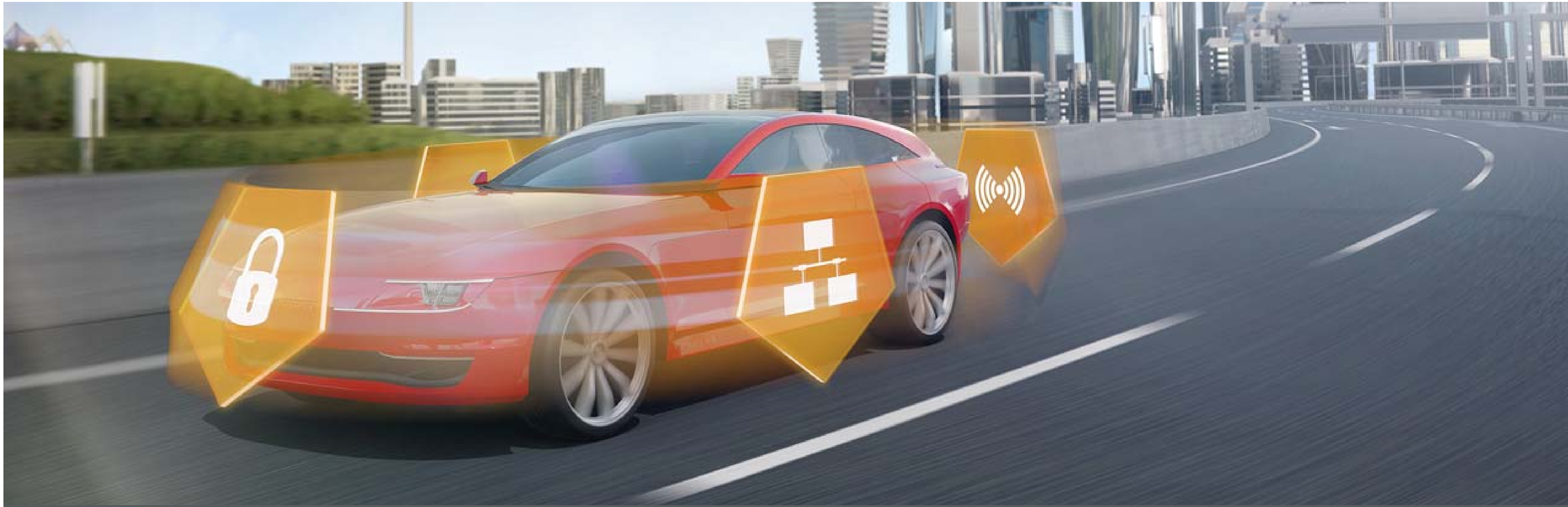
VECTOR



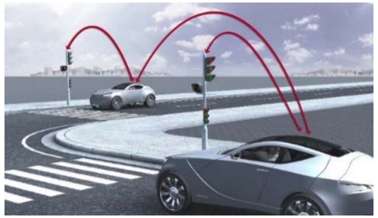
Automotive Cybersecurity: A steep learning curve

Vector Congress 2018

V1.0 | 2018-11-07

Attack Surface and Attack History

Automotive megatrends



Connectivity

~470 million
connected vehicles
by 2025[1]

Autonomous Driving

~80 million level 4/5
autonomous vehicles
by 2030[1]

>100 million lines of code per vehicle

Facebook: ~60 million lines of code by 2015[2]

➡ Increasing potential for
safety-critical cyber-attacks!

