Cybersecurity for the Software-defined Vehicle

Robert Kaster

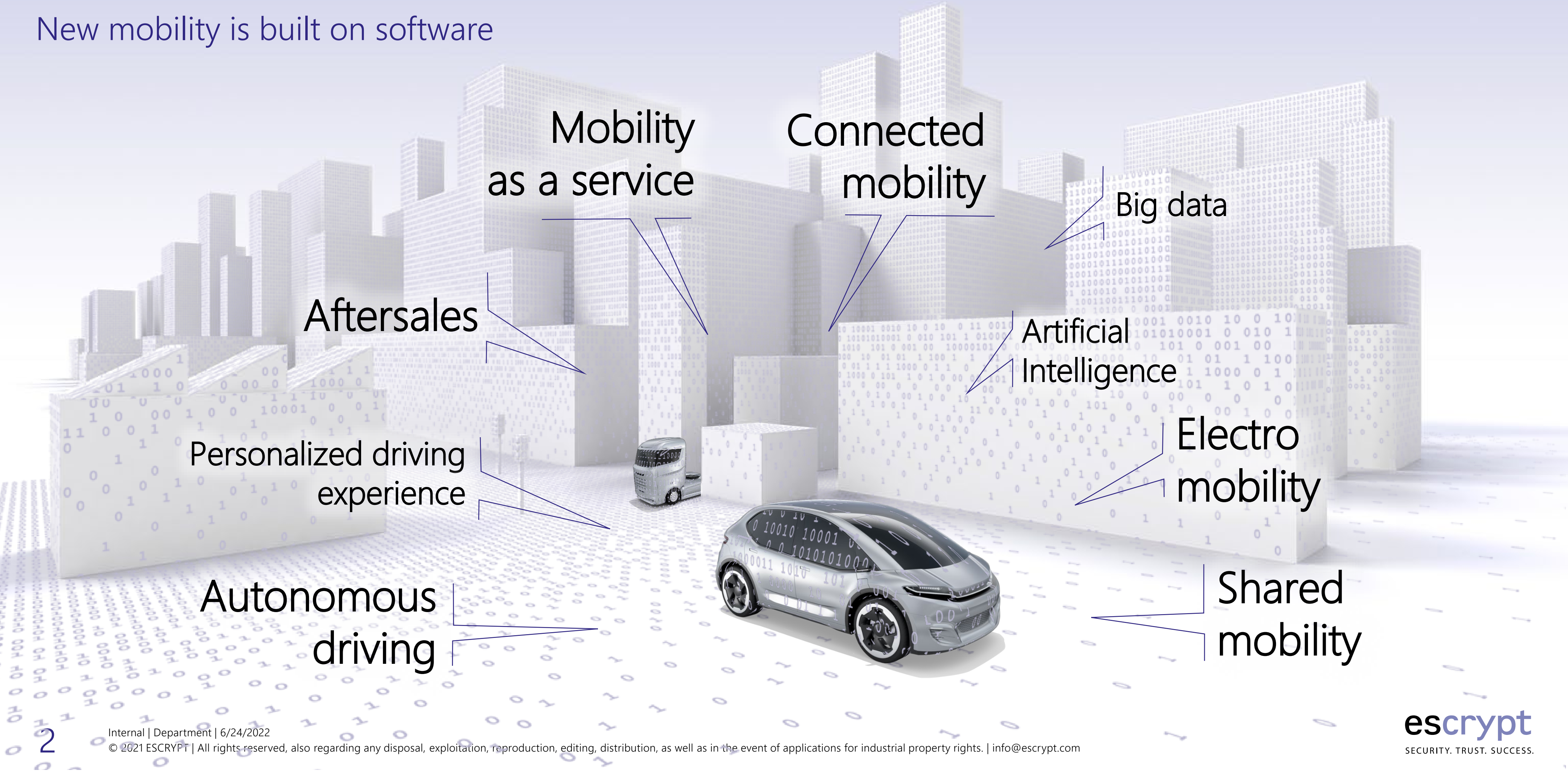
Bosch, Chief Technical Expert, NA Product Security Lead

escrypt

SECURITY. TRUST. SUCCESS.

