FTF 2016
TECHNOLOGY FORUM

ENABLING HYBRID CAN NETWORKS: CAN FD SHIELD

FTF-AUT-N1775

Bernd Elend
Principal
FTF-AUT-N1775
May 19, 2016

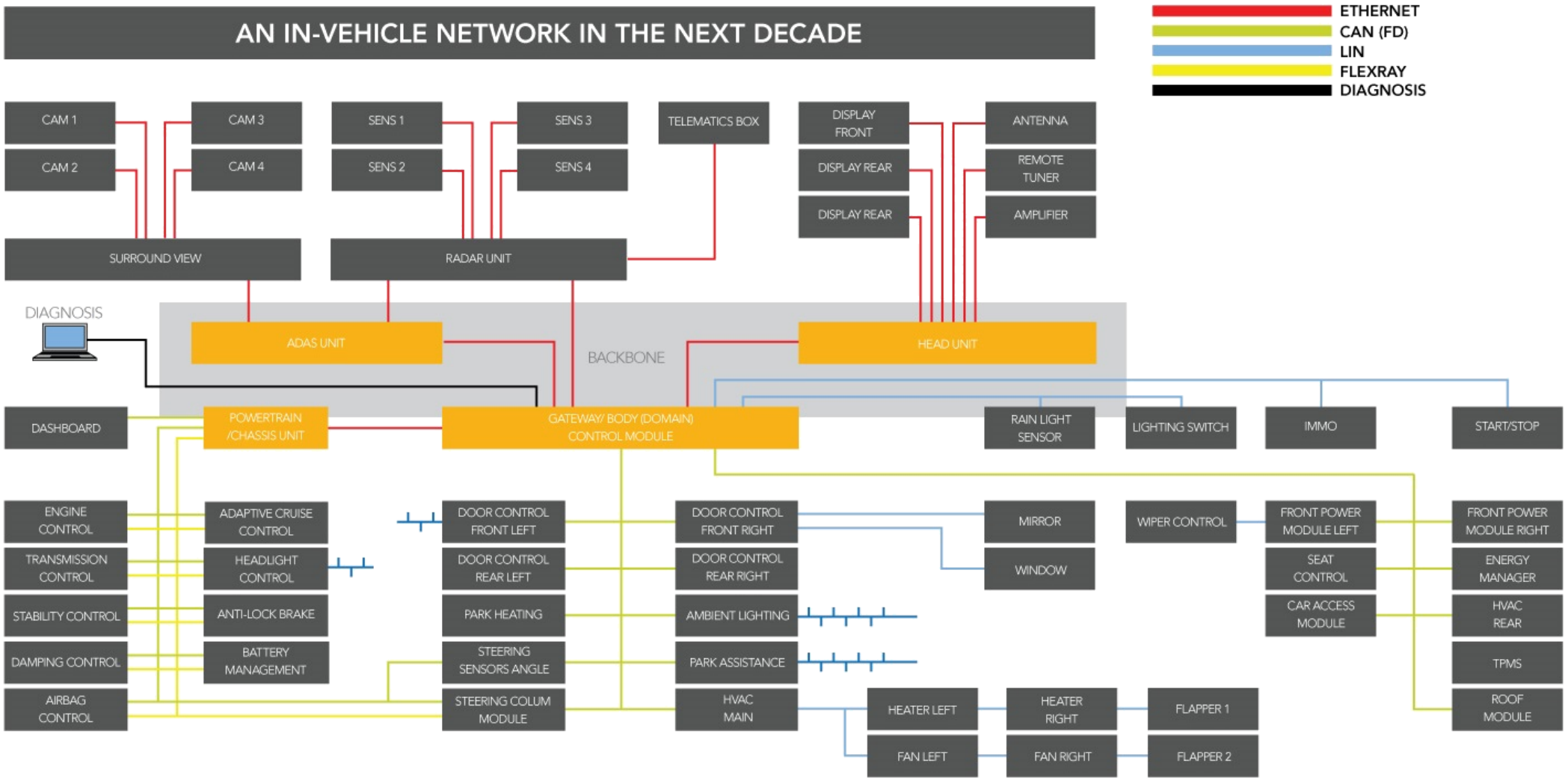
AGENDA

- Why CAN FD?
- First hybrid networks for ECU flashing
- Hybrid networks for full operation
- CAN FD shield operation
- Industry support & validation
- Summary and key messages
- Outlook to further smart transceiver functions
- Contact

90% of Automotive Innovation is Electronics

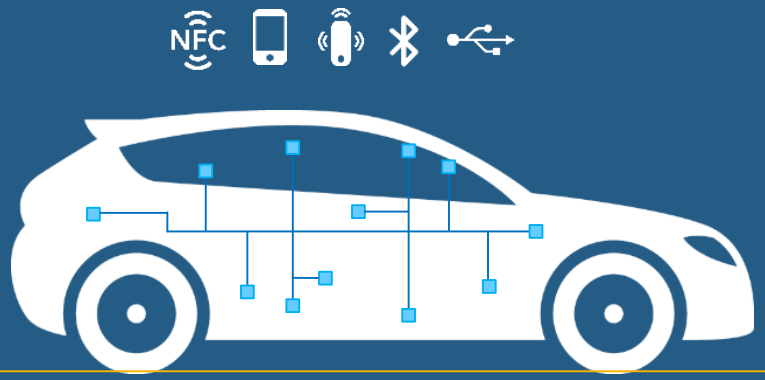
All this requires a high performant in-vehicle network

Modern In-vehicle Networks



Past Challenges for In-vehicle Networks: Ease of Use

Today



Almost no IT cyber security
Classical CAN

IVN issues solved by means of transceiver features

EMC
Emission & Immunity

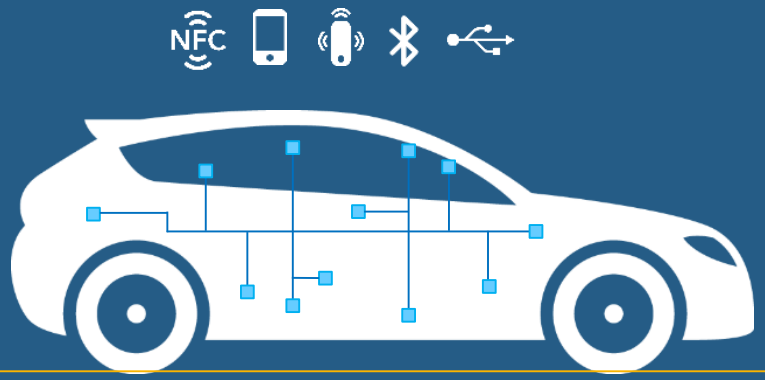
ESD
Protection

Low power modes
and remote wake-up

ECU power management
battery voltage high side switch

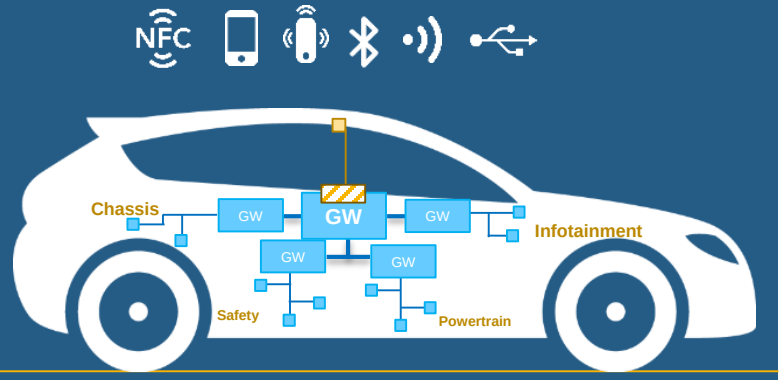
New Challenges For In-vehicle Networks: Speed and Security

