2026 NDIA MICHIGAN CHAPTER
GROUND VEHICLE SYSTEMS ENGINEERING
AND TECHNOLOGY SYMPOSIUM
MODULAR OPEN SYSTEMS ARCHITECTURE (MOSA) TECHNICAL SESSION
AUGUST 11-13, 2026 - NOVI, MICHIGAN

GOLDEN TESTER FRAMEWORK FOR SAE J1939-91C CYBERSECURITY

Mark Zachos, Prakash Kulkarni, Ph.D.

DG Technologies Inc., Farmington Hills, MI

ABSTRACT

The impending formal adoption of SAE J1939-91C creates an urgent need for rigorous, repeatable validation methods that extend beyond functional conformance. This paper presents a structured validation and benchmarking framework, with a focus on performance characterization across dynamic vehicle configurations. Building on prior work in secure network formation, rekeying, and Golden Tester concepts, we define a minimal, transport-agnostic set of cryptographic and protocol test vectors for deterministic validation of secure message authentication, alongside simulation-based methods for evaluating network formation and rekey behavior. The framework integrates performance metrics such as secure message latency, rekey time and throughput, while also introducing cybersecurity-specific diagnostics and logging requirements for gateway module implementation. Security validation scenarios are mapped to explicit detection and response benchmarks. The resulting methodology provides OEMs, Tier-1 suppliers, and research organizations with a practical, reproducible approach to validating J1939-91C implementations, supporting both development-phase evaluation and ongoing lifecycle assurance.

Citation: M Zachos, P. Kulkarni, "Golden Tester Framework for SAE J1939-91C Cybersecurity", In Proceedings of the Ground Vehicle Systems Engineering and Technology Symposium (GVSETS), NDIA, Novi, MI, Aug. 11-13, 2026.

1. INTRODUCTION

In the SAE J1939-91C protocol, secure message exchange only occurs after identity establishment and session key negotiation are complete. This is the part of the protocol implementation where normal J1939 PGNs are transmitted with cryptographic protection enabled, and where most real time performance and security validation concerns arise.

While the SAE J1939-91C standard does not number phases this way, implementers and researchers often think of the protocol in the following four phases:

1. Provisioning / Identity Context (Preoperational)

Certificates, VIN binding, trust anchors, and long-term credentials exist but are not exchanged dynamically during operation.

2. Network Formation & Authentication

ECUs authenticate one another, validate certificates and VIN bindings, and establish trust relationships when joining a vehicle network.

3. Session Key Establishment and Rekeying

Cryptographic session keys are negotiated, refreshed, or reestablished in response to time limits, freshness value exhaustion, or topology changes.

4. Secure Application Message Exchange ("Phase 4")

Normal J1939 application PGNs are transmitted with authentication (and optionally encryption), using freshness values and AES CMAC tags. Receivers perform deterministic verification and enforce acceptance or rejection decisions in real time.

This paper's validation focus is primarily on this fourth stage, because:

- It is where latency, throughput, and bus load impacts are observable.
- It is where spoofing, replay, and tampering attacks manifest as concrete CMAC failures or freshness violations.
- It is the only stage exercised continuously during vehicle operation, making it the most critical for benchmarking and regression testing.

2. BACKGROUND

2.1 J1939 Protocol Overview

SAE J1939 prescribes a vehicle architecture that allows the ECUs associated with different component manufacturers to communicate with each other based on a plug-and-play scheme.

From a cybersecurity perspective, the SAE J1939 open network presents a large attack surface. As there is no prescription to verify authenticity or integrity of the communication through the diagnostic port, any device connected to it needs to be inherently trusted. Malicious actors can exploit this vulnerability for nefarious purposes. For example, J1939 messages can be inserted through the diagnostics port to display an incorrect vehicle speed on the instrument cluster. A more dangerous attack can be raising the engine speed while the vehicle is being driven on the road.