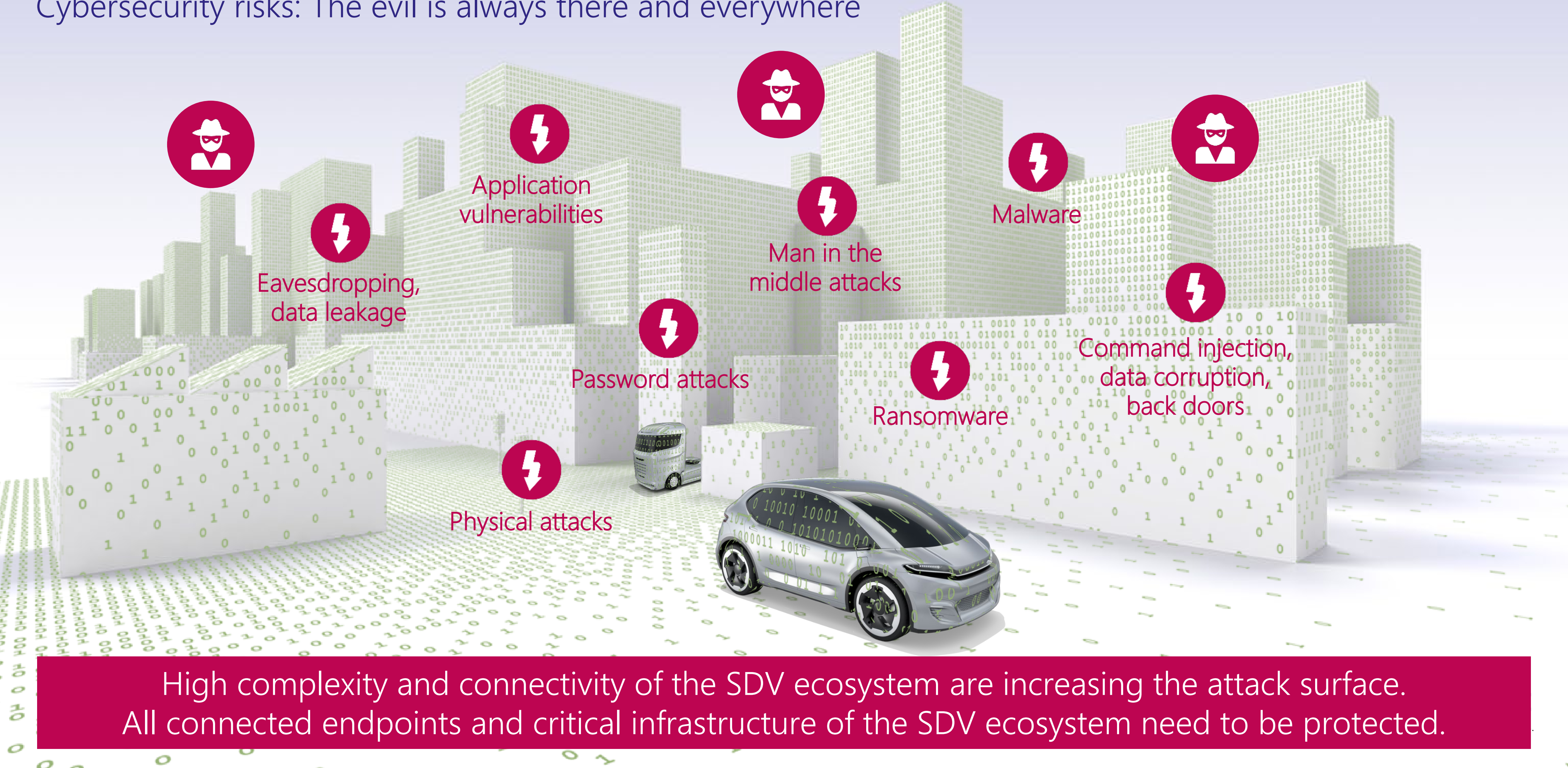
Software-defined vehicle

New mobility is built on software



Software-defined vehicle

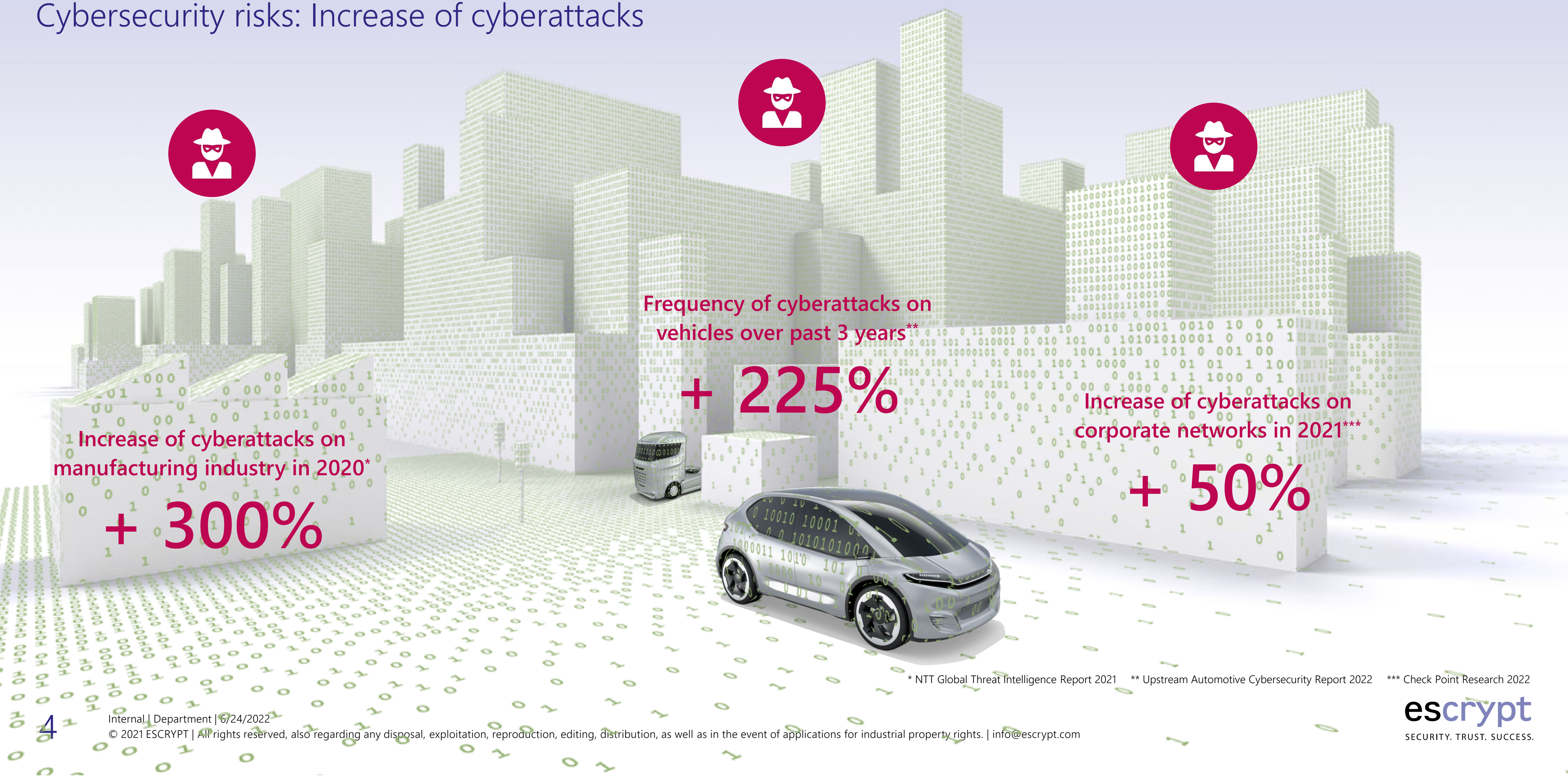
Cybersecurity risks: The evil is always there and everywhere


Application vulnerabilities
Eavesdropping, data leakage
Man in the middle attacks
Malware
Password attacks
Ransomware
Command injection, data corruption, back doors
Physical attacks

High complexity and connectivity of the SDV ecosystem are increasing the attack surface.
All connected endpoints and critical infrastructure of the SDV ecosystem need to be protected.

