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

LEVERAGING DOMESTIC AUTOMOTIVE SOFTWARE DEVELOPMENT BEST PRACTICES FOR MOSA AND GCIA/VICTORY IMPLEMENTATION

Douglas Priemer[1], Karl Sime[1]

[1]Western Labs, LLC, Troy, MI

ABSTRACT

*As the Department of Defense (DoD) reforms acquisition to deliver digital capabilities at speed and scale[1], the adoption of mature domestic automotive standards and methods provides new ways to accelerate this direction. This whitepaper explores the strategic alignment between automotive-grade safety (**ISO 26262**), cybersecurity (**ISO/SAE 21434**), quality (**ISTQB/ASPICE**), and software development/validation practices with military frameworks like **MOSA**, **GCIA**, and **VICTORY**[2,3,4,5,6]. By shifting focus toward these cross-industry best practices and integrating them with DoD system safety and modularity frameworks, the U.S. Army can achieve a "Software Defined Vehicle" (SDV) posture that ensures overmatch through rapid, secure, and verifiable technology insertion for modular and interoperable ground vehicle software and control systems.*

Citation: D. Priemer, K. Sime, "Leveraging Domestic Automotive Software Development Best Practices for MOSA and GCIA/VICTORY Implementation" In *Proceedings of the Ground Vehicle Systems Engineering and Technology Symposium* (GVSETS), NDIA, Novi, MI, Aug. 11-13, 2026.

• INTRODUCTION

The Department of Defense (DoD) is currently navigating a critical paradigm shift to modernize its ground vehicle fleets, driven by the statutory mandate to implement a Modular Open Systems Approach (MOSA) across all major capability acquisitions. Historically, the integration of Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance, and Electronic Warfare (C4ISR/EW) systems relied on a decentralized, "bolt-on" methodology. This approach has precipitated severe constraints regarding Size, Weight, and Power (SWaP), hindered interoperability, and convoluted the life-cycle sustainment of vehicular platforms. To resolve these operational bottlenecks, the DoD promulgated the Vehicular Integration for C4ISR/EW Interoperability (VICTORY) architecture, which dictates a data bus-centric design to minimize hardware redundancy through shared processing and standardized network transport.

Concurrently, the domestic automotive industry has successfully navigated a congruent architectural evolution,

transitioning from highly distributed, single-function Electronic Control Units (ECUs) to the centralized, high-speed computational frameworks characteristic of the modern Software Defined Vehicle (SDV). This commercial transition is underpinned by mature, highly rigorous engineering methodologies governing functional safety, software quality, and cybersecurity. While military system safety standards—such as MIL-STD-882E and the Joint Software Systems Safety Engineering guidelines—establish the foundational hazard management baselines for DoD procurements, they can be significantly augmented by leveraging prescriptive commercial standards. Frameworks such as ISO 26262 for electrical/electronic (E/E) functional safety, ISTQB and ASPICE for software process maturity, and ISO/SAE 21434 for automotive cybersecurity provide quantifiable, mathematically rigorous mechanisms for risk mitigation. Synthesizing these domestic automotive best practices with DoD modularity architecture offers a verified blueprint for satisfying the DoD's Software Modernization Goals and executing its Zero Trust architecture roadmap.

This whitepaper systematically explores the strategic convergence of these commercial automotive methodologies with military ground vehicle modernization imperatives to achieve a secure, interoperable SDV posture. The body of the paper is structured as follows: **Section 1** examines the alignment of ISO 26262 functional safety metrics with MIL-STD-882E software criticality assessments to define rigorous Verification and Validation (V&V) tasks. **Section 2** details the operationalization of MOSA pillars through ASPICE and ISTQB quality frameworks. **Section 3** contextualizes automotive cybersecurity engineering (ISO/SAE 21434) within the VICTORY Information Assurance tenets to ensure cyber resilience. **Section 4** explores the realization of VICTORY tenets through SDV domain controllers and Automotive Ethernet. **Section 5** addresses the complex risk management strategies required for Commercial-Off-The-Shelf (COTS) software integration. **Section 6** highlights V-Model traceability and extended lifecycle support. Finally, **Section 7** concludes with strategic recommendations for fostering cross-industry collaboration to expedite DoD capability fielding.

