Automotive CAN Networking How Innovation Will Keep it Relevant for Next-Generation Networks

Bastien Depp

Analog Field Application Engineer

PL IVN

November 2019

SECURE CONNECTIONS FOR A SMARTER WORLD

1993 – 2000

PCA82C250 – First Philips transceiver (shipped > 10 Mpcs in 2017)

SJA1000 – Standalone CAN controller (shipped > 3 Mpcs in 2017)

2000 – 2010

Gen-2 and Gen-3 launched

TJA1042, TJA1051 became standard in the market

HS-CAN becomes dominant automotive networking technology

2010 – 2020

CAN-FD and Ethernet rolling out

Mantis launched with benchmark EMC

Partial Networking defined and rolls out

Node explosion, increased competition

NXP acknowledged market leader

NXP leads on

Innovation, support, reliability and expertise

Portfolio, “no-hassle” quality and supply

Agenda

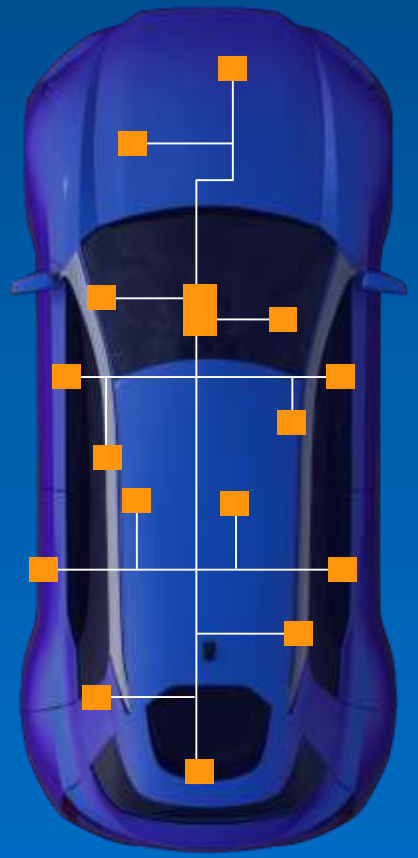
- CAN networks in transformation
- CAN innovation by NXP
  - TJA146x: CAN with signal improvement
  - Future outlook : CAN-XL
  - TJA115x: CAN security without cryptography

CAR NETWORKS IN TRANSFORMATION

towards self-driving and user-defined vehicle

CAR NETWORKS IN TRANSFORMATION

TODAY: FLAT

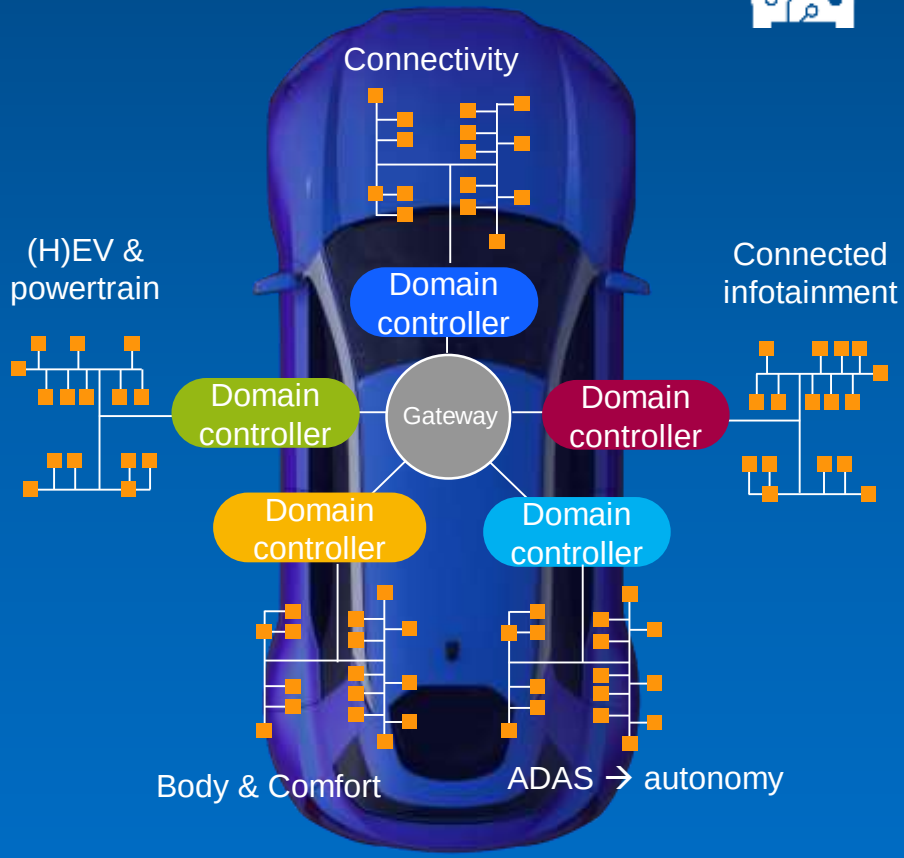


- Low bandwidth, flat and open network
- One application per module

Unfit to future mobility

Flat to hierarchical

TOMORROW: DOMAINS

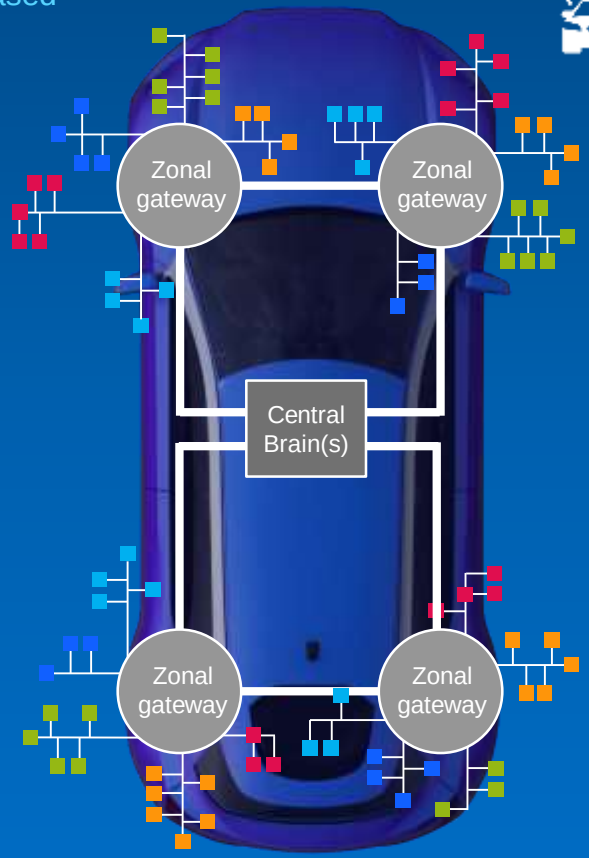


- Multi-apps aggregated in big processors
- Gateway handles cross-domain high speed traffic

To autonomous car

Signal-based to service-based

AFTER TOMORROW: ZONES

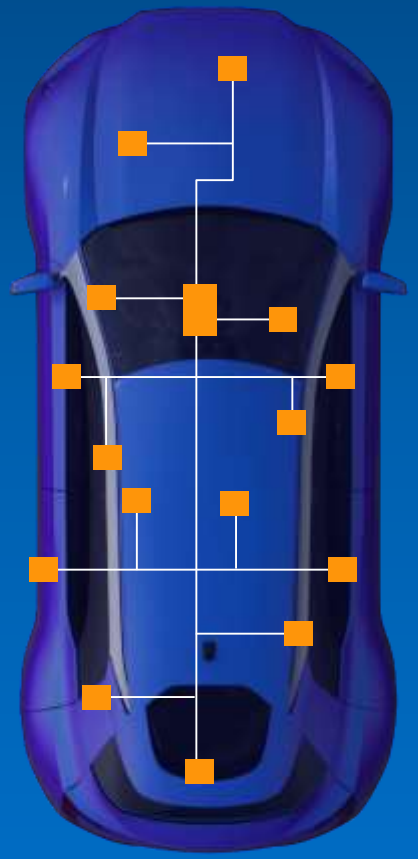


- Domains virtualized by SW – enabling high flexibility
- Easy enable/disable or update functions