2.2 J1939-based Heavy Vehicle Cybersecurity Solution

Daily and Kulkarni [1] developed a cybersecurity solution, shown in Figure 1, that was designed as an after-market retrofit solution for the large fleet of commercial vehicles in service that have the SAE J1939 vehicle network with CAN2.0. A Secure Gateway Module interfaces between the vehicle and the Diagnostic adapter via communication encrypted with an ephemeral session key. This system provided secured the vehicle diagnostics and maintenance functions that are carried out through the diagnostic port. The solution includes the vehicle diagnostic adapter, device drivers and maintenance software.

Subsequently, Daily et al [2] extended the solution with CAN Conditioners to secure the internal vehicle network and the connected ECUs. A custom, non-standard communication protocol was developed to implement the network security on a J1939 network with standard CAN (2.0).

This solution was implemented by DG Technologies on a Class 6 truck and demonstrated to the US Army Ground Vehicle Systems Center.

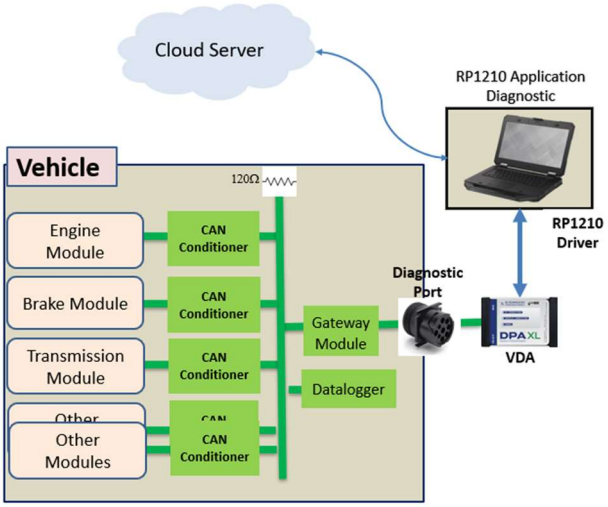

Figure 1: Cybersecurity solution for a J1939 network

2.3 The SAE J1939-91C Standard

The Society of Automotive Engineers (SAE) and other standard-making bodies are developing standards that address the diverse cybersecurity needs of industry.

The SAE J1939-91C – CAN-FD Network Security standard describes Secure On-board Communications with optional Encryption (SecOC/E) for an internal CAN FD network and the processes and infrastructure required to make it a secure J1939 network.

The objective of SAE J1939-91C is to secure all CAN messages exchanged between ECUs on a heavy-duty vehicle and establish trust between all network entities joining the intra-vehicle network. Zachos et al [3] provide an overview of -91C along with a simulation implementation that would be valuable for testing purposes.

The primary means by which J1939-91C enhances vehicle cybersecurity are:

2.3.1 Node Authentication

All nodes/ECUs communicating on the network should be authorized by a trusted third-party to prevent unknown ECUs from injecting malicious messages into the network. Authentication is handled during the network formation phase with each network member sharing a valid certificate before joining the secure network.

2.3.2 Data Integrity

Ensure that the received data has not been tampered with after being transmitted from the original source. This is achieved by the addition of a block cipher-based message authentication code (CMAC) to the security overhead.

2.3.3 Message Confidentiality

In addition to the regular “Unsecured” plaintext messages, J1939-91C supports two other types of messages. “Authentic messages” add a security overhead to the end of the plaintext message. The overhead is computed by CMAC AES-128 encryption with a locally generated symmetric key that is applied on the plaintext message. Additional security is provided for the most critical “Confidential” messages by encryption of the data payload.

2.3.4 Secure Key Generation

In J1939-91C, all ECUs on the network cooperatively establish ephemeral cryptographic keys for communication for each session. Typically, every power cycle is a new session. The session keys are essential for encoding (by sender) and decoding (by receiver) the messages on the network.

2.3.5 Data Freshness

Each member on the network maintains a ‘Freshness Value' (FV) for each message that it transmits. Each receiver of messages tracks the FV for every ECU sharing the network. The

Freshness Value is an enabler to prevent replay attacks in the network.

2.3.6 Rekeying

A rekeying process dictates the generation of session keys. In certain instances, the session key may need to be changed during a given power cycle. One such instance is if a new device, such as a Diagnostic Adapter, is added to the network. Another example is the overflow of the Freshness Value counter.