Software-defined vehicle

Cybersecurity risks: Increase of cyberattacks



Increase of cyberattacks on manufacturing industry in 2020*

+ 300%

Frequency of cyberattacks on vehicles over past 3 years**

+ 225%

Increase of cyberattacks on corporate networks in 2021***

+ 50%

* NTT Global Threat Intelligence Report 2021 ** Upstream Automotive Cybersecurity Report 2022 *** Check Point Research 2022

Software-defined vehicle

Security is key enabler for the SDV

Protect safety-critical systems & the safety of road users

Protect privacy in the vehicle & SDV ecosystem

Protect SDV-related assets & business opportunities

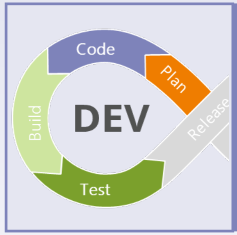
No software-defined vehicle without security

The 3 principles of SDV security

A holistic approach towards securing the SDV within its connected ecosystem

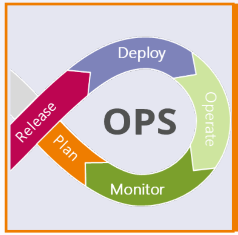
Defense in Depth

Make use of a Defense-in-Depth approach for the SDV and its ecosystem



Security by Design

Secure the SDV by design to mitigate risks during DEVelopment

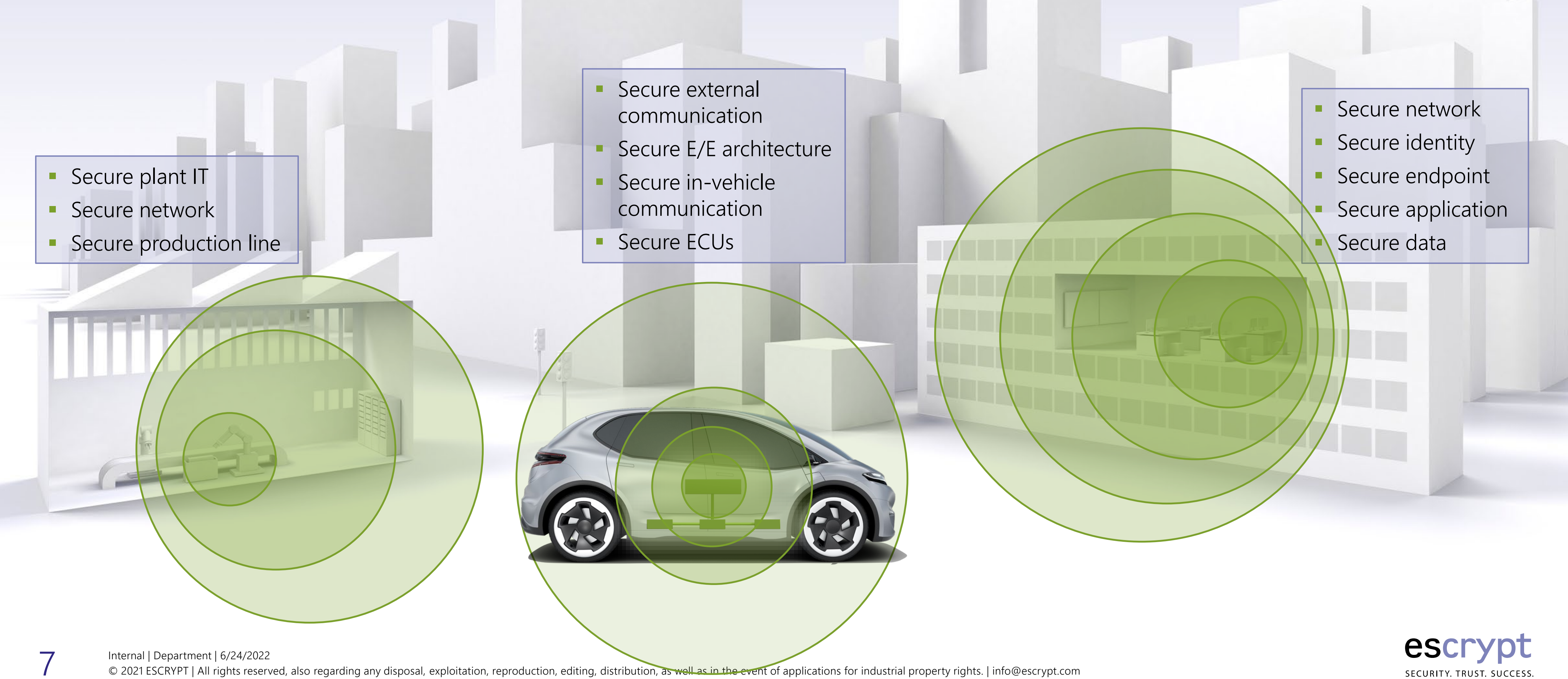


Continuous risk management

Manage security of the SDV within its connected ecosystem during OPerationS

#1: Defense in Depth

Establish a Defense-in-Depth approach for vehicle, production and backend



- Secure plant IT
- Secure network
- Secure production line

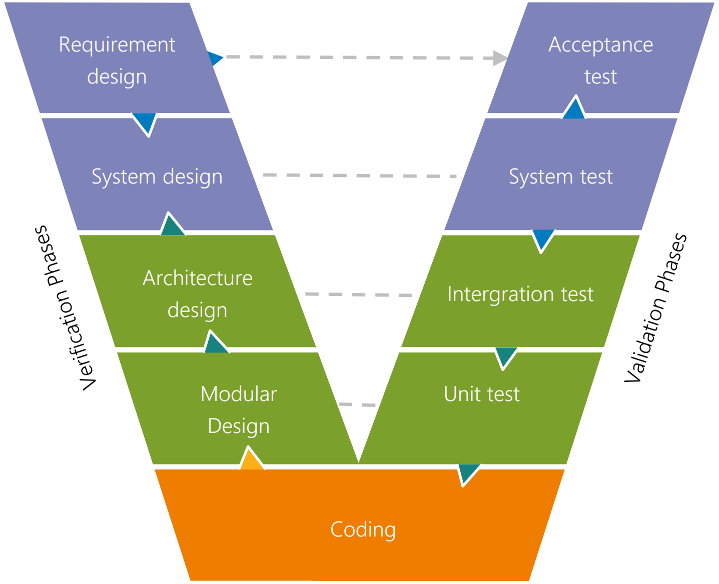
- Secure external communication
- Secure E/E architecture
- Secure in-vehicle communication
- Secure ECUs

- Secure network
- Secure identity
- Secure endpoint
- Secure application
- Secure data

#2: Security by design

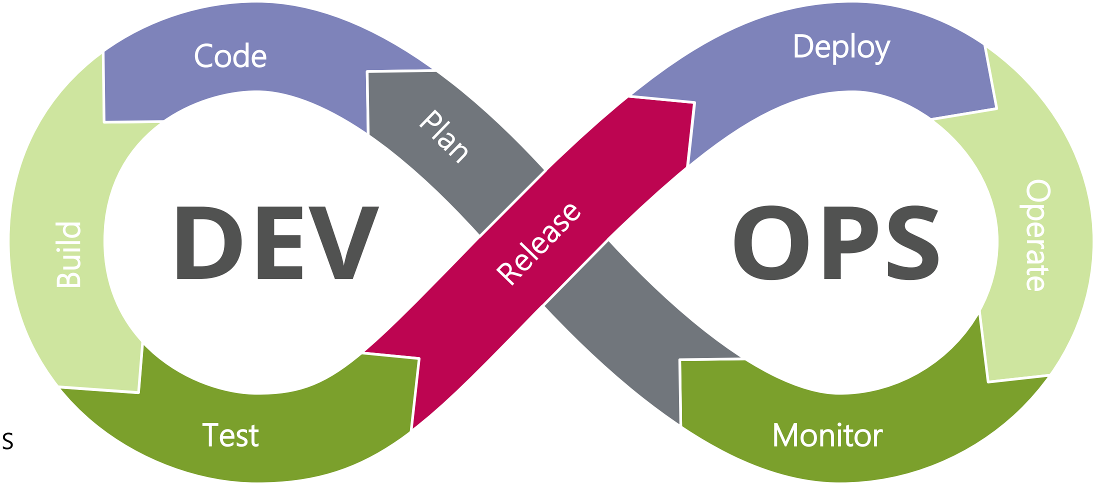
Secure SDV by design to mitigate risks right from start of development

With the software-defined vehicle and continuous updates development processes will also change.
The classic V-model will be joined by the agile, cloud-based DEV-OPS cycle.