To user-defined car

CAR NETWORKS IN TRANSFORMATION

TODAY: FLAT



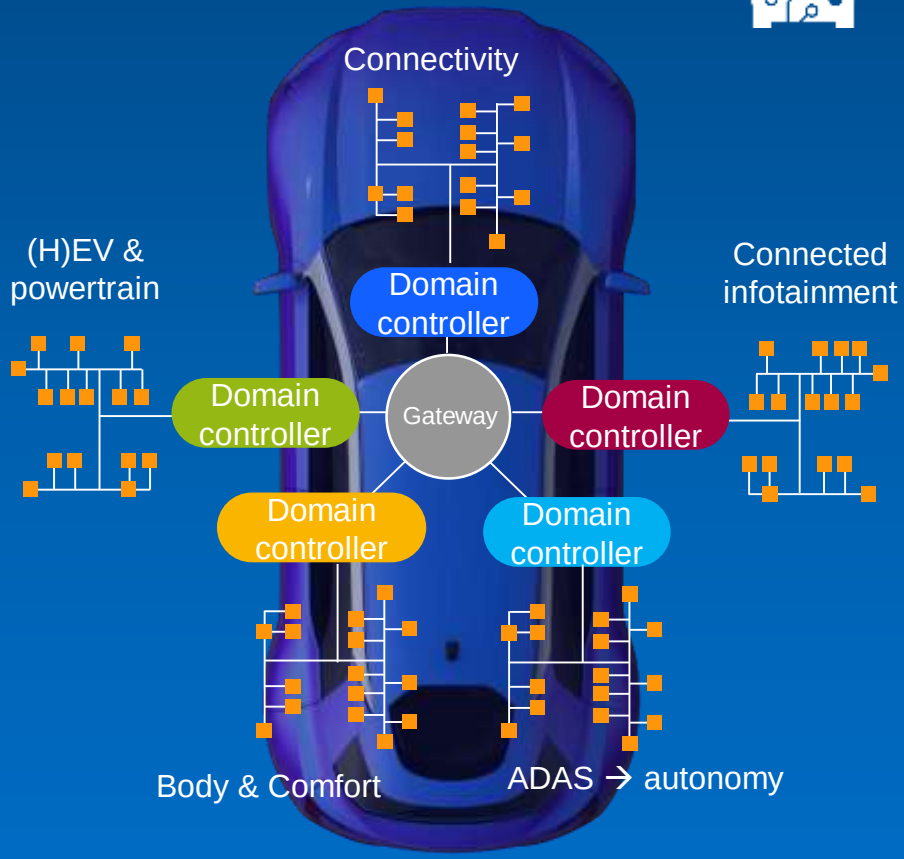
1Mb CAN
100Mb Ethernet

NO security

NO traffic engineering

Flat to hierarchical

TOMORROW: DOMAINS



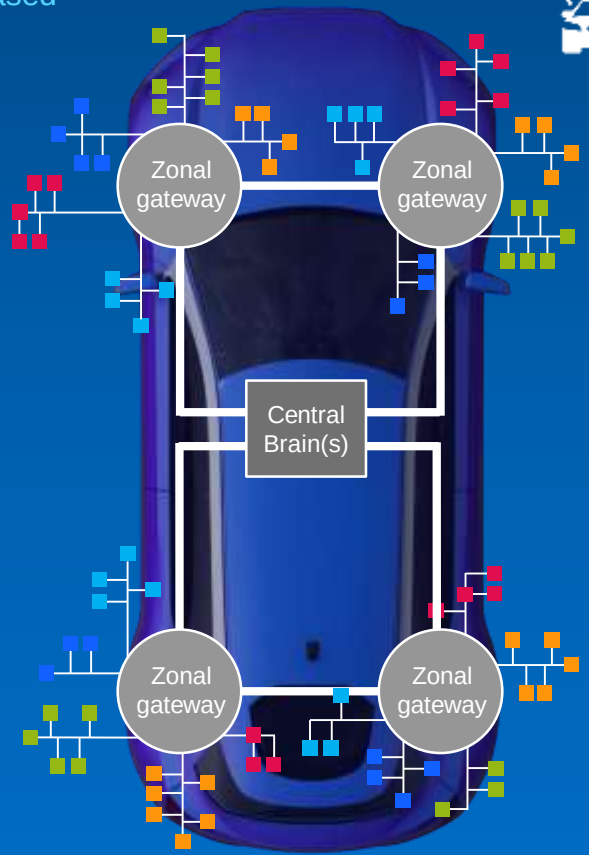
5Mb CAN
1Gb Ethernet

Firewall security

Basic TSN switches

Signal-based to service-based

AFTER TOMORROW: ZONES



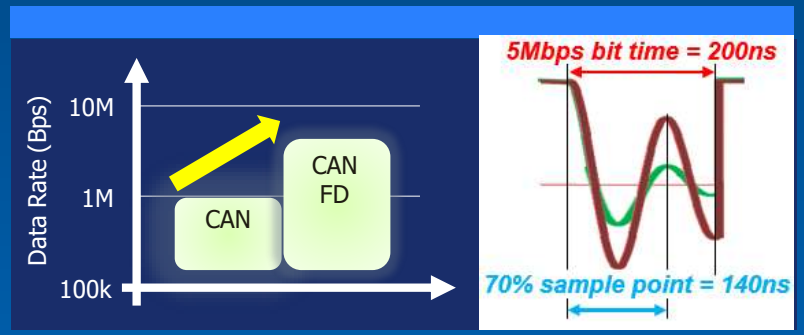
10Mb CAN/Eth
10Gb Ethernet

E2E security

Full-traffic engineering

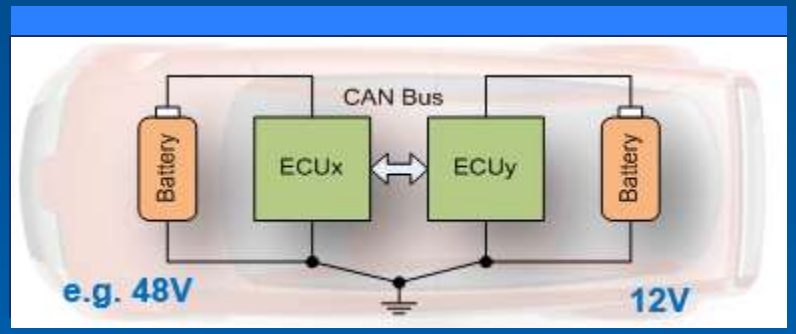
NXP STRATEGY to ENABLE CAN TRANSFORMATION

Provide a unique toolbox of solutions for each major problem



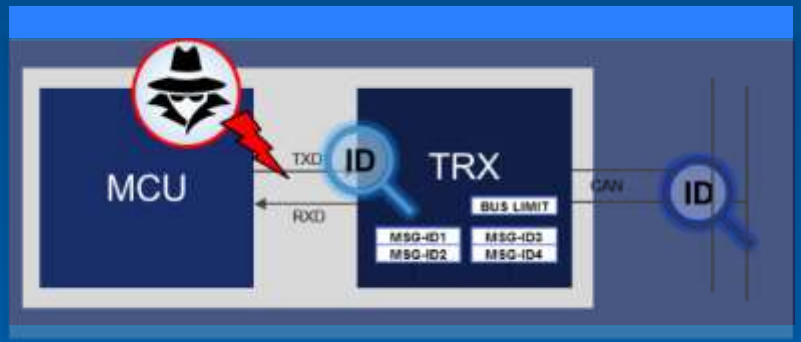
Accelerate CAN-FD

Provide fast, silent transceivers
Suppress signal ringing



Bridge voltage domains

Mix 48 V and 12 V domains
Standardize EV battery communication



Contain hack damages

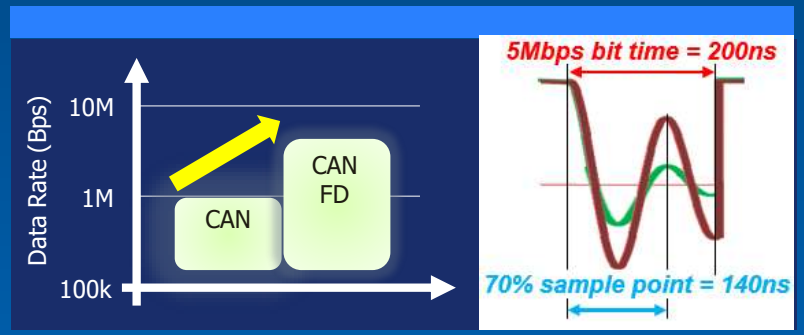
Police CAN traffic
Contain hacked host

Analog innovation → Digital innovation

Design freedom @ 2 Mbps and 5 Mbps	Simplify mild-hybrid and BMS	Drop-in, basic cyber-protection

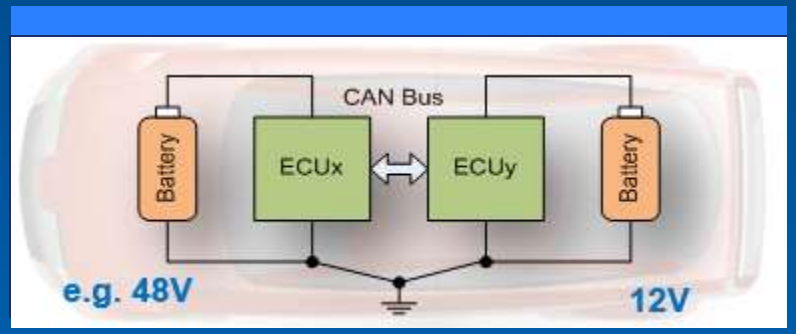
NXP STRATEGY to ENABLE CAN TRANSFORMATION

Provide a unique toolbox of solutions for each major problem



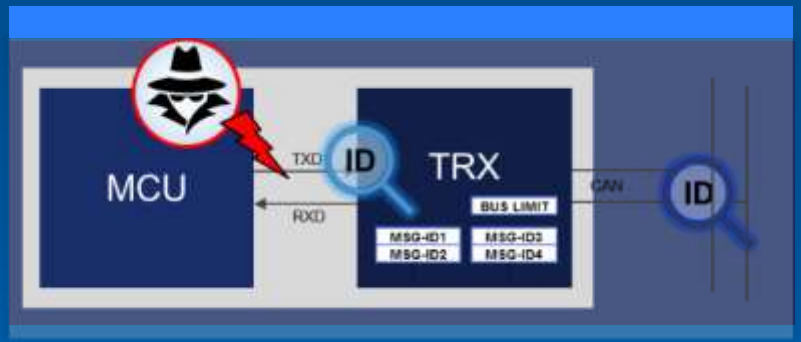
Accelerate CAN-FD

Provide fast, silent transceivers
Suppress signal ringing



Bridge voltage domains

Mix 48 V and 12 V domains
Standardize EV battery communication



Contain hack damages

Police CAN traffic
Contain hacked host

Analog innovation → Digital innovation

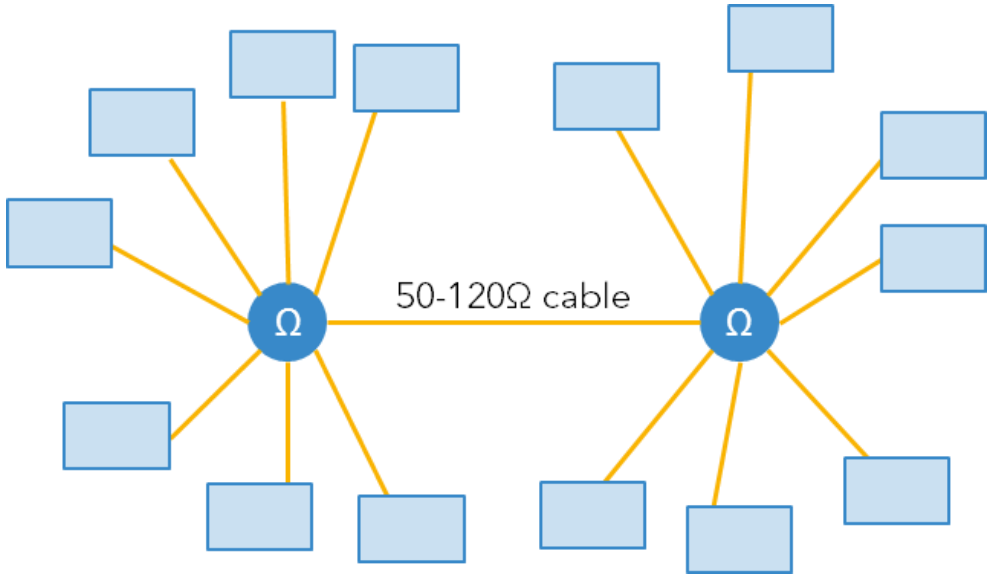
Design freedom @ 2 Mbps and 5 Mbps	Simplify mild-hybrid and BMS	Drop-in, basic cyber-protection

CAN INNOVATION – TJA146x

Re-thinking the CAN transceivers ready for tomorrow’s networks

CAN-FD CREATES MAJOR CABLE TENSION

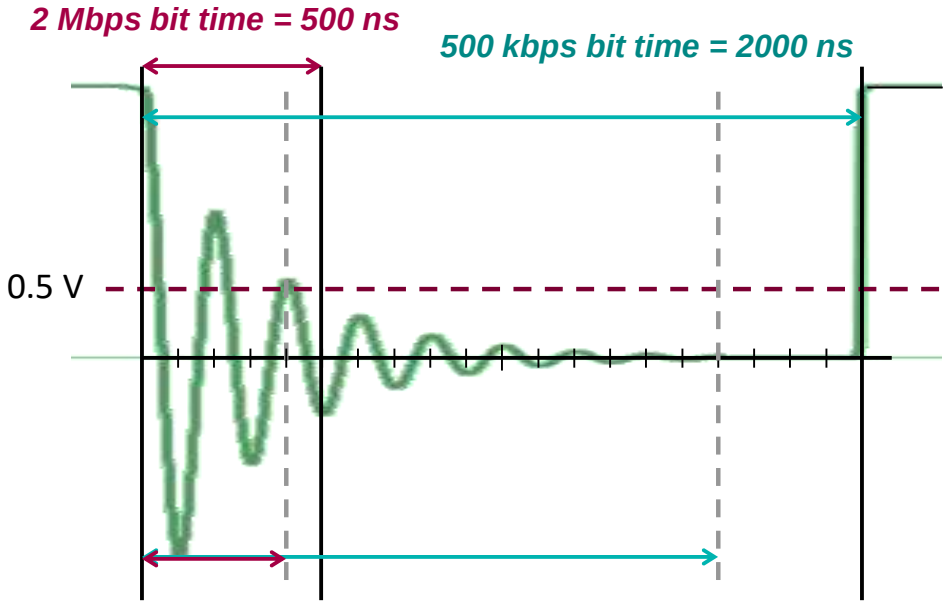
Ringing is highly relevant for CAN-FD networks because
two demands directly conflict with each other