A vehicle network designed to conform to SAE J1939-91C ensures the following security characteristics:

- freshness – replays and stale messages are rejected,
- integrity – evidence to believe the message has been created by a member of the secure network and has not been tampered with,
- confidentiality – the data portion of none, some or all the vehicle messages can be kept private to only members of the network,
- authenticity – only authentic ECUs participate in the secure network, and
- authorized – only specific ECUs, as identified by the organization creating the secure system (typically an OEM), are allowed into the network of a specific vehicle

3. CYBERUP OVERVIEW

Zachos and Kulkarni [4] presented a comprehensive security solution for heavy-duty vehicles, CyberUP, to enhance the cyber-resilience of vehicles based on the J1939 protocol.

This solution secures the network communication in-vehicle and through the diagnostics port, per SAE J1939-91C protocol. In addition, the system provides many advanced functions by utilizing the computational capability of the Gateway Module.

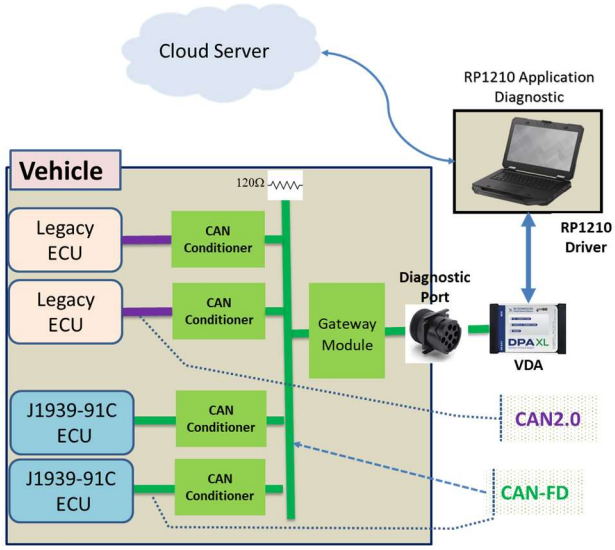

Figure 2: CyberUP - Mixed Vehicle Network Topology

CyberUP is shown schematically in Figure 2. This design is flexible to support both legacy ECUs (with CAN2.0) and those designed for a J1939-91C (with CAN-FD) vehicle network. With the introduction of the Secure Gateway Module and CAN Conditioners, the vehicle network now conforms to J1939-91C.

3.1 Secure Gateway Module

The GWM, which is located at the Diagnostic port, functions as an enhanced Firewall. In addition to facilitating the communication through the diagnostic port, it performs other "UP" functions towards increasing the up-time of the vehicle. The module includes GPS and Accelerometer sensors that support watchdog functions of CyberUP.

3.2 CAN Conditioner

The CAN Conditioner is an ECU gateway between the J1939-91C network and the ECU. The connection is through a short point-to-

point network with a terminating resistor built into the CC. With a legacy J1939/CAN2.0 ECU, the CC also functions as a translator to the J1939-91C/CAN-FD vehicle network. This includes implementation of 91C-specific requirements such as network formation, rekeying and secure message exchanges.

3.3 Back-end Applications

Additional functionality is provided by support utility applications that run off-line on the diagnostic computer and/or back-end server.

The various CyberUP functions together provide additional layers of security to enhance cyber-resiliency. Real-time detection and reporting of intrusions allows immediate implementation of mitigation actions, such as 'limp home' or 'safe' mode of operation. It must be noted that the 91C protocol does not prescribe any remedial actions. These are left to the vehicle designers.

3.4 CyberUP Core Functions

For the rest of this paper, we assume that all the devices on the vehicle network are compliant to the J1939-91C standard. CyberUP is a comprehensive system whose key features are:

"Impostor Parameter Group" Alert Generation

The GWM and the CAN Conditioner devices are designed to send an Impostor PG alert message when an attack is detected. The Impostor PG Alert parameter group in J1939 is used for this purpose.

