CAN Security: The Innovative Hardware Solution Enhancing Any Software Approach!

Francesco Sindaco

Director Strategy & Business Development

PL IVN

June 2019 | Session #AMF-AUT-T3629

NXP

SECURE CONNECTIONS
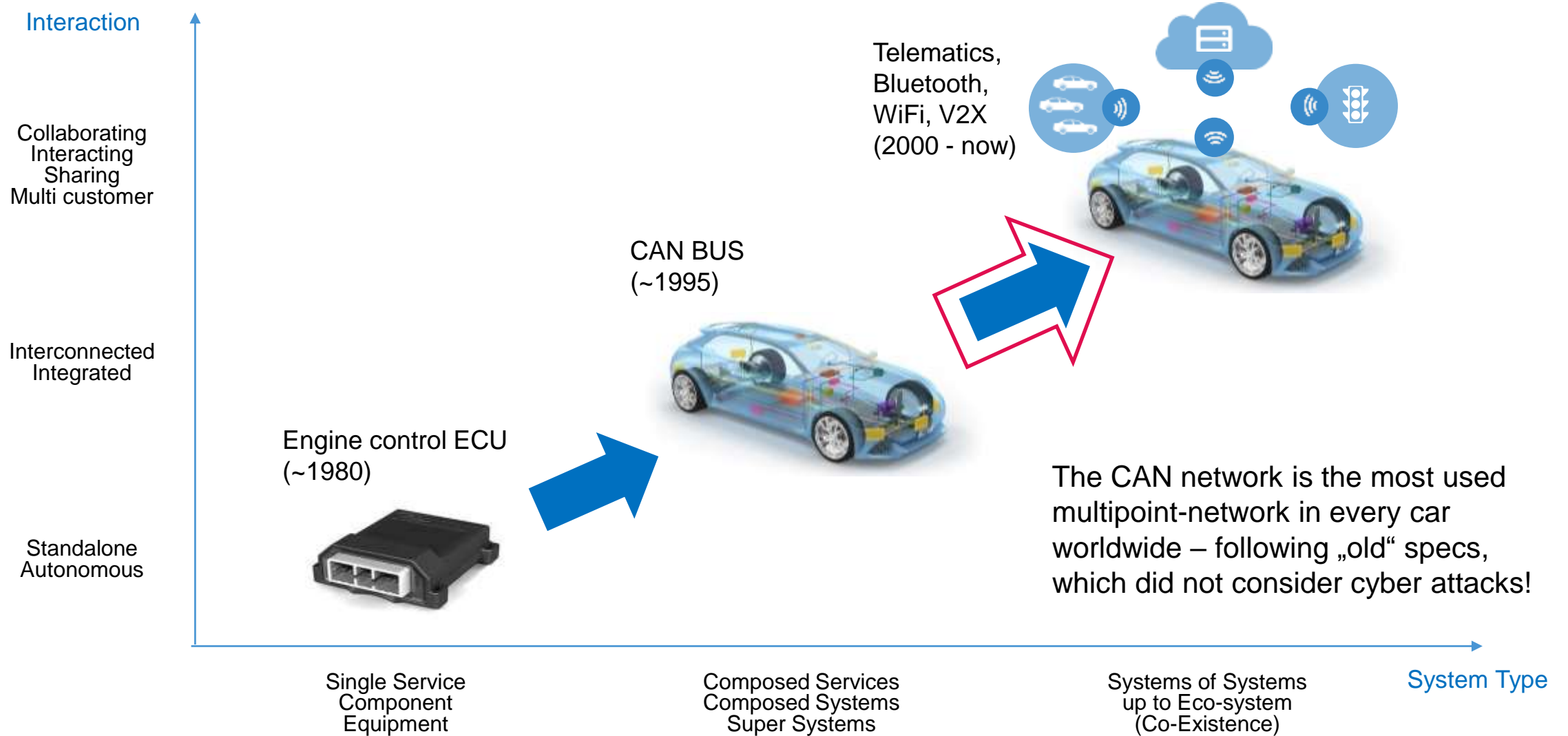FOR A SMARTER WORLD

Agenda

- Security Intro – Secure Network
- Security Value of Secure CAN Transceiver
  - Spoofing Protection
  - Tamper Protection
  - Flooding Prevention
- System Value of TJA115x
  - Saving Keys & Bandwidth
  - Offloading MCU & Cost Reduction
- Support for IDPS
- Confirmed Use Cases

NXP Security – Introduction

Vehicle Electronics & Connectivity

Interaction

Collaborating
Interacting
Sharing
Multi customer

Interconnected
Integrated

Standalone
Autonomous

Telematics,
Bluetooth,
WiFi, V2X
(2000 - now)

CAN BUS
(~1995)

Engine control ECU
(~1980)

The CAN network is the most used multipoint-network in every car worldwide – following „old" specs, which did not consider cyber attacks!

Single Service
Component
Equipment

Composed Services
Composed Systems
Super Systems

Systems of Systems
up to Eco-system
(Co-Existence)

System Type

No Safety Without Security

Security & Functional Safety (ISO 26262)

They are similar… Both are quality aspects, needed to ensure the proper operation of a system… but they are not the same

Functional Safety is concerned with unintentional hazards, which are predictable & regular

- Resulting from natural phenomena (e.g. extreme temperatures or humidity),
or from human negligence or ignorance (e.g. improper design or use)
- The environment doesn't change (and neither do the laws of physics…)

Security is concerned with intentional hazards, which are rather unpredictable & irregular

- Resulting from attacks planned and carried out by humans
- Hackers get smarter / better over time; and they don't follow "the rules"

No Safety Without Security

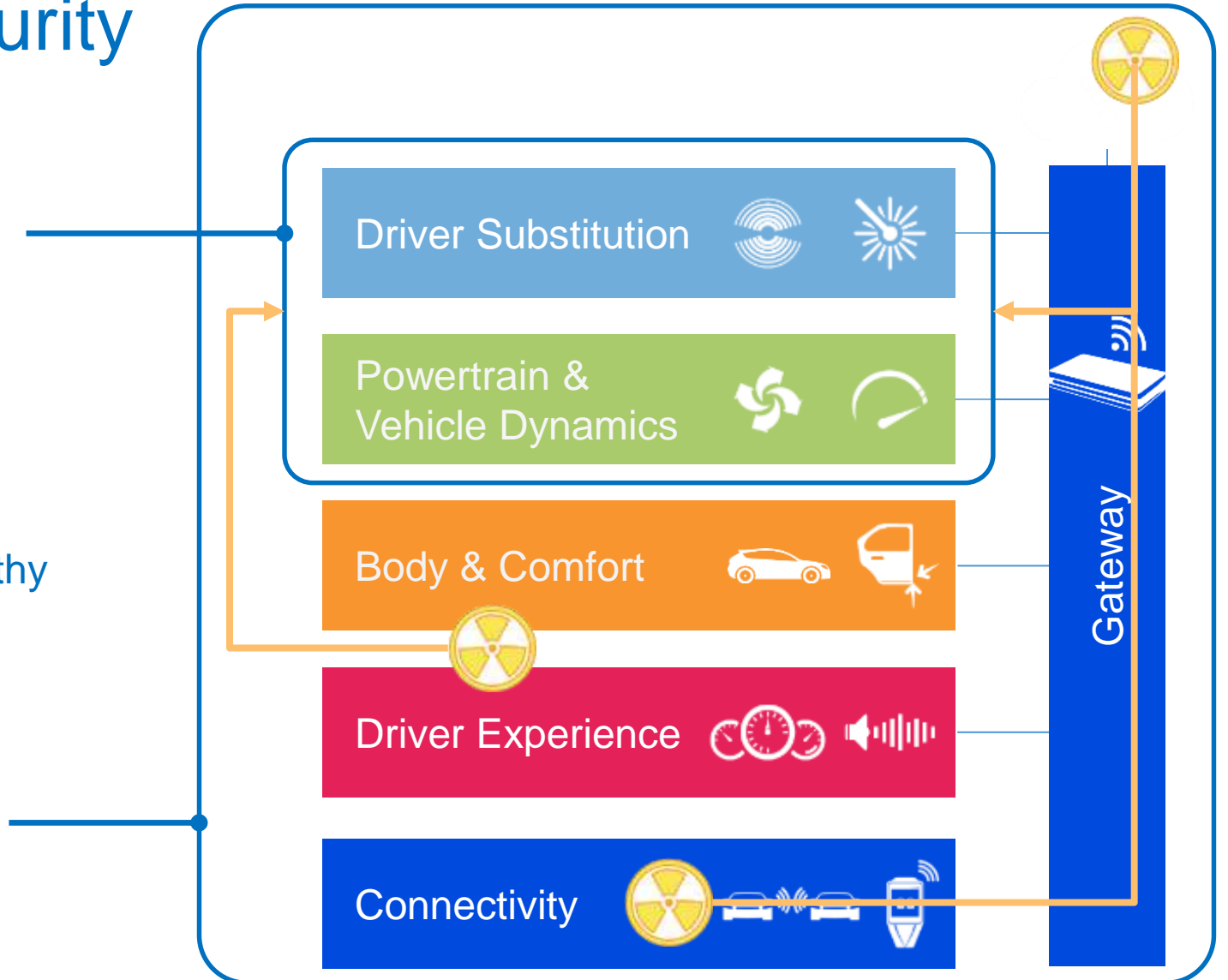#1 Objective: no functional hazards on mission-critical ECUs