Complex topologies

efficient from cost and production perspective

→ **create lots of ringing**



Demand for faster bit rates

significantly reduces time to dissipate ringing

→ **forces simpler topologies**

THE CAN TRANSCEIVER
RE-INVENTED FOR THE AUTONOMOUS CAR

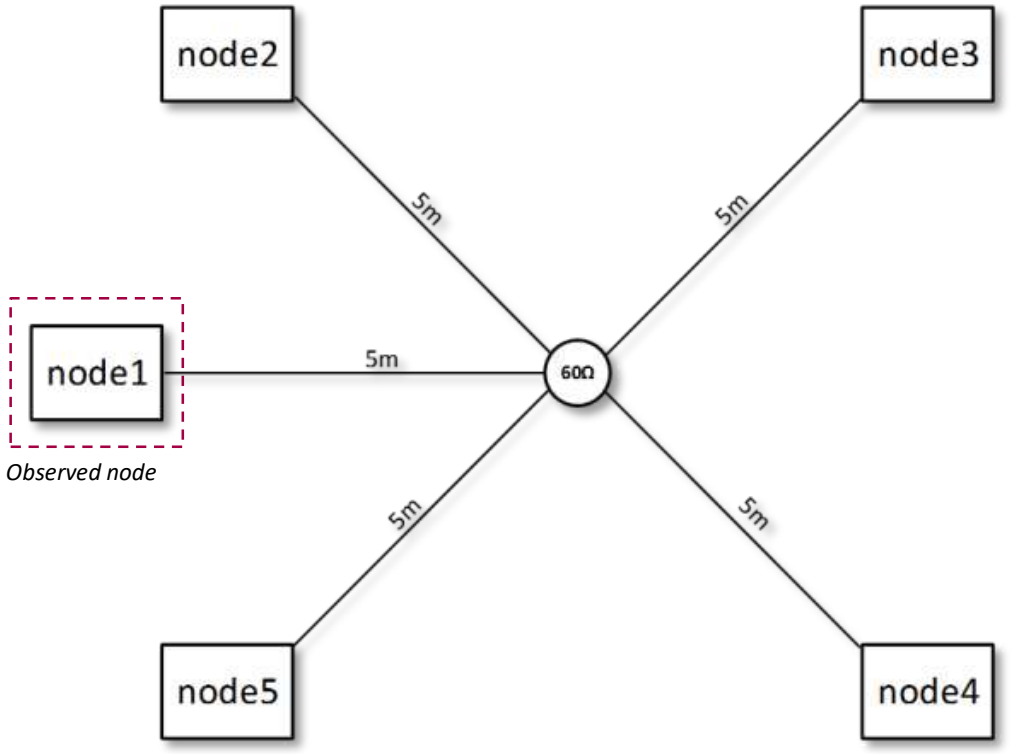
TJA146x CAN Signal Improvement transceivers

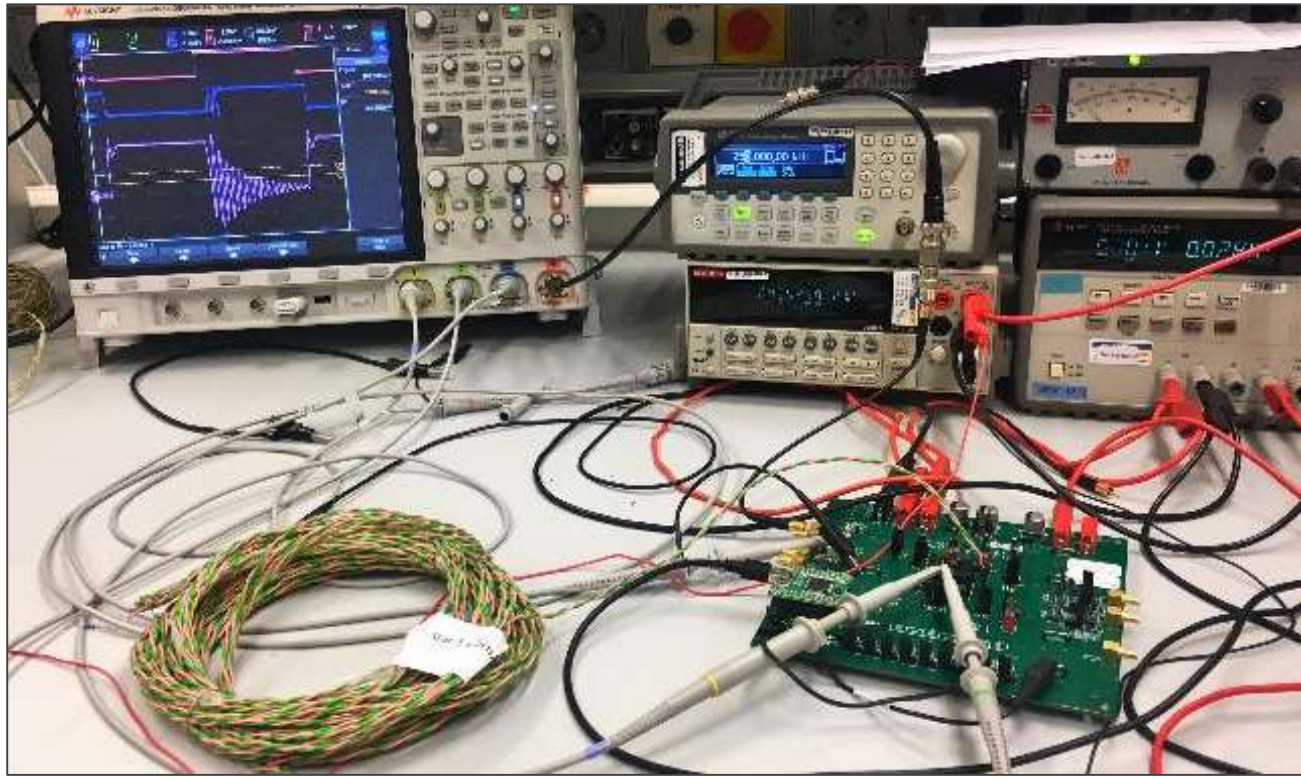
- CAN-FD networks on complex topologies
- Reduce cabling cost and weight
- Accelerate CAN-FD beyond 5 Mbps
- Directly replaces HS-CAN transceivers
- Fulfills CiA601-4 v2.0.0 specification

Signal improvement measurements

Network setup

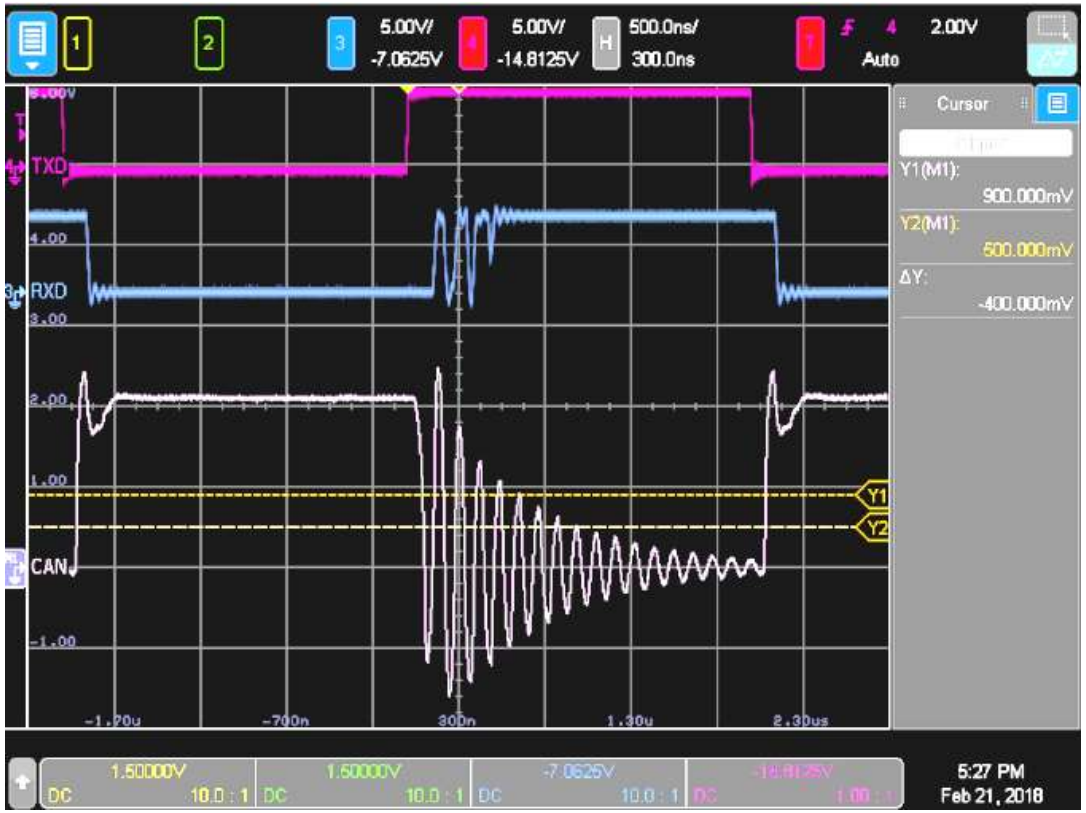
5 stubs of 5 m, connected with a star termination of 60 Ω at the star





