new eagle

RAPTOR®
INNOVATION
SUMMIT 2025

J1939-91C in Practice: A New Eagle approach to Secure Network Architecture

Presented by:
Collin Spencer, Staff Software Engineer, New Eagle

Agenda

new eagle

RAPTOR®
INNOVATION
SUMMIT 2025

J1939-91C Overview

- **Automotive Security (SecOC)**
- J1939-22
- J1939-91C
- Raptor Solution

Why is cybersecurity needed?

new eagle

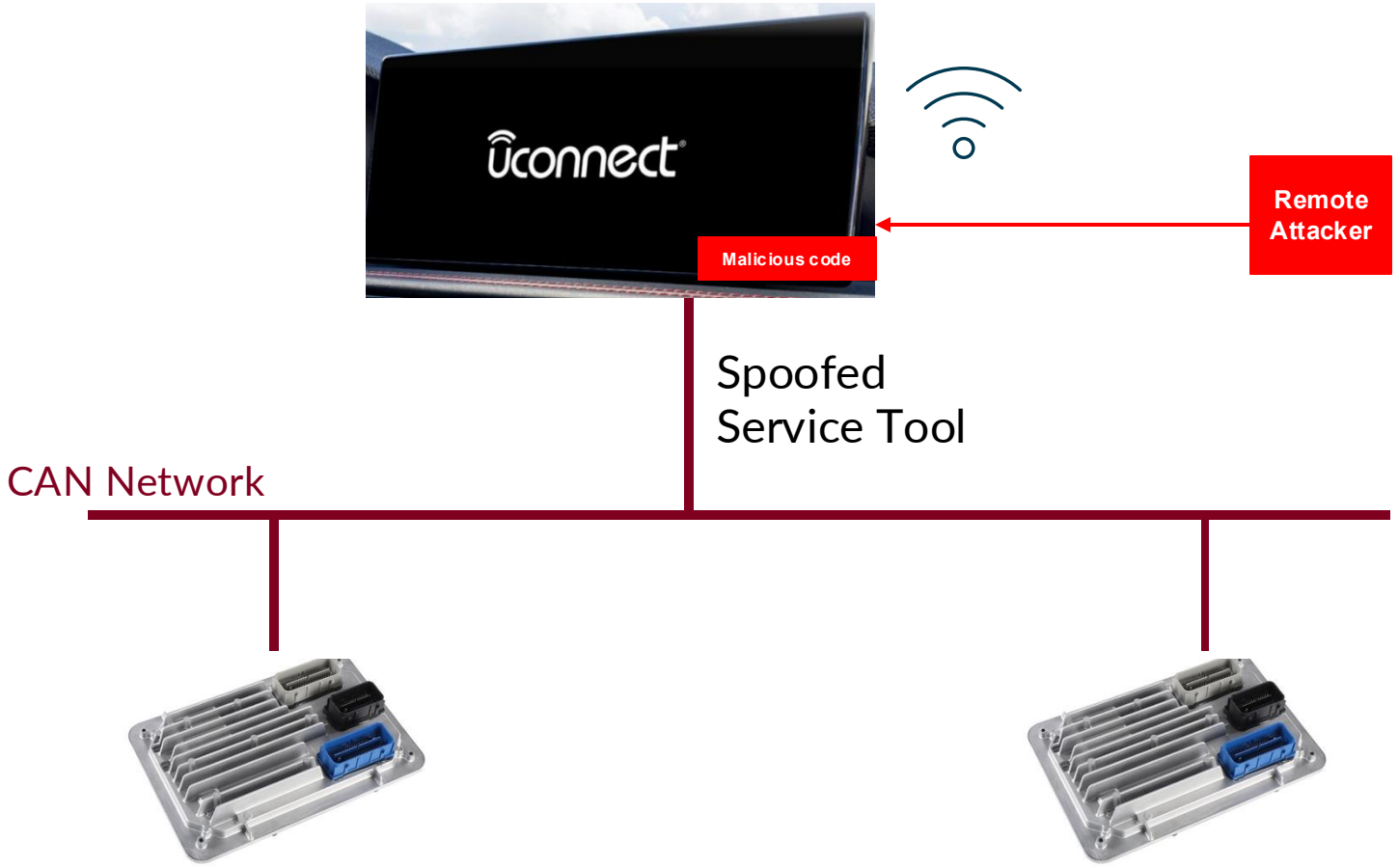
RAPTOR®
INNOVATION
SUMMIT 2025

ANDY GREENBERG SECURITY JUL 21, 2015 6:00 AM

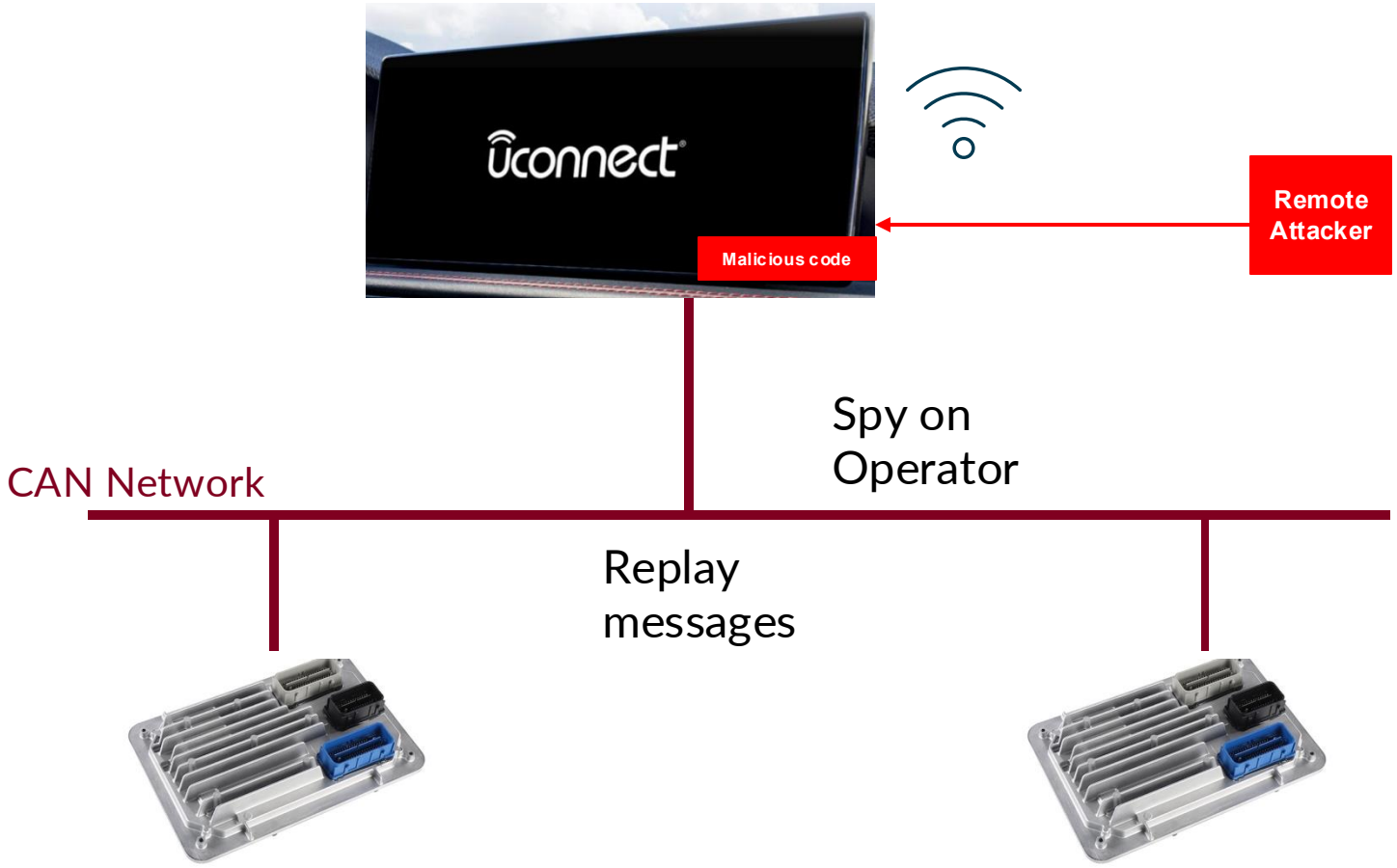
Hackers Remotely Kill a Jeep on the Highway—With Me in It

I was driving 70 mph on the edge of downtown St. Louis when the exploit began to take hold.

How did they do it?



What else could you do?



How do we prevent this outcome?

new eagle

RAPTOR® INNOVATION SUMMIT 2025

Layer 3: E/E-Architecture

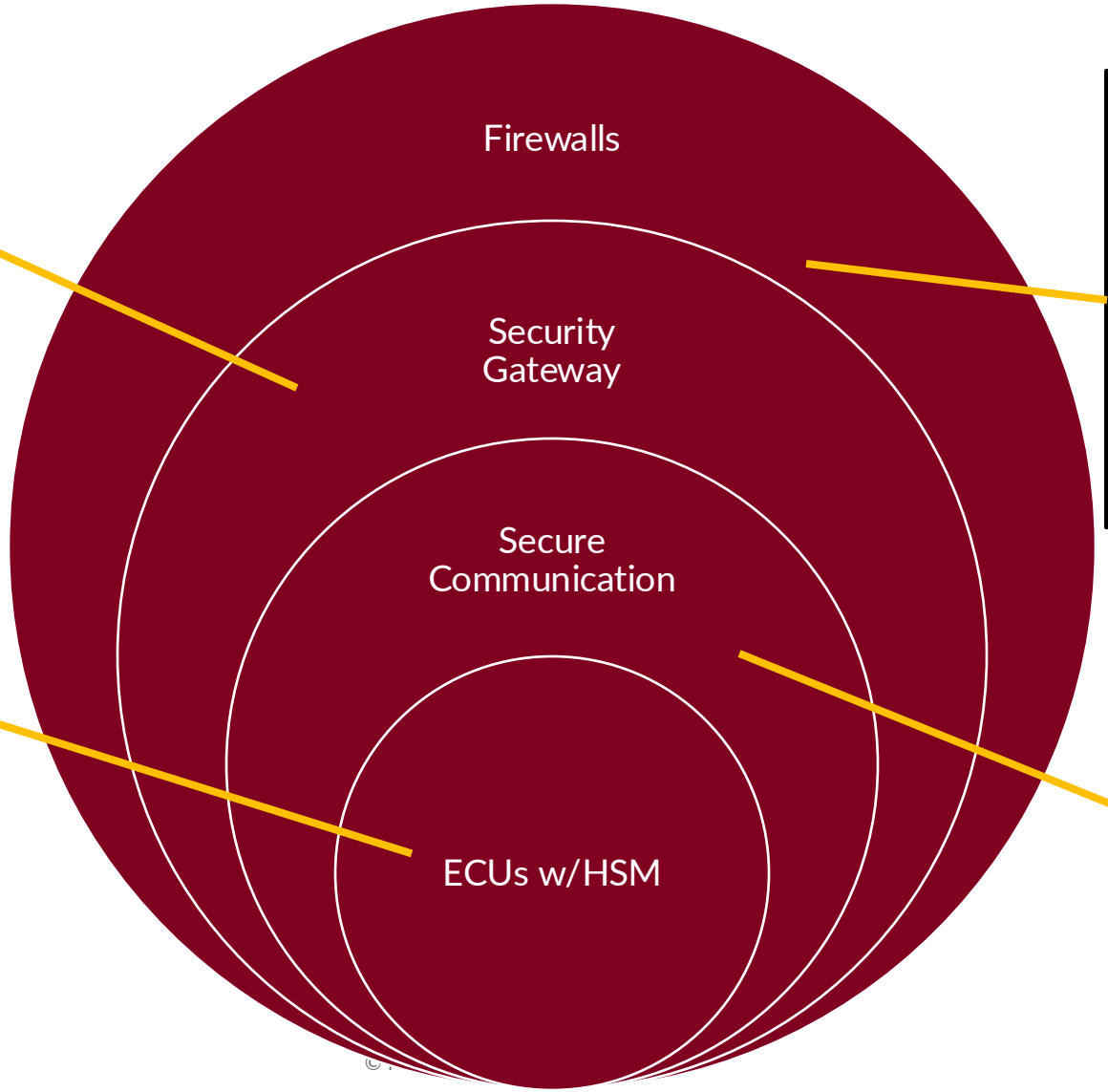
OEM

- Protect and separate domains
- Secure E/E architectures, and security gateways with adaptive rules to control traffic and access

Layer 1: Individual ECU

new eagle

- Protect integrity of ECU SW & data
- Secure Flashing
- Secure Access
- HSM as Trusted Anchor