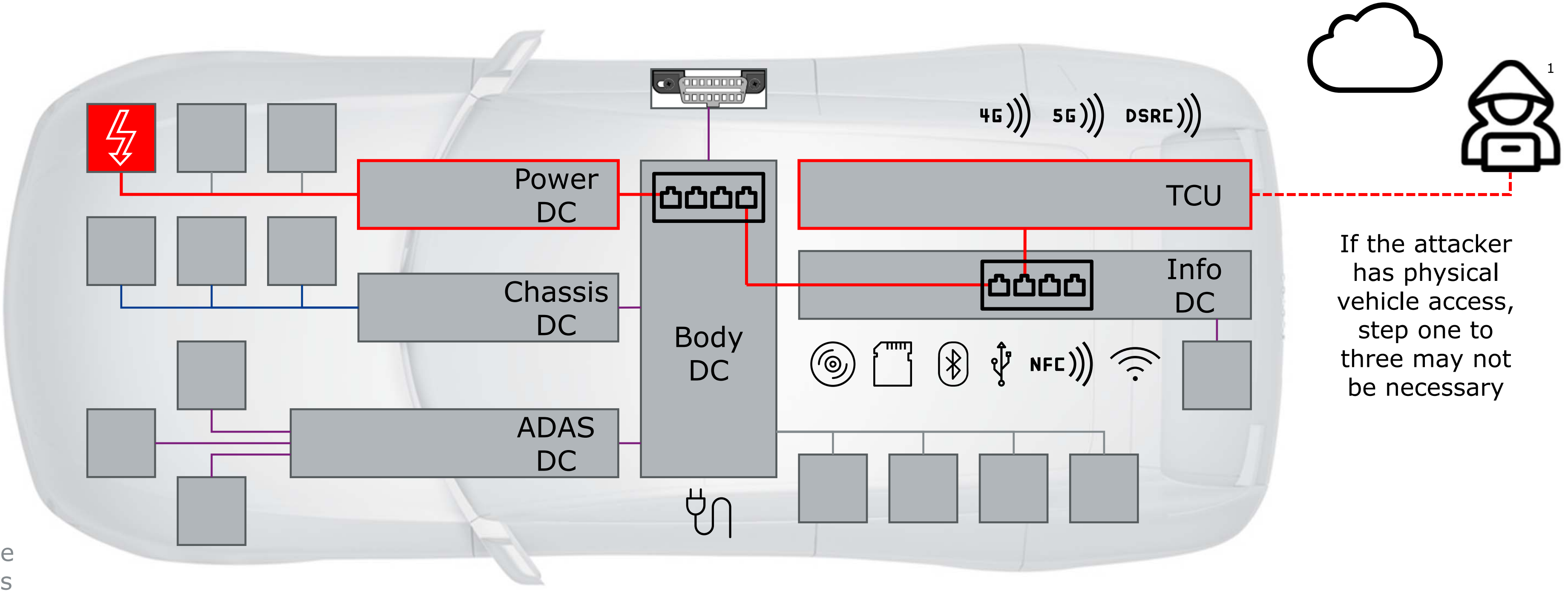
Attacks with safety-critical effects

2010 ◆	*local*: CAN access
2011 ◆	*local*: MP3; *remote*: Bluetooth, GSM
2012 ◆	
2013 ◆	*local*: OBD-II
2014 ◆	*remote*: OBD-II dongle
2015 ★	*remote*: GSM, OBD-II dongle 1. cybersecurity recall (1.4M vehicles)
2016 ◆	*local*: OBD-II; *remote*: details not published
2017 ◆	*local*: OBD-II; *remote*: details not published
2018 ◆	*local*: OBD-II, USB; *remote*: Bluetooth, GSM

[1] pwc, and strategy&. 2017. "The 2017 Strategy& Digital Auto Report: Fast and furious: Why making money in the "roboconomy" is getting harder." Accessed March 04, 2018. https://www.strategyand.pwc.com/media/file/2017-Strategyand-Digital-Auto-Report.pdf.

[2] "McCandless, David, Pearl Doughty-White, and Miriam Quick. 2015. "Codebases: Millions of lines of code." https://informationisbeautiful.net/visualizations/million-lines-of-code/."

Five Steps to Compromise an ECU



If the attacker has physical vehicle access, step one to three may not be necessary