It will be advantageous to assign unique SPN numbers to the different conditions leading to the alert. These include CMAC mismatch, Filter violations in the GWM/CC, Multiple address claims and CAN frame errors. Additional SPN numbers will need to be assigned as newer algorithms, such as alerts based on the vehicle context, are implemented.

Access Control Filters

Allow (Whitelist) and Block (Blacklist) filters are implemented in the GWM and CC to block messages from potential malicious sources and ensure only legitimate messages pass to the vehicle network. Any access violation will generate a J1939 IPG Alert diagnostic message. The filters will typically be based on J1939 Source Address (SA), J1939 Destination Address (DA) and J1939 PGNs. The filters can also be based on parameter value, for example, vehicle speed.

Back-end Utility Applications

The Diagnostic system includes applications running on the PC and/or a cloud server for

- Diagnostic services
- Key management on the server
- Device provisioning
- Log data viewing, including data decoding, display and analysis
- Secure Access Control Filter Module updates
- Module(s) configuration, reprogramming and update

A mechanism to securely update the filter parameters in the field is essential. Integrity, Authenticity and Confidentiality of the update parameters should be ensured.

Context Aware Algorithms

Vehicle systems engineers can utilize the computational power in the Gateway Module to detect and alert any vehicle intrusion attempts by correlating the vehicle context with the network messages. For example, an alert can be generated if Request for Diagnostic session is received when the vehicle is running.

Watchdog Functions

The Gateway module is a sentry device that inspects and logs all diagnostic communications on one side. On the other side, the device

monitors the vehicle network and looks for anomalies that may indicate an intrusion.

The Gateway Module generates an Impostor Parameter Group (IPG) alert message when anomalies, which may be hardware or firmware related, are detected in the vehicle network. Some examples are multiple address claims, CAN bus errors (CANBus events, bus off, bus warning, frame errors, etc.), timing reasonableness checks etc.

Data Recording (Datalogger)

The datalogger is designed to collect all vehicle network traffic for post processing, providing valuable data to further advance Cybersecurity defensive actions.

Electrical System Health Monitor

Generating alerts based on the state of health of vehicle components and systems is a significant value-addition to increasing vehicle up-time. One such application is DPA Health, developed by DG Technologies. The application monitors electrical system components – battery, charging system, alternator, ignition system – and alerts for any anomalies. A timely alert can lead to proactive maintenance actions and help to avoid a potential walk-home situation.

Platform for Advanced Algorithms

Many Cybersecurity research groups, both in the Government and Commercial arena, are very active in exploring new technologies and developing new algorithms. An example is the Active Defense Framework (ADF) activity, which has resulted in algorithms based on Artificial Intelligence and Machine Learning.

The Gateway Module in CyberUP provides a convenient platform to implement and test these prototype algorithms in the real world and help advance cybersecurity research. The specific detection and mitigation actions to exploit the capability of CyberUP are beyond the scope of this paper.

4. GOLDEN TESTER

Implementation of SAE J1939-91C for the vehicle network requires a large amount of effort to transition all ECUs on the vehicle network to follow the 91C protocol. This requires vehicle manufacturers and suppliers to carry out the entire development cycle, from design to validation. Surely, a formal methodology is needed to evaluate all components and ensure seamless integration on a vehicle.

Mark Zachos et al [5] developed a systematic method to evaluate the SAE J1939-91C network security operating over a CAN-FD network. Test vectors were created to validate key generations and cryptographic operations on simulated ECU in-vehicle network system hardware. The authors introduced a lightweight, transport-agnostic benchmark comprising deterministic AES-CMAC test vectors and a simple verification utility, requiring no specialized hardware or build system. This minimal artifact set enables reproducible and machine parsable validation of SAE J1939-91C security across diverse lab environments.

A 91C network simulation can be developed using commercial devices such as DG Beacon, STAR Flex or Raspberry PI to emulate the ECUs. The evaluation methodology for this simulation specifically focused on security validation, testing the robustness of the SAE J1939-91C implementation against spoofing, replay, and identity tampering attacks. Simulated threats included the injection of falsified Brake messages with incorrect CMAC tags, designed to mimic unauthorized control commands. These messages were shown to be consistently rejected by the receiving ECU due to CMAC verification failures.