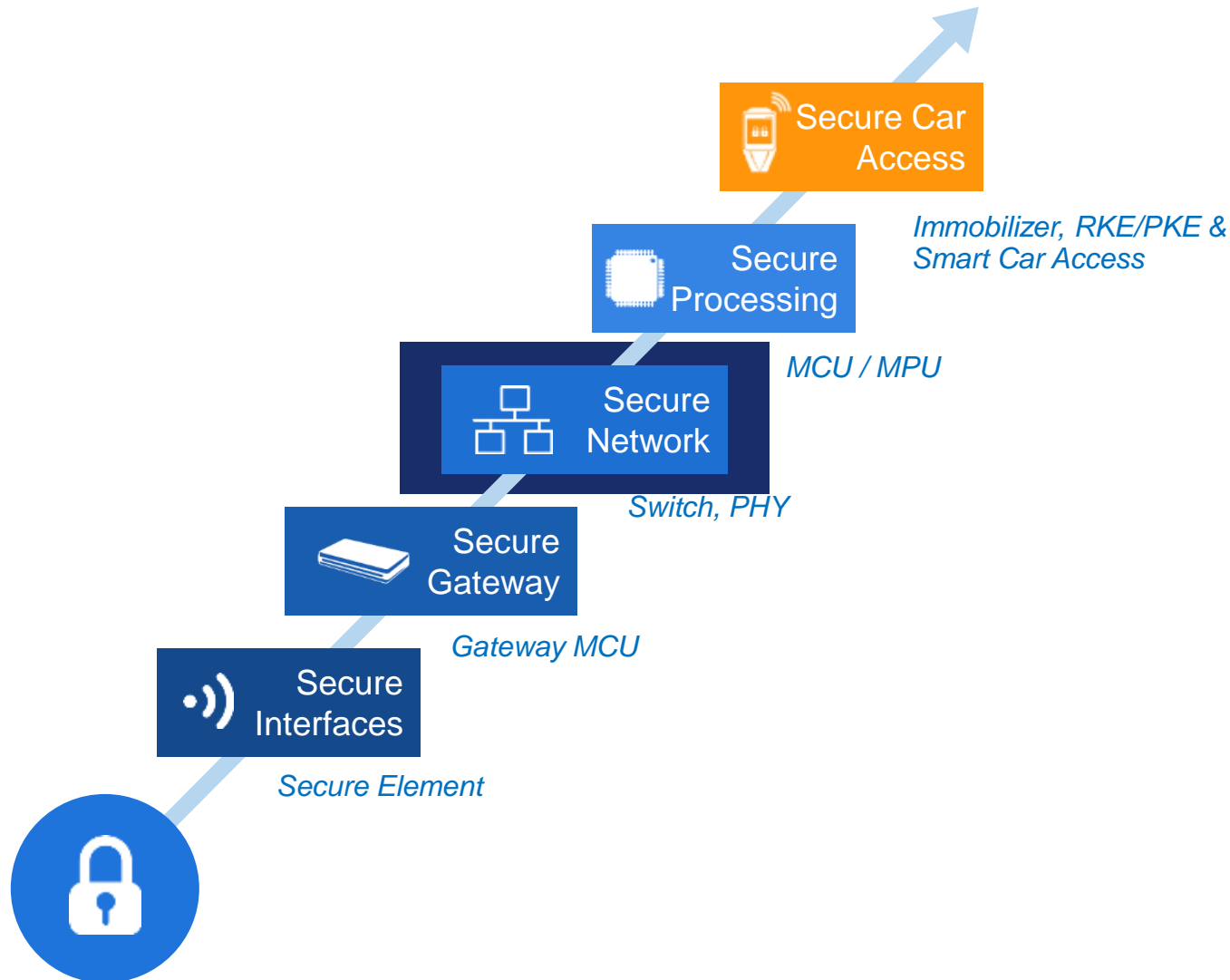*Collaterals:*
System availability ensured
Information received / processed trustworthy

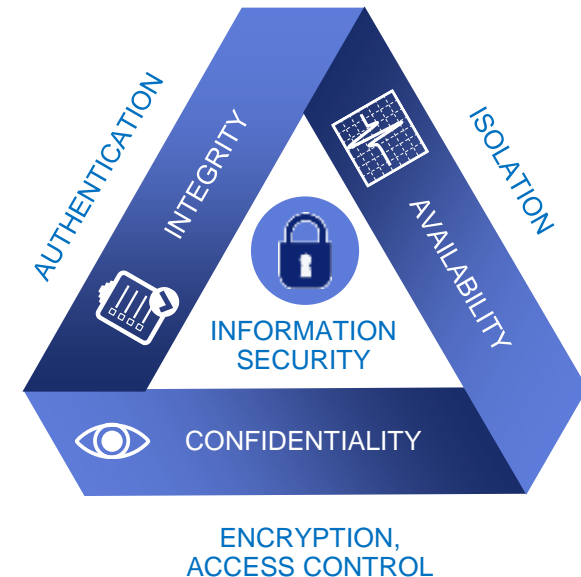Cyber-security is the mean to establish availability and trust in the system

Driver Substitution

Powertrain & Vehicle Dynamics

Body & Comfort

Driver Experience

Connectivity

Gateway

4+1 Approach: Most Scalable Auto Cybersecurity Solution

Secure Car Access

Immobilizer, RKE/PKE & Smart Car Access

Secure Processing

MCU / MPU

Secure Network

Switch, PHY

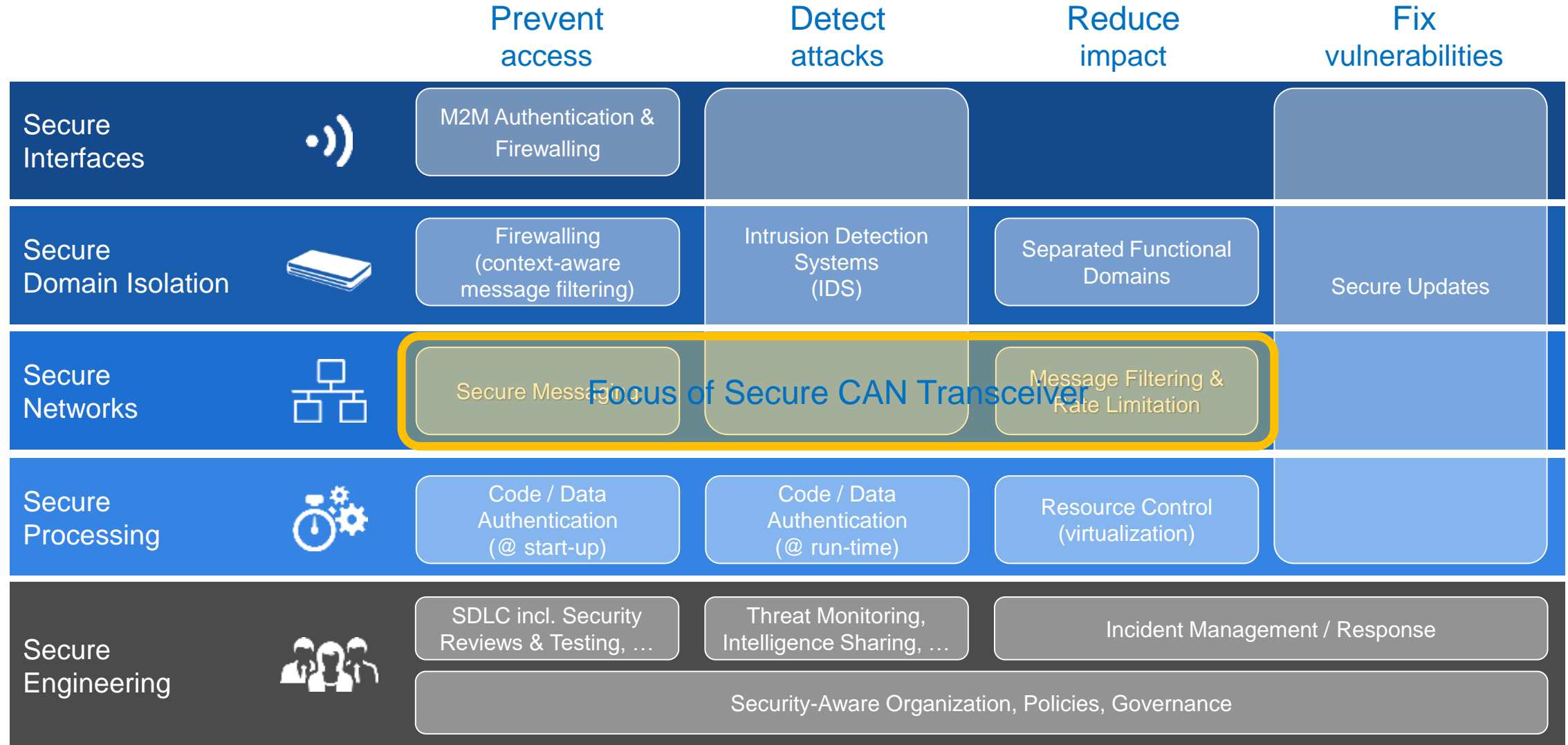**Secure Gateway**

Gateway MCU

Secure Interfaces

Secure Element

NXP #1 in Auto HW Security

4-Layer Cyber Security Solution, enabling defense-in-depth

Plus **'Best In Class'** Car Access Systems

AUTHENTICATION

INTEGRITY

ISOLATION

AVAILABILITY

INFORMATION SECURITY

CONFIDENTIALITY

ENCRYPTION, ACCESS CONTROL

Holistic Approach – Applying the Core Security Principles

		Prevent access	Detect attacks	Reduce impact	Fix vulnerabilities
Secure Interfaces		M2M Authentication & Firewalling			
Secure Domain Isolation		Firewalling (context-aware message filtering)	Intrusion Detection Systems (IDS)	Separated Functional Domains	Secure Updates
Secure Networks		Secure Messaging	Focus of Secure CAN Transceiver	Message Filtering & Rate Limitation	
Secure Processing		Code / Data Authentication (@ start-up)	Code / Data Authentication (@ run-time)	Resource Control (virtualization)	
Secure Engineering		SDLC incl. Security Reviews & Testing, …	Threat Monitoring, Intelligence Sharing, …	Incident Management / Response	
			Security-Aware Organization, Policies, Governance		

NXP Secure CAN Transceiver "TJA115x"

Direct CAN transceiver replacement!
Enables retrofit on running ECU designs

Pure hardware based solution.
Secure In-field reconfiguration possible

On-the-fly CAN ID Whitelist & Blacklist filtering
(HW Firewall)

Flooding prevention by Leaky bucket principle
from local host

Immediate Intrusion Containment by HW!

