

Enhancing the Security of your Vehicles: New Standards for Vehicle Cyber Security Defense



Mark Zachos

Professor

University of Detroit Mercy

Empowering Fleet Security

New Standards and Methods
for Vehicle Cyber Security
Defense and
Experiential Learning
in Vehicle Cyber Engineering



Mark Zachos

markzachos.net

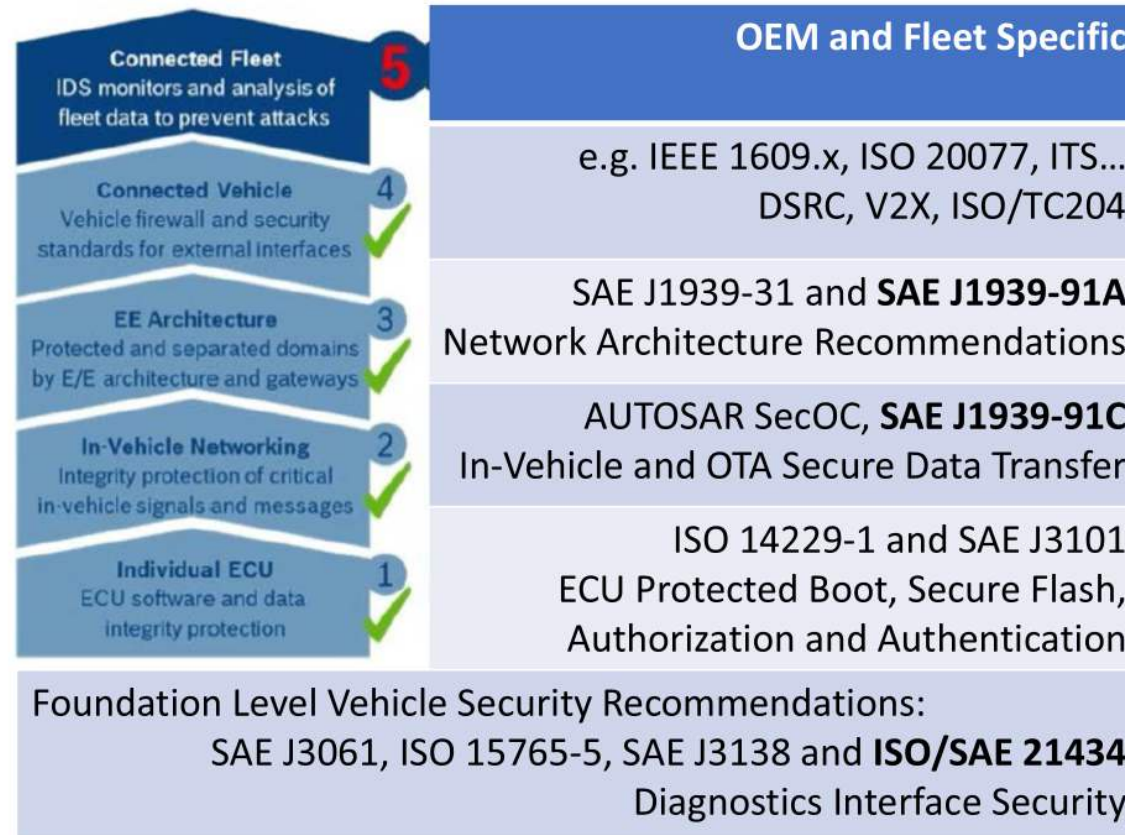
- Founder - The Dearborn Group Inc.; President and CEO of DG Technologies,
- Chair - ATA/TMC's Fleet Maintenance Cybersecurity Task Force
- Chair - SAE J1939 Cyber Security Task Force and Vehicle Diagnostics Link Security Committee
- Director – Vehicle Cyber Engineering at UD-Mercy



Agenda

- ✓ Overview of new technical standards for vehicle cyber security
 - ✓ ISO/SAE 21434, SAE J1939-91A, J1939-91C, and SAE J2534
- ✓ Discover how a Cyber Security Rating Framework (CSRF) can provide standardized way to assess and improve your fleet's cyber defenses.
- ✓ Demonstration of a J1939 network cyber attack using a vehicle testbed system developed at the University of Detroit Mercy.
- ✓ Discuss an Intrusion Defense System developed using SAE J1939-91C.

5 Layers of Vehicle Cyber Security Standards



SAE J1939-91C Big Picture

J1939-91C Requirements

- Important messages are kept secure
- Industry develops common key management
- Meet / exceed right-to-repair, securely

Security Characteristics

- Secure data flowing through a network should be relevant to the current system state ("fresh"),
- has not been intentionally or unintentionally modified ("integrity"),
- keeps private data private ("confidentiality"),
- is from a trusted source ("authentic") and
- the source is supposed to be participating in the conversation ("authorized").

ISO/SAE 21434

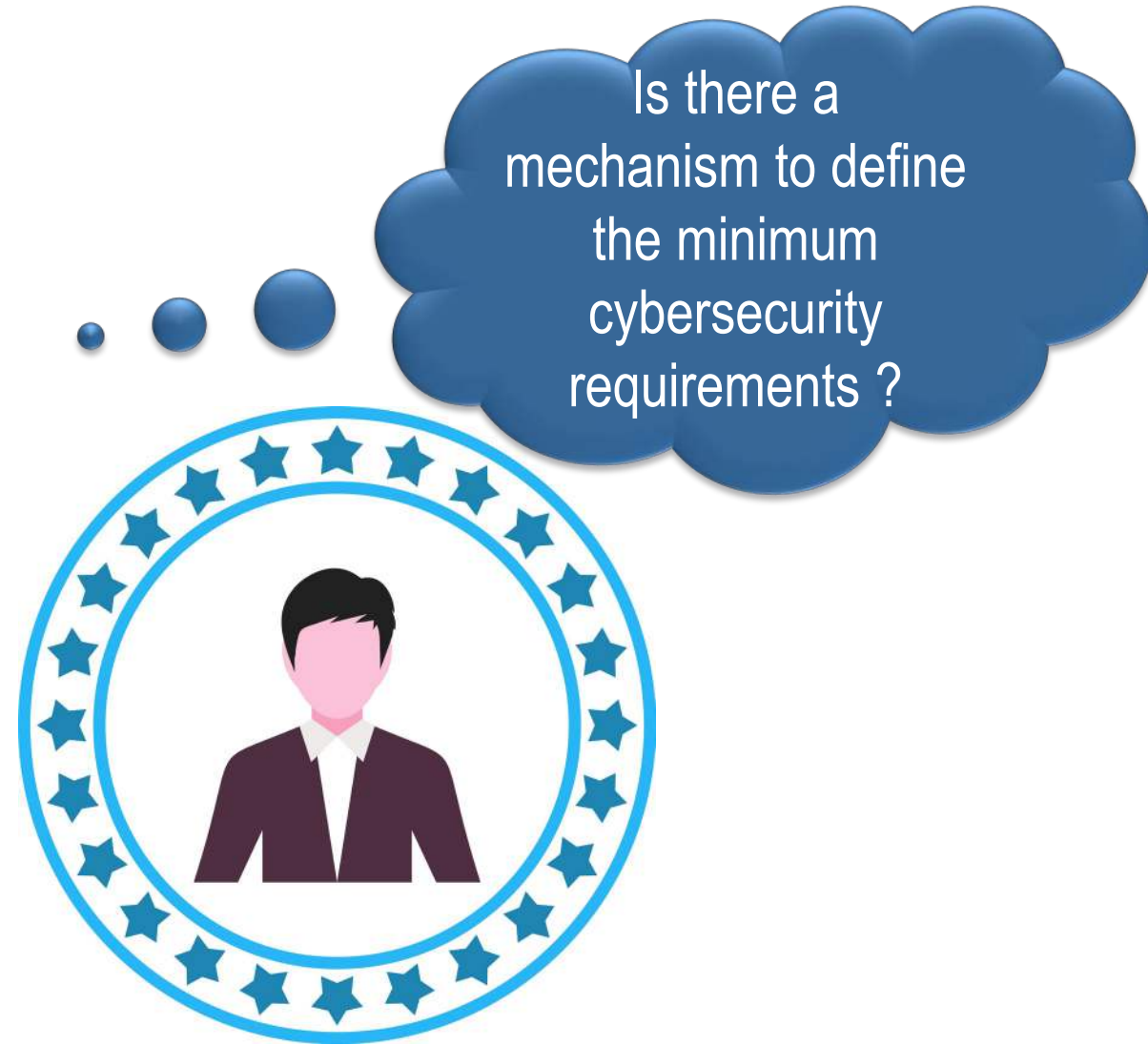
- Provides a framework for managing cybersecurity risks throughout the entire lifecycle of road vehicles.
- Applies to all electronic systems, components, and software in connected and autonomous vehicles, with the goal of reducing the risk of cyberattacks, ensuring user safety, and building trust.



ISO 21434 Certification

What and Why – Cybersecurity Rating Framework - CSRF

- Need a framework to standardize method for evaluating the cybersecurity posture of vehicles across different manufacturers. This ensures consistency in assessment and comparison
- A framework to define minimum cybersecurity requirements
- Specification ensuring that manufacturers comply with specified cybersecurity requirements



UD-M Research Projects and Technical Publications

2026-01-0092 Published 07 Apr 2026



The Golden Tester: Implementation and evaluation of a method to defend in-vehicle networks using SAE J1939-91C to authenticate network messages between multiple ECUs

Mark Zachos DG Technologies and UD-Mercy

Krishna Teja Medam International Motors LLC

Citation: Zachos, M. and Medam, K.T., "The Golden Tester: Implementation and evaluation of a method to defend in-vehicle networks using SAE J1939-91C to authenticate network messages between multiple ECUs," SAE Technical Paper 2026-01-0092, 2026, doi:10.4271/2026-01-0092.