Defense barriers

1. Remote Access

2. Access to in-vehicle network

3. Bridge domain boundaries

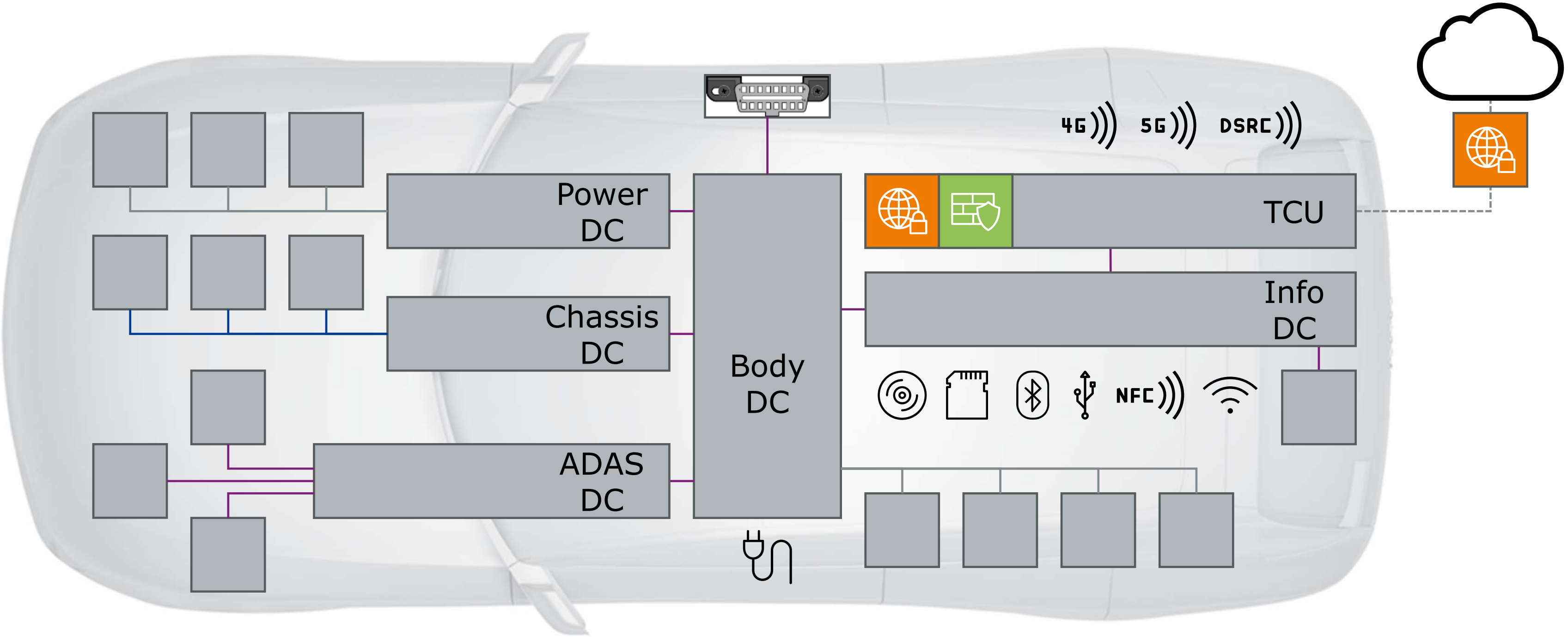
4. Access to target ECU

5. Manipulate ECU or vehicle behavior

DC: Domain Controller; TCU: Telematic Control Unit;
ECU: Electronic Control Unit

[1] www.freepik.com/www.flaticon.com

Securing the E/E Architecture – Defense in Depth (1.)



