FTF 2016
TECHNOLOGY FORUM

TRENDS IN VEHICLE ARCHITECTURES

FTF-AUT-N1813

ROBERT MORAN
AUTOMOTIVE CONNECTIVITY & SECURITY SYSTEMS
FTF-AUT-N1813
MAY 17, 2016
ROBERT.MORAN@NXP.COM

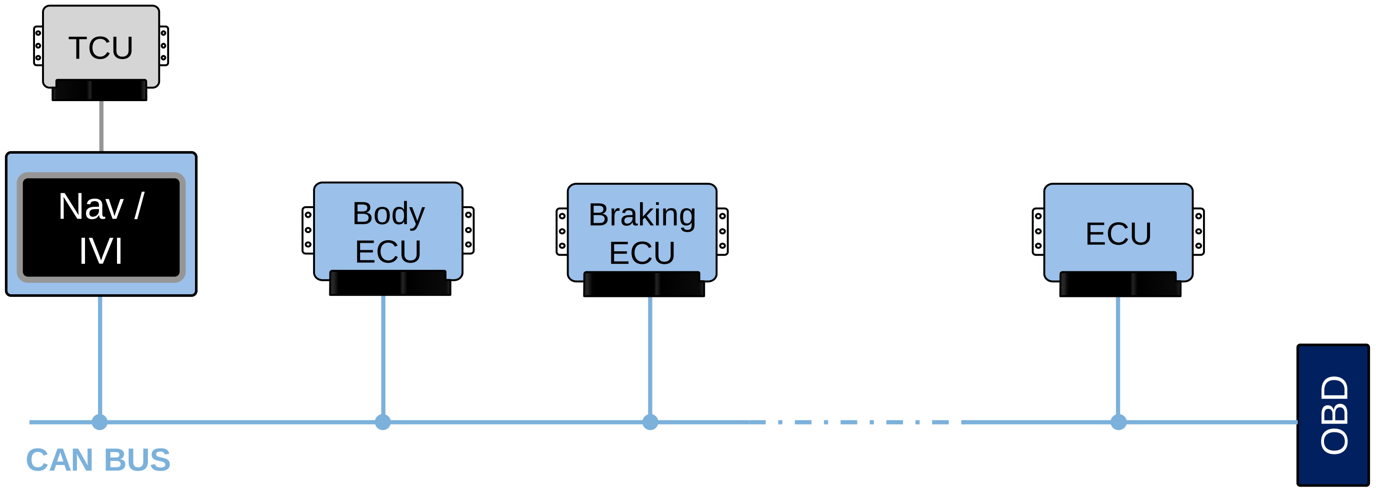
PUBLIC USE

AGENDA

- Trends in Vehicle Architecture
- Security of Vehicle Architecture
- Network Protocol Security
- Firmware Over-The-Air (FOTA)

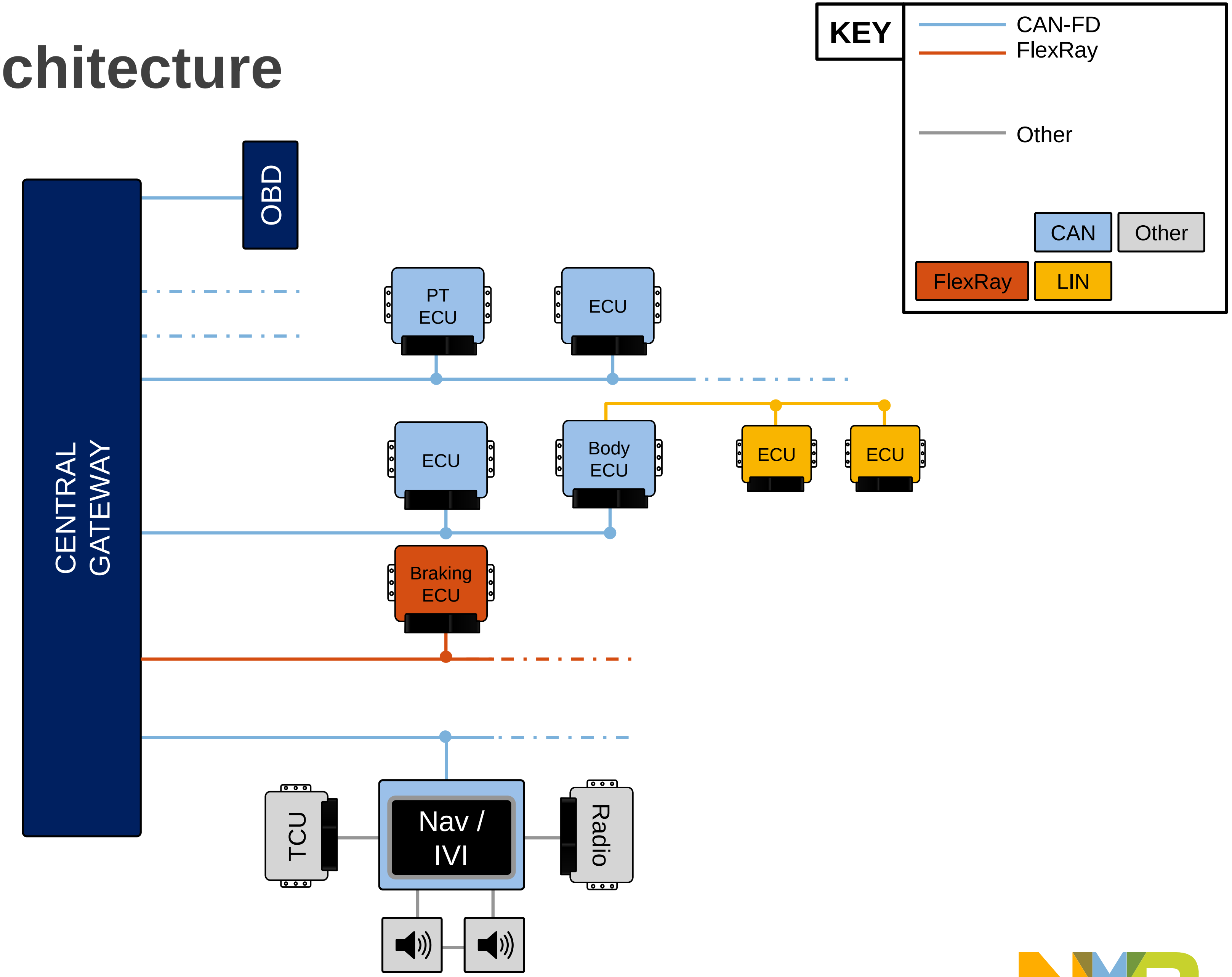
Evolution of Vehicle Architecture

- Flat bus architecture
  - Single / Twin CAN bus
  - Simple
- Security weakness
  - Shared medium between safety & non-safety ECUs
- Scalability limited
  - BW ÷ #ECUs



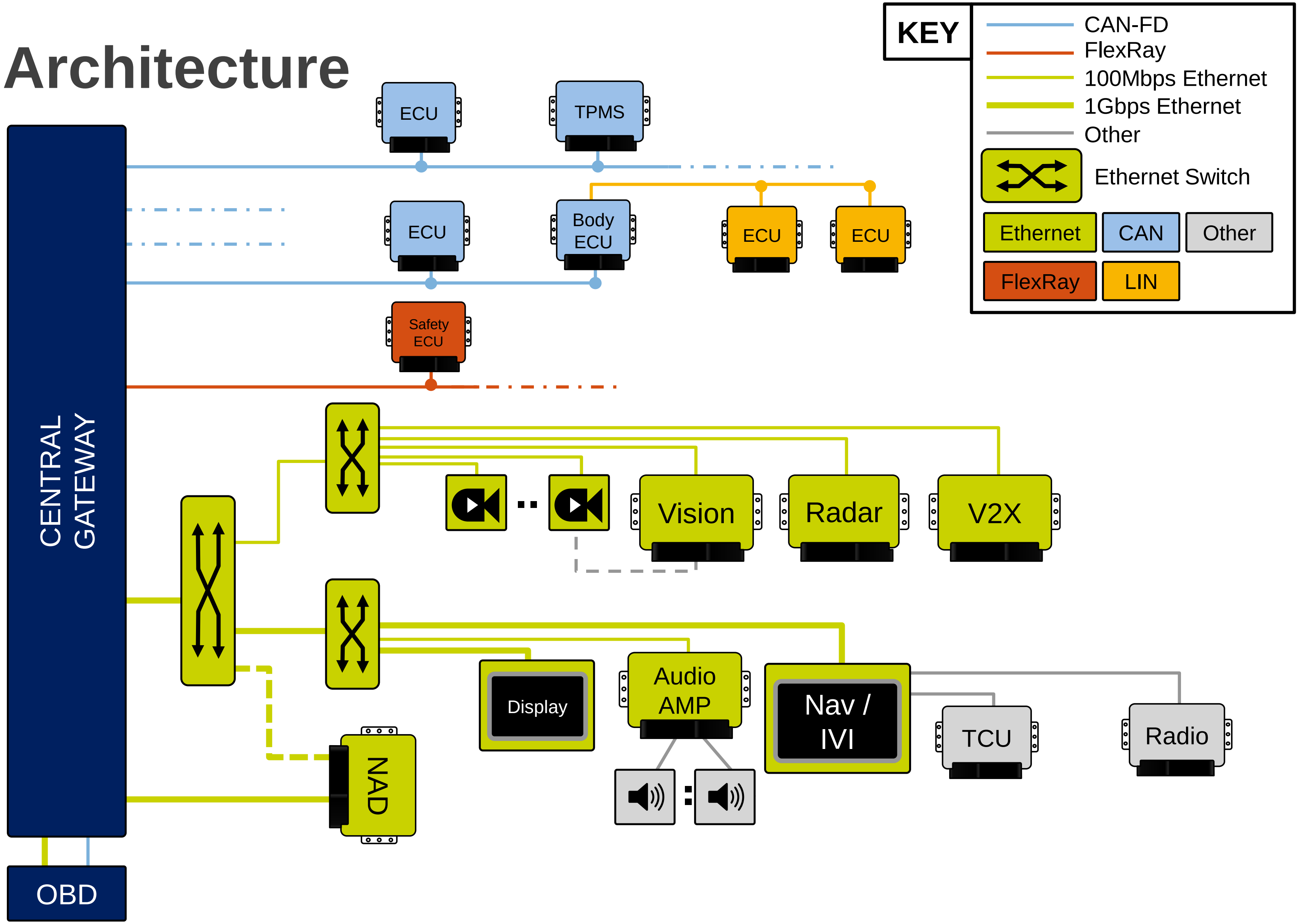
Evolution of Vehicle Architecture

- CAN Central Gateway architecture
  - Typically 3-8 CAN networks
  - Typically 1-2 FlexRay networks
- Increased bandwidth
  - but, small compared to consumer / networking world
  - Proprietary protocols for higher bandwidth (e.g. MOST)
- Physical Isolation
  - Functional domains
  - Safety / Non-safety
- Gateway role
  - Firewall internal traffic
  - Protocol translation



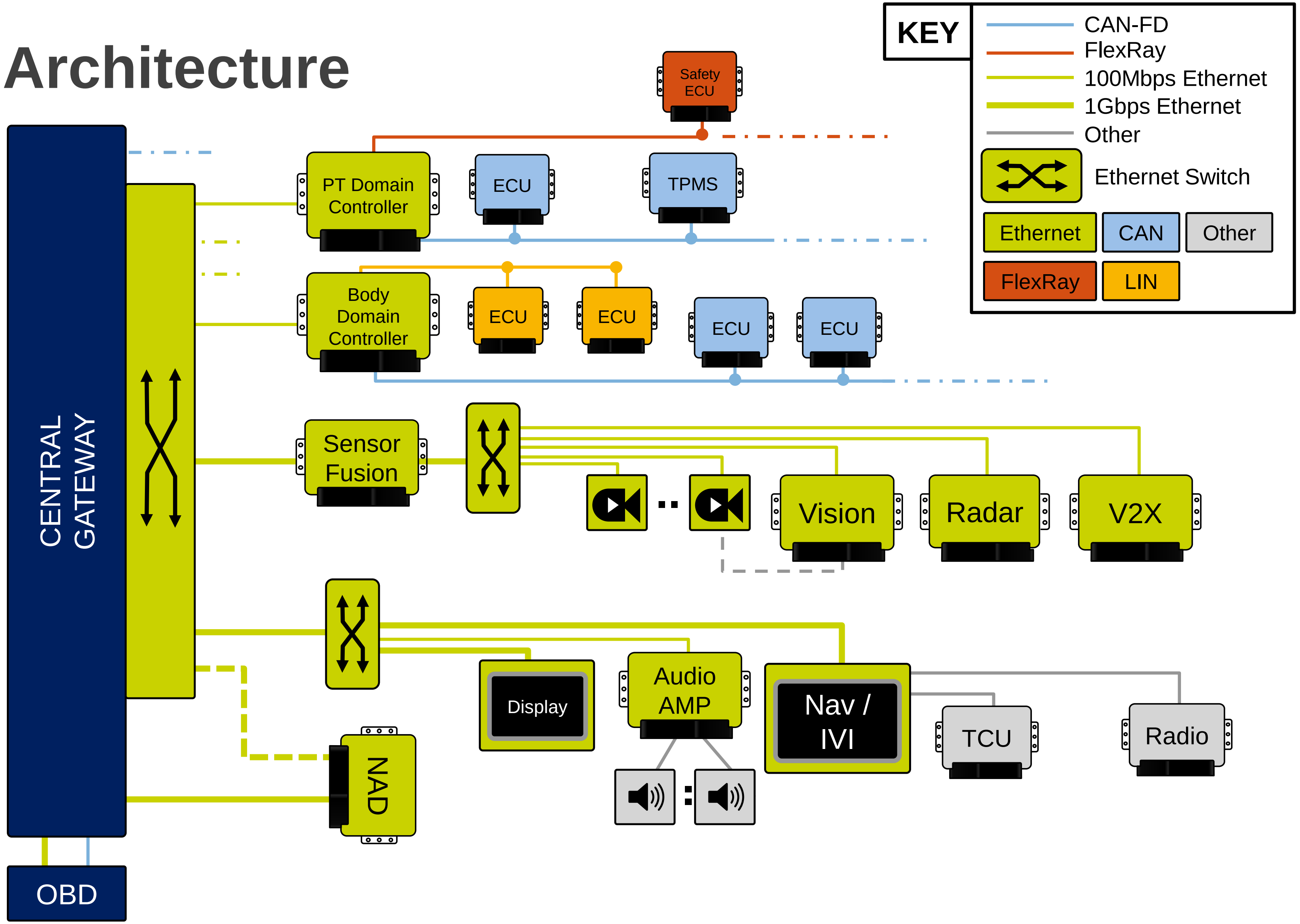
Evolution of Vehicle Architecture

- Hybrid Ethernet architecture
  - CAN, FlexRay & Ethernet
- High bandwidth
  - 100Mbit / 1Gbit Ethernet
  - Improved ECU program time in factory
- Gateway role
  - Firewall internal & external
  - Efficient protocol translation
  - ECU consolidation



