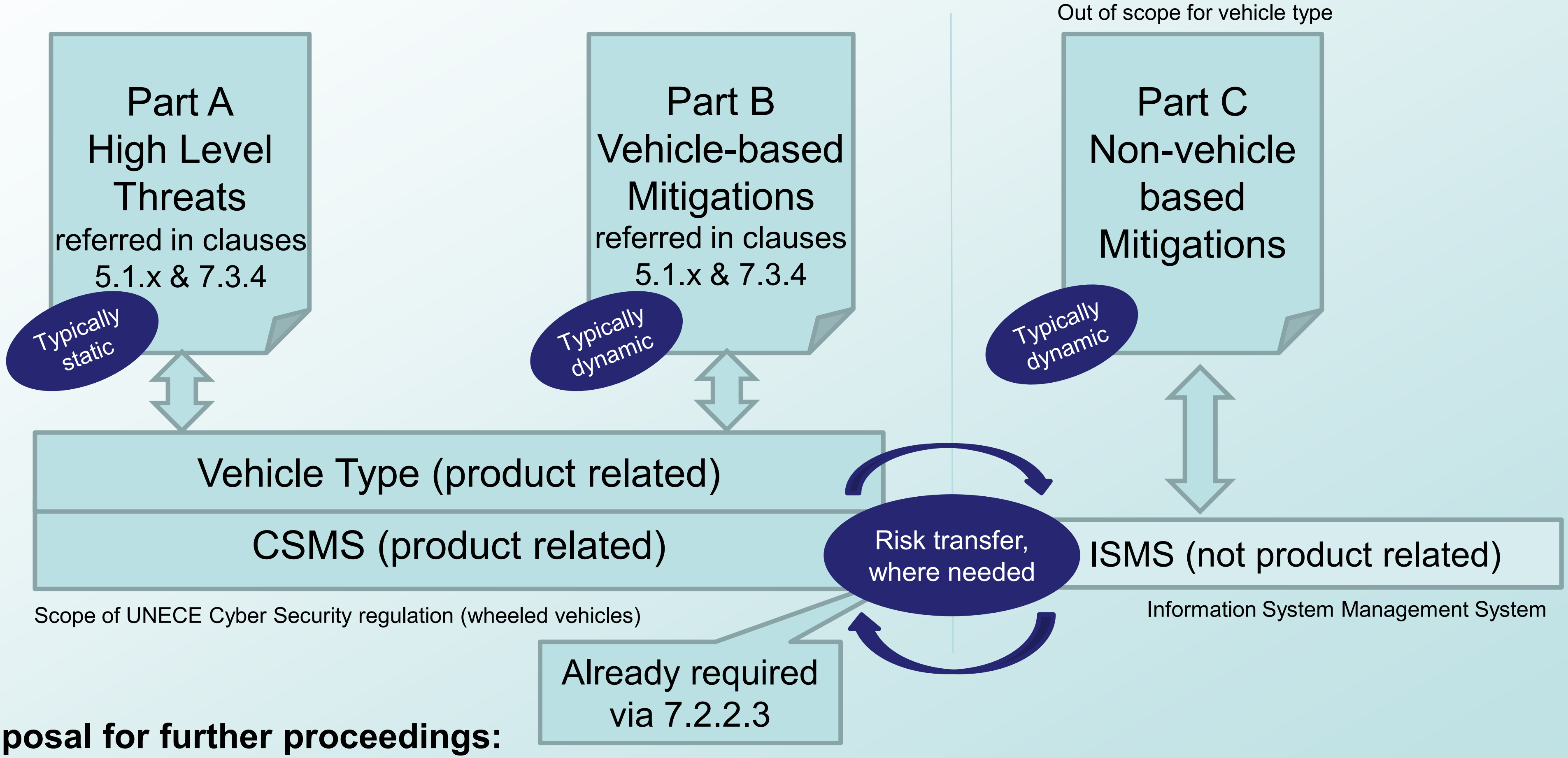


🟧 *Subject to Assessment of the Organisation*

🟦 *Subject to Assessment of Vehicle Type*

🟩 *Out of Scope*

Proposal how to proceed with Annex 5

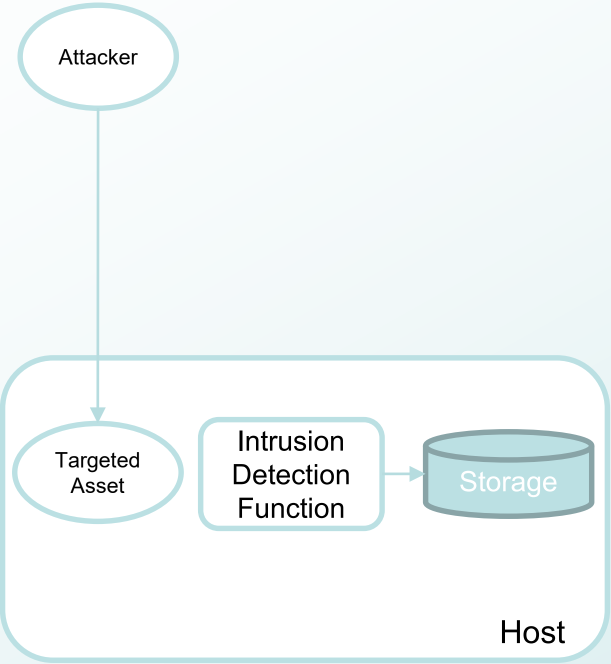


Proposal for further proceedings:

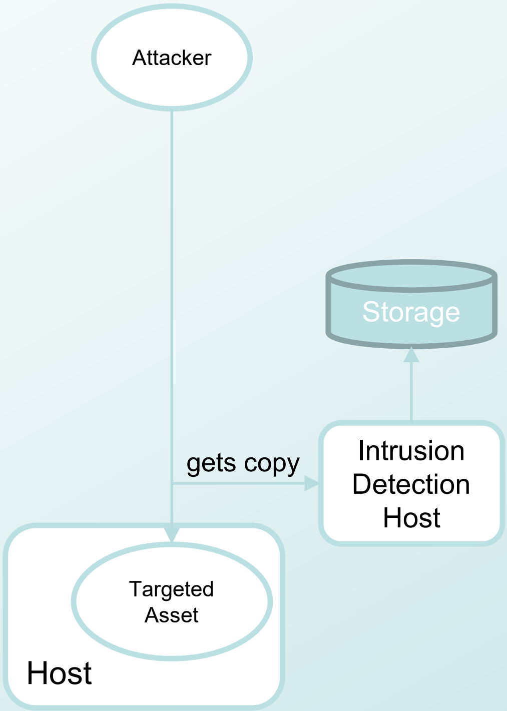
1. Short term: Split list of mitigations into two lists (parts B&C)
2. Long term: Transfer parts A&B&C to an open automotive vulnerability database and improve it continuously, like similar sectors do.