Today



Almost no IT cyber security
Classical CAN

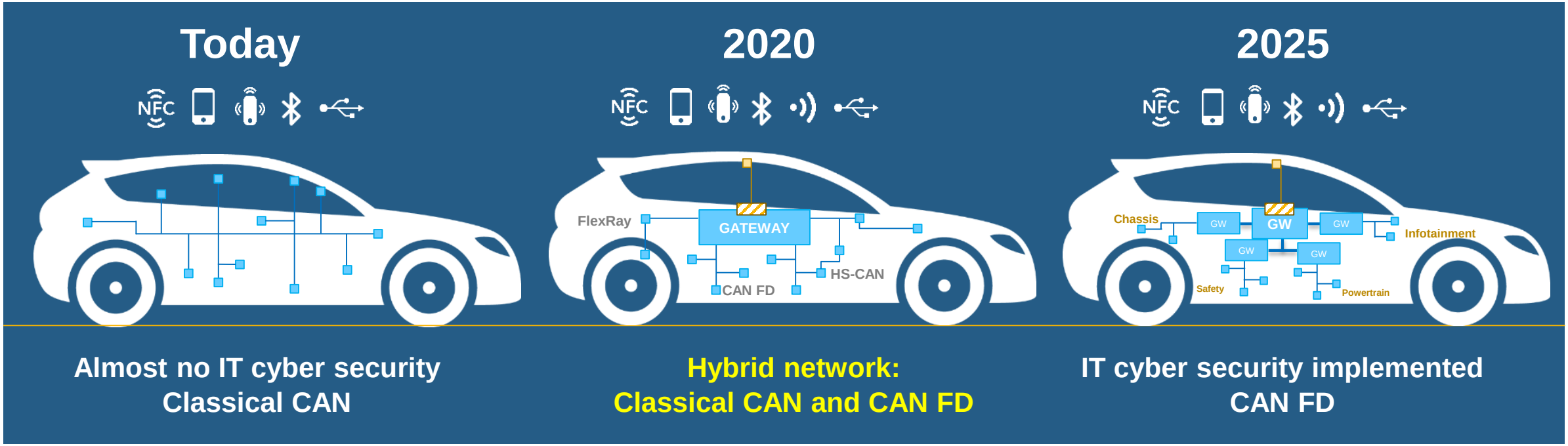
2025



IT cyber security implemented
CAN FD

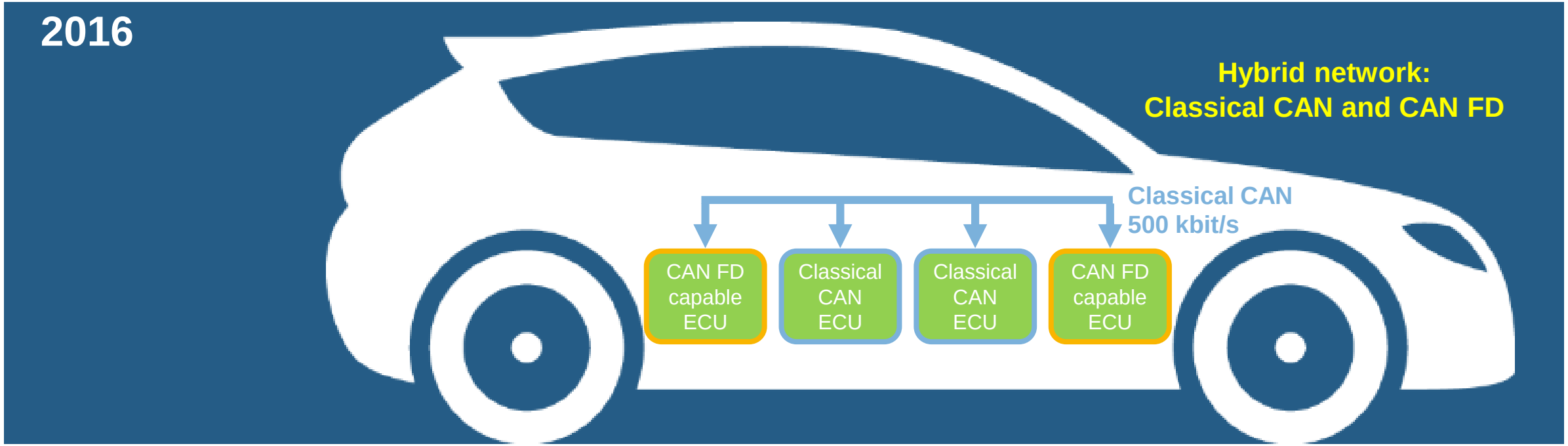
New challenges for in-vehicle networks	Higher bit rate for IT cyber security	Higher bit rate for enhanced safety	Higher bit rate for more comfort	Higher bit rate for improved ADAS	Higher bit rate for better infotainment

New Challenges For In-vehicle Networks: Speed and Security



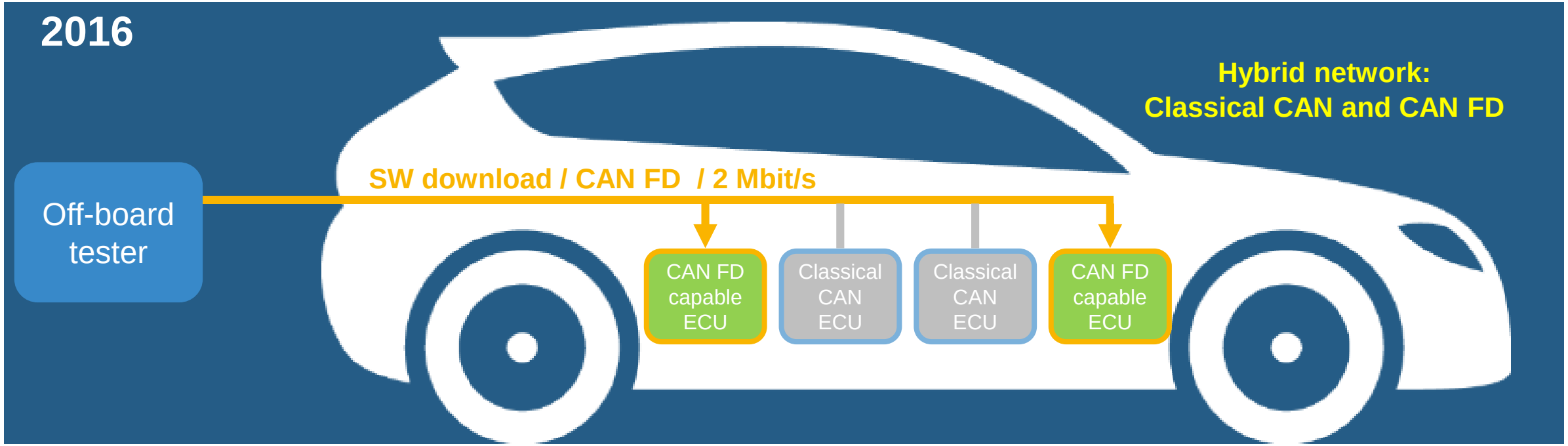
The hurdles in the transition phase	Major investments in network re-architecture necessary	Strong security not possible on Classical CAN	CAN FD hampered by ringing on long stubs	Lack of available CAN FD MCUs; esp. 8 and 16 bit	Auto Ethernet eco-system still not mature