1. DEEPENING SAFETY ALIGNMENT: ISO 26262, MIL-STD-882E, and Software Criticality

To achieve verifiable safety in an SDV posture, automotive safety standards can be mapped directly to DoD safety requirements, although this requires translating different risk calculation methodologies. Under MIL-STD-882E, safety-critical software is evaluated using the Software Safety Criticality Matrix (SSCM), which assesses the degree of control authority the software exercises over hazardous hardware[7]. This evaluation produces a **Software Criticality Index (SwCI)** ranging from 1 (extremely critical, autonomous control) to 5 (no safety impact).

Integrating automotive ISO 26262 ASIL (Automotive Safety Integrity Level) ratings directly into this matrix helps programs map commercial automotive hazard models to the DoD's required **Level of Rigor (LOR) tasks**[7]. Automotive practices fulfill the highest LOR verification requirements for highly critical SwCI 1 and SwCI 2 software by mandating **Modified Condition/Decision Coverage (MC/DC)**. This provides structural coverage analysis that

mathematically proves every logic gate in the code performs safely and as intended[8]. A large pool of automotive software safety engineers is available to provide their services and experience directly to the military to meet this end, proving new insights into how software can fail and innovative strategies for mitigation.

2. SOFTWARE QUALITY AND OPERATIONALIZING MOSA

2.1 The **ISTQB** and **ASPICE** frameworks provide a standardized language and rigorous methodology for software testing and process maturity that directly support the DoD Software Modernization Strategy. ISTQB professionalizes software testing with methodologies like boundary value analysis, ensuring that software factories produce repeatable, high-quality code that is auditable for DoD safety cases.

2.2 Modular Systems

ASPICE evaluates the maturity of the development process itself, which is critical for managing a diverse supply chain of Commercial-Off-The-Shelf (COTS) and third-party software. This componentized approach to software perfectly maps to the **five statutory Modular Open Systems Approach (MOSA) pillars** required for all DoD acquisition programs[4]:

2.2.1 Establish an Enabling Environment: Aligning organizational structures, acquisition strategies, and business practices to support MOSA. This requires aligning the programmatic acquisition strategy, intellectual property (IP) framework, and technical management processes prior to system development. Such foundational alignment ensures that cross-functional teams operate within a unified systems engineering ecosystem conducive to continuous integration and technology insertion. The automotive industry has a well-established framework of organizations (such as SAE, AUTOSAR, ISO, MISRA, and many others) that support these efforts with resources readily leveraged by the military.

2.2.2 Employ a Modular Design: Decomposing systems into self-contained, scalable, and reusable functional elements. ASPICE evaluations offer a direct method to audit supplier capabilities to deliver these decoupled software modules. This architectural paradigm strictly partitions system functionality into discrete, cohesive, and loosely coupled subsystems. By encapsulating functional elements, programs can independently upgrade or interchange specific modules without propagating unintended technical debt or disrupting the overarching system architecture. Most automotive software architectures are highly modular and re-usable which lends a wealth of experience, potentially assisting a smoother execution of MOSA initiatives.

2.2.3 Designate Key/Modular Interfaces: Decoupling interface specifications from their service implementations so they can follow separate lifecycles. By explicitly demarcating shared boundaries between major system platforms and components, systems engineers can sever the lifecycle dependencies of individual modules. This

decoupling relies on well-defined physical, logical, and functional characteristics that facilitate seamless data exchange and subsystem interoperability. Similarly, the automotive software industry has migrated to software architectures that emphasize modularity to facilitate reuse, a practice which addresses the prohibitive cost and long development cycles associated with re-writing software for every new domestic vehicle platform.

2.2.4 Leverage Consensus-Based Open Standards: Using widely accepted, non-proprietary standards to prevent vendor lock-in and increase competition. Implementing non-proprietary, widely ratified standards at these interface boundaries mitigates vendor lock-in and fosters a competitive defense industrial base. This strategic standardization is vital for ensuring that disparate components can interoperate efficiently while maintaining strict adherence to DoD system performance specifications. Automotive Open System Architecture (AUTOSAR) is the go-to open-source standard used by all automotive OEMs and provides many examples of frameworks and methods that could potentially benefit the development and release of military ground vehicle software.

2.2.5 Certify Conformance: Rigorously verifying and validating that systems comply with open interface standards. A rigorous verification and validation (V&V) framework must be established to mathematically and empirically prove that instantiated modules strictly adhere to the mandated open interface standards. Conformance certification fundamentally guarantees that independent subsystem development does not compromise the holistic integrity or interoperability of the ground vehicle system. The automotive industry is rich in companies that provide V&V services, some now utilize AI to accelerate the conformance timeline while increasing the coverage of ever-increasing numbers of software functions, features, and complexity[9].