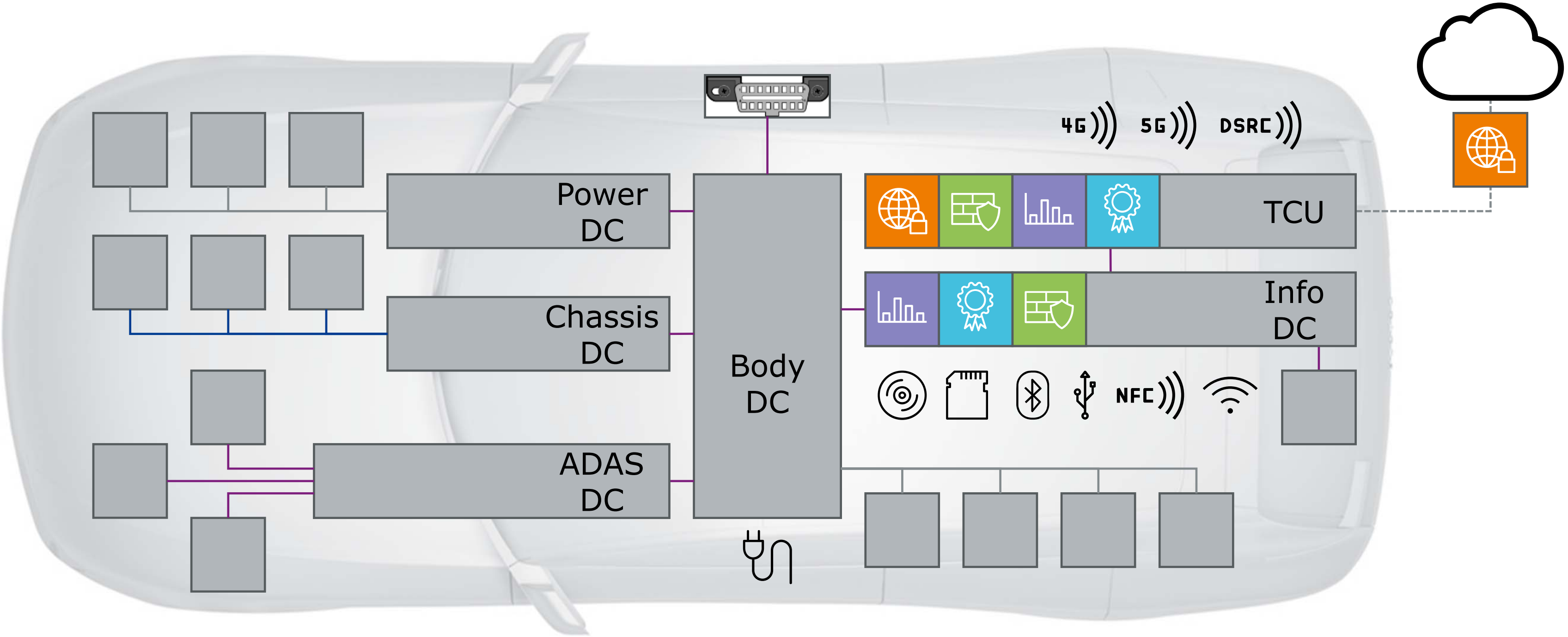
Prevent/restrict remote access

🟧 Secure vehicle-external interfaces
- TLS, IPsec

🟩 Firewalling
- White-listing (inbound/outbound traffic)

E/E: Electric/Electronic; TLS: Transport Layer Security; IPsec: Internet Protocol Security

Securing the E/E Architecture – Defense in Depth (2.)

