Continental
The Future in Motion

Simple security countermeasures to achieve complex behavior.

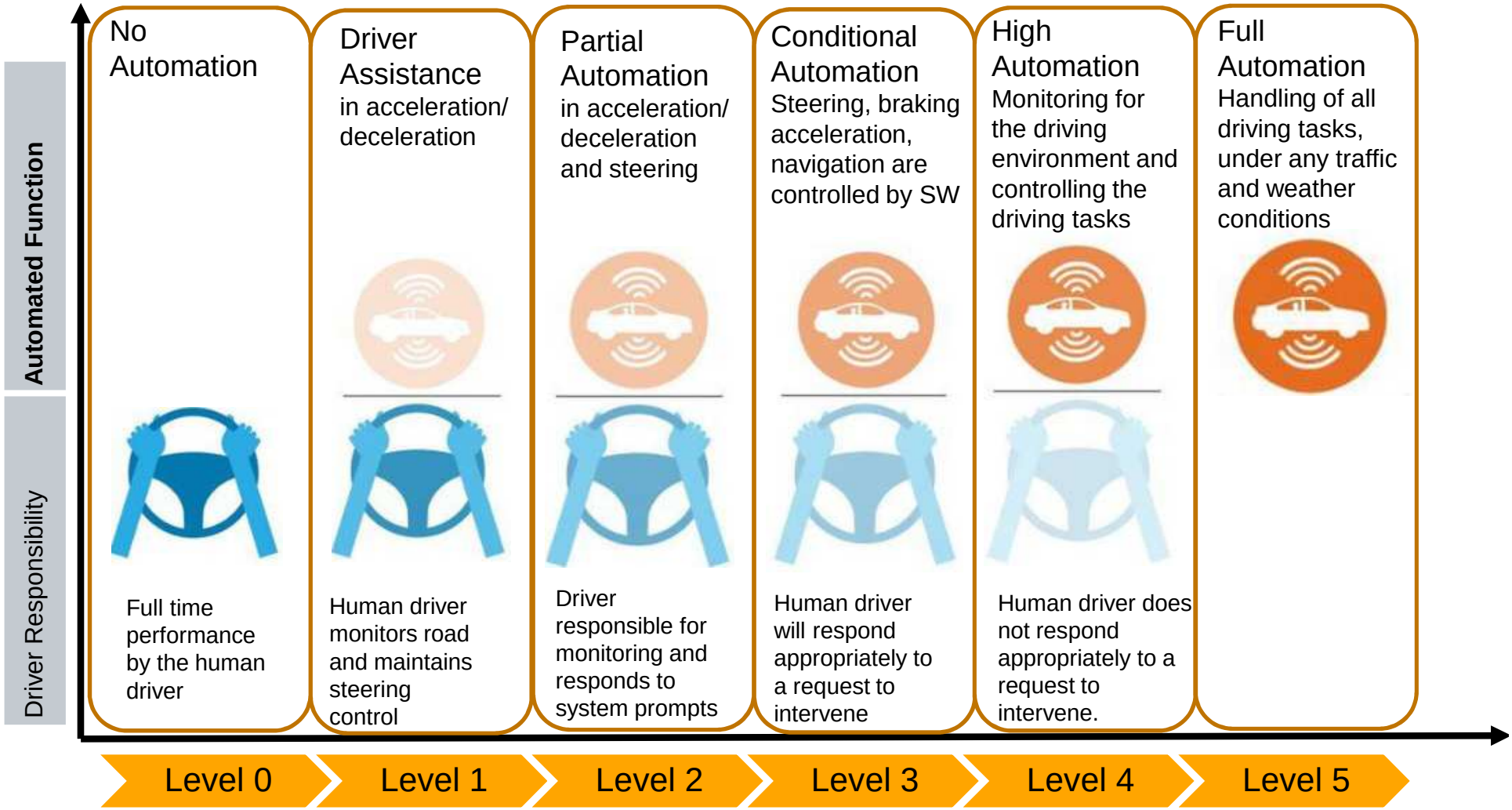
"If you think cryptography is the solution to your problem, then you don't know what your problem is."
- Peter G. Neumann

