



AMERICAN CENTER FOR MOBILITY
SAFE. SUSTAINABLE. SECURE.

Dynamic Cybersecurity Validation for Software-Defined Mobility

A Cybersecurity Insights Brief by Drivesec and
American Center for Mobility

A decorative graphic in the bottom right corner consisting of several overlapping diagonal stripes in shades of blue and red.

Foreword

Connected and automated mobility platforms are evolving into software-defined cyber-physical systems. In this new paradigm, core vehicle behaviors — from torque management and braking to perception and autonomous decision-making — are governed by continuously updateable software. Over-the-air (OTA) updates now introduce ongoing operational change, transforming vehicles into platforms that evolve throughout their lifecycle.

This shift creates a moving cybersecurity and safety target. Changes in software timing, perception thresholds, or compute workload can alter system behavior in ways that only become visible under real-world driving conditions. As a result, cybersecurity can no longer be treated as a discrete engineering activity; it is inseparable from safety assurance.

At the same time, automation is advancing from advanced driver assistance systems (ADAS) toward higher levels of automated driving systems (ADS), including robotaxis, autonomous trucking, and remotely supervised logistics platforms. As the human fallback layer diminishes, vehicles become increasingly dependent on the reliability and integrity of digital systems. This evolution also makes them high-value targets for cyber threats, as disruptions to perception, control, or backend communications can directly influence safety outcomes.

These trends are occurring alongside rising regulatory expectations and public scrutiny. Governments and industry bodies increasingly expect evidence-based cybersecurity validation across the entire vehicle lifecycle.

Reuben Sarkar - President & CEO, American Center for Mobility

Giuseppe Faranda - President, Drivesec

About ACM and Drivesec / Weseth®

The American Center for Mobility (ACM) is a 500-acre purpose-built proving ground designed to safely test, validate, and demonstrate advanced mobility technologies under controlled, real-world conditions. Its infrastructure supports the evaluation of connected and automated vehicle systems across complex environments.

Drivesec provides cybersecurity automation technologies tailored to the mobility sector. Its Weseth® platform enables secure remote access, automated cyber-test orchestration, and continuous evidence generation across both static and dynamic testing environments.

Together, ACM and Drivesec combine physical testing infrastructure with automated cybersecurity validation, enabling repeatable cyber-physical experimentation in motion. This collaborative ecosystem allows organizations to validate cybersecurity performance under conditions that closely mirror real-world operations.

FRAMEWORKS ADDRESSED

This paper aligns with global cybersecurity frameworks including:

- UN ECE R155 & R156
- ISO/SAE 21434 (cited under R155/156)
- NHTSA Cybersecurity Best Practices (2022)
- Auto-ISAC Industry Best Practices
- China's GB 44495 cybersecurity requirements
- Cyber Resilience Act (CRA)
- RED (ISO 18031)
- IEC 62443
- IACS UR E26 & E27

Executive Summary

Software-defined vehicles operate within complex cyber-physical environments where system behavior is influenced by motion, sensor variability, and computational load. Traditional static cybersecurity testing conducted in laboratories or on benches is no longer sufficient to fully evaluate these systems.

Centralized compute architectures and integrated sensor stacks behave differently under real-world conditions such as vehicle speed, perception confidence, environmental noise, and network latency. Issues that remain hidden in static environments can become safety-relevant only when the vehicle is in motion.

Over-the-air updates further increase this complexity. Frequent software updates can introduce subtle changes to perception algorithms, arbitration logic, and control systems. Each update potentially alters the system's cyber-physical behavior, making regression validation essential.

Dynamic cybersecurity validation addresses this challenge by evaluating systems during real-world operation, providing evidence that cybersecurity controls remain effective across changing conditions.

THIS PAPER IS INTENDED FOR

- Product leaders responsible for SDV platforms
- Cybersecurity and safety engineering teams
- Operational technology (OT) leaders managing connected fleets
- Regulators and policy stakeholders evaluating cyber-physical risk



REPRESENTATIVE DYNAMIC CYBERSECURITY SCENARIOS

Perception Spoofing	Introducing inconsistencies between camera, radar, or lidar inputs to evaluate perception fallback and AEB decision-making during emergency braking.
Network Fuzzing	Identifying timing or arbitration faults that may influence torque blending or deceleration profiles under high-regeneration braking.
Sensor Fusion Conflict	Simulating environmental interference, drift, or saturation affecting localization and perception logic.
ADS Lane-Change Anomalies	Introducing perception noise or timing discrepancies to observe fallback transitions and system controllability.
Fleet Command & API Integrity	Simulating backend degradation or manipulation affecting remote mission updates or operational commands.

BUSINESS OUTCOMES

- **Reduced cyber-safety risk** after OTA updates through automated validation cycles
- **Lower validation costs** by automating scenario execution, logging, and reporting
- **Faster time-to-validation** after software releases
- **Cross-team collaboration** between cybersecurity and safety engineering teams
- **Evidence packages** aligned with global regulatory expectations

1. Why Dynamic Cybersecurity Validation Matters

Cybersecurity risks in software-defined vehicles increasingly emerge from interactions between software logic and physical vehicle behavior. These cyber-physical interactions depend on dynamic conditions such as speed, torque demand, sensor confidence levels, and compute load.