Network Security Implementation

Mohamad Ali Mokhadder

John Potter

Mark Zachos



What and Why – Cybersecurity Rating Framework - CSRF

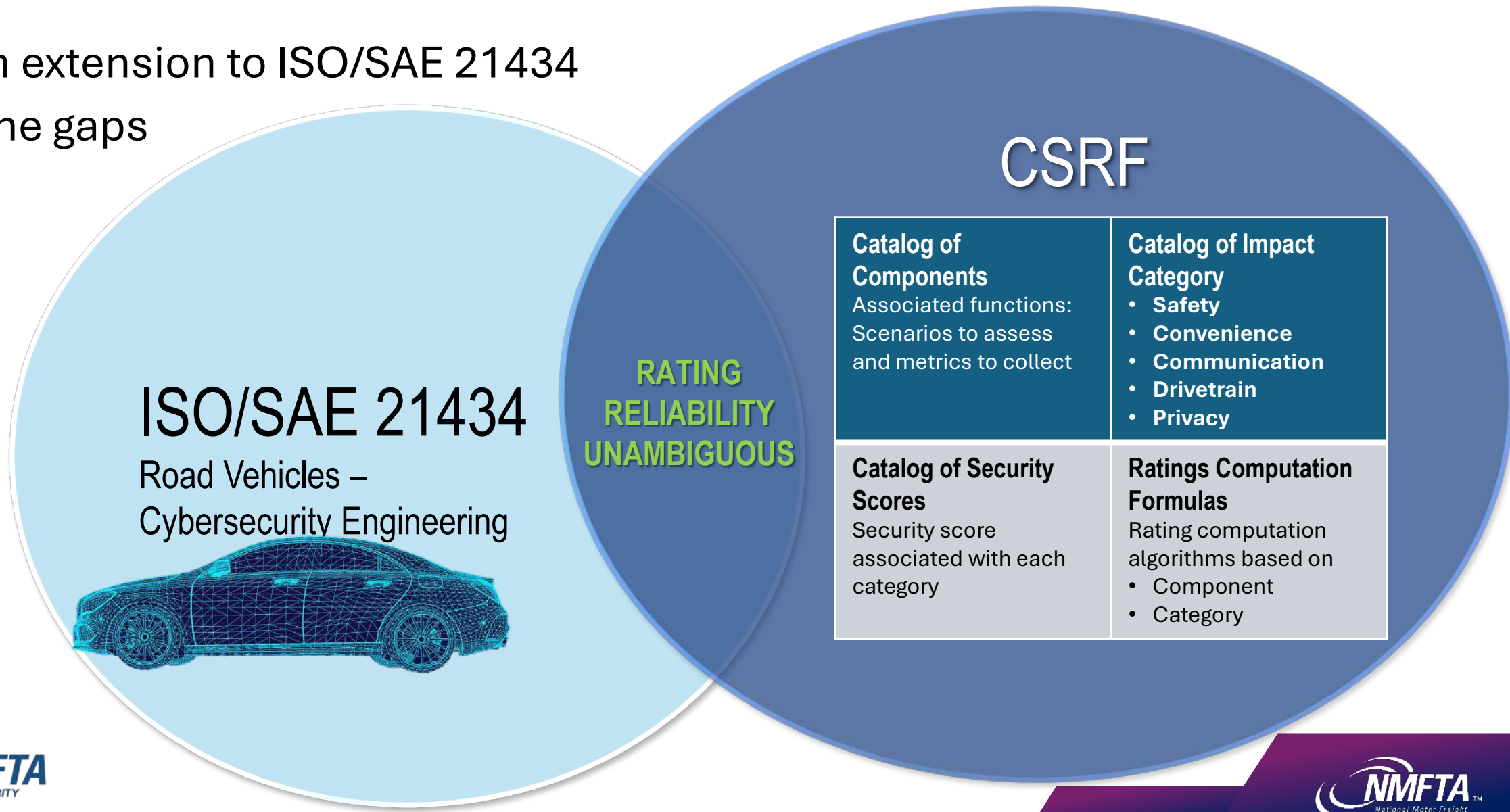
How much has the security improved with the measures I have taken?



- Need structured approach for evaluating security controls, vulnerabilities, and threats specific to vehicles
- A mechanism to validate if security testing is exhaustive, are there any gaps
- Track security improvements quantifiably
- Benchmark different vehicles based on a common measure

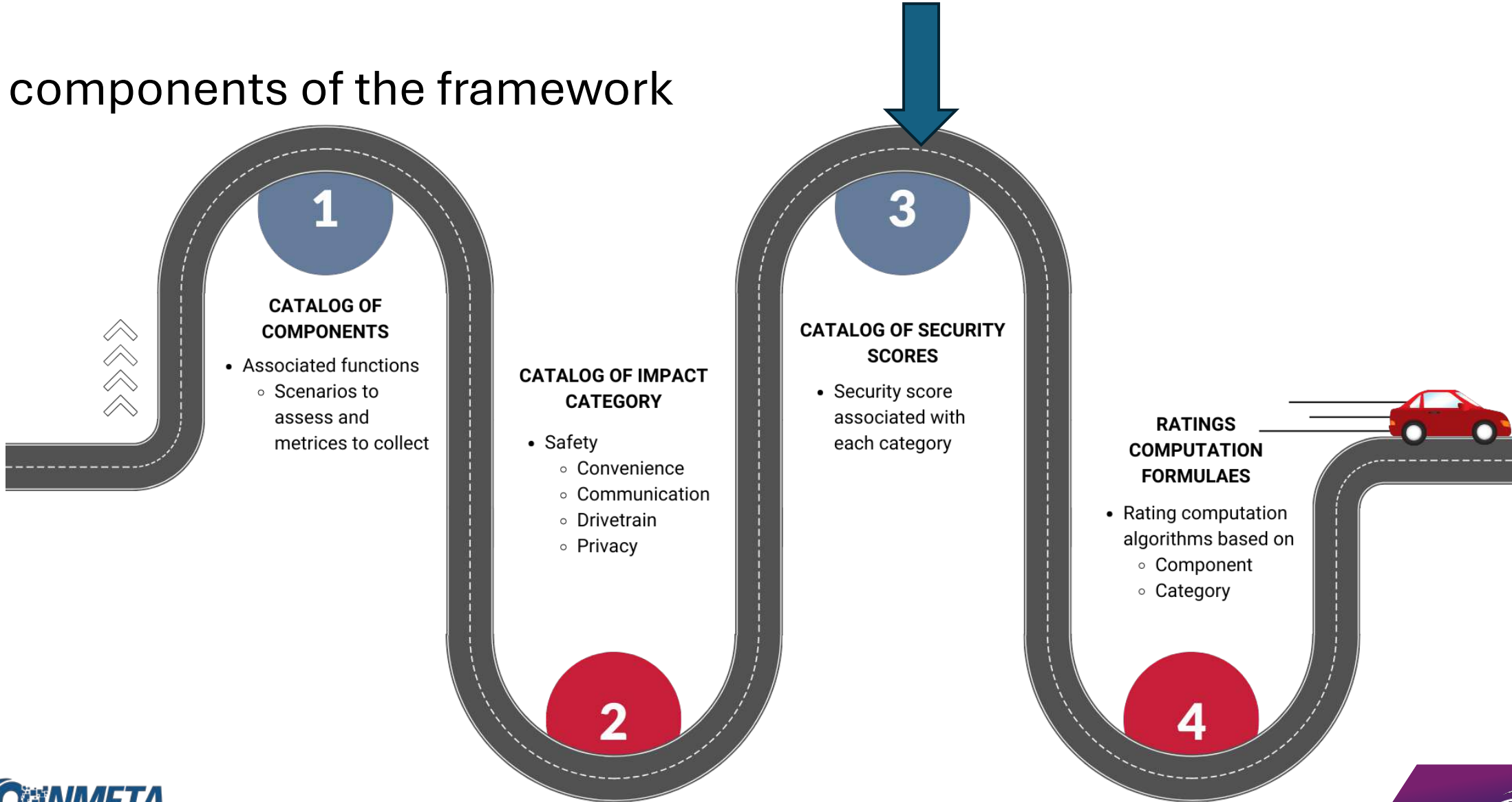
CSRF – Cybersecurity Rating Framework

- CSRF an extension to ISO/SAE 21434
- Bridge the gaps



CSRF – Cybersecurity Rating Framework

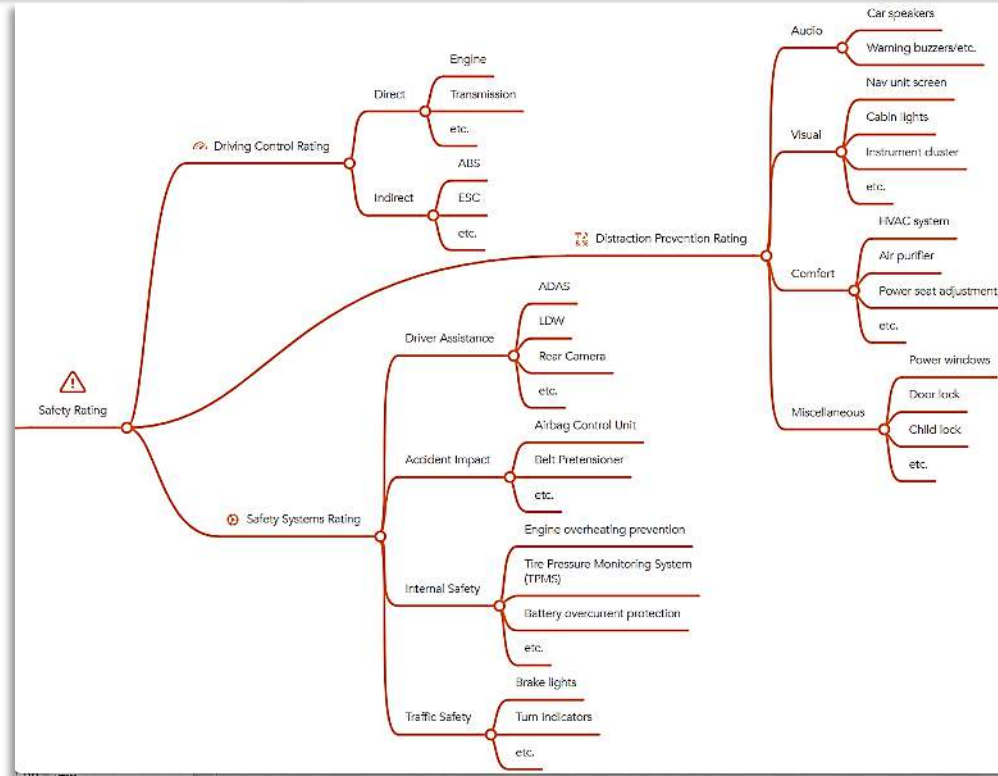
Key components of the framework



CSRF – Cybersecurity Rating Framework

- Catalog of security weights
- Vehicle functionality grouped by impact category

Weight	Description
1	LOW impact
2	MEDIUM impact
3	HIGH impact
4	CRITICAL impact



CSRF Applied to a Vehicle Using SAE J1939-91C

Evaluation Based On ISO/SAE 21434

Attack Scenario	Impact Rating	Attack Feasibility Rating	Risk Value
Spoofing of messages through compromised critical ECU	HIGH	LOW	3
Man-in-the-middle attack	MEDIUM	LOW	2
Starvation attack	HIGH	MEDIUM	4
ECU impersonation attack	HIGH	LOW	3
Replay attacks	MEDIUM	MEDIUM	3
Kill Chain	HIGH	MEDIUM	4
Fuzzing	MEDIUM	MEDIUM	3
Denial of service attack	HIGH	LOW	3

CSRF Risk Value

Attack Scenario	Risk Value	CSRF Cyber Impact Category and Weight	Weighted Risk Value
Spoofing of messages through compromised critical ECU	3	4	12
Man-in-the-middle attack	2	2	4
Starvation attack (impacting critical functionality)	4	2	8
ECU impersonation attack	3	4	12
Replay attacks	3	2	6
Kill chain	4	3	12
Fuzzing	3	2	6
Denial of service attack	3	3	9

CSRF Applied to a vehicle using SAE J1939-91C

Computing the Rating



Maximum Score

The maximum score will be equal to the Sum (Max Risk Value * CSRF Category Impact Weight)



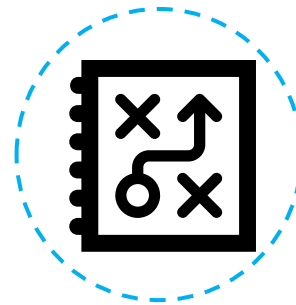
Final CSRF Score

The final CSRF score for the example vehicle utilizing the SAE J1939-91C protocol simulation is - 69/110.



Maximum Risk Value

5 as per ISO/SAE 21434. The total CSRF weighted risk value is Sum (All individual Weighted Risk Values).



