

Secure CAN Transceiver

Allen Houck

Business Development – In Vehicle Networking and Cybersecurity

October 2018 | AMF-AUT-T2854



SECURE CONNECTIONS
FOR A SMARTER WORLD

Agenda

- Security Intro – Secure Network
- Security Value of TJA115x :
 - Spoofing Protection
 - Tamper Protection
 - Flooding Prevention
- System Value of TJA115x
- Customer Value & Product

NXP Security- Introduction



Did You Know?

>10

Vehicle hacks
published since 2015

1.4 M

Vehicle recalled
in the largest
incident to date



Why hacking?

Valuable Data
attracts hackers

Car-generated data may
become a USD 750 B
market by 2030



Why is it possible?

High System Complexity
implies high vulnerability

Up to 150 ECUs per car,
up to 200 M lines of
software code



Why now?

Wireless Interfaces
enable scalable attacks

250 M connected
vehicles on the
road in 2020



Why does it affect?

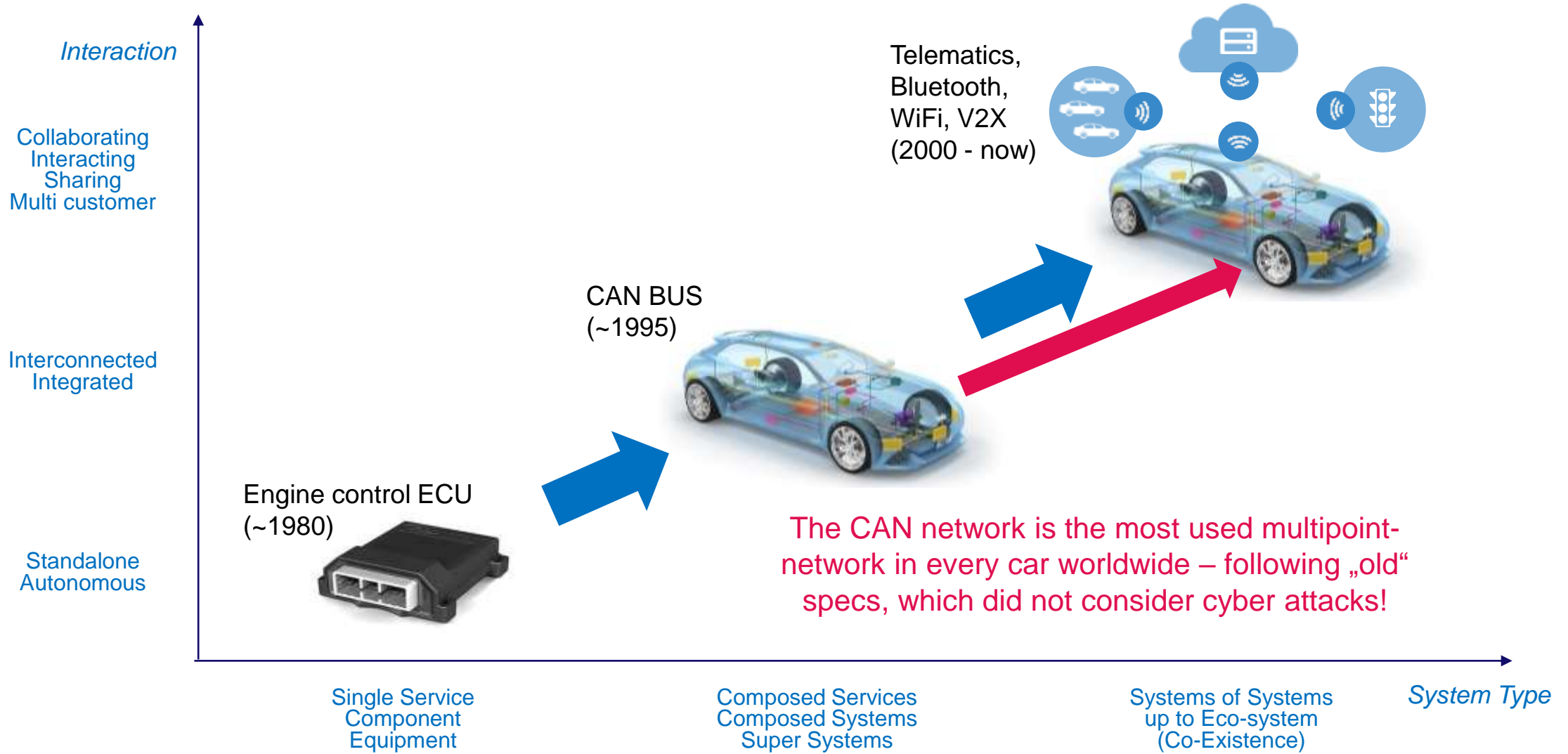
Abusing ingenuous ECU
forces unintended behavior

Immediate intrusion
prevention is hard to
guarantee

CAN-LEVEL SECURITY IS AN INSURANCE AGAINST INTRUSION

Note: Most reported security incidents are safety critical due to capability to control the targeted ECU.

Vehicle Electronics & Connectivity



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



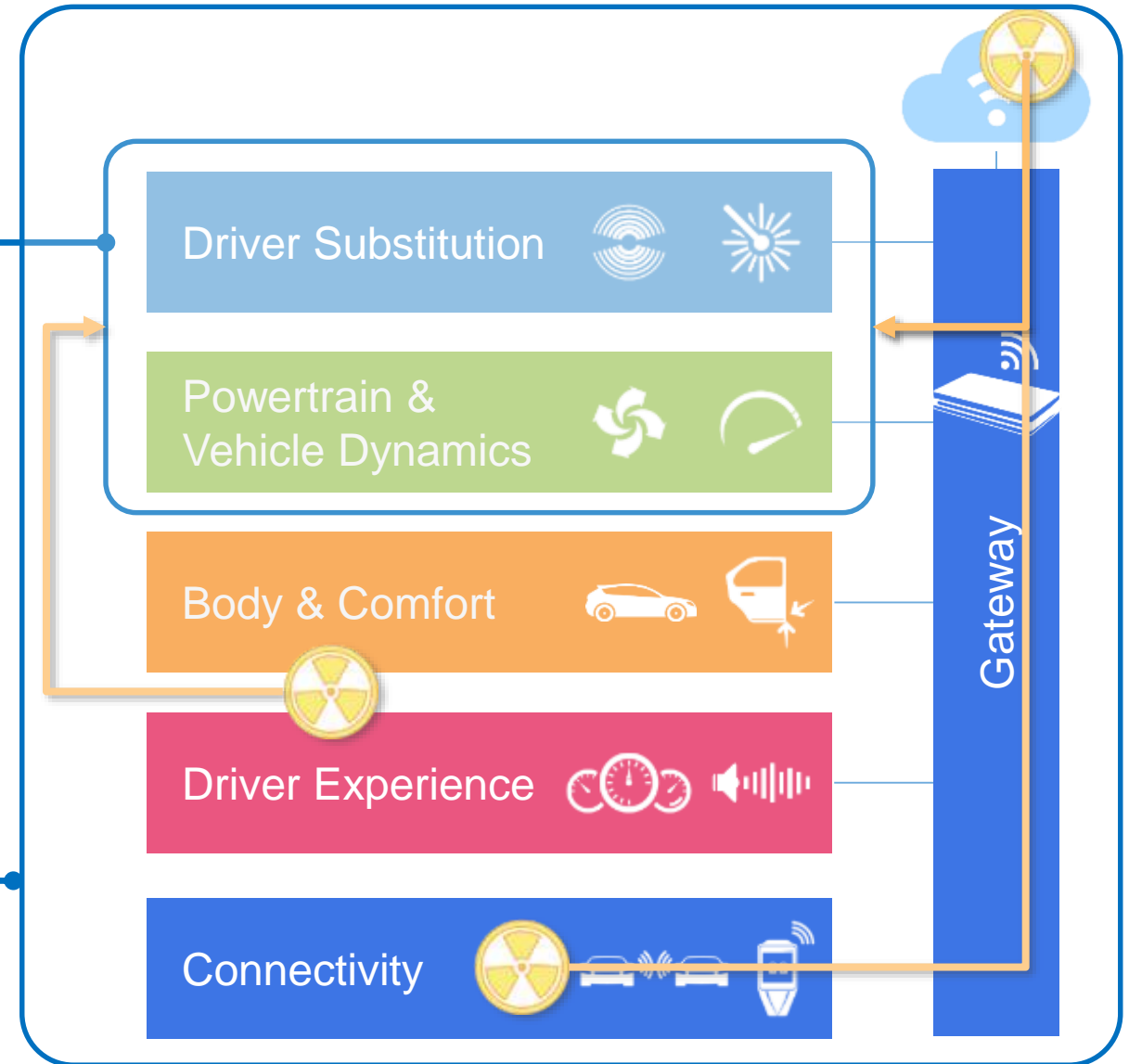
Collaterals:

System availability ensured

Information received / processed trustworthy



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



Functional Safety & Security – System-Level Concerns

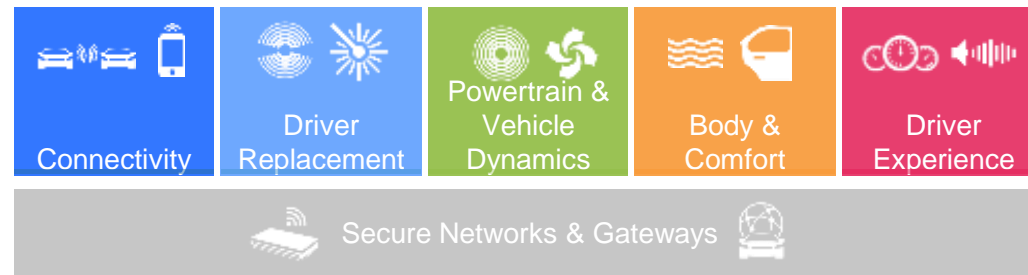
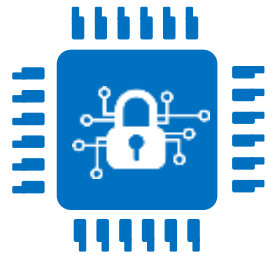
CHIP-LEVEL SAFETY & SECURITY SOLUTIONS