First Hybrid Networks for ECU Flashing



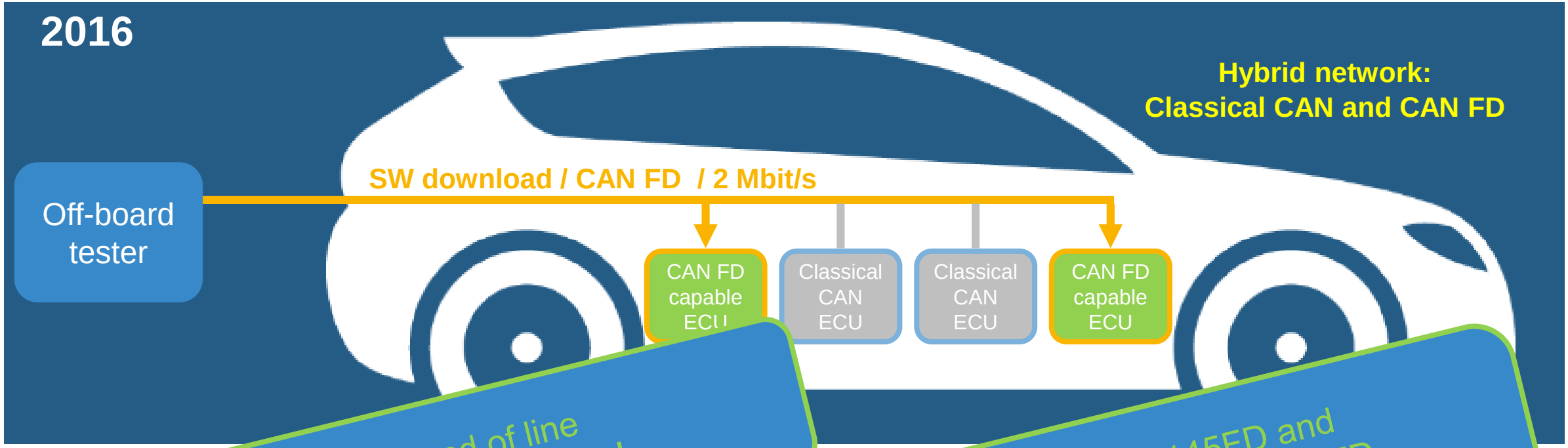
Mixing Classical CAN and CAN FD	For some modules the µC family is already available with CAN FD	Modules with 8 and 16 bit µC are often not available with CAN FD	Classical CAN modules destroy CAN FD frames with error frames	At least SW flashing at the end of line should be made available	Classical CAN modules need to be “deaf” when CAN FD frames occur

First Hybrid Networks for ECU Flashing



Mixing Classical CAN and CAN FD – managed by partial networking transceivers	Only those ECUs are updated that have a huge demand on SW download and MCU as CAN FD MCU available	ECUs that do not have CAN FD capabilities remain in low-power modes during CAN FD communication	Transceiver wake-up initiated by dedicated Classical CAN frame after flashing is complete	Step-wise introduction of CAN FD	CAN FD operation only during flashing or other special vehicle operation modes

First Hybrid Networks for ECU Flashing



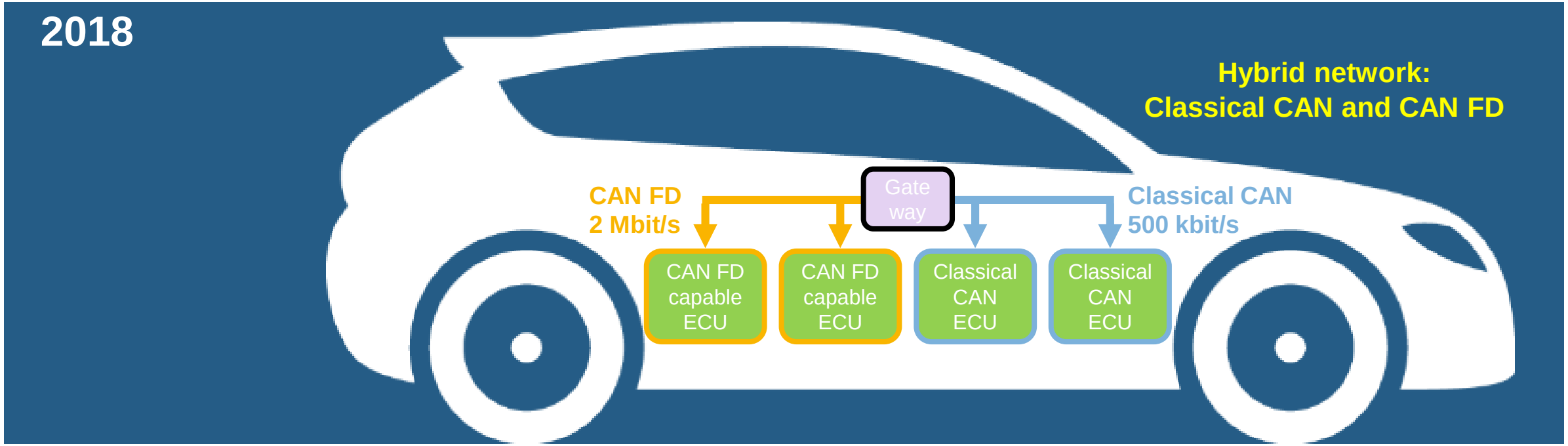
Speeding-up end of line SW flashing in to the vehicle!

Transceiver TJA1145FD and SBCs UJA1169 and UJA1132FD are available in mass production and will be used for exactly this use case!