Desired complement for SW based IDPS
solutions due to support for reporting and logging

Enables OTA Service for legacy ECU´s

Helps to reduce system cost
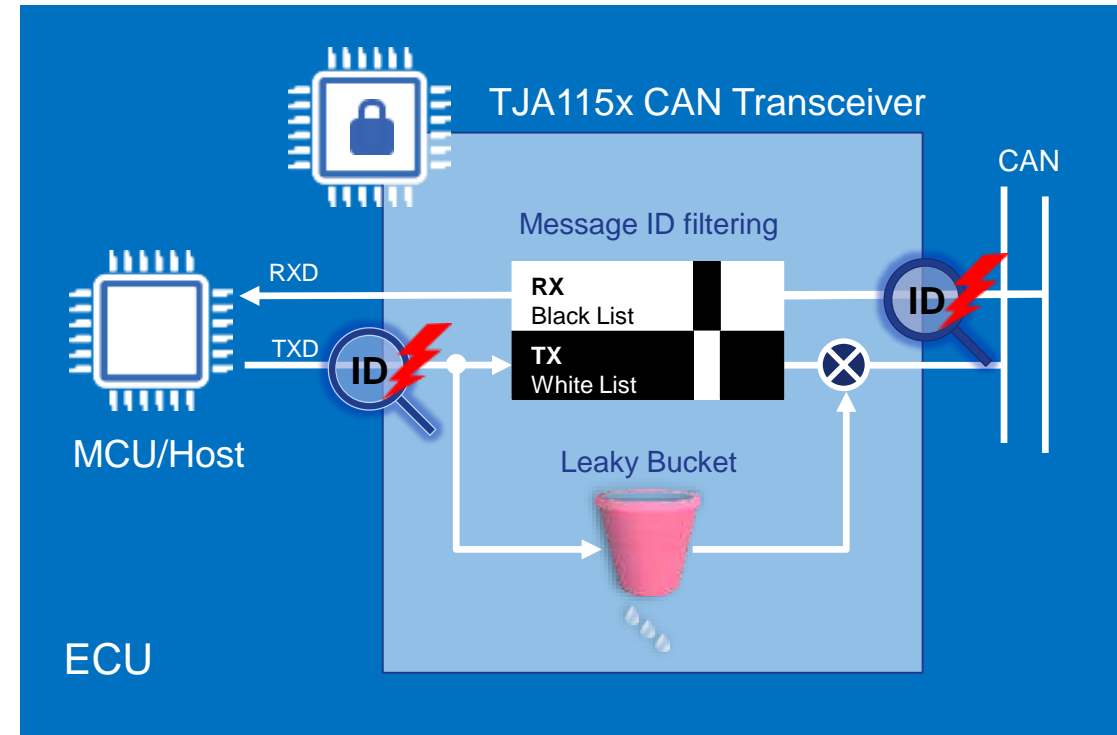
Spoofing Detection & Prevention

TJA115x – Spoofing Prevention – Transmit Path

- ECU 2 gets compromised and pretends to be another ECU (Spoofing)
- Only messages with ECU 2 legitimate ID [ID 0x400] can pass the TJA115x hardware filter!
- TJA115x TX Whitelist stops transmission of any non-legitimate ID from ECU 2
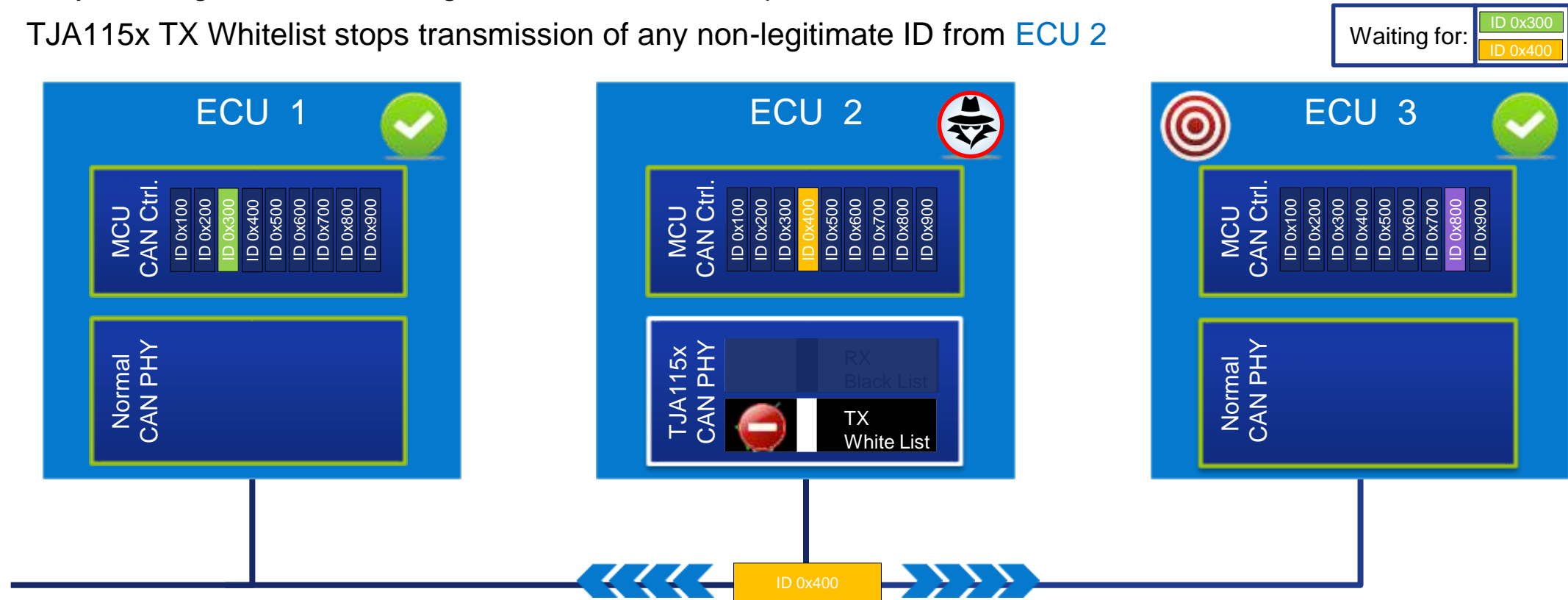
TJA115x protects the network against sending non-legitimate ID´s

TJA115x – Spoofing Prevention – Receive Path

- Compromised ECU 1 pretends to be another ECU (Spoofing)
- TJA115x RX Blacklist guards it´s own legitimate ID on the bus by detection and elimination with active error flag
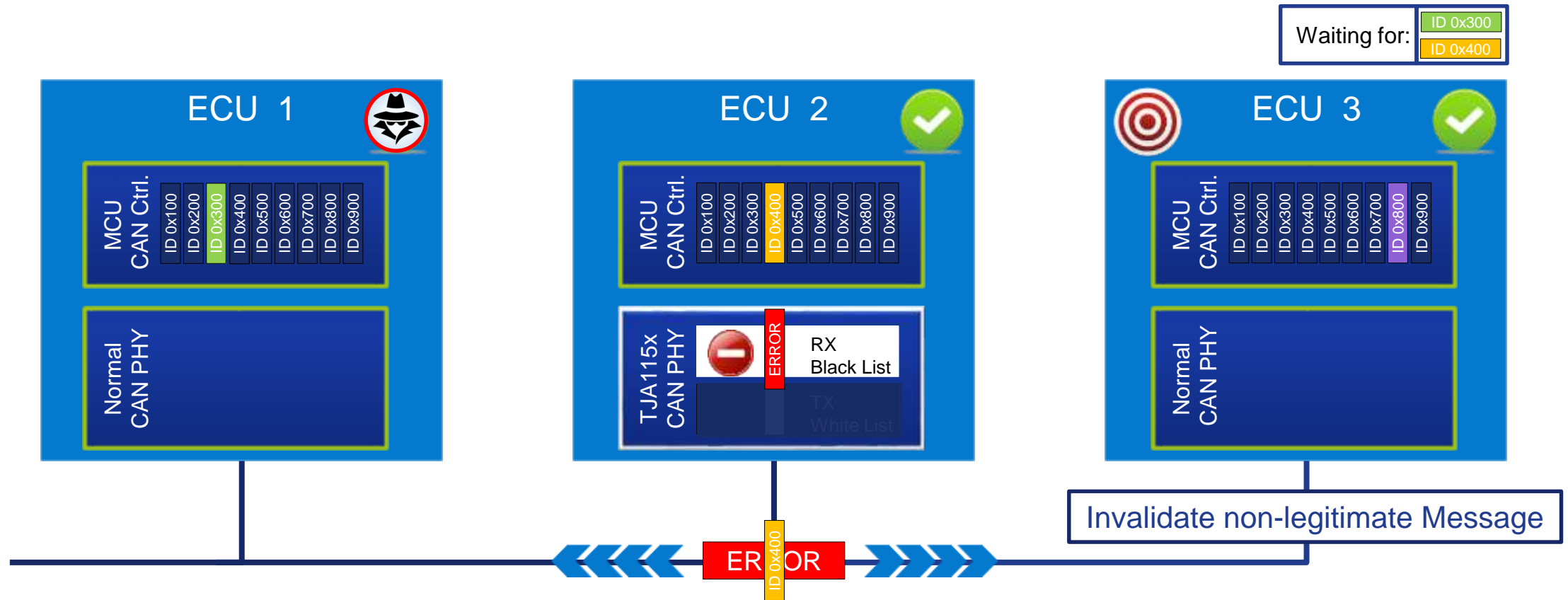
TJA115x protects the network by guarding its own ID

Tamper Protection

Principle Of Tampering

Spoofing Legitimate Message Content

- Goal: Circumvent spoofing protection by tampering messages (legitimately initiated) which may be of critical operation for the car

- Attacker aims to adjust a message, which another ECU is currently sending on the bus

- Take control on data field, send dominant bit while the legitimate ECU sends recessive bit (bit flip)

- Cyclic redundancy check (CRC) need also be adjusted to match the tampered data

ECU2 stops transmission, when first recessive bit is overwritten by a dominant one.

ECU2 transmits	SOF	Identifier	Control	Data	

ECU1 transmits	Rogue Data	CRC

ECU1 starts with rogue data

ECU3 transmits	ACK

ECU3 acknowledges, as it sees a complete frame with correct CRC
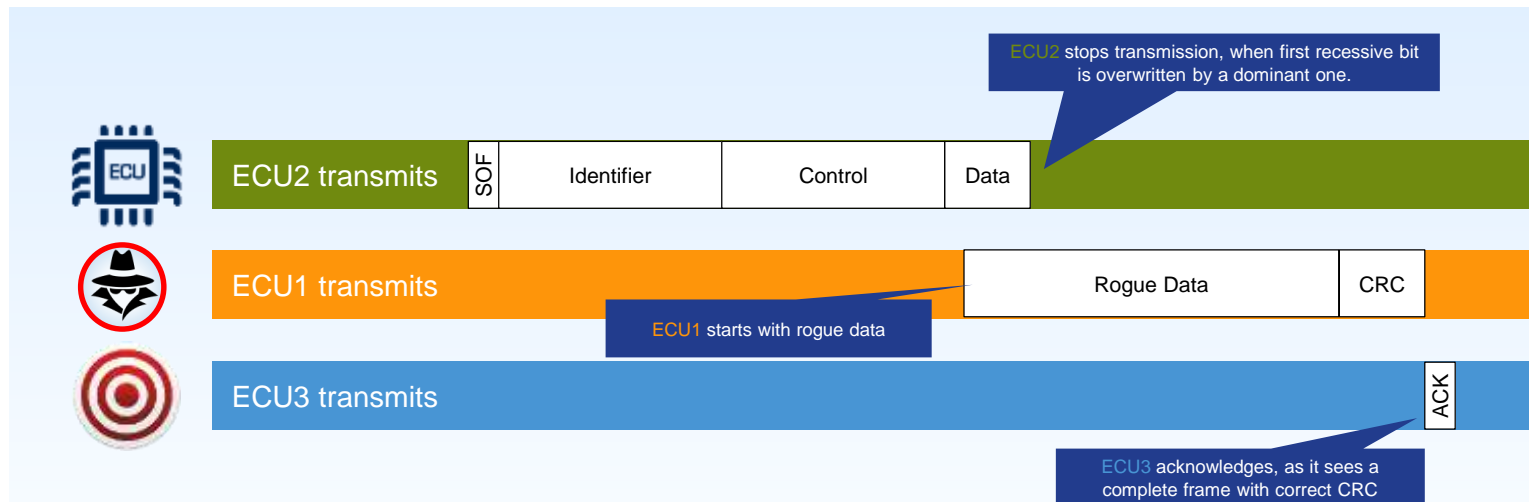
Timeslot For Tampering