Iasi, CyberShare 2019

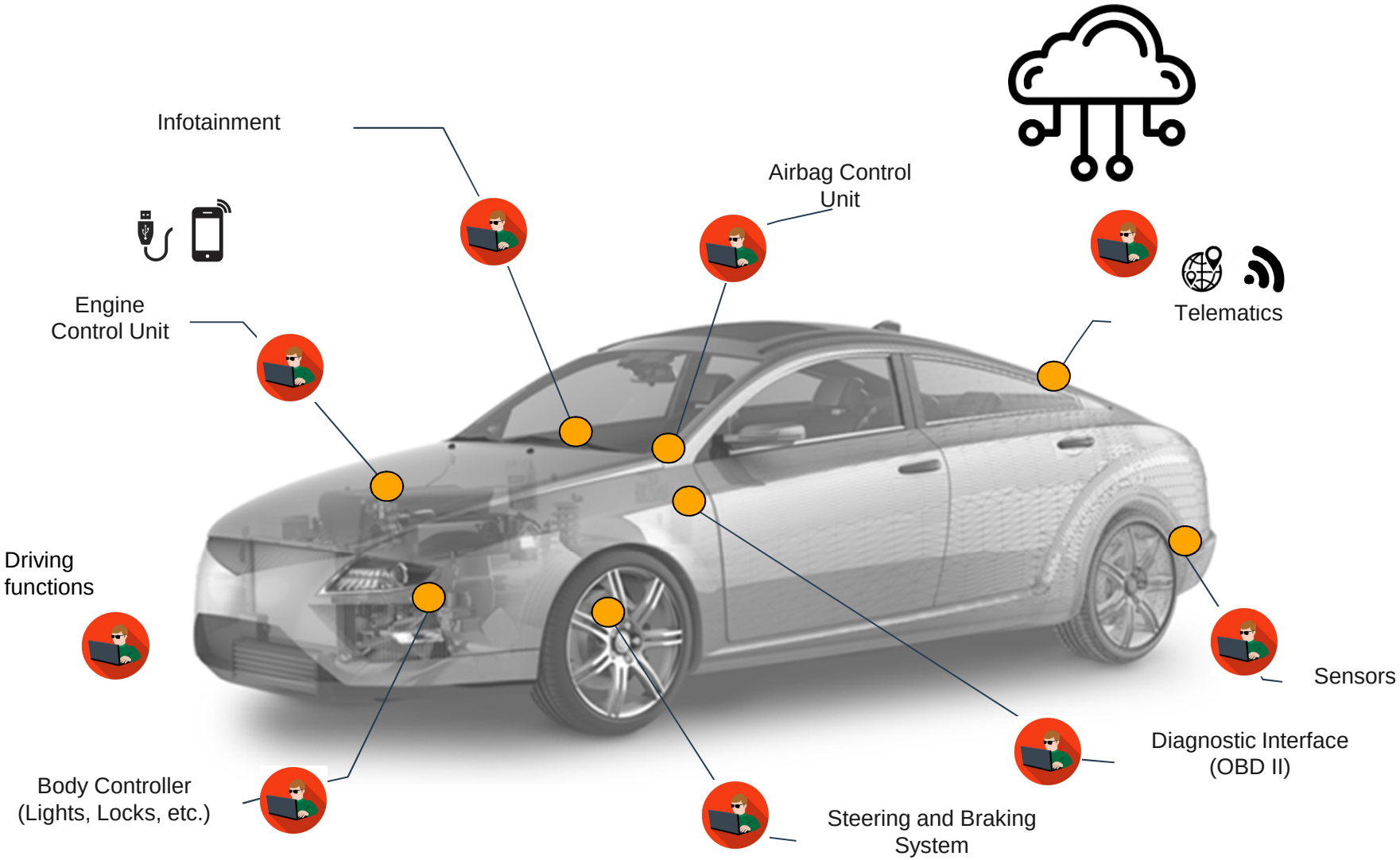
Agenda

1. Levels of Automation
2. Attack Surface
3. Recent Automotive Incidents
4. Attacks & Countermeasures
5. Proposed Concept - Patented Solution
6. Conclusions
7. Bibliography

Levels of Automation



Attack surface



Recent automotive incidents

BMW ConnectedDrive

- No communication security

2015

[Hackers Remotely Kill a Jeep on a Highway]

Tesla remote control

- Vulnerability to MIM attack;
- Autopilot takeover leads to complete remote control

2016

2019

Volkswagen remote control

- Exploitability of network open ports and access rights

2017

Malware attacks

- Proof of concept research for ransomware attacks
- Crypto mining, e.g. use car ECU resources