download and MCU as CAN FD MCU available

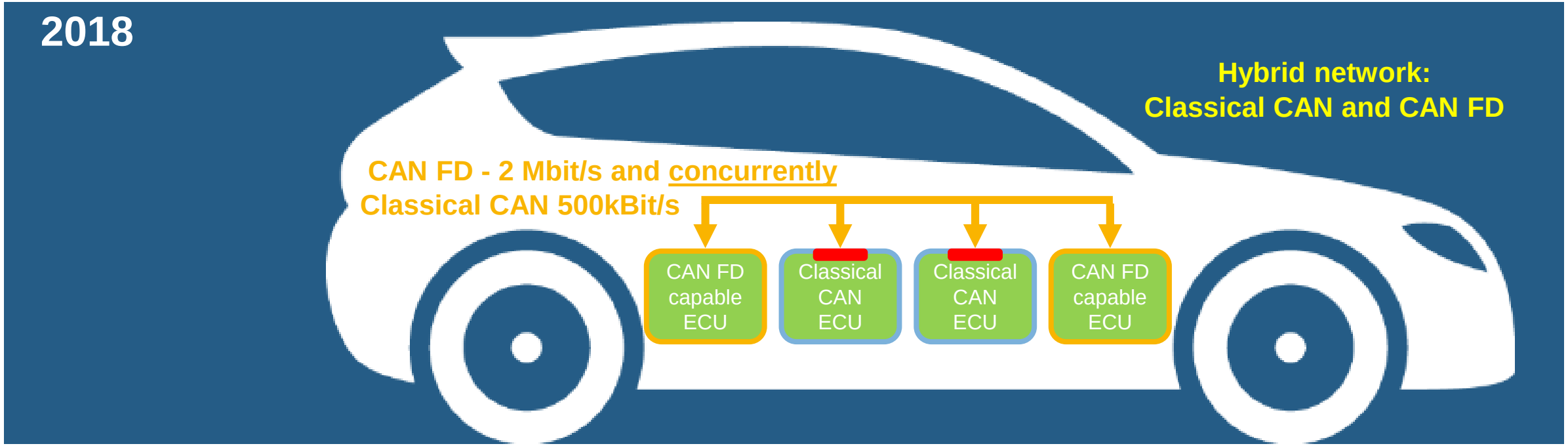
vehicle operation modes

First Hybrid Networks for ECU Flashing



Mixing Classical CAN and CAN FD – New network layout	One solution is adding a gateway; which is costly	Modules are now grouped by CAN FD capabilities and not by vehicle domains	Enormous change in the wire harness required	In-flexible solution when further modules can be changed to CAN FD	??????

Hybrid Networks for Full Operation



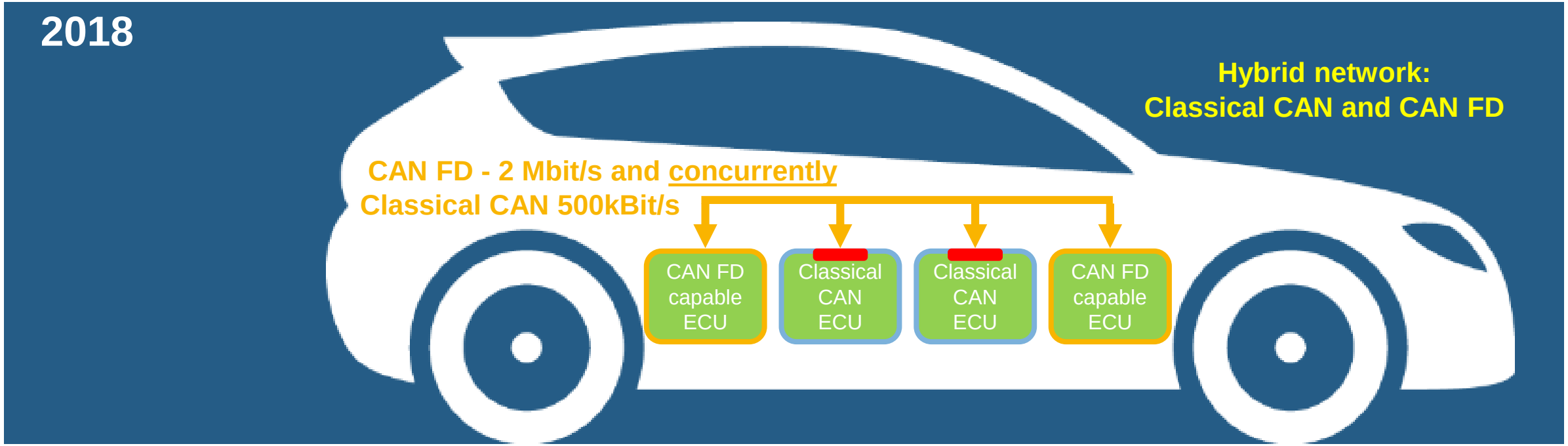
Mixing Classical CAN and CAN FD – FD shield

Classical CAN frames shall have the possibility to equally arbitrate against CAN FD frames

CAN FD frames shall not be destroyed by error frames from Classical CAN controllers

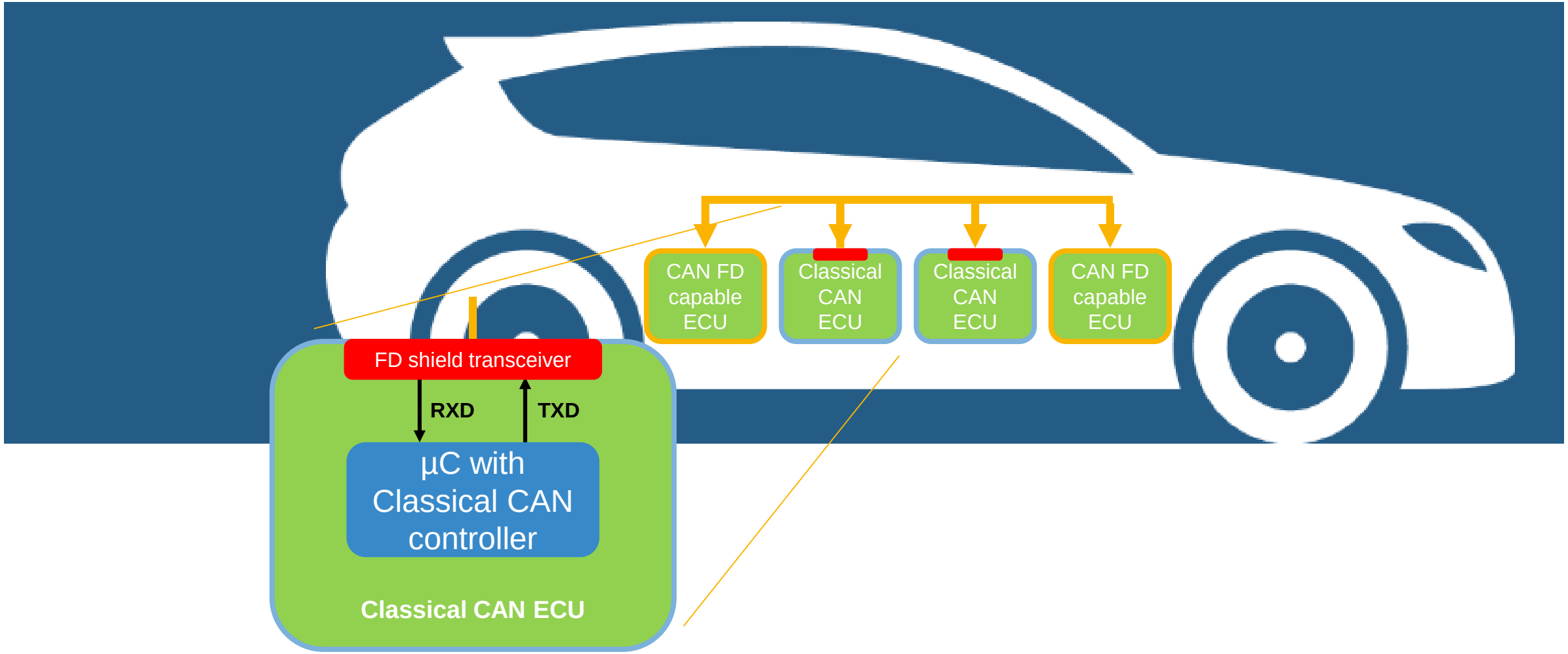
A “FD shield” transceiver is needed that keeps CAN FD frames away from Classical CAN controllers