- Legitimate sender must be forced into Error-passive state, otherwise an active error will be reported on the bus when the attacker causes a bit flip

- Error-passive state enforced by intentionally publishing errors on the bus for several times (16 attempts)

Error Active:
Actively publish errors when they are detected

Error Passive:
Send as normal, but no longer publish errors on the bus

Bus Off:
Do not send messages anymore

Messages:
Triggered by compromised ECU, sending dominant bit, while legitimate ECU sends recessive bit → Bit Flip: ERROR reported

16 additional attempts
- Of the legitimate ECU sending it´s message – without reporting errors when encountered!
- Bit flip errors not reported!

No messages send anymore by legitimate sender – Denial of Service

→ Gap for successful tamper / spoofing attack

TJA115x – Tamper Protection

- Compromised ECU 1 forces ECU 2 into „Error passive" state first
- Data field of the message initiated by ECU 2 gets tampered by compromised ECU 1
- TJA115x of ECU 2 identifies a bit flip (Direction Change) and issues an active error flag
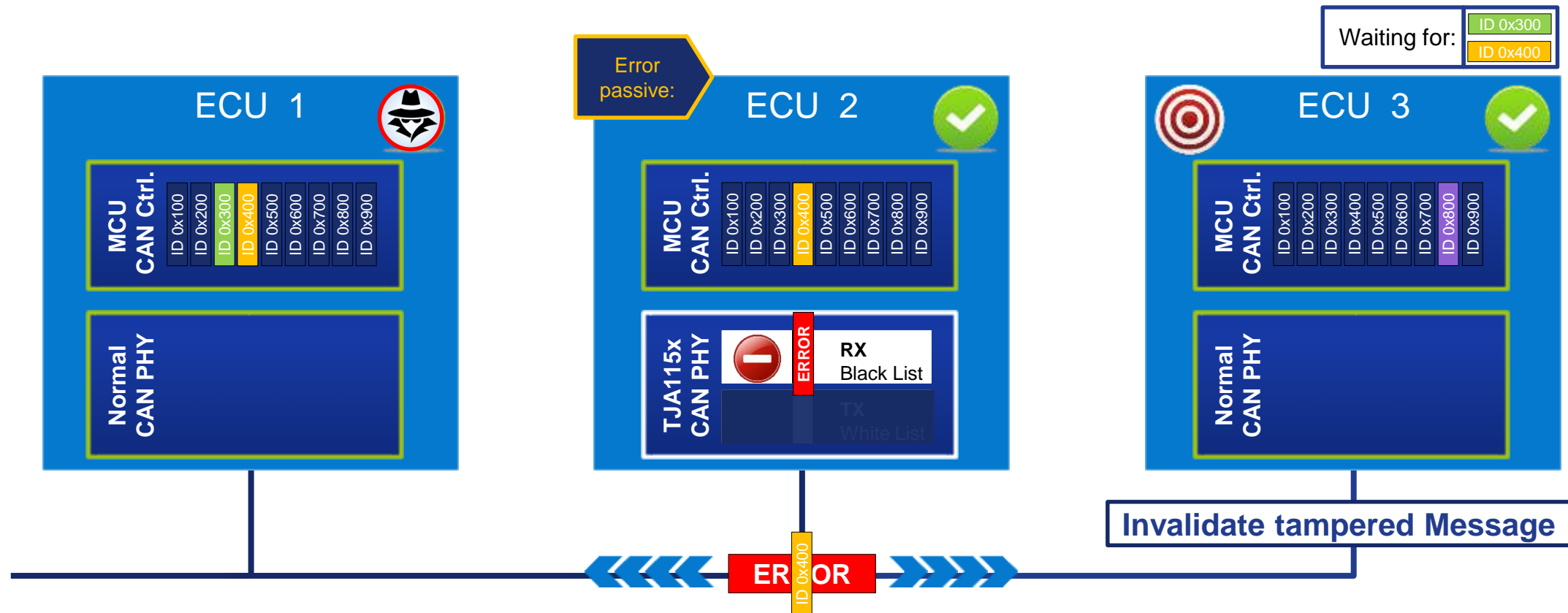
TJA115x is protecting the error passive state

Prevention & Denial of Service/ Flooding
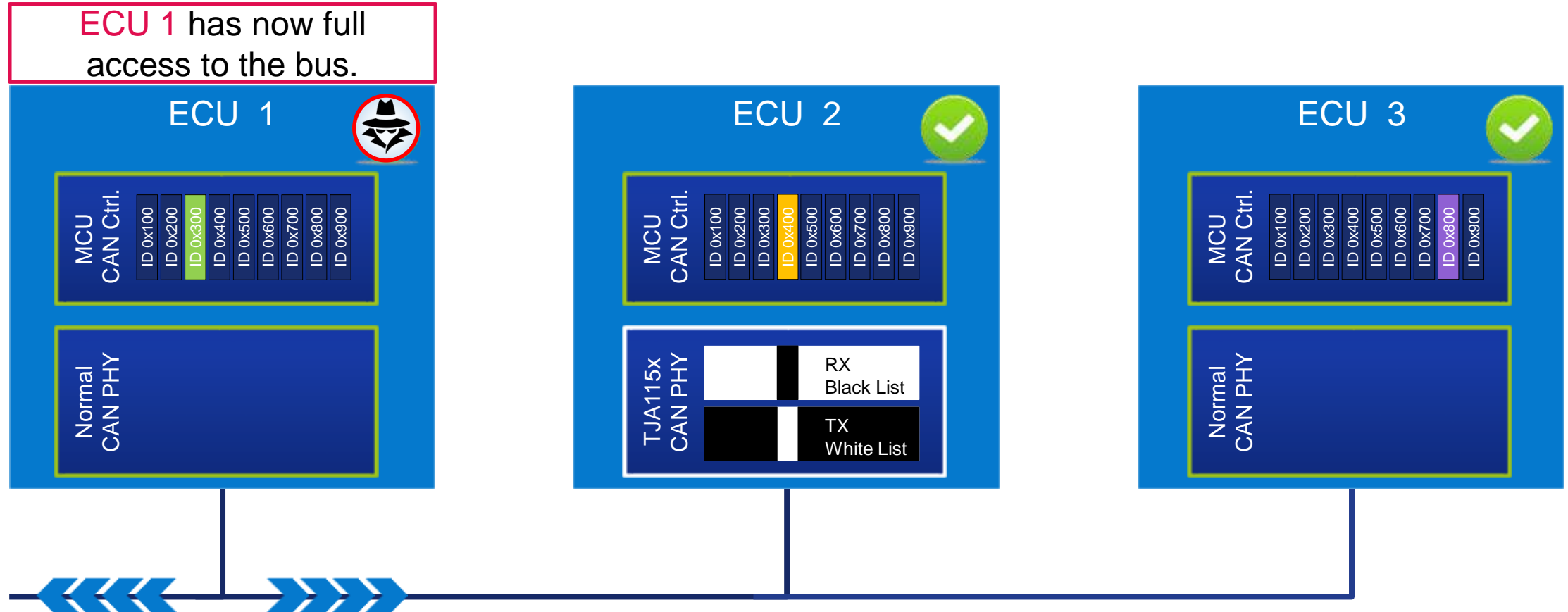
TJA115x – Flooding Prevention

- **ECU 2** gets compromised and can now try to flood the bus
- When the increased busload violates configured TJA115x ruleset, the local host is set into Bus Off/Secure State
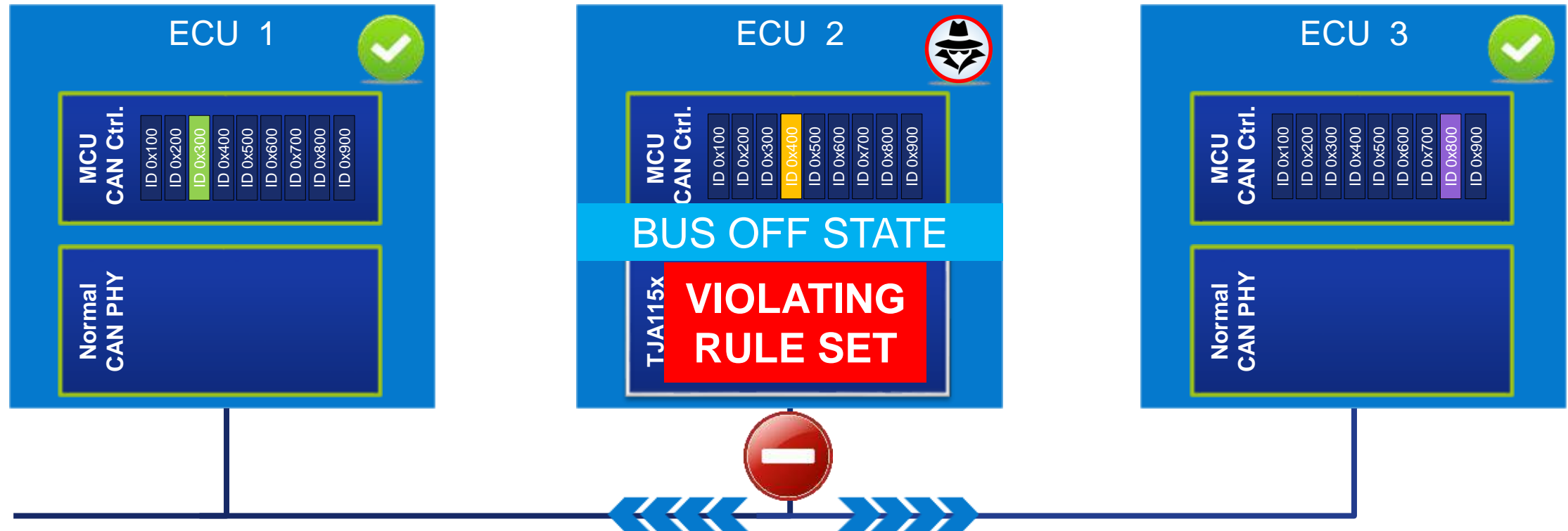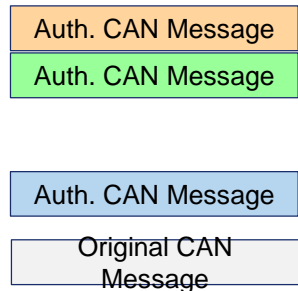

TJA115x protects the network against flooding!