SAFE & SECURE DOMAIN ARCHITECTURES



SAFE AND SECURE MOBILITY



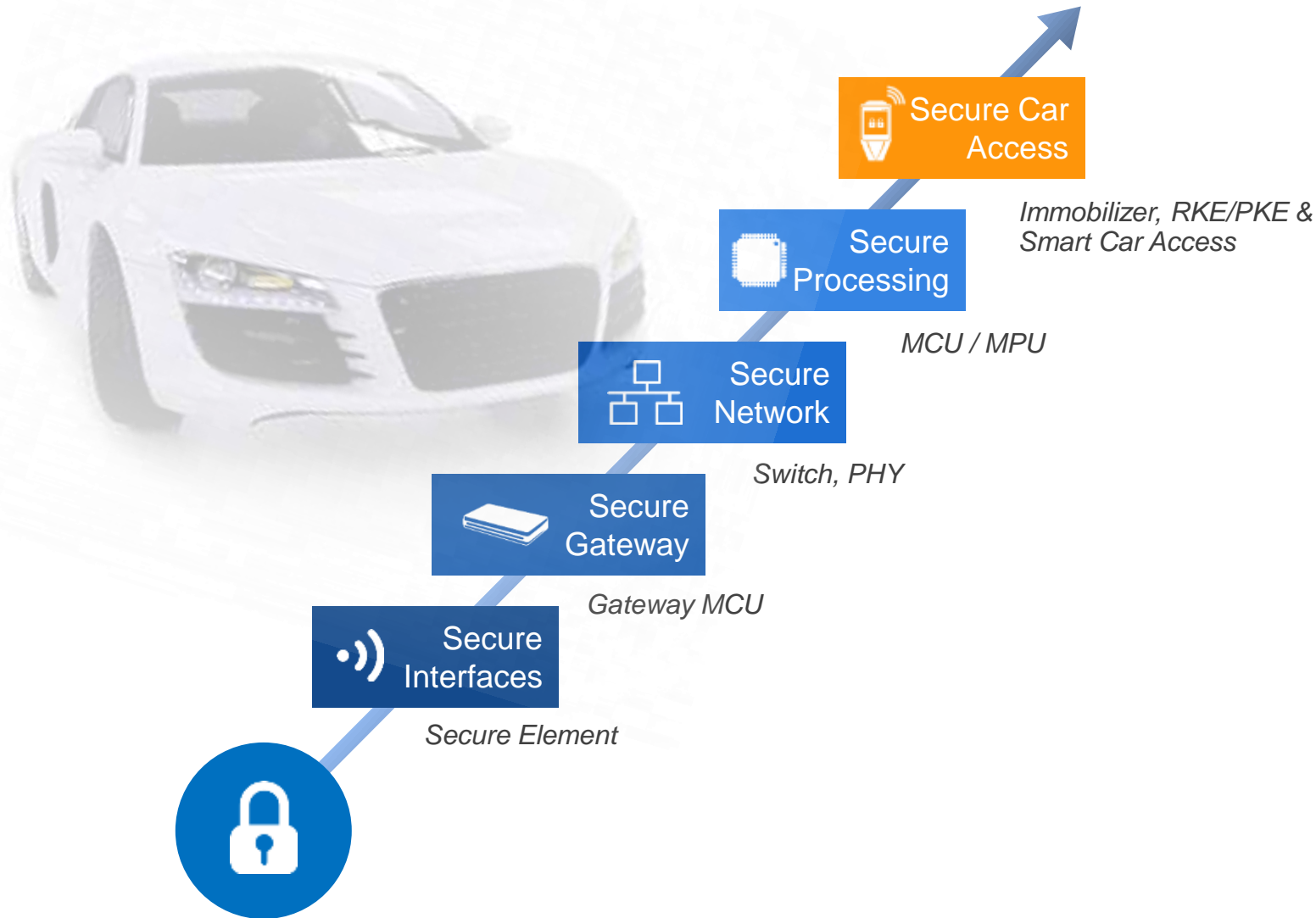
- Resource Isolation
- On-Die Monitoring
- Integrity & Authenticity Checks
- ...

- Domain Isolation
- Firewalls
- Network Intrusion Detection
- ...

- Fail Operational
- Resilient against Cyber Attacks

NXP's 4+1 Automotive Security Framework

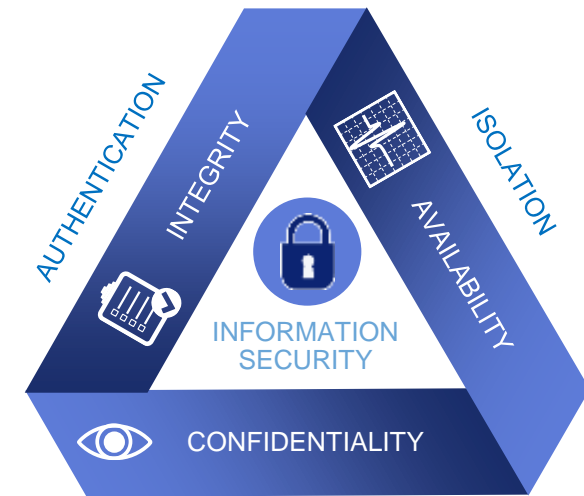
Complete product portfolio, enabling our customers to implement the core security principles



NXP #1 in Auto HW Security





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

Plus 'Best In Class' Car Access Systems



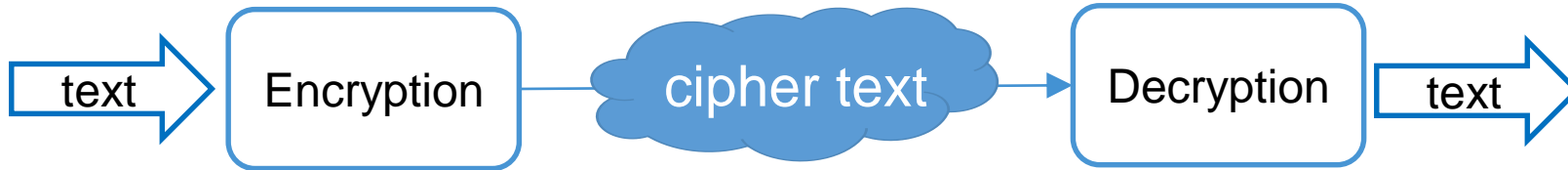
ENCRYPTION,
ACCESS CONTROL

Applying The Core Security Principles

		Prevent access	Detect attacks	Reduce impact	Fix vulnerabilities
Secure Interfaces		M2M Authentication & Firewalling			
Secure Gateway		Firewalling (context-aware message filtering)	Intrusion Detection Systems (IDS)	Separated Functional Domains	Secure OTA Updates (firmware, policies, ...)
Secure Networks		Secure Messaging (e.g. SecOC)	Focus of Secure CAN Transceiver		Message Filtering & Rate Limitation
Secure Processing		Code / Data Authentication (@ start-up)	Code / Data Authentication (@ run-time)	Resource Control (virtualization)	

Encryption is not Authentication

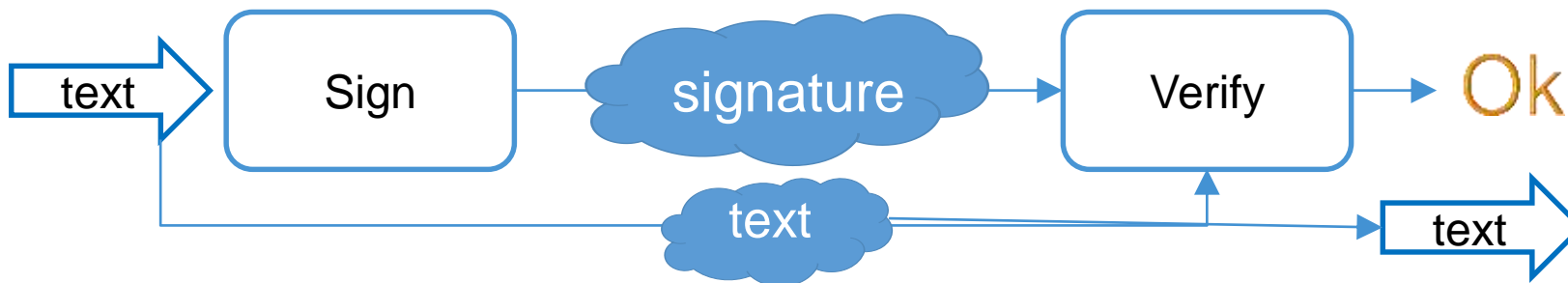
Encryption



Only the receiver can see the text in the clear

- Encryption supports confidentiality
 - Based on shared secret
 - Apply a reversible transformation
 - Result of transformation is not interpretable (cipher text)

Authentication



Receiver can determine identity of the sender,
make sure the text wasn't changed

- Authentication identifies the sender
 - Based on signature of plain text
 - Prevent Spoofing
 - Prevent Tampering

CAN Network Security - Hurdles Faced During Implementation



Secure Keys

- Key Management...
 - too complex to deploy and manage?
 - to be maintained over the lifetime of the vehicle!

Start Up

- Time to first (secure) message is too long after ignition/start (Not meeting realtime requirements).

Software

- Additional and complex Software.
- Impossible software changes due to cost or development and module (re-)validation & timing

Processing

- Software based authentication process for secure CAN communication applies for every secure CAN message at any time (processing burden).

Bandwidth/ Transmission

- CAN network bandwidth is already tight
- Unaffordable extra transmission/processing delay by security needs

TJA115X HELPS TO SOLVE THOSE PROBLEMS IN AN ACCEPTABLE WAY

NXP Secure CAN Transceiver “TJA115x”