Hybrid Networks for Full Operation

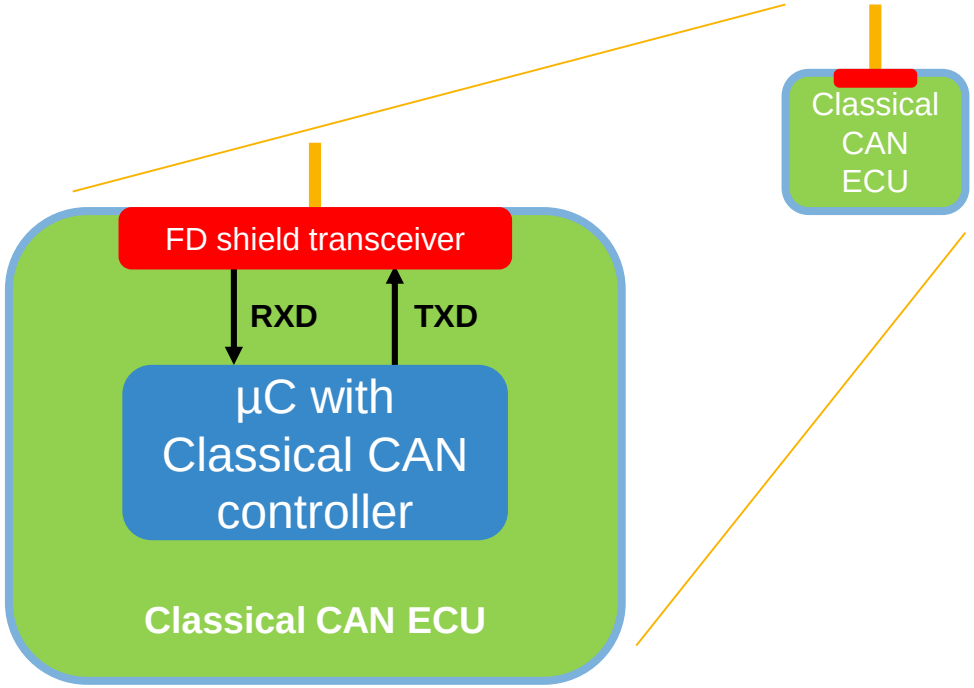


Mixing Classical CAN and CAN FD – FD shield	Autosar compatible – no additional SW efforts	Transceiver drop in replacement for standard transceivers	Data consistency shall be guaranteed – no frames lost	Error management shall work as defined in ISO11898-1	The compound of a Classical CAN controller and FD shield shall behave like a “CAN FD tolerant node” as defined in ISO11898-1