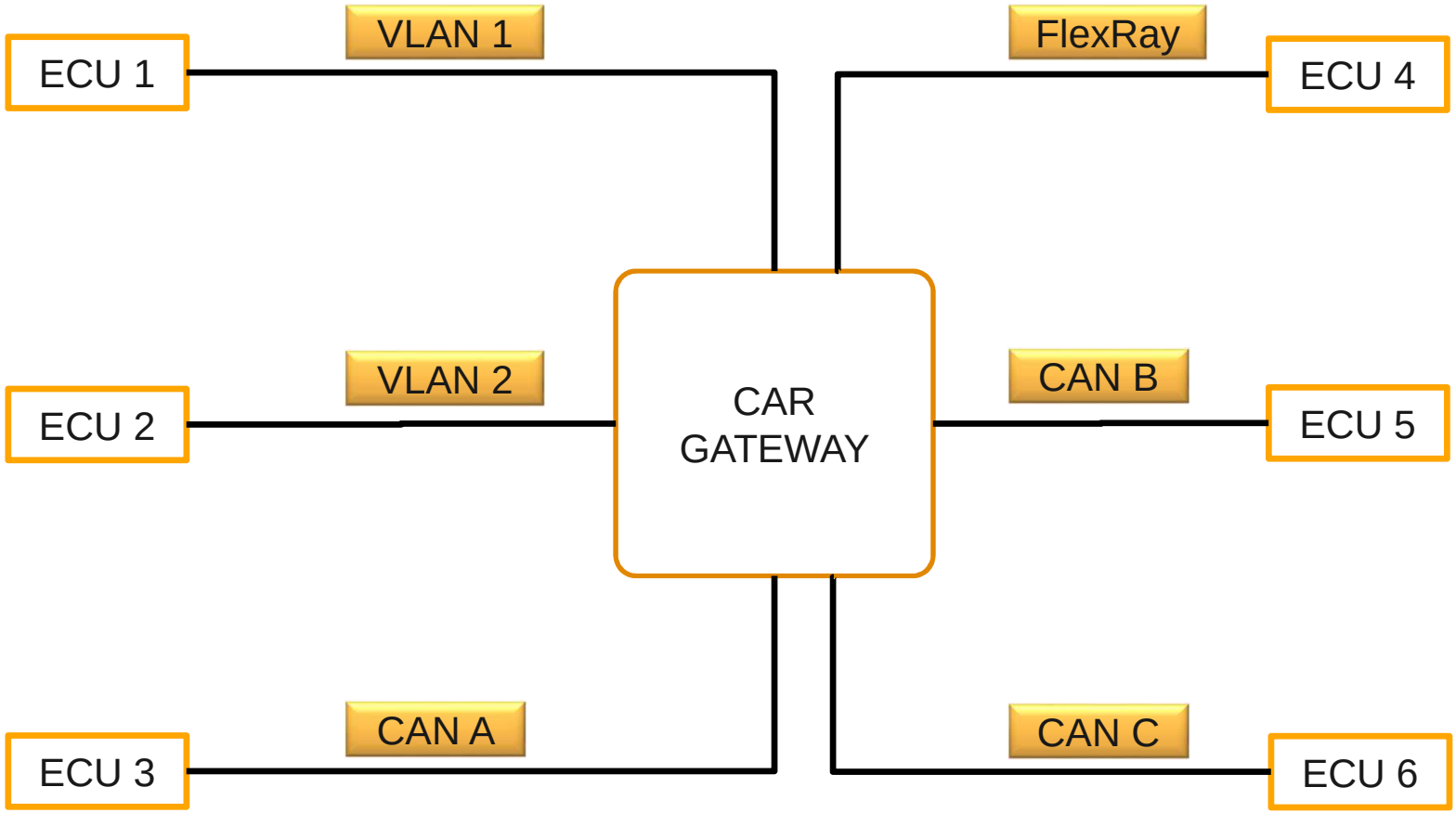
> 2018

Attacks & Countermeasures (1/3)
(Physical) Tampering

- Physical access to car ECUs that allows to directly read data (e.g. flash memory)
- Rowhammer: executing a program over and over on a "row" of transistors in a computer's memory chip - exploit tiny data changes in the adjacent row to gain more system access.
- Side-channel attacks (e.g. power analysis attacks)

