SAFE AND SECURE

MACSEC IMPLEMENTATION IN THE CONTEXT OF ISO26262

ETHERNET & IP @ AUTOMOTIVE TECHNOLOGY DAY

Steffen Lorenz

SEPTEMBER 2023

SECURE CONNECTIONS
FOR A SMARTER WORLD

CAN WE TRUST MODERN CARS?

Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

This PSA is a joint product by the Federal Bureau of Investigation, the Department of Transportation and the National Highway Traffic Safety Administration.

March 17, 2016

Alert Number
I-031716-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field

MOTOR VEHICLES INCREASINGLY VULNERABLE TO REMOTE EXPLOITS

As previously reported by the media in and after July 2015, security researchers evaluating automotive cybersecurity were able to demonstrate remote exploits of motor vehicles. The analysis demonstrated the researchers could gain significant control over vehicle functions remotely by exploiting wireless communications vulnerabilities. While the identified vulnerabilities have been addressed, it is important that consumers and manufacturers are aware of the possible threats and how an attacker may seek to remotely exploit vulnerabilities in the future. Third party aftermarket devices with Internet or cellular access plugged into diagnostics ports could also introduce wireless vulnerabilities.

WIRED SUBSCRIBE

Hackers Remotely Kill a Jeep on the Highway—With Me in It

I WAS DRIVING 70 mph on the edge of downtown St. Louis when the exploit began to take hold.

Forbes / Security

JUL 14, 2015 @ 12:00 PM 26,209 VIEWS

Tesla Model S Digital Weaknesses To Be Exposed By Hackers Next Month

CNN Money U.S. + Business Markets Tech Media Personal Finance Small Biz Luxury stock tickers

The Cybercrime Economy

Traffic lights are dangerously easy to hack

engadget

OnStar hack remotely starts cars, GM working on a fix

by Jessica Conditt | @jessconditt | July 30th 2015 At 1:58pm

c't magazin

Startseite Artikel Hotline & FAQ Blog Aktuell

Magazin Internet Software Hardware Know-how Praxis Editorial Prozessorgef

c't > Magazin

Dieter Spaar, Translation: Fabian A. Scherschel 05.02.2015

Beemer, Open Thyself! – Security vulnerabilities in BMW's ConnectedDrive

SECURITY IS A MUST-HAVE FOR VEHICLES -

AGENDA

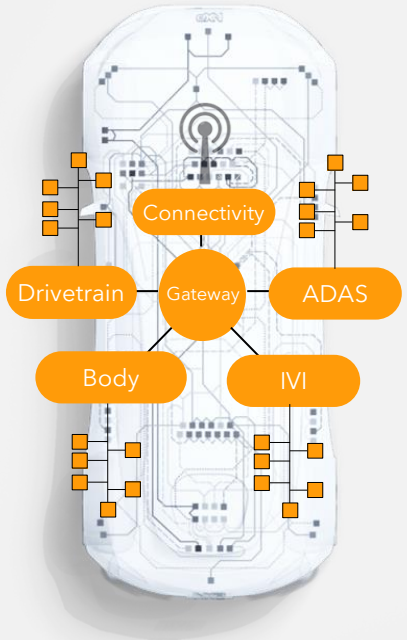
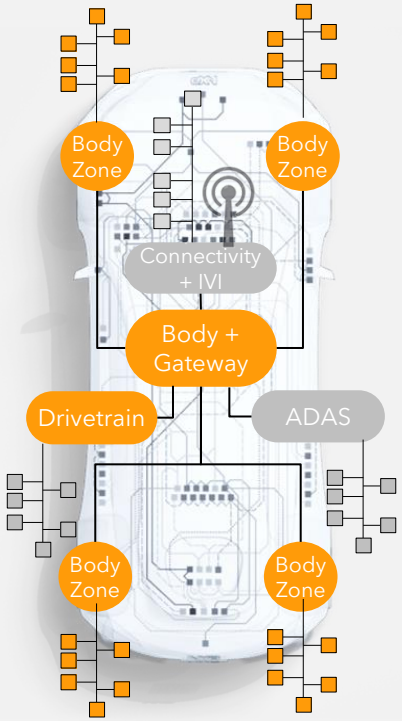
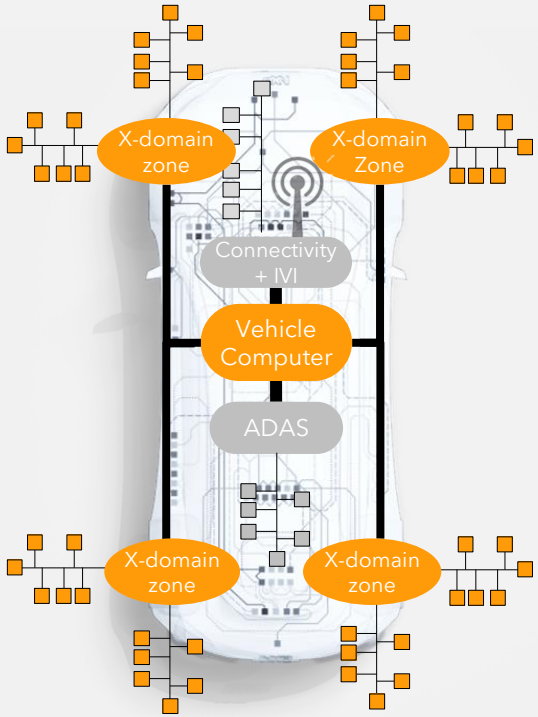
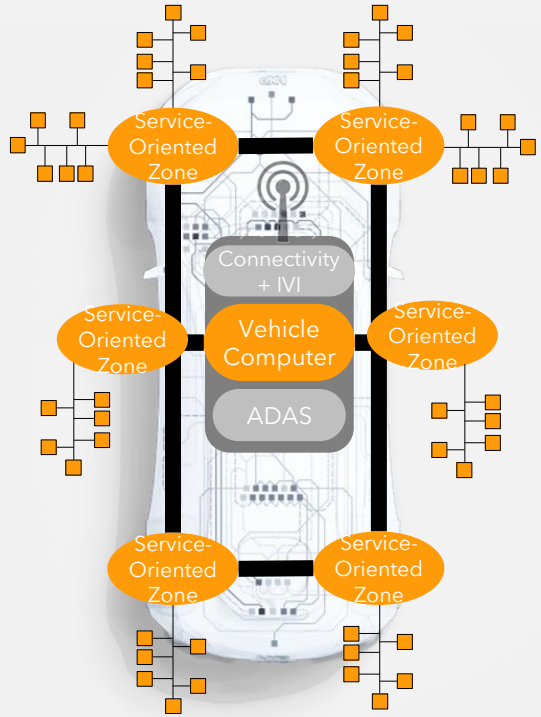
- *Security in automotive - MACsec in a nutshell*
- *Functional Safety*
- *FuSa @ MACsec*
- *Summary and conclusion*