2.3 Government Reference Architectures

To operationalize MOSA effectively, DoD organizations frequently adopt standardized Government Reference Architectures (GRAs) to establish baseline expectations for subsystem and system-level modularity. A critical example for military vehicles is the Ground Combat Systems Common Infrastructure Architecture (GCIA). By incorporating GRAs like GCIA directly into system specifications, program offices can clearly mandate the required level of modularity and ensure the consistent application of modular system interfaces across different platforms and vendors. AUTOSAR closely parallels the approach taken by the government by providing reference architectures for both conventional (Classic Platform) and Autonomous (Adaptive Platform) domestic vehicles.

2.4 Intellectual Property

Implementing MOSA requires the acquisition of necessary interface technical data and computer software rights (such as Government Purpose Rights) to allow the

DoD to flexibly replace or upgrade modular components via third-party developers. The automotive industry is highly experienced in negotiating these same concerns with most third-party software development and validation service providers.

3. ADVANCING CYBERSECURITY AND ZERO TRUST: ISO/SAE 21434 AND VICTORY INFORMATION ASSURANCE

3.1 While ISO 26262 addresses functional safety (hazards caused by system malfunctions), modern SDVs require robust defenses against malicious external threats. The **ISO/SAE 21434** standard provides the definitive framework for road vehicle cybersecurity engineering[6]. By establishing a Cybersecurity Management System (CSMS) and mandating Threat Analysis and Risk Assessment (TARA) throughout the product lifecycle, ISO/SAE 21434 ensures "security by design." This perfectly complements the DoD's mandates for cyber resilience and survivability across systems, software, and supply chains.

These automotive cybersecurity principles operationalize the DoD's Zero Trust roadmap ("never trust, always verify") and integrate seamlessly with the VICTORY Architecture's Information Assurance (IA) capability group[5]. VICTORY treats IA as a "first-class citizen" by defining shared components to create a "defense in depth" posture:

3.2 Access Control: VICTORY defines an Attribute-Based Access Control (ABAC) model utilizing standard Authentication Services, Policy Decision Services, and Policy Enforcement Services to protect vulnerable network interfaces. This ABAC infrastructure evaluates contextual policies dynamically, ensuring that only authenticated and authorized entities can manipulate safety-significant data. It effectively operationalizes the Zero Trust tenet by compartmentalizing network access and mitigating the risk of lateral threat movement across the vehicular bus. The military should consider the extraordinarily strong cybersecurity implementations successfully used by the automotive industry worldwide, such as Secure Onboard Comms (SecOC) which rigorously protects both internal and external messages and the safety critical software stacks using complex authentication routines.

3.3 Data Integrity and Confidentiality: VICTORY mandates component types such as Data Signing Services, Inline Network Encryptors (INE), and Data at Rest (DAR) Encryptors to ensure data is protected both in transit across the VICTORY Data Bus (VDB) and while stored. Utilizing advanced cryptographic primitives, such as Data Signing Services and Inline Network Encryptors (INE), guarantees the non-repudiation and opacity of data both at rest and in transit. This defense-in-depth layer is mathematically foundational to prevent adversarial interception, spoofing, or malicious corruption of critical C4ISR/EW communications.

3.4 Hardware-Backed Root of Trust: Aligning with advanced automotive

practices, these IA services are strengthened by Signal-Level Authentication (Message Authentication Codes) and Hardware Security Modules (HSMs) that isolate secret cryptographic keys from digital extraction. Hardware Security Modules (HSMs) provide a tamper-resistant enclave for cryptographic key generation and storage, structurally isolating secrets from software-based exploitation. By anchoring Message Authentication Codes (MACs) to this immutable silicon root, the architecture establishes a highly deterministic foundation for verifiable system integrity. The automotive software and embedded controls industry uses similar methods, offering lessons learned and enhancements to military ground vehicle controls modernization efforts.