Layer 4: Connected Vehicle

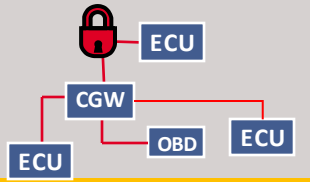
OEM

- Protect safety & integrity of vehicle and privacy of driver
- Vehicle firewalls and security standards for communication and external interfaces

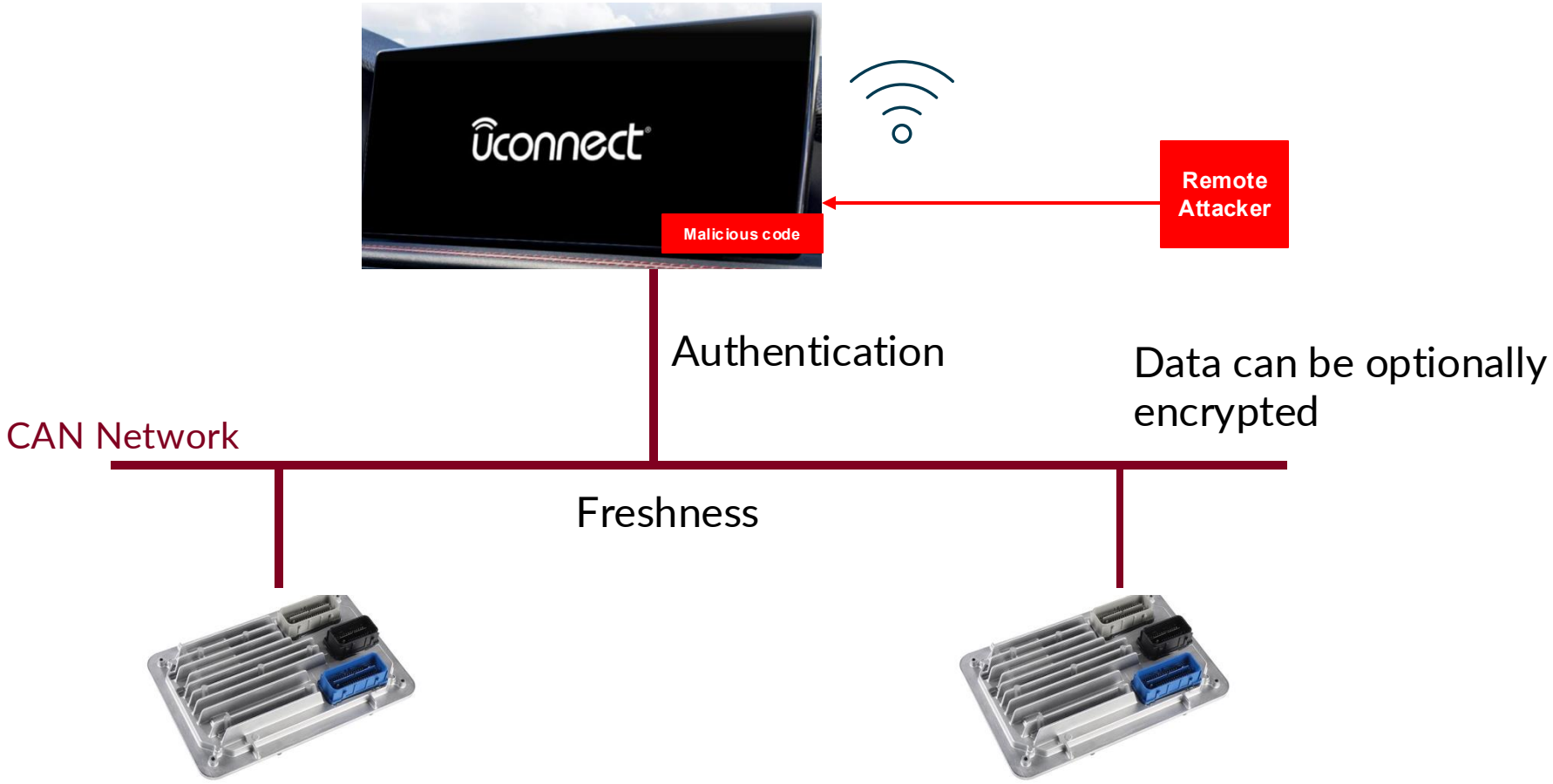
Layer 2: In-vehicle Network

OEM

- Protect the integrity of critical in-vehicle signals
- Authentic communication



SAE J1939–91C Network Security



Agenda

new eagle

RAPTOR® INNOVATION SUMMIT 2025

J1939-91C Overview

- Automotive Security
- **J1939-22**
- J1939-91C
- Raptor Solution

J1939-22 Introduction

new eagle

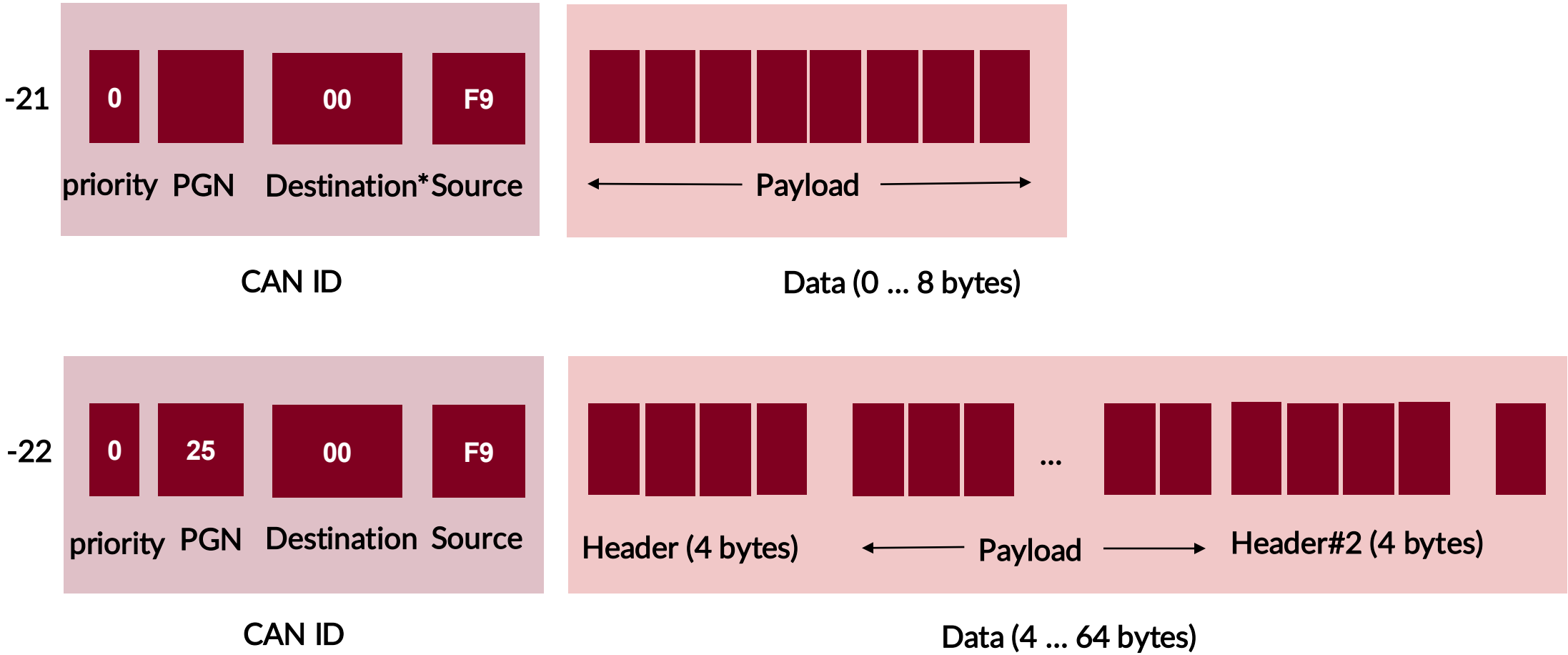
RAPTOR®
INNOVATION
SUMMIT 2025

SAE INTERNATIONAL®

SURFACE VEHICLE RECOMMENDED PRACTICE	J1939™-22	SEP2022
	Issued 2021-03 Revised 2022-09 Superseding J1939-22 JUL2021	
CAN FD Data Link Layer		

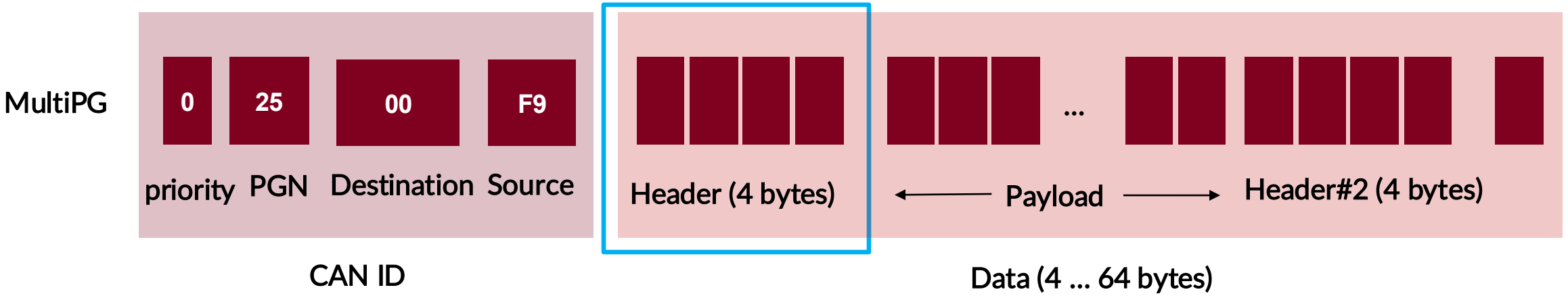
INNOVATE FASTER. SCALE SMARTER

J1939-22 MultiPG vs. J1939-21 PGN



J1939-22 MultiPG Header

new eagle
RAPTOR®
INNOVATION
SUMMIT 2025



J1939-22 MultiPG Header

new eagle

RAPTOR® INNOVATION SUMMIT 2025

TOS	TF Value	Trailer format
001_b	000_b	Reserved
001_b	001_b	32-bit manufacturer specific (OEM) cybersecurity assurance data
001_b	010_b	32-bit manufacturer specific (OEM) functional safety assurance data
001_b	011_b	32-bit manufacturer specific (OEM) cybersecurity followed by a 32-bit manufacturer specific (OEM) functional safety assurance data
001_b	100_b	Reserved
001_b	101_b	64-bit manufacturer specific (OEM) cybersecurity assurance data
001_b	110_b	64-bit manufacturer specific (OEM) functional safety assurance data
001_b	111_b	Reserved
010_b	000_b	SAE J1939 with no assurance data
010_b	001_b - 111_b	Reserved
011_b - 111_b	Reserved	Reserved