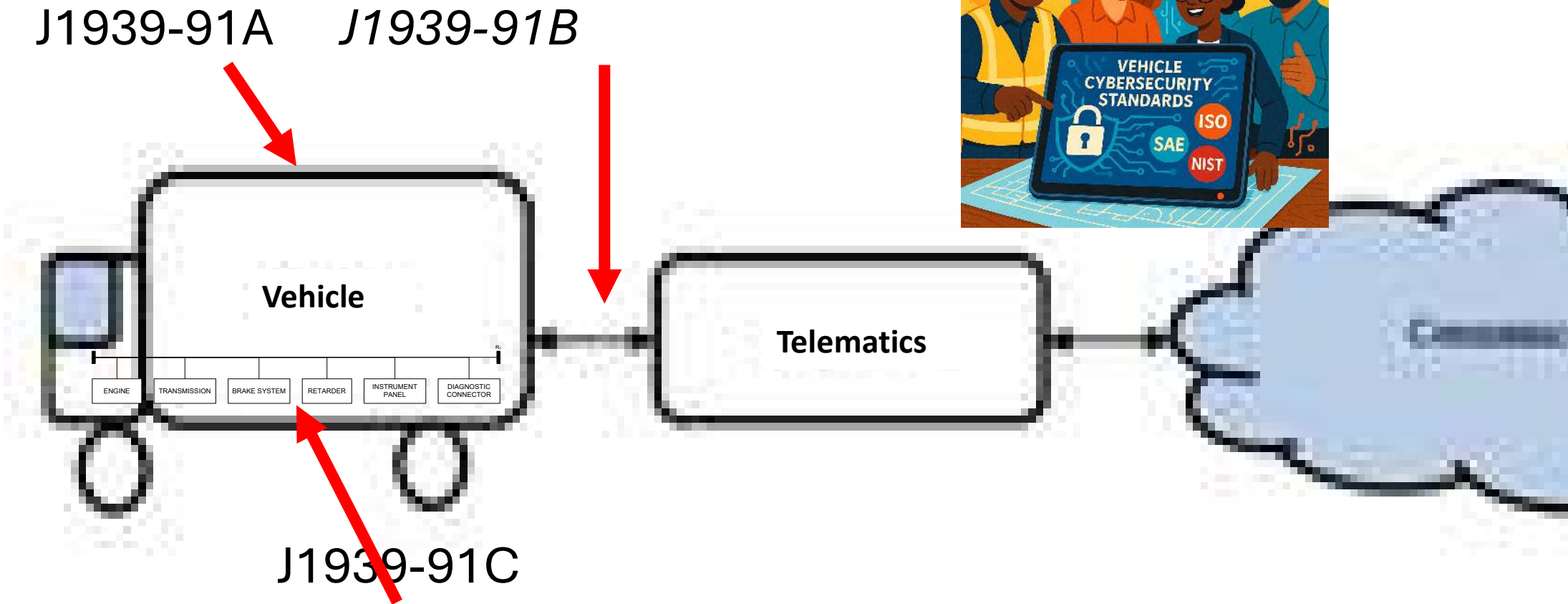
% Weighted Risk Value

The percentile of Weighted Risk Value is 63%. This represents that this example vehicle network using SAE J1939-91C **CSRF Security Rating is 2**

The security score of the entire vehicle variant can be computed based on the individual scores for other components and features in the vehicle.

SAE J1939 Network Security

J1939-91 Scope

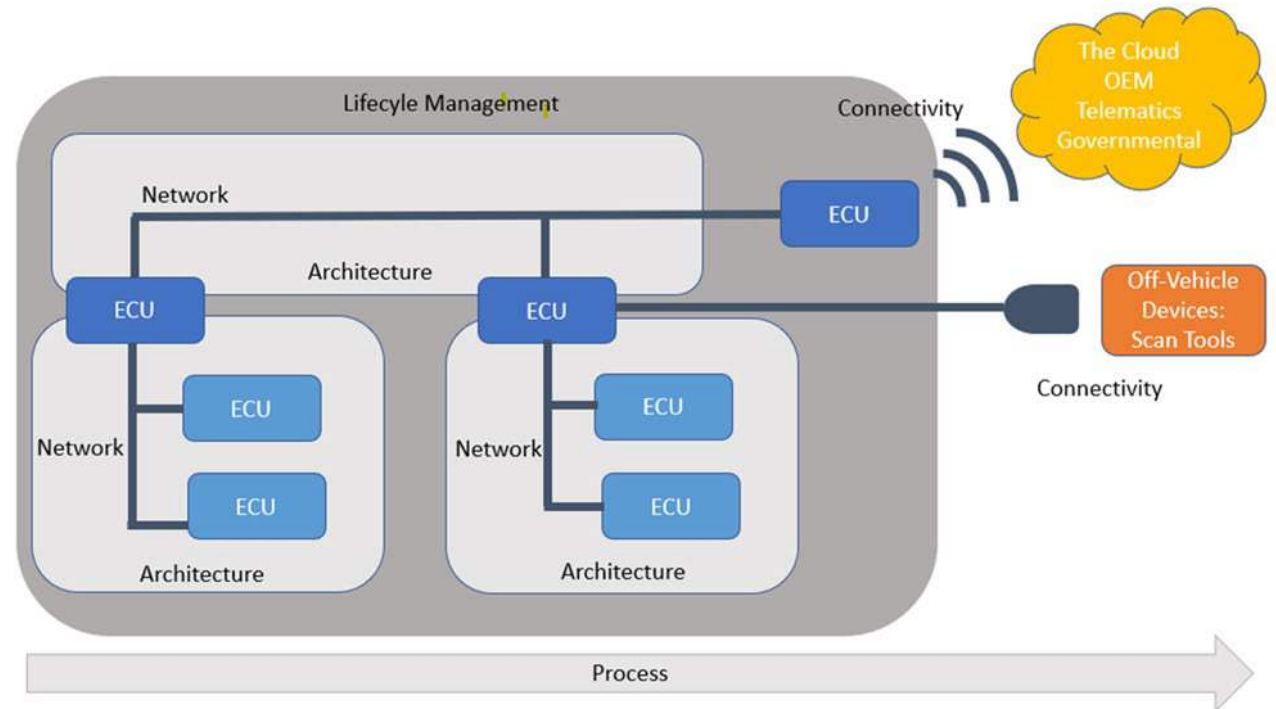


SAE J1939-91“A”

Foundation Layer Security

J1939-91A defines recommendations for security of the vehicle side of the J1939-13 connector.

- Recommendations for vehicle communications functions with a device which is connected to J1939-13 interface - diagnostics interface security. [Similar to SAE J3138 diagnostics link security and SAE J3005-2 “dongle” device security]
- General requirements for “Imposter Reporting” for devices that may spoof J1939-13 Source Addresses.
- Update General Vehicle Network Gateway recommendations and network topology reference related to J1939-31



J1939-91”C” Big Picture

Challenges

- 100% Security is Not Possible
- We are protecting critical infrastructure

Goals

- Make it too expensive (time/money) to make attacks worthwhile
- Set a high bar

Key Concepts in J1939-91C

- Node Authentication
- Secure Key Generation, Rekeying
- Network Formation
- Data Integrity, Data Freshness
- Insecure, Authentic and Confidential messages

SAE has provided this Draft document for the SAE Committee. This document is SAE-copyrighted, intellectual property. It may not be shared, downloaded, duplicated, or transmitted in any matter outside of the SAE Committee without SAE's approval. Please contact your staff representative for additional information.



SURFACE VEHICLE RECOMMENDED PRACTICE

J1939™-91C

MTH2022

Issued

2022-XX

CAN FD Network Security

RATIONALE

This document facilitates the secure use of SAE J1939 CAN networks with flexible data rate (CAN FD) data frame format for communication use cases. This recommended practice provides methods for establishing trust and securing messages on CAN FD networks with optional encryption.

FORWARD

The SAE J1939 communications network is developed for use in heavy-duty environments and suitable for the integration of different combinations of loose package components, such as engines and transmissions, that are sourced from many different component suppliers. The SAE J1939 common communication architecture strives to offer an open interconnect system that allows the ECUs associated with different component manufacturers to communicate with each other.

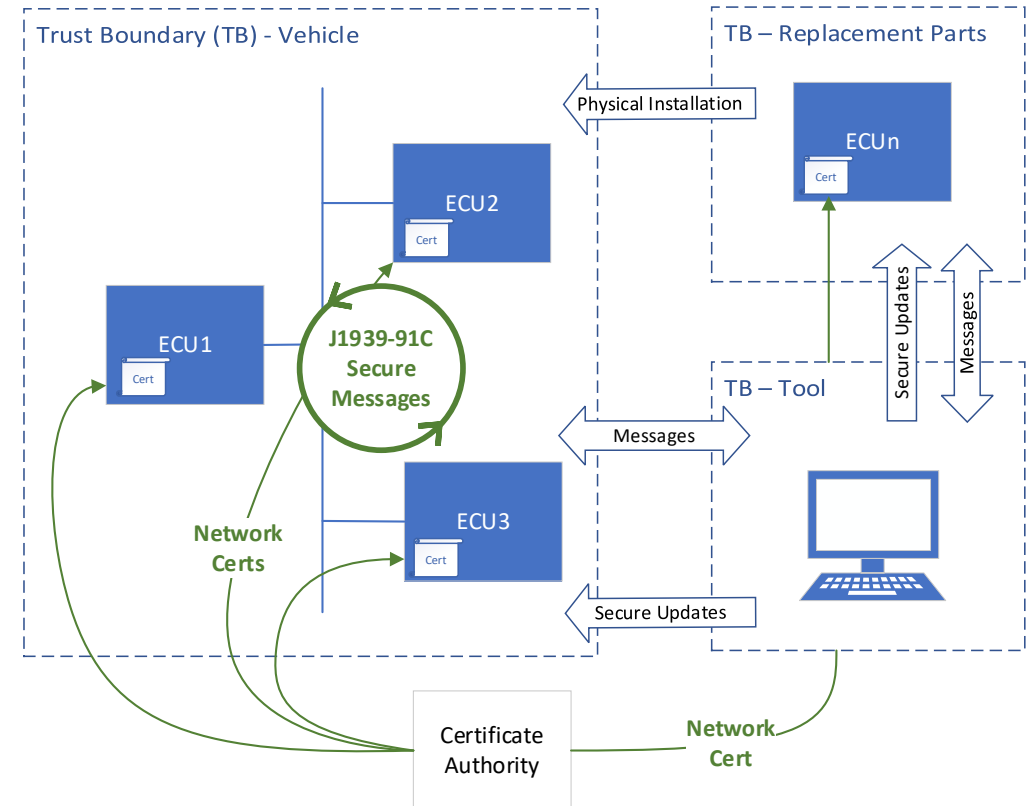
The SAE J1939-91A/B/C provide cybersecurity recommendations for secure architectures, secure vehicle to infrastructure communications and secure on-board communications. The SAE J1939-91A document focuses on security measures related to on-vehicle network architecture and security measures for communication interfaces between devices or networks. The SAE J1939-91B focuses on secure over the air communications via a telematics interface to the vehicle.

This particular document, SAE J1939-91C, describes the cryptographically secure transfer of messages between ECUs with optional encryption. It describes the techniques required to establish trust through key management and extend it throughout the vehicle's life cycle.