Security in automotive

MACsec in a nutshell

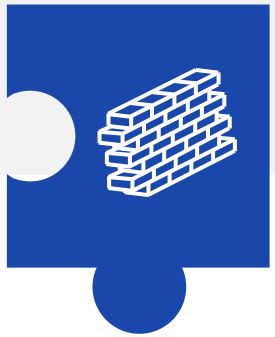
SECURE CONNECTIONS
FOR A SMARTER WORLD

NEW E/E ARCHITECTURES ARE EMERGING TO MANAGE INCREASING HARDWARE AND SOFTWARE COMPLEXITY

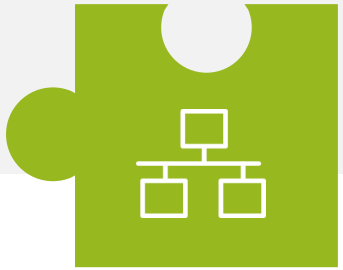
DOMAIN	BODY-ZONAL	X-DOMAIN ZONAL	SDV-OPTIMIZED
			
Creates logical separation to isolate processing of domain functions with static network policies	Creates physical separation for body domain functions enabling smart data and power distribution and reducing wiring/weight/complexity	Creates physical separation for cross-domain functions in zones for further wiring/weight/complexity reduction using distributed compute architecture	Centralized, service-oriented compute architecture with zones supporting SDV SW deployment and further wiring optimization

CORE SECURITY PRINCIPLES FOR DEFENSE IN DEPTH

SECURE
EXTERNAL INTERFACES

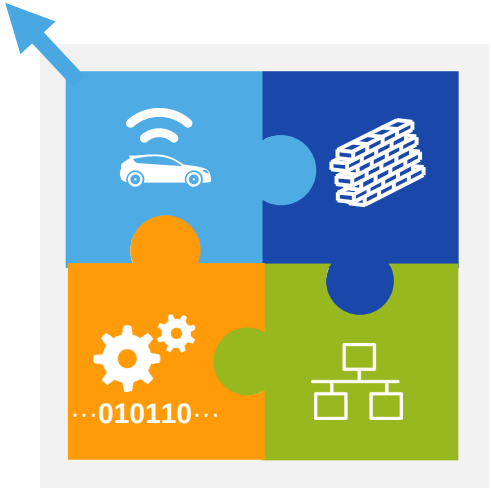


SECURE
DOMAIN ISOLATION



SECURE
INTERNAL COMMUNICATION

SECURE
SOFTWARE EXECUTION



Multiple layers of protection – in ***any*** E&E network!