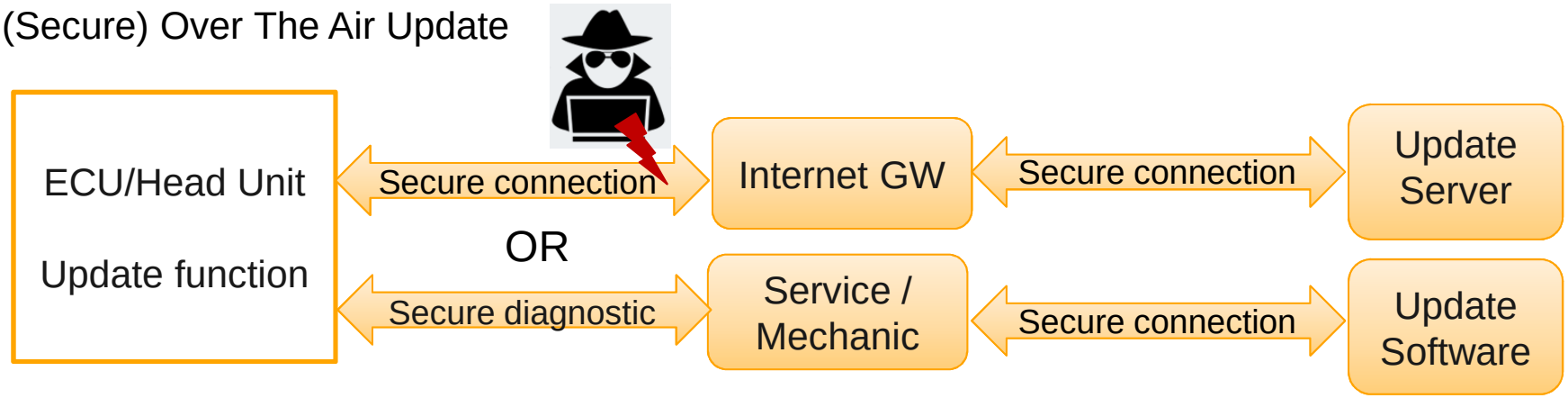
- Trusted Platform Module: at minimum use a hardware anchor.
- Chain-of-trust: sequential start of the next validated routine.
- Secure boot: authentic and integer boot loader/environment.
- Execution Isolation:
  - HW: Trust Zone from ARM or Trust Execution Environment
  - SW: containers, virtualization