Agenda

new eagle

RAPTOR®
INNOVATION
SUMMIT 2025

J1939-91C Overview

- Automotive Security
- J1939-22
- **J1939-91C**
- Raptor Solution

Introduction to J1939-91C

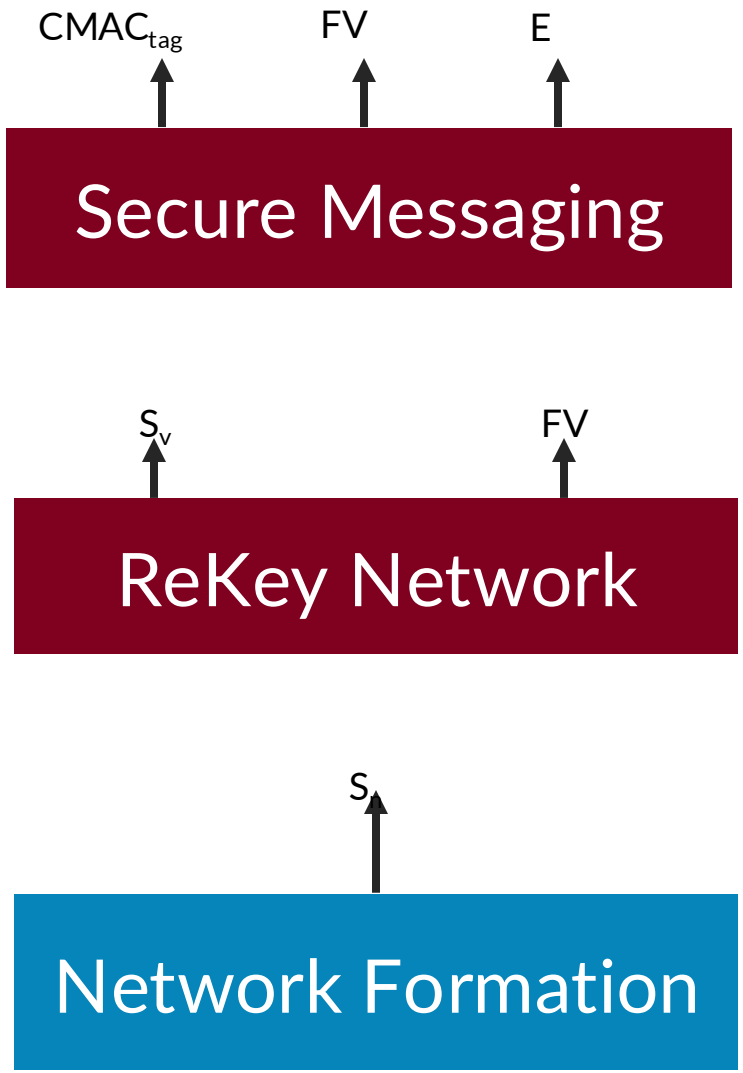
new eagle

RAPTOR®
INNOVATION
SUMMIT 2025

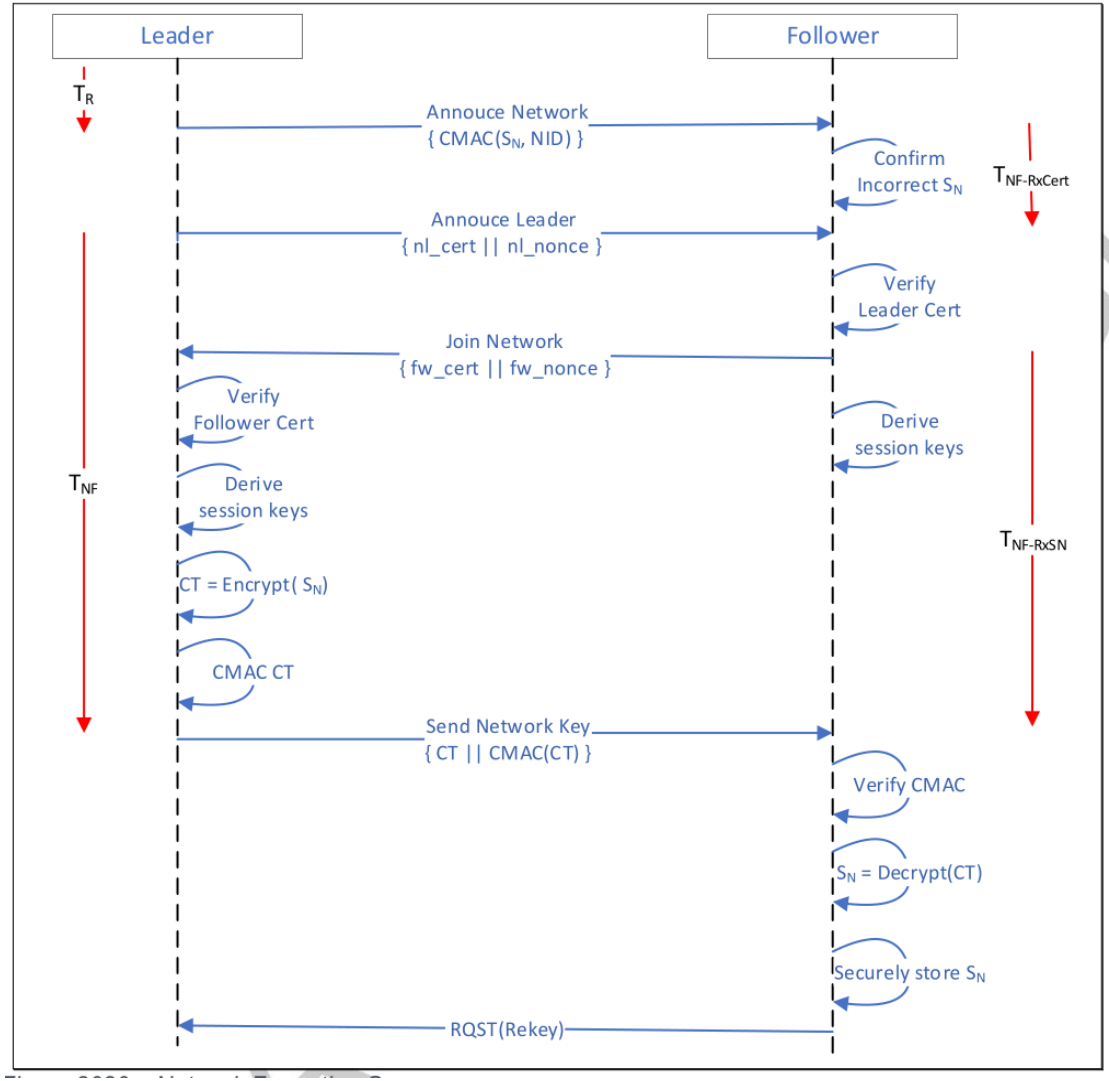
SURFACE VEHICLE RECOMMENDED PRACTICE	J1939™-91C	MTH2023
	Issued 2023-XX	
CAN FD Network Security		