4. ADVANCING VICTORY VIA THE SOFTWARE DEFINED VEHICLE

4.1 Vehicular Integration for C4ISR/EW Interoperability (VICTORY) architecture was developed to eliminate the practice of "Bolt On" systems that duplicate hardware, increase Size, Weight, and Power (SWaP) demands, and cramp crew compartments. The domestic automotive industry's evolution toward the Software Defined Vehicle (SDV)—driven by centralized computing and high-speed networking—provides direct, commercially proven methodologies for realizing VICTORY's tenets:

4.2 The VICTORY Data Bus (VDB): VICTORY mandates a "data bus-centric" design utilizing "on-the-wire" network interface (typically IP/Ethernet). The VDB acts as the central integration mechanism for transporting data and integrating C4ISR/EW systems. The VDB acts as the foundational convergence layer, typically utilizing IP/Ethernet protocols, to aggregate disparate C4ISR/EW subsystems into a unified, on-the-wire network topology. Domestic automotive manufacturers are executing this exact architectural transition by replacing legacy, domain-specific networks (such as standard CAN buses) with high-speed Automotive Ethernet backbones. Leveraging this commercial "Ethernet-first" approach enables military ground vehicles to support high-bandwidth data routing, multicast distribution, and Over-the-Air (OTA) technology updates using commercially mature routing and Quality of Service (QoS) protocols. This bus-centric paradigm eliminates point-to-point hardwiring, thereby optimizing data transport routing, multicast distribution, and differentiated Quality of Service (QoS) metrics.

4.3 Shared Hardware and Services: By using shared hardware computing resources (Shared Processing Units), Data Loggers, and shared Position, Navigation, and Timing (PNT) services, software applications can be deployed across the VDB without adding dedicated, redundant hardware boxes. This directly mirrors the automotive industry's shift from employing dozens of federated, single-function Electronic Control Units (ECUs) to using consolidated, high-performance "Domain

Controllers" or "Zonal Compute Clusters." Furthermore, by adopting domestic automotive virtualization best practices, program offices can establish Virtual ECUs (V-ECUs) to simulate the entire software stack independently of real-time hardware execution. This "virtual first" methodology front-loads defect discovery and parallelizes testing in the cloud, ensuring that only verified code is deployed to the physical vehicle. By abstracting application layers from underlying hardware via Shared Processing Units (SPUs) and Network Attached Storage (NAS), the architecture dramatically reduces the Size, Weight, and Power (SWaP) footprint. This virtualization enables dynamic resource allocation and eliminates the redundant instantiation of physical hardware, such as disparate GPS receivers for Position, Navigation, and Timing (PNT).

4.4 Modular Open RF Architecture (MORA) and ADAS Sensor Abstraction: For complex Radio Frequency (RF) and Electronic Warfare missions, the MORA extension introduces a Low Latency Bus (ML2B). This transports digital signal data, allowing RF signal resources (like antennas and amplifiers) to be separated from processing resources. This decoupling leverages the exact automotive methodology used for Advanced Driver-Assistance Systems (ADAS), where raw, low-latency sensor data (from LiDAR, high-definition cameras, and Radar) is physically separated from the central autonomous compute brains. By applying domestic automotive standards for deterministic, low-latency data transport, the DoD can ensure real-time control of digitized RF payloads without duplicating external aperture hardware, enabling split-second threat response comparable to commercial autonomous collision avoidance.

5. MANAGING COMMERCIAL OFF-THE SHELF (COTS) RISKS

5.1 Because automotive SDV best practices heavily rely on third-party COTS and Non-Developmental Item (NDI) software, integration requires specific safety engineering strategies.

5.2 The "Black Box" Challenge: COTS vendors rarely provide the internal design documentation or source code required to perform standard DoD hazard analyses. Consequently, program offices must conduct "black box" testing, evaluating the software based solely on its interaction with the target system. Because proprietary constraints typically preclude source code review, safety engineers must employ rigorous black-box testing methodologies to assess the COTS item's failure modes within the broader system context. This necessitates sophisticated boundary value analysis and fault injection testing to empirically characterize the software's non-deterministic behavior when subjected to anomalous operational states. The same problem exists in the automotive industry where OEMs concerned with IP exposure will resort to black box testing which is the accepted norm in many cases. It is important to note that software architecture

must be designed to facilitate black box testing, providing I/O access to all testable processes while at the same time not creating an easy pathway to reverse engineering the concealed software.