Get a handle on complexity, cost, quality and time-to-market

Gain speed, efficiency and flexibility within shorter innovation cycles



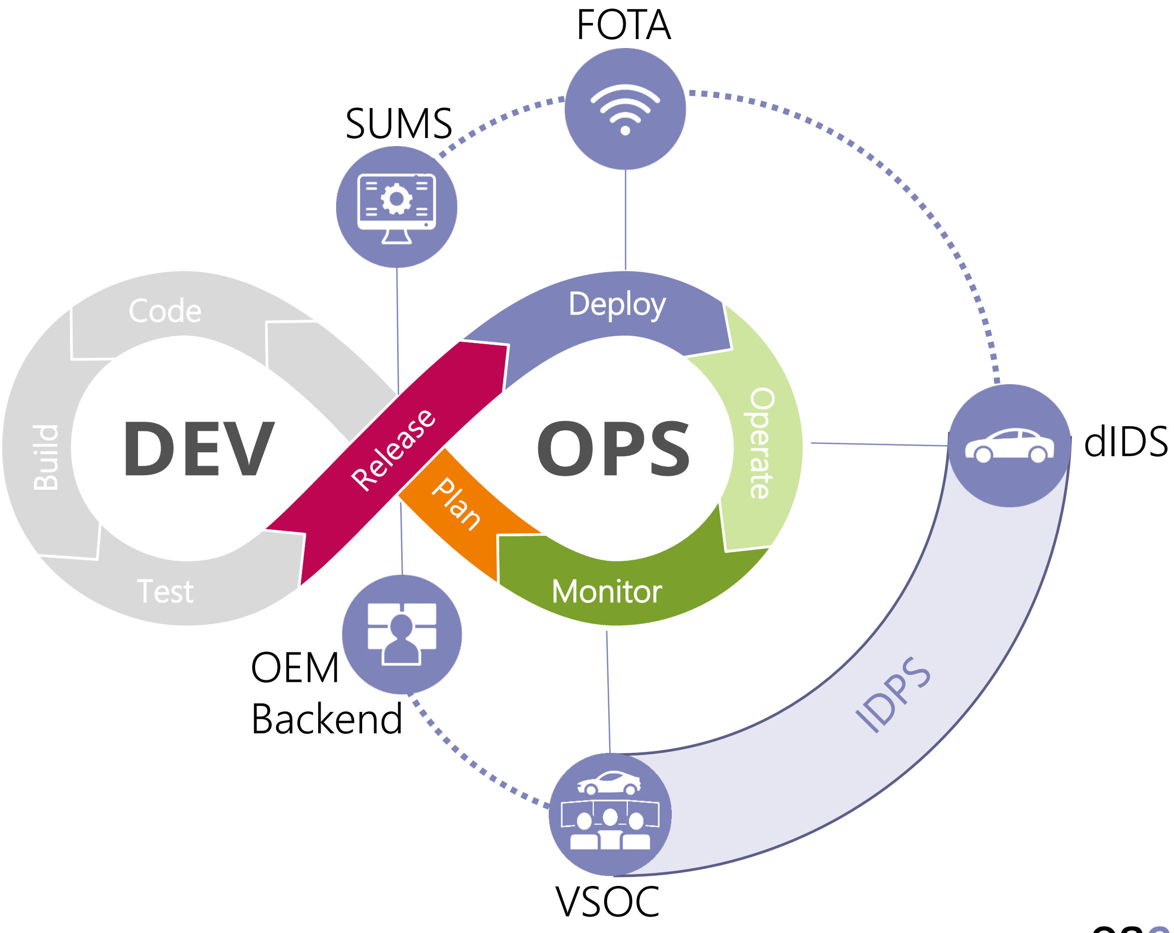
→ Security-by-design becomes an inherent guiding principle along the rapidly evolving software development cycle

#3 Continuous risk management

Detect and respond to security incidents across the connected SDV fleet

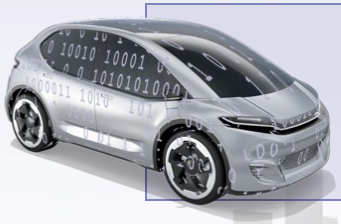
Implement and operate an "immune system" for the connected SDV fleet:

- Intrusion Detection & Prevention Solution **IDPS**
  - Distributed Intrusion Detection System **dIDS**
  - Vehicle Security Operations Center **VSOC**
- Software Update Management System **SUMS**
- Firmware Over-the-Air **FOTA**