How TJA115x Helps

TJA115x Has No Bandwidth Overhead & Transmission Delay for Local Secure CAN Communication

Message

Counter

MAC

SW Payload Auth.
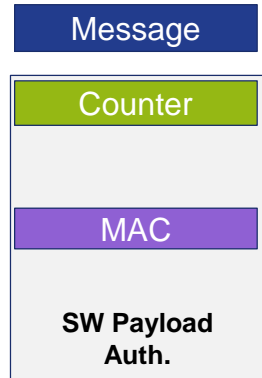
- Original Message (example 2 Bytes)

- Increasing Busload - Delays transmission

- More complex SW
- MACing requires keys and extra processing
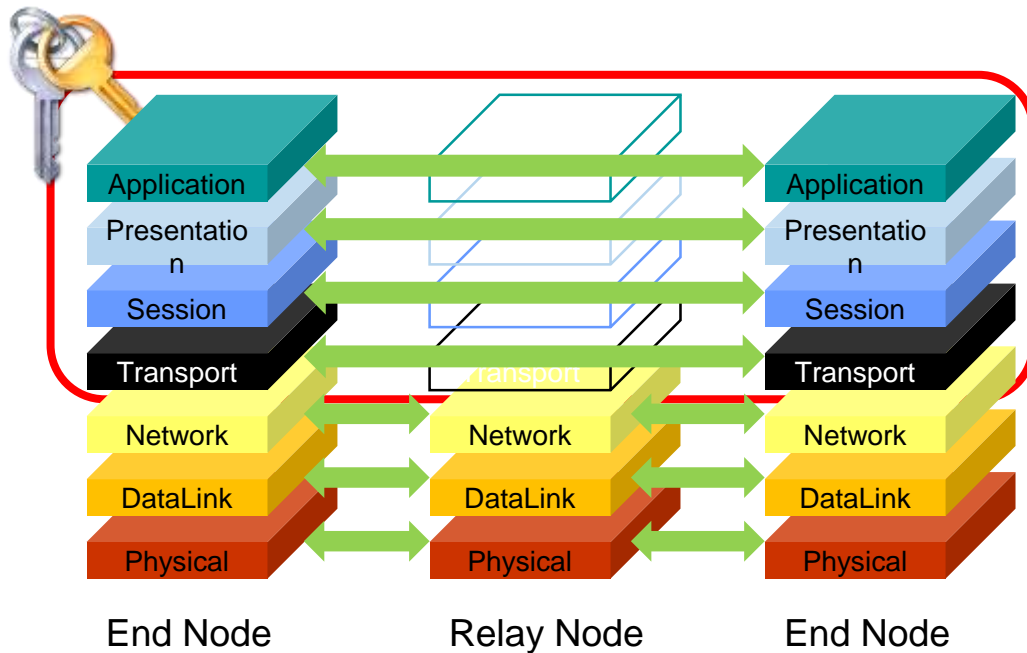- Increasing Busload - Delays transmission

Auth. CAN Message

Auth. CAN Message

| 1 Byte | 1 Byte | 1 Byte | 1 Byte | 1 Byte | 1 Byte | 1 Byte | 1 Byte | 1 Byte | 1 Byte | 1 Byte | 1 Byte |

| 1 Byte | 1 Byte | 1 Byte | 1 Byte | 1 Byte | 1 Byte | 1 Byte | 1 Byte | 1 Byte |

Auth. CAN Message

Original CAN Message

| 1 Byte | 1 Byte | 1 Byte | 1 Byte | 1 Byte | 1 Byte | 1 Byte |

| 1 Byte | 1 Byte |

Payload HS-CAN Frame (8 bytes)

Auth. Bandwidth Overhead (Classical CAN)

☐ Auth Payload Time [2+8]
☐ Auth Payload Time [2+5]
☐ Auth Payload Time [1+4]
☐ Plain Payload Time

TX Time [µs]

x2.5

Secure CAN Transceiver TJA115x provides HW based Authentication without cryptography!

Plain Payload Size [bytes]

Secure Network Communication

End2End	On local CAN bus

- AUTOSAR SecOC (or alike) defines secure communication on OSI layers above DataLink.

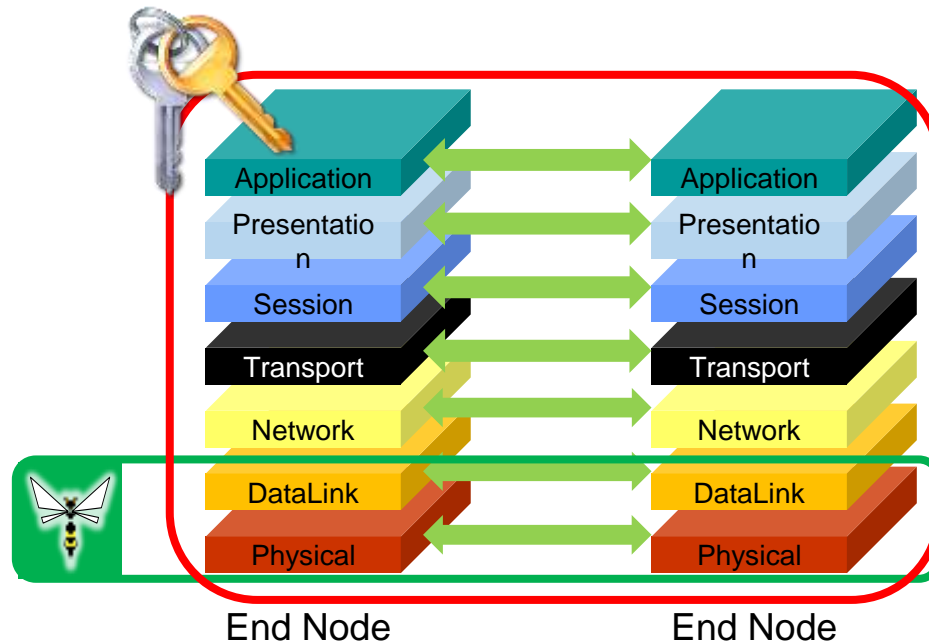- End2End secure communication that crosses different ECU´s cannot rely on DataLink protection.

- For secure communication on a local CAN bus, protection at any layer is equivalent.

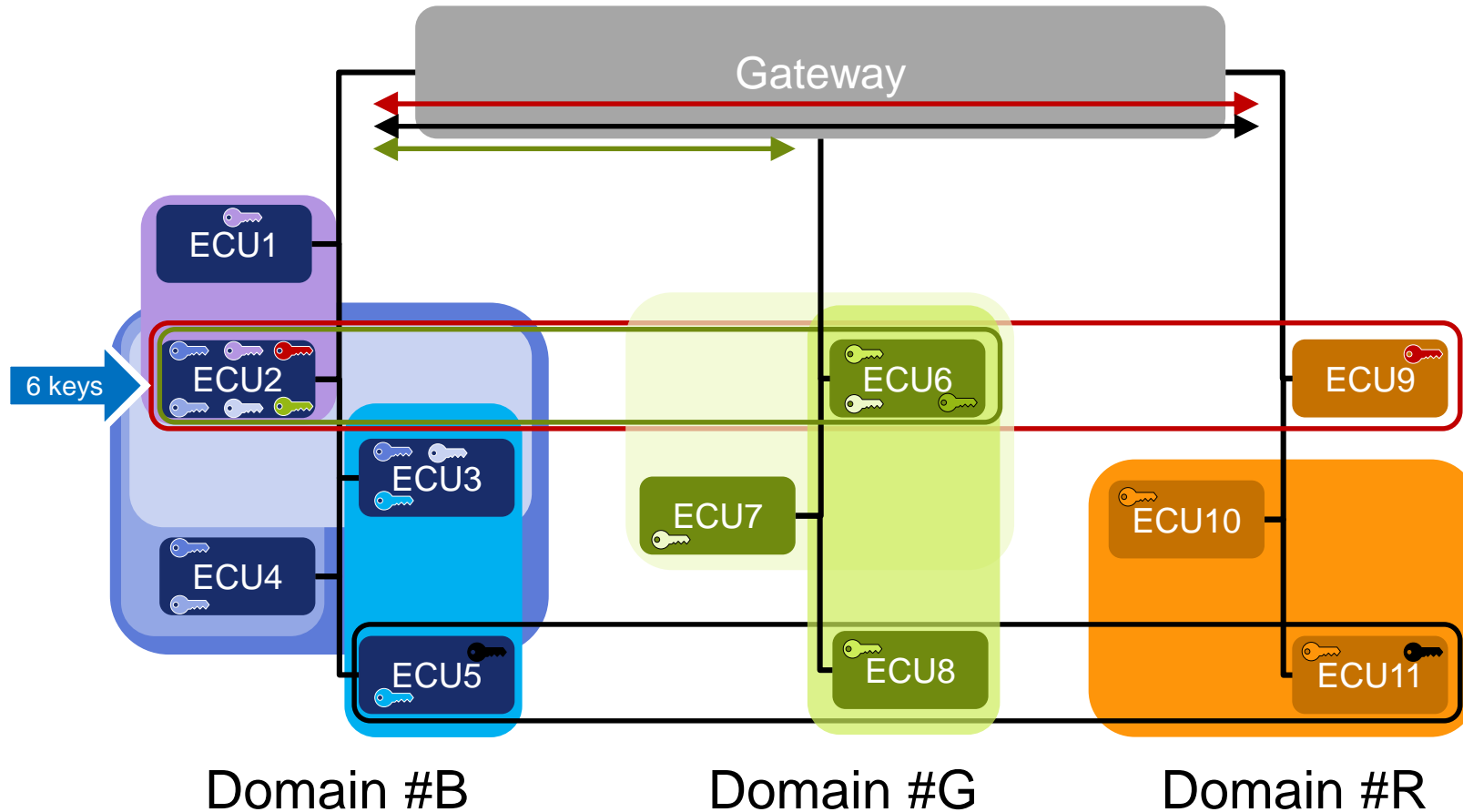- Data Link protection is sufficient for local bus communication

Efficient Solution without secure keys:
- Apply TJA115x on Physical/DataLink layer
- Achieve same level of protection like AUTOSAR SecOC or alike.