RATIONALE

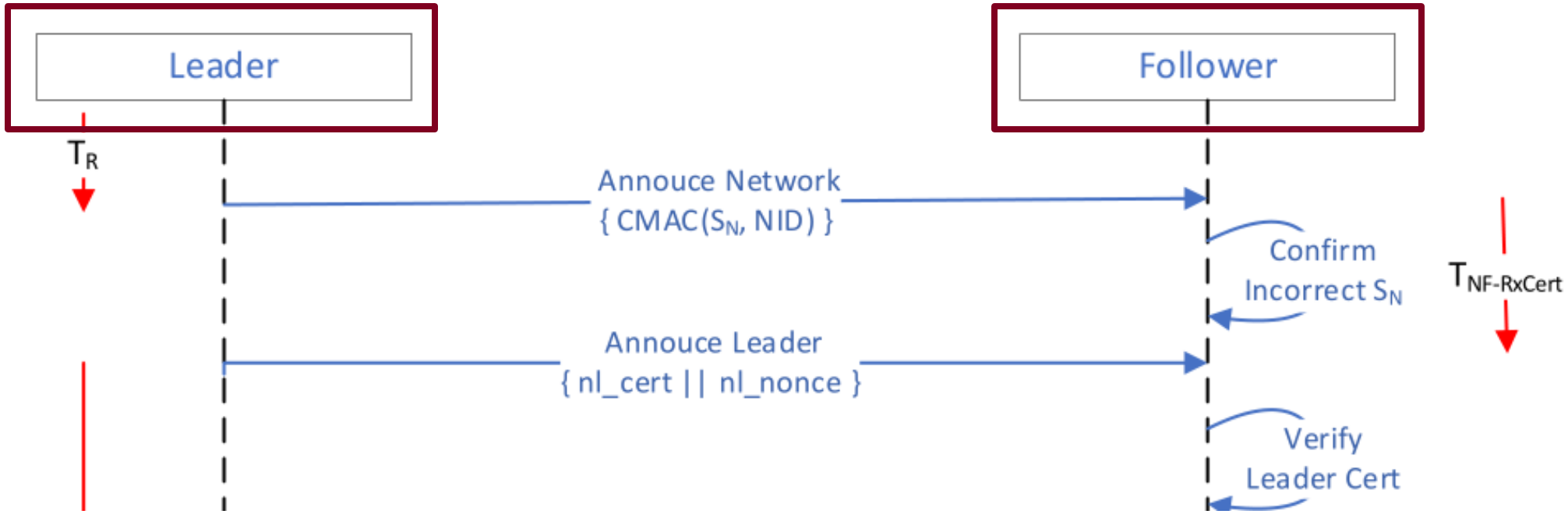
J1939-91C Three Phases



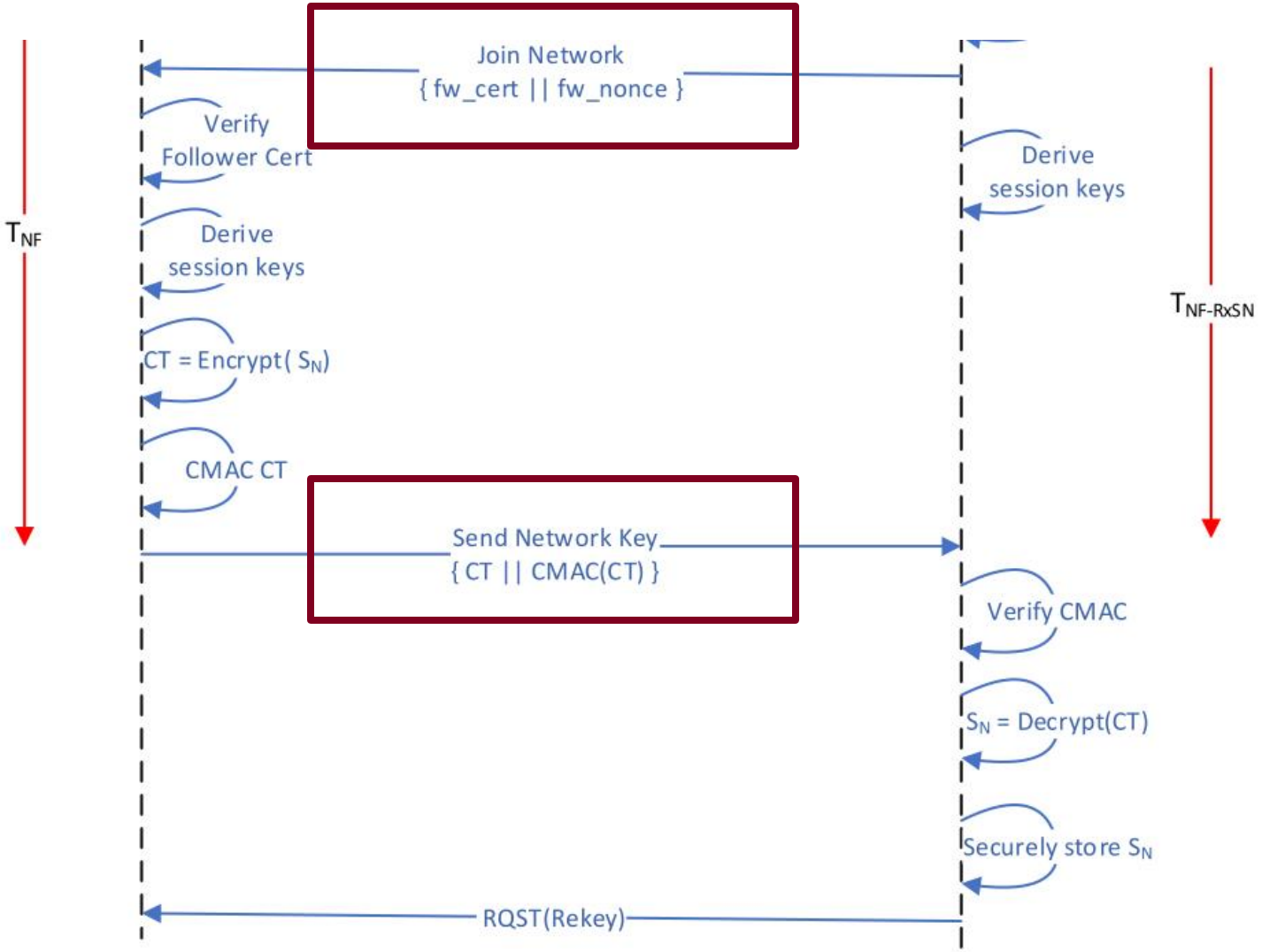
Network Formation



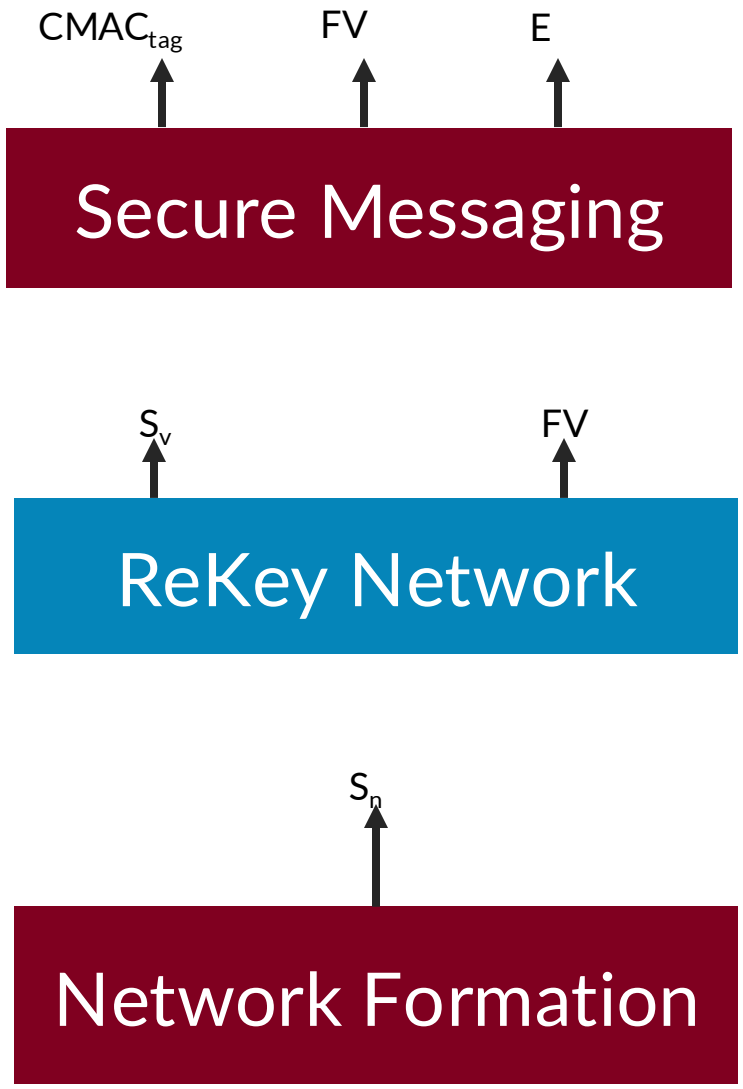
Network Formation – Network Roles



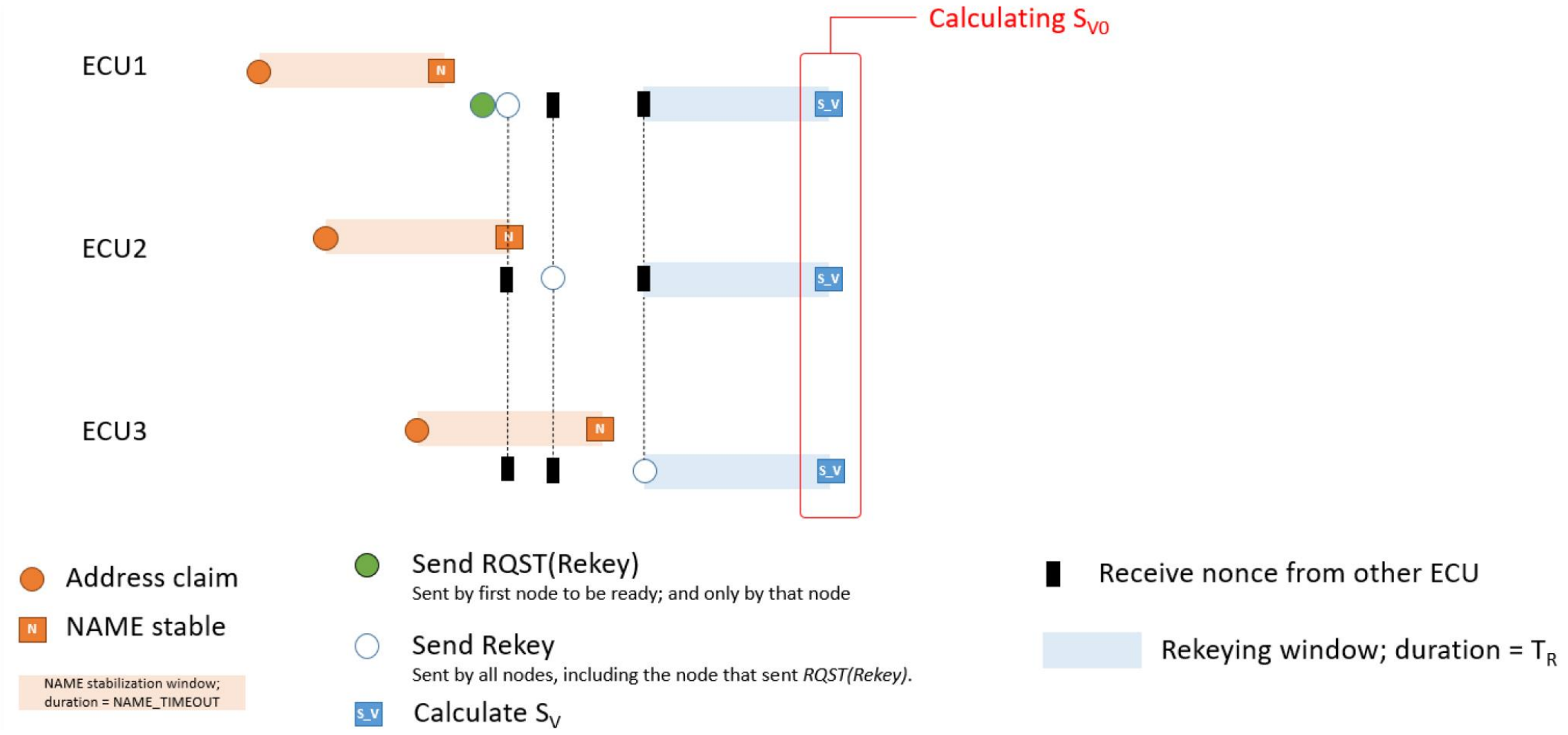
Network Formation – Join Network



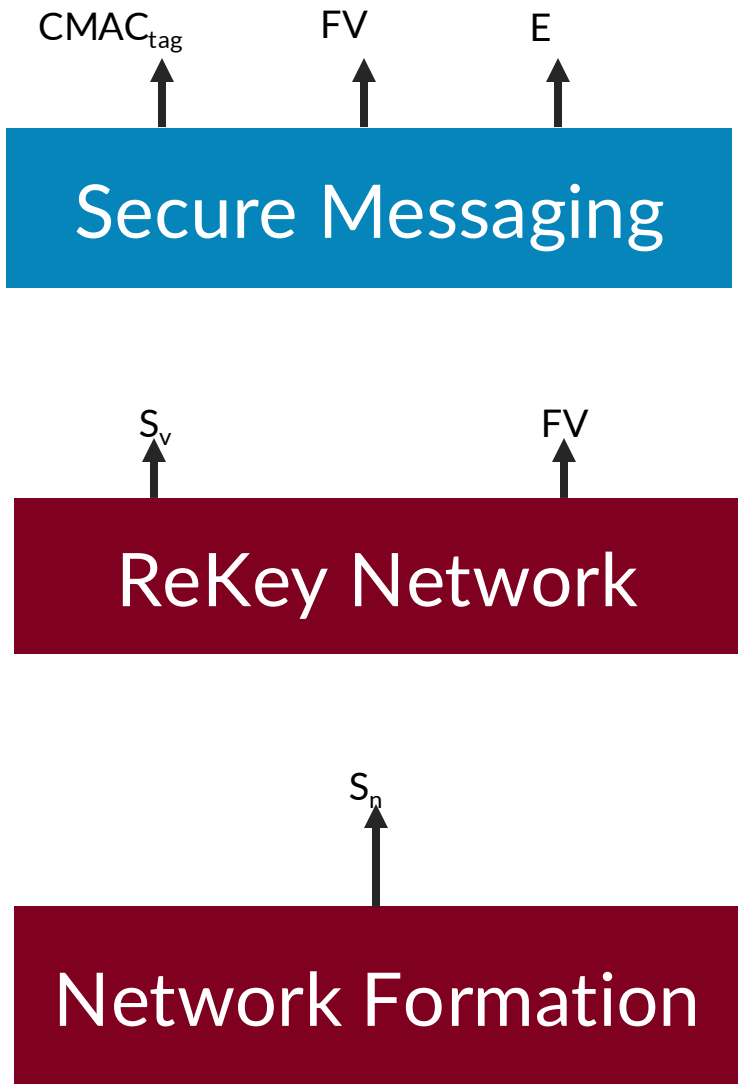
J1939-91C Three Phases



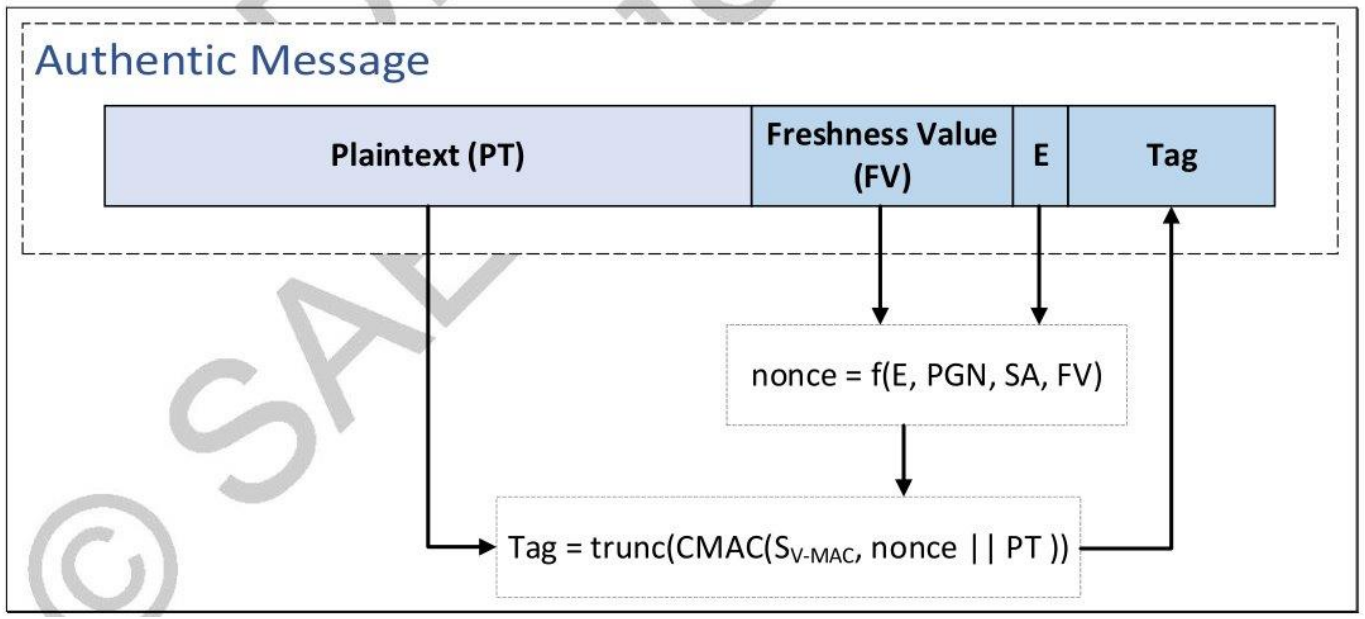
Rekey Sequence



J1939-91C Three Phases



Secure message format



f() = ((E << 23) OR'ed PGN) || SA || FV

Note: If the new FV value is larger than the maximum allowed value, the Tx device should request a rekey at its earliest opportunity.

Rekey and Secure Messaging

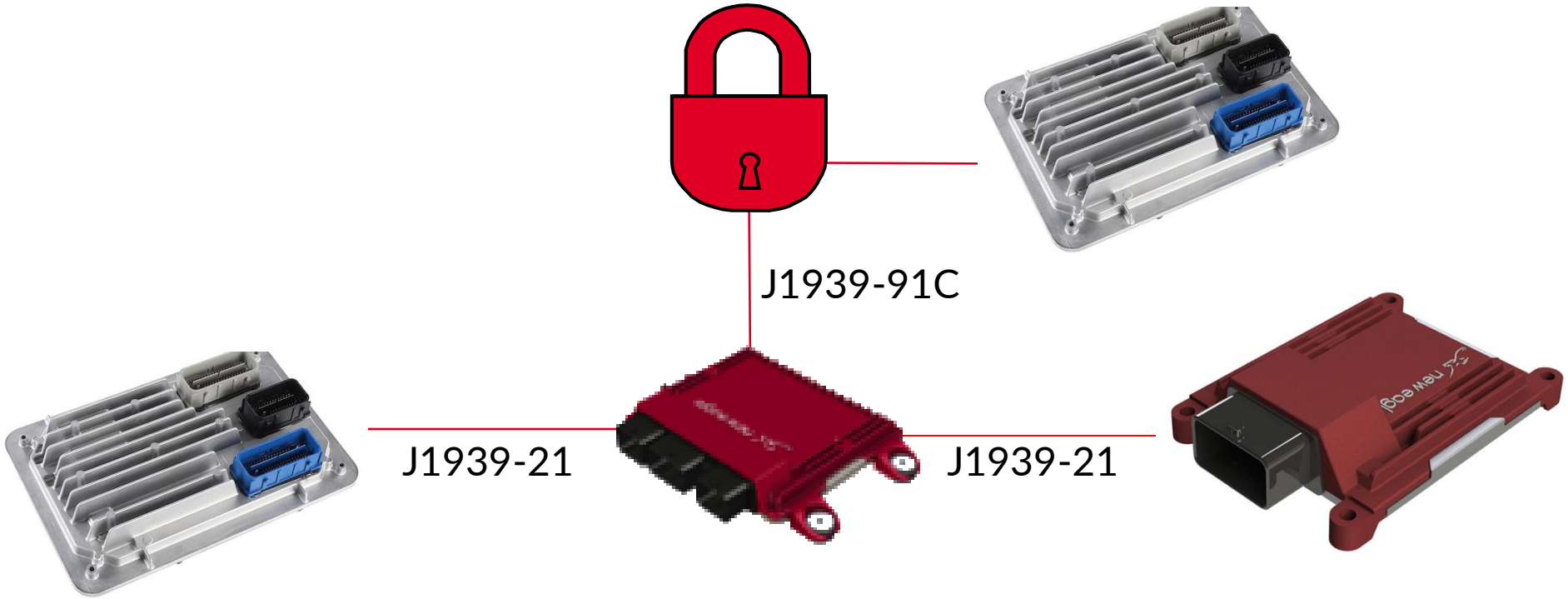
```
CAN 2  0025FF02      XFB    7      5939.097
       40 EA 00 03 04 FA 00

CAN 2  0025FF02      XFB    48     5939.114
       40 FA 04 24 FF FF 01 FF     CA FE FE 5A 53 63 27 53
       89 C0 9A 7F DE 7D CA FE     A3 6E B3 DD 67 65 E0 D6
       95 31 F9 62 12 7E 0A DE     00 00 00 AA AA AA AA AA

CAN 2  1C25FF00      XFB    48     5939.129
       40 FA 04 24 FF FF 01 FF     00 00 00 10 50 81 D7 50
       50 80 00 2D 00 00 00 10     4D 87 37 3F B1 DB 74 65
       42 1E A3 50 BF 67 0F B2     00 00 00 AA AA AA AA AA

CAN 2  00250200      XFB    16     5940.632
       34 02 00 0C 00 00 00 00     00 00 00 00 8B BD 9C C5
```