Hybrid Networks for Full Operation



FD Shield Operation

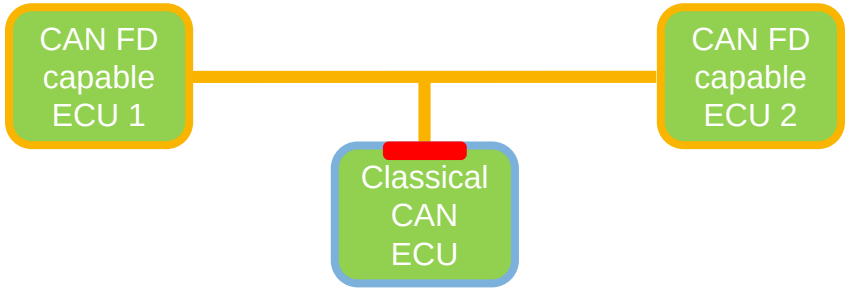


Standard transceiver in SO8 or SO14 replaced by FD shield transceiver

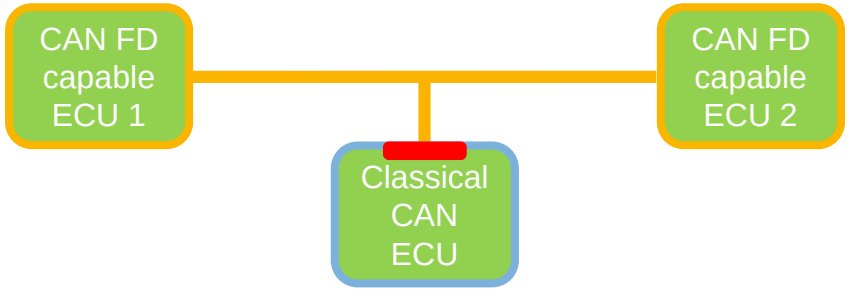
No change of µC

No change of printed circuit board

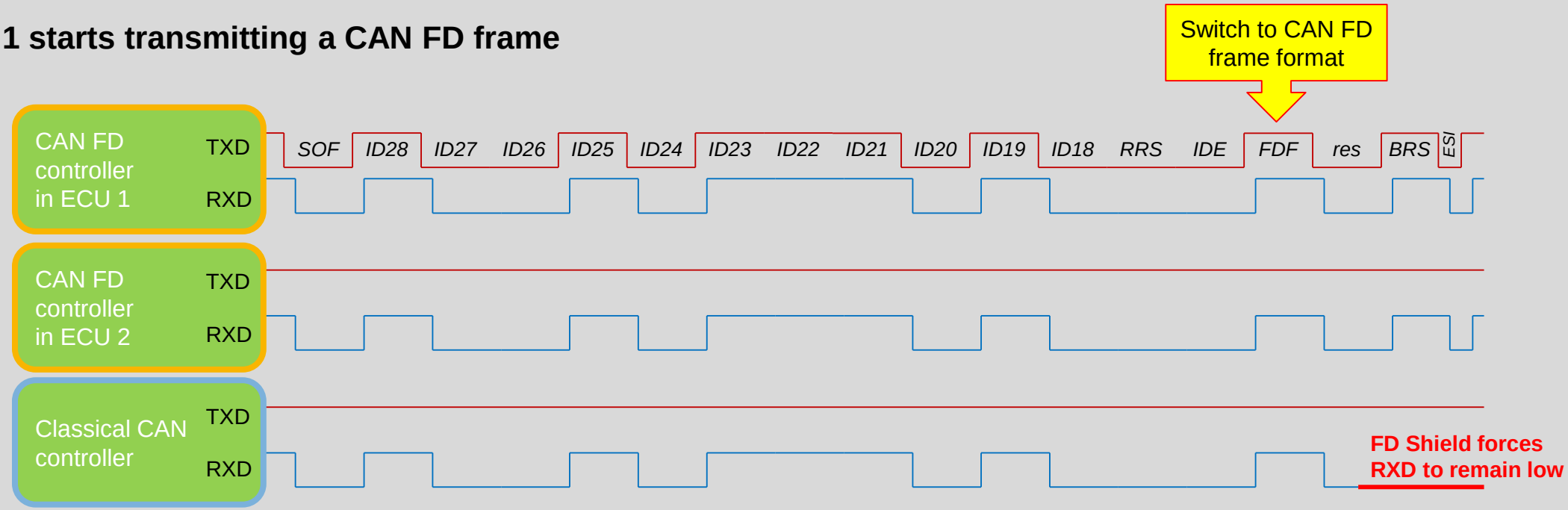
FD Shield Operation



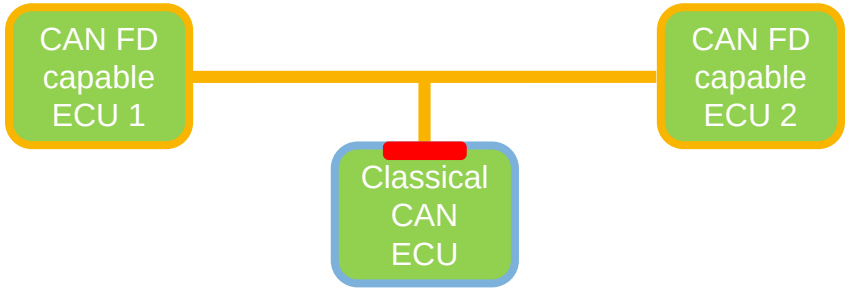
FD Shield Operation



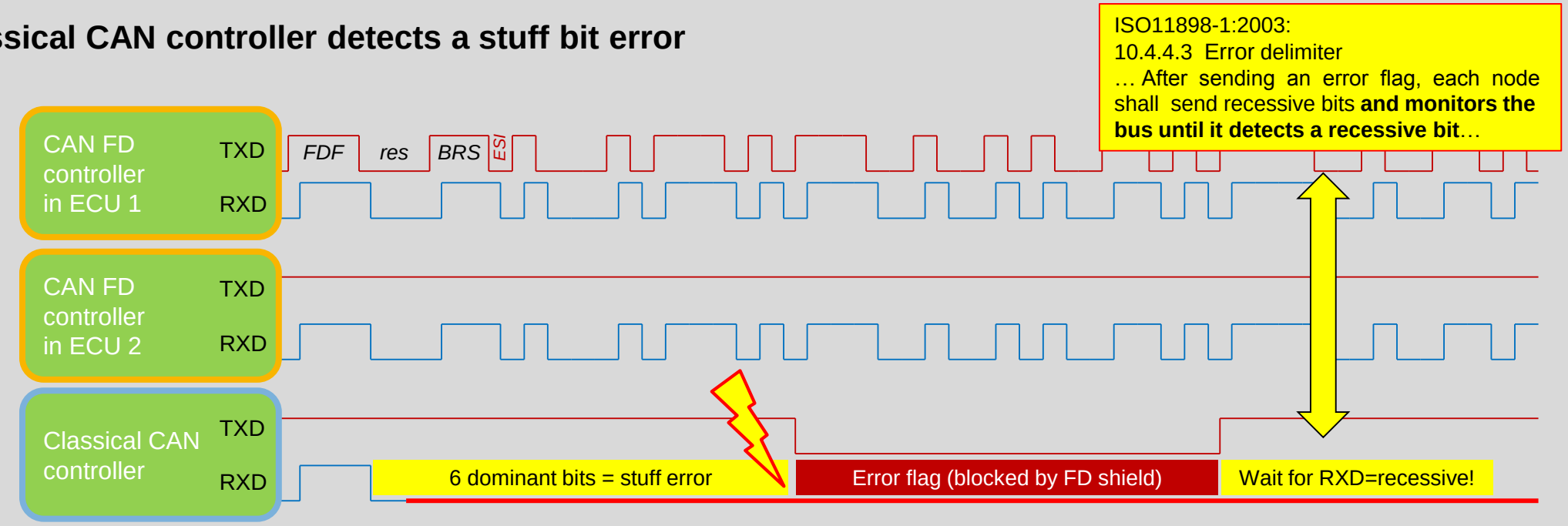
ECU 1 starts transmitting a CAN FD frame



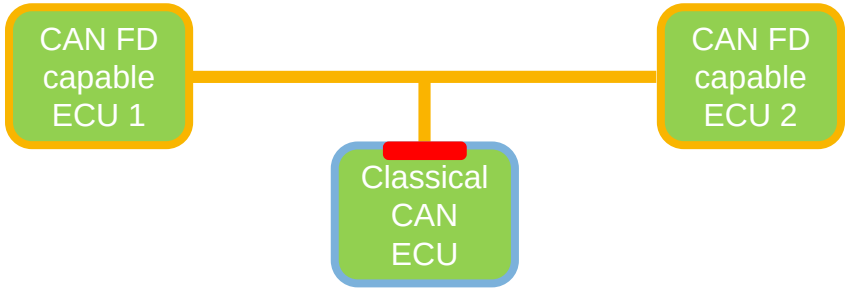
FD Shield Operation



Classical CAN controller detects a stuff bit error

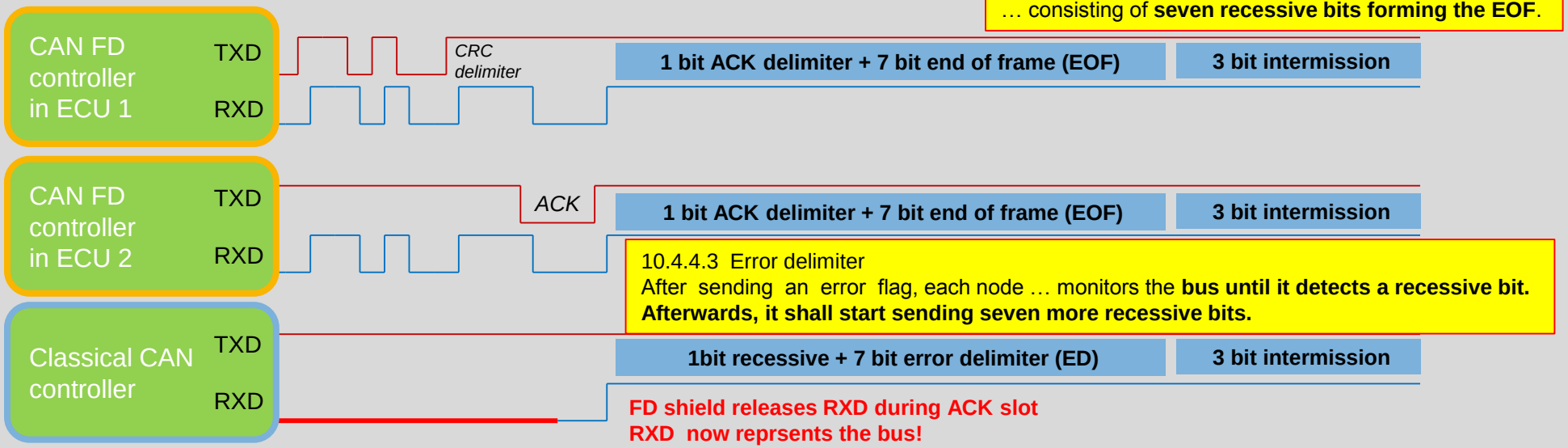


FD Shield Operation



All controllers are re-synchronize at “intermission”

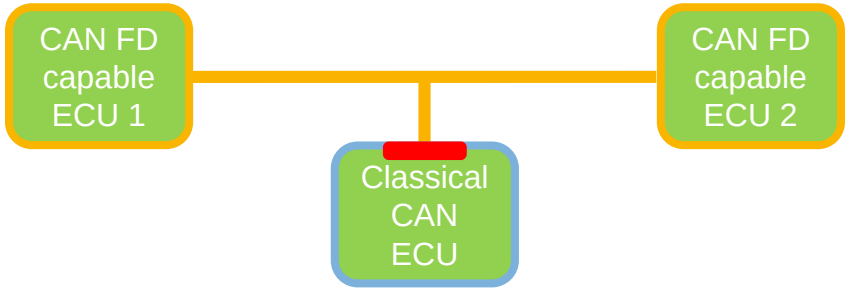
ISO11898-1:2003:
10.4.2.7 ACK field
…**The ACK delimiter, …, shall be a recessive bit.** …
10.4.2.8 EOF
… consisting of **seven recessive bits forming the EOF**.