A key element in this validation is the use of VIN binding within the X.509 certificate, which is implemented as a custom extension using OID 1.0.20828.3, in accordance with SAE J1939-91C.

Benchmarking provides a consistent basis for comparing the current implementation with alternatives architectures, cryptographic methods or hardware problems. Well-defined benchmarking criteria are required to evaluate the simulation framework to assess system performance, security robustness and system scalability.

Performance metrics include the

- latency of secure message transmission,
- the time required for session key negotiation (Phase 2), and
- the throughput of CMAC-authenticated messages under varying bus loads.

Profiling tools can measure CPU usage and memory footprint on embedded ECUs, such as the Raspberry Pi, to determine the efficiency of cryptographic operations. Additionally, the system's ability to sustain real-time constraints under high message frequency or bus congestion can be stress-tested using CAN utilities like candump and canplayer.

Security validation benchmarks involve injecting replayed messages, tampered certificates, or mismatched VINs to assess detection accuracy and response timing.

4.1 Adversary Model and Assumptions

The assumed adversary in this evaluation is

- capable of injecting arbitrary CAN-FD frames onto the vehicle network, either through a compromised ECU or a rogue node with bus access
- The attacker may modify or replay authenticated messages
- attempt to join the secure network using altered certificates or incorrect VIN bindings, or cross tool boundaries by abusing diagnostic or tester interfaces that legitimately allow message injection, ECU resets, or diagnostic service access, but are not intended to authorize participation in secure application-level message exchange.

4.2 Spoofing and Tampering Scenarios

Spoofing attack resistance was evaluated offline using crafted secure message frames derived from benchmark vectors. These frames include both valid authentication tags and systematically invalid variants generated through source address manipulation, freshness-value replay, and encoding errors.

A certificate-tampering scenario was created by intentionally modifying the VIN embedded in the ECU's X.509 certificate before initiating the Join Network request. The leader ECU successfully immediately identified a mismatch between the presented certificate's VIN and the actual VIN and triggered an explicit "certificate hash mismatch" error, leading to termination of session-key negotiation.

4.3 Cryptographic Test Vectors

The authors define a minimal, transport-agnostic set of cryptographic test vectors that focus exclusively on the deterministic components of SAE J1939-91C secure message exchange with encryption disabled (E = 0). Each vector specifies a canonical set of inputs - including a 24-bit Parameter Group Number (PGN), Source Address (SA), 32-bit Freshness Value (FV), and application payload - from which the authentication nonce and AESCMAC tag are derived.

The benchmark comprises

- one positive “golden-path” vector and
- three negative vectors that intentionally violate normative assumptions:
    - an incorrect source address
    - a stale or replayed freshness value
    - an endianness error in freshness-value encoding.

Together, these vectors enable byte-accurate and reproducible validation of both CMAC computation and receiver decision logic, while remaining independent of certificates, key-exchange state, or physical CAN-FD hardware.

Reproducibility concerns are addressed via a defined and structured logging model. A structured log format captures certificate validation status, authentication outcomes, and lifecycle state transitions. A reference log structure for secure message evaluation includes: (i) message receipt timestamp, (ii) PGN and source address, (iii) CMAC verification result, (iv) freshness evaluation result, and (v) resulting protocol state transition.

This evaluation focuses on functional correctness rather than timing performance. Offline verification using crafted secure message frames establishes protocol-level detection behavior independent of platform-specific performance characteristics which vary across implementations.

4.4 Benchmark Artifacts for Reproducibility

- Rationale for a Minimal Benchmark

The authors provide lightweight, transport-agnostic artifact sets that any laboratory can run on a laptop or mixed-CAN setup. This approach ensures deterministic validation of AES-CMAC logic without dependence on build tools, repositories, or FD transmit capability.

- Deterministic Crypto & Protocol Vectors

A set of JSON test vectors (/vectors/crypto/) containing PGN, SA, payload, freshness value (FV), AES-Key, and expected AES-CMAC are created. A Python utility recomputes and verifies each vector against the provided "expected_cmac_hex". Negative vectors (e.g. wrong SA, replay FV, fv_endianness) demonstrate correct rejection paths.