Attacks & Countermeasures (2/3)
Network Isolation

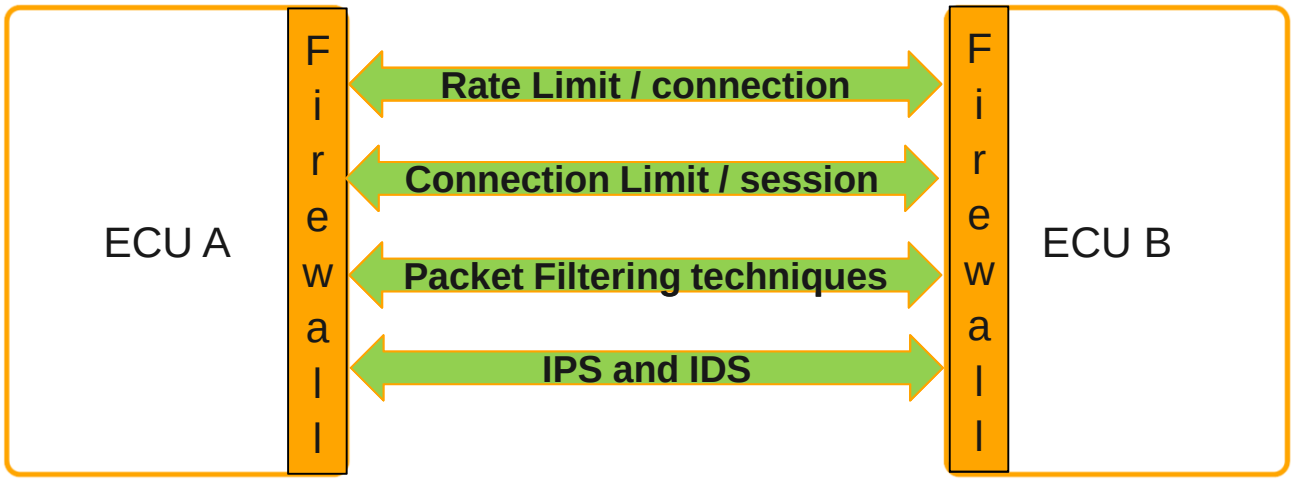


Attacks & Countermeasures (3/3)
Firewall, IDS, IPS

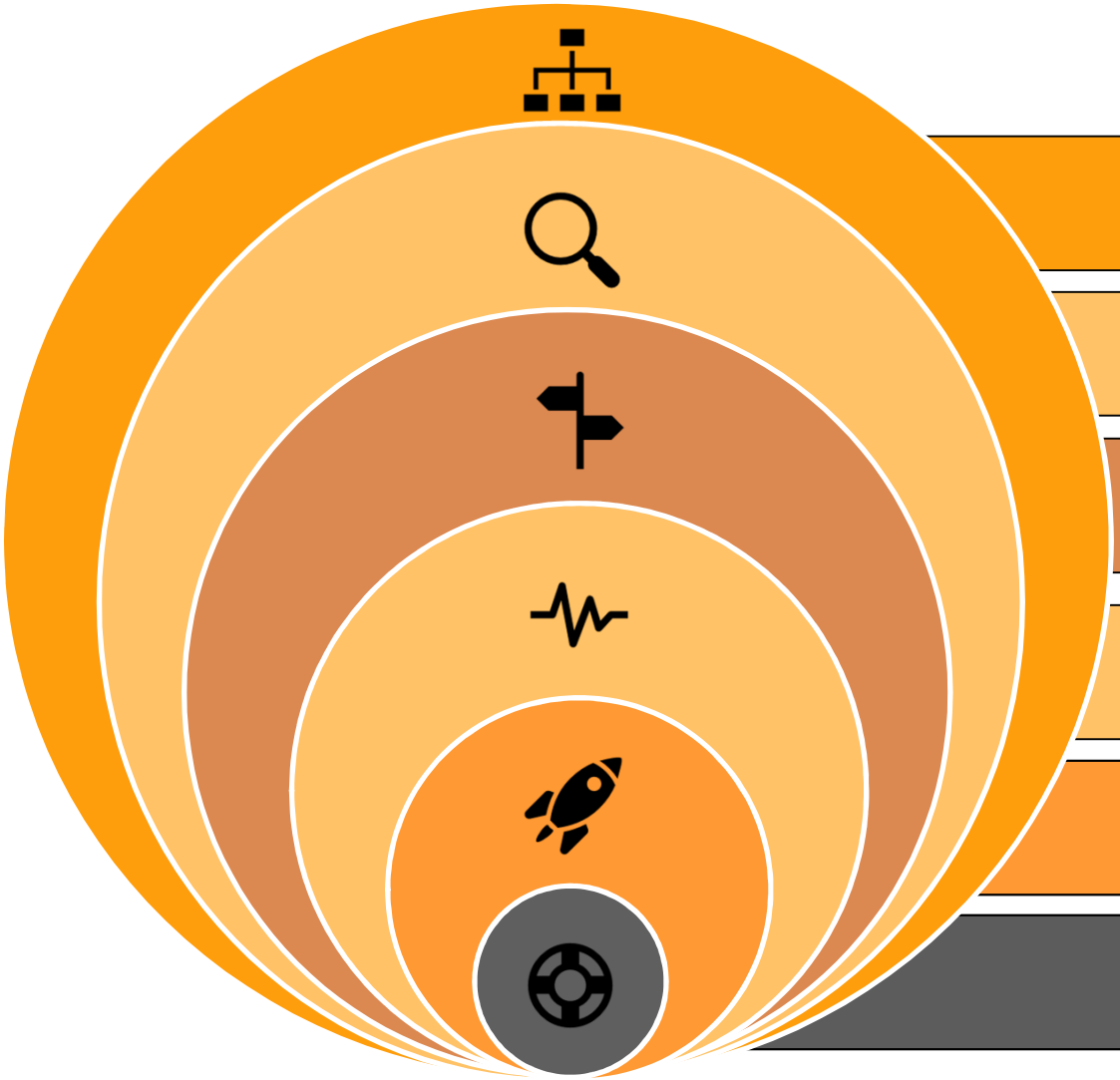
› (Secure) Over The Air Update



› Firewall with IDS and IPS capabilities