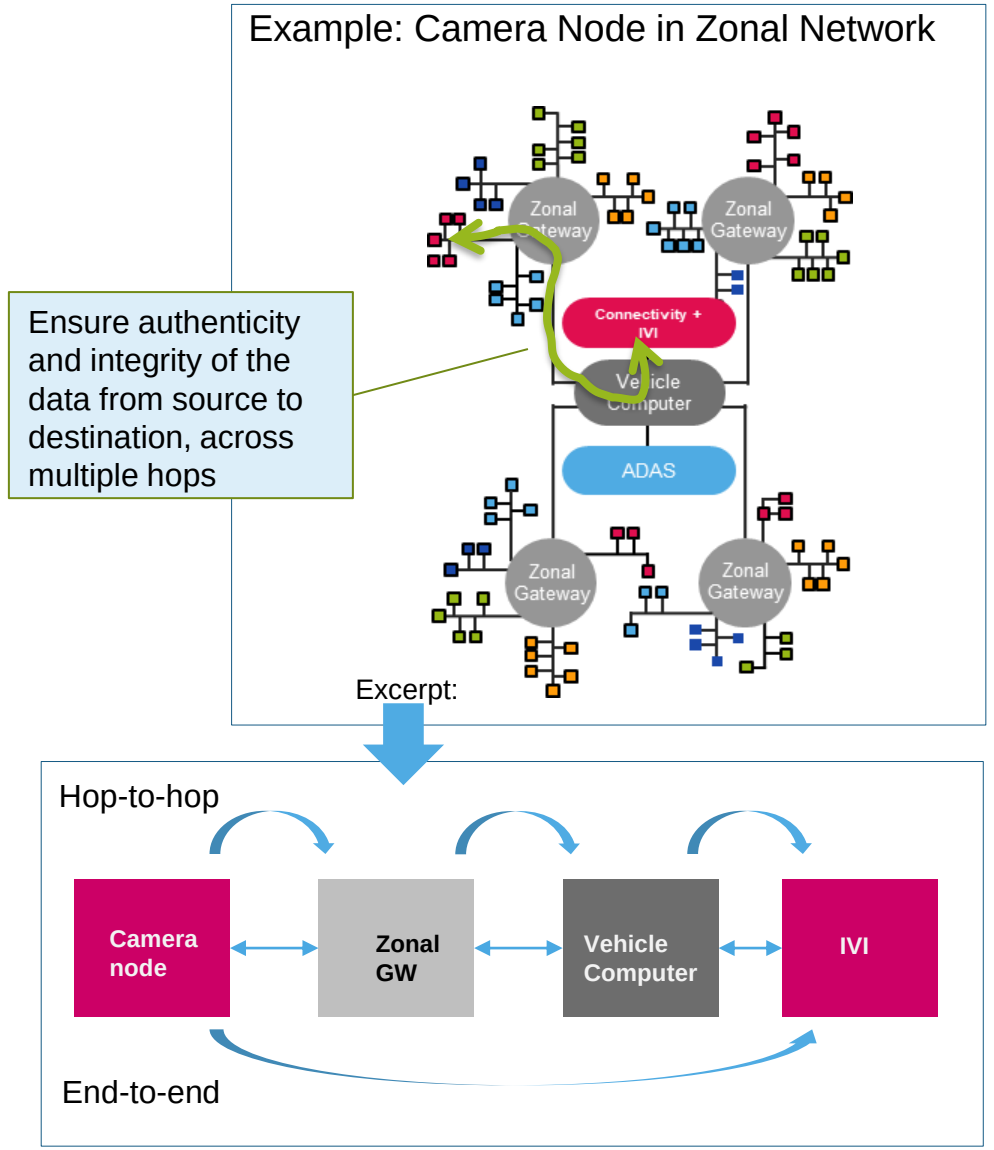
- To mitigate the risk of one component of the defense being compromised or circumvented
- Regardless of the actual vehicle network architecture and implementation

SCOPE OF NETWORK SECURITY

- E/E-Architectures are moving away from fixed function boxes
- Data is shared, aggregated, pre- and post-processed in different locations of the network

- Scope of Network Security:
  - Authenticity and Integrity of data
    - Data originated from the expected sender (trusted source)
    - Data was not modified on its way
  - Confidentiality of data
    - Privacy of communication by data encryption per AES standard

- 2 different types of secure associations:
  - Hop-to-hop (or point-to-point)
  - End-to-end