- Example Vector for AES-CMAC Verification

Four canonical test vectors are defined in JSON. Each vector includes a descriptive name, the PGN in hexadecimal, the source address SA, the message payload_hex, the 32-bit freshness value FV, encryption bit (E) and the computed expected_cmac_hex.

- Extensions to this benchmark

Freshness-value rollover and sliding-window acceptance behavior are identified as important extensions for future work. By including these scenarios as part of a testing framework, developers will be enabled to rapidly prototype, extend, and validate secure message handling behavior within embedded and simulated ECU environments

4.5 Gaps in existing SAE J1939-91C Standard

The authors point out the lack of guidance on handling failures as the most significant gap in the existing standards.

For example, while the standard explicitly mandates certificate VIN-binding verification, it does not currently specify recommended actions or recovery procedures following a VIN or certificate validation failure during ECU authentication, secure software updating, or network formation stages.

4.6 Proposed Enhancements to SAE J1939-91C

The authors proposed practical recommendations to address these shortcomings, The following is a summary of the recommendations:

- Diagnostic Reporting:

Emit a standardized diagnostic message clearly indicating a VIN binding or certificate verification failure, enabling external diagnostic tools or gateway/head ECUs to record the event explicitly and trace it back to the "ECU Authentication" or "Secure Software Updating" stage.

- Immediate Session Reset:

Automatically return the affected ECU(s) to a controlled state, such as "Network Formation," as indicated in the J1939- 91C vehicle maintenance trust diagram.

- Detailed Audit Logging:

Capture and store detailed information on certificate mismatches or validation failures, including the incorrect VIN, certificate serial number, involved ECU ID, verification stage, and timestamp for forensic analysis.

- Secure Certificate Re-provisioning:

Implement a secure and structured mechanism, involving the OEM's Certificate Authority, to retrieve and reinstall fresh, verified certificates. This process aligns with the “ECU Authentication” phase to promptly restore secure and authenticated communication.

The authors conclude that the current version of J1939-91C needs additional refinement. Specifically, it needs to incorporate the recommended recovery procedures and address limitations identified to offer comprehensive and practical protection suitable for deployment in modern vehicle cybersecurity architectures.

5. DEVELOPMENT CHALLENGES TO EMPLOY SAEJ1939-91C:

5.1 Overview

A heavy-duty vehicle network incorporates ECUs and other devices from different suppliers. Conformance of each device to the J1939 protocol is essential for vehicle integration – this interoperability is confirmed at vehicle build. The cybersecurity requirements of J1939-91C present additional development challenges for vehicle integration. A few critical issues are noted below.

5.2 Dynamic Vehicle Formation

All ECUs in the vehicle network participate in network formation at the beginning of every power cycle. ECUs (devices) on the vehicle network may be introduced or removed from a vehicle for maintenance or upgrade purposes. Also, ECU development teams may introduce new features periodically. Conformance to the 91C protocol for all vehicle configurations is essential. The vehicle integration process must address vehicle configuration changes that may occur during the life of the vehicle. Clearly, it is not sufficient to perform integration testing solely at initial vehicle build. The development process must provide a proactive approach to ensure smooth vehicle integration.

5.3 Standard Process and Tools

The vehicle development activity is distributed over development teams in different organizations. In addition to the comprehensive standard, the development processes and tools need to be standardized to the extent possible.

5.4 Performance Standards

The performance metrics noted earlier, such as latency of secure message transmission and the time required for session key negotiation can negatively affect system performance. For example, an ECU that responds significantly

slower than the other ECUs on the network may cause too many rekey attempts. The 91C standard should establish an acceptable minimum and maximum time periods for this response. Similarly, other critical performance metrics should be identified, and suitable performance standards should be specified.

5.5 Performance Testing Method

Many performance metrics can be affected by vehicle and hardware variations and vehicle operating conditions. Hence, it is not sufficient to determine the metrics solely in a development environment or in a single vehicle configuration. A well-defined methodology to perform the measurements on-demand and on-the-vehicle would be very valuable. An SAE Recommended Practice can help uniform adoption in the field.