For example, a timing anomaly introduced by a software update may only manifest when the vehicle is operating at highway speed while processing high-volume sensor data. Static laboratory testing may not expose such interactions.

Dynamic cybersecurity validation allows engineers to observe how cyber anomalies translate into real-world safety outcomes.

DYNAMIC TESTING CAN REVEAL

- Cyber-physical timing dependencies
- Sensor and actuator interaction faults
- Vehicle state-dependent vulnerabilities
- Perception degradation under environmental variability

OTA development pipelines further amplify this challenge. Each software release has the potential to shift perception thresholds, arbitration logic, or network timing. Dynamic regression testing ensures these changes do not introduce unintended vulnerabilities or unsafe behaviors.

As automation progresses toward higher levels of ADS deployment, vehicles rely increasingly on software systems rather than human intervention. Cybersecurity weaknesses in these systems can therefore translate directly into safety outcomes.

Dynamic validation helps ensure that automated mobility systems remain trustworthy, resilient, and safe under real-world conditions.

2. Standards and Guidance Landscape

Regulatory and industry frameworks increasingly require evidence-based cybersecurity management throughout the vehicle lifecycle.

UN Regulation ECE R155

Requires manufacturers to implement cybersecurity management systems (CSMS) and demonstrate evidence of risk mitigation across the vehicle lifecycle.

ISO/SAE 21434

Defines engineering processes for identifying, assessing, and mitigating cybersecurity risks during product development.

NHTSA Cybersecurity Best Practices (2022)

Emphasizes layered defenses, system monitoring, and incident response capabilities.

Auto-ISAC Industry Best Practices

Provides governance models and collaborative approaches for detection and response.

GB 44495

Establishes cybersecurity validation requirements for vehicles entering the Chinese market.

EU Cyber Resilience Act (CRA)

Establishes baseline cybersecurity requirements for connected products and software, including secure development, vulnerability management, and documentation obligations. It extends compliance responsibilities to the full supply chain and product lifecycle.

Radio Equipment Directive (RED) — Delegated Cybersecurity Acts

Mandates protections against network misuse, unauthorized access, and privacy risks for wireless-enabled products. Requires manufacturers to demonstrate secure configurations and safeguard data transmitted over radio interfaces.

IEC 62443 Series (Industrial & OT Cybersecurity)

Provides a structured framework for securing industrial automation and control systems through defense-in-depth and maturity-based security levels. Helps ensure that connected mobility and industrial systems integrate securely into operational environments.

IACS Unified Requirements E26 & E27

Define cybersecurity requirements for control systems used in marine and industrial sectors, covering secure integration and resilience against operational disruption. Ensure cyber-physical systems meet stringent robustness expectations in safety-critical environments.

Dynamic cybersecurity validation supports these frameworks by providing real-world verification of cybersecurity controls and generating evidence that organizations can use to support compliance and regulatory engagement.

3. Proving Ground as a Cyber-Physical Safety Laboratory

Testing cyber-physical interactions safely requires specialized infrastructure. Proving grounds provide environments where high-risk scenarios can be executed without exposing the public to safety risks.

ACM PROVING GROUND ENABLES

- Configurable road environments replicating urban and highway conditions
- Integrated connectivity infrastructure
- Controlled environments for repeatable testing scenarios

Repeatability is critical for cybersecurity validation. Engineers must be able to reproduce anomalies under consistent conditions to confirm vulnerabilities and validate mitigation strategies.

Certain cyber scenarios — such as GNSS interference — cannot be safely radiated due to regulatory and environmental constraints. However, equivalent effects can be replicated through controlled methods:

- Conducted signal injection
- Software-based spoofing
- Recorded data replay through system interfaces

These methods allow researchers to study cyber-physical behaviors while maintaining compliance with aviation and communications regulations.