Evolution of Vehicle Architecture

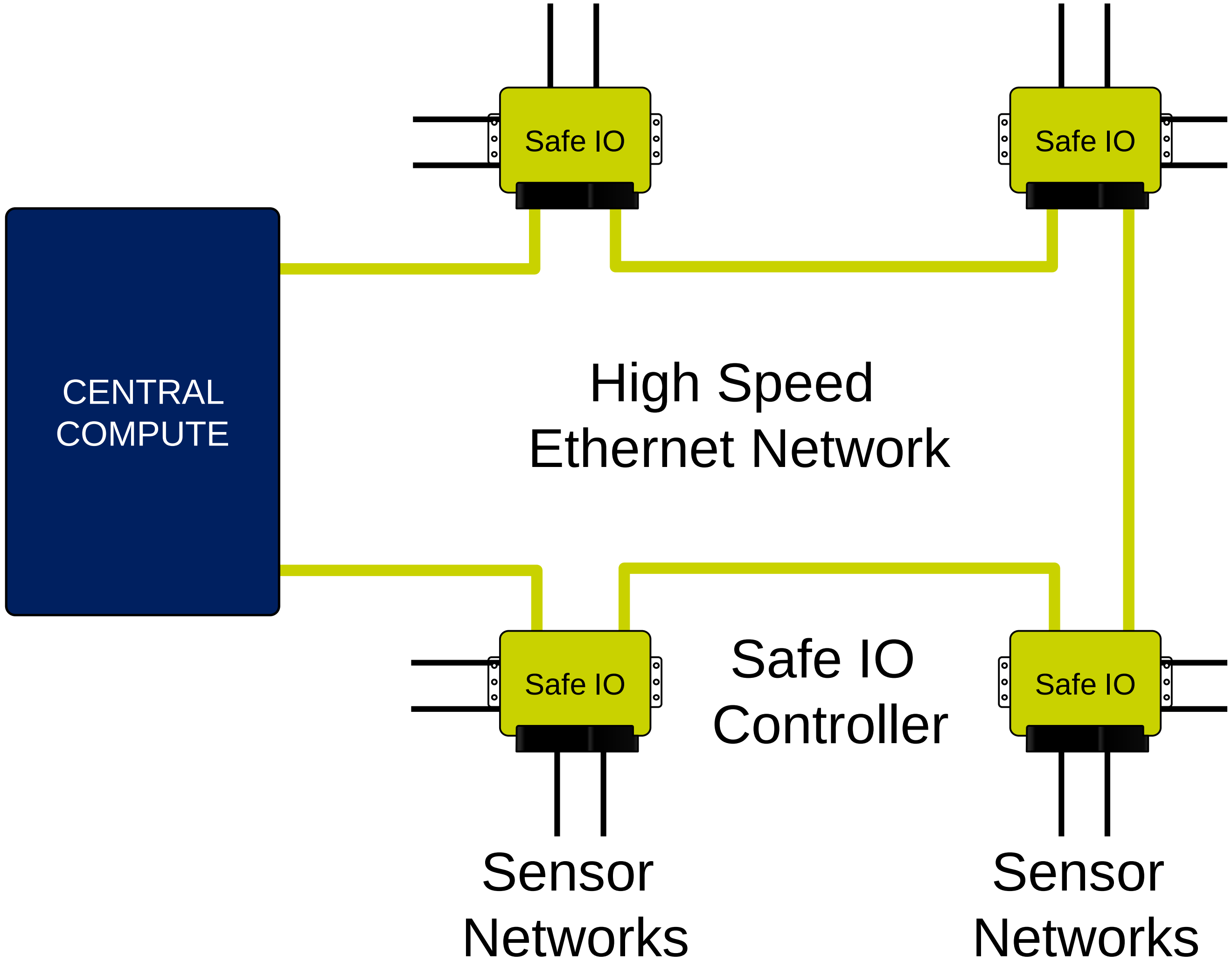
- Ethernet Backbone with Domain controllers
  - ECU consolidation
  - Distributed gateway
- Determinism over Ethernet
  - Time Sensitive Networking (TSN)
- High performance firewall



Evolution of Vehicle Architecture

- Central Compute Platform
  - High performance compute
  - Distributed safe IO processing

- High performance network
  - Bandwidth / Latency
  - Determinism
  - Strong firewall & security



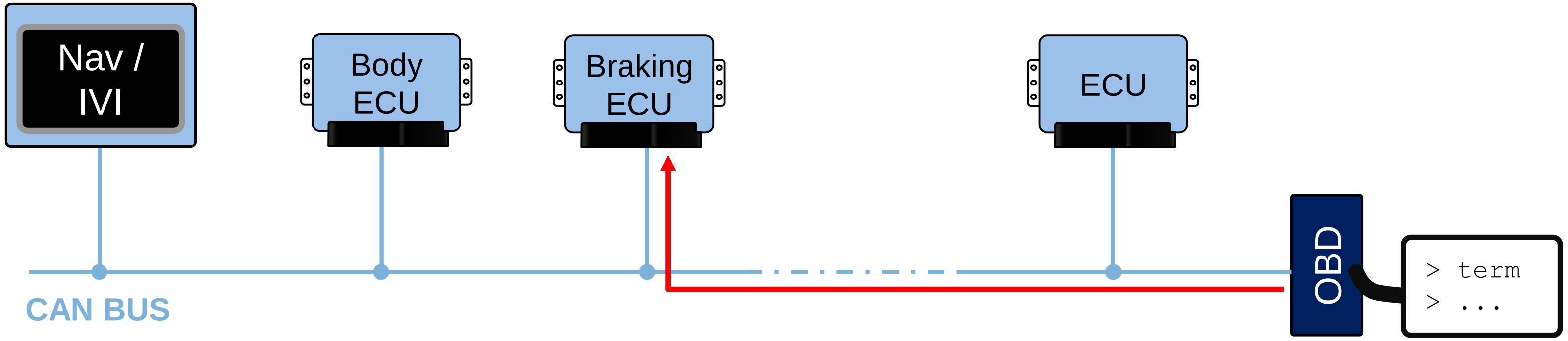
SECURITY OF VEHICLE ARCHITECTURE

Flat Architecture: Vulnerabilities

- Wide attack surface
  - OBD port direct onto network
  - One hacked ECU can access entire network

- No monitoring of bus traffic

- No firewall of traffic to safety ECUs

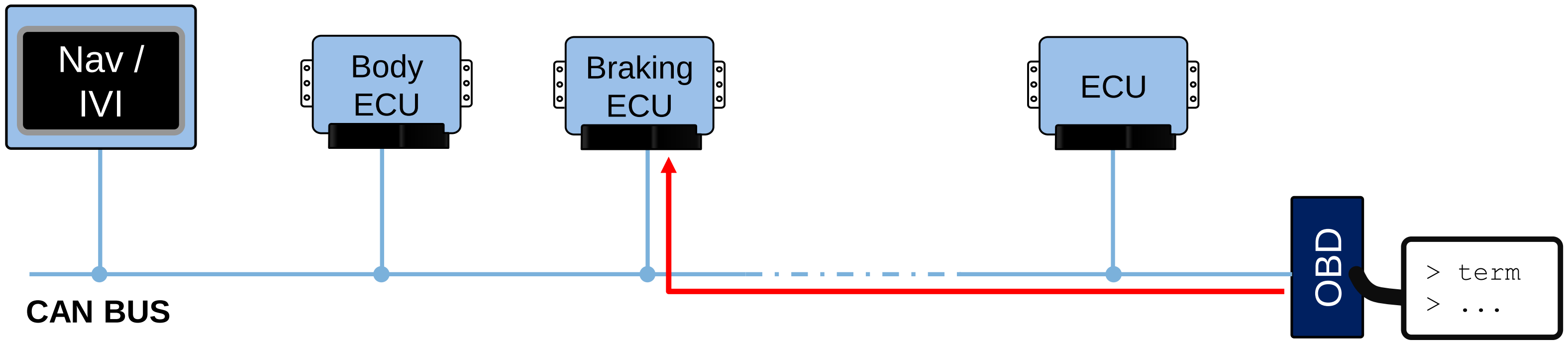


```
> term
> ...
```

Flat Architecture: Physical Attack

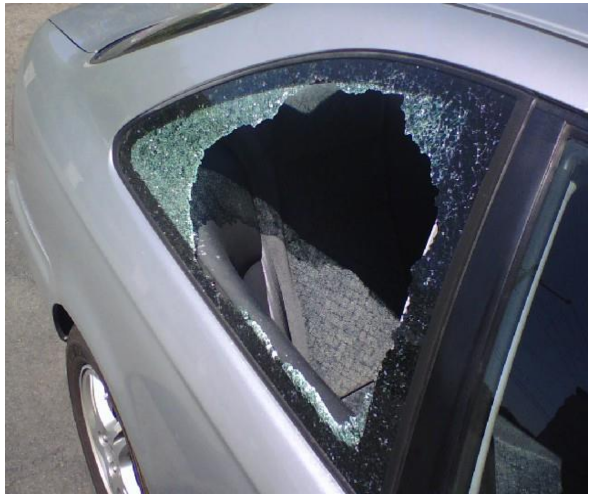
- Physical access required to attack
  - OBD port in cabin
  - CAN bus in wing mirror

- Gains?
  - Visible damage



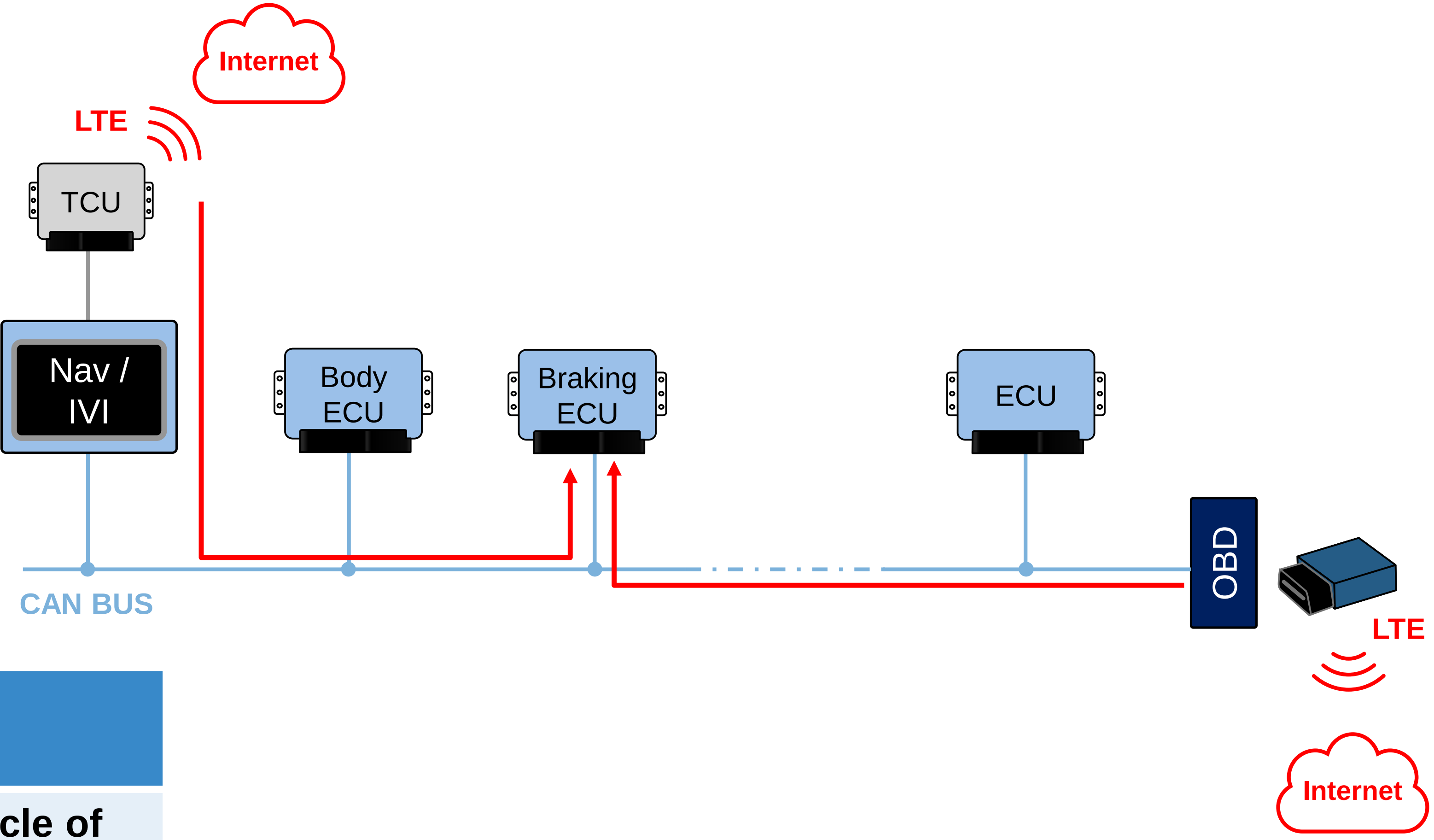
```
> term
> ...
```

Hackers Motivation	Risk of occurring	Impact	Comments
Direct harm to occupants	Low	Single vehicle	e.g. Cannot remotely trigger brakes. Could plant a virus
Theft of vehicle / contents	High	Single vehicle	Easier than a brick through window?
Theft of OEM software	High	All models of vehicle	Basic security on ECU could prevent (e.g. secure boot)