We summarize that there is a need for

- performance benchmarks
- ability to test against the benchmarks on an ongoing basis
- record the performance
- well defined development environment
- performance benchmarking tool, such as a simulator

6. PROPOSED GOLDEN TESTER FRAMEWORK

The preceding discussion has identified several areas for improvements of the 91C specification, the Golden Tester and the development tools. The following is a preliminary list prepared by consolidating these ideas.

6.1 Proposed J1939-91C Protocol enhancements

Cybersecurity Diagnostic Trouble codes
Assign SPNs for specific IPG alerts, including

- CMAC mismatch
- Filter violations in the GWM/CC
- Multiple address claims
- CAN frame errors.

Establish Cybersecurity related Performance Measures
It will be valuable to monitor a 91C vehicle network via critical performance parameters for each ECU on the network. This can help pin down any performance bottlenecks and improve cyber-resilience. Some important parameters are

- Number of instances of compromised credentials
- Rekey time
- Number of rekey requests initiated
- Reasons for rekey requests, such as FV overrun or new module.
- Number of tag errors in the last few, say 5, power cycles
- Vehicle Network configuration - Modules present in the vehicle network

Diagnostic Request messages
As discussed earlier, it is important to be able to determine the performance measures in a vehicle set up. This is best achieved by interrogating the vehicle network via the Diagnostic port. Request messages should be designed for specific actions, including

- Request Cybersecurity Diagnostic trouble codes
- Request all recorded Performance measures (noted above)
- Conduct a self-test with static test vectors
- Conduct a self-test to determine the response to edge cases such as FV overflow

Diagnostic Reporting
The J1939 91C specification should standardize reports for benchmarking the cybersecurity

performance of vehicles. Towards this end, the standard should

- Define a structured log format for each request
- Develop a standard cybersecurity performance report

6.2 Gateway Module Functions

The diagnostic port interface is typically used for diagnostic and reprogramming purposes. In a 91C-equipped vehicle, the Gateway Module isolates external devices from participating in the vehicle network. In the present definition, diagnostic port communication with the diagnostic adapter is retained with J1939 over CAN 2.0. The GWM, being a part of the vehicle network, is a suitable platform for

- many of the CyberUP functions described earlier, including Electrical System Health Monitor, context aware algorithms and other advanced algorithms
- datalogger to record all network traffic, the performance measures
- execute the proposed self-tests

These functions are largely independent of the modules on the vehicle network.

6.3 Simulator Requirements

A simulator is a valuable development tool to provide repeatable performance in a controlled environment. Simulations can be used for development and testing for the detailed requirements, representing both nominal and edge conditions that can be expected in the field.

In practice, depending on the particular use, a simulation system may consist of a number of different platforms, both hardware, software and mixed hardware-in-the-loop simulations.

The primary requirements for the simulation system are outlined below:

Enable Protocol testing

- Nominal operation per J1939-91C
  - Secure Message exchange, message validation
  - Rekeying, with Leader/Follower
  - Network formation
- Extensions
  - Multi-ECU environment - rekeying
  - Introduction of new ECU/device in network

Enable Stress testing

- Time limit driven rekeying
- Quick changes in network configuration

Generate Attacks

- Spoofing
- Replay attack
- MITM
- Identity tampering
- Repository of attacks

6.4 Implementation of the Golden Tester Framework

A comprehensive Golden Tester is being developed in stages by DG Technologies.

Initial development of the tractor-trailer simulation employing SAE J1939-91C and the Golden Tester were done on a commercial Raspberry-PI platform. While this hardware and the associated tools are suitable for early development, the hardware is not suitable for the comprehensive functionality envisaged in the Golden Tester Framework.

The Beacon and LENS platforms [6], developed by DG Technologies, provide a rugged and proven development environment that is suitable to integrate all the functionalities of the Golden Tester Platform. The Beacon has form factor that is suitable for a desktop tester and provides many support applications that enable quick prototyping. The LENS is a

compact device that is suitable for in-vehicle implementation. Another platform under consideration is the Flex [7] device, a product of STAR Cooperation.