J1939-91C Gateway



Agenda

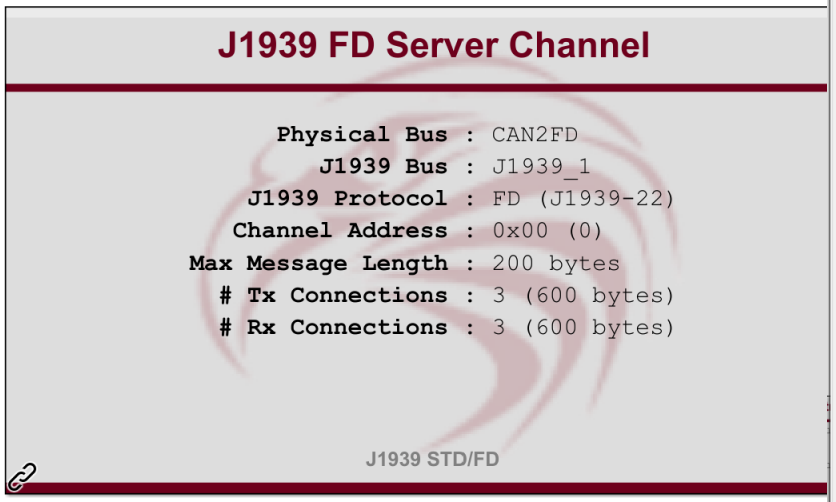
new eagle

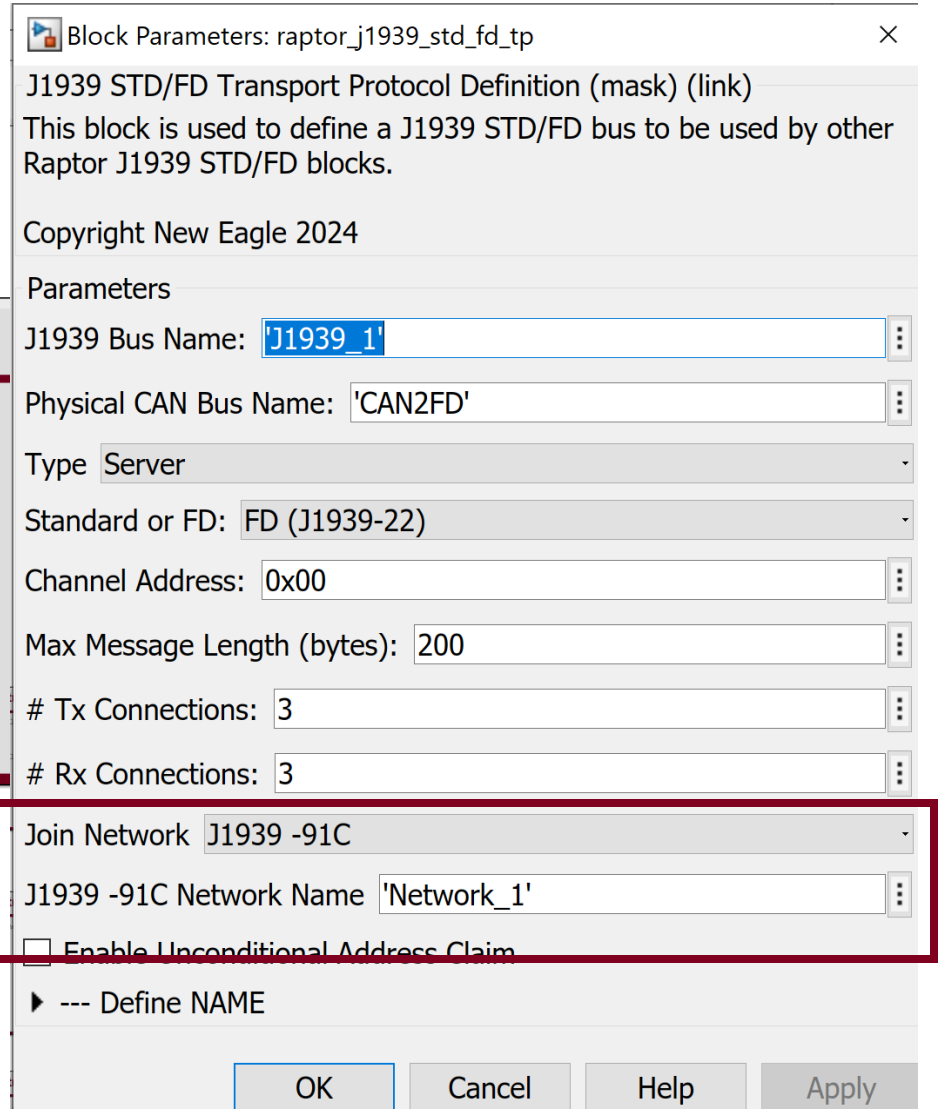
RAPTOR® INNOVATION SUMMIT 2025

J1939-91C Overview

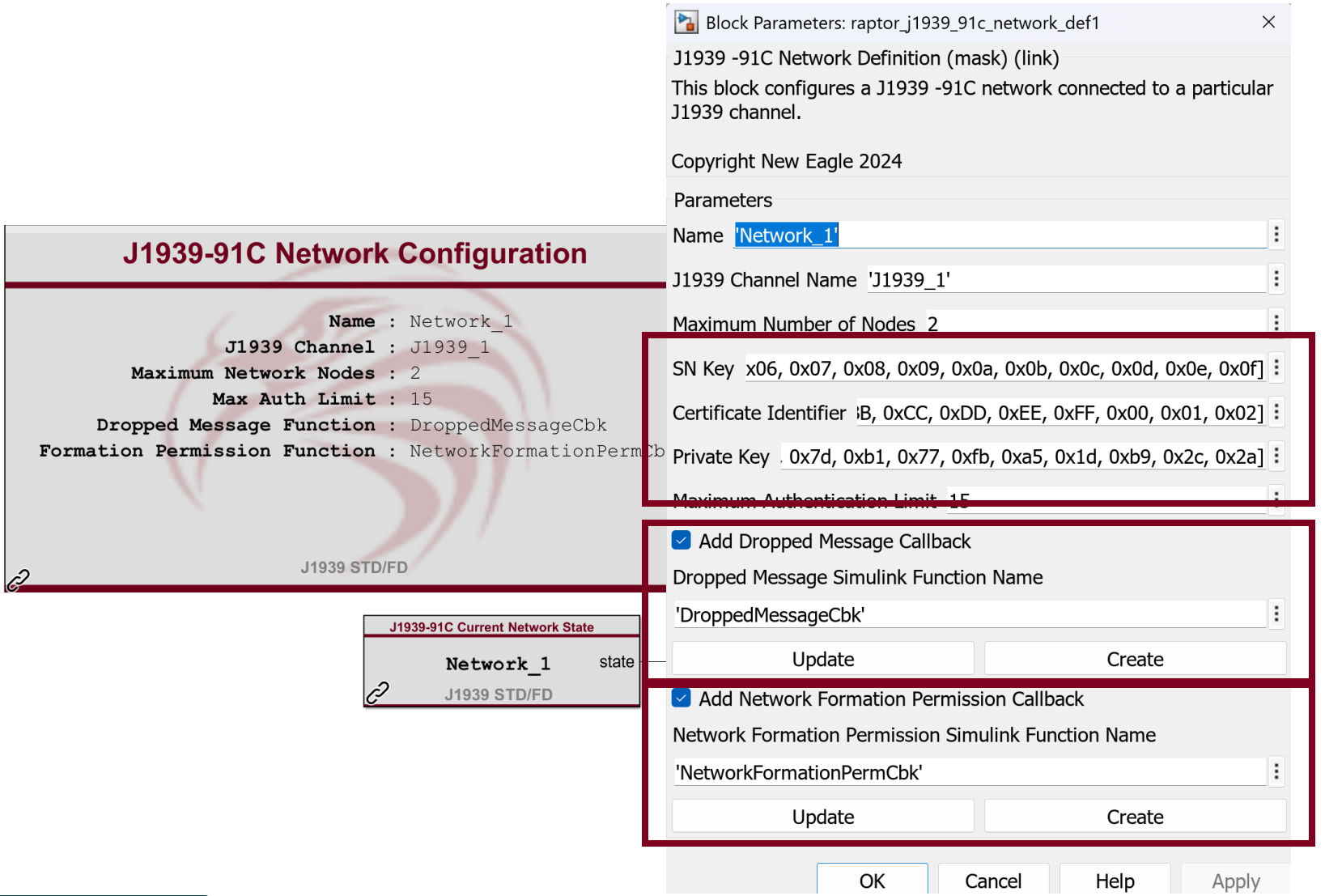
- Automotive Security
- J1939-22
- J1939-91C
- **Raptor Solution**

J1939-22 Transport Protocol





J1939-91C Network Definition

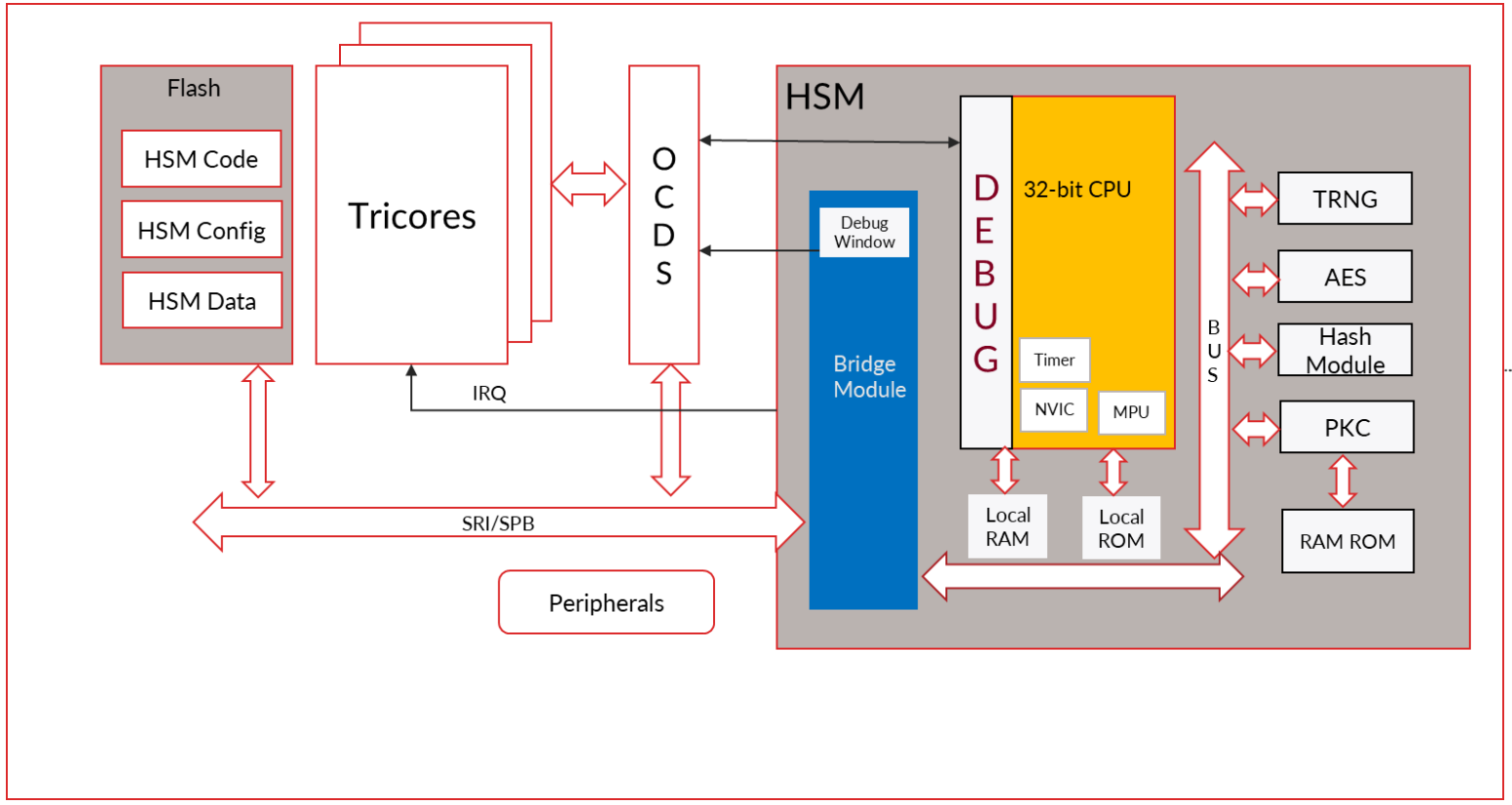


!!!!