Intrusion Containment System

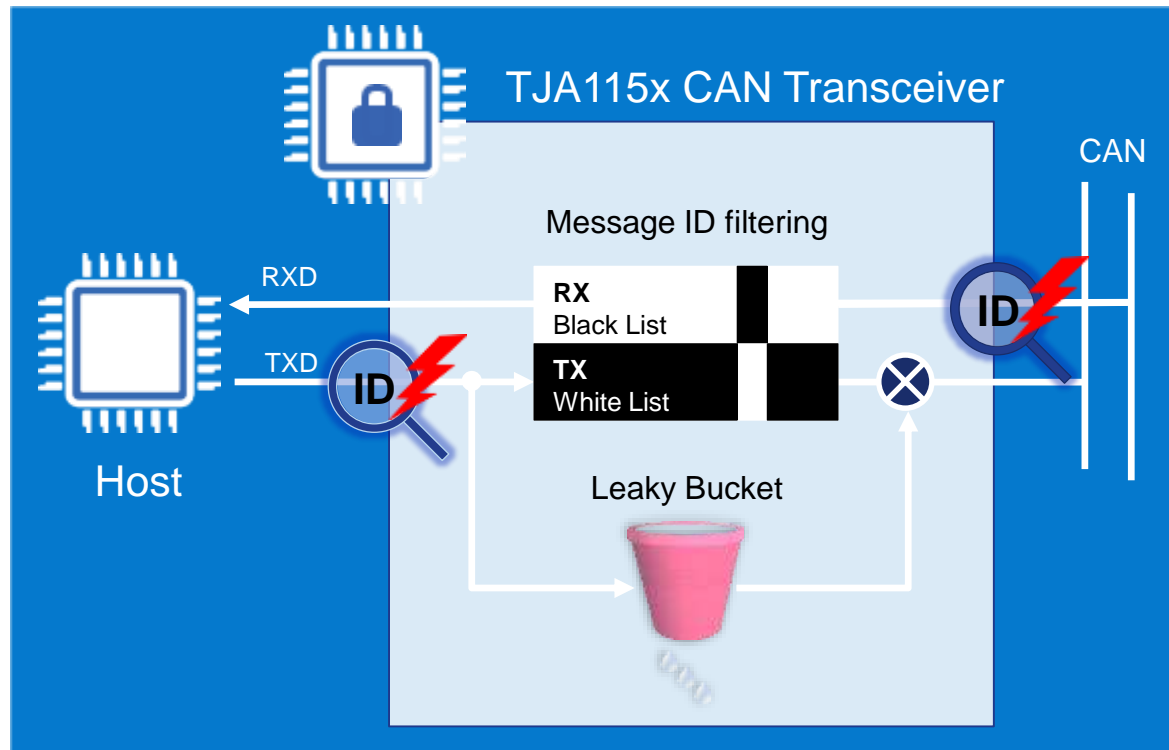
CAN supervisor protecting

- Own messages and
- Own bus behavior



Protecting & helping
the target of a hack

Assures legitimate senders
without cryptography



- **Intrusion detection & prevention (IDS / IPS)**
 - On-the-fly CAN ID filtering (TX) and bus-guarding (RX) based on user configurable white & black list, preventing Spoofing & Tampering
 - Reporting & Logging support
- **Flooding prevention (DoS)**
 - Threshold on message transmission: leaky bucket strategy weighted on frame size
- **Simple CAN transceiver replacement**
 - No Software - purely hardware based solution.
 - In-field reconfiguration possible

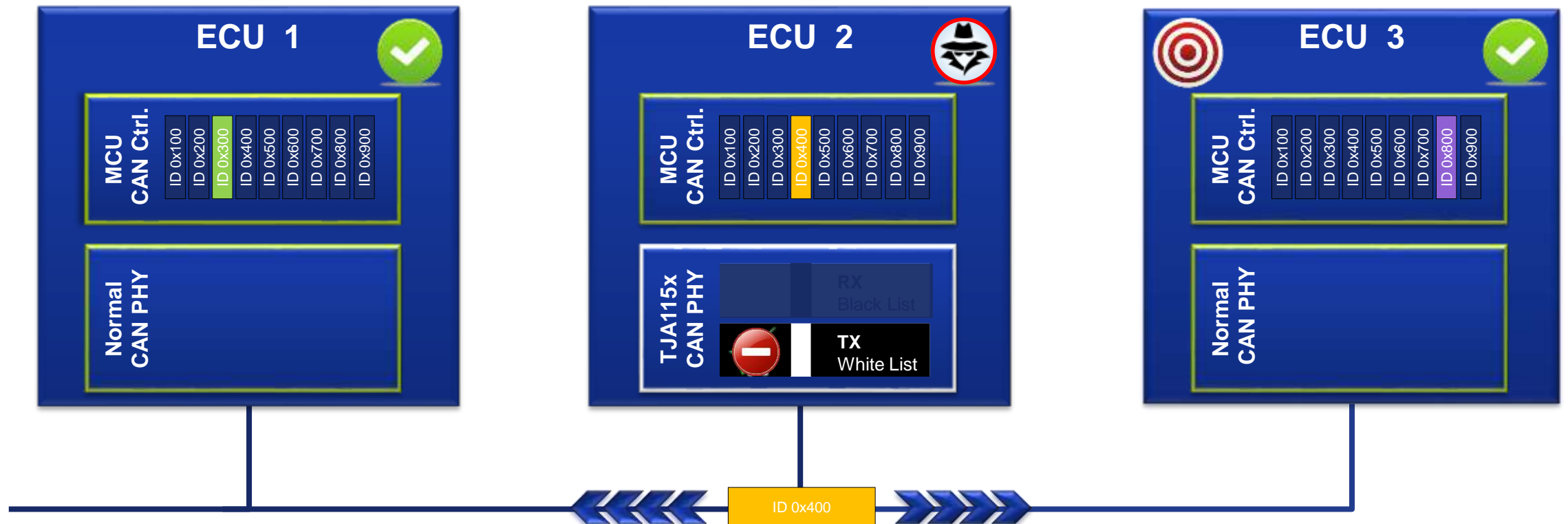
Spoofing Detection & Prevention

Security Value of TJA115x



TJA115x - Spoofing Prevention – Transmit Path

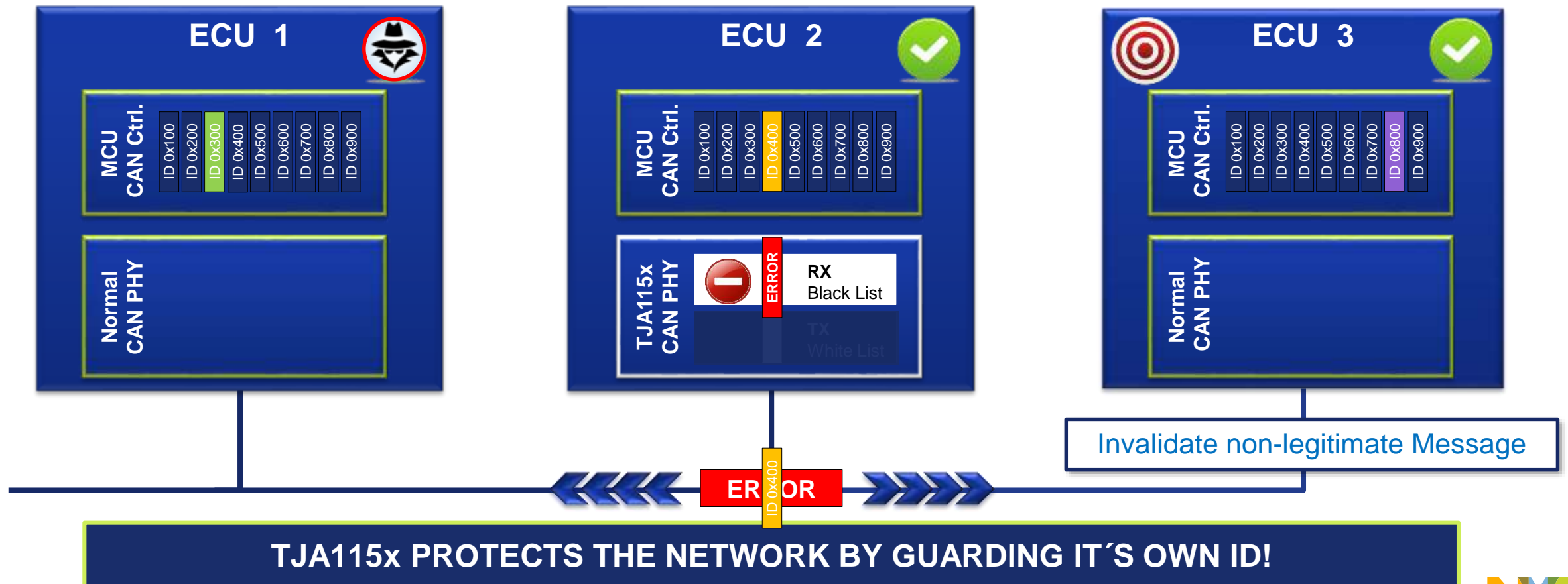
- ECU 2 gets compromised and pretends to be another ECU (Spoofing)
- Only messages with ECU 2 legitimate ID **ID 0x400** can pass the TJA115x hardware filter!
- TJA115x TX Whitelist stops transmission of any non-legitimate ID from ECU 2



TJA115x PROTECTS THE NETWORK AGAINST SENDING NON-LEGITIMATE ID'S!

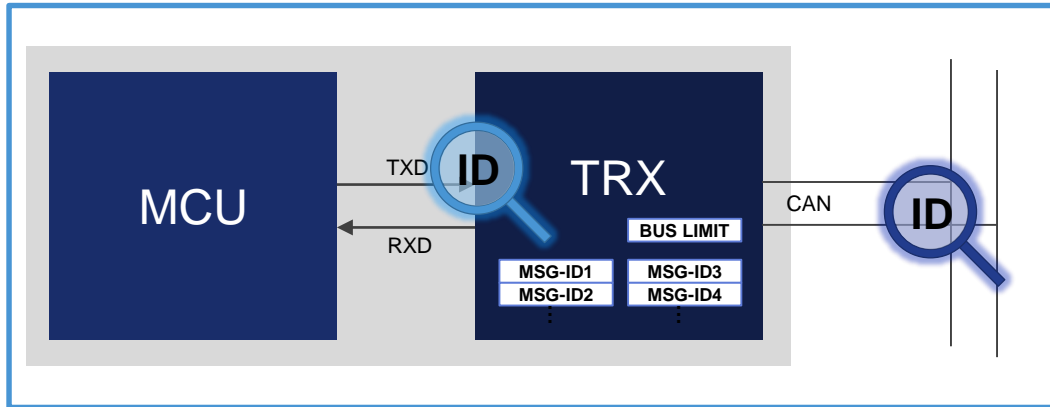
TJA115x - Spoofing Prevention – Receive Path

- 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 Offers HW-Based Spoofing Protection

- TJA115x is a simple transceiver replacement for CAN and FD networks to immediately contain the effects of spoofing attacks, based on on-the-fly ID monitoring and real-time action.