4. Decision Criteria for Product and OT Leaders

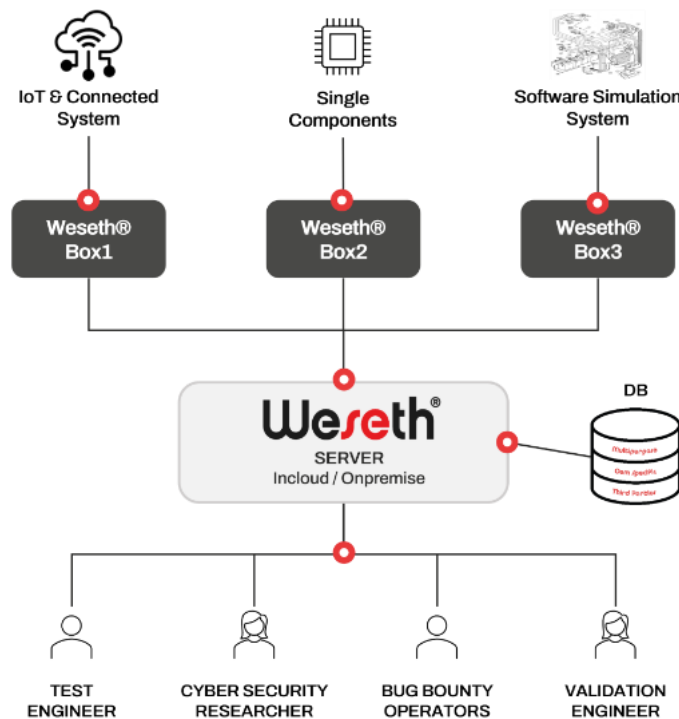
Organizations should consider dynamic cybersecurity validation when deploying technologies that increase cyber-physical complexity.

TYPICAL DECISION TRIGGERS

- Launching OTA updates affecting perception or control systems
- Deploying Level 3 or higher automated driving capabilities
- Operating autonomous fleet platforms
- Integrating new sensor or compute architectures

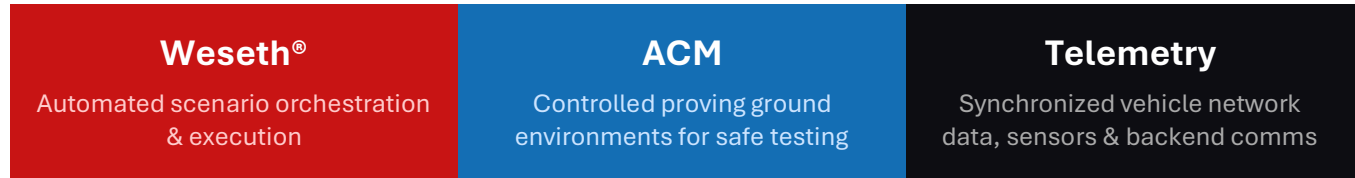
KEY OUTCOMES FOR DECISION-MAKERS

Safety Outcome Validation	Evaluating controllability, fallback behavior, and recovery during cyber events.
Lifecycle Cybersecurity Evidence	Generating documentation aligned with R155, ISO 21434, and other regulatory frameworks.
Operational Efficiency	Automating validation cycles to accelerate testing after software updates.



5. Drivesec Weseth® + ACM Execution Model

The collaboration between Drivesec and ACM combines automated cybersecurity validation with real-world proving ground infrastructure.



This architecture enables repeatable cyber-physical experimentation and supports continuous validation cycles across OTA releases.

6. Dynamic Cybersecurity Use Cases

Dynamic validation scenarios can be categorized into several core risk domains. These scenarios reflect real-world conditions encountered by modern SDV platforms and ADS fleets.

Perception Manipulation

- Perception spoofing during emergency braking
- Sensor fusion conflict scenarios

Control System Stress

- High-regen braking under stateful network fuzzing

ADS Operational Integrity

- Lane-change and merge anomalies
- Fleet command and API integrity testing

7. Evidence, Metrics, and Reporting

Dynamic validation programs generate detailed evidence packages supporting engineering, governance, and regulatory needs.

TYPICAL DELIVERABLES

- Scenario execution logs
- Vehicle telemetry and network traces
- Sensor data recordings
- Attack vectors and detection outcomes
- Mitigation validation results

Safety Metrics

- Controllability ratings
- Fallback success rates
- Recovery time after cyber anomalies

Cybersecurity Metrics

- Detection fidelity
- Attack window reduction
- Regression coverage mapped to regulatory frameworks

8. Program Blueprint

A typical validation program may follow a structured multi-phase approach.

Phase 0	Scoping (Weeks 0–1) Define target platform, features, and testing scenarios.
Phase 1	Static Baseline (Weeks 1–2) Conduct bench and HIL hardening with scenario preparation.
Phase 2	Controlled Dynamics (Weeks 2–5) Execute cyber-physical scenarios within proving ground environments.
Phase 3	Backend Scenarios (Weeks 5–6) Simulate OTA pipelines, API interactions, and backend communication disruptions.
Phase 4	Closeout and Scale (Weeks 6–8) Generate evidence packages and establish recurring validation cycles.

After pilot completion, organizations can scale testing programs across additional vehicle platforms or fleet deployments.

9. Call to Action

The transition toward software-defined and automated mobility systems requires a new approach to cybersecurity validation. Dynamic cybersecurity validation enables organizations to evaluate cyber-physical risks under realistic operating conditions while generating evidence aligned with global regulatory expectations.

Drivesec and the American Center for Mobility invite OEMs, Tier-1 suppliers, and ADAS & ADS developers to collaborate on pilot programs that explore dynamic cybersecurity validation in motion. These collaborations can help shape future validation methodologies while establishing a foundation for continuous cyber-physical assurance across the mobility ecosystem.