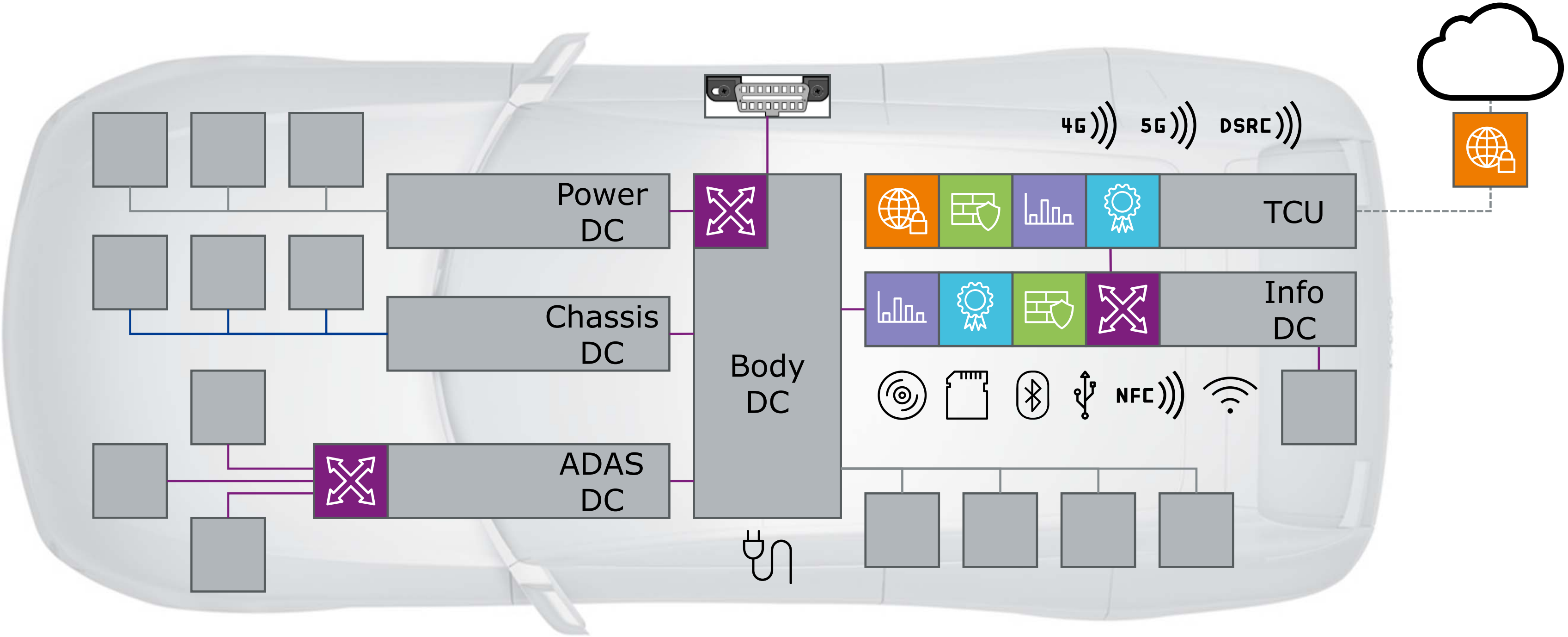


Prevent/restrict access to in-vehicle networks

- Isolation of execution context
  - OS, Hypervisor
- Policing
  - Minimum rights
- Firewalling
  - White-listing

OS: Operating System

Securing the E/E Architecture – Defense in Depth (3.)