J1939-91C Key Concepts

What is 91C and What isn't 91C

- Is
 - Secure CAN-FD messages between trusted ECU's
 - Trust established via PKI certificates
- Isn't
 - Diagnostics
- Requires
 - Secure ECU Hardware
 - Secure S/W updates



J1939-91C Key Concepts

- **Node Authentication**
 - All nodes/ECUs communicating on the network are authorized by a trusted third party
 - Authentication is handled during Network formation phase
- **Data Integrity or Message Authentication**
 - Ensures that the data received is not tampered after being transmitted from the original source
 - A block cipher-based message authentication code (CMAC) is added to the security overhead
- **Message Confidentiality**
 - For critical messages, confidentiality is obtained by encryption per the SecOC/E standard.
 - AES-128 encryption is employed with a locally generated symmetric key
- **Secure Key Generation**
 - Network ECUs cooperatively establish a new set of cryptographic keys for each session
 - Typically, every power cycle is a new session
 - Hence, hacking to decode the keys for a single session will not benefit decoding for any other session
- **Rekeying**
 - The standard includes a provision for generating new session keys during a given power cycle
 - One such instance includes adding a Rekeying is required, for example,
- **Data Freshness**
 - Freshness Value (FV) is a count maintained by each transmitting node and each receiving node for every ECU sharing the network
 - FV is an enabler to prevent replay attacks
- **Message Types**
 - 3 types: (1) Insecure, (2) Authentic and (3) Authentic and Confidential

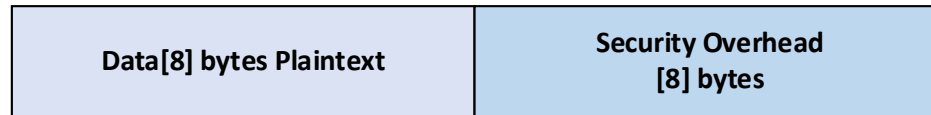
J1939-91C Key Concepts (Cont'd)

Three Message Types

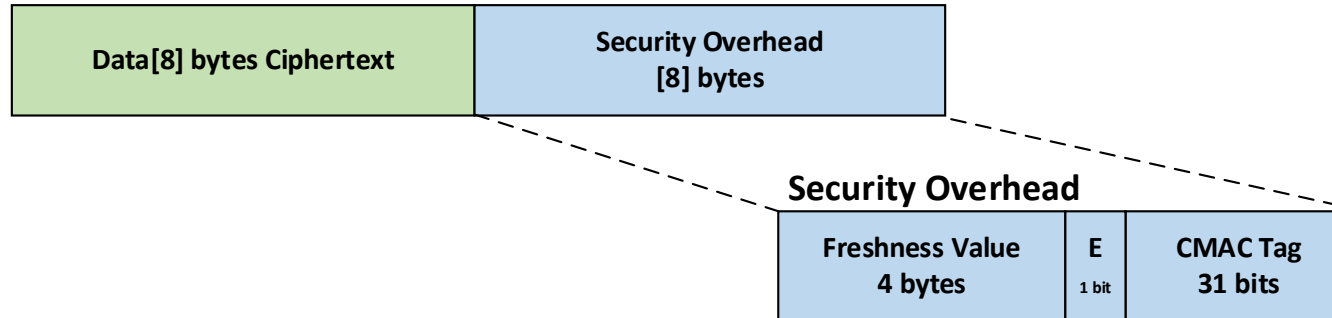
Insecure Message



Authentic Message



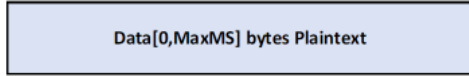
Authentic and Confidential Message



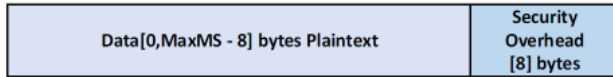
J1939-91C CAN Message Structure

Three Message Types

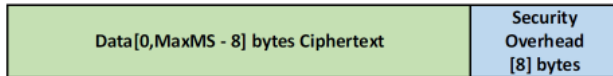
Insecure Message



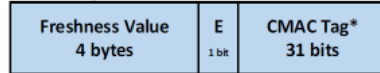
Authentic Message



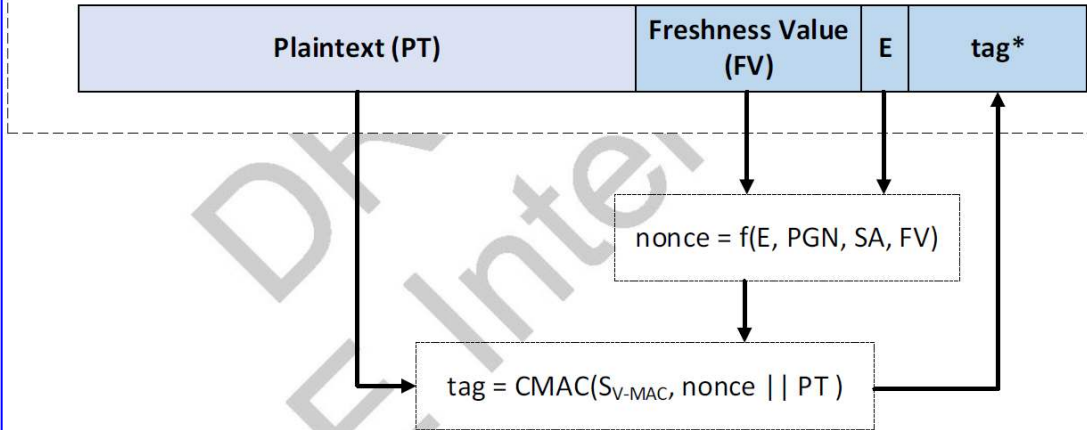
Authentic and Confidential Message



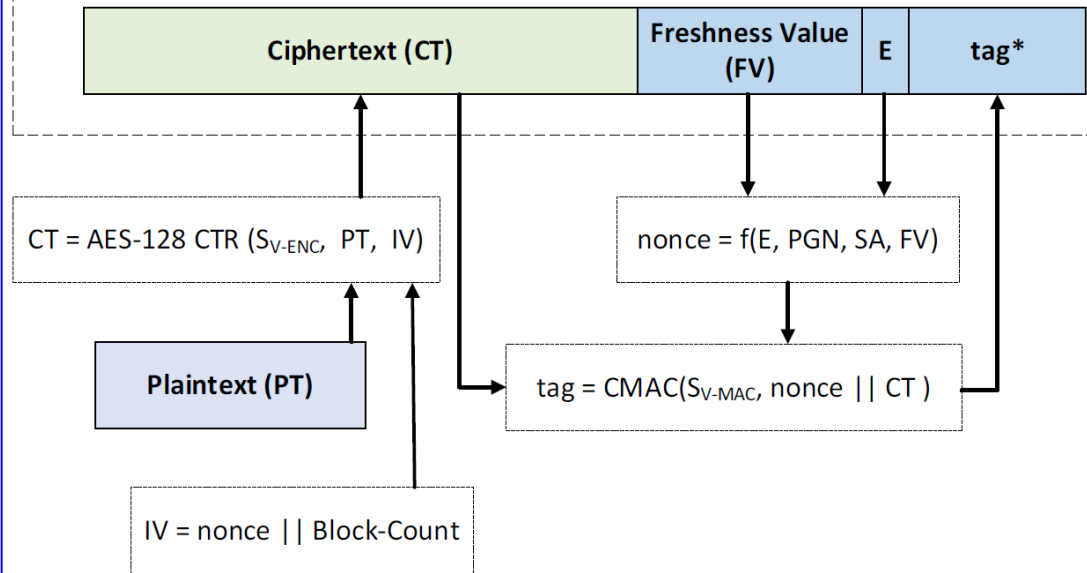
Security Overhead



Authentic Message

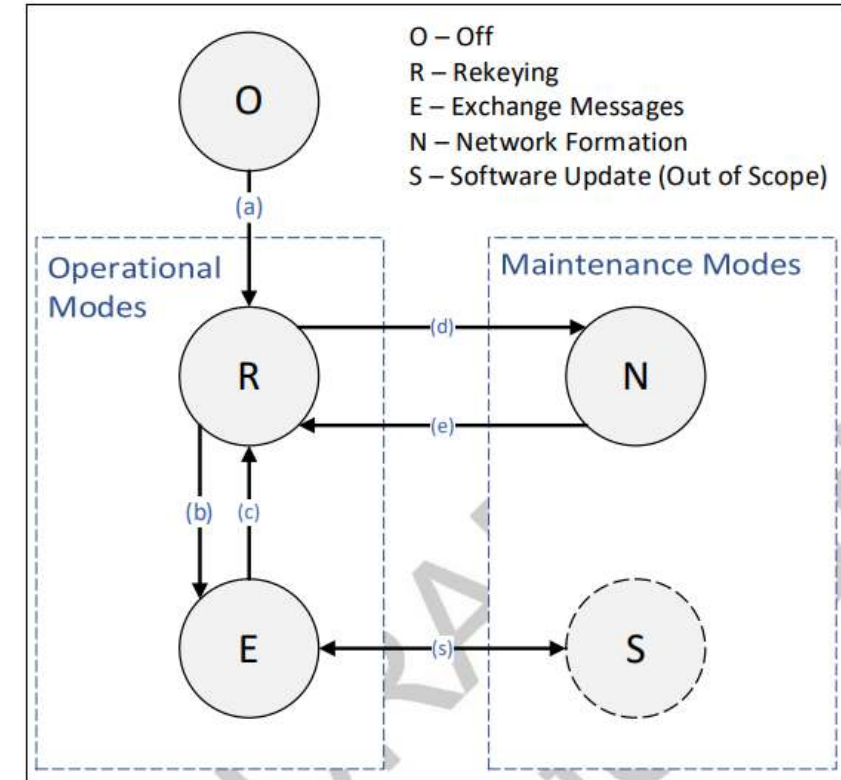
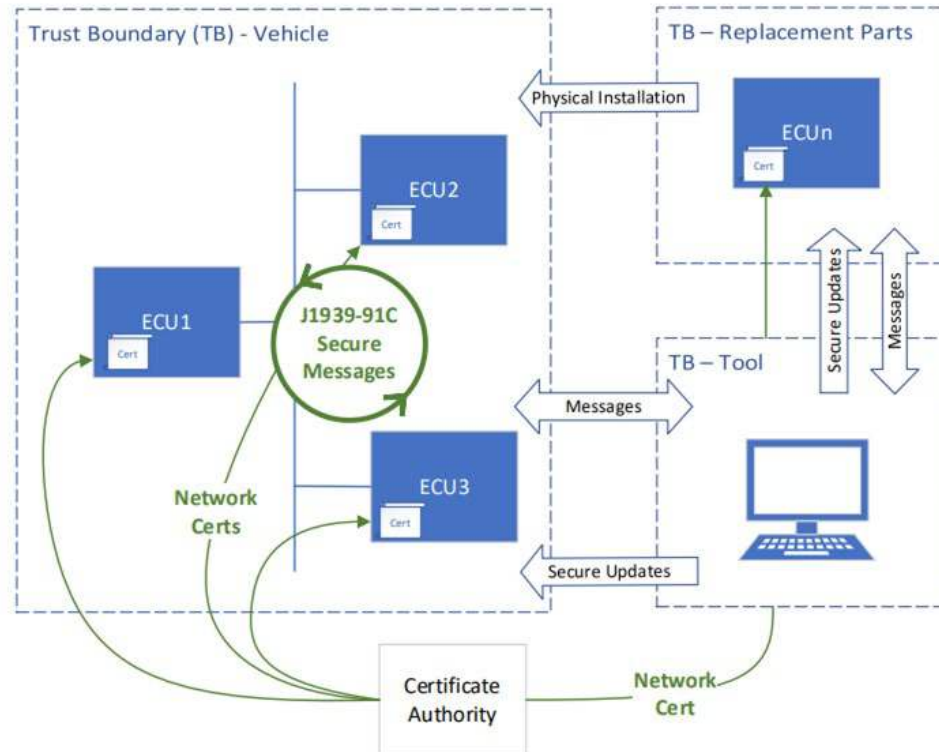