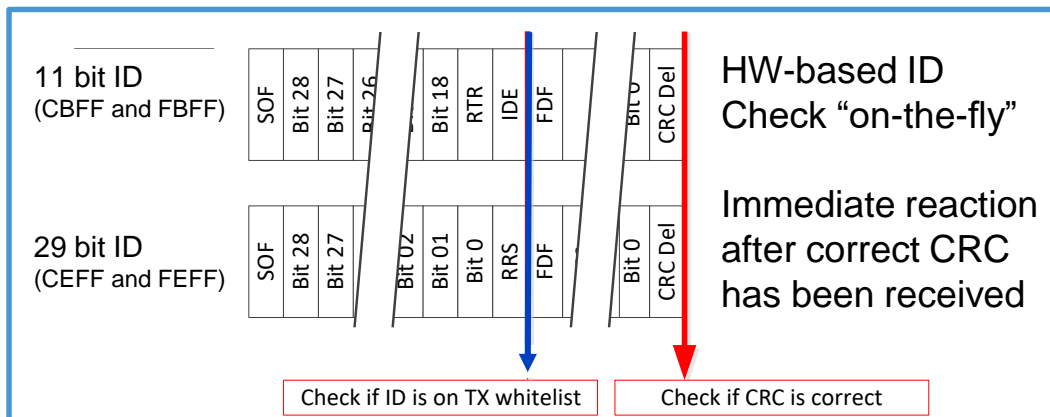
ID White-listing on TXD from MCU

TJA115x checks frames ID on TXD from Host MCU
 If ID is not in white-list, frame invalidated with ERROR frame
Effect Host MCU cannot “spoof” another ECU
Effect Host MCU cannot trigger unwanted diagnosis session



ID Monitor on CAN bus via RXD

TJA115x checks on-the-fly ID of frames on the bus
 If TJA115x finds ID match with its blacklist & ID is flagged to be monitored, frame is invalidated with ERROR frame.
Effect “Polices” other ECUs that “spoof” this ECU



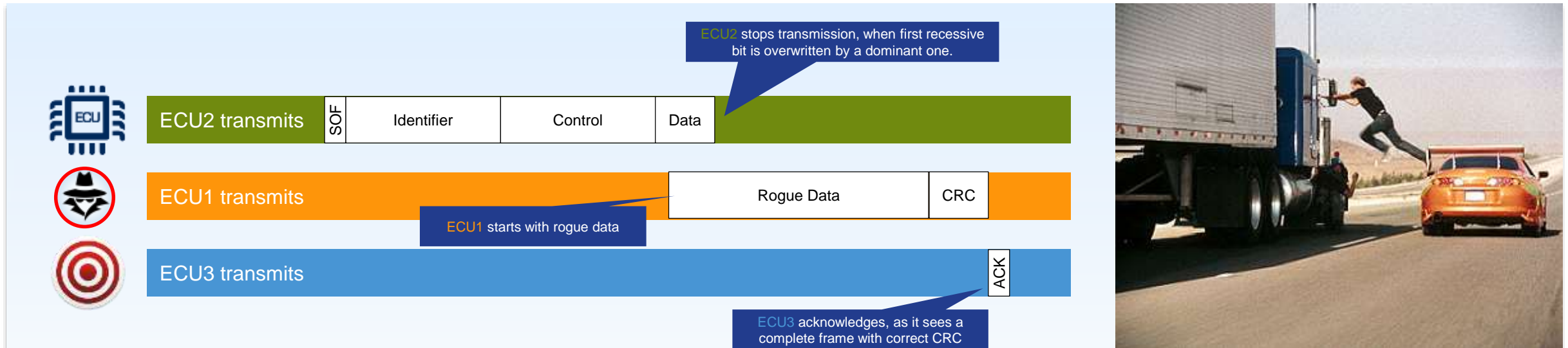
Temper Protection

Security Value of TJA115x



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.



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

Messages:

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

ERROR PASSIVE:

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

16 additional attempts

- of the legitimate ECU sending it's message – without reporting ERRORS when encountered!
- Bit flip ERRORS not reported!

BUS OFF:

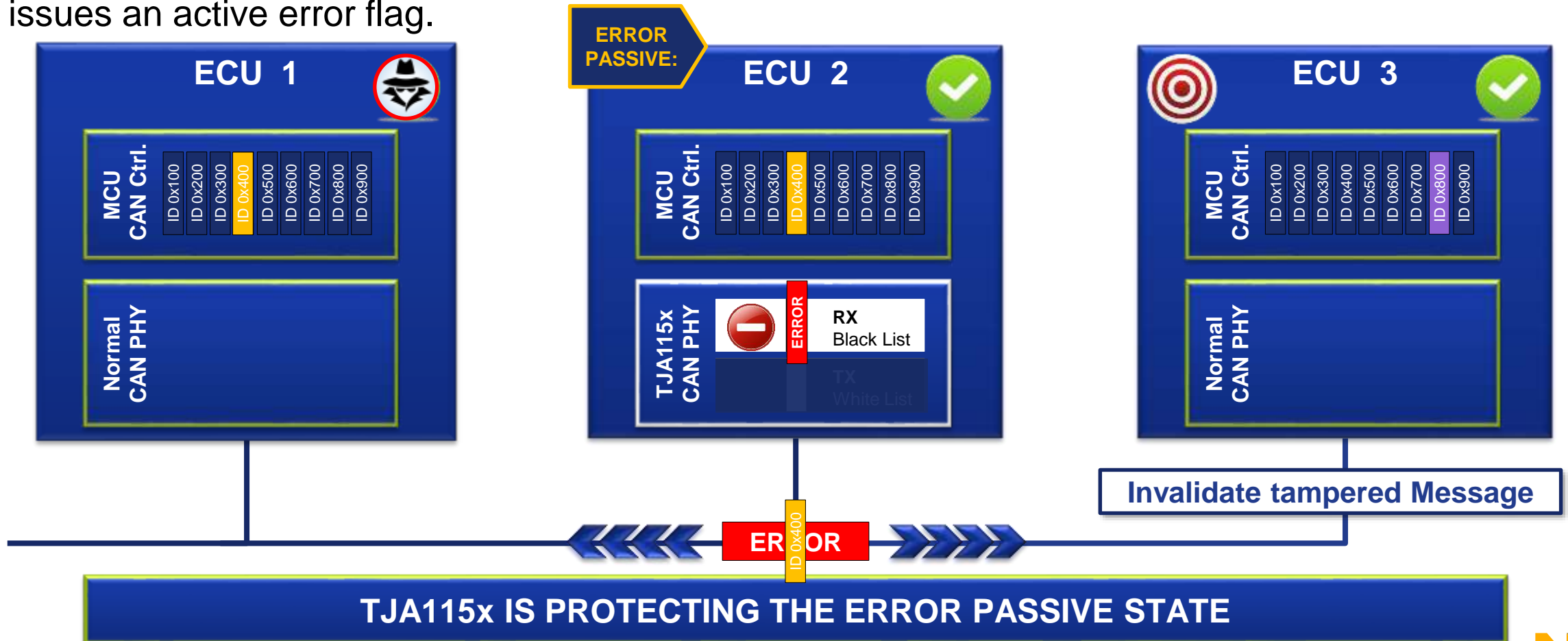
Do not send messages anymore

- No Messages send anymore by legitimate sender
- Denial of Service

→ GAP FOR SUCCESSFUL TAMPER / SPOOFING ATTACK

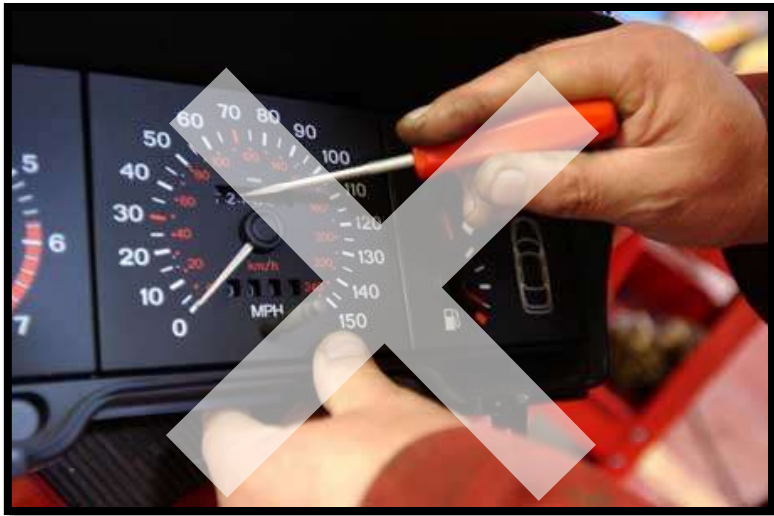
TJA115x – Tamper Protection

- 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 that identifier was send and CRC received (Direction Change) and issues an active error flag.



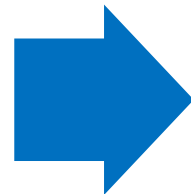
TJA115x Offers Tamper Protection

- TJA115x is a simple transceiver replacement for CAN and CAN FD networks - containing tampering attacks during ERROR passive state



Tamper Protection

- TJA115x detects the situation where the local node stops transmitting a message which continues on the bus.
- When message is completed by a remote node including a correct CRC, then TJA115x issues an active error flag.
- TJA115x will not send an error flag in case the message includes an incorrect CRC (Avoid unnecessary busload)



Remote Host MCU cannot spoof by tampering the payload (incl CRC) of a correctly initiated message (i.e. part of TX whitelist).