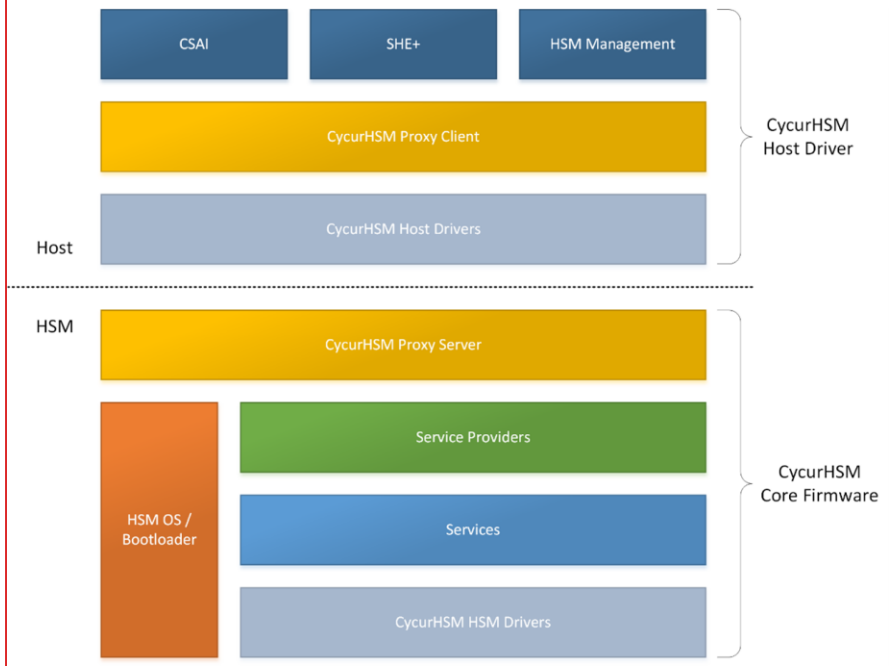
HSM Architecture and CycurHSM

new eagle
RAPTOR® INNOVATION SUMMIT 2025

Hardware Security Module (HSM)