Confidential (and Authentic) Message

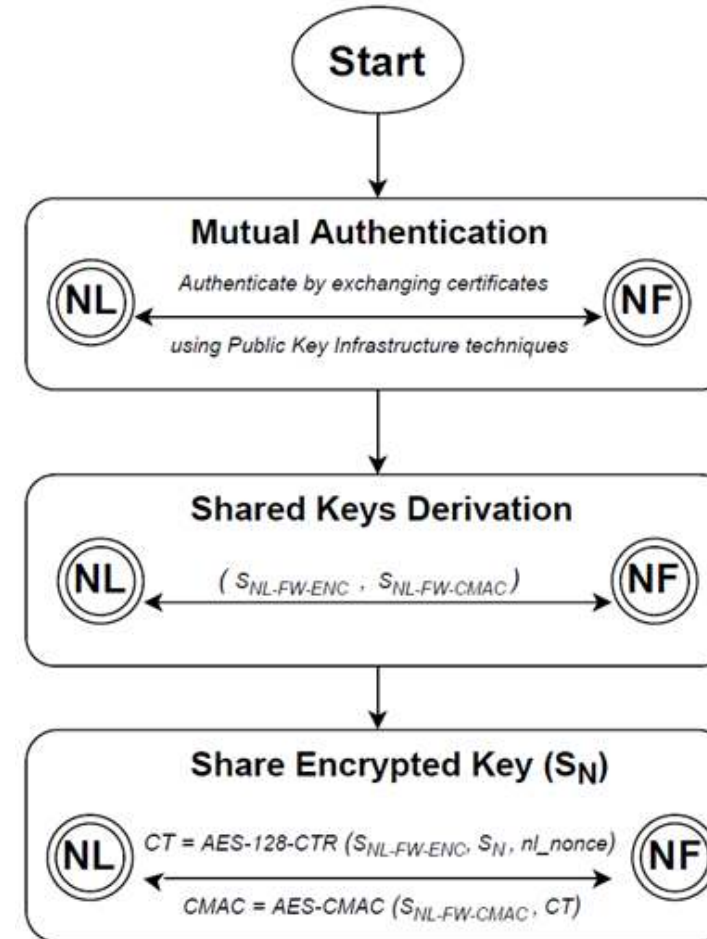
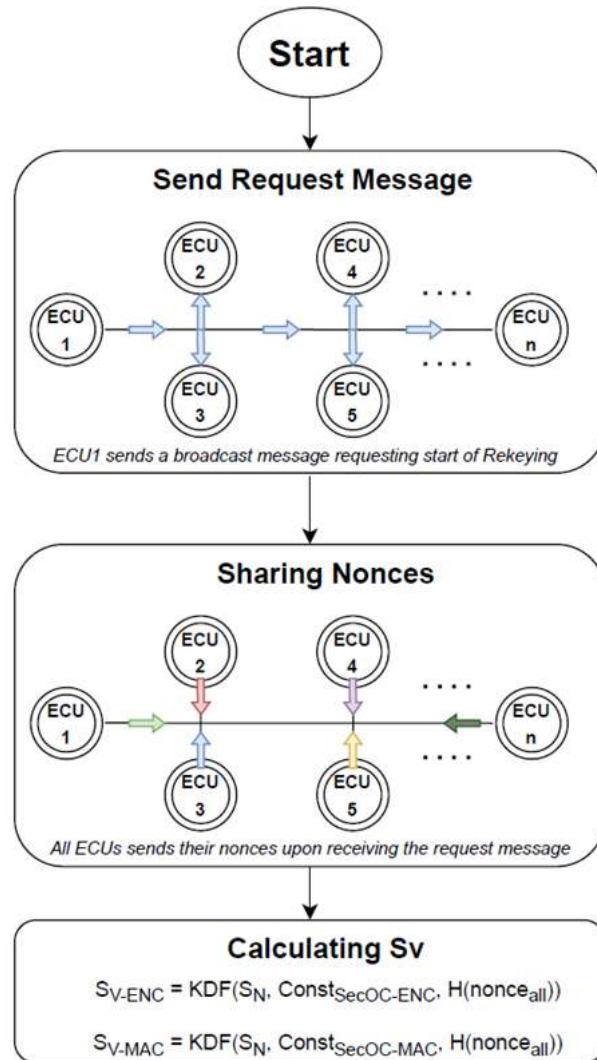


J1939-91C Operation Modes

J1939-91C Scope, State Machine



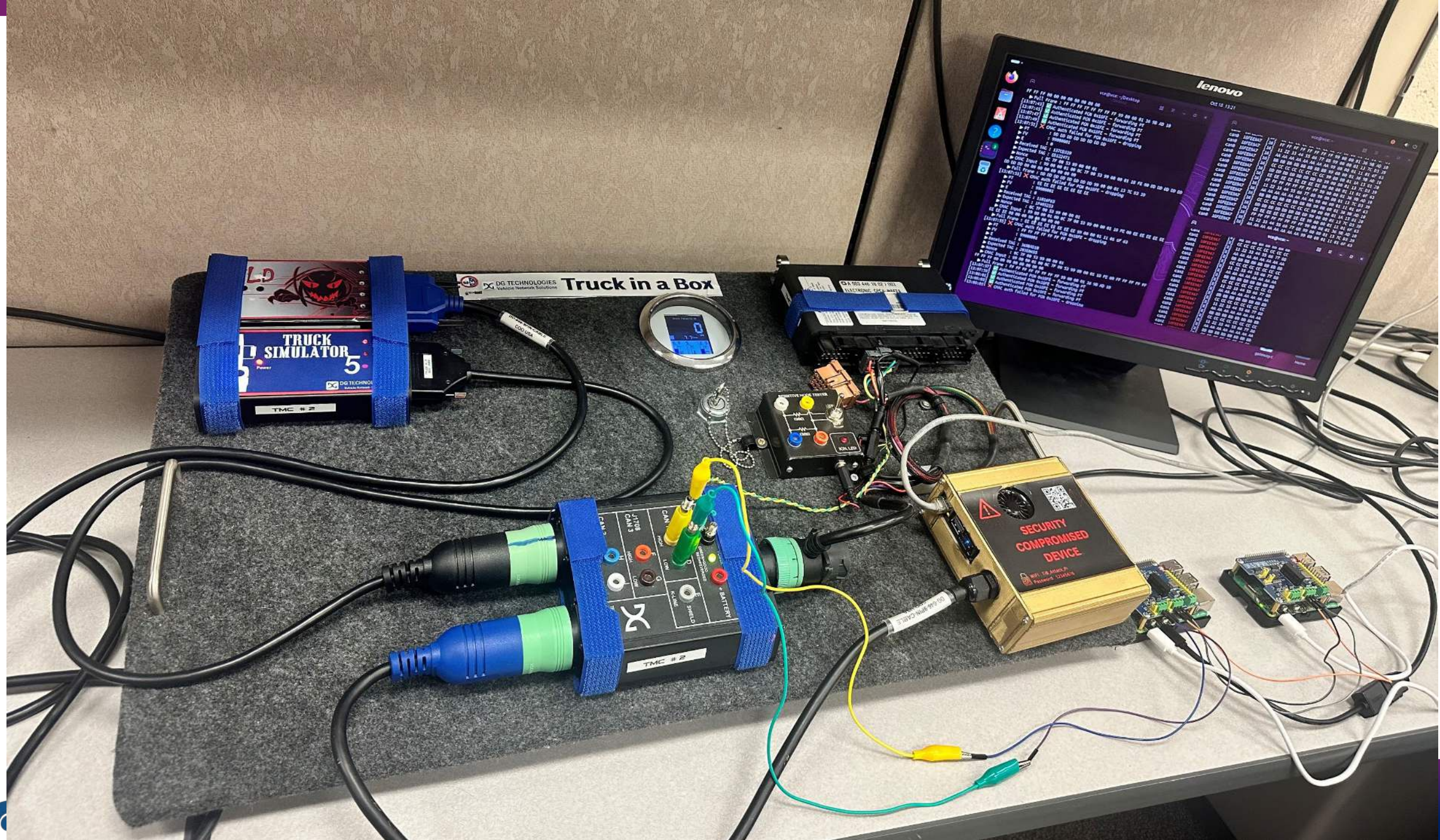
J1939-91C Network Formation



Addressing the growing need for cybersecurity engineers with real world automotive industry hardware to provide students with valuable real-world experience.

<https://eng-sci.udmercy.edu/academics/engineering/vehicle-cyber-eng>

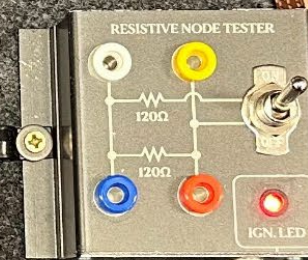
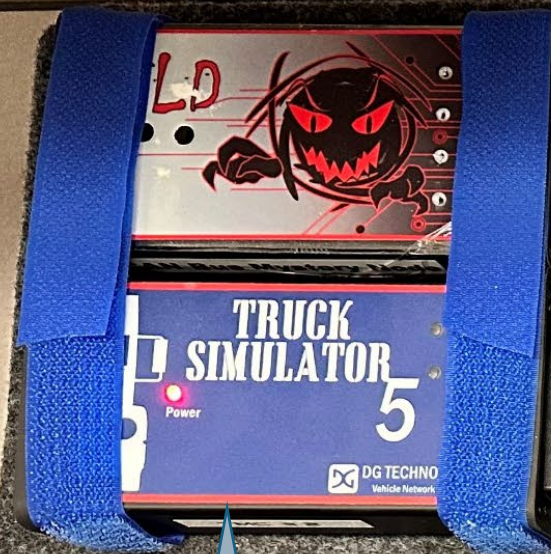






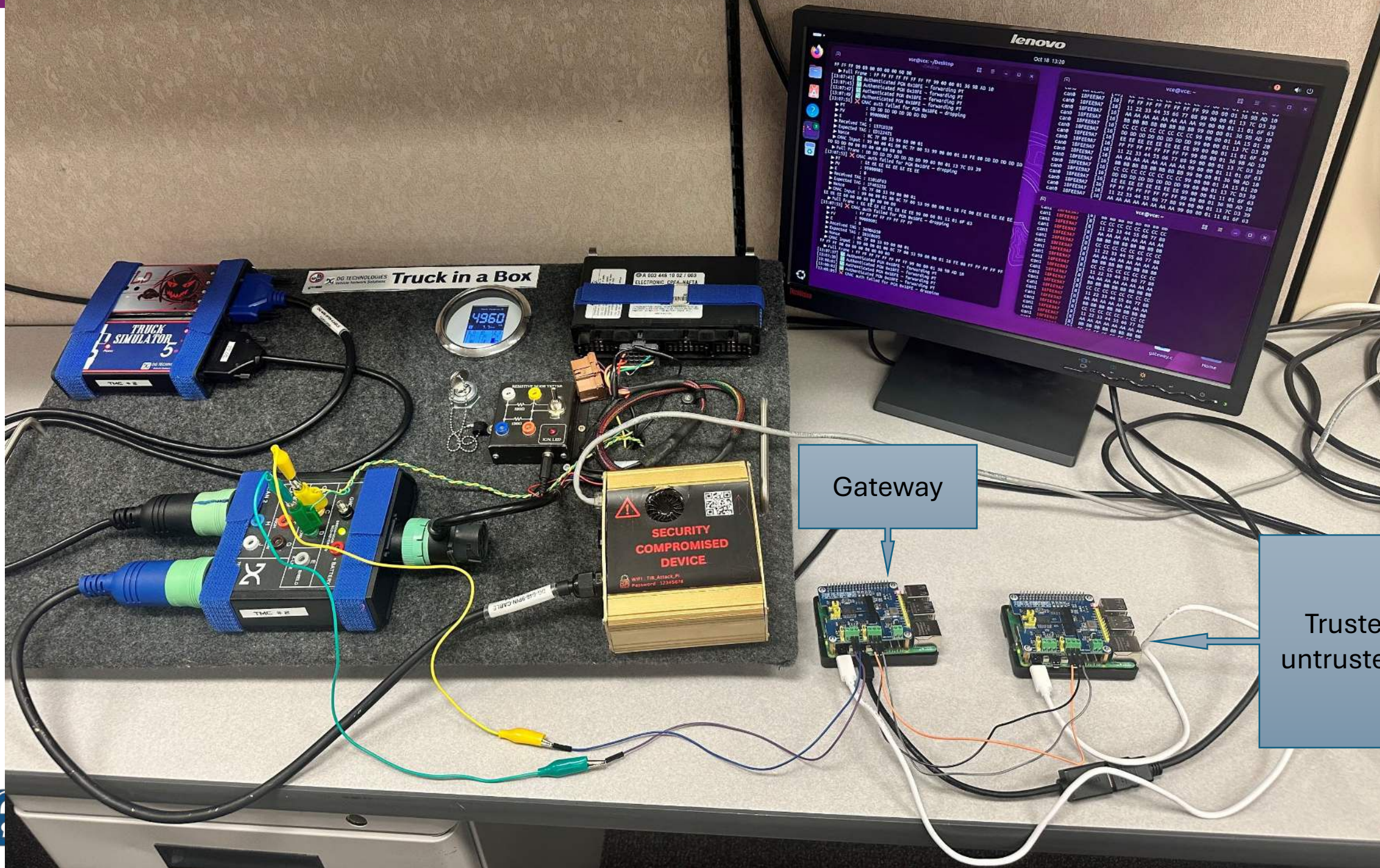
DG TECHNOLOGIES
Vehicle Network Solutions