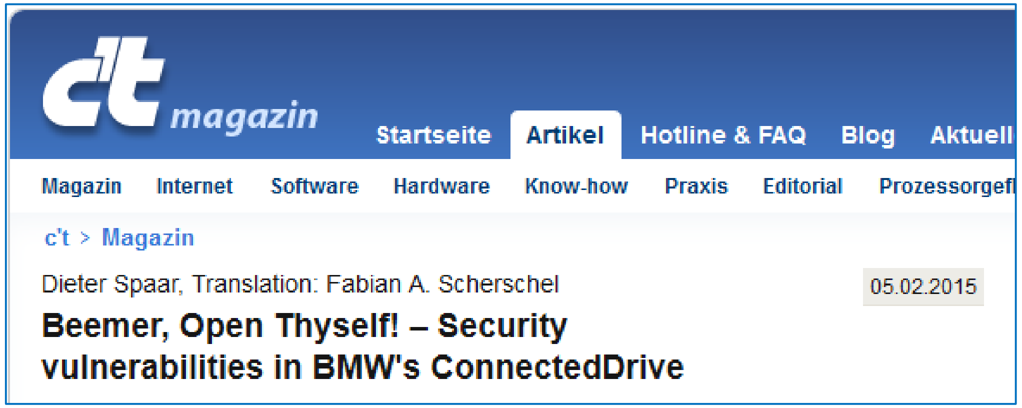
Flat Architecture: Remote Attack

- Remote attack coming into the mainstream
  - Telematics Control Unit (TCU) for entertainment / apps
  - 3rd Party Connected OBD dongles for insurance, fleet, eco-driving, etc…



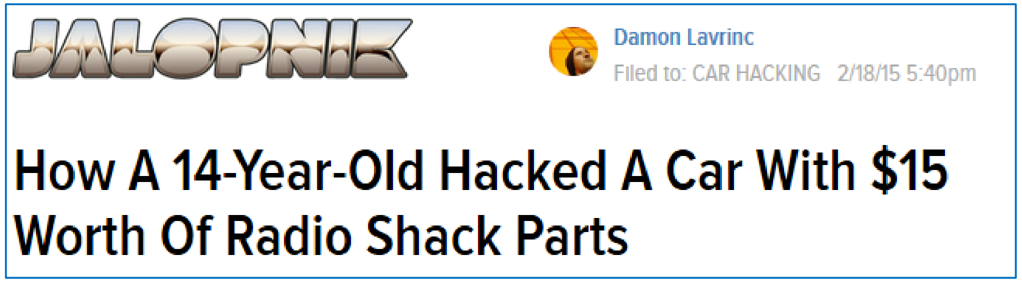
Hackers Motivation	Risk	Impact
Direct harm to occupants	High	**Any vehicle of same model**

Remote Attacks Are Happening…



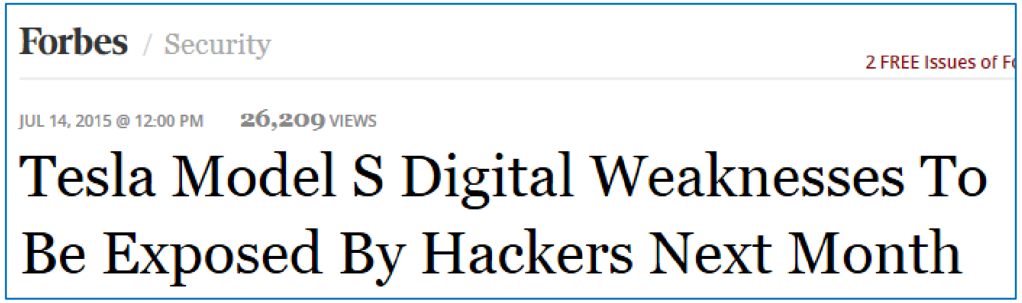
Dieter Spaar, Translation: Fabian A. Scherschel 05.02.2015

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



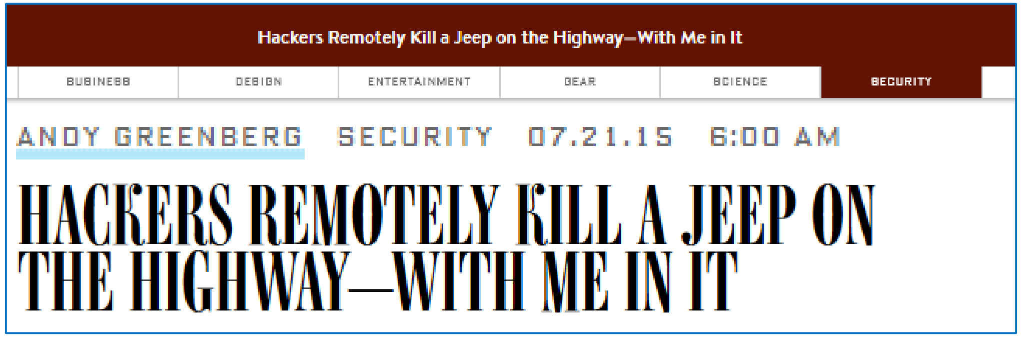
Damon Lavrinc
Filed to: CAR HACKING 2/18/15 5:40pm

How A 14-Year-Old Hacked A Car With $15 Worth Of Radio Shack Parts



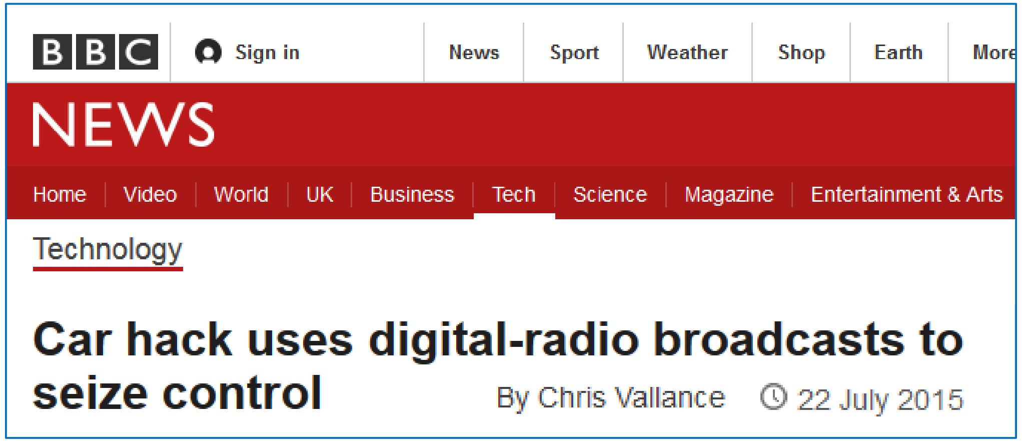
JUL 14, 2015 @ 12:00 PM 26,209 VIEWS

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



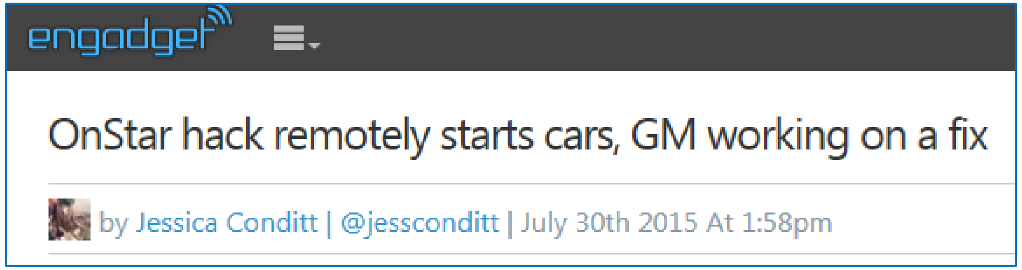
ANDY GREENBERG SECURITY 07.21.15 6:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT



Car hack uses digital-radio broadcasts to seize control

By Chris Vallance 22 July 2015



OnStar hack remotely starts cars, GM working on a fix

by Jessica Condit | @jesscondit | July 30th 2015 At 1:58pm

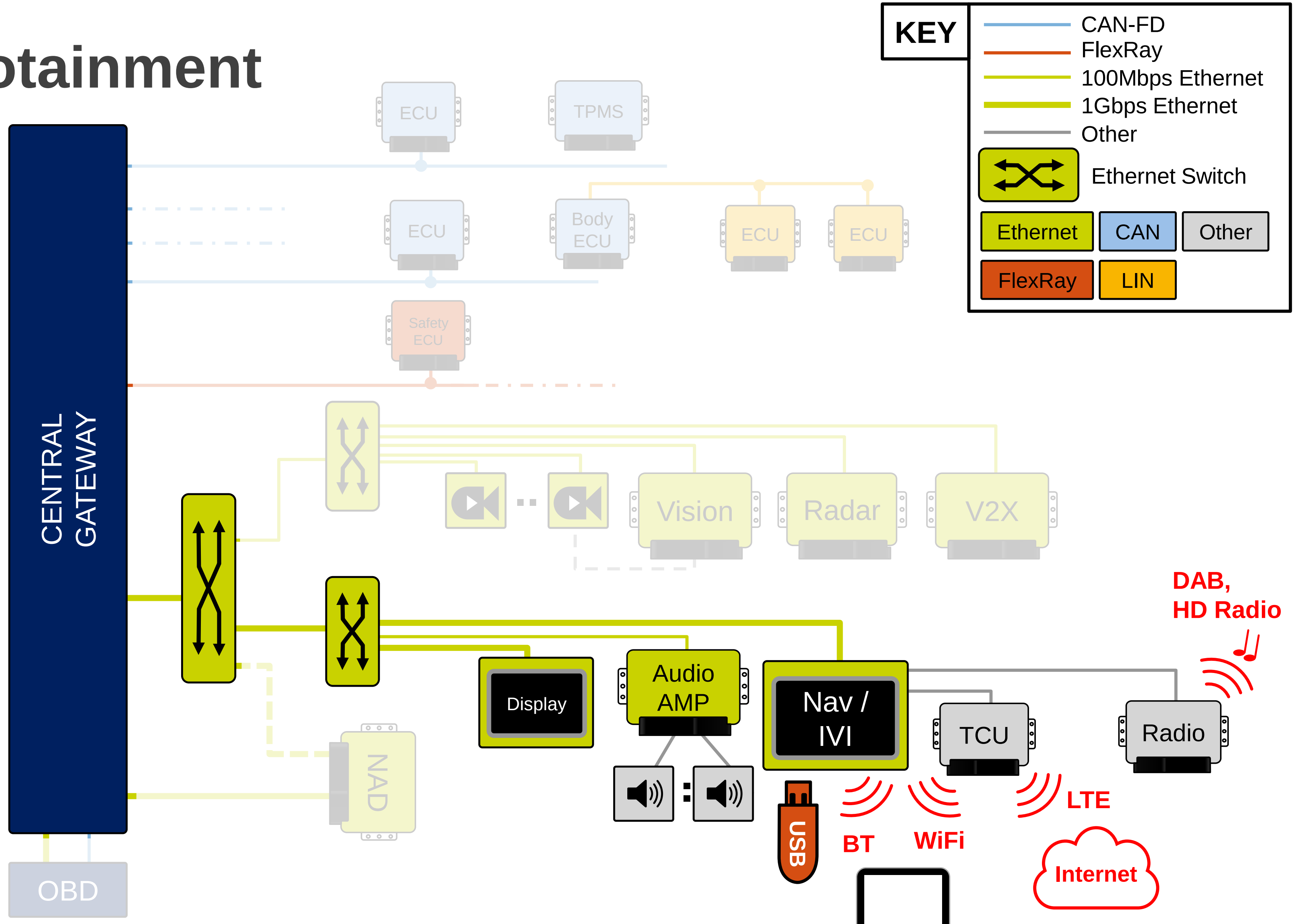
Remote Attacks: Infotainment

- Range of connected interfaces & features

I/F	Cellular (e.g. LTE)
Use Case	Internet, Video & Audio stream
Range	(1) Anywhere (Remote IP address) (2) KMs (Spoof cell tower)

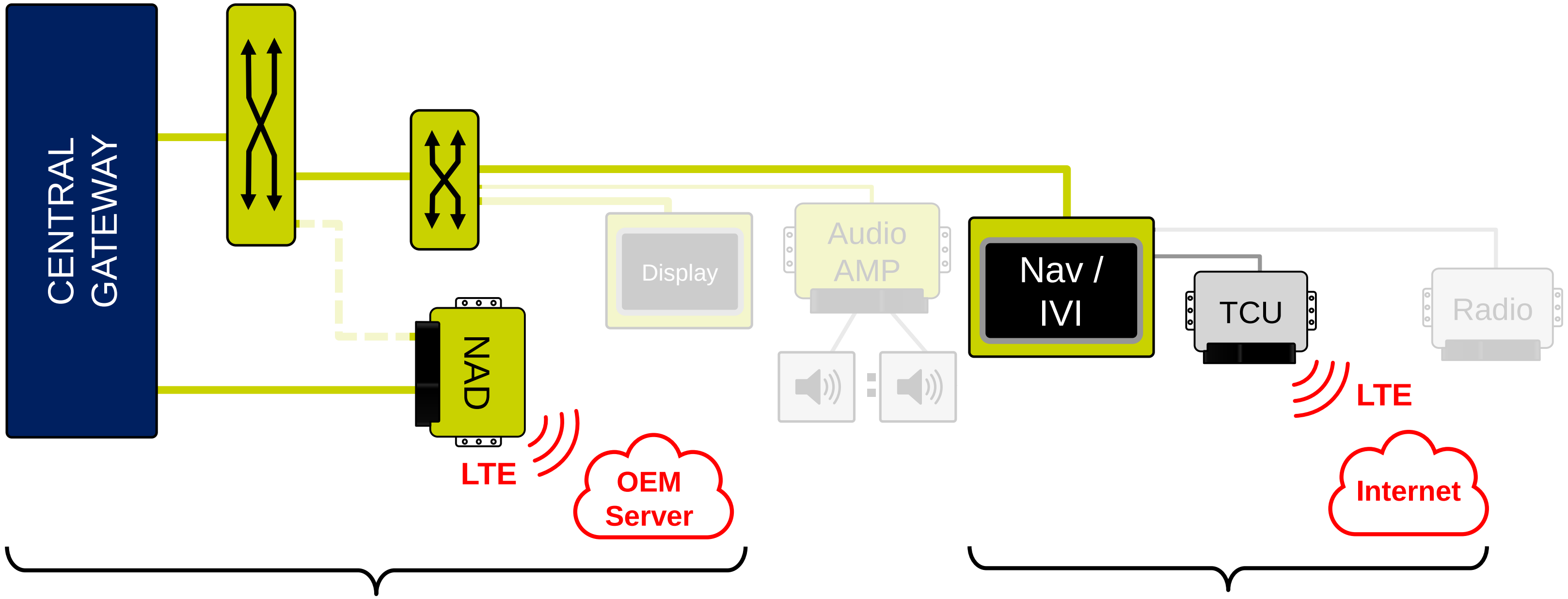
I/F	WiFi
Use Case	Hotspot, Carplay, Android Auto
Range	<30M

I/F	Digital Radio (DAB, HD-Radio)
Use Case	Radio, Digital Service (backdoor)
Range	KMs (DAB transmitter)