7. CONCLUSIONS

This paper presented a practical validation and benchmarking methodology for secure on vehicle communications based on SAE J1939-91C, addressing the need for repeatable implementation independent verification as the standard moves toward formal adoption. Using the protocol implementation shown in Figure 3, SAE J1939-91C operation can be decomposed into provisioning and identity context, network formation and authentication, session key establishment and rekeying, and steady state secure message exchange. This decomposition enables clear separation of control plane and data plane behaviors and provides a structured basis for aligning validation objectives, threat scenarios, and performance metrics.

A key contribution is the definition of a minimal, transport agnostic set of cryptographic test vectors focused on authenticated application layer messaging. By isolating deterministic AES CMAC computation and receiver decision logic from certificate handling, key exchange state, and CAN FD hardware dependencies, these vectors support reproducible validation, regression testing, and cross vendor interoperability assessment. Simulation based security and performance benchmarks further quantify rekey behavior, adversarial resilience, latency, throughput, and resource utilization under dynamic network conditions.

Finally, the paper highlighted the importance of cybersecurity specific diagnostics and logging within the Gateway Module to support Golden Tester based evaluation and ongoing lifecycle assurance. Together, these methods provide a practical foundation for validating SAE J1939-91C implementations in both development and operational contexts.

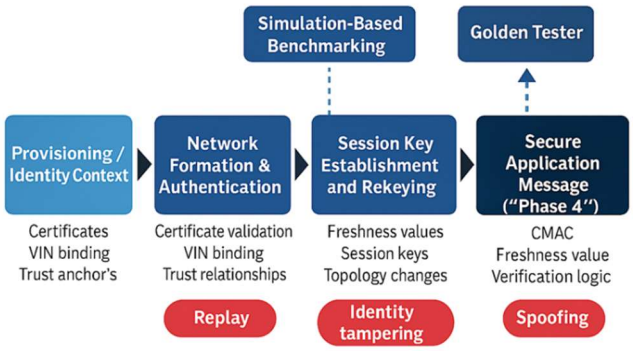

Figure 3: SAE J1939-91C protocol lifecycle with validation artifact mapping

REFERENCES

[1] J. Daily, P. Kulkarni, "Secure Heavy Vehicle Diagnostics," In Proc. Of the Ground Vehicle Systems Engineering and Technology Symposium (GVSETS), NDIA, Novi, MI, Aug. 13-15, 2020.

[2] J. Daily, D. Nnaji, B Ettlinger, "Securing CAN Traffic on J1939 Networks," Workshop on Automotive and Autonomous Vehicle security (Autosec) 2021, Feb21, 2021, https://dx.doi.org/10.14722/autosec.2021.23031

[3] M. Zachos, M. A. Mokhadder, J. Potter, "SAE J1939-91C Network Security Testing," Proceeding of WCX, April 2023

[4] M. Zachos, P. Kulkarni, "CyberUP – A Heavy Vehicle Cybersecurity Solution" In Proc. Of the Ground Vehicle Systems Engineering and Technology Symposium (GVSETS), NDIA, Novi, MI, Aug. 15-17, 2023.

[5] K. Medam, M. Zachos, M, "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 26AE-0018, Unpublished.

[6] DG LENS and BEACON device data sheet https://www.dgtech.com/wpcontent/uploads/2022/11/Beacon-flyer2022.pdf

[7] STAR FLEX device data sheet https://www.starcooperation.com/assets/uploads/dateien/kompetenzen/elektronik/datenblaetter/190213-specsheetflexdevice-l-en.pdf

8. CONTACT INFORMATION

Mark Zachos
President, DG Technologies
33604 W 8 mile road
Farmington Hills, MI 48335
Mzachos@dgtech.com
248-888-2000

Prakash Kulkarni, PhD
Director, DG Technologies
33604 W 8 mile road
Farmington Hills, MI 48335
PKulkarni@dgtech.com
248-888-2000