Prevention & Denial Service/Flooding

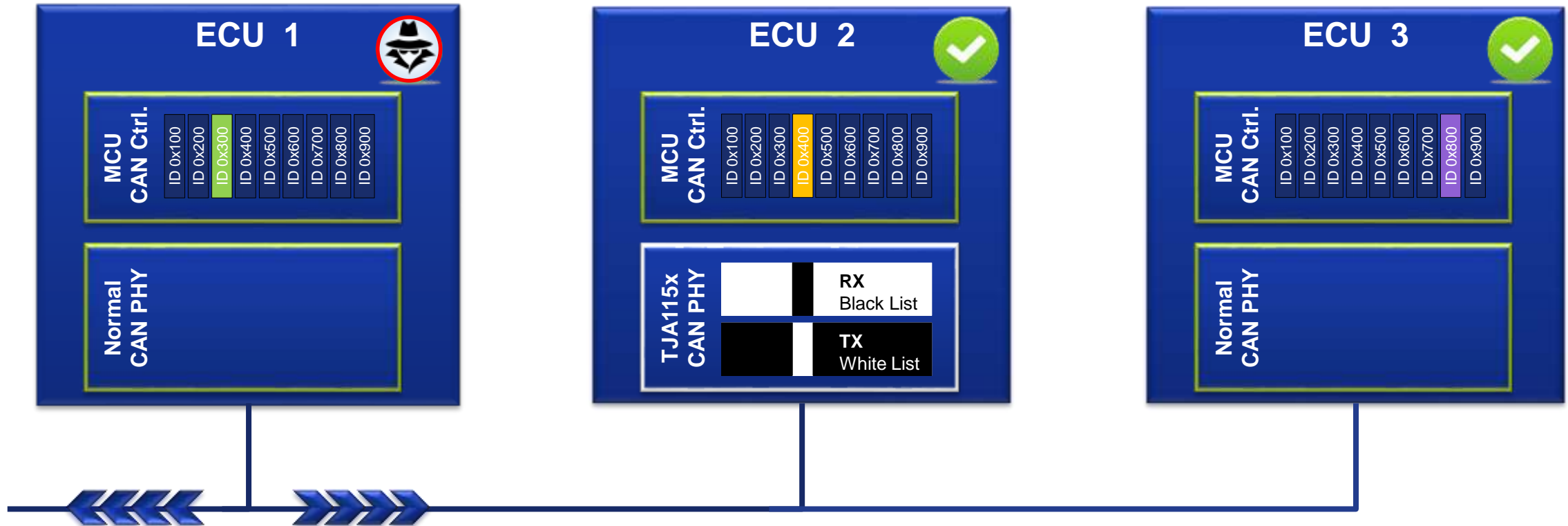
Security Value of TJA115x



Use Case: A Successful Attack..... Flooding

- ECU 1 gets compromised

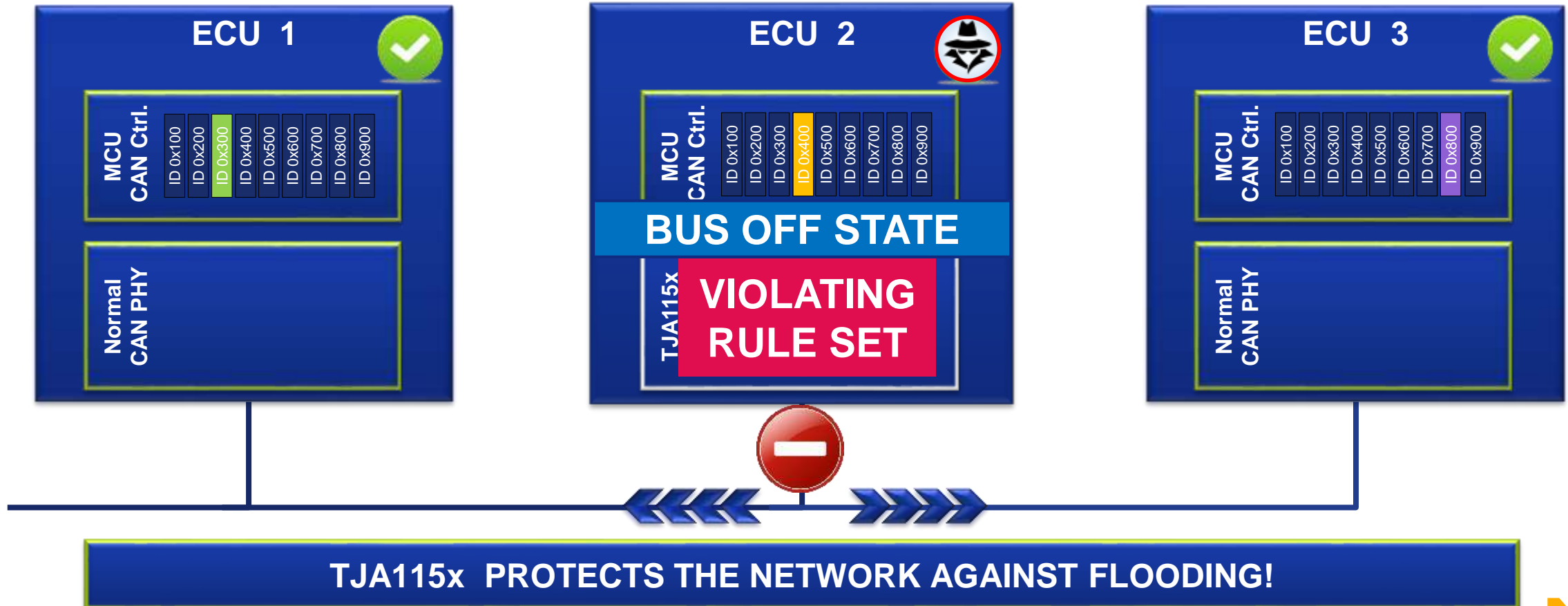
ECU 1 has now full access to the bus.



ECU 1 is flooding the bus – Bus killed - DENIAL OF SERVICE

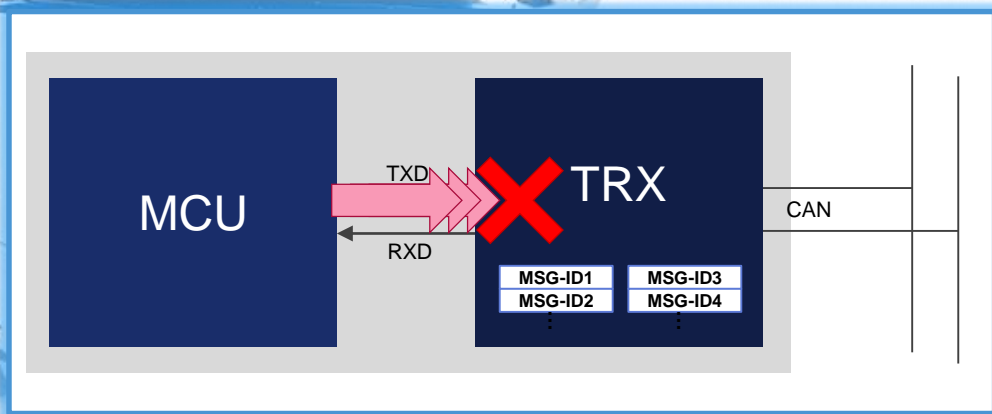
TJA115x - Flooding Prevention

- 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 Offers Flooding Prevention

- TJA115x is a simple transceiver replacement for CAN and CAN FD networks - containing impacts of denial-of-service attacks to ensure sufficient network availability.



Flooding Prevention

- TJA115x implements a “leaky bucket” and adds weighted value for every transmission, reflecting frame length.
- Beyond a specified bus load, TJA115x moves into “Secure Mode”
- Effect Host MCU cannot flood bus to disrupt communications

Secure Mode

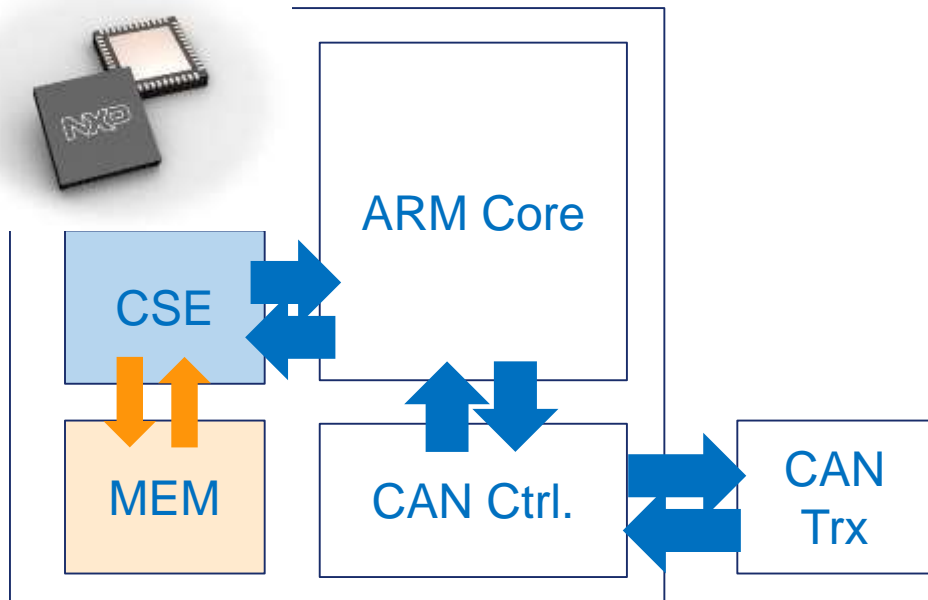
- TXD disabled (HIGH), RXD LOW, blocking host CAN controller
- TJA115x “recovers” after 2s, RXD released, TXD re-connected (only when TXD is internally pulled HIGH to avoid glitches)

How TJA115x Helps

Security Value of TJA115x



Application Secure MCU + CAN Transceiver

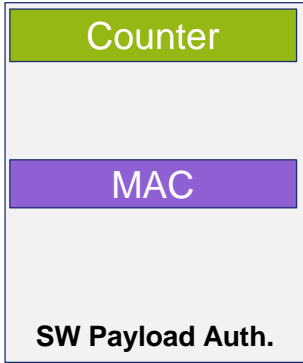


Authentication:

- Keys required for local communication and E2E beyond other ECU's
- Key storage in secured flash
 - Max 17 (new 20 for some low end MCUs)
 - Extension with SW to external embedded flash possible but complex and requires extra SW & CPU processing.
- MAC-ing requires extra CPU cycle (Processing delay)
- Adding bytes to payload resulting in higher busload and transmit delay
- **Method applies for every secure message every time.**
- Payload Authentication does not work with HS-CAN (due to data overhead).