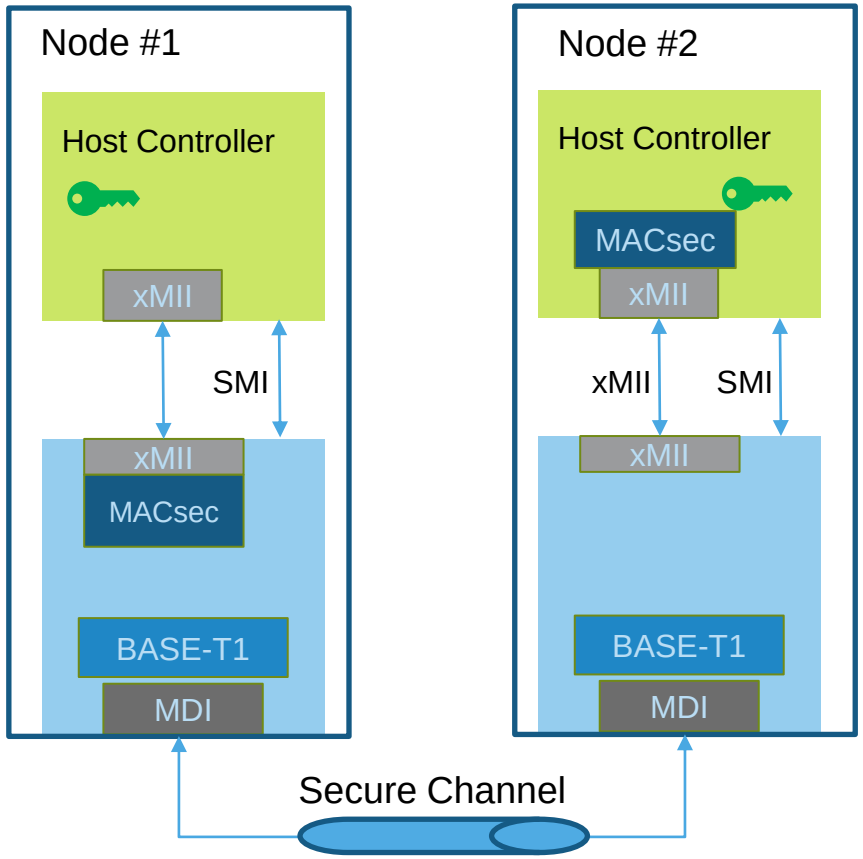


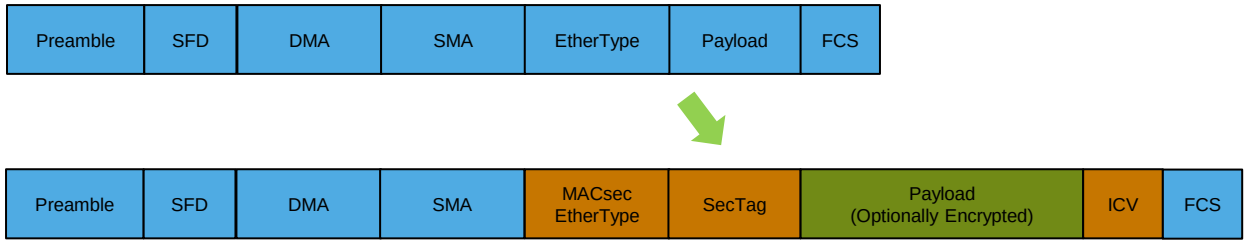
HOW DOES MACSEC INTERACT WITH HOST?

Host runs EAP and IEEE 802.1X protocol Port-Based Network Access Control

- Authenticating / authorizing the supplicant device
- Key exchange management
- Configuration / provision of session keys to PHY in clear
- Make provision for MACsec overhead

- MACsec 802.1AE tasks:
  - With MACsec enabled, all data or control traffic (except for 802.1x packets) gets blocked until session is secured
  - Establish Secure Channel (TX, RX), Secure Channel Identifier
  - Establish and maintain secure associations by exchanging temporary association key (key rotation)
  - On transmit:
    - Add SecTag (MAC Security Tag, 8-16B)
    - Add ICV (Integrity Check Value, 8-16B)
    - Optional: Payload encryption
  - On receive:
    - Decrypt the packets
    - Check SecTag authenticated link partner
    - Check integrity modified in transmit
    - Remove SecTag and ICV