Connected Apps Location

- New OEM services being introduced to vehicles
  - Firmware Over-The-Air (FOTA)
  - Big Data
- Requires strong security
- Trusted: Gateway
  - Dedicated NAD
  - OEM software only
- Untrusted: IVI
  - Many 3rd Party SW
  - User Interface/Interaction



OEM Apps Only
(e.g. FOTA, Big Data)

Trusted

3rd party Apps (e.g. Spotify, Pandora)

Untrusted

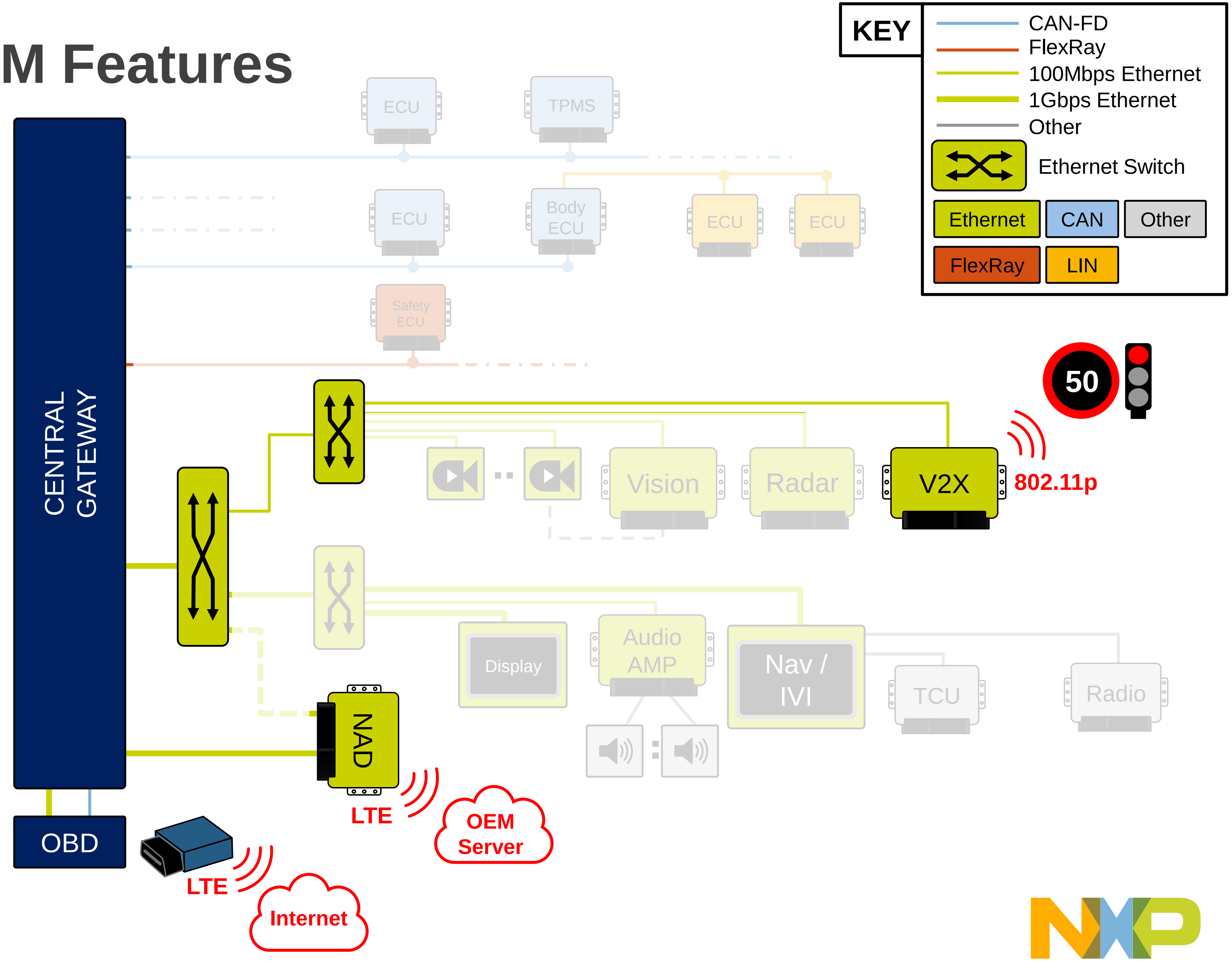
Remote Attacks: OEM Features

- New connected features being introduced by OEMs

I/F	NAD – Cellular (e.g. LTE)
Use Case	Over-the-Air Updates, Big Data
Range	(1) Anywhere (Remote IP address) (2) KMs (Spoof cell tower)

I/F	DSRC – 802.11p
Use Case	Vehicle to Infrastructure, Vehicle to Vehicle
Range	< 2KM

I/F	3rd Party OBD - Cellular (e.g. LTE)
Use Case	Insurance, Fleet, Eco-driving
Range	(1) Anywhere (Remote IP address) (2) KMs (Spoof cell tower)

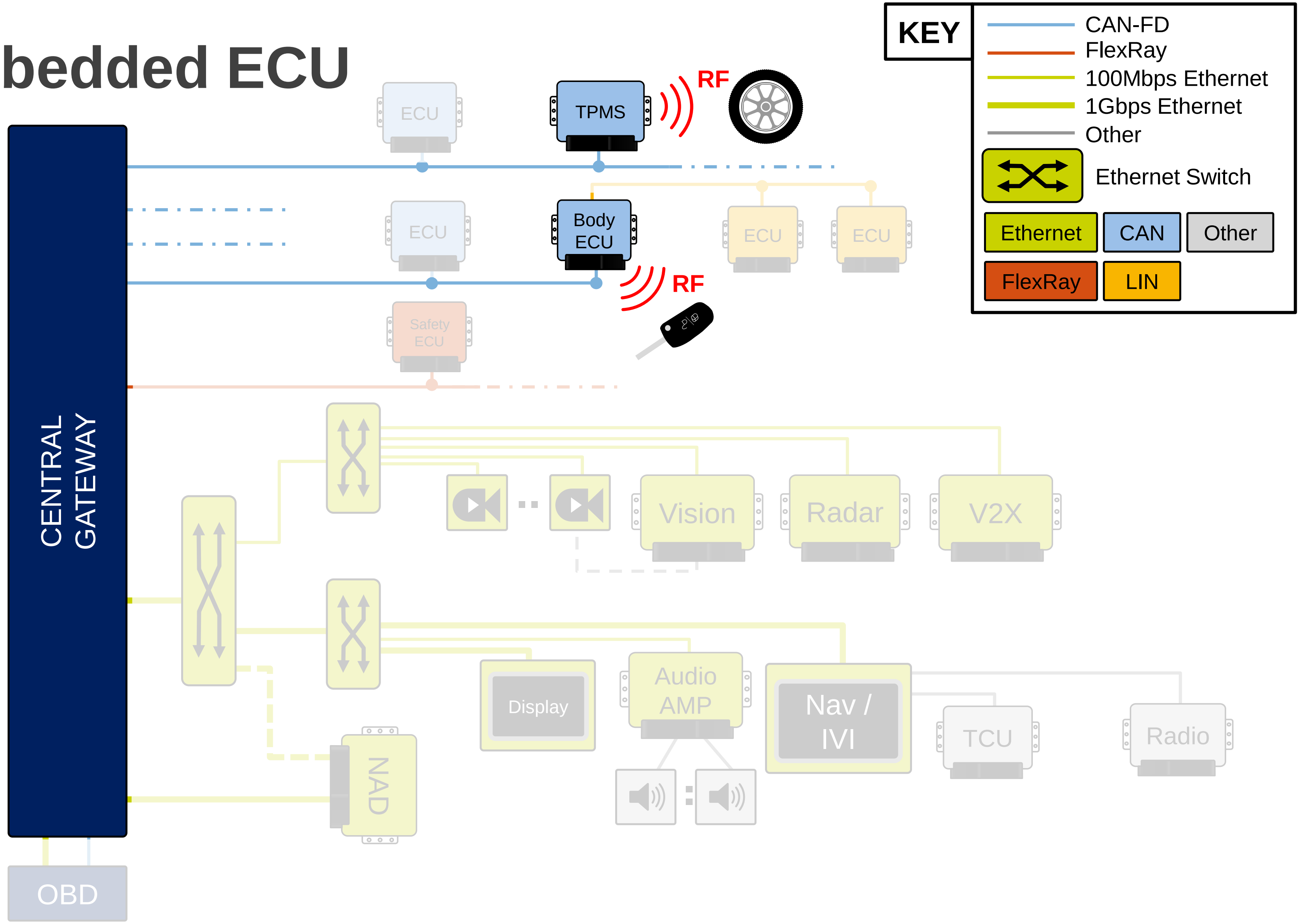


Remote Attacks: Embedded ECU

- Wireless interfaces for highly embedded systems could expose backdoor

I/F	TMPS – Low Freq RF
Use Case	Tire Pressure Monitoring System (TMPS)
Range	<10M

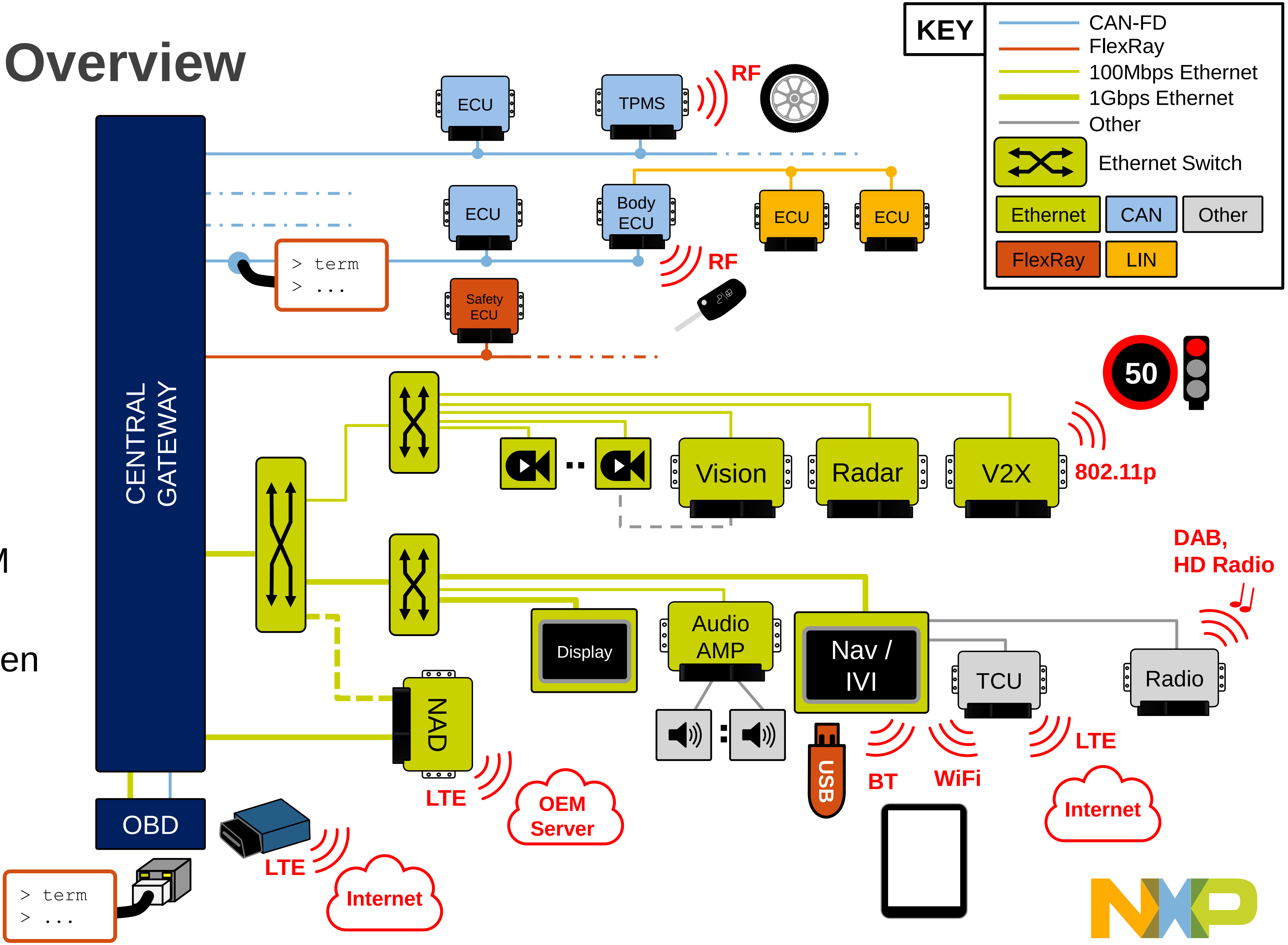
I/F	RKE - RF
Use Case	Remote Keyless Entry
Range	<100M



Remote Attacks: Overview

- Wide Range of Remote Entry Points
  - Range limitations to be considered
  - Analysis vs Direct Manipulation

- Central Gateway
  - Physical Isolation
  - Secure location for OEM connected applications
  - Strong firewalling between sub-networks is key
    - Stateless & Stateful