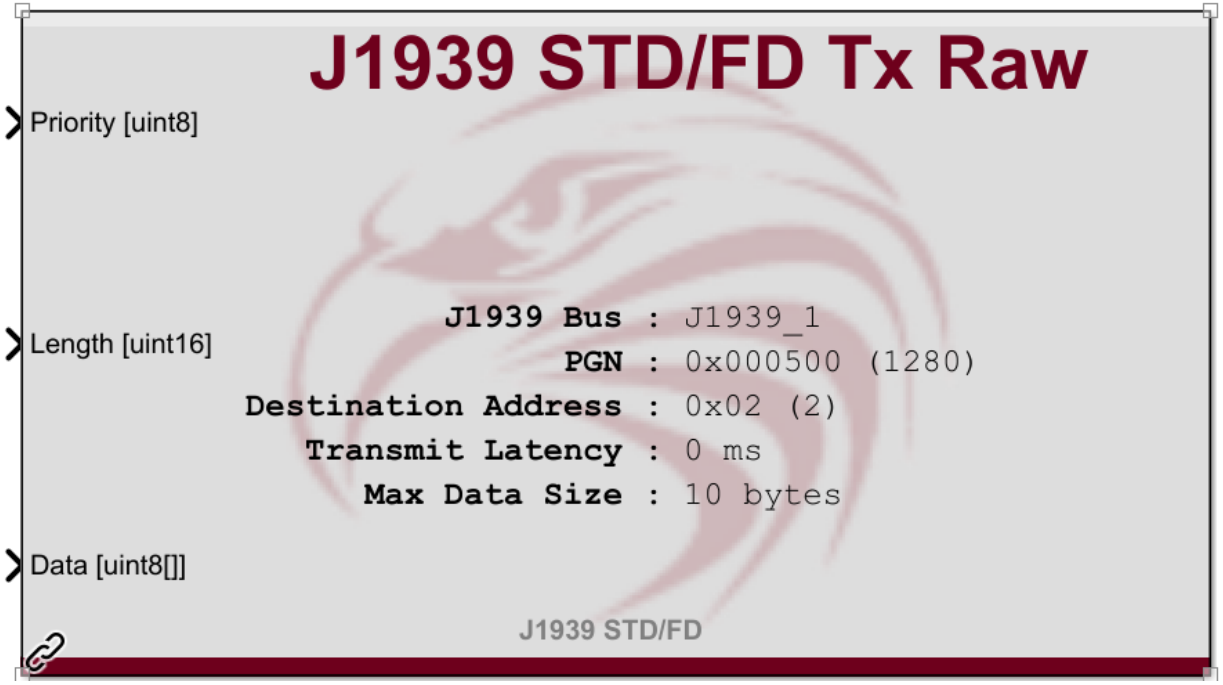


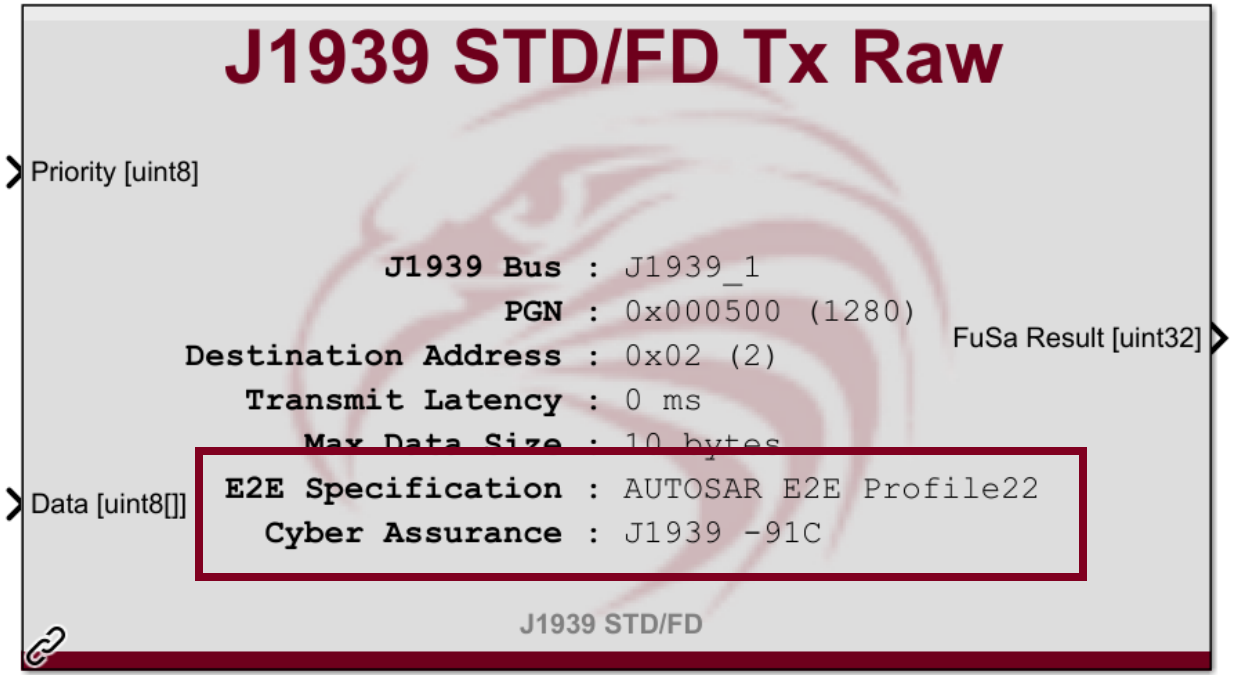
ETAS Cycur HSM software



INNOVATE FASTER. SCALE SMARTER

Transmit Block

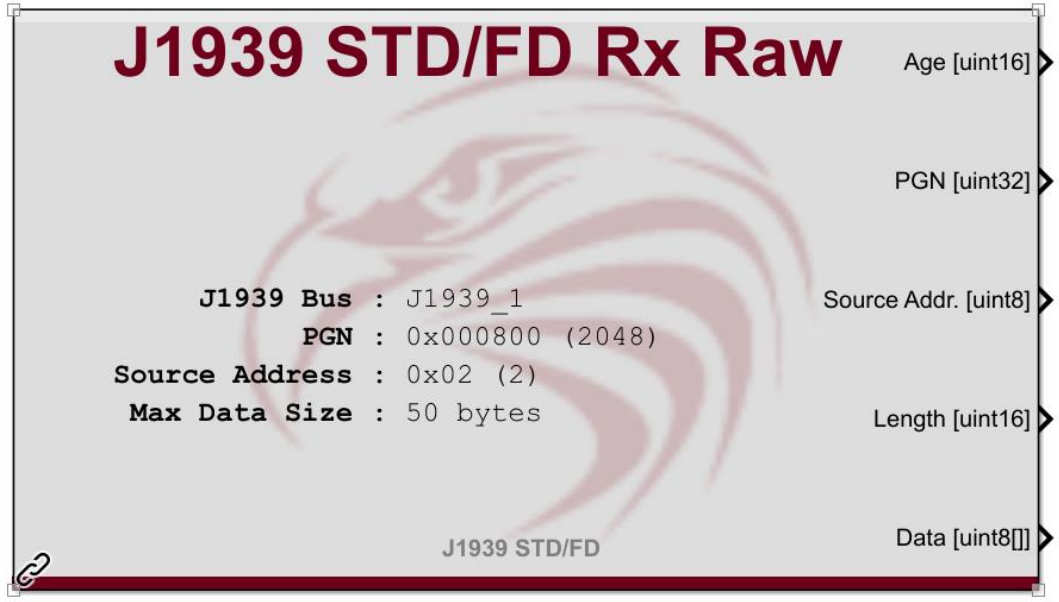


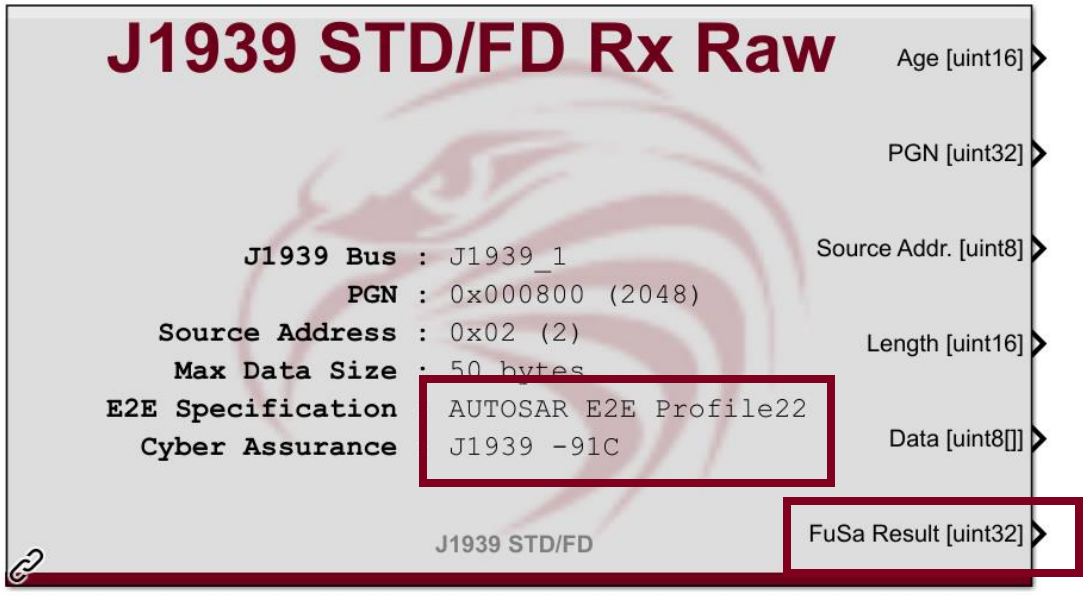


Receive Block

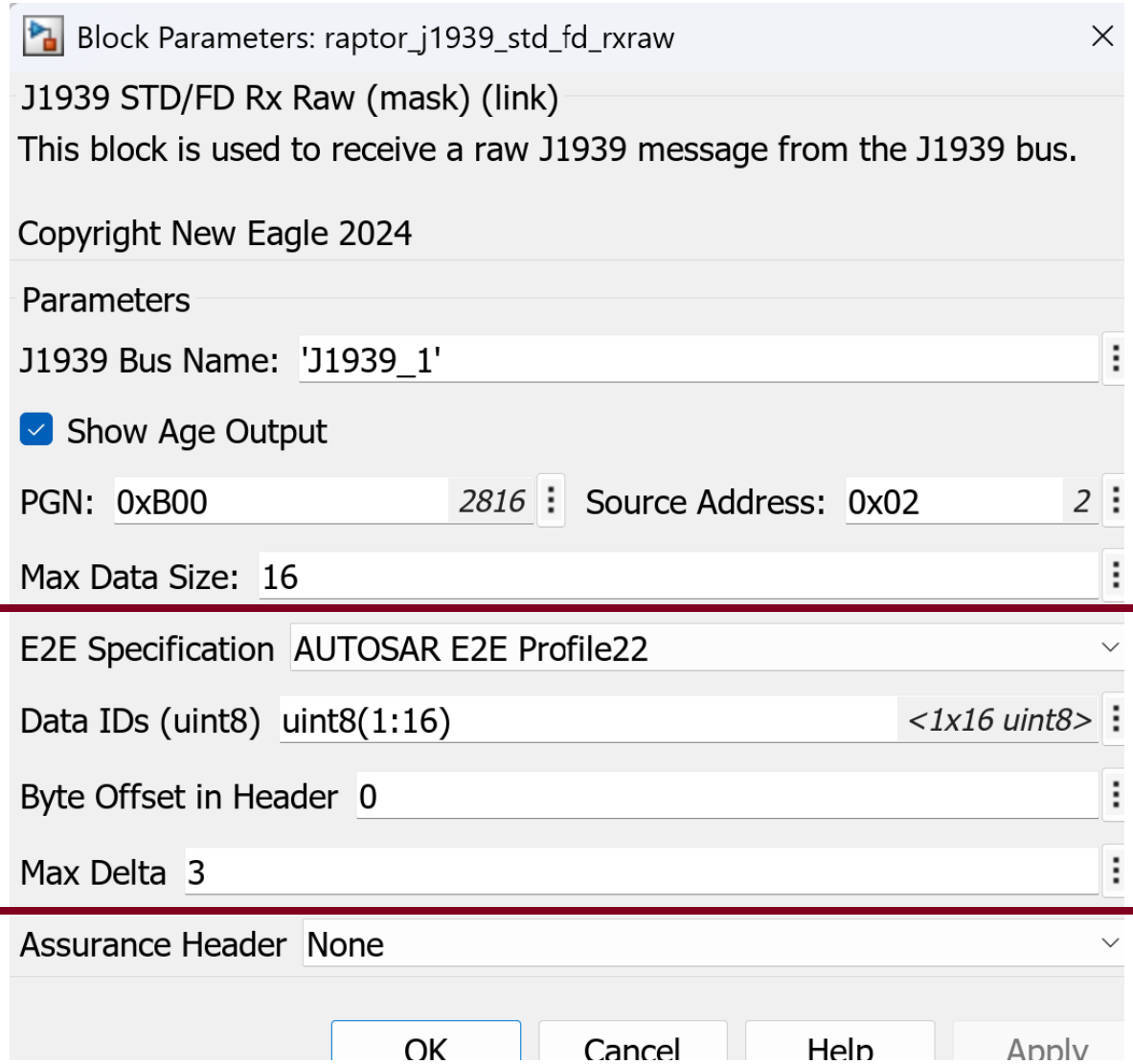
new eagle

RAPTOR®
INNOVATION
SUMMIT 2025

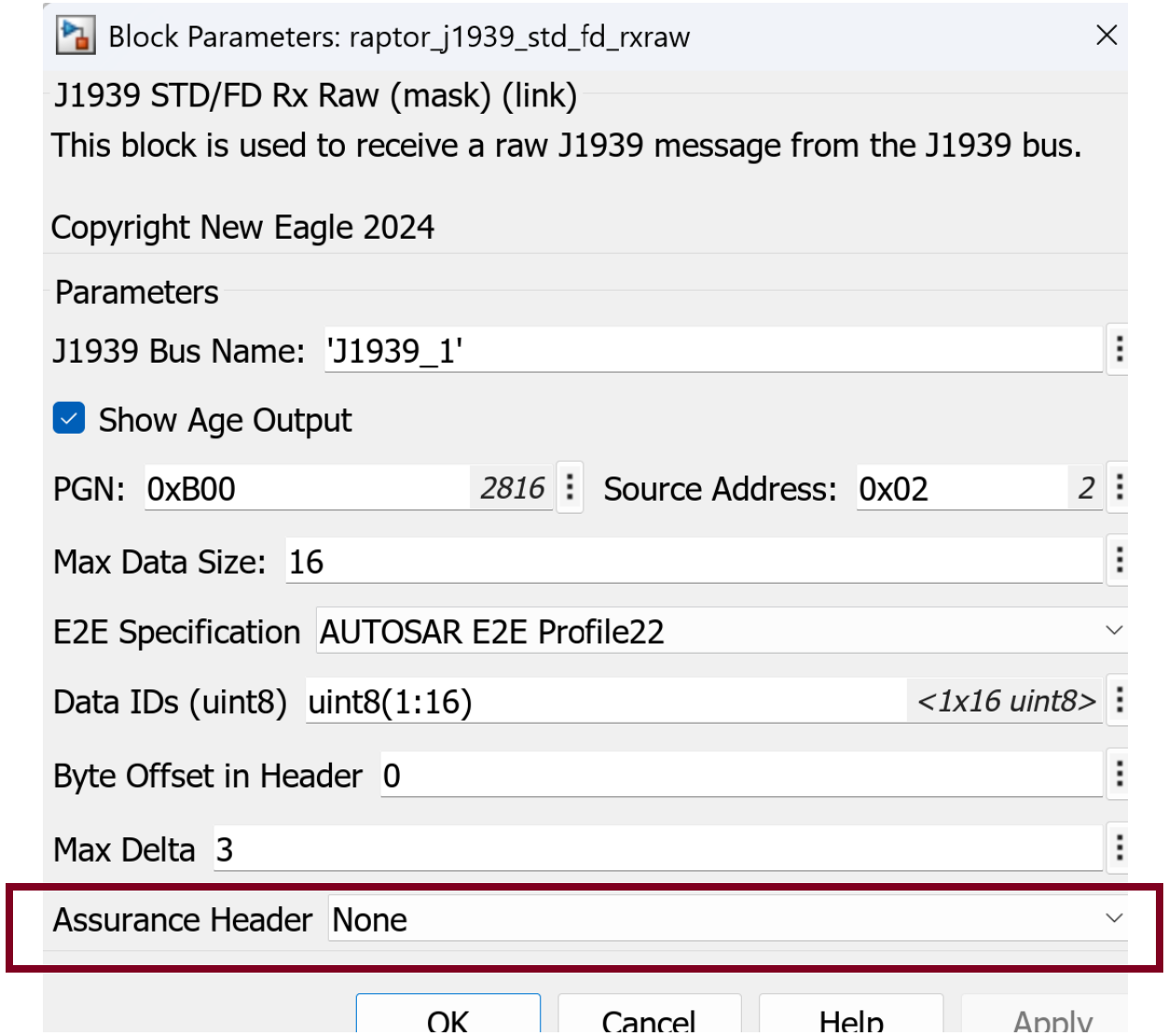




J1939-22 E2E Configuration



J1939-22 E2E Configuration



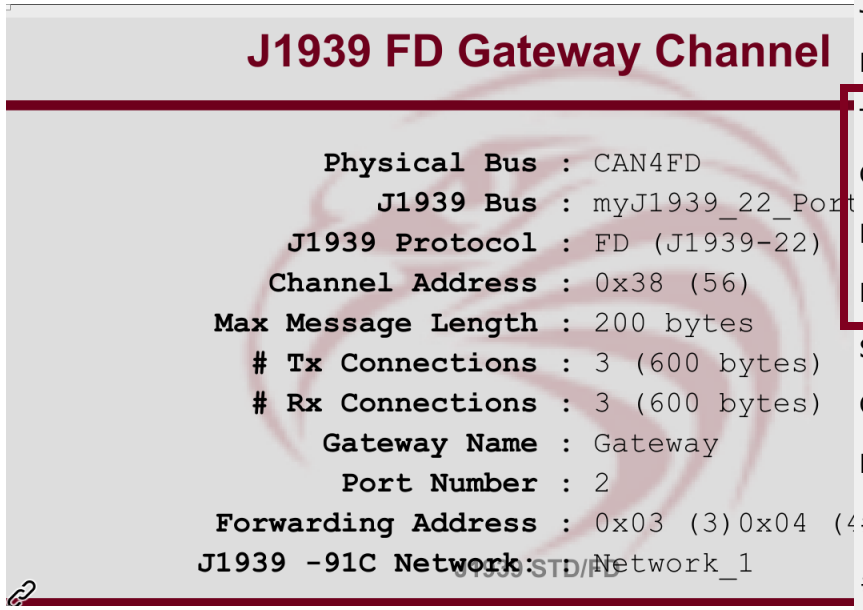
J1939-22 Assurance Configuration

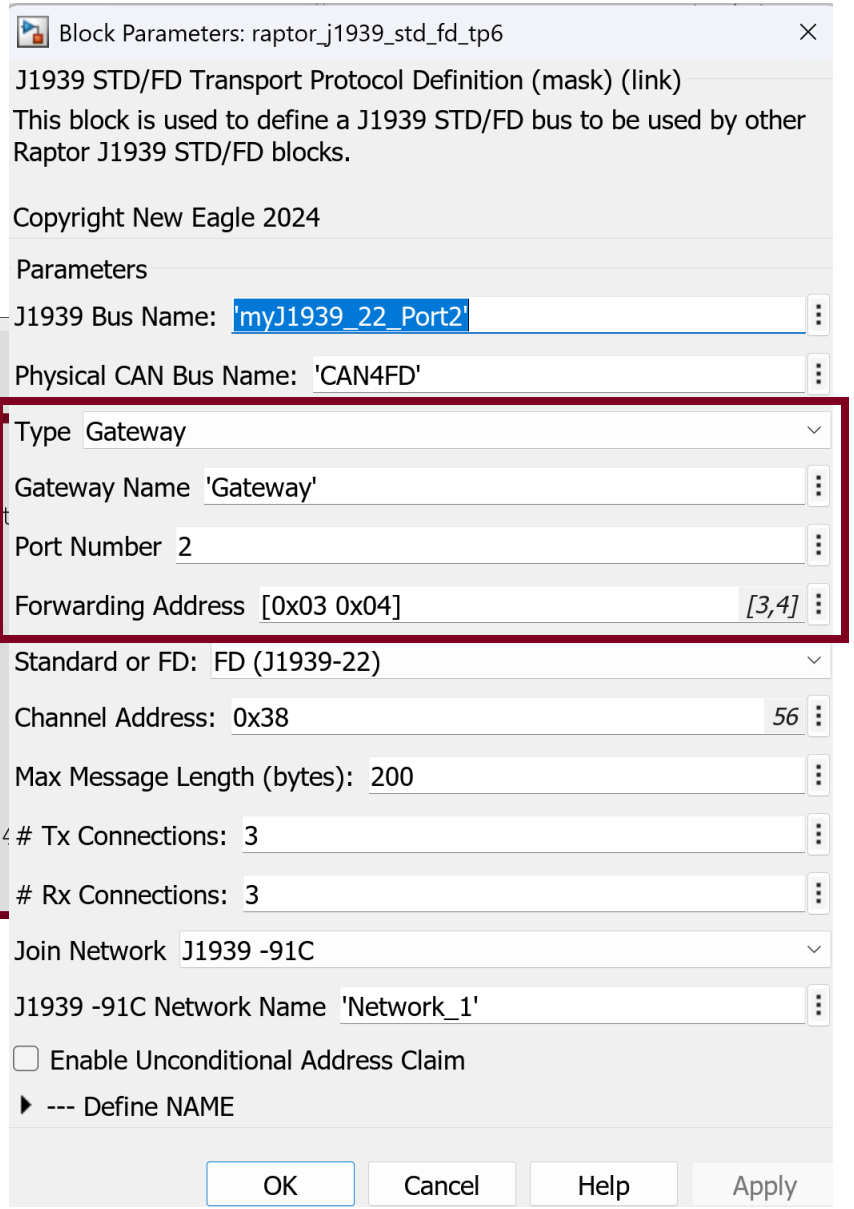
new eagle

RAPTOR®
INNOVATION
SUMMIT 2025