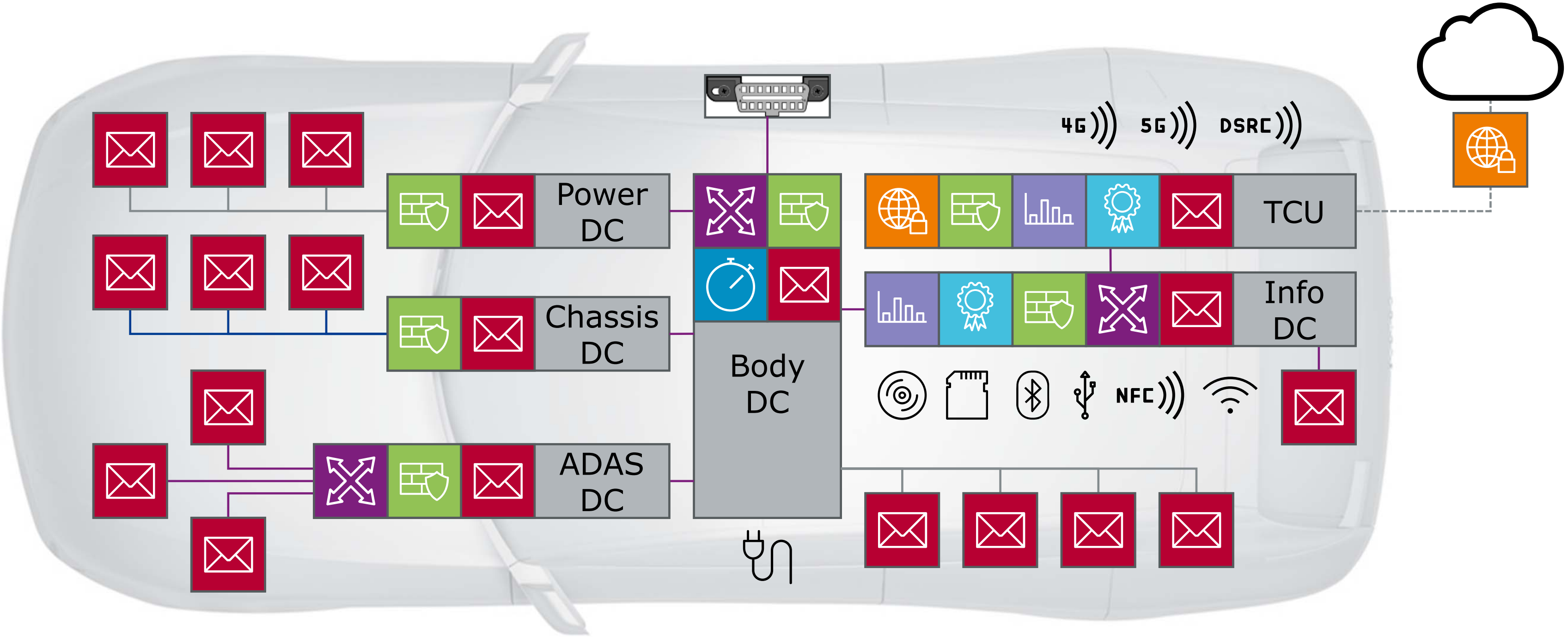
Domain isolation

- E/E architecture design
  - ▶ Security development process

- Message forwarding/routing
  - ▶ Ethernet: VLANs

VLAN: Virtual Local Area Network

Securing the E/E Architecture – Defense in Depth (4.)



Restrict/limit access to single ECUs

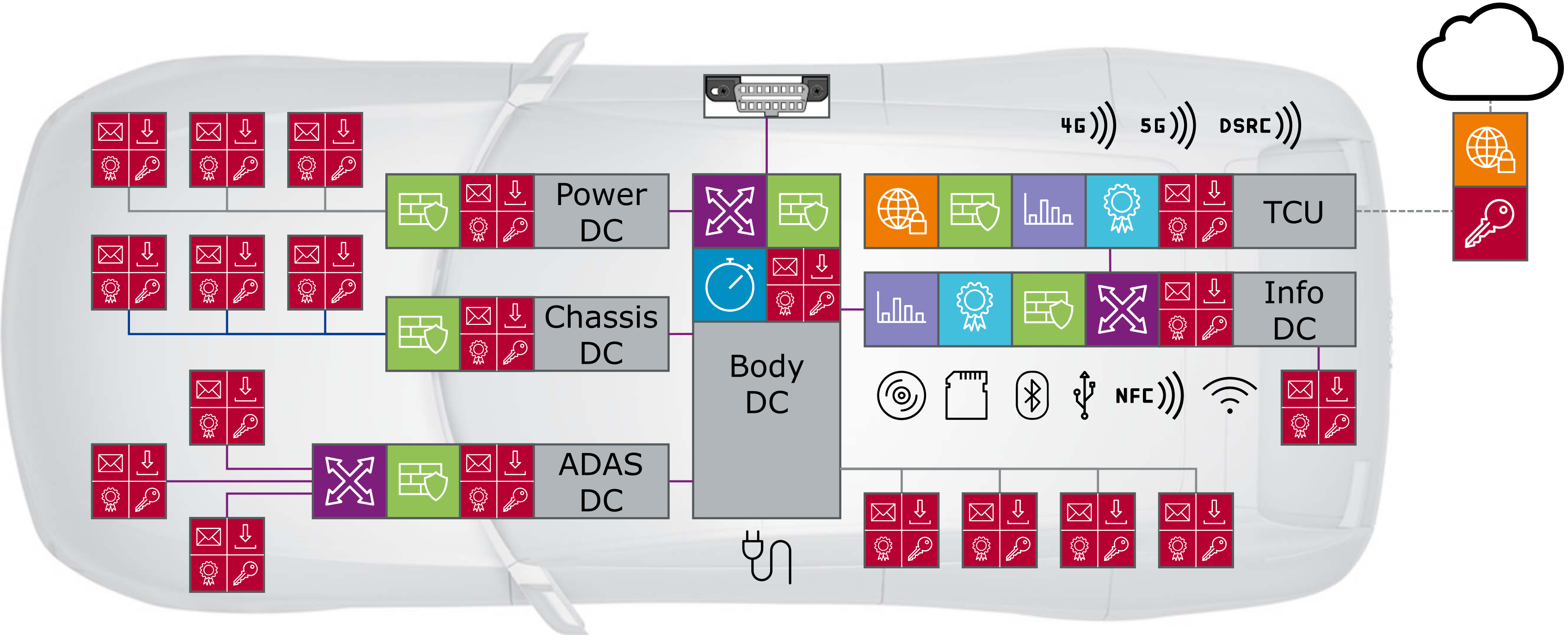
🟩 Firewalling
- ▶ White-listing

🟦 Secure time
- ▶ Time synchronization

🟥 Secure messaging
- ▶ SecOC, TLS, IPsec

SecOC: Secure Onboard Communication

Securing the E/E Architecture – Defense in Depth (5.)