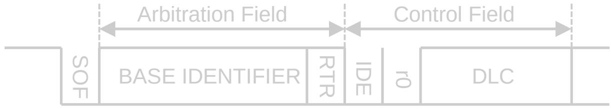


NETWORK PROTOCOLS

The ‘traditional’ Automotive Protocols

CAN Classic

Classic CAN Base Format



Unsecure Payload

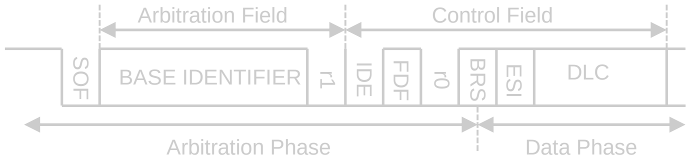
Data

8-bytes

Effective Data Rate @ 500kHz ~ **4MB/s**

CAN-FD

CAN FD Base Format



Secure Payload

Data	CMAC (full/truncated)
8-bytes	16-bytes

Effective Data Rate @ 1.5MHz ~ **4MB/s**

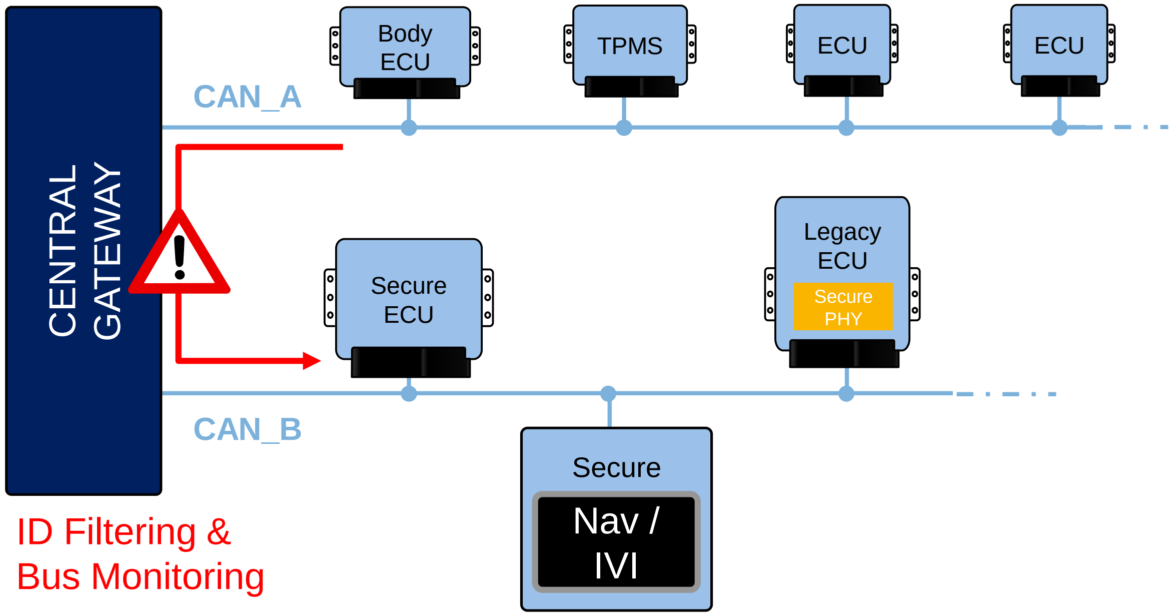
- Traditional Network Protocols
  - LIN, FlexRay, etc…
  - CAN is dominant for vehicle network

Protocol	Max Payload Data Rate	Max Payload Size
CAN (Classic)	1MBit/s	8-bytes
CAN-FD	2MBit/s (runtime) 5MBit/s (diag.)	64-bytes

- CAN has no security requirements in protocol
  - AutoSAR SecOC provides methods for integrity / authentication of PDU in CAN payload
    - Full or Truncated CMAC

Gateway Firewall of CAN traffic

- Static Firewall
  - Static ID filter in GW will provide isolation between buses
- Stateful Firewall
  - Bus snooping monitors characteristic of traffic & detects anomalies
    - Intrusion Detection System (IDS)

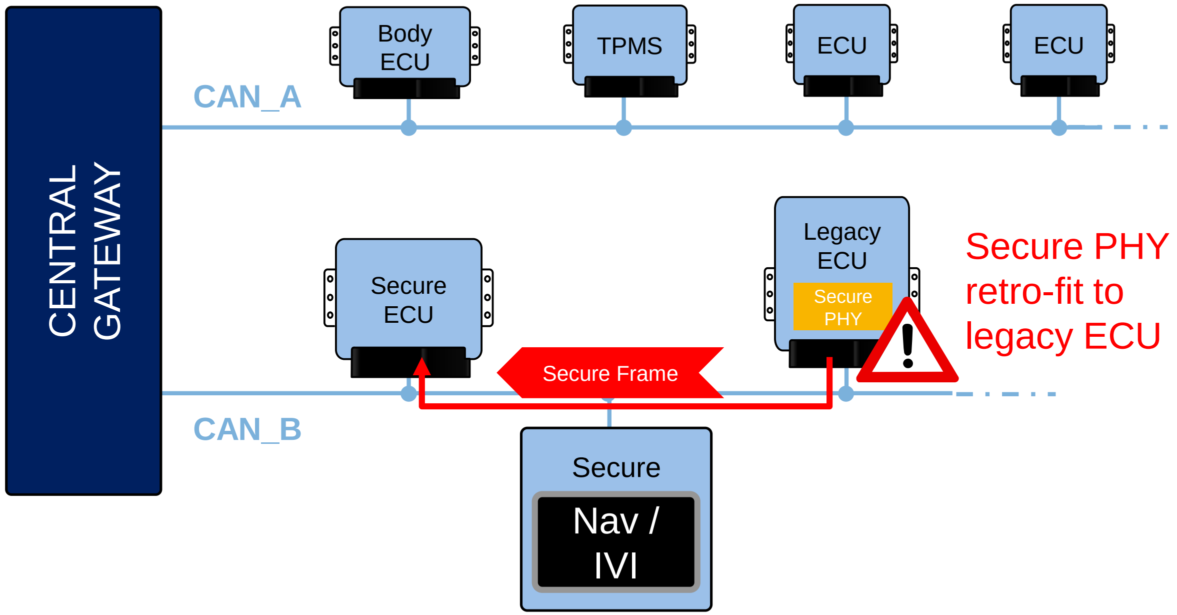


ID Filtering & Bus Monitoring

Challenges of Securing CAN

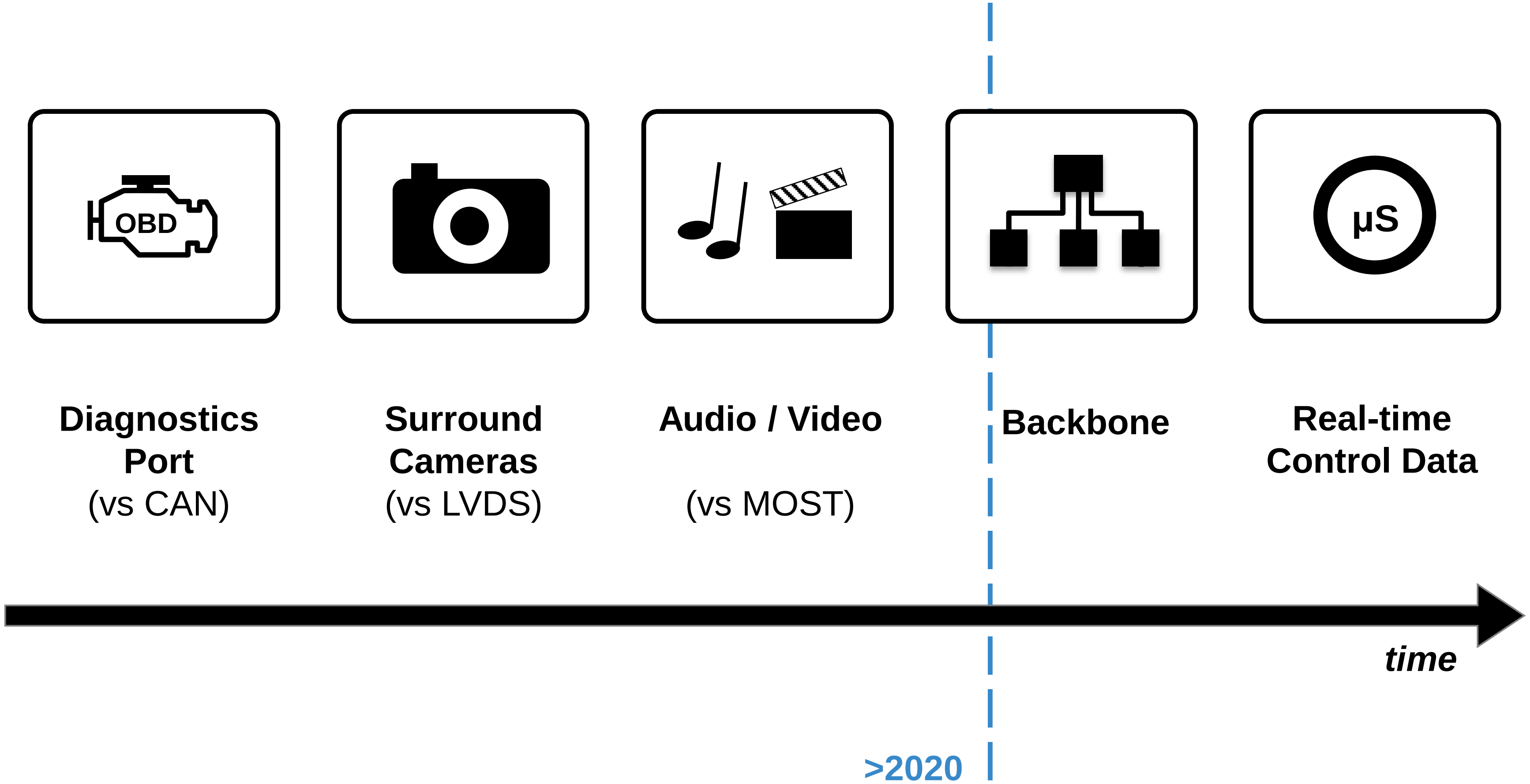
- How to block an invalid message within same CAN bus
  - Secure MCU can terminate in software (e.g. bad CMAC)

- Legacy ECU considerations
  - Many legacy ECU have no security support
  - Desire to avoid complete ECU redesign
  - Add secure functionality into PHY



Secure PHY retro-fit to legacy ECU

Evolution of Ethernet in the Vehicle



Diagnostics Port
(vs CAN)

Surround Cameras
(vs LVDS)

Audio / Video
(vs MOST)

Backbone

Real-time Control Data

time

>2020

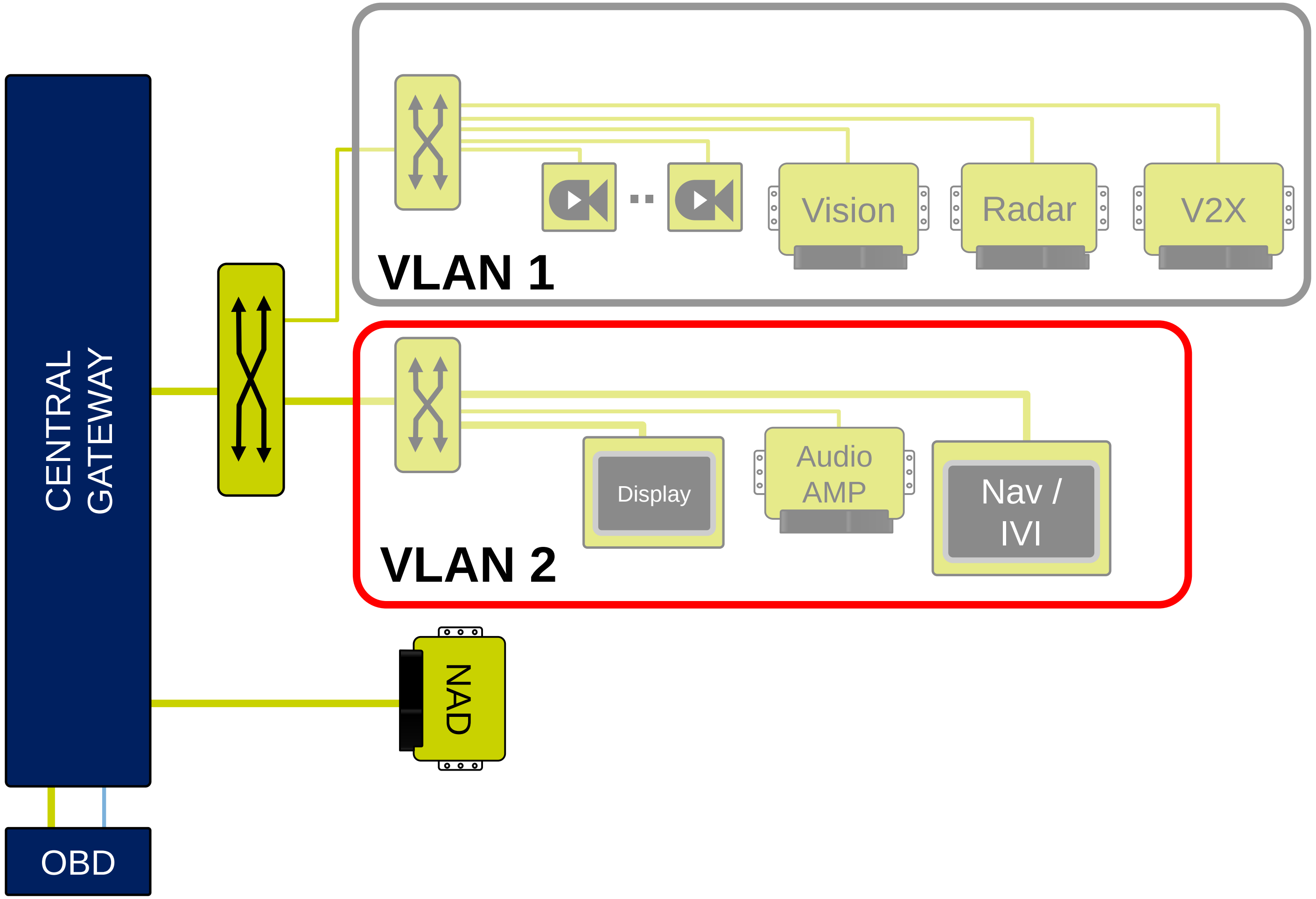
Ethernet in the Vehicle

	Web, Network Control, Address Config, etc...	Diagnostics	Non-Deterministic Control Data	Audio / Video Streaming	Deterministic Control Data
Layer 7	HTTPS	DoIP	SOME/IP	Media Control + Streaming	Data Control + Streaming (e.g. CANopen)
Layer 6					
Layer 5	TLS				
Layer 4	TCP	TCP	UDP / TCP		
Layer 3	IPv4 / 6	IPv4 / 6	IPv4 / 6	IEEE 1722(a)	IEEE 1722(a)
Layer 2	802.3 (MAC / VLAN)	802.3 (MAC / VLAN)	802.3 (MAC / VLAN)	802.3 (MAC / VLAN) 802.1AS (IEEE 1588)	802.3 (MAC / VLAN) 802.1AS (IEEE 1588)
Layer 1	100BASE-TX	100BASE-TX	1TPCE / OABR	1TPCE / OABR	1TPCE / OABR