CAN-FD communication at 500 kbps

Classical CAN transceiver

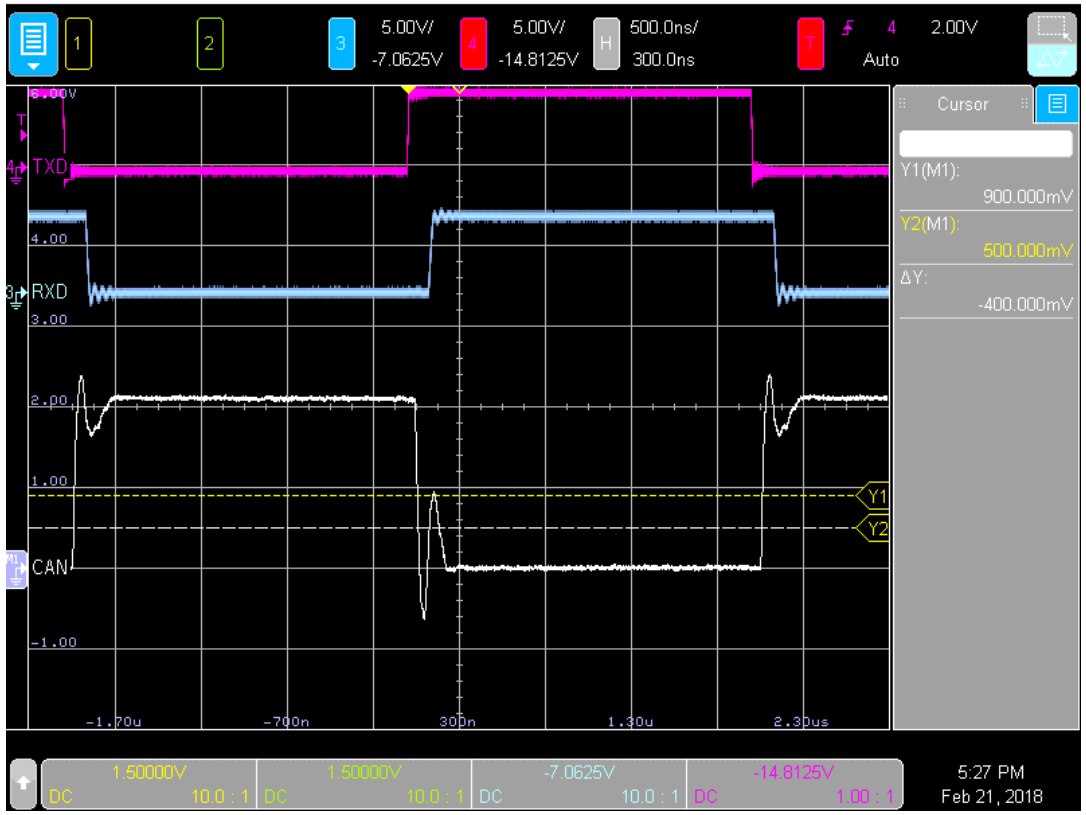


TXD

RXD

V_{diff} (bus)

TJA146x transceiver

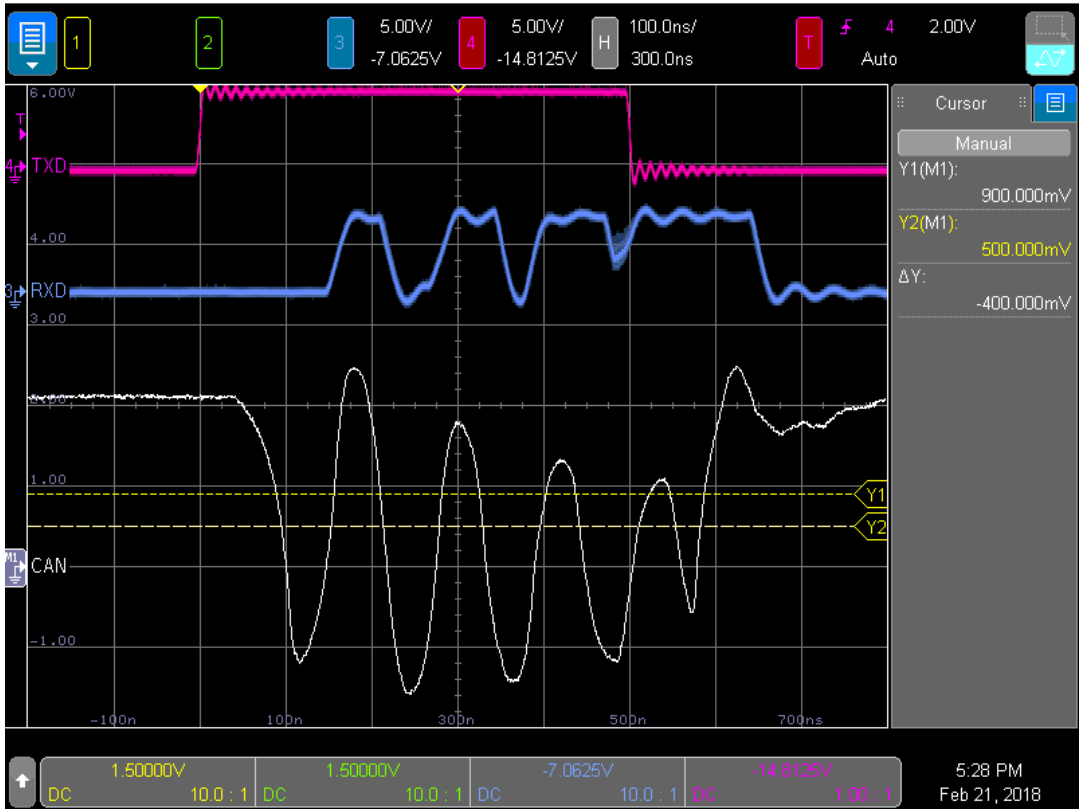


Ringing visible with classical transceiver, causing toggling on RxD

With TJA146x, bus is quickly stable and **RxD remains clean**

CAN-FD communication at 2 Mbps

Classical CAN transceiver

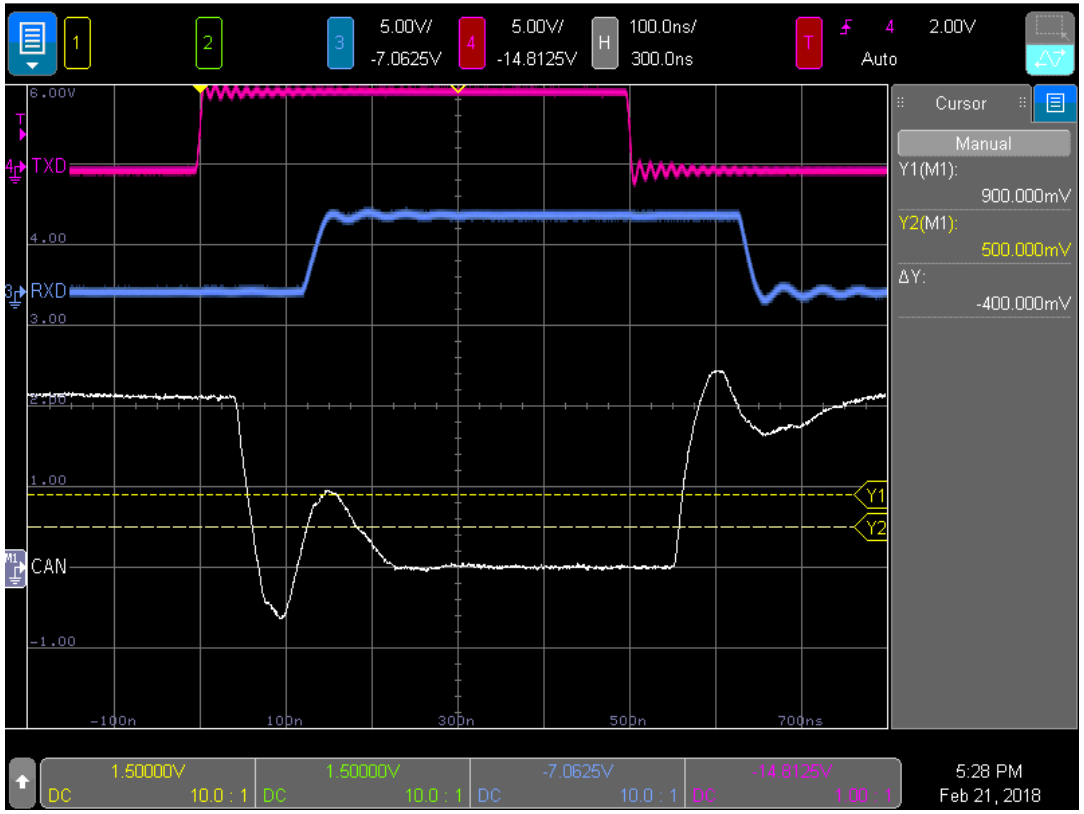


TXD

RXD

V_{diff} (bus)

TJA146x transceiver



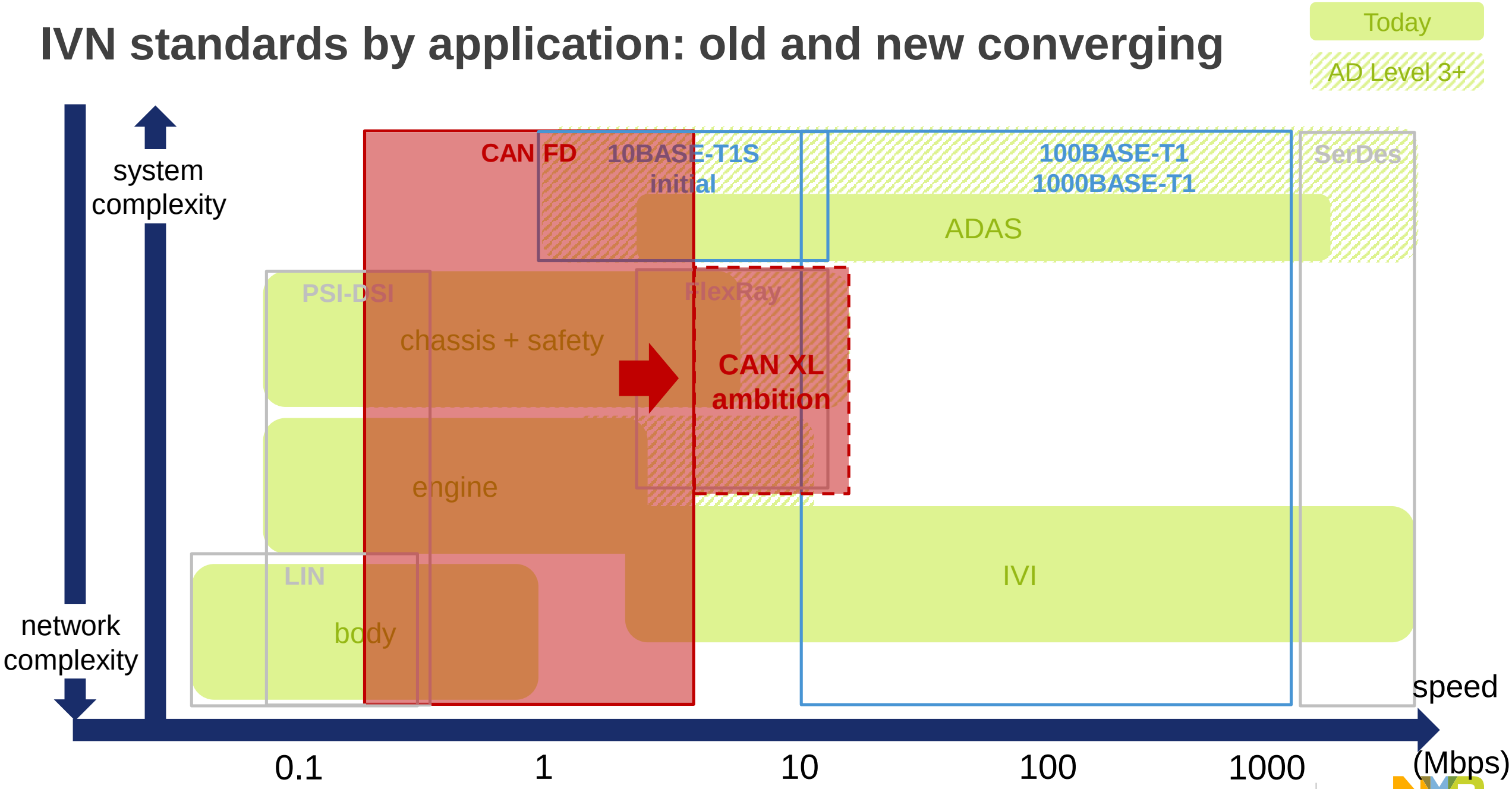
Ringing visible with classical transceiver,
causing toggling on RxD **during sample point**