Truck in a Box



Truck Simulator with 120 OHM resistor

ECM/PCM with 120 OHM resistor

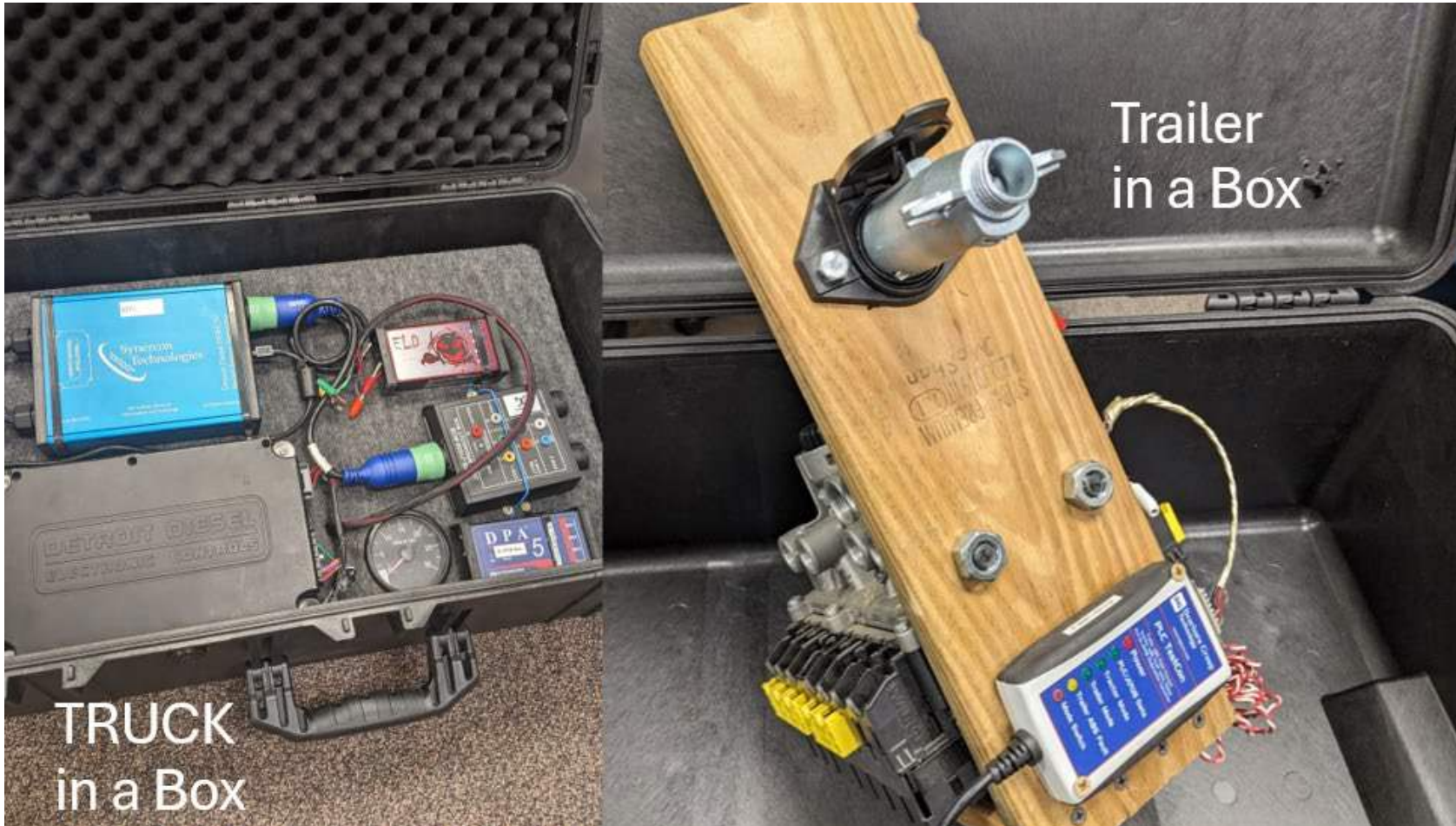


Gateway

Trusted/
untrusted Pi



Trailer in a Box Project



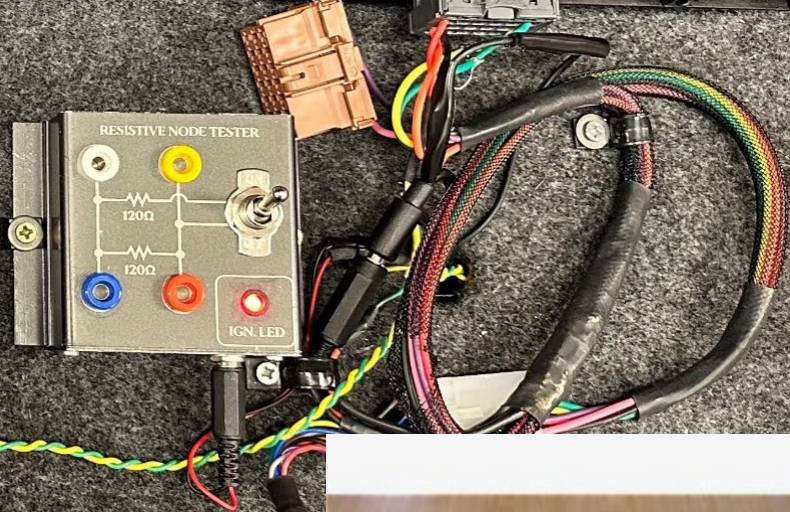
Vehicle Cyber Engineering Laboratory



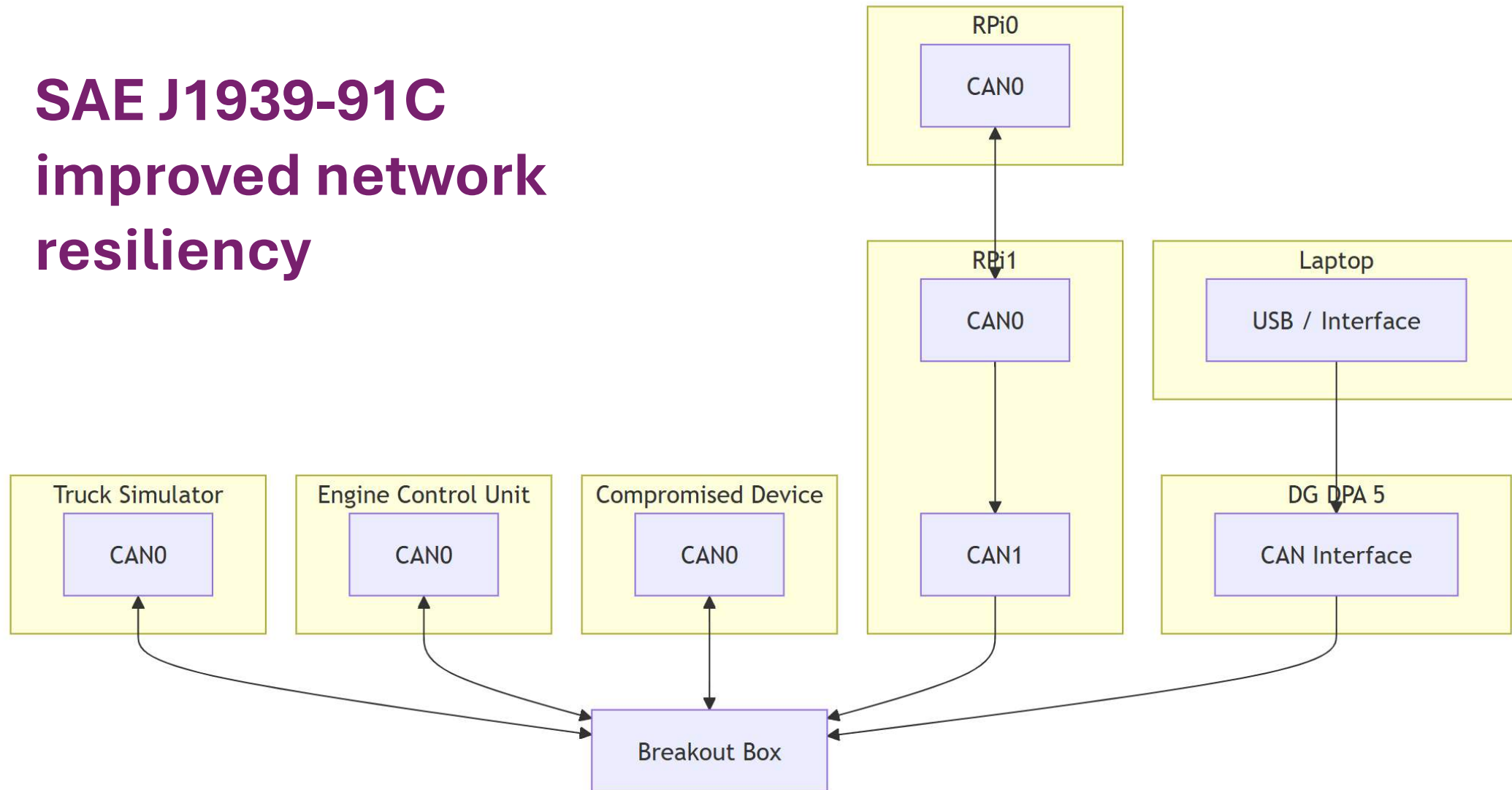


DG TECHNOLOGIES
Vehicle Network Solutions

Truck in a Box



SAE J1939-91C improved network resiliency





The Golden Tester: Implementation and evaluation of a method to defend in-vehicle networks using SAE J1939-91C to authenticate network messages between multiple ECUs

Mark Zachos DG Technologies and UD-Mercy

Krishna Teja Medam International Motors LLC

Citation: Zachos, M. and Medam, K.T., "The Golden Tester: Implementation and evaluation of a method to defend in-vehicle networks using SAE J1939-91C to authenticate network messages between multiple ECUs," SAE Technical Paper 2026-01-0002, 2026.