Securing the software-defined vehicle

New challenges at all levels

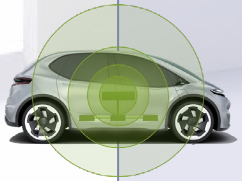


The software-defined vehicle (SDV) as part of an interconnected software-based ecosystem

- Increasing connectivity and complexity
- Increasing attack surface

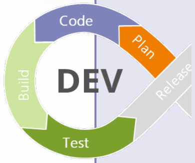
Security is key enabler for the SDV – No software-defined vehicle without security

- Protect safety
- Protect privacy
- Protect assets & business opportunities



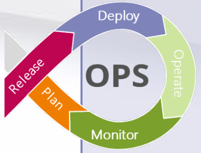
#1 Defense in Depth

- For the vehicle
- For production and backend



#2 Security by design

- Holistic security approach from start-of-development
- Beyond SOP within the recurring DEV-OPS-cycle



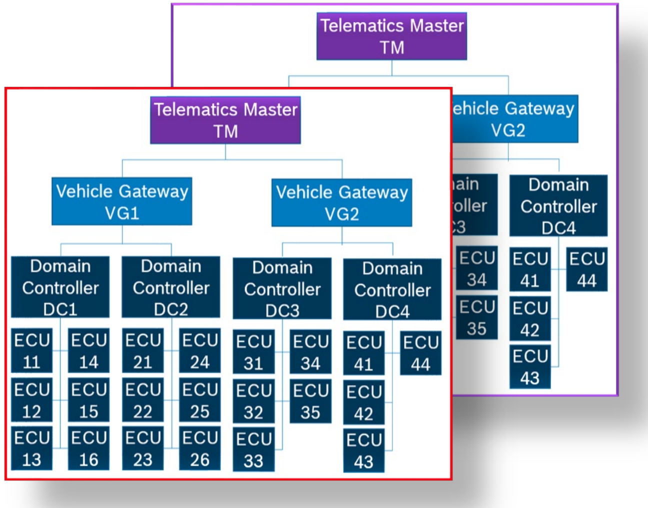
#3 Continuous risk management

- For connected SDV fleet, throughout lifecycle
- IDPS, SUMS & FOTA

Bosch Americas AV Security
Personal Research Focus

Attestation in real-time cyber-physical systems is different from laptops or cell phones

- Self Attestation
  - Boot time – functional safety – processor capacity – security goals
  - How to find a solution that meets all criteria?
- Remote Attestation
  - How can a buyer, AV user, or government regulator verify that the SW inside the vehicle is correct without access to the original code?
- Peer Attestation
  - How can a SW module be confident that its partners are using correct code?
  - How can a vehicle with a compromised module reach a secure state in a safe manner?



Telematics Master TM

ehicle Gateway VG2

ain oller 3

Domain Controller DC4

ECU 34

ECU 35

ECU 41

ECU 42

ECU 43

ECU 44

Telematics Master TM

Vehicle Gateway VG1

Vehicle Gateway VG2

Domain Controller DC1

Domain Controller DC2

Domain Controller DC3

Domain Controller DC4

ECU 11

ECU 12

ECU 13

ECU 14

ECU 15

ECU 16

ECU 21

ECU 22

ECU 23

ECU 24

ECU 25

ECU 26

ECU 31

ECU 32

ECU 33

ECU 34

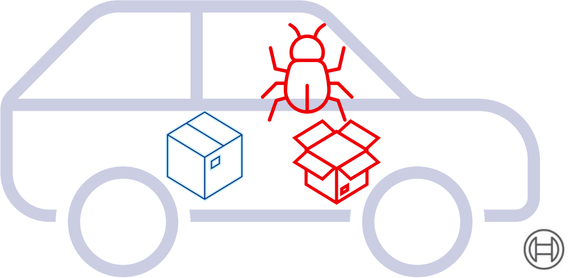
ECU 35

ECU 41

ECU 42

ECU 43

ECU 44



Thank you

ETAS GmbH
ESCRYPT – Solution Field Cybersecurity

Wittener Straße 45
44789 Bochum
Germany

Phone: +49 234 43870-200

info@escrypt.com
www.escrypt.com

escrypt
SECURITY. TRUST. SUCCESS.