Functional Safety

SECURE CONNECTIONS
FOR A SMARTER WORLD

ISO 26262 – The Science of Quantifying Risk

Severity Exposure Controllability →

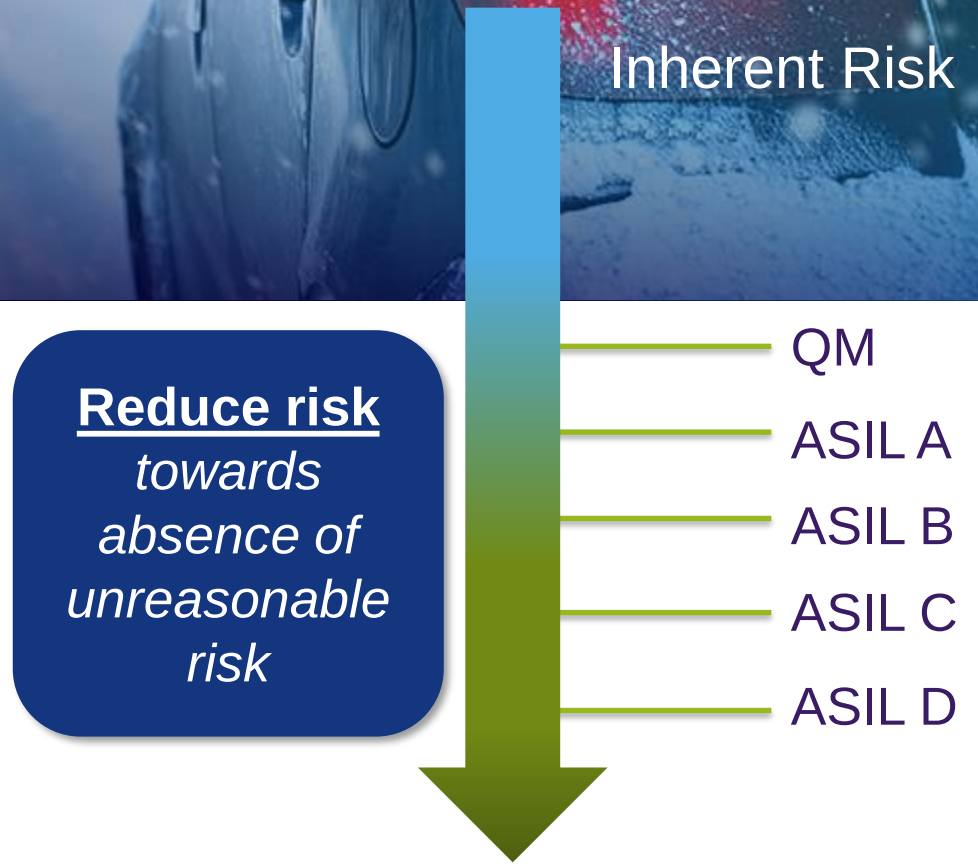
ASIL
Automotive Safety Integrity level

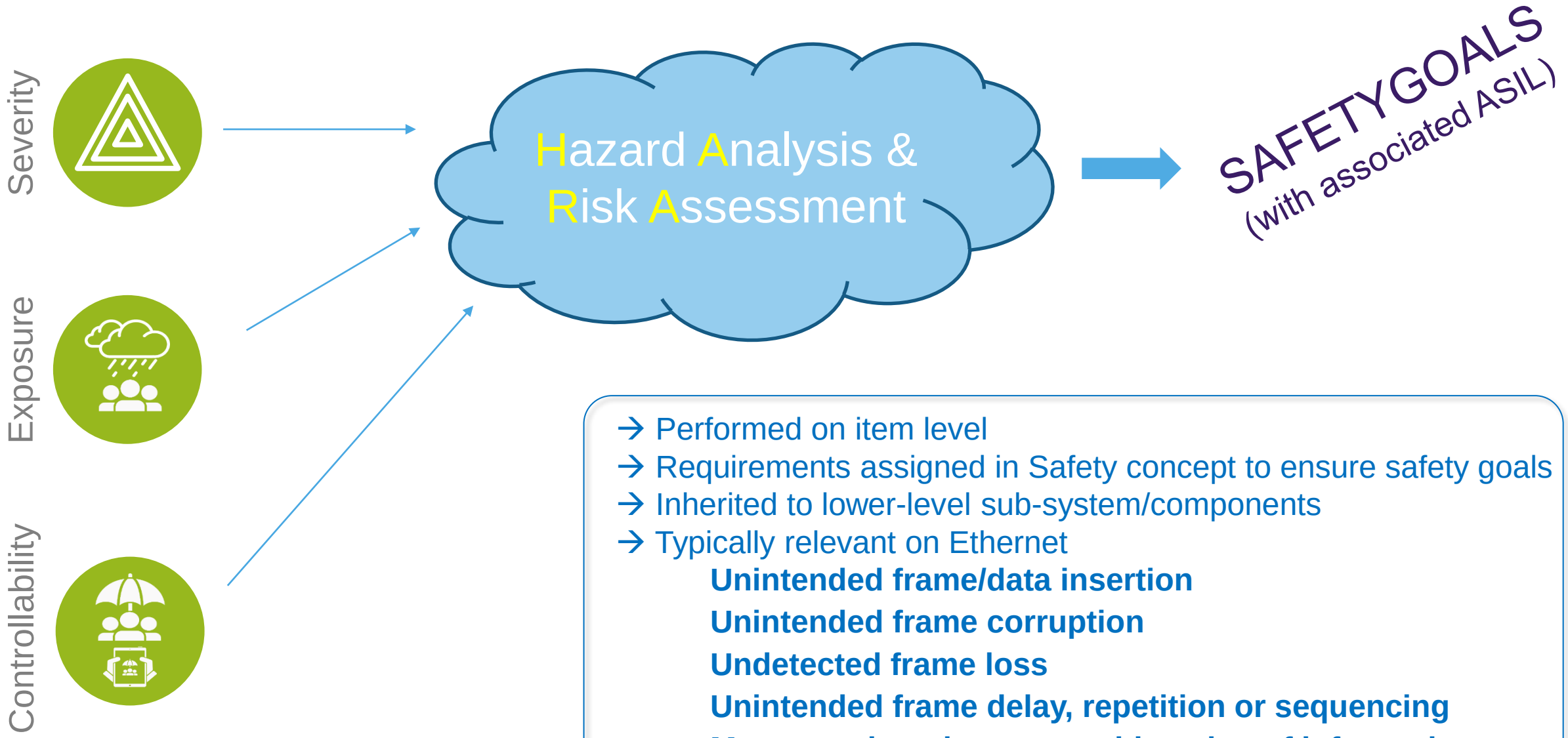
How much harm is done?

How often is it likely to happen?

Can the hazard be controlled?

ISO 26262, part 1:
"absence of unreasonable risk due to hazards caused by malfunctioning behaviour of E/E systems"





- → Performed on item level
- → Requirements assigned in Safety concept to ensure safety goals
- → Inherited to lower-level sub-system/components
- → Typically relevant on Ethernet
  - **Unintended frame/data insertion**
  - **Unintended frame corruption**
  - **Undetected frame loss**
  - **Unintended frame delay, repetition or sequencing**
  - **Masquerade or incorrect addressing of information**

HOW THE NETWORKING IC BRINGS SAFETY TO THE ZONE

- Networking ICs are not the only part of the communication chain, E2E will be needed
- Vehicle service availability improved by ensuring availability of communication services in the vehicle → fail operational systems need more than E2E
- Networking ICs can:

Prevent Failure

- High reliability
- Freedom from interference

Predict Failure

- (Self-)Diagnostic features

React to Failure

- Improved response time to increase FTTI margin
- Even correct some failures

Design for Functional Safety goes far beyond the single product…
It requires a living safety culture and development process.