With TJA146x, bus is quickly stable and
RxD remains clean

CAN INNOVATION – CAN-XL

Re-thinking the CAN transceivers ready for tomorrow’s networks

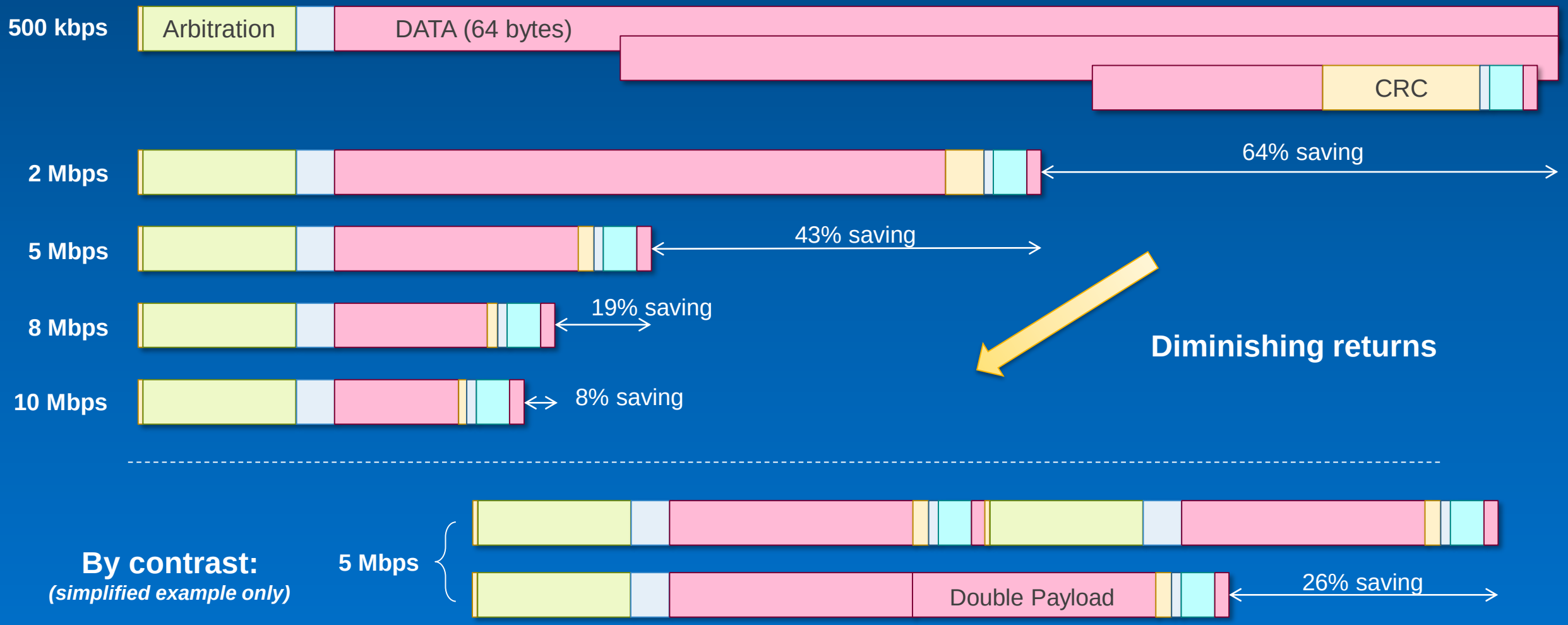
IVN standards by application: old and new converging



Future Outlook: CAN-XL – Extension of CAN-FD

TJA146x redefined the market in terms of possibilities

Next challenge: extend CAN-FD payload limit



(64% for a 2048 byte frame)

Future Outlook: CAN-XL – Extension of CAN-FD

TJA146x redefined the market in terms of possibilities

Next challenge: extend CAN-FD payload limit

Target use-cases of CAN-XL:

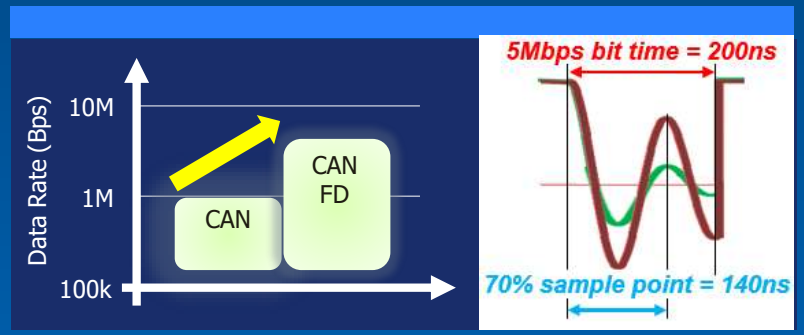
- Bit rates between 2 – 10 Mbps, where 100 Mbps Ethernet is overblown and FlexRay too complex
- Networks which do not require deterministic or IP-based communication
- Applications where bus topologies give major cost advantage

Examples:

- Connection of peripherals (e.g. sensors and actuators requiring 1 – 10 Mbps)
- Audio (e.g. microphone for eCall)
- Fast end-node links in zonal architectures

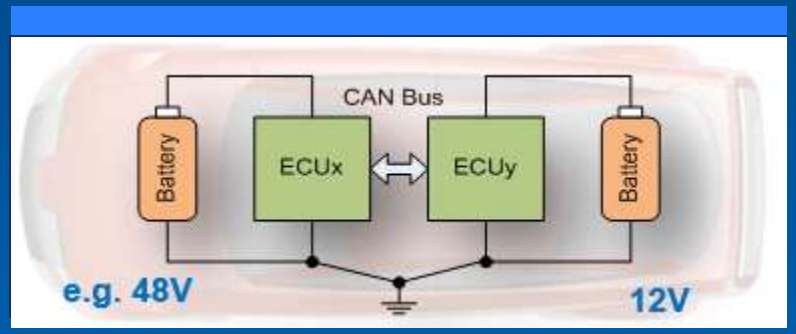
NXP STRATEGY to ENABLE CAN TRANSFORMATION

Provide a unique toolbox of solutions for each major problem



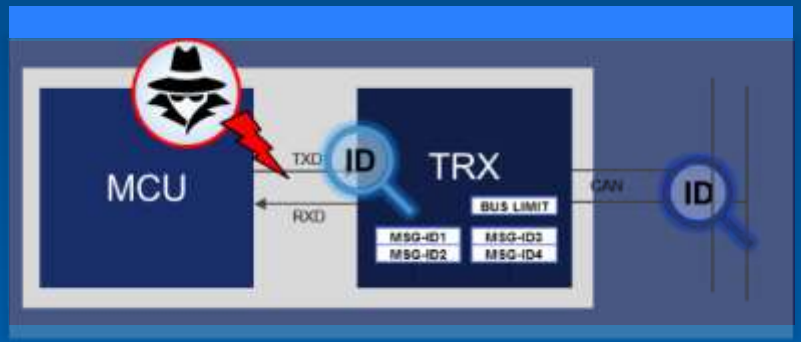
Accelerate CAN-FD

Provide fast, silent transceivers
Suppress signal ringing



Bridge voltage domains

Mix 48 V and 12 V domains
Standardize EV battery communication



Contain hack damages

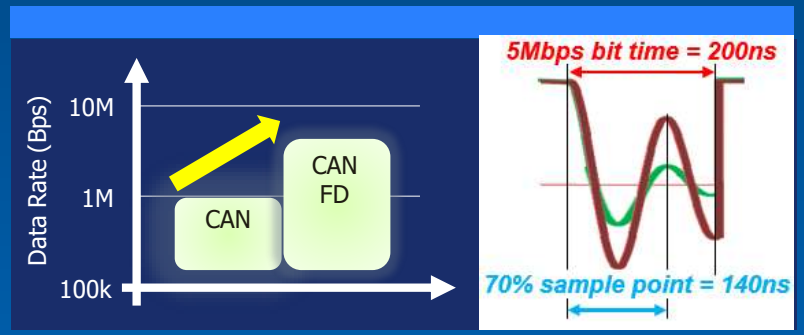
Police CAN traffic
Contain hacked host

Analog innovation → Digital innovation

Design freedom @ 2 Mbps and 5 Mbps	Simplify mild-hybrid and BMS	Drop-in, basic cyber-protection

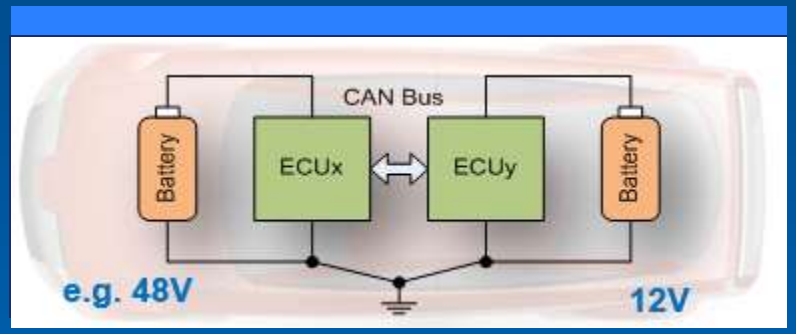
NXP STRATEGY to ENABLE CAN TRANSFORMATION

Provide a unique toolbox of solutions for each major problem



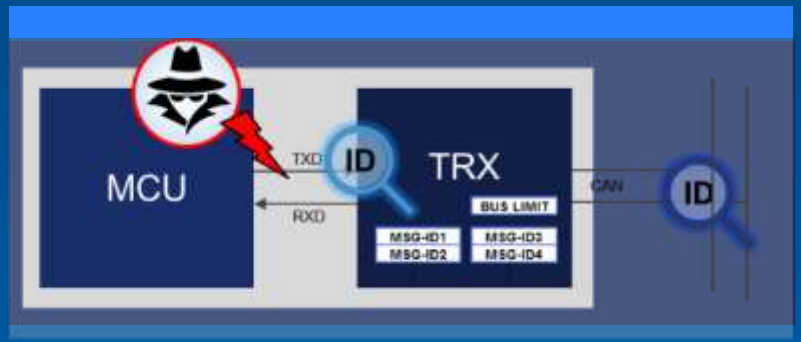
Accelerate CAN-FD

Provide fast, silent transceivers
Suppress signal ringing



Bridge voltage domains

Mix 48 V and 12 V domains
Standardize EV battery communication



Contain hack damages

Police CAN traffic
Contain hacked host

Analog innovation → Digital innovation

Design freedom @ 2 Mbps and 5 Mbps	Simplify mild-hybrid and BMS	Drop-in, basic cyber-protection