Secure ECU hardware and software

- Secure firmware
  - ▶ Boot/update
- Secure diagnostics
  - ▶ Policing, SEM
- Key management
- Root of trust
  - ▶ Crypto, HSM

SEM: Security Event Memory; HSM: Hardware Security Module

Applicability and Availability on AUTOSAR Classic

Mechanism	AUTOSAR Classic	
	4.4	MICROSAR (*Vector-specific*)
Secure vehicle-external interfaces	¾	TLS, *IPsec*
Firewalling	½	↻ Static configuration, *EthFW*, *CanFW*
Policing	n/a	(Hard-coded and compiled)
Isolation of execution context	½	OS, *Hypervisor (PikeOS)*
Message forwarding/routing	✓	VLAN, switch configuration, static routing
Secure time	¾	↻ Time synchronization
Secure messaging	✓	SecOC, TLS, *IPsec*
Secure firmware	✗	*Secure boot/secure update*
Secure diagnostics	✓	↻ Security access, policing, SEM
Key management	½	Crypto stack, *customer specific*
Root of trust	½	Crypto stack, *veHsm*

↻ Work ongoing

Applicability and Availability on AUTOSAR Adaptive

Mechanism	AUTOSAR Adaptive		
	18.10	Library	MICROSAR (*Vector-specific*)
Secure vehicle-external interfaces	✓	TLS, DTLS, IPsec	
Firewalling	n/a	(netfilter/iptables)	
Policing	¼	OS	EM, IAM
Isolation of execution context	½	OS	*Hypervisor (PikeOS)*
Message forwarding/routing	½	VLAN	IAM
Secure time	✗		
Secure messaging	✓	TLS, DTLS, IPsec	Communication (SecOC)
Secure firmware	½		↻ UCM, *secure boot*
Secure diagnostics	¼		Diagnostics (sec. access)
Key management	½		Cryptography, *cust. spec.*
Root of trust	½		Cryptography, *veHsm*

↻ Work ongoing

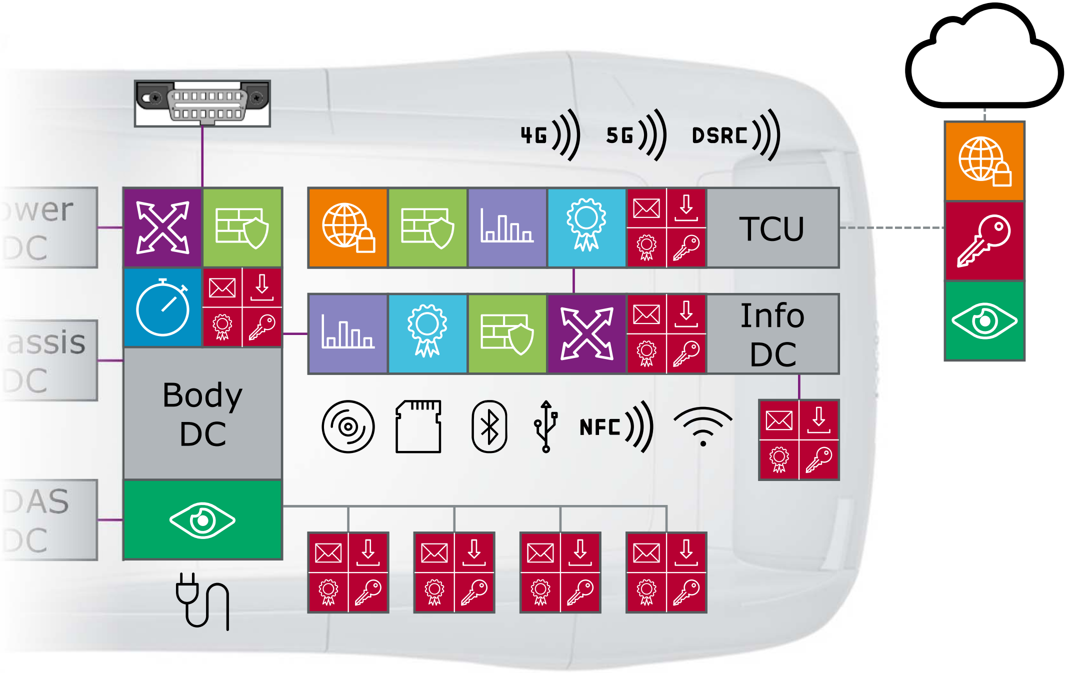
DTLS: Datagram Transport Layer Security; EM: Execution Management;
IAM: Identity and Access Management; UCM: Update and Config Management