LATENT FAULTS

- If a safety mechanism is not working, the related fault gets uncovered
- It is a multiple-fault, but occurrence of two faults could be spread over long time
  - Probability of two independent faults happening at similar time is low
  - Much higher when no time constraint
- This creates a latent fault
- To prevent this, on regular base (e.g. startup) the safety mechanism is proven to work, by e.g.
  - BIST
  - Functional check
- Contributes to the Latent fault metric

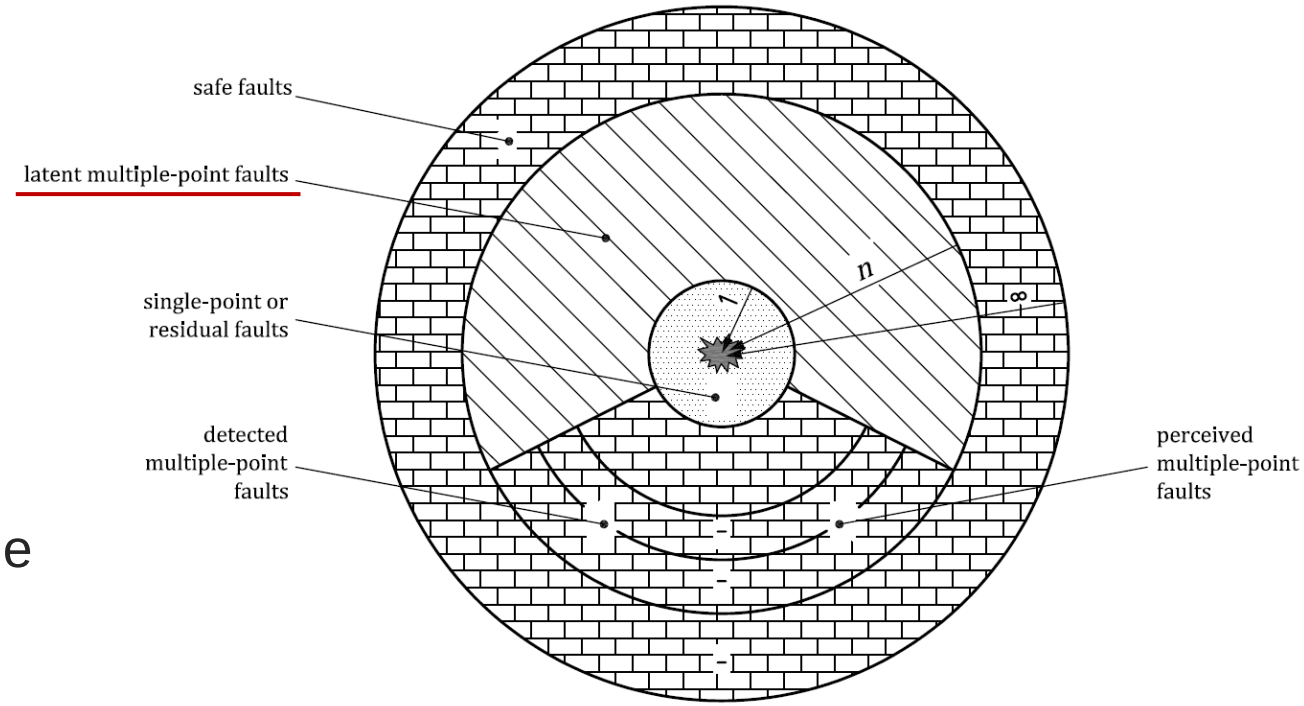


Figure C.1 — Fault classification of safety-related hardware elements of an item

Source: ISO26262-5:2018

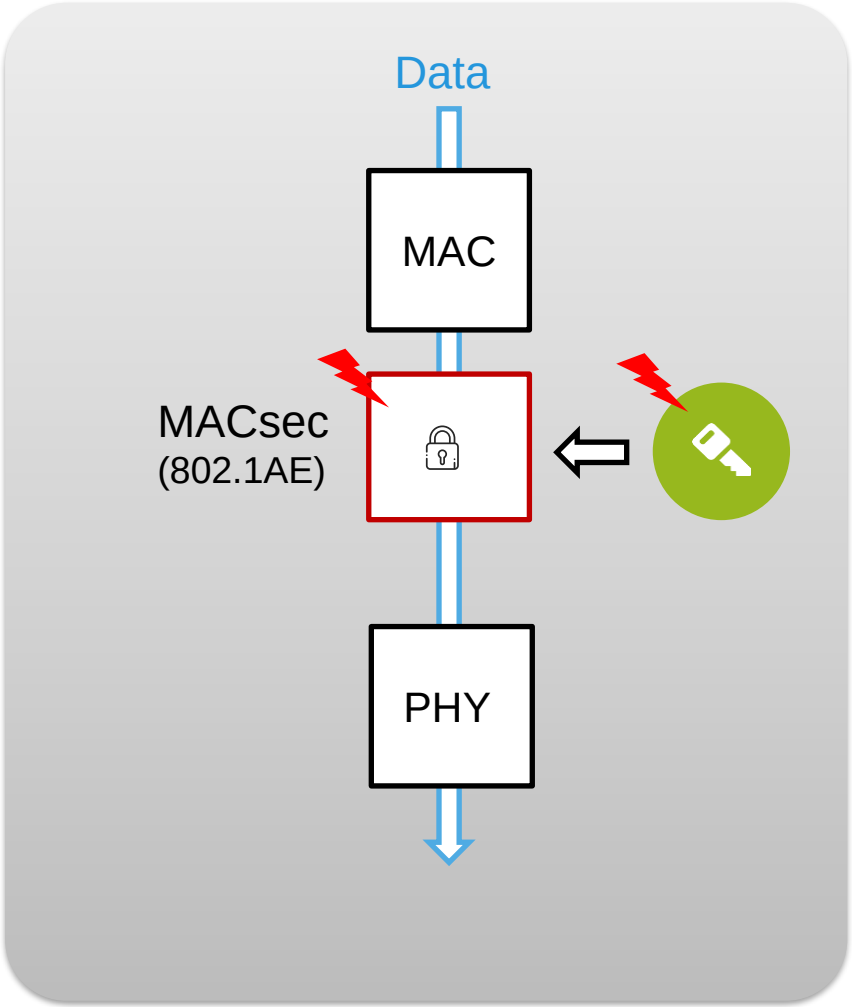
FuSa @ MACsec

Safe & Secure

SECURE CONNECTIONS
FOR A SMARTER WORLD

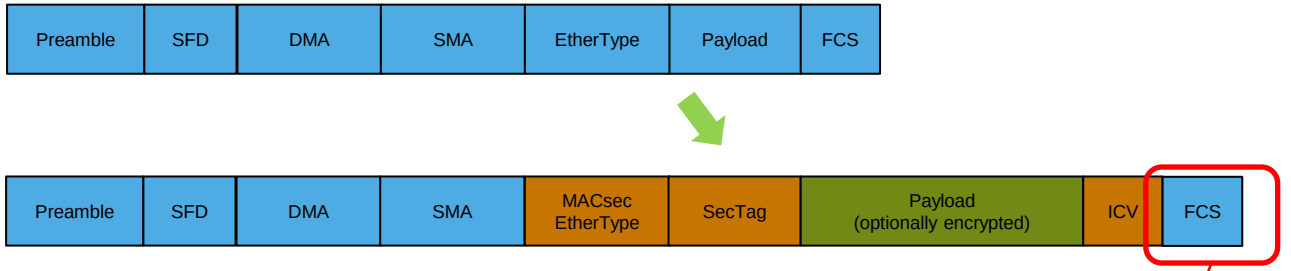
MACSEC ADDS NEW FAILURE MODES

- Adding a security measure increases the complexity and silicon area