Secure keys need to be applied on one of the upper layers

Traditional Solution: Secure keys can to be applied at any layer.

Typical Network Secured By Payload Authentication And Keys

Gateway

ECU1
ECU2
6 keys
ECU3
ECU4
ECU5

ECU6
ECU7
ECU8

ECU9
ECU10
ECU11

Domain #B   Domain #G   Domain #R

- 1 Gateway
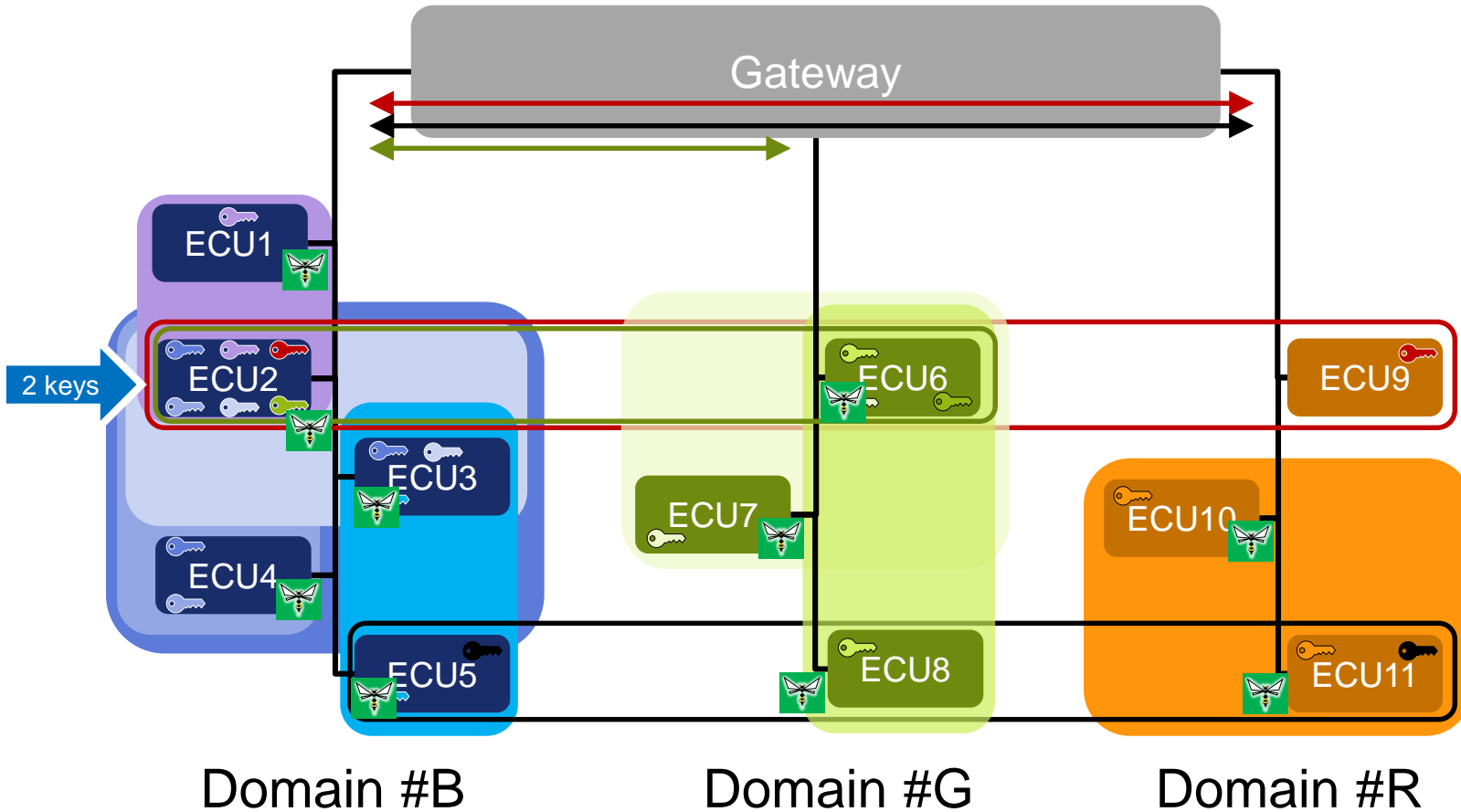- 3 Domains
- 11 ECUs
- Multiple local domain applications

- 3 cross domain / E2E applications

- Secured by keys
  - ECU #2 needs many keys

Local Communication Secured With TJA115x – Same Network

Gateway

ECU1
ECU2
2 keys
ECU3
ECU4
ECU5

ECU6
ECU7
ECU8

ECU9
ECU10
ECU11

Domain #B   Domain #G   Domain #R

- 1 Gateway
- 3 Domains
- 11 ECUs
- Multiple local domain applications

- 3 cross domain / E2E applications

  Remains 3 keys for E2E comm.

- No keys for local application

  – Less keys for ECU #2

System View – How Does TJA115x Help?

Impact of SW-based authentication

Benefit of using TJA115x

Secure Keys
- Keys for E2E communication
- Keys for local CAN communication

- Removes keys for <u>local</u> CAN communication

Saving keys!

Start Up
- Delayed by check on counter, exchange of freshness values (session setup)

- No delay – Authenticated by HW

No extra startup delay!

Software
- Complex SW process applies for secure E2E and local CAN communication
- Increased complexity, if secure flash is not sufficient – extension by external embedded flash is required

- Local CAN communication can follow simple CAN communication – no extra SW required!

Less complex

Processing
- SW process for secure CAN communication applies for <u>every</u> CAN message at any time

- Extra processing only applies for secure E2E communication – not required at all for local CAN communication

Offloading MCU

Bandwidth/ Transmission
- Overhead data (counter, MAC) added to every secure CAN message – Increase of busload and transmit time
- Realtime capability on high risk

- No overhead – No delay for local CAN communication
- Realtime capable!

No overhead, no delay

NXP

Logging/ Reporting – IDS

IDPS – On CAN Communication

- Intrusion Detection & Prevention Systems aim to identify an unspecified behavior and malicious ECUs

- Identifying the sender in a CAN system is per CAN ISO-Specification not supported

- TJA115x do provide mechanisms to indentify the sender – perfectly closing the Spec gap to support IDS:

  → IDS/IDPS system can now properly perform it´s task with the right assumption – knowing the sender of the message is the legitimate one

- TJA115x enables immediate and effective containment of the intrusion.

  → No delay by any SW analysis/processing

TJA115x – Reporting Of Security Incidents – Transmit Path

- The length of the error frame (6 bit or 11 bit) is user configurable

- The length of an 11 bit error flag after CRC delimiter is a unique sign of a TJA115x reported security incident.
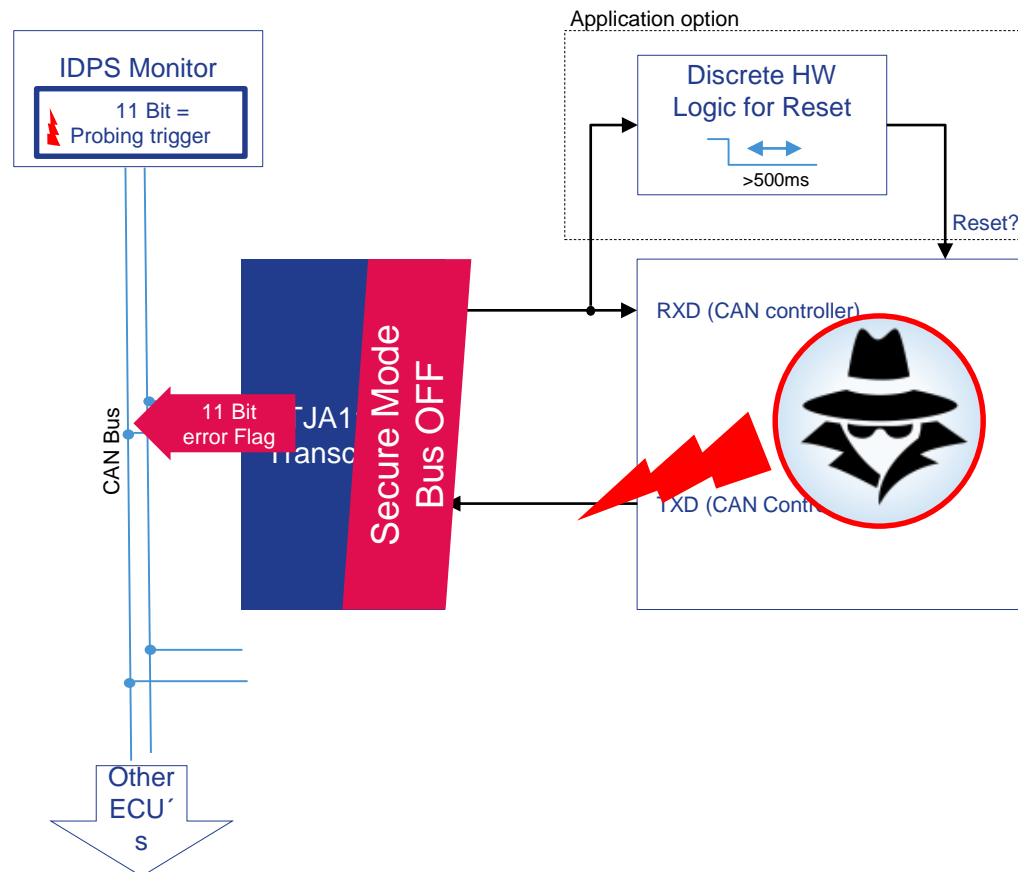
- There is no value in reporting to the compromised host that it <u>is</u> compromised!

- When TJA115x is triggered from local host by Whitelist Filtering or Busload violation (Flooding), then TJA115x
  - Sends the 11 bit error flag
  - Enters Secure Mode and disconnects from the bus (Bus OFF for 2s)
    - *RXD = Low* for more than 500ms – could be used to enforce a secure re-boot (by discrete HW logic).

- A node probing the bus (IDPS Monitor) has the ability to read CAN IDs and data from the bus and gets to know whether a invalid frame that was invalidated by a TJA115x or not.