NXP CAN SECURITY

THE INNOVATIVE HARDWARE SOLUTION ENHANCING ANY SOFTWARE APPROACH

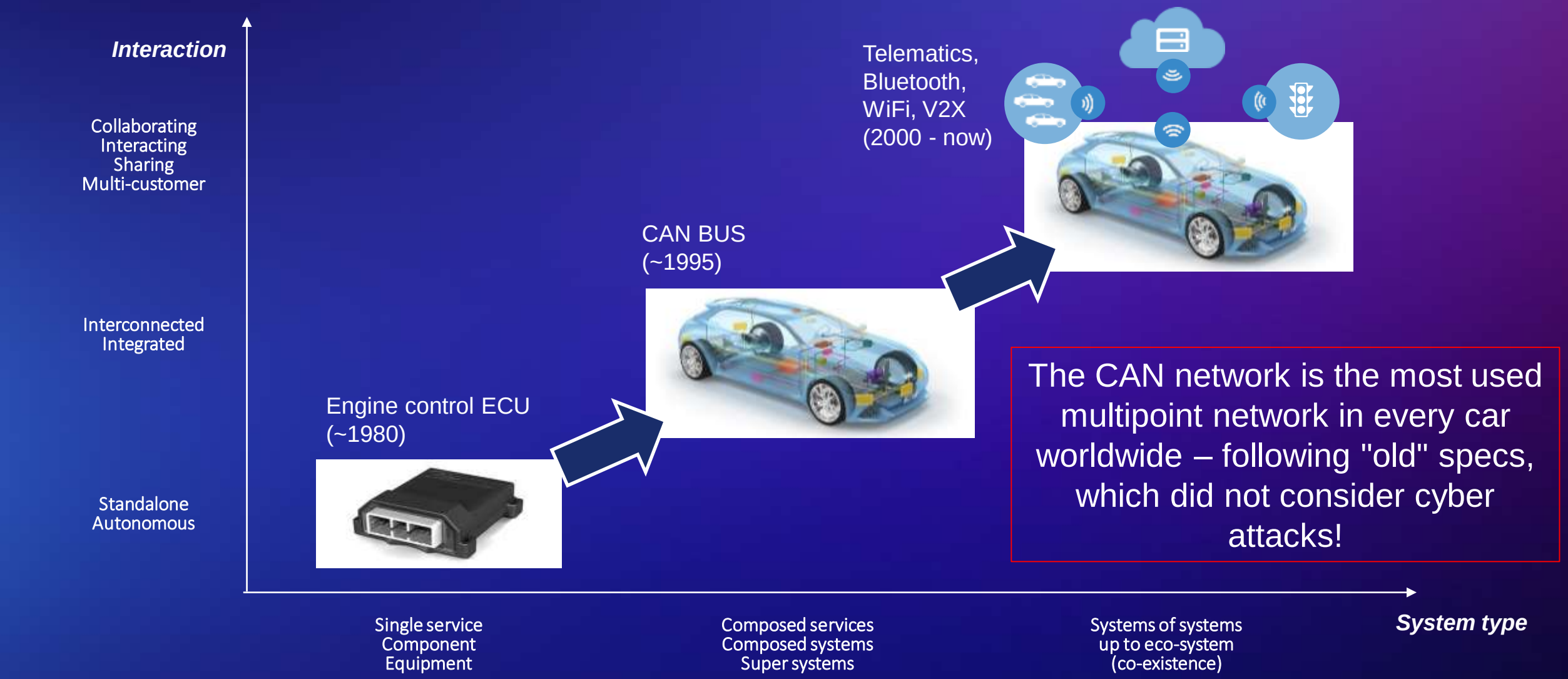
Secure CAN transceiver

TJA115x

SECURE CONNECTIONS FOR A SMARTER WORLD

CAN SECURITY

Vehicle electronics & connectivity



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

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 200M lines of software code

Why now?

Wireless interfaces
enable scalable attacks

250M connected vehicles on the road in 2020

Why does it affect?

Abusing ingenuous ECU
forces unintended behavior

Immediate intrusion prevention is hard to guarantee

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

CAN-LEVEL SECURITY IS AN INSURANCE AGAINST INTRUSION

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 do not follow "the rules"

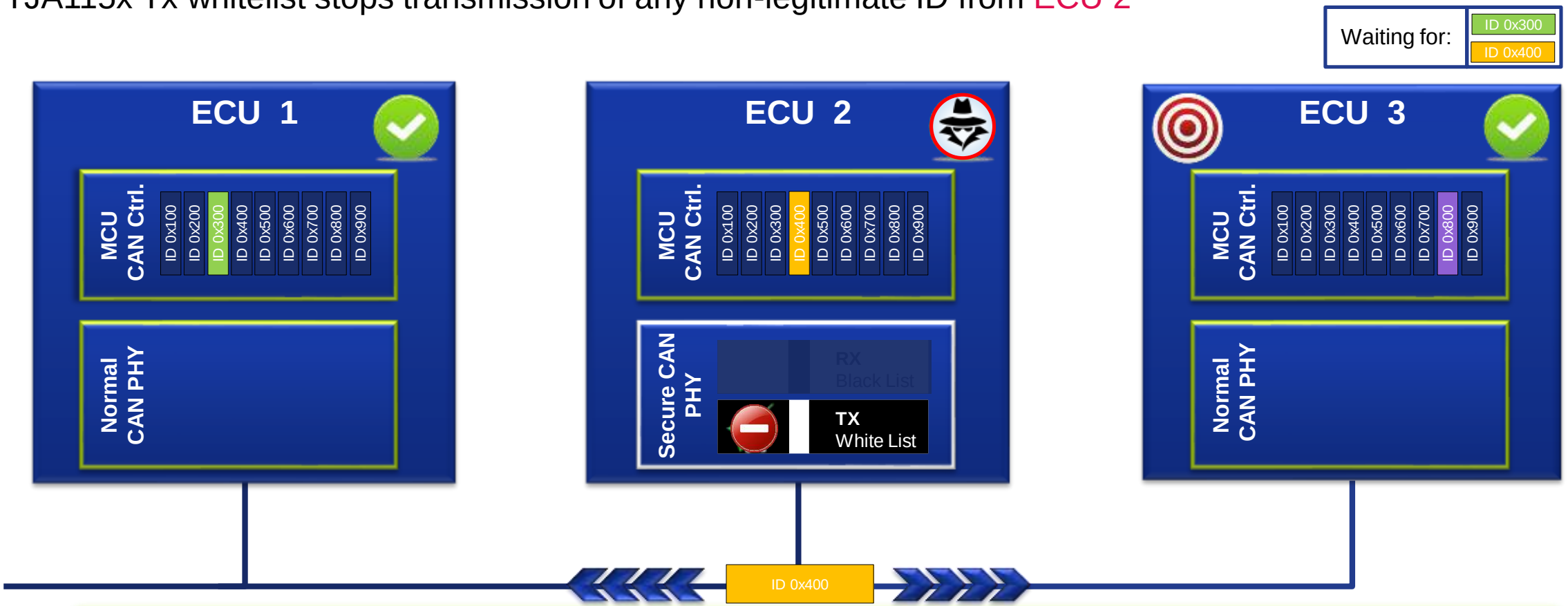
NXP SECURE CAN TRANSCEIVER

TJA115x

Spoofing detection & prevention

TJA115x - Spoofing prevention – transmit path

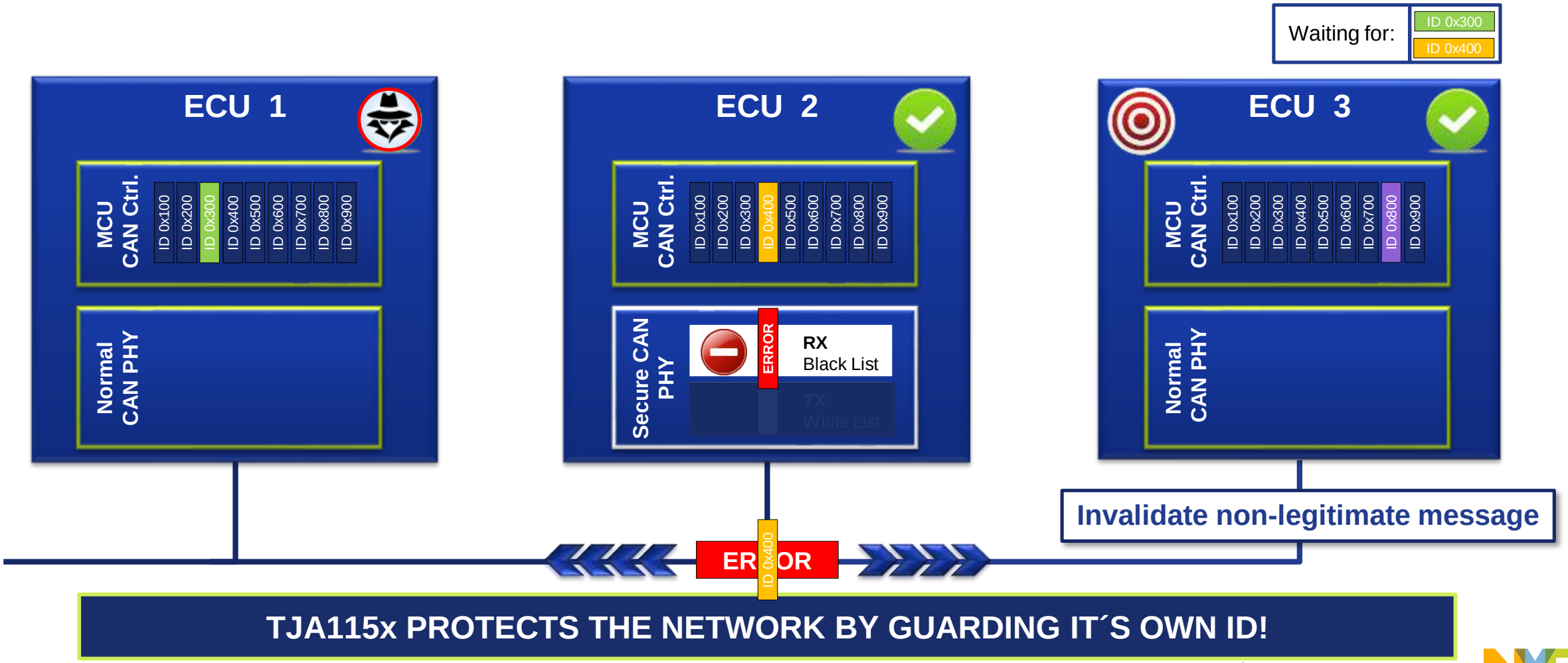
- ECU 2 gets compromised and pretends to be another ECU (spoofing)
- Only messages with ECU 2 legitimate ID ID 0x400 can pass the secure transceiver hardware filter!
- TJA115x Tx whitelist stops transmission of any non-legitimate ID from ECU 2