Intrusion Detection (ID) vs. Intrusion Prevention (IP) Large differences between two technologies.

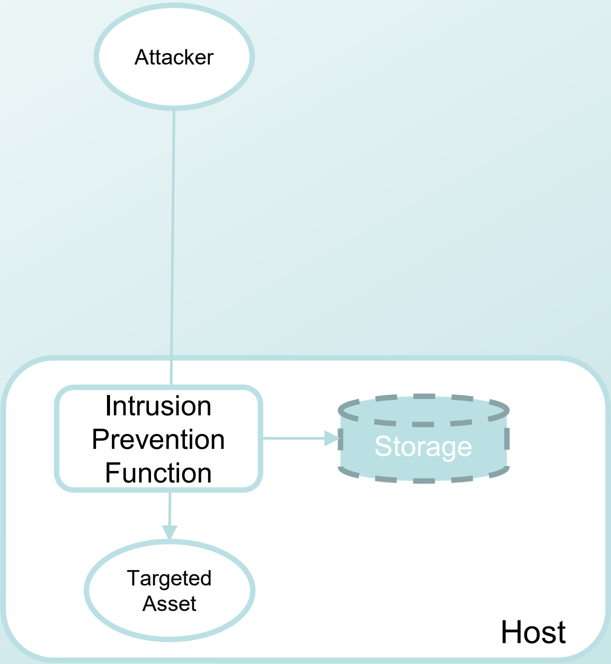
Host-based
Intrusion **Detection**



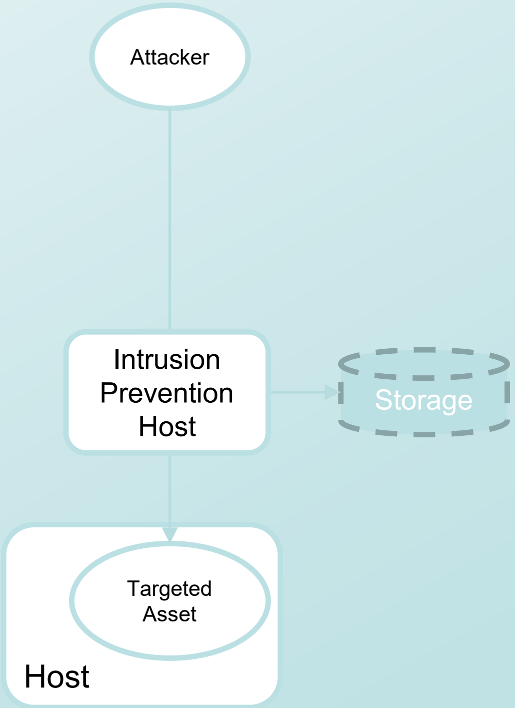
Network-based
Intrusion **Detection**



Host-based
Intrusion **Prevention**



Network-based
Intrusion **Prevention**



- Logging is main function of ID system.
- Typically log resources are high (network, storage, CPU…).
- Defence is second to insight and intelligence.