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

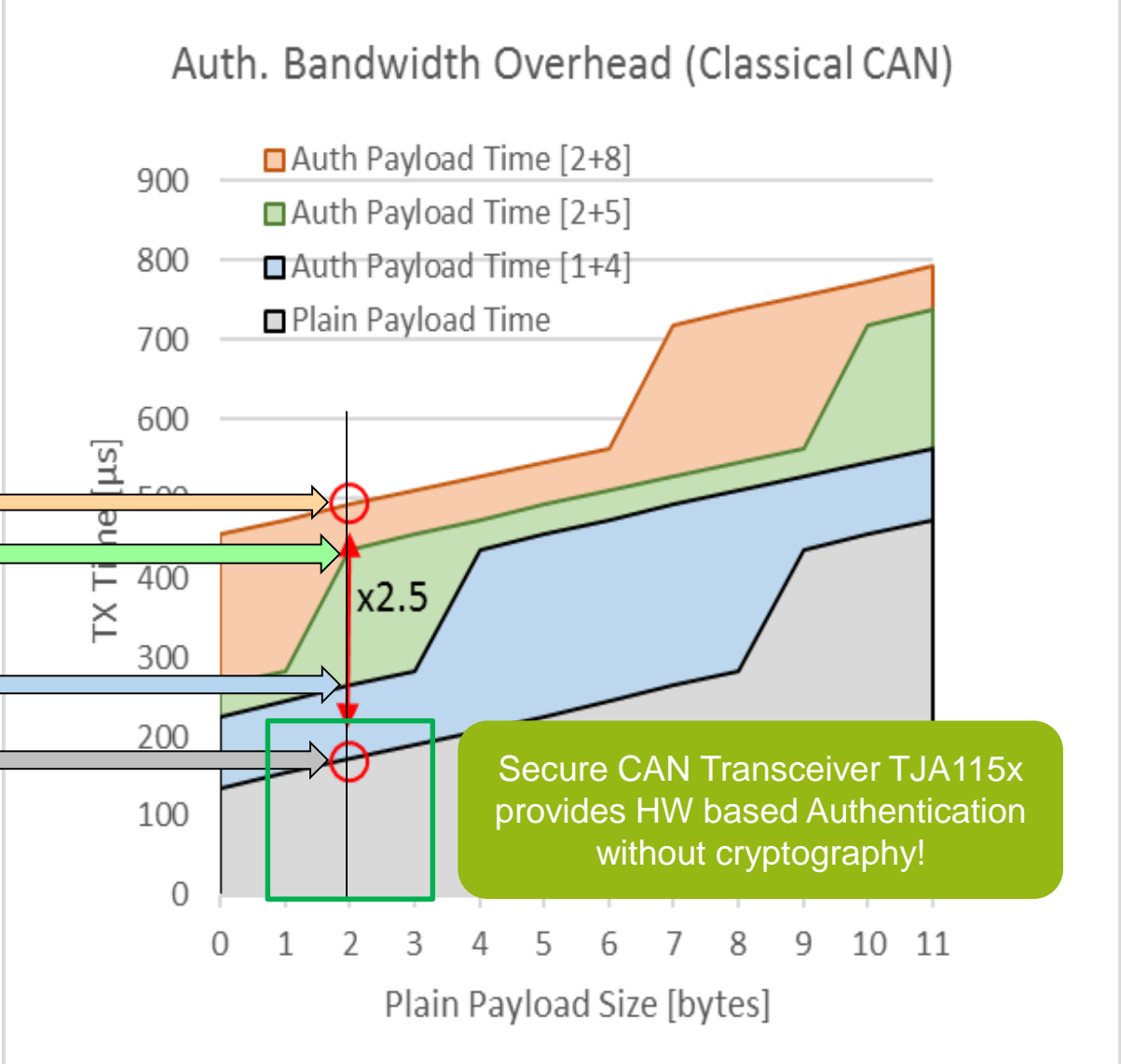
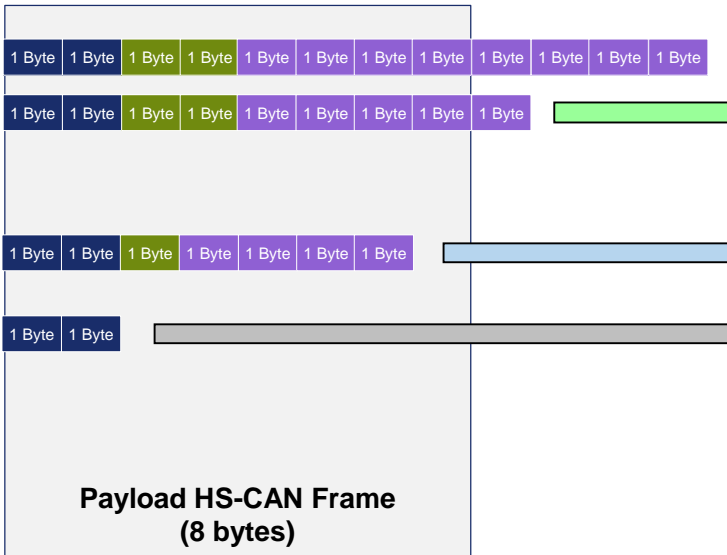
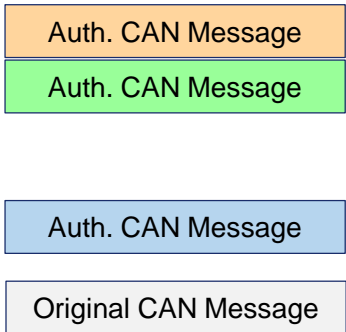
Message



- Original Message (example 2 Bytes)

- Increasing Busload - Delays transmission

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

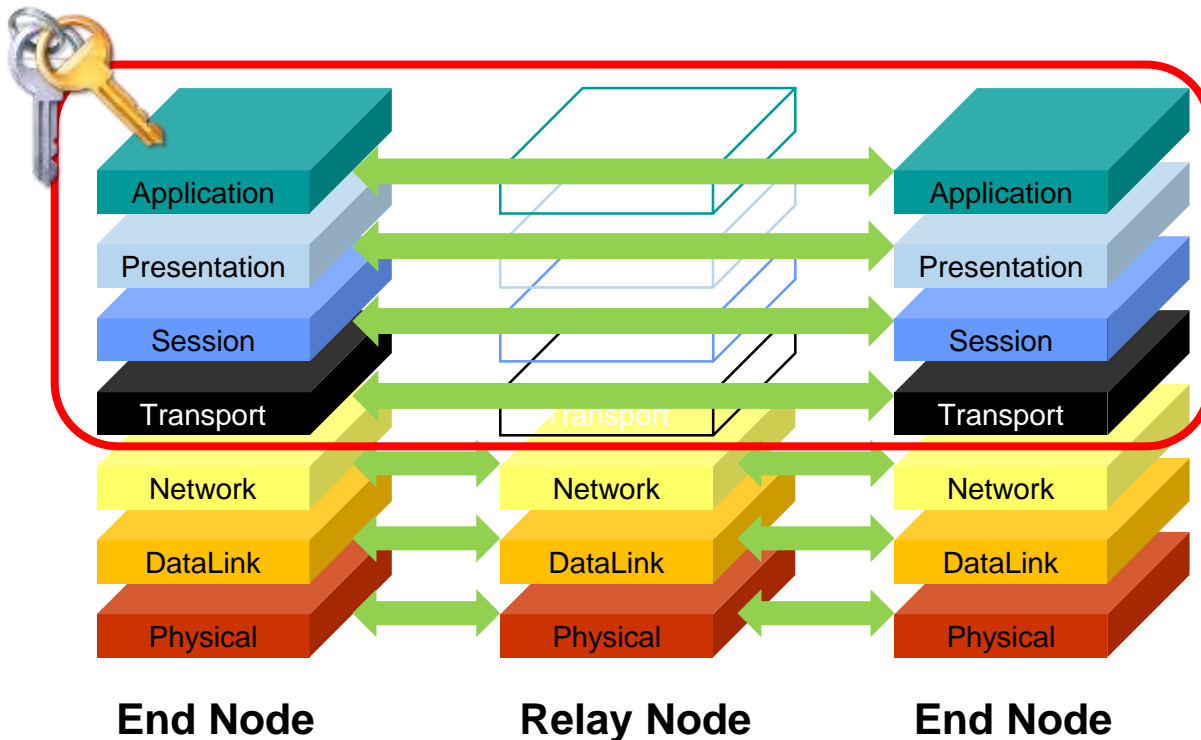


Secure Network Communication

End2End

- 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.

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



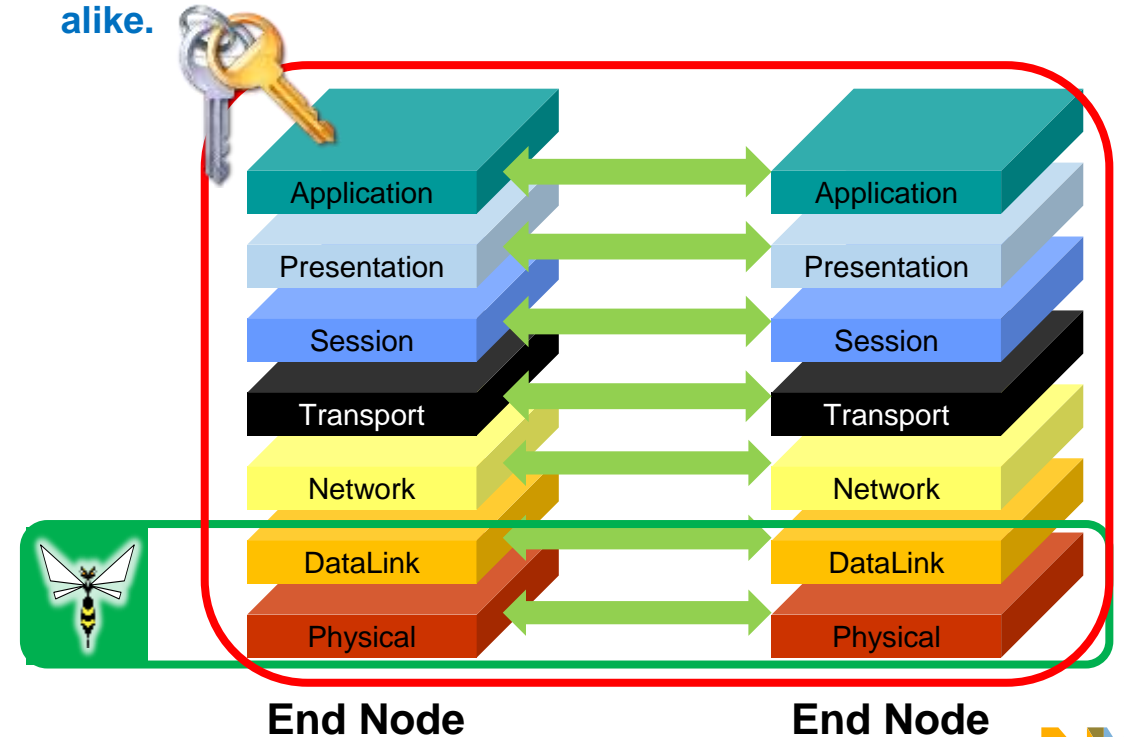
On local CAN bus

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

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

Efficient Solution without secure keys:

- Apply TJA115x on Physical/DataLink layer
- Achieve same level of protection like AUTOSAR SecOC or alike.