- Data runs through additional processing
- Additional configuration
- This adds new failure modes – *more things can go wrong*



FAILURE MODES

- MACsec 802.1AE tasks:
  - With MACsec enabled, all data or control traffic (except for 802.1x packets) gets blocked until session is secured
  - Establish Secure Channel (TX, RX), Secure Channel Identifier
  - Establish and maintain secure associations by exchanging temporary association key (key rotation)
  - On transmit:
    - Add SecTag (MAC Security Tag, 8-16B)
    - Add ICV (Integrity Check Value, 8-16B)
    - Optional: Payload encryption
  - On receive:
    - Decrypt the packets
    - Check SecTag authenticated link partner
    - Check integrity modified in transmit
    - Remove SecTag and ICV



Secure channel depends on correct configuration

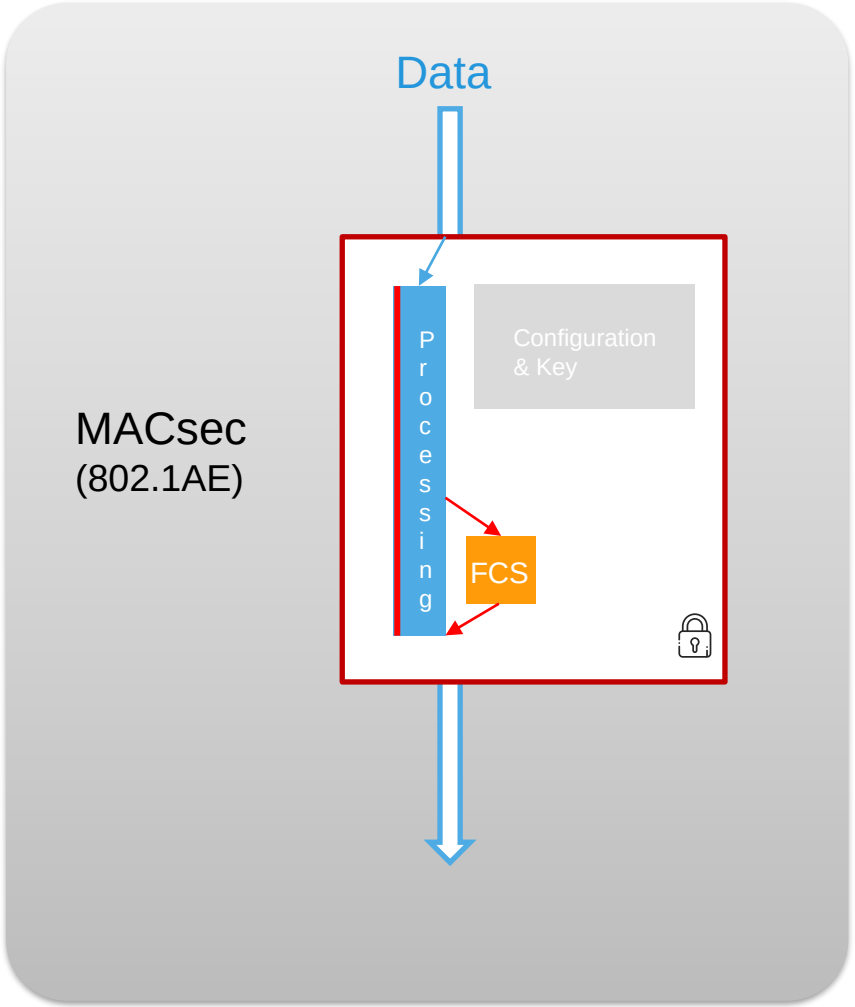
Adding content to the frame will require a new FCS