2026 Research Project



STRIDE Threat Model

Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege.

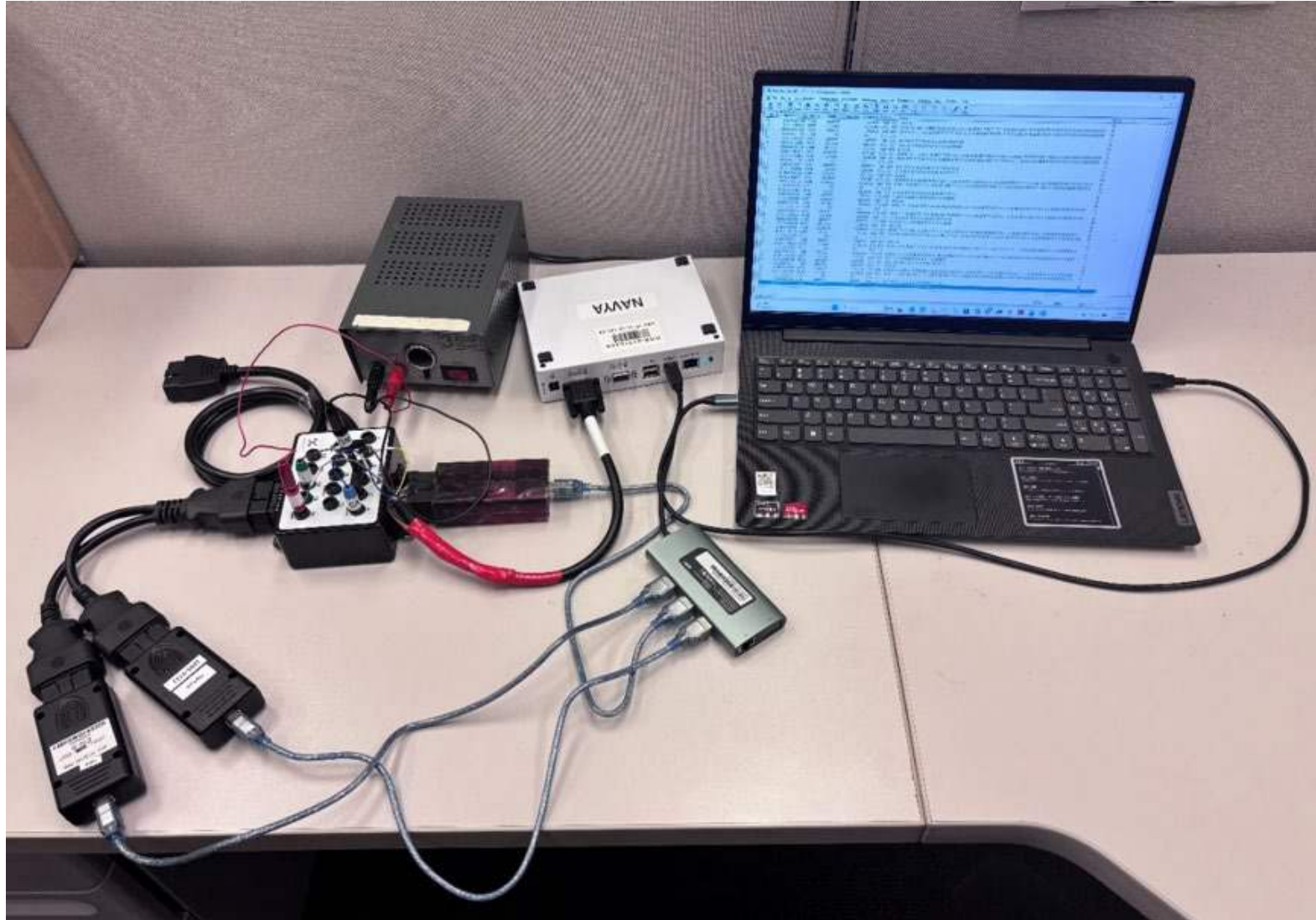
Attacker with CAN injection capability

Focused threats:

- Spoofing
- Tampering
- Replay



SAE J1939-91C Golden Tester



System Architecture

- ECU-A (Leader / Beacon / Laptop)
- ECU-B (Follower / Raspberry Pi)
- Secure link to DPA test tool
 - “Golden” Leader/Follower



Foundation of the Golden Tester

IMPLEMENTATION FOUNDATION

- Core 91C protocol
 - Operating modes
 - Network Formation (N)
 - Rekeying (R)
 - Exchange Messages (E)
 - Key edge cases
 - Established test coverage
- Network simulation
 - 3 nodes: 1 Leader, 2 Followers
 - Representative J1939 traffic
 - Test hooks in core modules
- Golden Tester framework
 - Nominal and edge-case tests
 - Cyber-resiliency tests
 - Man-in-the-middle (MITM)
 - Spoofing and replay
 - Extensible customer validation

REUSABLE TEST FOUNDATION

- System-level validation
 - 3-node Leader/Follower environment
 - Representative J1939 traffic
 - Test coverage
 - Nominal and edge cases
 - Cyber-resiliency scenarios
 - Man-in-the-middle (MITM)
 - Spoofing and replay
 - **Golden Tester**
 - Repeatable customer engagement
 - Bench-based integration
 - Tailored test setup
 - Pass/fail evidence
 - Test report and observations
 - **Customer value**
 - Validates 91C implementation
- Without a full vehicle build
- Supports development decisions

Key Findings and Gaps Identified

- Key Findings
 - J1939-91C effectively enforces:
 - Identity validation
 - Message integrity
 - Replay protection
 - Benchmark; enables reproducibility
- Gaps
 - No defined behavior after certificate failure
 - No recovery guidance
 - Operational state ambiguity

Ongoing Research and System Verification Testing

- **Tester Objectives**

- Test fidelity of customer's 91C implementation
- Suitable for both Leader and Followers
- Provides simulation environment to test and document
 - fidelity of protocol implementation
 - Cyber-resiliency

- **Test framework enables**

- Black Box Testing – external attack vectors
- White box testing – with customer collaboration

- **Suite of test applications for**

- Unit Testing
 - All protocol modes - O, R, E, N
 - Transitions between modes
- Cyber-resiliency testing
 - Man-in-the-Middle
 - Spoofing attack, Replay attack



Threat Model for a HD Vehicle – Attack Vectors

1. Attack Scenario 1: Malicious Firmware

- Infected firmware is transferred to the diagnostic PC or gateway without detection

2. Attack Scenario 2: Hijack the VDA Driver

- Attack by a shim DLL modifying the Windows DLL that interprets the diagnostic commands

3. Attack Scenario 3: Overwrite the VDA Embedded Firmware

- Rogue Embedded firmware installation by attacking the update mechanism

4. Attack Scenario 4: Man-in-the-Middle (MITM) at the Diagnostic Port

- Bypass of the authentication mechanism by a physical man-in-the-middle (MITM) device

5. Attack Scenario 5: Introducing a Rogue Node

- Rogue impersonates legitimate nodes and sends false information – e.g. network flooding

6. Attack Scenario 6: Supply chain tampering

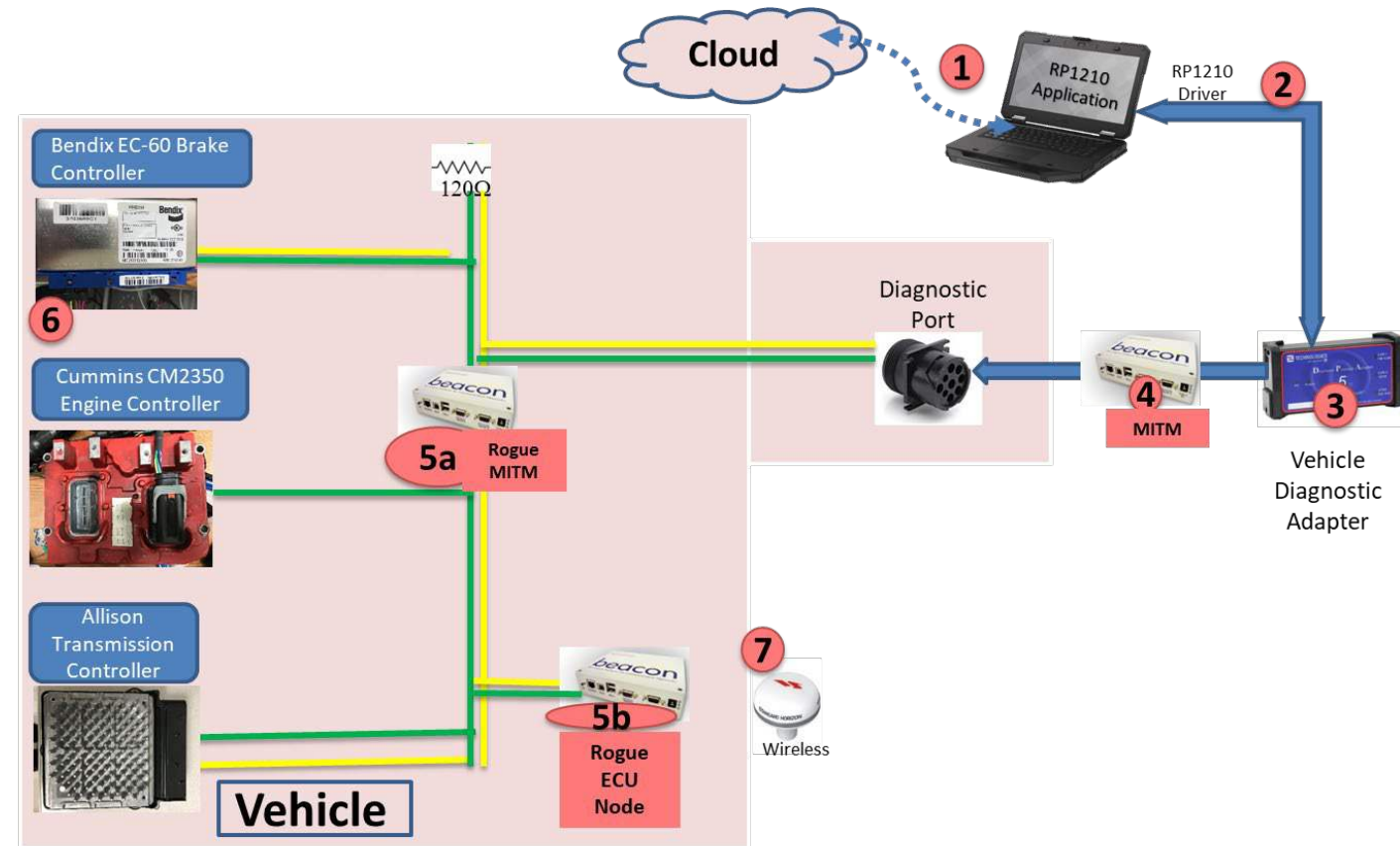
- An attacker subverts the modules somewhere in the supply chain

7. Attack Scenario 7: Wireless Attacks

- Attack on a wireless device that communicates with the device

8. Unknown Attacks

- To be identified through experience and brainstorming



Note: Attacks can occur via the Diagnostic Port

Note: This is only an example – not a complete threat model

Federal prosecutors say they have uncovered a large-scale vehicle theft operation in the Washington, D.C. region, one that allegedly relied on OBD-II tools and an export pipeline that stretched as far as Africa.