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

TJA115x - Spoofing prevention – receive path

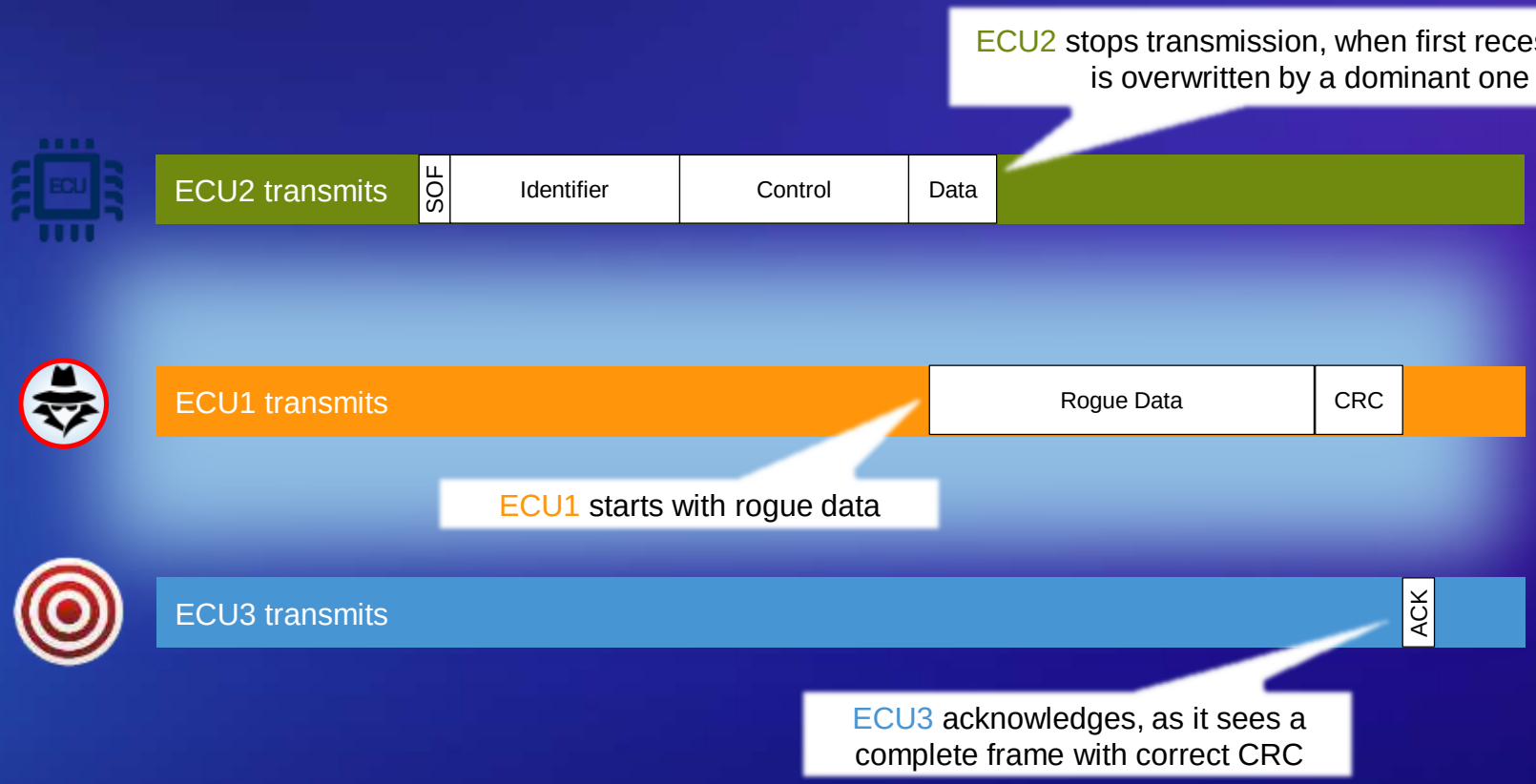
- Compromised ECU 1 pretends to be another ECU (spoofing)
- TJA115x Rx blacklist guards its own legitimate ID on the bus by detection and elimination with active error flag



TAMPERING PROTECTION

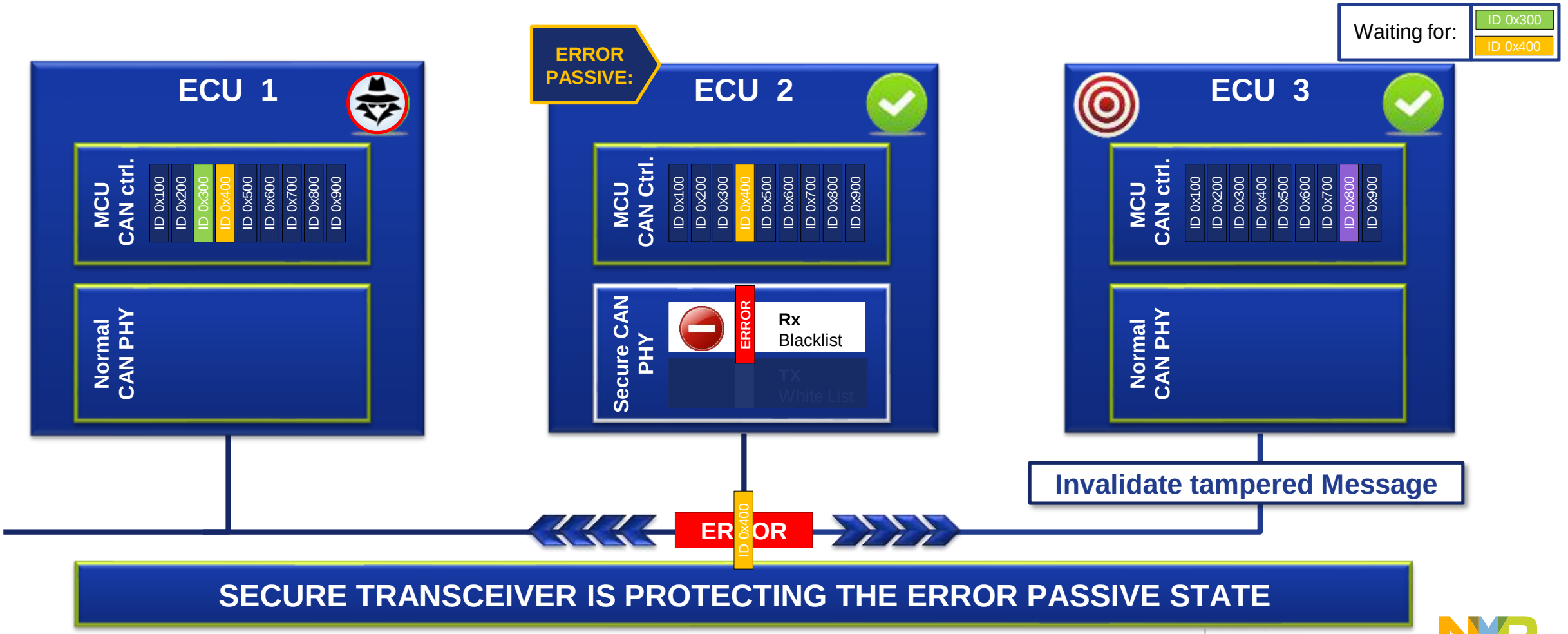
Principle of tampering – Altering legitimate message content

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



Secure transceiver – 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
- Secure transceiver of ECU 2 identifies a bit flip (direction change) and issues an active error flag