Ethernet in Automotive Network

- Introduce organisation of Ethernet network with VLANs

- Typically be domain or shared function
  - e.g. ADAS

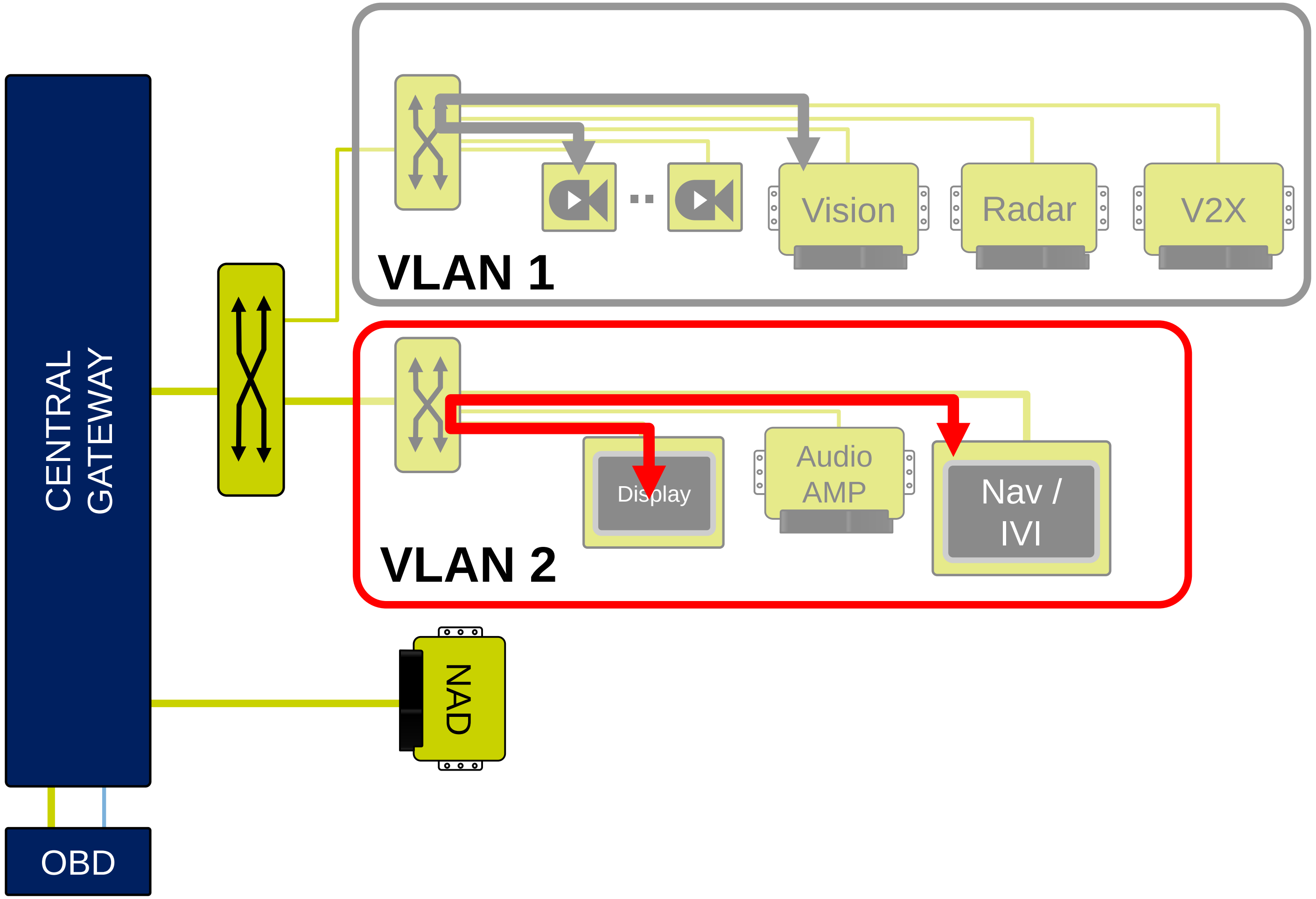


Communication inside VLAN

- Layer 2 switch handles inter-VLAN traffic
  - MAC address resolution

- Policing on switch ports
  - VLAN tag
    - Port assigned (tag on port)
    - Source assigned (tag at source)
  - Directional policing
    - E.g. Uni-directional VLAN for ADAS video to IVI
  - Filtering: MAC + VLAN tag

- Broadcast traffic only within VLAN
  - E.g. ICMP broadcast attack

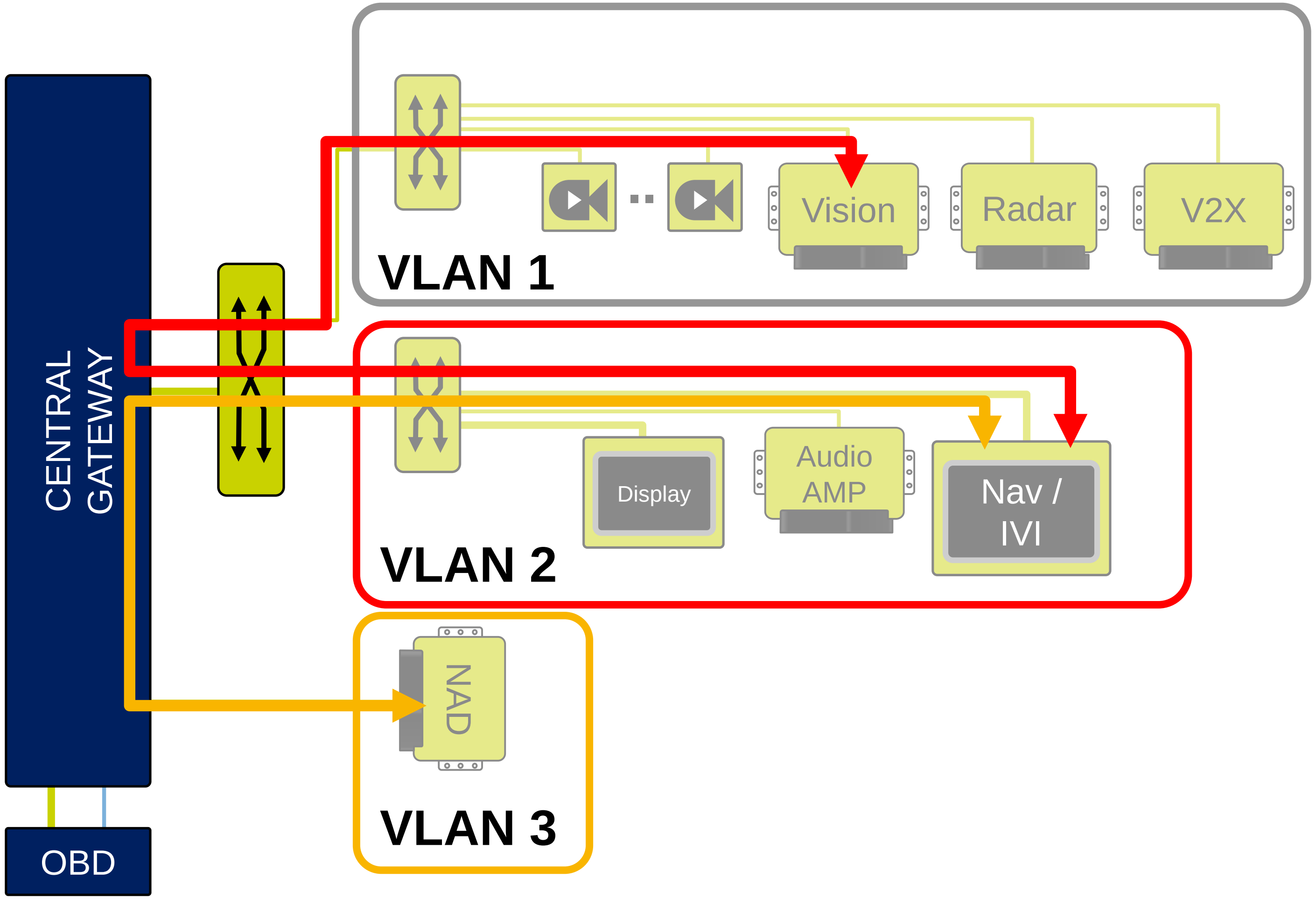


Communication between VLAN – IP Routing Need

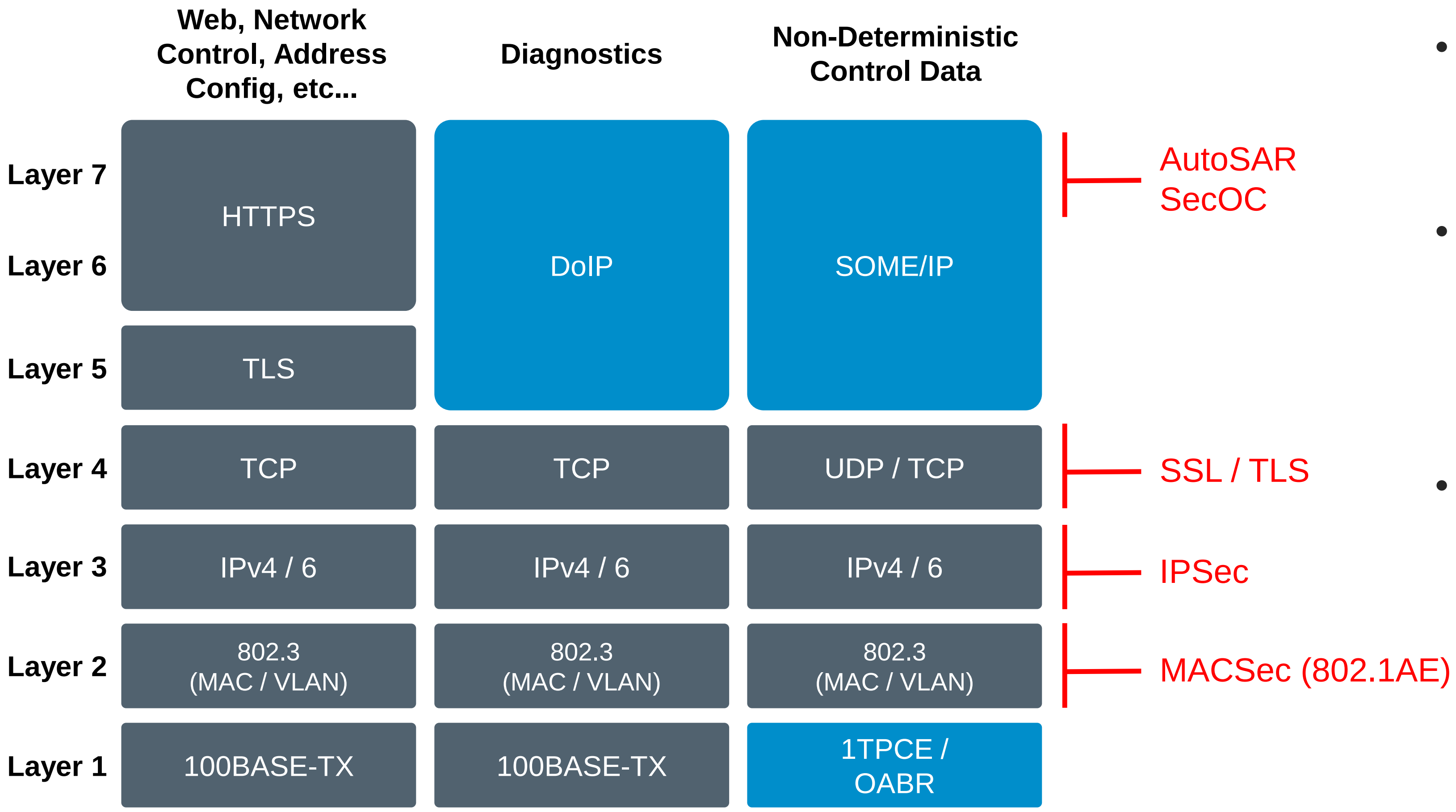
- L2 Switch cannot resolve VLAN-to-VLAN route

- Default Gateway / IP Router
  - Resolve VLAN-to-VLAN route
  - IP address to MAC address resolution

- Inspection / Firewall of traffic
  - Layer 3 (IP addr), Layer 4 (Port#) header inspection
  - Stateful Inspection



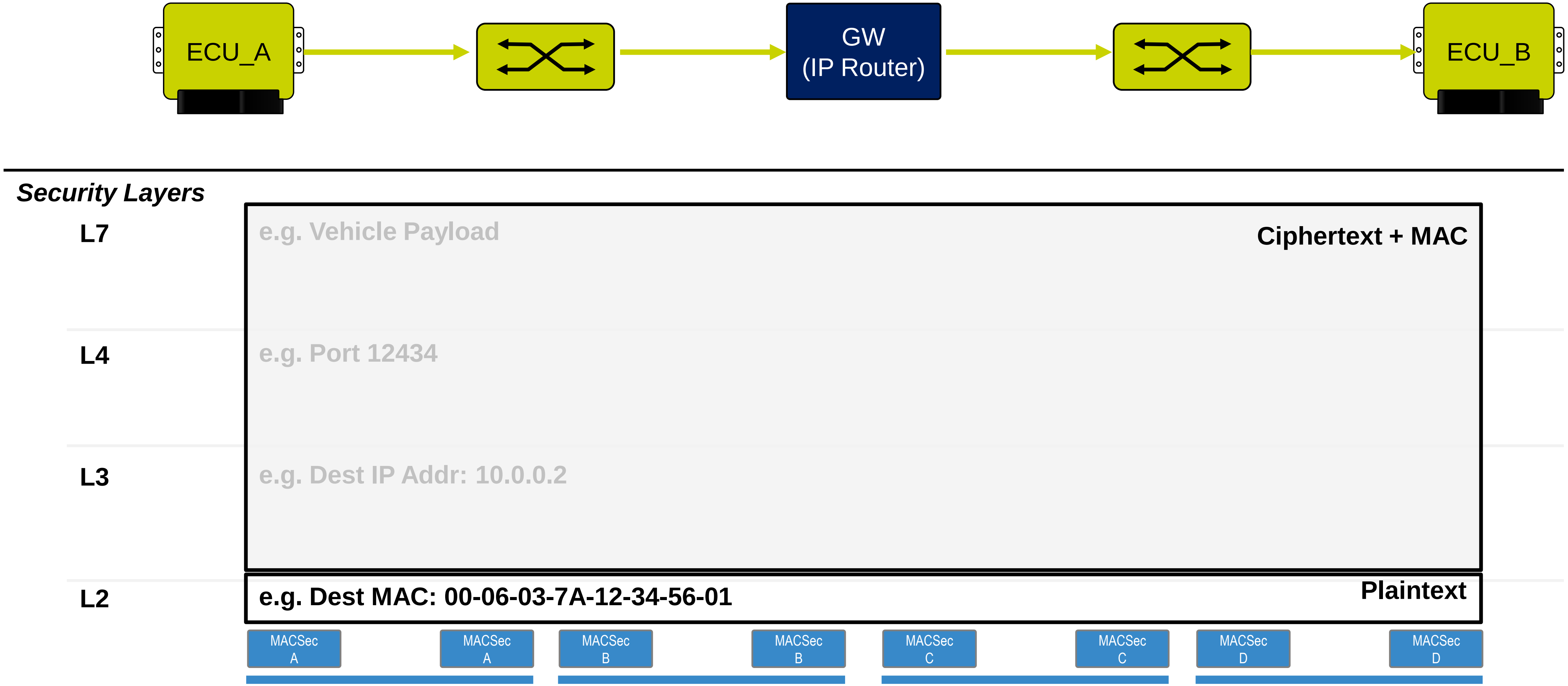
Authentication / Encryption over Ethernet