Encryption processes whole data

Software trusts to receive frame decrypted and received on correct secure channel

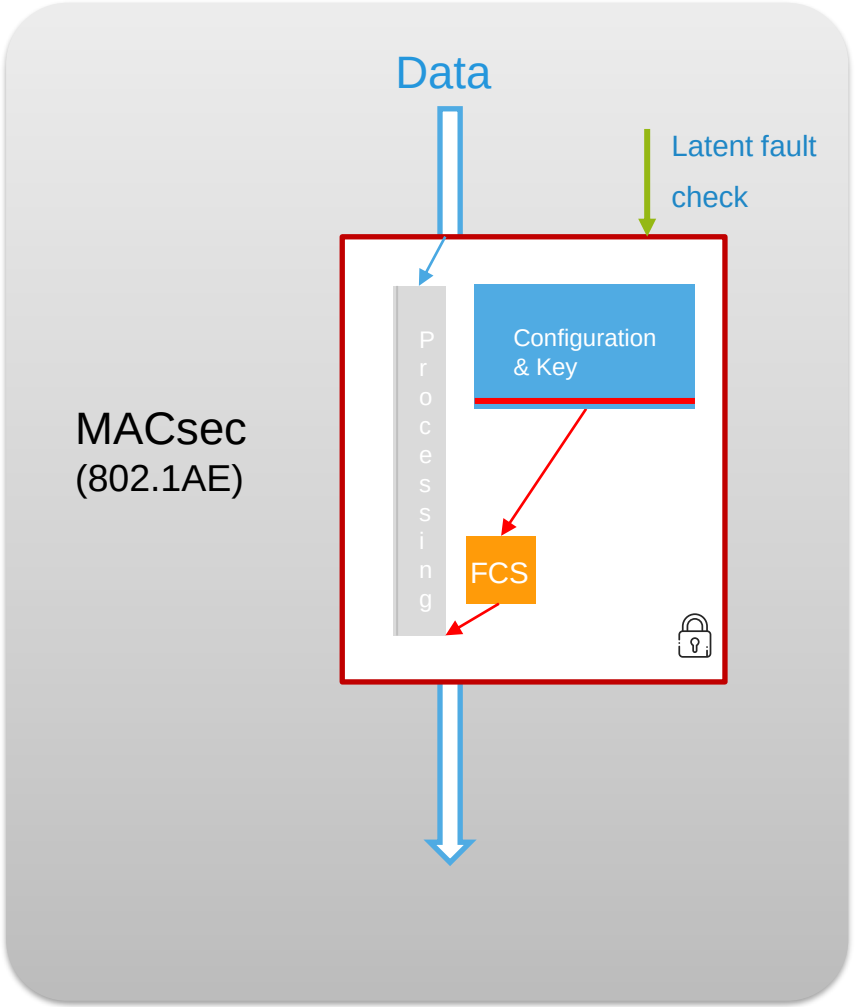
SAFETY GOALS

- Frames must not be forwarded with corrupted integrity
  - Protect the data during processing
  - Invalidate FCS of corrupted frame to prevent FCS escape



SAFETY GOALS

- Frames must not be forwarded with corrupted integrity
  - Protect the data during processing
  - Invalidate FCS of corrupted frame to prevent FCS escape
- Frames must not be forwarded to incorrect secure channel
  - Protect configuration
  - Latent fault check on processing/configuration



SUMMARY AND CONCLUSIONS

- Security is a must-have for vehicles, especially for SDVs
- MACsec is one of the ingredients for multi-layer protection
- Functional safety is another must-have in E/E architectures
- A safe MACsec has to fulfill certain safety goals and should allow for latent fault checks
- It will help to keep the secure network safe and increase its availability

SECURE CONNECTIONS
FOR A SMARTER WORLD