Typical Network Secured By Payload Authentication and Keys

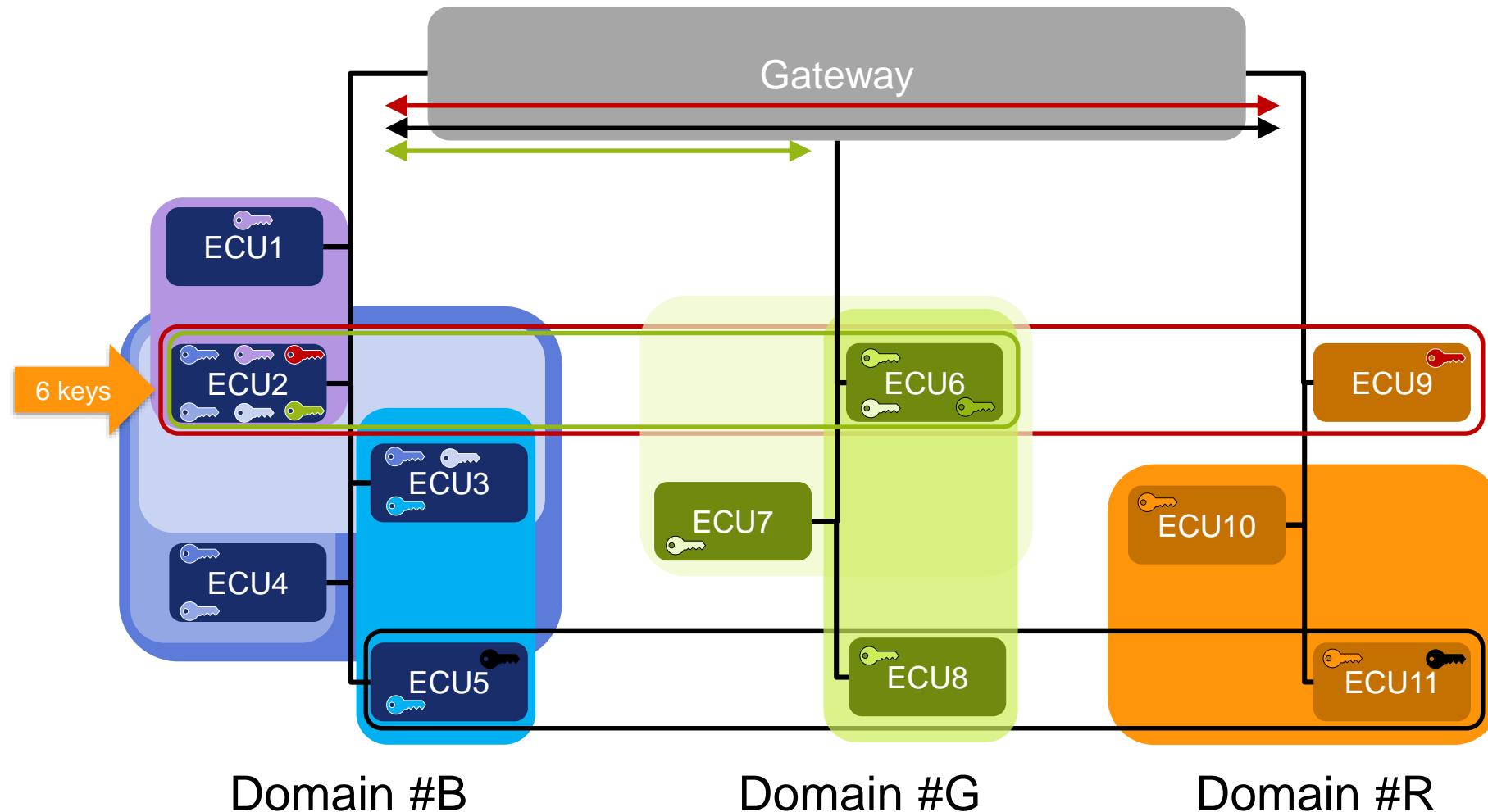
- 1 Gateway
- 3 Domains
- 11 ECUs
- Multiple local domain applications



- 3 cross domain / E2E applications



- Secured by keys
 - ECU #2 needs many keys



Local Communication Secured With TJA115x – Same Network

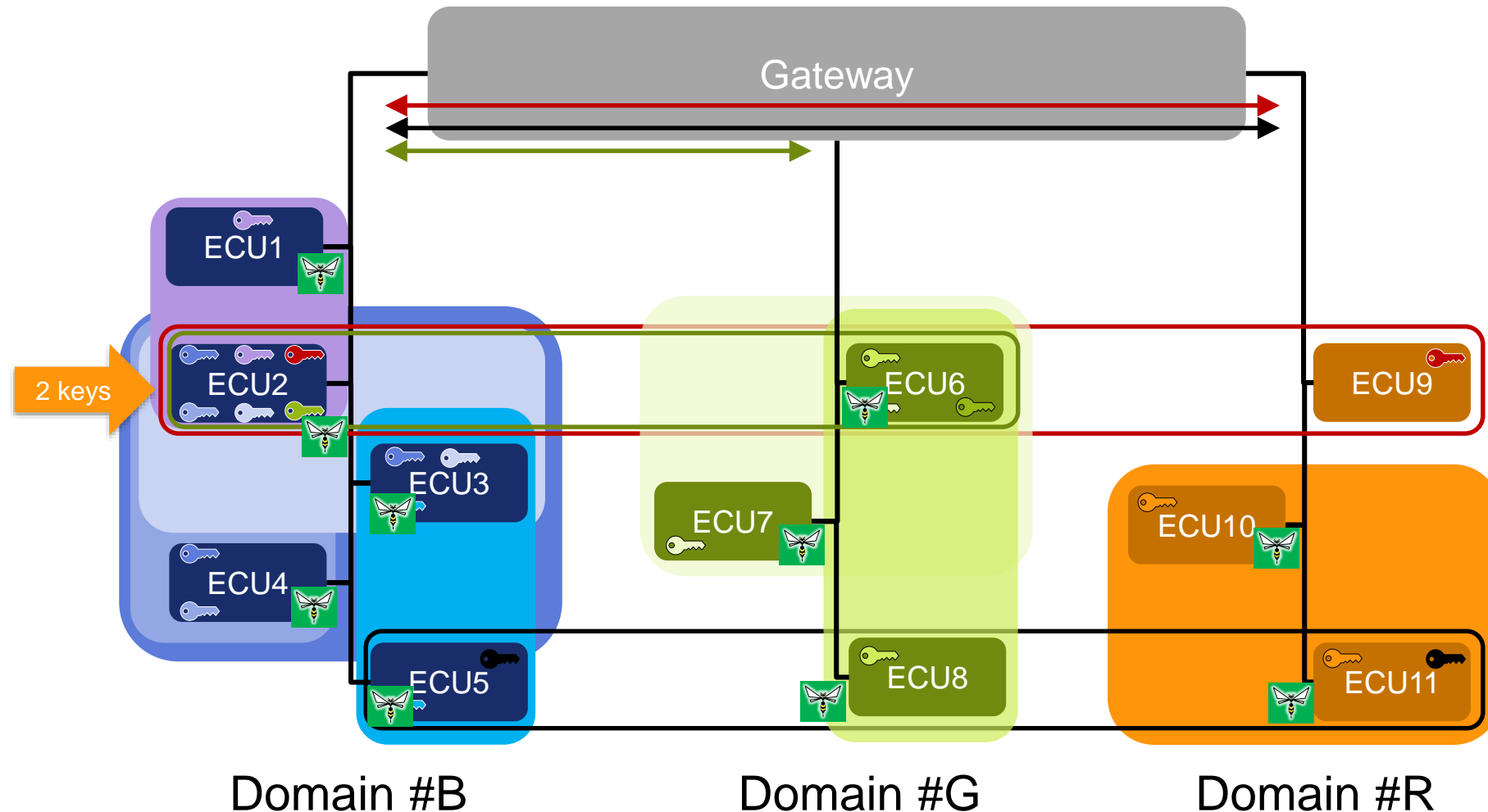
- 1 Gateway
- 3 Domains
- 11 ECUs
- Multiple local domain applications



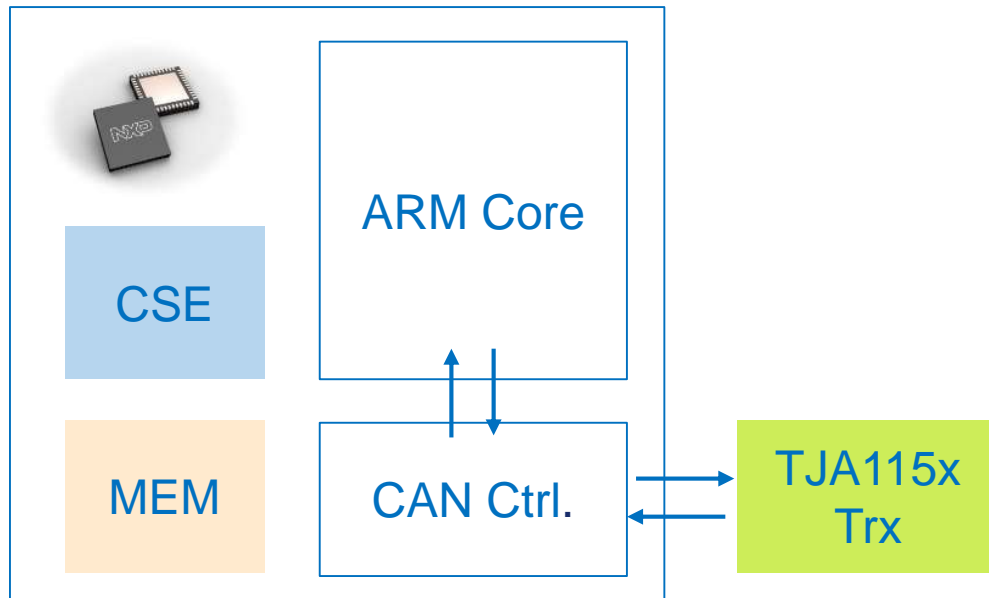
- 3 cross domain / E2E applications



- No keys for local application
– Less keys for ECU #2



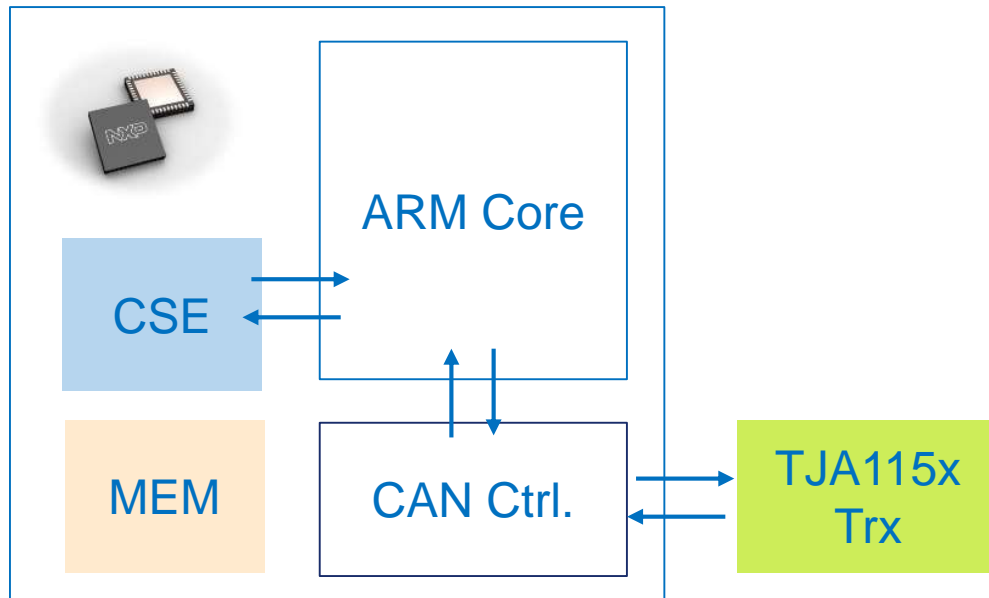
Application Secure MCU + Secure CAN Transceiver TJA115x