Security basic principles

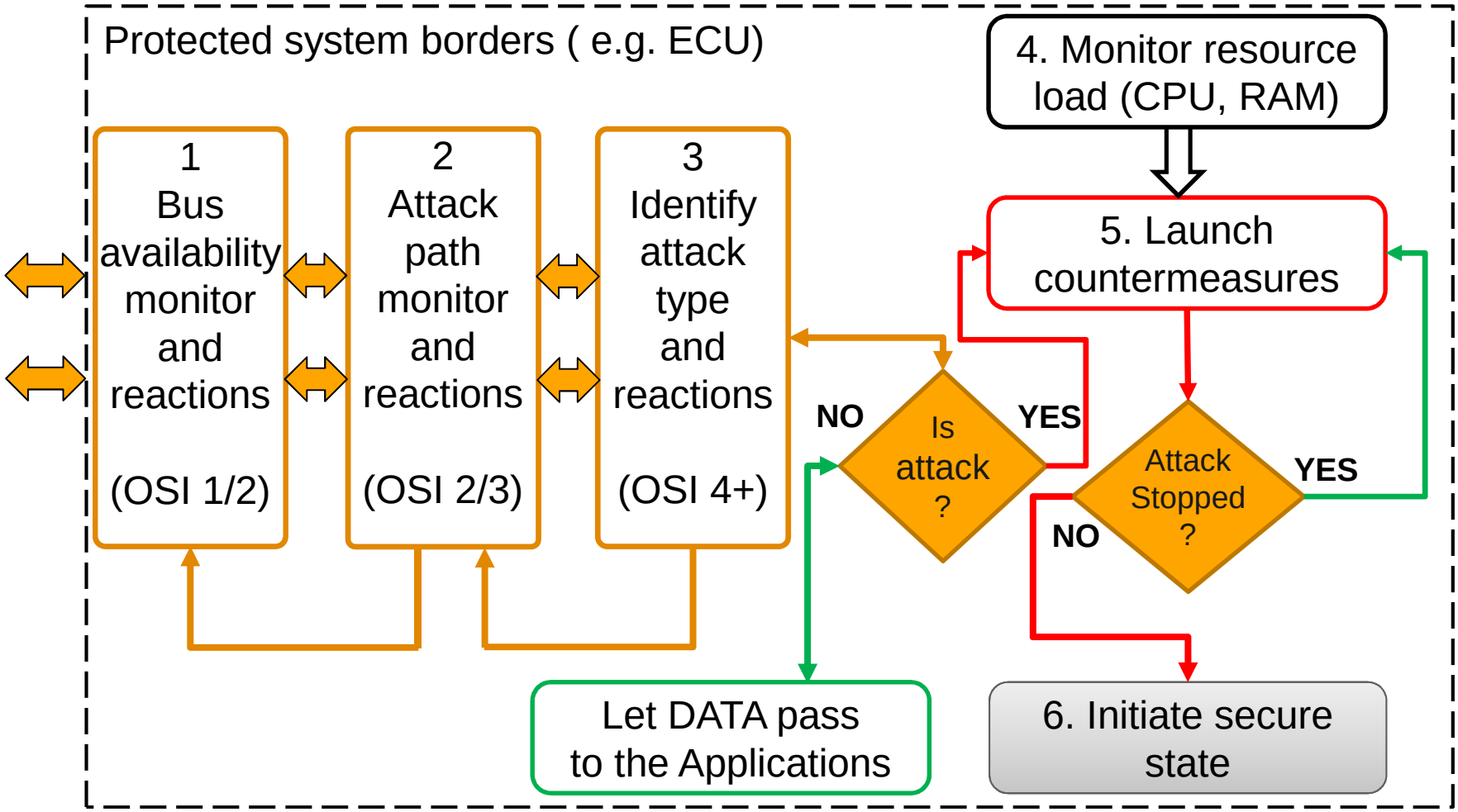


- Monitor bus availability
- Monitor attack paths / channels
- Identify attack type
- Monitor host HW resources (e.g. CPU, RAM)
- Launch countermeasures
- Initiate secure state