Busted International Car Theft Ring Used OBD-II Scanners From Amazon



by AutoGuide.com News Staff

Published: April 24th, 2026

f Share



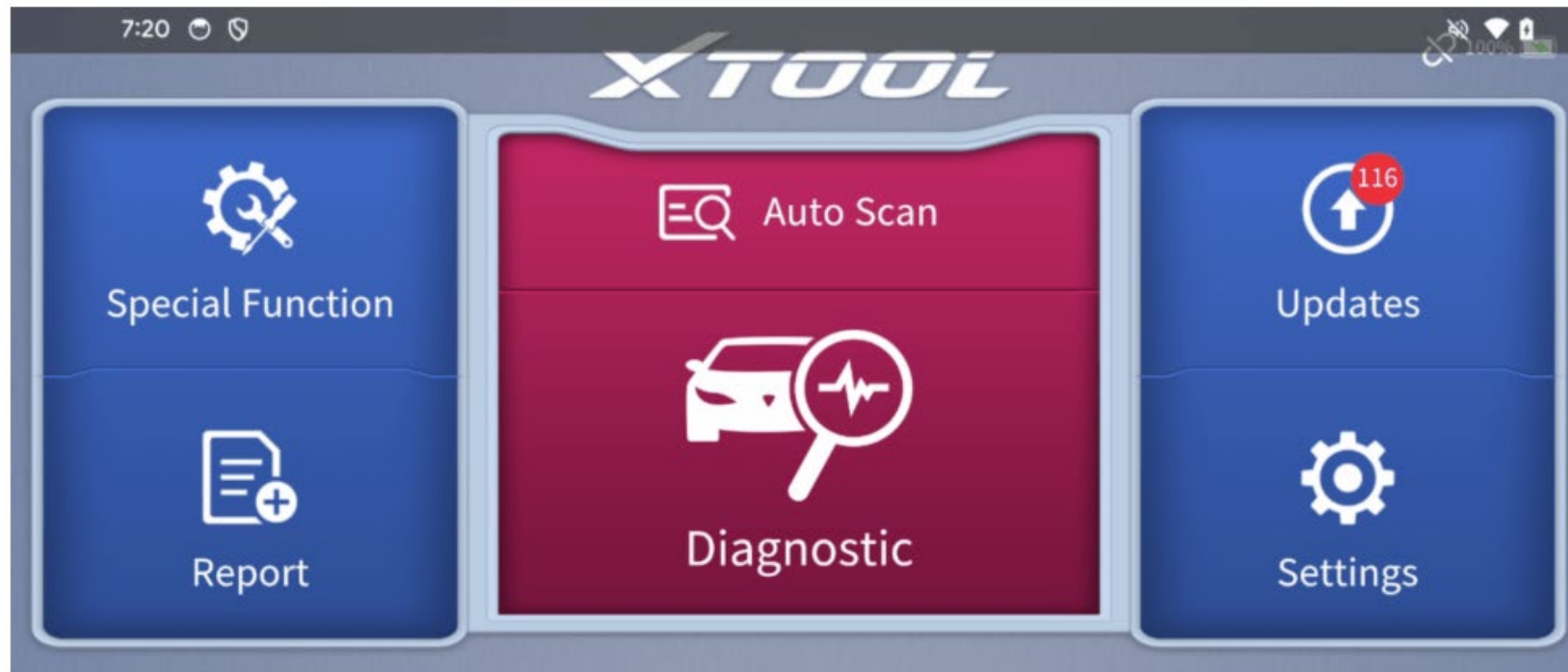
According to officials, the group used handheld OBD-II scanners—readily available online—to bypass factory security systems. These tools can reprogram a vehicle to accept a blank key fob, allowing thieves to take a car without forced entry. Authorities say the process can be completed in under a minute.

“They don't need keys and they don't need hot wiring,” Pirro said. “No smashed windows, no drama. Just a sleek electronic device called an Autel, A-U-T-E-L. And in under a minute, the car's brain is rewritten. The car is gone in 60 seconds. Welcome to the new world of car theft.”



Remote Code Execution Discovered in XTool AnyScan App: Risks to Phones and Vehicles

On a fresh install of the app, the user is prompted to install over 100 updates. If none of these updates are installed, the app will not connect to a vehicle, so the user must use the remote-download feature to achieve basic functionality.

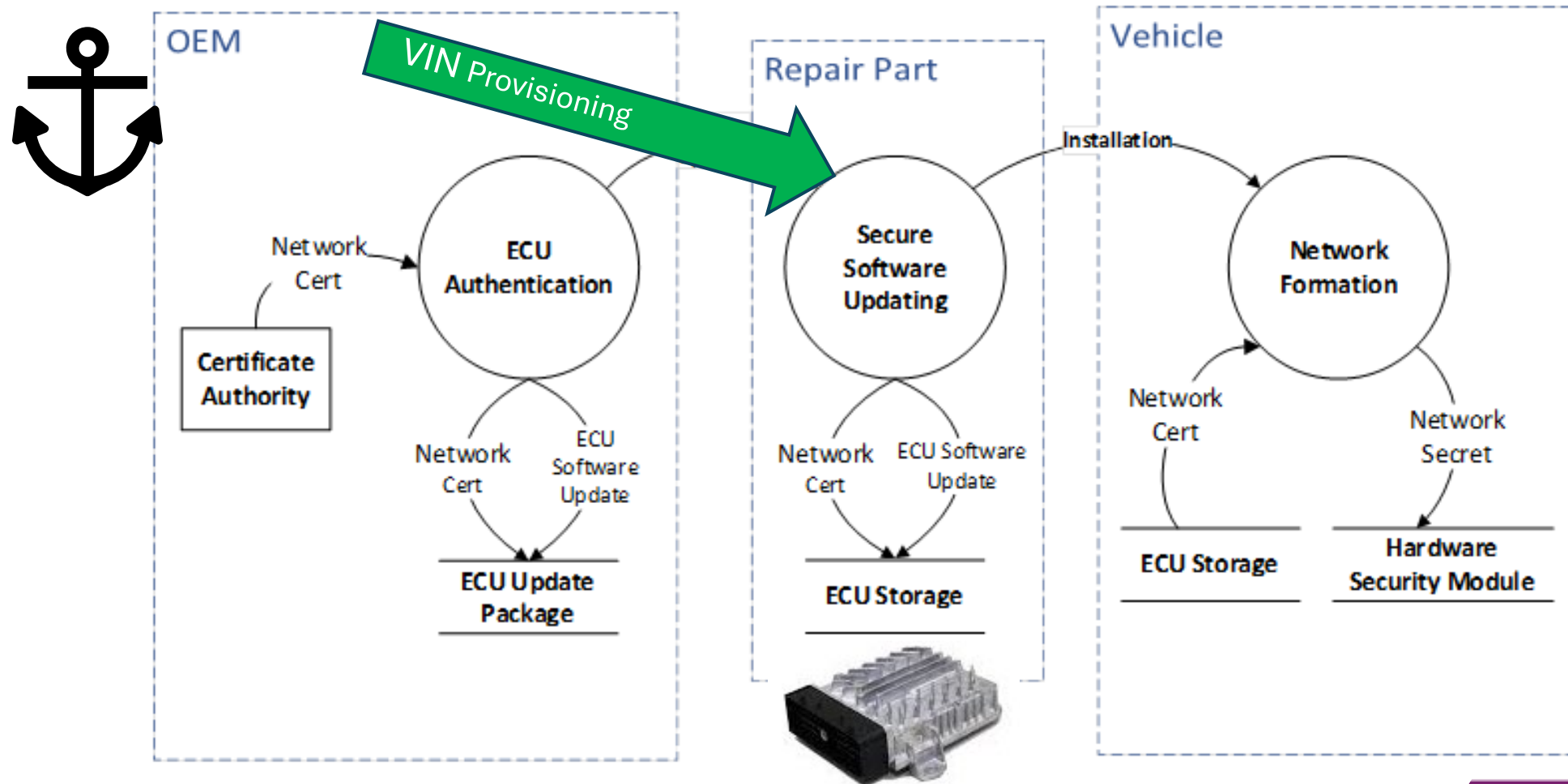


NDIA Presentation

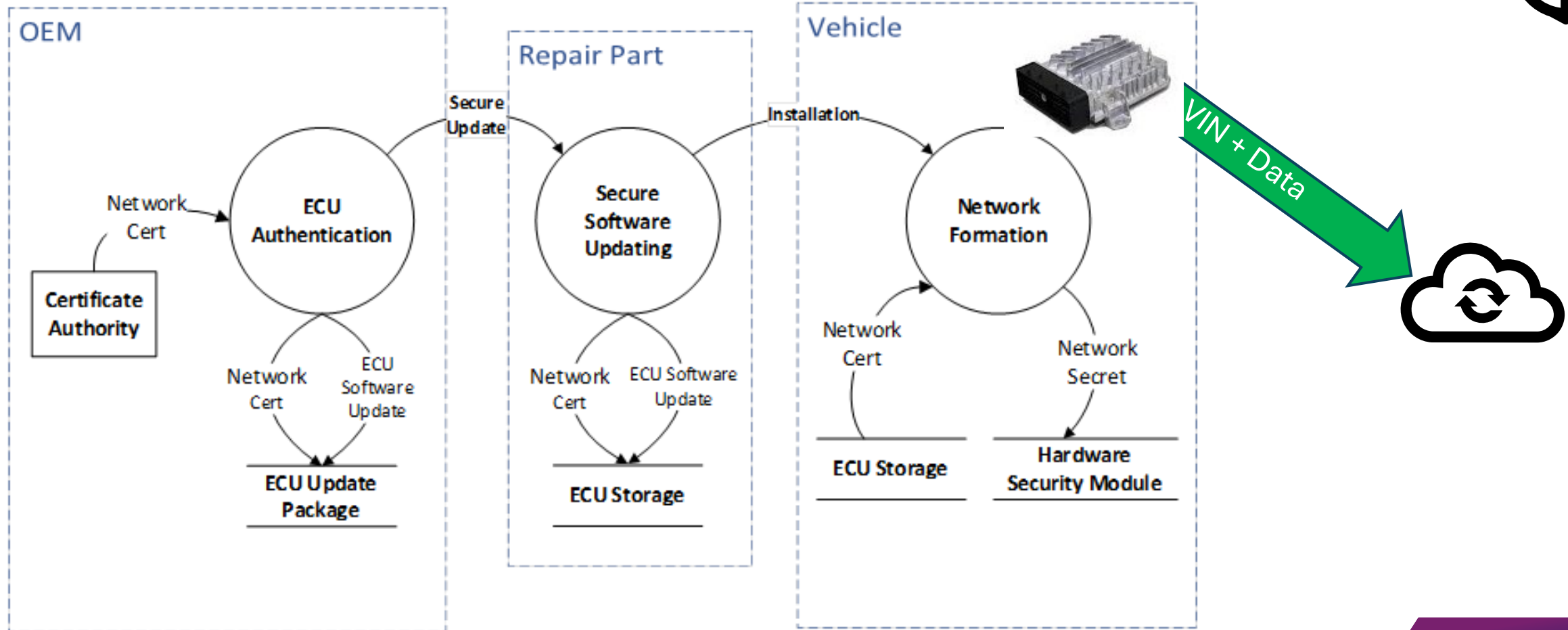


NMFTATM
National Motor Freight
Traffic Association, Inc.

SAE J1939-91C and Vehicle Repair Security



SAE J1939-91C and Secure Diagnostics Data Transfer



Power Up!



MarkZachos.net

zachosmp@UDMercy.edu