5.3 Wrapper and Middleware Protection: To safely integrate COTS software, the architecture should utilize "wrappers" or middleware. This intermediary layer of software isolates the COTS product, ensuring it cannot negatively impact safety-critical data or interrupt the execution of core defense applications. To strictly enforce functional partitioning, systems engineers must design abstraction layers—or wrappers—that actively filter and isolate the data streams interacting with the COTS module. This architectural firewall prevents unverified commercial code from asserting uncontrolled authority over safety-critical hardware, thereby containing potential faults before they propagate into a catastrophic system failure. The automotive embedded software control industry widely utilizes multi-layered software signal abstractions (AUTOSAR) for the same reason while at the same time providing a remarkably high degree of modularity.

6. TRACEABILITY, DOCUMENTATION, AND LIFECYCLE SUPPORT

6.1 Military environments require demonstrable compliance with regulatory and safety standards, making transparency essential[10]. This would be no different from approaches taken by the automotive industry.

6.2 Requirements Tracking: Every requirement is tracked from initial concept to final deployment, maintaining accountability across interdisciplinary teams. Implementing a highly disciplined Requirements Traceability Matrix (RTM) ensures bidirectional linkage from high-level system specifications down to discrete computer software units (CSUs). This systematic traceability is critical for verifying that all derived safety constraints, including mitigating software safety requirements (MSSRs), have been functionally instantiated and empirically validated. There are many commonly available tools used by the automotive industry (Jira, Doors, Polarion, and others) that ensure all development and test activities are linked to every element in the software requirements specification (SRS) documents.

6.3 Support for Long Lifecycles: The structured nature of the hybrid V-Model and DevSecOps toolchains provides a robust foundation for maintaining and systematically upgrading vehicles over long operational lifecycles as innovative technologies emerge. Utilizing robust DevSecOps toolchains within a Modified V-Model framework accommodates the evolutionary nature of prolonged acquisition lifecycles. This ensures that subsequent technology insertions and obsolescence management efforts can be continuously integrated, regression-tested, and certified without requiring holistic architectural redesigns. Though many domestic automotive models are short lived

compared to military ground vehicles that can have 30 year or more lifecycles, it is not difficult to extend coverage of domestic toolchains to meet the longer cycles of military ground vehicles.

6.4 Supplier Collaboration: For complex multi-disciplinary developments, the domestic automotive V-Model facilitates the seamless integration of subsystems from various suppliers and subcontractors. A federated system-of-systems (SoS) approach dictates that prime contractors and Tier-1 suppliers meticulously define Interface Control Documents (ICDs) to govern module boundaries. This formalized cross-functional synergy is essential to mitigate interface-related hazard causal factors and ensure deterministic interoperability among decentralized development nodes.

6.5 Vendor Lock: Deep concerns about supplier vendor lock are shared by both domestic automotive and military software and controls work groups and is one of the primary challenges of true interoperability and modularity. Despite growing efforts for military to promote modularity and interoperability from within the defense community, it does not appear to promote the same goals for products available from the domestic automotive industry. These barriers may unintentionally exclude the vast knowledge base and experience of the domestic automotive software and embedded controls industry from making substantial contributions to the modernization of military ground vehicle software and systems.

7. CONCLUSION AND RECOMMENDATIONS:

To fully realize the operational and economic potential detailed in this whitepaper, the Department of Defense should proactively collaborate with the commercial sector. The following recommendations outline the strategic initiation of a collaborative inter-industry community to accelerate military ground vehicle modernization:

7.1 Establish a Cross-Industry Community of Interest (COI): Form a dedicated joint workgroup comprising DoD systems engineers, commercial automotive software architects, and defense industrial base stakeholders to bridge the paradigm gap between commercial Software Defined Vehicle (SDV) advancements and military ground vehicle modernization. This collaborative forum will facilitate the mutually beneficial exchange of intellectual property strategies and technical data rights frameworks necessary to operationalize continuous technology insertion. It will serve as an incubator for translating rapid commercial innovation into actionable acquisition policy for the Department of Defense.

7.2 Align Commercial Toolchains with MOSA Objectives: Leverage the COI to systematically map commercial automotive software development and validation tools—such as advanced DevSecOps pipelines and cloud-based virtualization—directly to the DoD's statutory Modular Open Systems Approach (MOSA) pillars. By standardizing the use of these commercial-off-the-shelf

integration methodologies, the DoD can more efficiently decouple major system components from their underlying hardware platforms. This abstraction is vital for enforcing vendor independence, enhancing lifecycle affordability, and rapidly scaling interoperable capabilities across the fleet.