TJA115x secures local BUS communication:

- No MAC-ing for local CAN communication required!
 - No keys!
 - No extra CPU cycles, no delay
- **Full performance for application available!**
- No data added for local CAN communication
 - No busload/bandwidth overhead!
 - Real time capable, No transmit delay
- On-the-fly bus monitoring and real time action at security incident (Spoofing, Tampering)

Application Secure MCU + Secure CAN Transceiver TJA115x



TJA115x secures local BUS communication:

- No MAC-ing for local CAN communication required!
 - No keys!
 - No extra CPU cycles, no delay
- **Full performance for application available!**
- No data added for local CAN communication
 - No busload/bandwidth overhead!
 - Realtime capable, No transmit delay
- On-the-fly busmonitoring and realtime action at security incident (Spoofing, Tampering)

HW & SW based mixed Authentication:

- Keys required **only** for E2E beyond other ECU's
 - Can save several keys → Key storage of current CSE most likely sufficient.
 - Extension with SW to external embedded flash not necessary → Saving SW & CPU cycles

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 local 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 every 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

Systemplay with Secure MCU

Secure CAN Transceiver TJA115x helps the Secure-MCU

- Trust incoming messages without cryptography for local CAN communication
- Send messages legitimated by TJA115x
- Reduce (symmetric) key management for CAN level communication.

Remaining duties for Secure-MCU:

- Secure end-to-end communications (encryption/decryption required)
- Hardware security for key storage
- Secure boot
- Secure protocols
- Secure firmware update
- Authenticated diagnostic
- Secure gateway routing

Threat	Security Property	TJA115x	SMCU		Secure MCU + TJA115x
		Classical CAN CAN FD	Classical CAN	CAN FD	Classical CAN CAN FD
Spoofting	Authentication	Green	Orange	Orange	Secure μ C + TJA115x
Tampering	Integrity	Green	Orange	Orange	
Repudiation	Non-repudiation	Red	Green	Green	
Information disclosure	Confidentiality	Red	Green	Green	
Denial of service	Availability	Green	Red	Red	
Elevation of privilege	Authorization	Orange	Green	Green	

Combination of secure μ C + TJA115x results in full coverage of efficient Defense-In-Depth!

Legend Cost/Benefit
No Support
Higher Impact
Moderate Impact
Least impact or unique option
Highest benefit with multiple layers of defense (DiD)

TJA115x enables, improves & simplifies secure CAN communication



Customer Value & Product



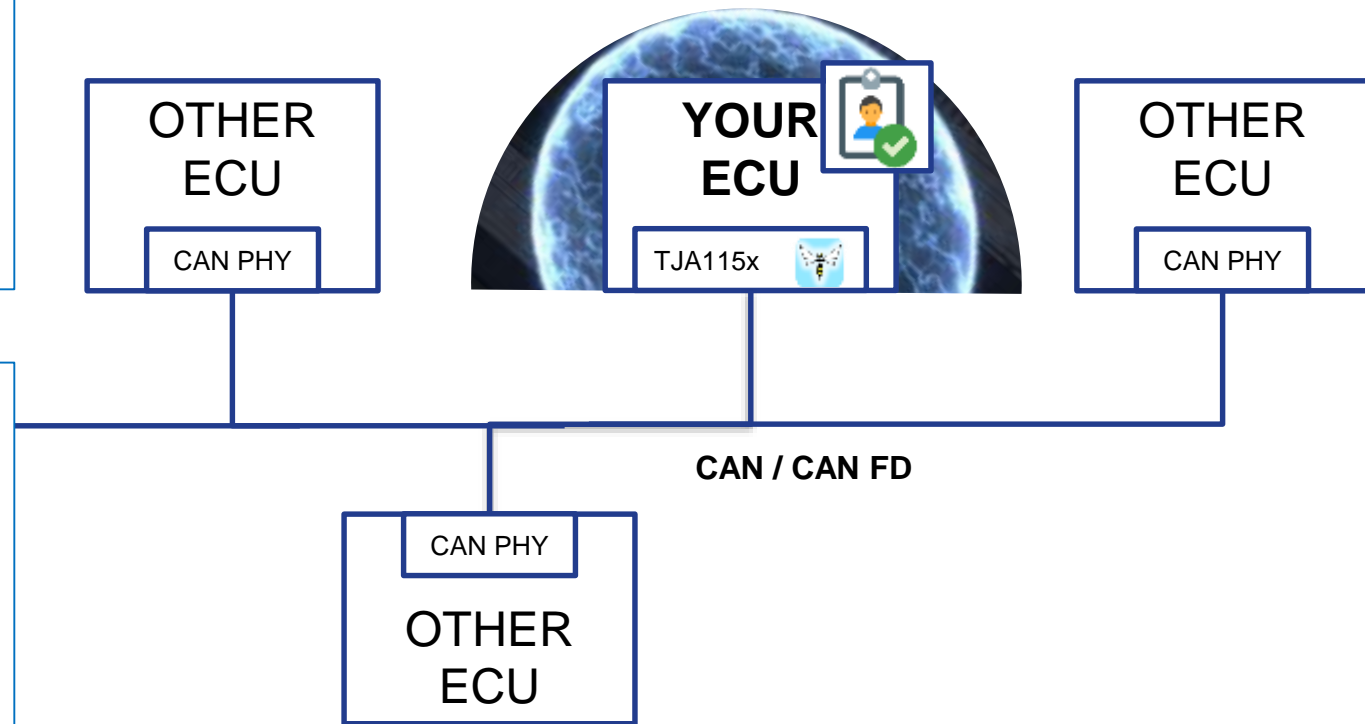
TJA115x Value For Tier1's – Avoid Liability Issues

Use TJA115x as Assurance:

- Assure by HW that YOUR ECU can only communicate within the boundaries of the module assigned ID's (OEM Spec).
- Even if YOUR ECU is compromised – TJA115x limits the maximum impact to the assigned ID's!
 - e.g. a radio remains to communicate as radio – can not act as anything else – proven by HW!

Use TJA115x as INSURANCE:

- Add proof point tool /building block
- YOUR ECU protects it's own ID in the connected CAN network.
- Even if any other module in the network is hacked - NO other ECU can pretend to be YOUR ECU (Taking control over your messages)!



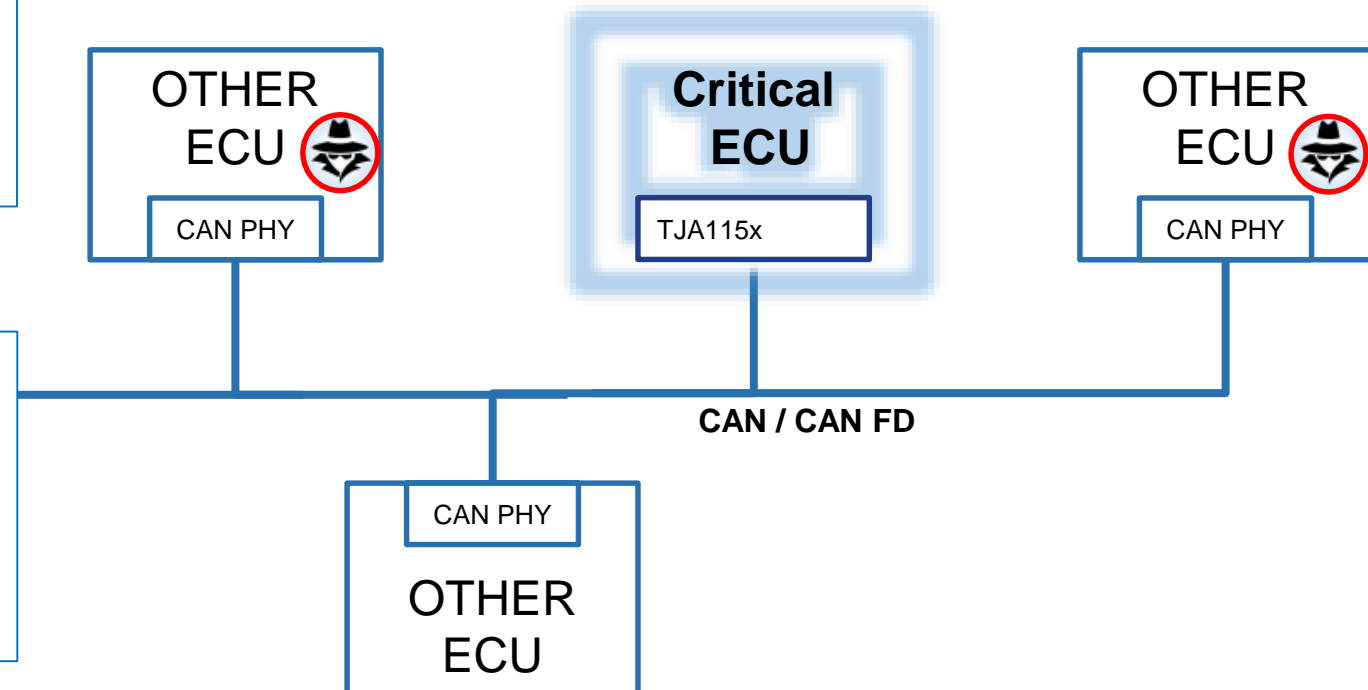
TJA115x Value For OEM – Constrain The Un-Defined

Use TJA115x to GUARD the specification:

- Ensure by the module specification that, at any time, the module (ECU) can only communicate within the boundaries of the module assigned ID's.
- Constrain any possibility by HW to leave these boundaries – even if compromised - Limiting hackers' playground area

Use TJA115x to protect critical messages:

- Ensure by HW that this critical ECU is the only ECU within the connected network which is able to send the defined critical messages
- Independent, how many and which other ECUs get directly connected on the CAN network.



**Define what the ECU is supposed to do (WoW of today)
→ Use HW to define (TJA115x) the undefined.**

Final Message

- No safety anymore without security
- Encryption is not authentication
- TJA115x is a HW replacement for existing CAN transceiver
- TJA115x Assures 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
- Think system for cybersecurity solution.



SECURE CONNECTIONS
FOR A SMARTER WORLD

www.nxp.com