	Web, Network Control, Address Config, etc...	Diagnostics	Non-Deterministic Control Data	
Layer 7	HTTPS	DoIP	SOME/IP	AutoSAR SecOC
Layer 6				
Layer 5	TLS			
Layer 4	TCP	TCP	UDP / TCP	SSL / TLS
Layer 3	IPv4 / 6	IPv4 / 6	IPv4 / 6	IPSec
Layer 2	802.3 (MAC / VLAN)	802.3 (MAC / VLAN)	802.3 (MAC / VLAN)	MACSec (802.1AE)
Layer 1	100BASE-TX	100BASE-TX	1TPCE / OABR	

- Several possibilities for security over Ethernet
- External traffic
  - e.g. to Internet/OEM
  - Internet stds: TLS
- Internal traffic
  - Need: Auth + Integrity
  - Opt: Encryption
  - No industry consensus on which layer to protect
  - Balance cost vs protection

MACSec – 802.1AE



ECU_A

GW
(IP Router)

ECU_B

Security Layers

L7 e.g. Vehicle Payload

Ciphertext + MAC

L4 e.g. Port 12434

L3 e.g. Dest IP Addr: 10.0.0.2

L2 **e.g. Dest MAC: 00-06-03-7A-12-34-56-01**

Plaintext

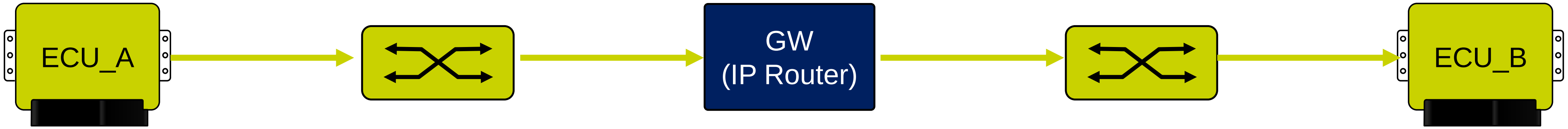
MACSec A — MACSec A

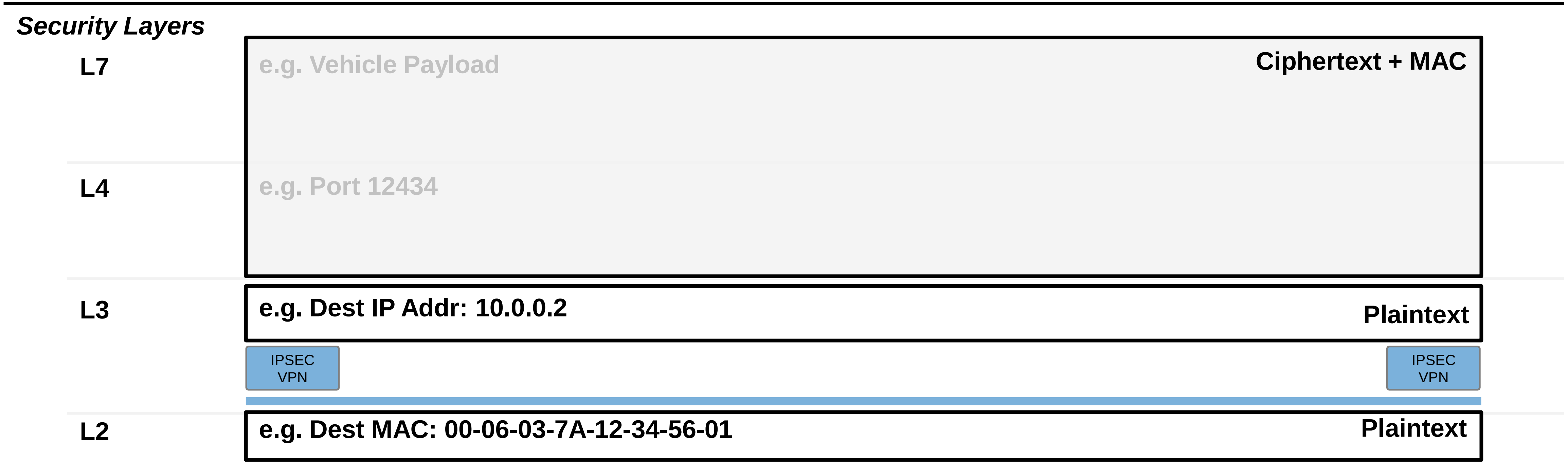
MACSec B — MACSec B

MACSec C — MACSec C

MACSec D — MACSec D

IPSec VPN





Security Layers

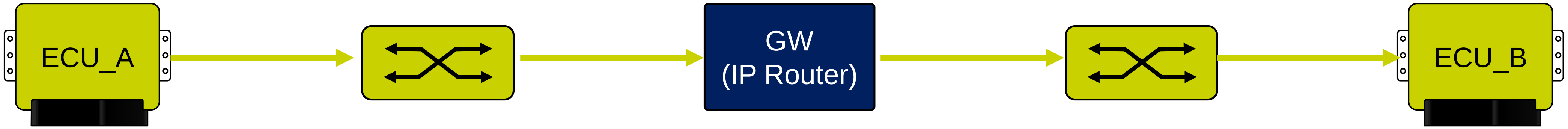
L7 e.g. Vehicle Payload **Ciphertext + MAC**

L4 e.g. Port 12434

L3 **e.g. Dest IP Addr: 10.0.0.2** **Plaintext**

L2 **e.g. Dest MAC: 00-06-03-7A-12-34-56-01** **Plaintext**

Transport Layer Security (TLS)



Security Layers

L7 — e.g. Vehicle Payload — **Ciphertext + MAC**

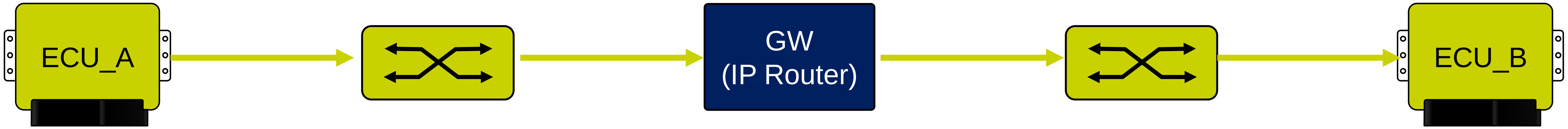
L4 — **e.g. Port 12434** — **Plaintext**

TLS TLS

L3 — **e.g. Dest IP Addr: 10.0.0.2** — **Plaintext**

L2 — **e.g. Dest MAC: 00-06-03-7A-12-34-56-01**

Application Layer (e.g. AutoSAR SecOC)



Security Layers

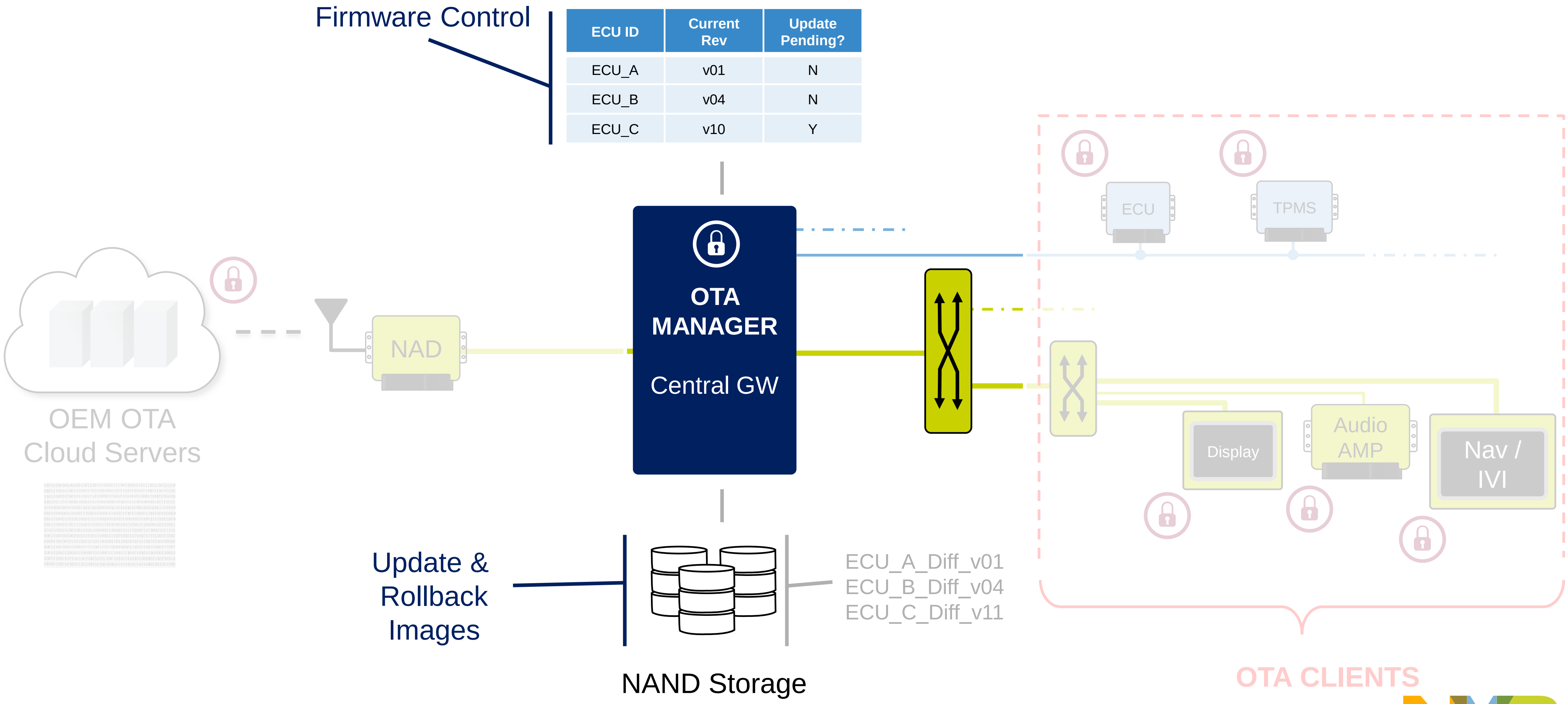
L7	e.g. Vehicle Payload	**Plaintext + MAC**
	SecOC	SecOC
L4	**e.g. Port 12434**	**Plaintext**
L3	**e.g. Dest IP Addr: 10.0.0.2**	
L2	**e.g. Dest MAC: 00-06-03-7A-12-34-56-01**	

FOTA

Firmware Over-the-Air (FOTA)

- Static software is a security vulnerability
  - Lifespan of vehicle >10 years
- Examples in recent years of safety issues resulting from SW bugs.
  - How long before security issues?
- Strong need to remotely update & patch application software and security weaknesses
  - Controlled by a trusted entity in vehicle

Firmware Over-the-Air (FOTA) Architecture

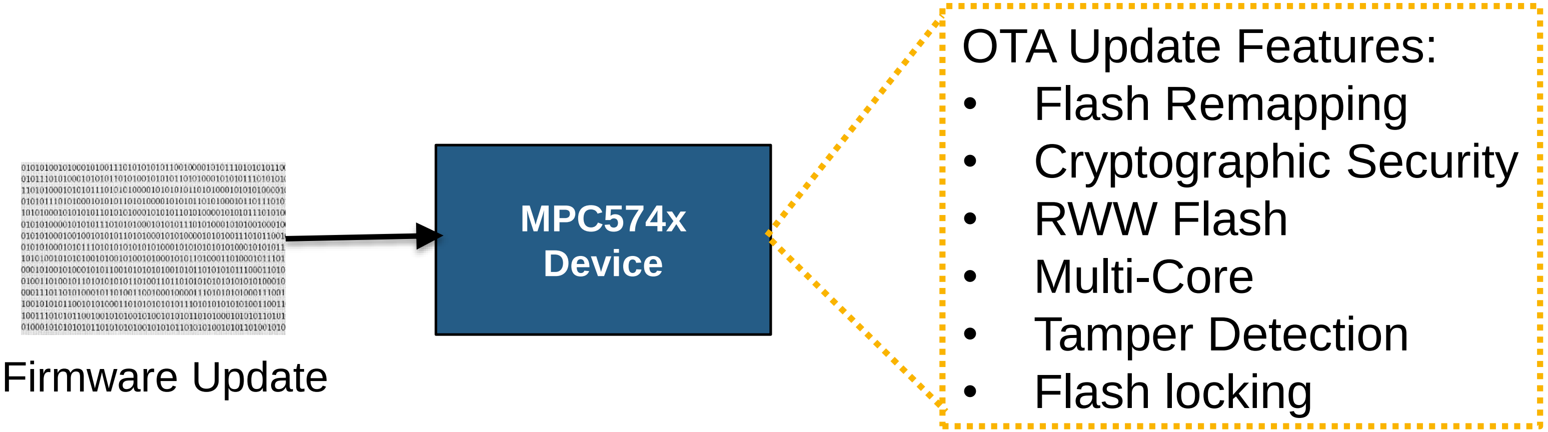


ECU ID	Current Rev	Update Pending?
ECU_A	v01	N
ECU_B	v04	N
ECU_C	v10	Y

ECU_A_Diff_v01
ECU_B_Diff_v04
ECU_C_Diff_v11

OTA Client (ECU) Features

The MPC574x family is OTA update enabled and contains hardware features to help with each stage of the OTA process!



OTA Update Features:

- Flash Remapping
- Cryptographic Security
- RWW Flash
- Multi-Core
- Tamper Detection
- Flash locking

OTA Benefits for OEM:

- Save money on recalls
- Ability to immediately patch critical bugs
- Allow addition of new features, post-purchase

OEM Demands:

- Minimal affect on drivers (e.g. no vehicle down time during update)
- no risk of failed update leaving car unusable.