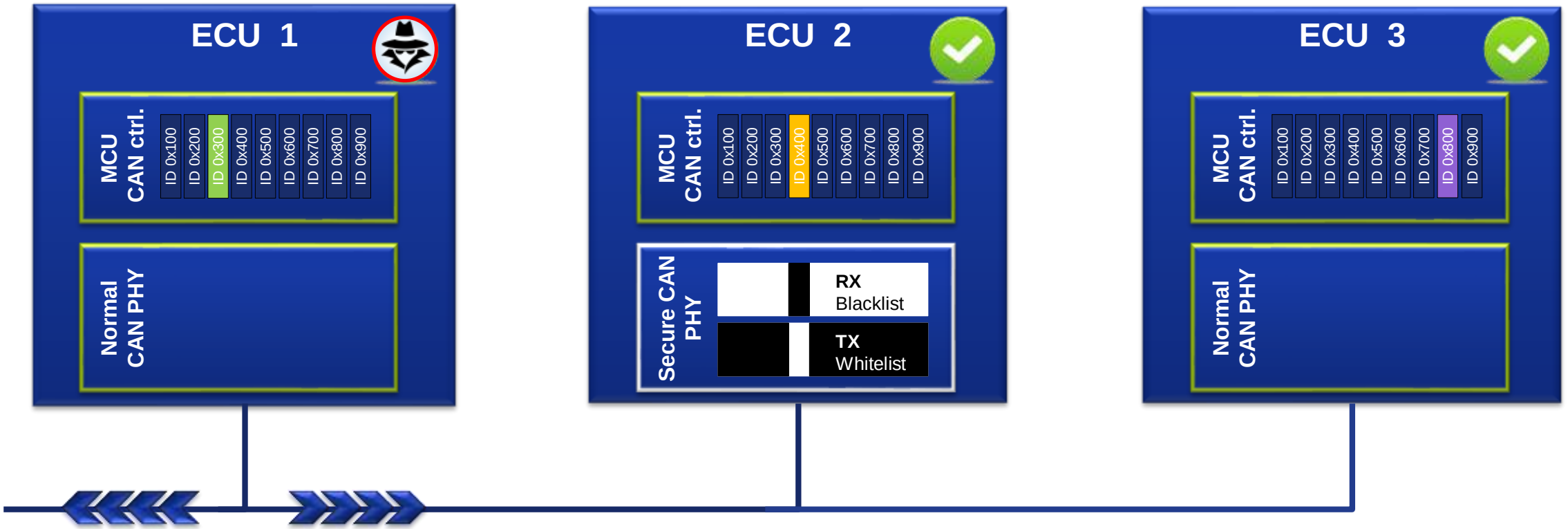


PREVENTION AGAINST DENIAL OF SERVICE BY FLOODING

A successful attack: flooding…

- ECU 1 gets compromised

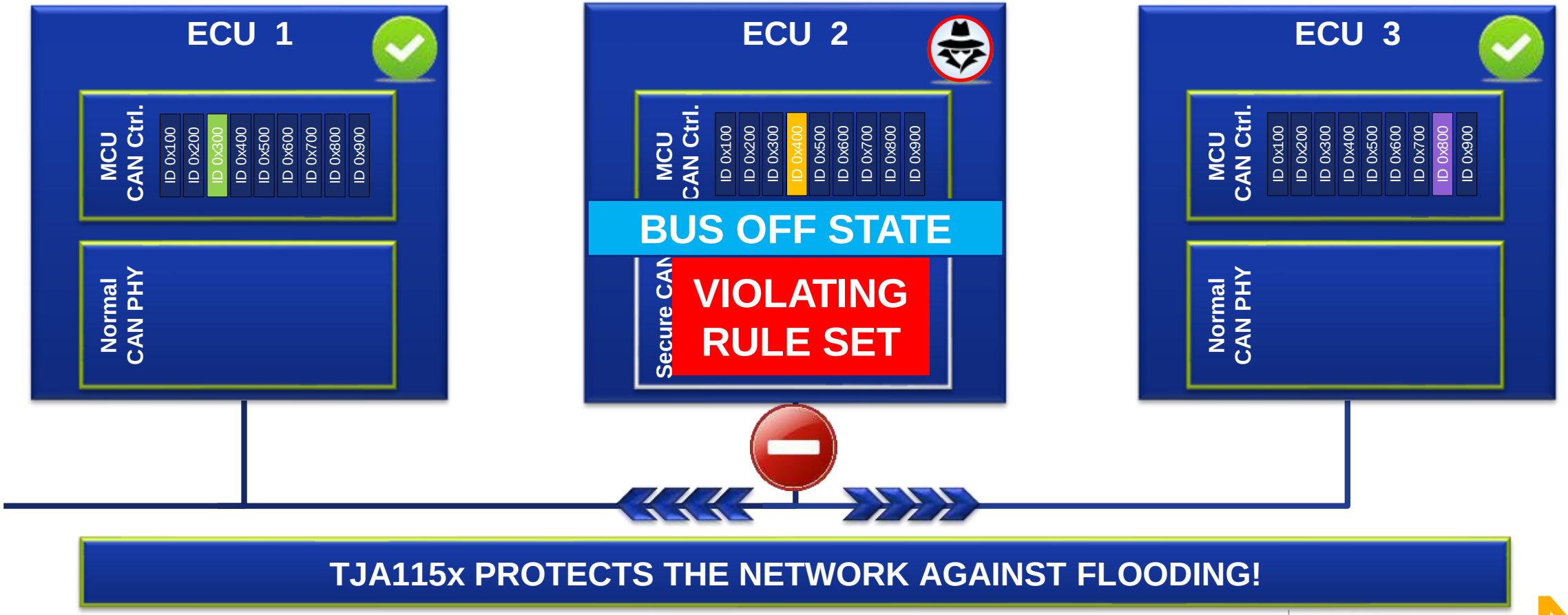
ECU 1 now has full access to the bus



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

TJA115x - flooding prevention

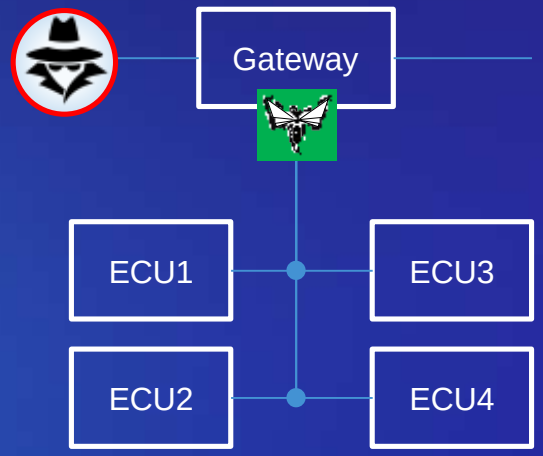
- ECU 2 gets compromised and can now try to flood the bus
- When the increased busload violates configured secure transceiver ruleset, the local host is set into *Bus Off* / *Secure* State



CONFIRMED USE CASES

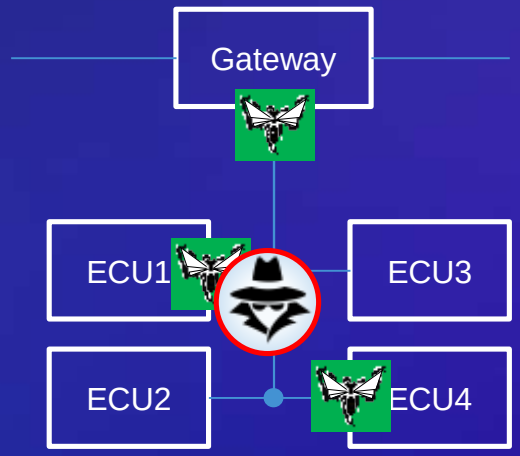
Confirmed OEM use cases

Firewalling flooding protection



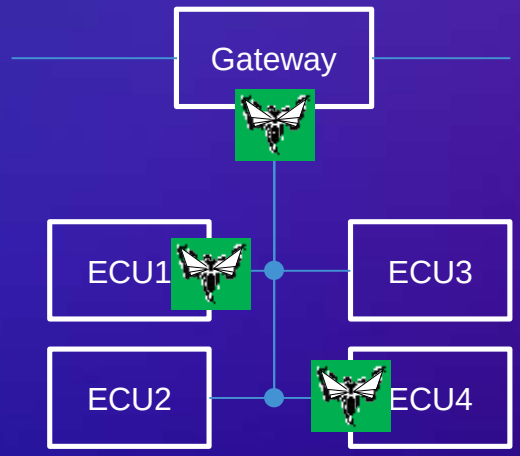
Legacy
New platforms

Immediate protection by HW – no SW!



Legacy
New platforms

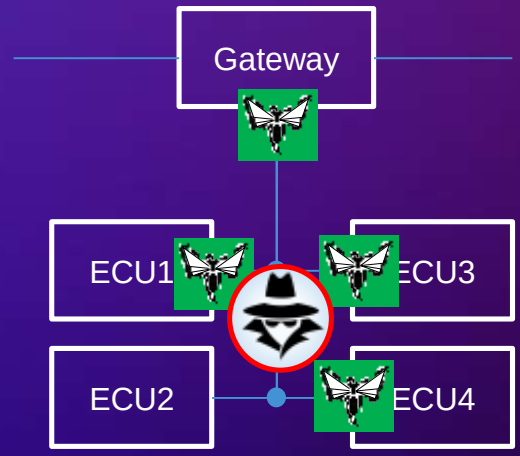
Offloading MCU Saving bandwidth Saving keys



New platforms

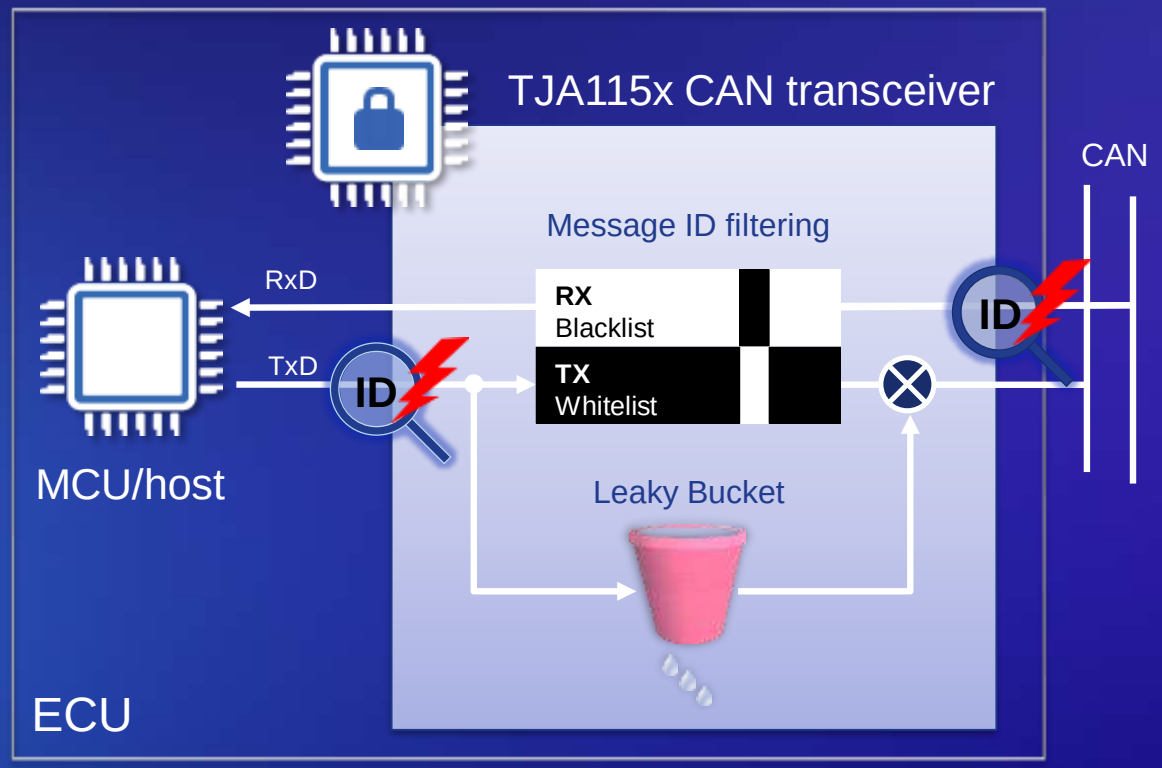
IDPS support

Monitor



New platforms

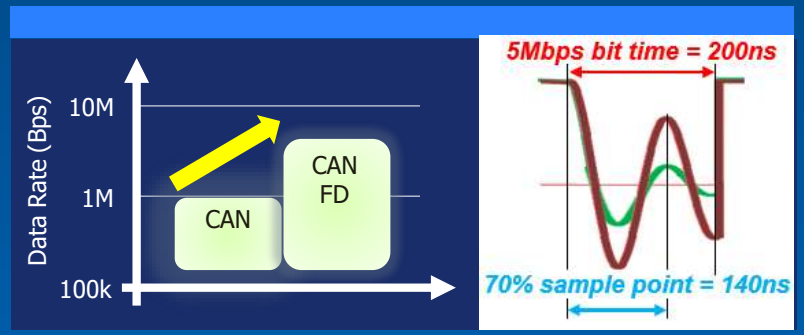
NXP secure CAN transceiver TJA115x



- 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 ECUs
- Helps reduce system cost

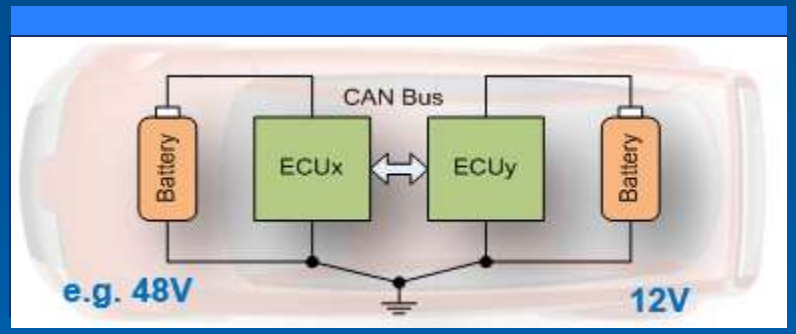
NXP STRATEGY to ENABLE CAN TRANSFORMATION

Provide a unique toolbox of solutions for each major problem



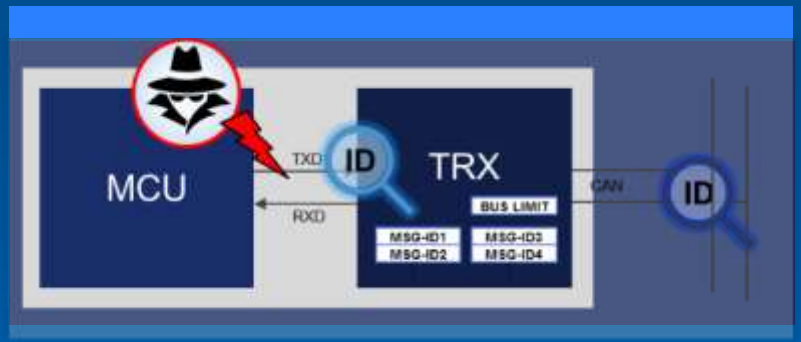
Accelerate CAN-FD

Provide fast, silent transceivers
Suppress signal ringing



Bridge voltage domains

Mix 48 V and 12 V domains
Standardize EV battery communication



Contain hack damages

Police CAN traffic
Contain hacked host

Analog innovation → Digital innovation

Design freedom @ 2 Mbps and 5 Mbps	Simplify mild-hybrid and BMS	Drop-in, basic cyber-protection

SECURE CONNECTIONS
FOR A SMARTER WORLD