10.4.4.3 Error delimiter
After sending an error flag, each node … monitors the **bus until it detects a recessive bit. Afterwards, it shall start sending seven more recessive bits.**

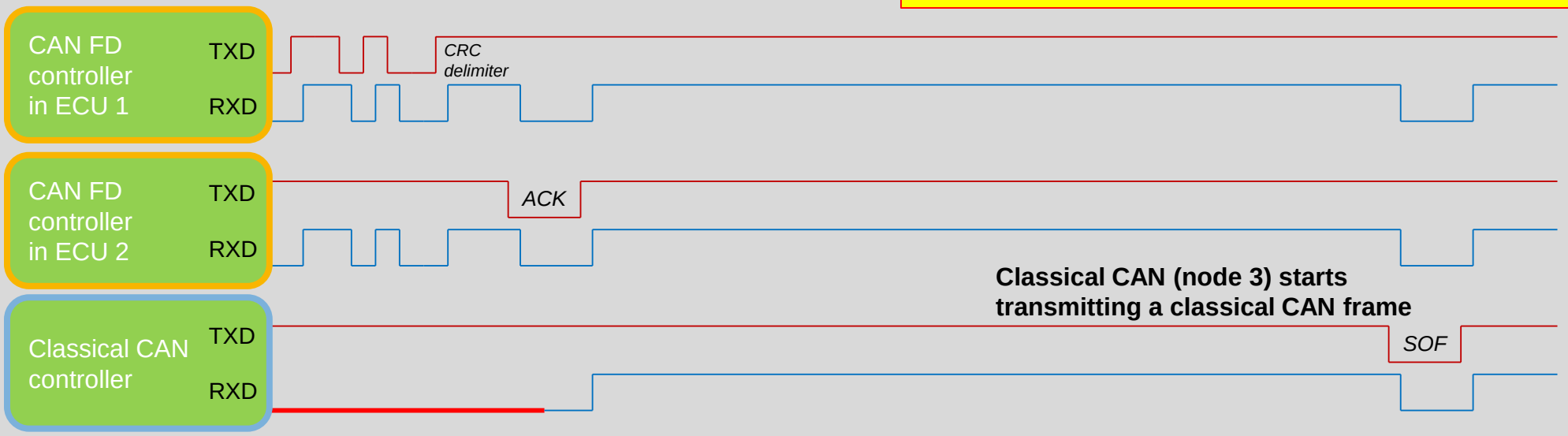
FD shield releases RXD during ACK slot
RXD now reprsents the bus!

FD Shield Operation



Equal arbitration between Classical CAN and CAN FD is possi

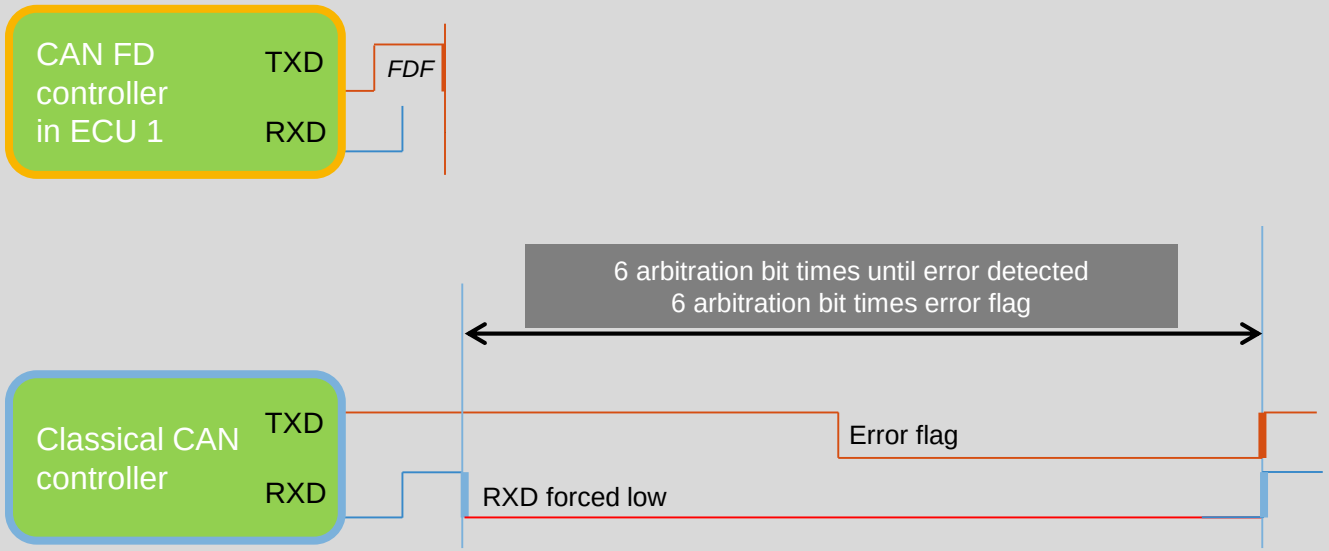
All nodes remain constantly synchronized
Classical CAN and CAN FD ECUs can immediately arbitrate to send the next frame
No interruption between messages
No complicated bit synchronisation



FD Shield Operation – Constraints

The CAN FD frame needs to be long enough to allow the Classical CAN node to complete its error handling

Minimum number of data bytes > (fast phase bit rate / arbitration bit rate) - 3



With 500kBit/s in arbitration phase

and 2000 kBit/s in fast phase:

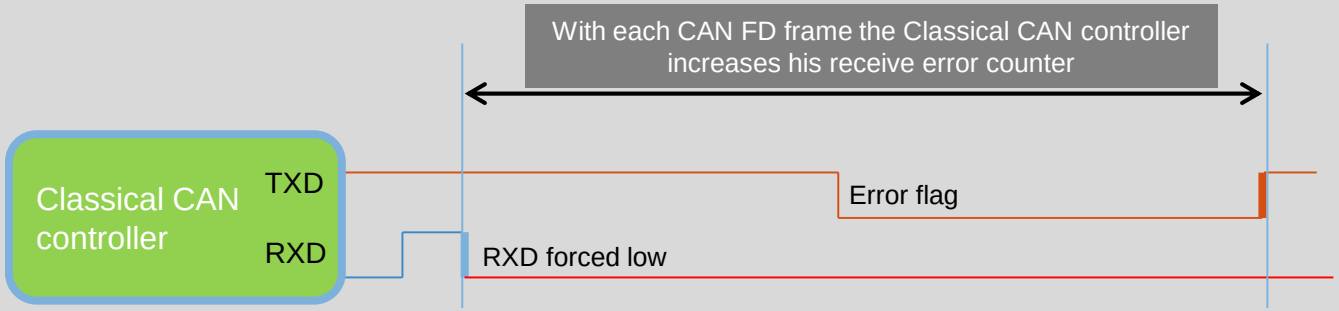
Min {number of data bytes} > (2000/500) - 3

Min {number of data bytes} = 2

FD Shield Operation – Error Management

The Classical CAN controller will toggle between being error passive and error active, depending on the ratio of CAN FD to Classical CAN frames

In case the Classical CAN controller has problems receiving a Classical CAN frame while being error passive it cannot enforce the repetition of that Classical CAN frame. Therefore FD shield takes over the error management!