- A node probing the network status can detect the secure state/bus-off by unexpected but recognizable lack of periodic status message (known pattern) which helps to identify the compromised node.
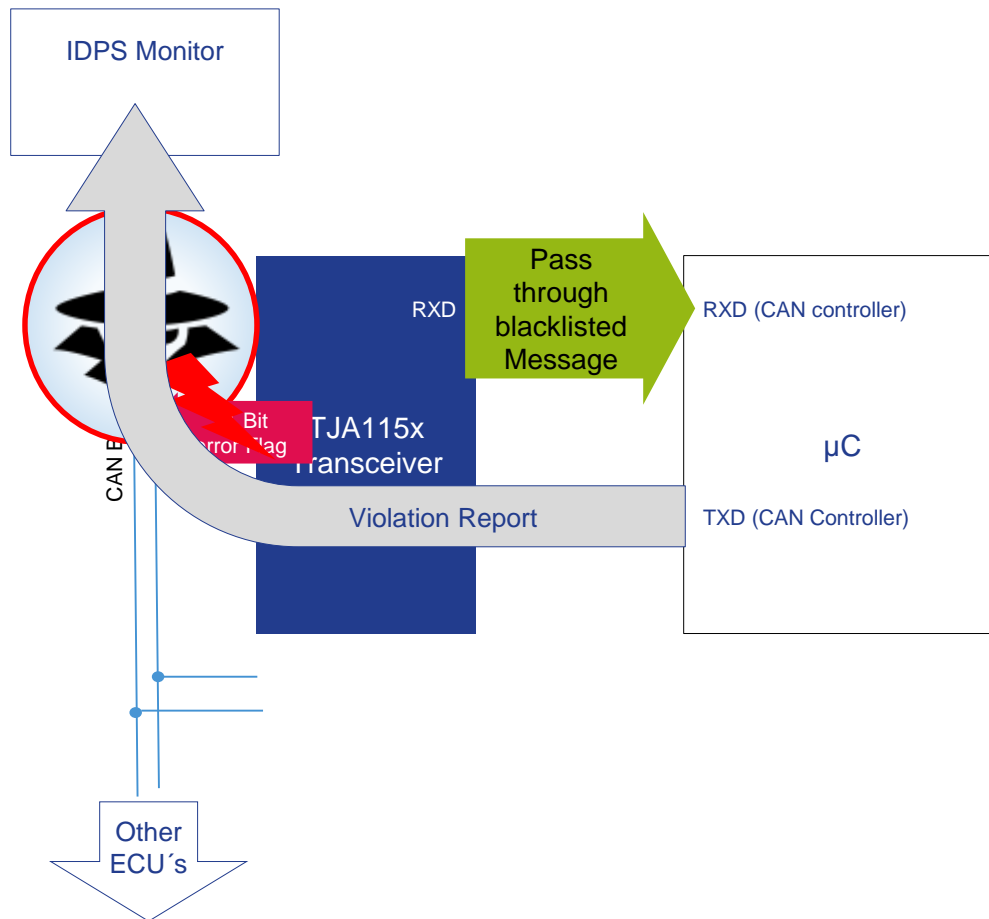
Application – IDPS Support

- Recommended for CAN-ECU´s, which send critical messages

- When locating a malicious CAN ECU is required!
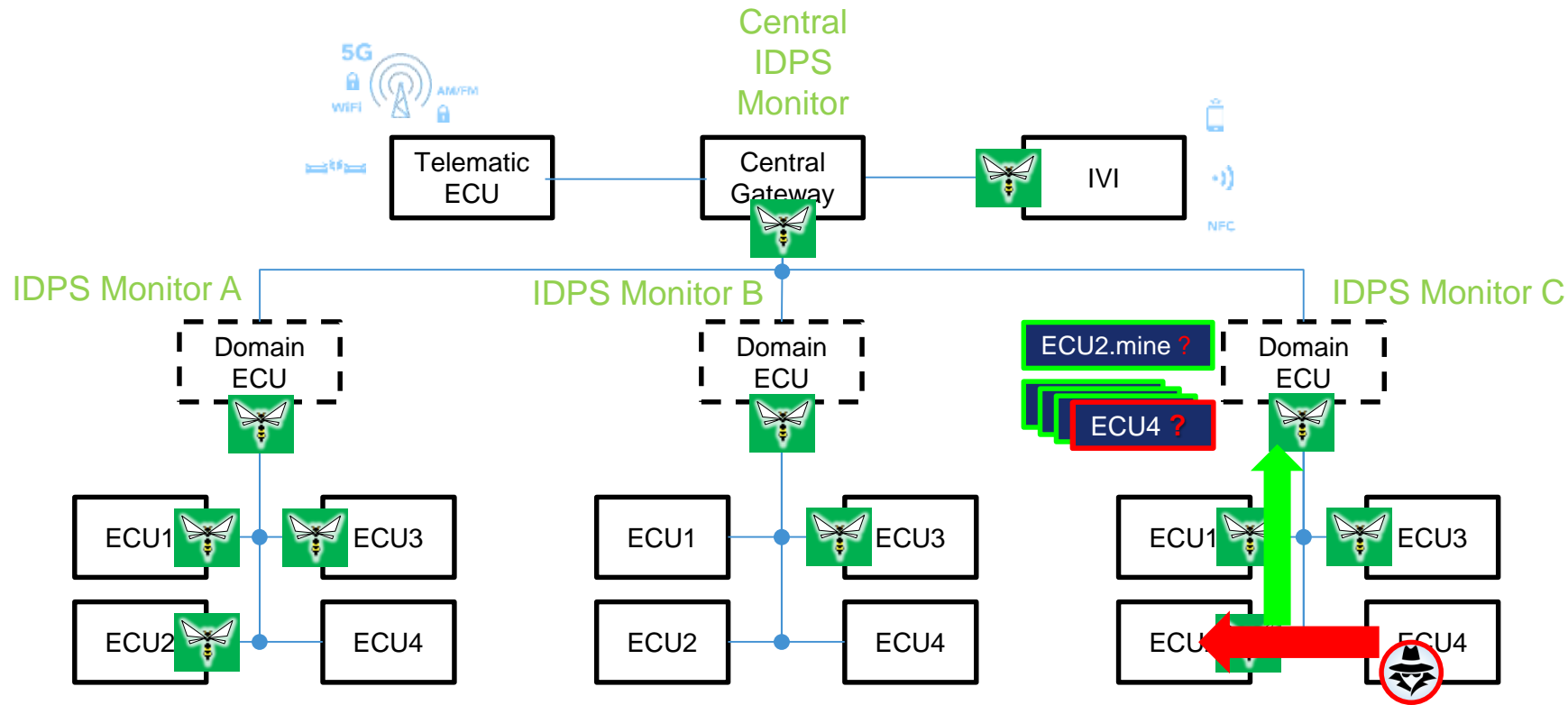
- When immediate containment is desired.
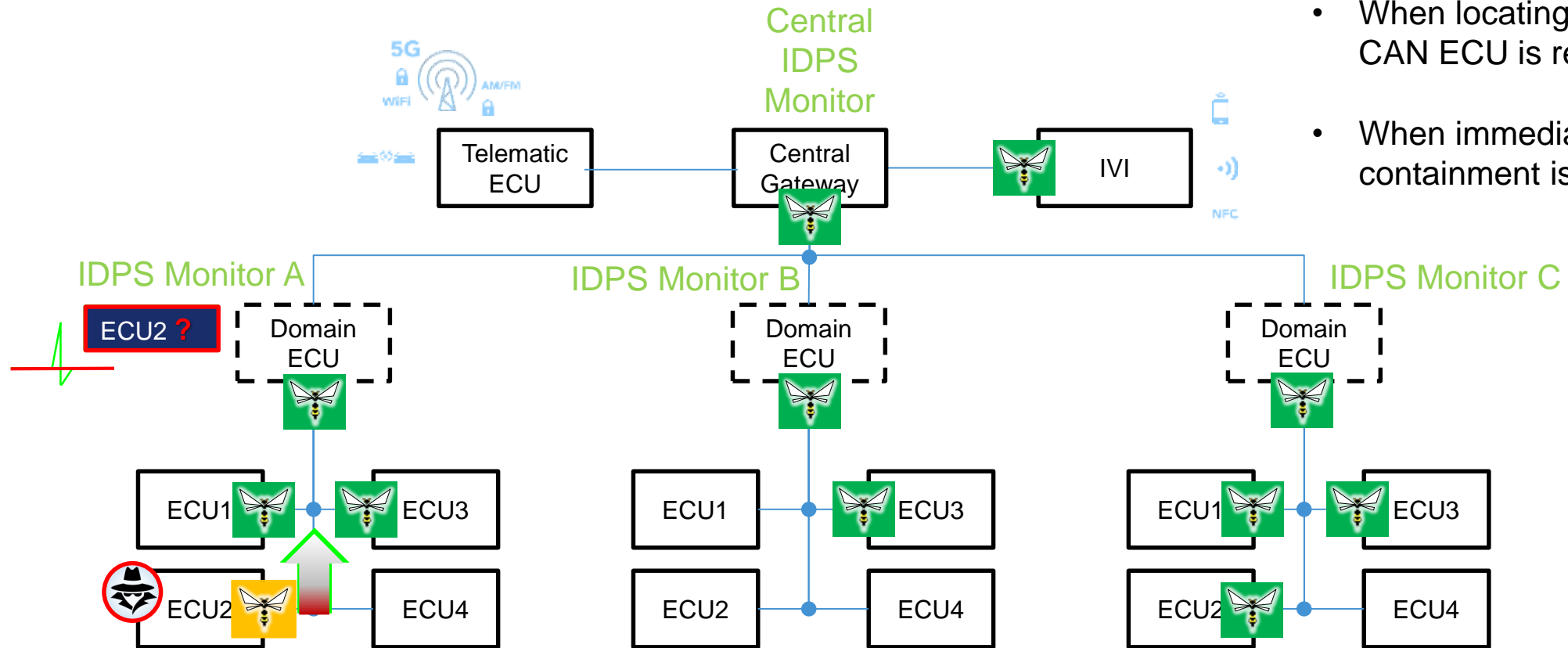
Example Only! Evaluation, where to use Secure CAN transceiver strongly depends on the E/E architecture and the threat model/use cases considered by the OEM.

TJA115x – Reporting Of Security Incidents – Receive Path

IDPS Monitor

Pass through blacklisted Message

RXD

TJA115x Transceiver

Bit Error Flag

Violation Report

µC

RXD (CAN controller)

TXD (CAN Controller)

CAN B

Other ECU´s

- Typically a CAN node does not have receive buffers configured for CAN IDs it is supposed to send.