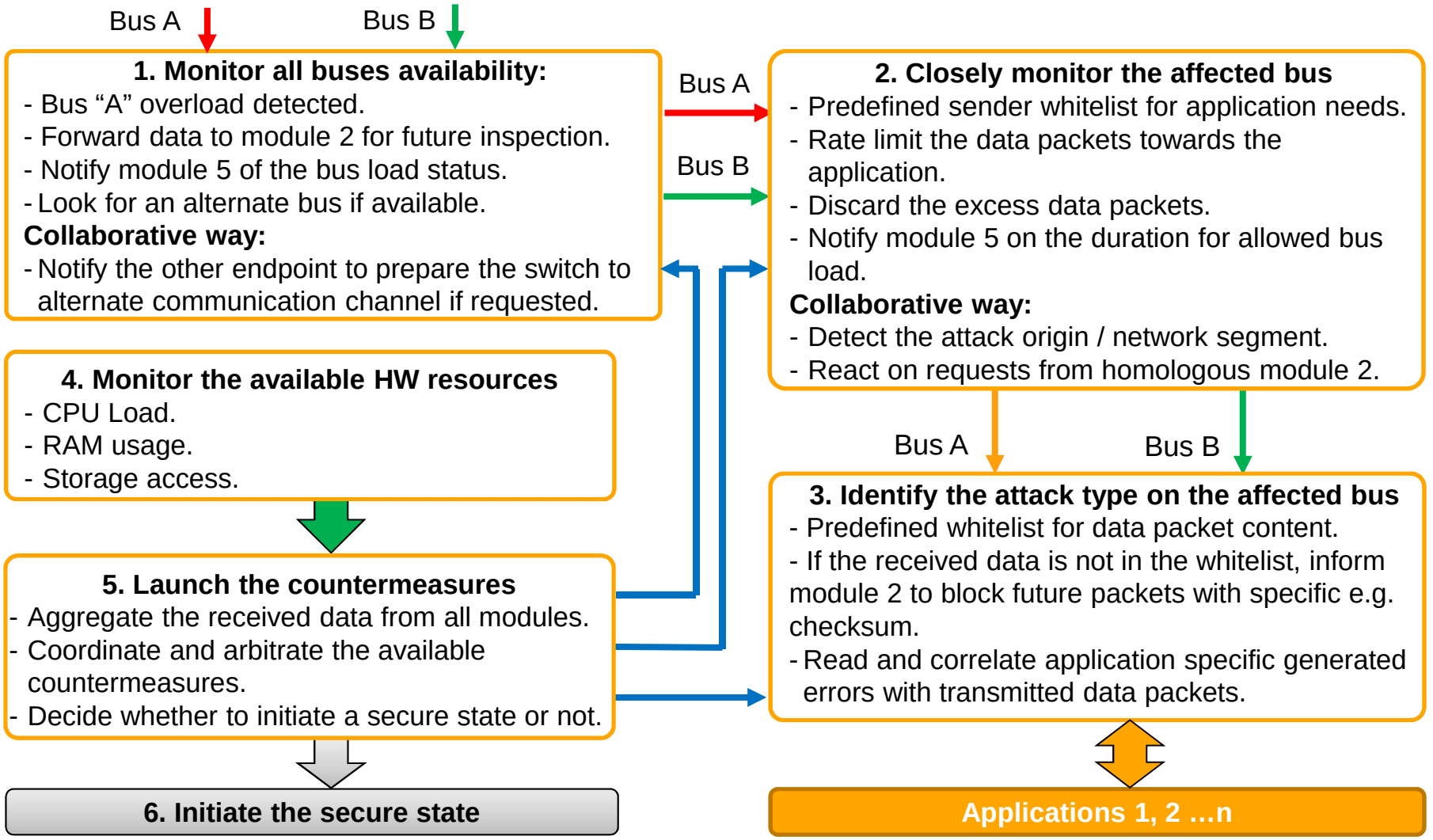
Automotive main advantages

- **Predefined and known software packages**:
  - mostly made “in-house”.
  - custom made for specific needs.
- **Software is not changing often**:
  - max. 5% changes on the entire lifecycle of the vehicle.
  - mostly bugfixes for functional or safety.
- **Predefined and known communication matrix**:
  - used communication bus – e.g. CAN A and Ethernet B.
  - sent and received data and content.
  - what function send/receive which data at what timeframe.