Securing the E/E Architecture – Extended Defense in Depth

Besides prevention, intrusion detection is required to identify cyber-attacks

Automotive observer/intrusion detection system with backend connection for fleet analytics

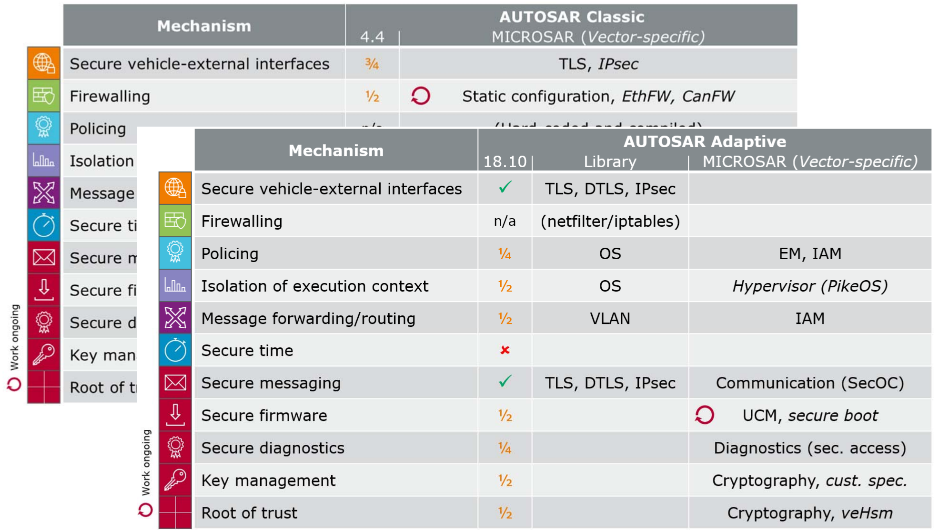
- Multi-instance
  - *Only one instance depicted*
- Network- and host-based anomaly detection
  - Static checks and machine learning
- Additional challenges for dynamic systems like AUTOSAR Adaptive
  - The system behavior may change during operation and due to user interaction
  - 1. possibility: Intrusion detection based on application-independent information only
  - 2. possibility: Intrusion detection has to be adapted as well or adapts itself



Summary and Outlook

Various security mechanisms are available and standardized in AUTOSAR Classic and AUTOSAR Adaptive

- Continuous improvement and extension
- *A summary for both platforms is included in the handout*



Mechanism	AUTOSAR Classic 4.4	 MICROSAR (*Vector-specific*)
Secure vehicle-external interfaces	¾	TLS, *IPsec*
Firewalling	½	↻ Static configuration, *EthFW, CanFW*
Policing	n/a	(Hard-coded and compiled)
Isolation		
Message		
Secure ti		
Secure m		
Secure fi		
Secure d		
Key man		
Root of t		

↻ Work ongoing

Mechanism	AUTOSAR Adaptive 18.10	 Library	 MICROSAR (*Vector-specific*)
Secure vehicle-external interfaces	✓	TLS, DTLS, IPsec	
Firewalling	n/a	(netfilter/iptables)	
Policing	¼	OS	EM, IAM
Isolation of execution context	½	OS	*Hypervisor (PikeOS)*
Message forwarding/routing	½	VLAN	IAM
Secure time	×		
Secure messaging	✓	TLS, DTLS, IPsec	Communication (SecOC)
Secure firmware	½		↻ UCM, *secure boot*
Secure diagnostics	¼		Diagnostics (sec. access)
Key management	½		Cryptography, *cust. spec.*
Root of trust	½		Cryptography, *veHsm*

↻ Work ongoing

Besides preventive measures, intrusion detection is required

- All defense barriers will eventually be broken
- Provide insights to develop countermeasures

Modern E/E architectures are already much more secure than in the past …

… but there are still security topics and mechanisms to be addressed!

Your questions are welcome!

Author:
Weber, Marc
Vector Germany