- In case the node wants to see whether another node is abusing his messages, it might be reasonable to configure receive buffers accordingly.

- When TJA115x detects a Blacklist violation or Tampering, it…

  - Invalidates the message on the bus by the 11 bit error flag – but not on RX- by keeping RXD on recessive after the ACK, while the bus is dominant! !

  - Able to present this message correctly to the CAN controller, even when invalidated on the bus.

    ▪ By this, the node can see that a compromised host has made the unsuccessful attempt to send one of its CAN IDs

  - Able to report – protected by TJA115x - that buffered message to the IDPS Monitor for further analysis.

Application – IDPS Support

- Recommended for CAN-ECU´s, which send critical messages

- When locating a malicious CAN ECU is required!

- When immediate containment is desired

Example Only! Evaluation, where to use Secure CAN transceiver strongly depends on the E/E architecture and the threat model/use cases considered by the OEM.

# IDPS on CAN – SW Solution Only (Local Bus)

OEM-Requirement for	Sending out of context data	Tampering CAN data	Spoofed CAN message by local host	Spoofed CAN message by remote host	Flooding Transmission
Detection of incident	✓	(✓) As „Out of Context" Data	(✓) As „Out of Context" Data	(✓) As „Out of Context" Data	✓
Prevention of incident	X	X	X	X	X
Origin of incident	X	X	X	X	X
Time of incident	✓	✓	✓	✓	✓
Additional Details	✓	✓	✓	✓	✓

Jointly reviewed with different Cyber Security SW companies

IDPS on CAN – TJA115x Completes Any SW Solution

X Not supported
✓ Fully supported

OEM-Requirement for	Sending out of context data	Tampering CAN data	Spoofed CAN message by local host	Spoofed CAN message by remote host	Flooding Transmission
Detection of incident	✓	✓ Transmission aborted	✓ Transmission Whitelist	✓ Bus Blacklist Monitor	✓ Leaky Bucket rules
Prevention of incident	X	✓ Invalidating by Error Flag	✓ Invalidating by Error Flag	✓ Invalidating by Error Flag	✓ Secure Mode
Origin of incident	✓ Validated by TJA115x	X	✓ Secure Mode	(✓) Node w/o TJA115x	✓ Secure Mode
Time of incident	✓	✓ 11 Bit Error Flag	✓ 11 Bit Error Flag	✓ 11 Bit Error Flag	✓
Additional Details	✓	✓	✓	✓ Report blacklisted Msg.	✓

Jointly reviewed with different Cyber Security SW companies

NXP + Elektrobit + ARGUS – IDPS Solution
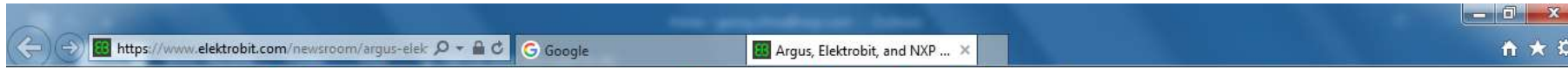
Argus, Elektrobit, and NXP provide combined solution to protect connected and automated vehicles

January 7, 2019

Comprehensive solution provides real-time prevention, defense in depth, and the ability to respond, recover, and protect vehicle fleets against even the most sophisticated attacks as they emerge.

Share this

LAS VEGAS (CES 2019, North Hall Booth #6106), January 7, 2019 – Elektrobit (EB), a visionary global supplier of embedded and connected software products for the automotive industry, and its subsidiary, Argus Cyber Security (Argus), a global leader in automotive cyber security, announced today that they are collaborating with NXP to bring to market the industry's first complete software-hardware solution that delivers comprehensive protection against even the most sophisticated cyberattacks. With vehicle safety as the highest priority, it is critical that OEMs have the ability to provide passengers with optimal defense against cyber threats. The combined solution enables car makers to comply with upcoming regulations and current guidelines that require equipping vehicle systems with the ability to detect and respond to cyber-security incidents.

This first-of-its-kind solution consists of:

- NXP's Secure CAN Transceiver for a vehicle's controller area network (CAN) bus, which detects and prevents malicious activity at the CAN bus level;

- Argus' Intrusion Detection and Prevention Software (IDPS), which detects potentially malicious activity through data and timing heuristics, and then reports this activity to a security backend to enable an appropriate response;

- EB cadian Sync software, which enables continuous over-the-air (OTA) updates in the vehicle, including critical updates to ECUs as necessitated by the NXP Secure CAN Transceiver and Argus IDPS findings.

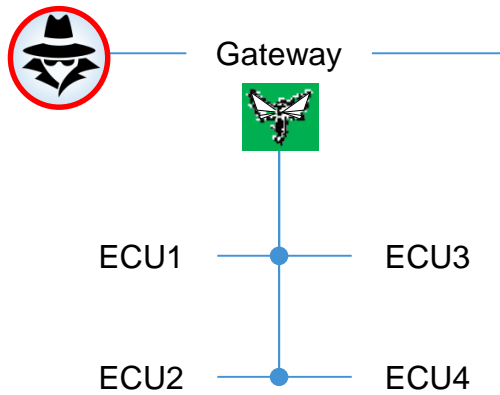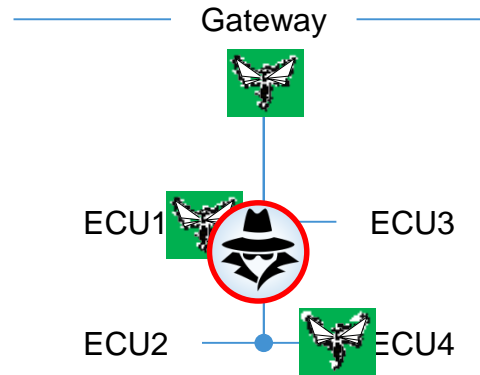**Joint demonstrator presented at CES 2019 in Las Vegas**

Confirmed Use Cases
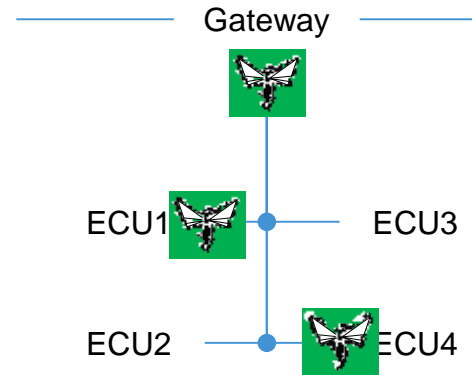
Confirmed OEM Use Cases

Firewalling
Flooding
Protection

Immediate protection
By HW – No SW!

Offloading MCU
Saving Bandwidth
Saving keys

IDPS
Support

Monitor

Gateway

ECU1   ECU3

ECU2   ECU4

Gateway

ECU1   ECU3

ECU2   ECU4

Gateway

ECU1   ECU3

ECU2   ECU4

Gateway

ECU1   ECU3

ECU2   ECU4

Legacy
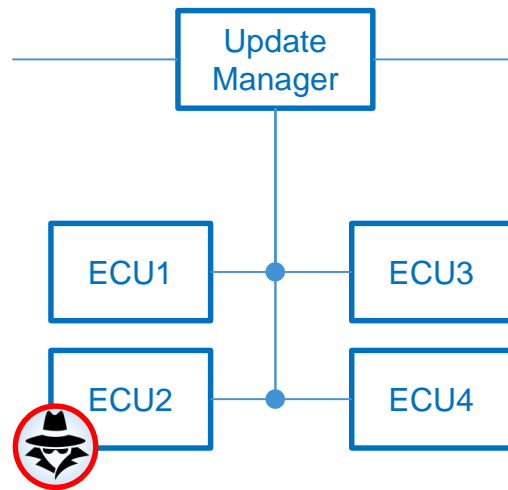New Platforms

Legacy
New Platforms
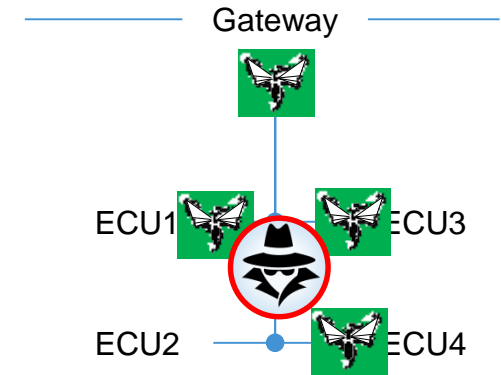
New Platforms

New Platforms

TJA115x Helps for OTA Service for Legacy ECU´s
Request for Legacy ECU´s, Which Do Not Have a Strong Security Mechanism

- Recommend TJA115x at OTA Manager (Sender/Updater)

- Enable Control of CAN access to OTA Client

- CAN ID to address the OTA Client is part of the BBL of the OTA Manager TJA115x
  - Nobody else, other than the OTA Manager, can update the OTA client!

- OTA Client update is only possible by a trusted OTA manager
  - Running on authentic code following secure boot!
  - Enabling the CAN ID to address the OTA Client only volatile in TWL – removing again before closing config session
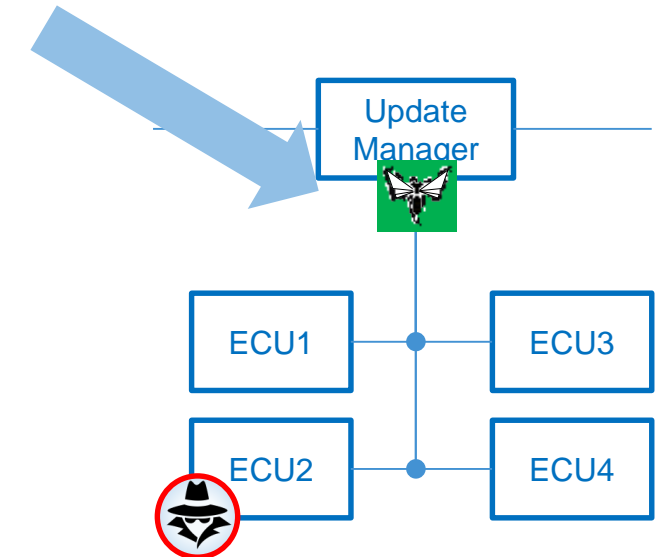
Final Message

- No Safety without Security
- TJA115x is a HW replacement for existing CAN transceiver.
- TJA115x legitimate sender without cryptography for local CAN communication
- TJA115x enables, improves and simplifies security for CAN communication.
- TJA115x is complementing secure MCU´s to make the system much more efficient.
- TJA115x nicely complements and support IDPS systems.
- Think system for cybersecurity solution.

SECURE CONNECTIONS
FOR A SMARTER WORLD