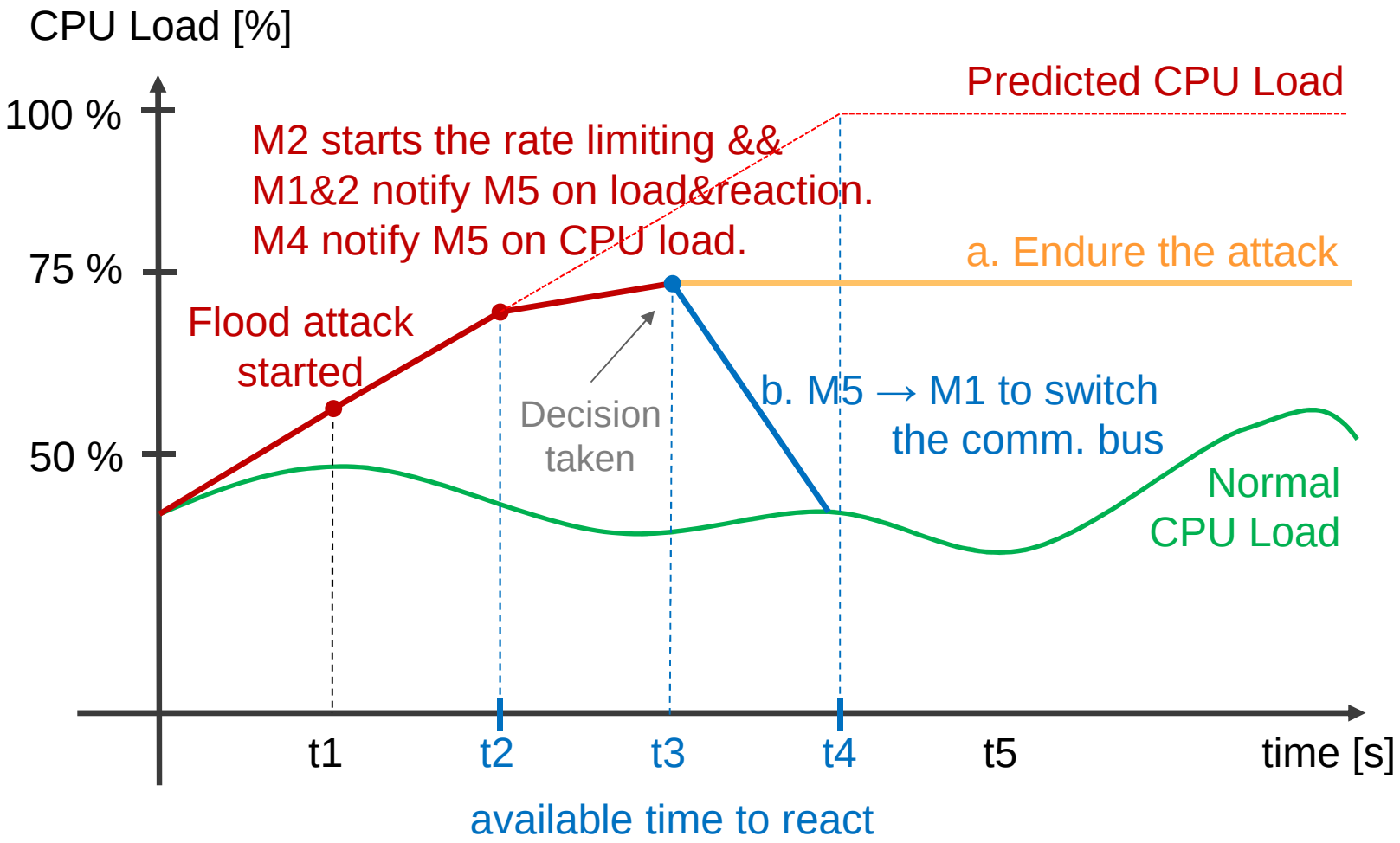
Simplified system diagram



Case study – flood attack



Case study – Countermeasure time constrains



Conclusions

- Abnormal system behavior detection and reaction with almost no false-positive.
- Unknown threats detection due to predefined and known monitored parameters.
- Ability to combine multiple countermeasures
- Close collaboration with the protected application.
- Resource friendly due to push-back mechanism.
- Adaptive to on-going attacks.
- Collaborative with other implementations of this system.

Bibliography

- Volkswagen: https://threatpost.com/volkswagen-cars-open-to-remote-hacking-researchers-warn/131571/
- Hackers disable brakes in moving cars: https://www.wired.com/2013/07/hackers-disable-brakes-in-moving-cars/
- BMW: https://www.cs.bu.edu/~goldbe/teaching/HW55815/presos/bmw.pdf
- https://www.automotiveworld.com/news-releases/fev-analyzes-automotive-cyber-attacks/
- Tesla: https://www.theguardian.com/technology/2016/sep/20/tesla-model-s-chinese-hack-remote-control-brakes .
- Mercedes : http://www.telegraph.co.uk/news/2017/11/27/mercedes-car-stolen-without-using-key-seconds-relay-theft/
- Keyfob: https://hackaday.com/tag/keyfob/

Thank you
for your kind Attention!

Irina Oancea

Continental Automotive Romania
Chassis and Safety
ADAS System Engineering
Iasi, Romania

eMail: Irina.Oancea@continental-corporation.com

Florin Iftene

Continental Automotive Romania
Chassis and Safety
ADAS System Engineering
Iasi, Romania

eMail: Florin.Iftene@continental-corporation.com