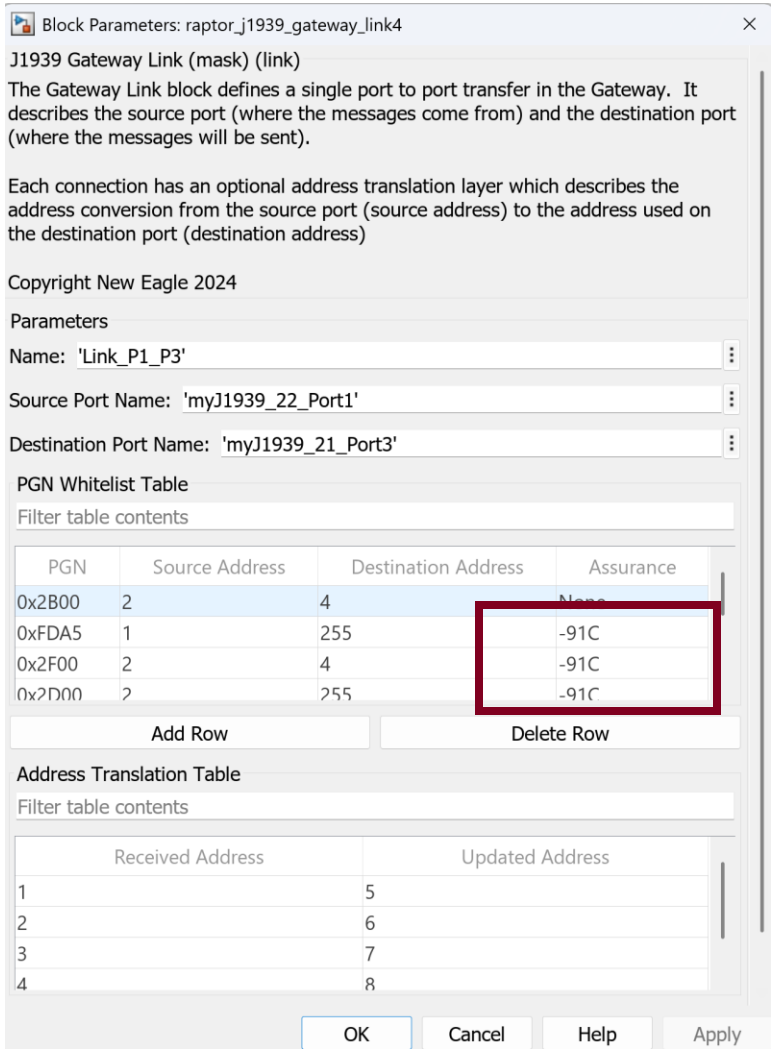
INNOVATE FASTER. SCALE SMARTER

J1939-22 Gateway

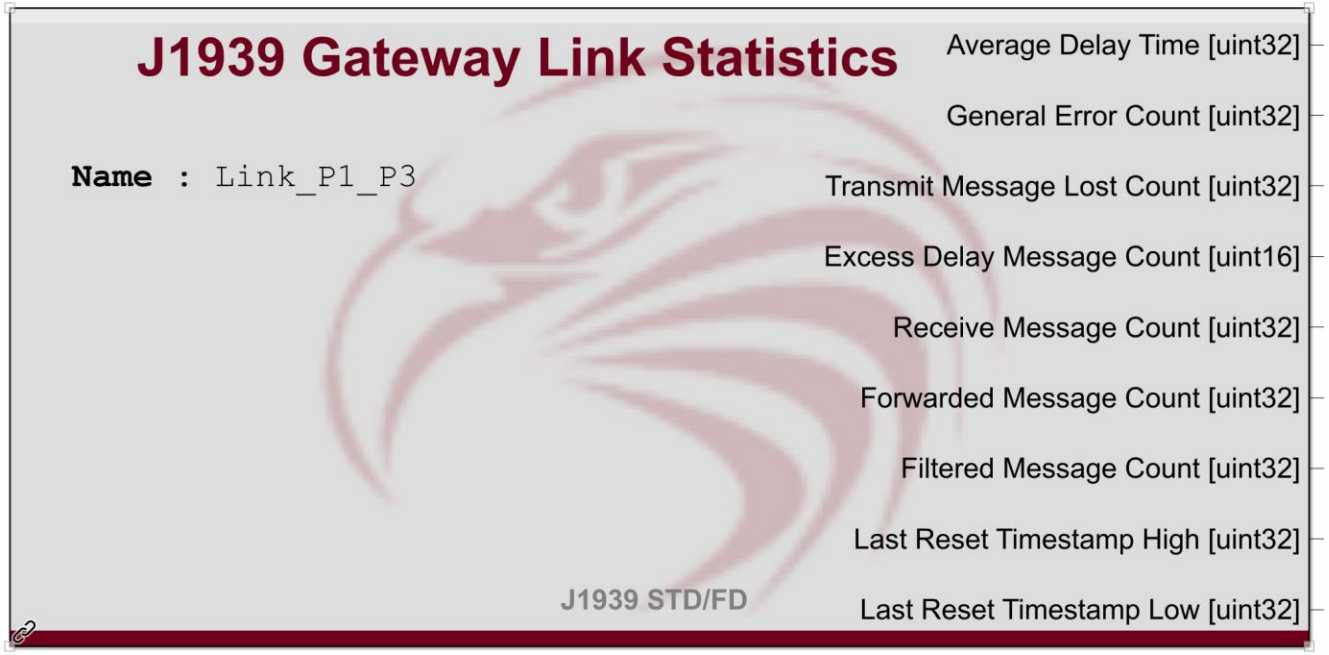




J1939-22/-21 Gateway Link Configuration



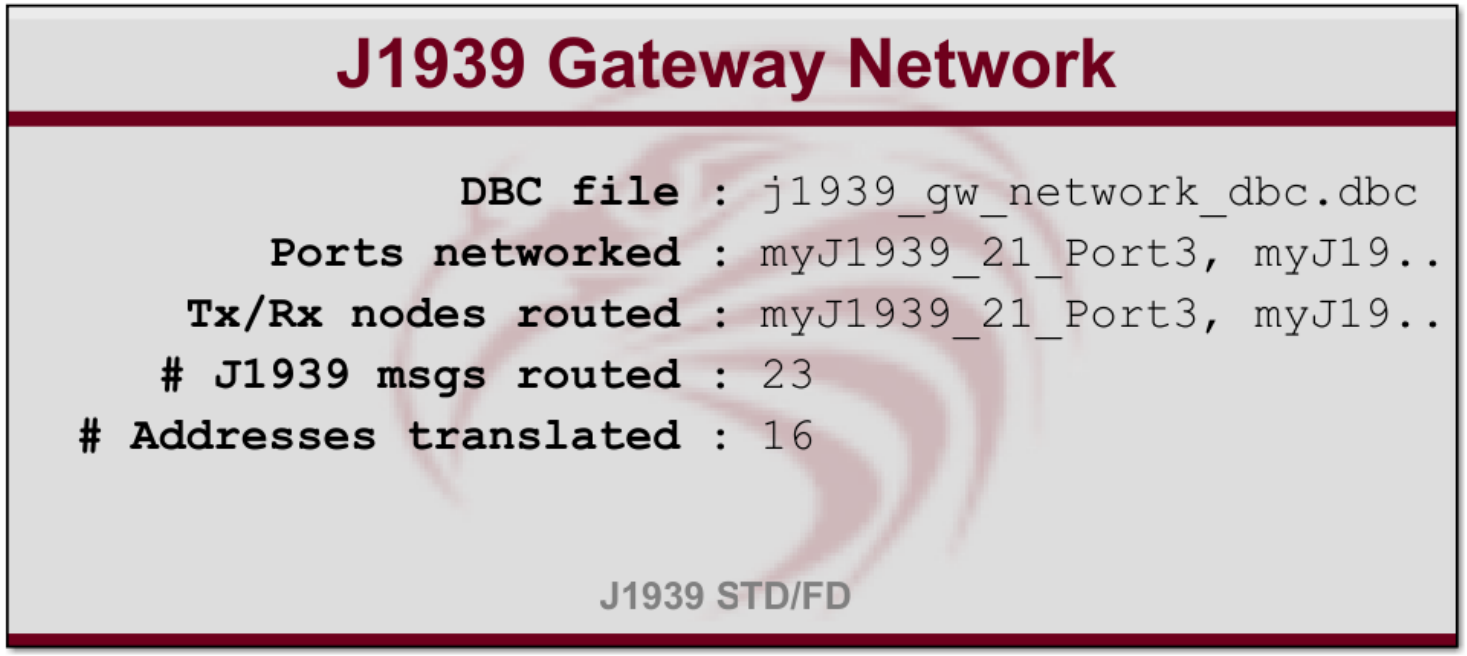
J1939-22/-21 Gateway Statistics



J1939-22/-21 Gateway Network Configuration

new eagle

RAPTOR®
INNOVATION
SUMMIT 2025



Summary

new eagle

RAPTOR®
INNOVATION
SUMMIT 2025

SecOC

Why its important

Protocols

J1939-22

J1939-91C

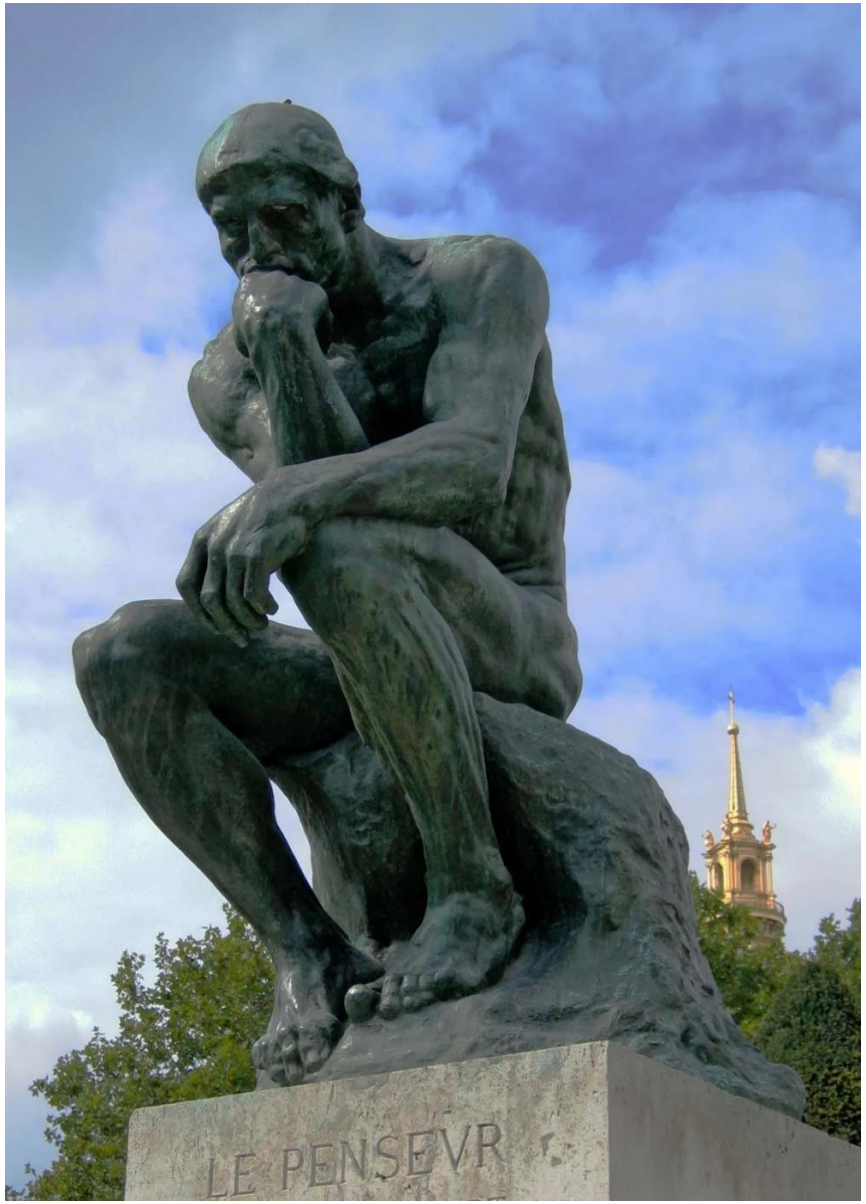
AUTOSAR P22 Support

Raptor Solutions

Protocol Support

Gateway

Questions?



new eagle

RAPTOR®
INNOVATION
SUMMIT 2025

INNOVATE FASTER. SCALE SMARTER