Industry Support and Validation of FD Shield

Full ISO conformance of FD Shield technology

Collaboration with C&S (conformance testing house),
confirming FD Shield's compliance to all rules of ISO11898-1 and -2.
Test vs. ISO "CAN FD Tolerant" specification successful
Expert evaluation of NXP's FD Shield Technical Paper **confirming No Issues!**

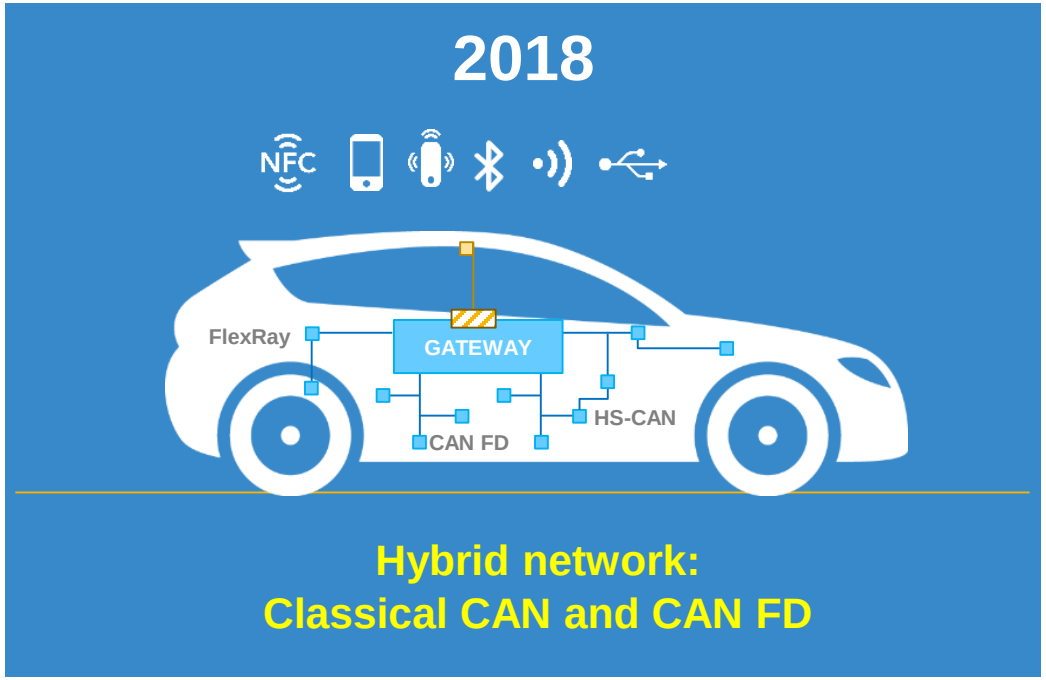
Fully compatible with AUTOSAR

Vector (expert AUTOSAR software supplier) evaluating NXP's FD Shield's operation in combination with AUTOSAR SW stack, ensuring seamless operation of Classical CAN and CAN FD networks.

Network analysis tools to evaluate CAN FD adoption available as part of Vector toolchain CANoe:

Enables analysis of partial upgrade to CAN FD to assess bandwidth improvement impact.
Can utilize real world test data or simulated network as inputs.

Summary and Key Messages



Enabling Classical CAN and CAN FD ECUs to co-exist on the same bus can save the automotive value chain a lot of work when moving to higher bandwidth in vehicles

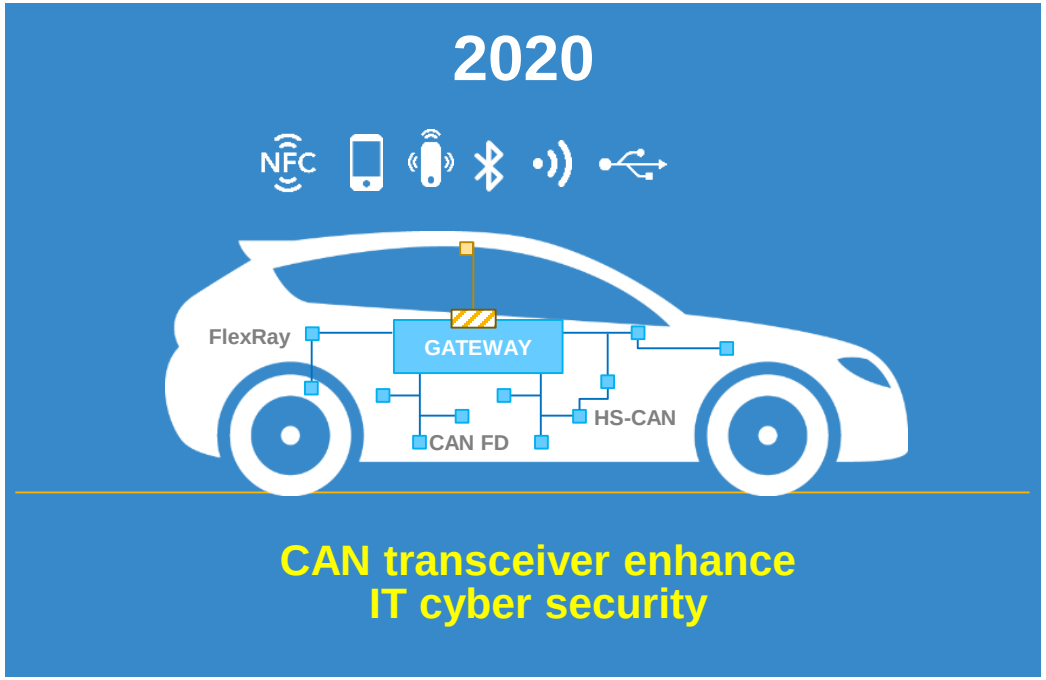
Hybrid networks provide more elegant solutions considering scalability, security and investments

FD Shield enables this co-existence, as a drop-in replacement CAN transceiver, making Classical CAN ECUs “CAN FD tolerant”, without any further hardware or software changes

More than a purely theoretical solution, FD Shield is validated by key industry partners against ISO and AUTOSAR for compliance, and available in silicon implementation

Existing CAN networks can be analyzed with off-the-shelf tooling for upgrading options, simulated within tools like Vector’s CANoe and realized with NXP’s FD Shield

Outlook to Further Smart Transceiver Functions



FD shield implements a filter for CAN FD frames, but can also be used differently	The filter can also be used to filter “unwanted” messages	Thus FD shield will be further developed as simple intrusion detection and prevention system **“Stinger”**	**Stinger** mitigates the effect of cyber attacks without cryptography by enforcing certain policies	**Flooding prevention prevents a denial of service attack**	**Spoofing protection and tamper protection can be realized**	**The physical layer is the last line of defense !**

Contacts

Questions?

FD shield contacts:

- Ron.Timmermans@nxp.com – Product Marketing Manager
- Bernd.Elend@nxp.com – Technical Expert

SECURE CONNECTIONS
FOR A SMARTER WORLD

ATTRIBUTION STATEMENT