- Typically log resources are low.
- Defence is immediately applied („realtime“) for known and precisely identified attacks.

- Both technologies rely on regularly receiving updates in order to identify new attacks by new characteristic patterns.

“Detect” and “Prevent”
IT Requirements vs. Automotive Requirements

ID / IP aspect	IT	Automotive
Administrator/root interaction in case of problems	There is an administrator who can tell by expertise and human judgement to clarify problems. Interacts on a regular basis (e.g. daily).	There is no administrator available.
Performance for detection/prevention	Detection: verbose logging causes high CPU and storage demands Prevention: performance is key (« wire-speed! »)	Detection: logging must not cause drawbacks in other functions. Prevention: other performances must be preserved at all costs, e.g. safety functions.
False Positive	Shall be avoided in order to not block production traffic. False Positive could cause IT function to fail.	Shall be avoided at all costs in order to not block safety related messages which could cause fatal accident or malfunctions.
False Negative	Acceptable but should be reduced to close 0.	Acceptable but should be reduced to close 0.
Baselines and deviations	Baselining extremely difficult because of changing environments.	Baselining possible but gaps can cause fatal accidents or malfunctions, s. above. Functions have to be tested in all possible conditions to exclude errors. This includes updates.
Updates	Are necessary to keep up to date with attack pattern changes (similar to antivirus identification patterns). There have been cases of an update causing IPS blocking (unintended 100% load). Log configuration changes may change load heavily.	Must not increase to the load beyond specified range. Deviations can cause fatal accidents or malfunctions, s. above. Log configuration changes must not change load beyond specified range.
Resource Consumption Behaviour (e.g. due to update or increased data traffic)	Is allowed to increase basically because the system itself is monitored. Should not increase on dedicated components (e.g. servers) over lifetime. Admin intervention would be inevitable.	May increase on dedicated components within specified limits. Must not increase on safety related components (with ASIL rating) over lifetime. Admin intervention would not be possible.
Lifecycle	Typically exchanged after 3-5 years of operations. New hardware to be installed on existing premises.	Has to work for lifetime of the vehicle which is much longer than in the IT domain.
Disk space	In IT systems data storage is actively administered.	Particular data space management algorithm needs to be integrated and log data optimized.
Prevent vs. Detect.	The requirements for IPS in terms of false positives and performance are way higher than for IDS. This leads to the use of differing technology.	Where the reasonable use of ID seems within reach, intrusion prevention technology shall be used with extreme caution due to the high safety relevance in the automotive domain compared to the IT domain. There further research is required.

Comments on requirement to “prevent cyber-attacks”

- Automotive technology requirements are higher that in IT. There is less tolerance towards technology failures, see previous slide.
- Currently, there is no proven automotive technology available to “prevent cyber-attacks”: Features to prevent cyber-attacks (i.e. intrusion) still lack maturity and yield a high risk of causing heavy problems in vehicles.
- Generally the relatively long lifetime-support and the lack of both administrative skills and privileges make it problematic to transfer existing IT concepts to automotive domain 1-to-1.

Further remarks:

7.3.7. The vehicle manufacturer shall implement measures for the vehicle type to:

(a) detect ***and respond to*** ~~***prevent***~~ *cyber-attacks against vehicles of the vehicle type;*

- 7.3.7 obviously focuses on providing evidence and indication to detect attacks and manipulations. Measures to “prevent cyber-attacks” go beyond this idea.
- Wording issue – Impossibility to prevent cyber-attacks: Attacks may not be preventable (e.g. DoS attacks) because the attacker simply decides to attempt the attack. (In other words: intrusion ≠ cyber-attack)
- According to type approval mechanisms new technology needs sound justification to be transferred to legacy products. In the current draft, 7.3.7 a) does not distinct between existing and new E/E architectures.

Where 7.3.7 leaves space for solutions *outside of vehicle types* (“measures for vehicles types”) the requirement nonetheless uses pre-defined terms which shall be avoided in legal texts. Reword “prevent” to “respond”!