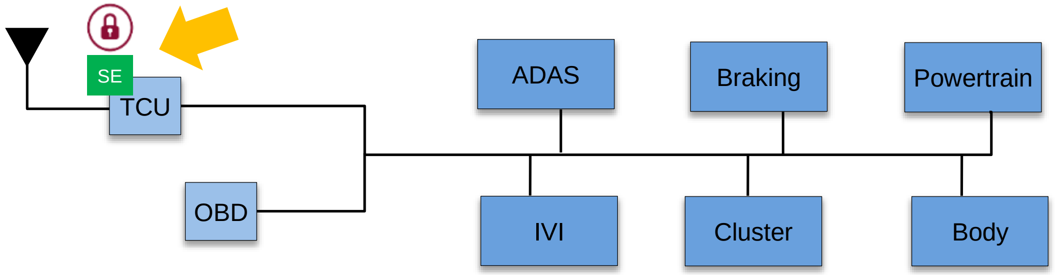
The MPC574x family is designed to support **secure** OTA updates which can occur seamlessly as a background task with **no vehicle downtime.**

LAYERED SECURITY MODEL

4 LAYERS TO SECURING A CAR

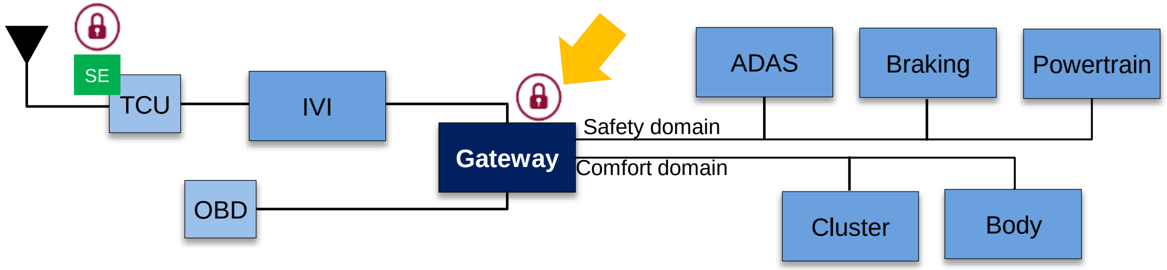
Layer 1: Secure Interface

Secure M2M authentication, secure key storage



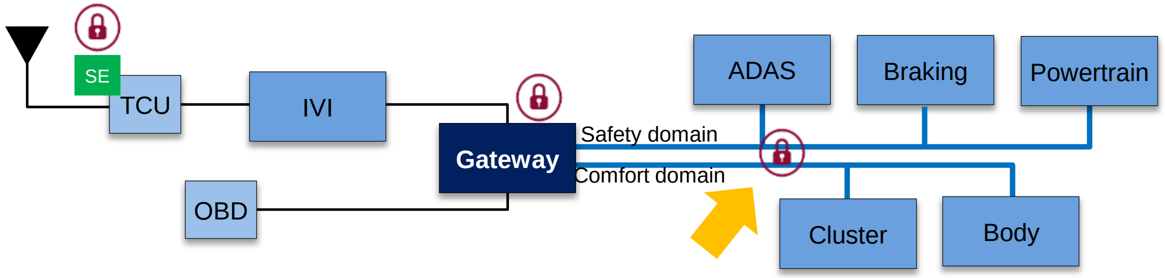
Layer 2: Secure Gateway

Domain isolation, firewall/filter, centralized intrusion detection (IDS)



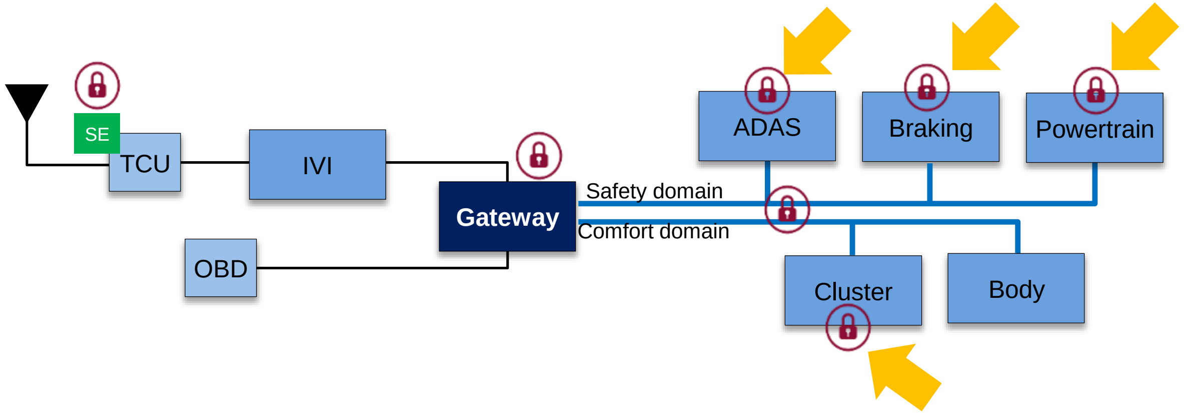
Layer 3: Secure Network

Message authentication, CAN ID killer, distributed intrusion detection (IDS)

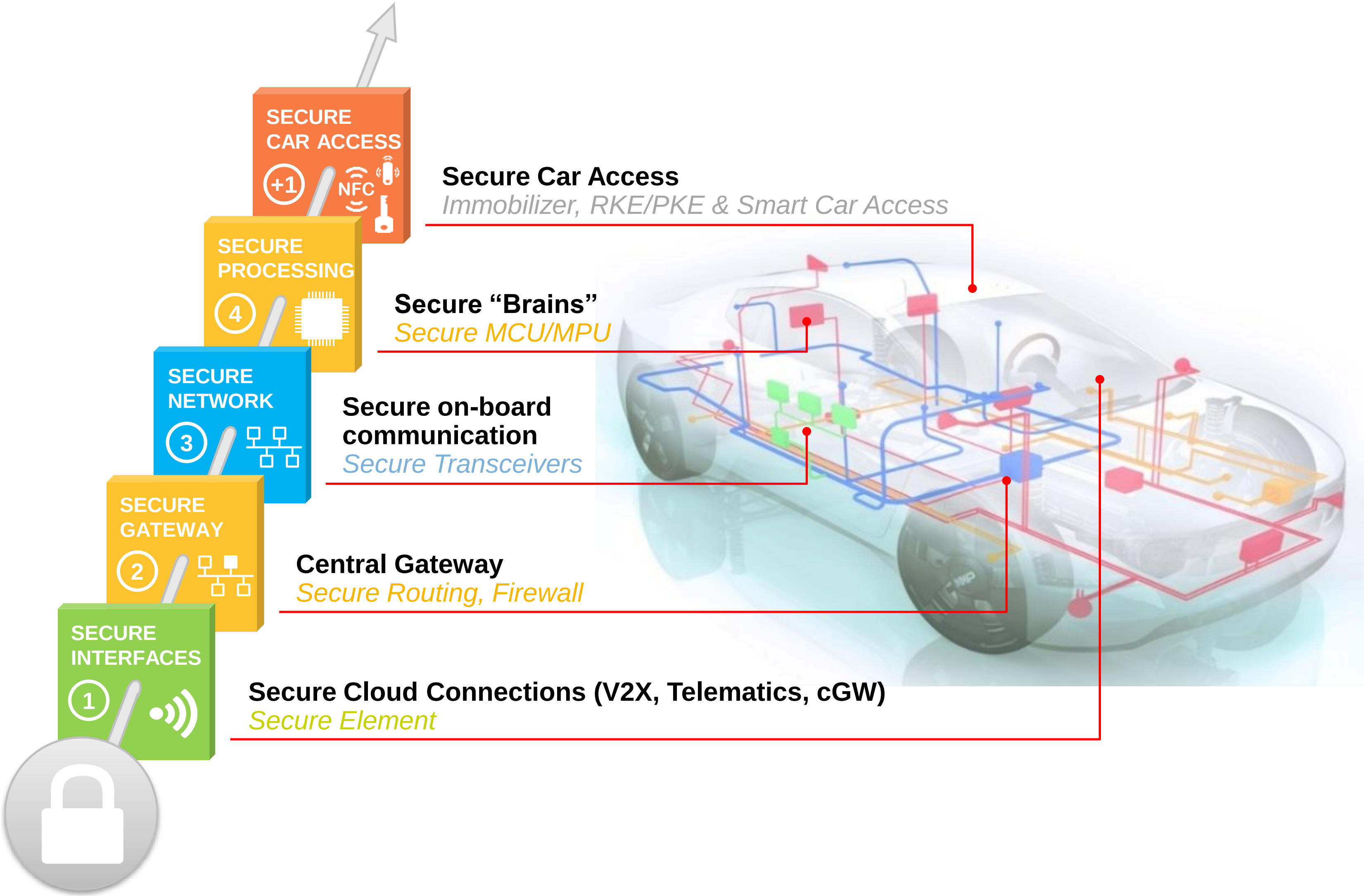


Layer 4: Secure Processing

Secure boot, run time integrity, OTA updates



NXP AUTOMOTIVE SECURITY (4+1 SOLUTION)



Secure Car Access
Immobilizer, RKE/PKE & Smart Car Access

Secure "Brains"
Secure MCU/MPU

Secure on-board communication
Secure Transceivers

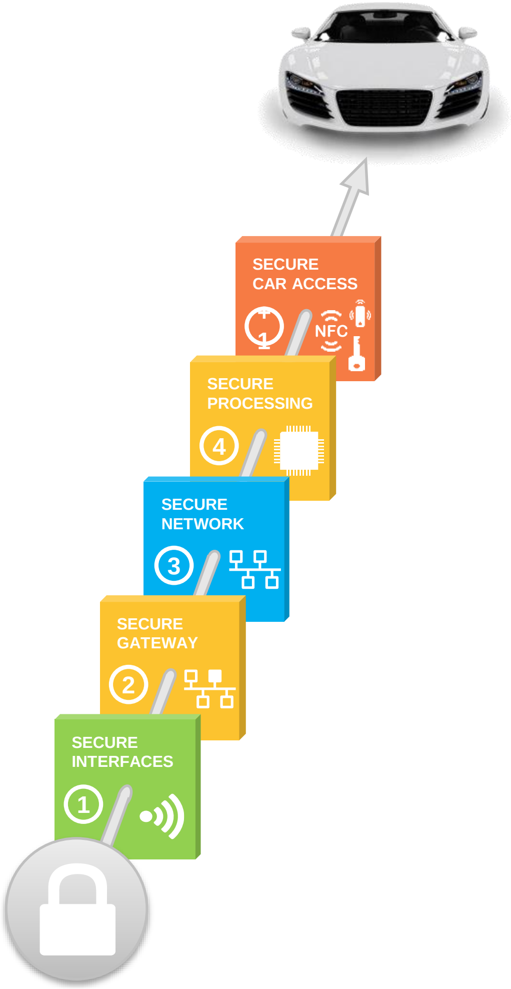
Central Gateway
Secure Routing, Firewall

Secure Cloud Connections (V2X, Telematics, cGW)
Secure Element

- **NXP #1 in Auto HW Security**
- **4-Layer Cyber Security Solution**
- **Plus 'Best In Class' Car Access Systems**
- **Recognized Thought & Innovation Leader**
- **> 900 security patent families, ~ 200 specific to Automotive**
- **Partner of Choice for OEMS, T1s & Industry Alliances**

MORE DETAILS IN THE FOLLOWING SESSIONS

Topic	Session	Type	Timeslot
4 Layers of Automotive Security for Connected Cars	FTF-AUT-N1811	Lecture	Mon 2:00 PM
Future RF Technologies - **UltraWideBand** for Car Access	FTF-INS-N1777	Lecture and demo	Mon 4:15 PM
Secure Car Access and Remote Management	FTF-AUT-N1776	Lecture and demo	Tue 12:00 PM
Trends in Vehicle Architectures: **Central Gateway**	FTF-AUT-N1813	Lecture	Tue 11:00 AM
Recent Advances in **Secure MCU** Security Offerings	FTF-AUT-N1812	Lecture	Mon 3:15 PM
Maximizing Security using the **Secure MCU** Features	FTF-AUT-N1810	Lunch & Learn	Tue 1:15 PM
Creating Secure Networks for **V2X Communications**	FTF-AUT-N1764	Lecture	Tue 2:30 PM
Techniques for **Crypto Key Management** Using i.MX Application Processors	FTF-DES-N1894	Lecture	Tue 3:30 PM
NFC for Connected Cars	FTF-AUT-N1781	Lecture	Tue 4:45 PM
CAN Security (L3)	FTF-AUT-N1815	Lecture	Tue 5:45 PM
Automotive Gateway Security Made Easy	FTF-AUT-N1792	Hands-on workshop	Wed 2:30 PM
Security vs Functional Safety - Complementary or Contradictory?	FTF-AUT-N1814	Lecture	Wed 4:45 PM
Secure CAN Networks	FTF-AUT-N1783	Hands-on workshop	Wed 4:45 PM
Automotive Cyber Security: A Tough Issue Needing Robust Solutions	FTF-AUT-N1763	Panel discussion	Wed 4:45 PM



SECURE CONNECTIONS
FOR A SMARTER WORLD

ATTRIBUTION STATEMENT

NXP, the NXP logo, NXP SECURE CONNECTIONS FOR A SMARTER WORLD, CoolFlux, EMBRACE, GREENCHIP, HITAG, I2C BUS, ICODE, JCOP, LIFE VIBES, MIFARE, MIFARE Classic, MIFARE DESFire, MIFARE Plus, MIFARE FleX, MANTIS, MIFARE ULTRALIGHT, MIFARE4MOBILE, MIGLO, NTAG, ROADLINK, SMARTLX, SMARTMX, STARPLUG, TOPFET, TrenchMOS, UCODE, Freescale, the Freescale logo, AltiVec, C 5, CodeTEST, CodeWarrior, ColdFire, ColdFire+, C Ware, the Energy Efficient Solutions logo, Kinetis, Layerscape, MagniV, mobileGT, PEG, PowerQUICC, Processor Expert, QorIQ, QorIQ Qonverge, Ready Play, SafeAssure, the SafeAssure logo, StarCore, Symphony, VortiQa, Vybrid, Airfast, BeeKit, BeeStack, CoreNet, Flexis, MXC, Platform in a Package, QUICC Engine, SMARTMOS, Tower, TurboLink, and UMEMS are trademarks of NXP B.V. All other product or service names are the property of their respective owners. ARM, AMBA, ARM Powered, Artisan, Cortex, Jazelle, Keil, SecurCore, Thumb, TrustZone, and μVision are registered trademarks of ARM Limited (or its subsidiaries) in the EU and/or elsewhere. ARM7, ARM9, ARM11, big.LITTLE, CoreLink, CoreSight, DesignStart, Mali, mbed, NEON, POP, Sensinode, Socrates, ULINK and Versatile are trademarks of ARM Limited (or its subsidiaries) in the EU and/or elsewhere. All rights reserved. Oracle and Java are registered trademarks of Oracle and/or its affiliates. The Power Architecture and Power.org word marks and the Power and Power.org logos and related marks are trademarks and service marks licensed by Power.org. © 2015–2016 NXP B.V.