7.3 Harmonize Verification and Validation (V&V) Frameworks: Task the workgroup with synthesizing commercial automotive safety standards (e.g., ISO 26262) with the rigorous hazard mitigation mandates of MIL-STD-882E to create a unified V&V protocol for open interfaces. By mathematically proving conformance to consensus-based standards via automated structural coverage analysis (MC/DC), the DoD can aggressively streamline its certification timelines. This unified methodology will provide acquisition authorities with the deterministic, objective evidence required to confidently accept residual safety risks associated with modular C4ISR/EW integrations.

7.4 Pilot a Virtual-First Interoperability Initiative: Initiate a joint pilot program utilizing Virtual Electronic Control Units (V-ECUs) and digital twin models to simulate the integration of disparate automotive and military subsystems via the VICTORY Data Bus (VDB). This "virtual first" approach will allow the inter-industry team to empirically evaluate architectural modularity and network resilience without the prohibitive costs of physical hardware-in-the-loop testing. This empirical data will prove that leveraging automotive Ethernet and centralized compute clusters can successfully reduce vehicle Size, Weight, and Power (SWaP) constraints while ensuring solid overmatch capabilities.

8. REFERENCES

[1] DoD Strategic Directives: Secretary Hegseth Memorandum (March 2025) and Army Software Modernization Goals.

[2] Western Labs / Karl Sime (2024-2025): Briefings on Domestic Automotive Standards for MOSA, GCIA, and VICTORY.

[3] Automotive Industry Standards (Safety & Quality): ISO 26262 (Functional Safety), ISO 23150 (Sensor Interfaces), ISTQB, AUTOSAR, and ASPICE.

[4] MOSA Implementation Guidebook (2025): *Implementing a Modular Open Systems Approach in Department of Defense Programs*, Office of Systems Engineering and Architecture (February 2025).

[5] VICTORY Architecture (2019): *Vehicular Integration for C4ISR/EW Interoperability (VICTORY) Architecture*, Version A (April 2, 2019).

[6] Industry Standards (Cybersecurity): ISO/SAE 21434: *Road Vehicles – Cybersecurity Engineering (External Reference).*

[7] MIL-STD-882E w/CHANGE 1 (2023): *Department of Defense Standard Practice: System Safety* (27 September 2023).

[8] Joint Software Systems Safety Engineering Handbook (2010): Developed by the Joint Software Systems Safety Engineering Workgroup (August 27, 2010).

[9] D. Priemer, "AI-Assisted Verification Workflows for Software-Defined Ground Vehicle Systems," In Proceedings of the Ground Vehicle Systems Engineering and Technology Symposium (GVSETS), NDIA, Novi, MI, Aug. 11-13, 2026.

[10] Western Labs / The "V" for DoD (2024): Application of domestic automotive V-Model frameworks for Department of Defense vehicle programs.

9. CONTACT INFORMATION

Douglas Priemer
Vice President, Engineering
Western Labs
Troy, Michigan, USA
douglas.priemer@westernlabs.com

Karl Sime
Sr. Consulting Engineer
Western Labs
Troy, Michigan, USA
karl.sime@westernlabs.com

10. ACKNOWLEDGMENT

This work was inspired by NDIA, NAMC, GVSETS, APEX accelerators, and many other organizations dedicated to building strength, effectiveness, and outreach of the Federal Acquisition System. I am also grateful to my colleagues at Western Labs, LLC, and Methodica Technologies LLC, for their encouragement and support.

11. ACRONYMS

ADAS	Advanced Driver-Assistance Systems
ASIL	Automotive Safety Integrity Levels
AUTOSAR	AUTomotive Open System ARchitecture
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
COI	Community of Interest
COTS	Commercial-Off-The-Shelf
DFMEA	Design for Failure Mode & Effects Analysis
DoD	Department of Defense
E/E	Electrical and Electronic
GCIA	Ground Combat Systems Common Infrastructure Architecture
HARA	Hazard Analysis and Risk Assessment
HSM	Hardware Security Manager
ISO	International Organization for Standardization
ISTQB	International Software Testing Qualifications Board
LiDAR	Light Imaging, Detection, and Ranging
MAC	Message Authentication Code
ML2B	MORA Low Latency Bus
MORA	Modular Open Radio frequency Architecture
MOSA	Modular Open Systems Approach
SDLC	Software Development Life Cycle
SDV	Software Defined Vehicle

V&V	Verification and Validation
V-ECUs	Virtual Electronic Control Units
VICTORY	Vehicular Integration for C4ISR/Electronic Warfare Interoperability