RUNSAFE SECURITY

Complete Vehicle-Wide Visibility

RUNSAFE SECURITY'S APPROACH TO R155/ISO21434

As vehicles become increasingly software-defined and interconnected, cybersecurity now plays a direct role in vehicle safety and operational integrity. New global standards and regulatory requirements reflect this shift, recognizing that vulnerabilities in connected ECUs, over-the-air update systems, and supplier-provided components can introduce real-world safety risk. The compliance landscape is evolving from process documentation to demonstrable, lifecycle cybersecurity assurance.

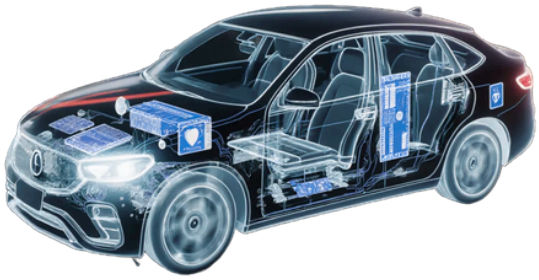
NEW EXPECTATIONS: ISO 21434

Automotive manufacturers and suppliers face increasing regulatory scrutiny under ISO/SAE 21434 and UNECE R155. An SBOM alone is not enough. To ensure vehicle safety and regulatory approval, OEMs are expected to demonstrate:

- A complete, validated SBOM
- A clear understanding of vulnerabilities
- A risk-based remediation strategy
- Vehicle lifecycle monitoring and response processes

HOW RUNSAFE SUPPORTS AUTOMOTIVE COMPLIANCE

RunSafe strengthens the technical evidence required to support ISO/SAE 21434 engineering activities and UNECE R155 CSMS regulatory obligations — without compromising functional safety under ISO 26262 (including ASIL A-D).



SOFTWARE TRANSPARENCY & SBOM ACCURACY

Complete, validated SBOM ready to meet ISO 21434 standards as key aspect for software component management.

- Automated build-time SBOM generation for embedded systems
- Accurate ECU software inventory
- CycloneDX-compliant and aligned to NTIA minimum elements

EXPLOITABILITY-BASED RISK CLARITY

Risk prioritization grounded in clear, outlined vulnerability posture.

- Maps CVE to SBOM components in real time
- Assesses and prioritize vulnerability by exploitability — not just presence
- Determines urgency (patch, mitigate, monitor, accept risk)
- Supports VEX documentation

MEASURABLE RISK REDUCTION

Demonstrable reduction of of exploitable software risk.

- Makes classes of memory-based vulnerabilities non-exploitable
- Reduces risk when patches are unavailable
- No source code rewrites required

LIFECYCLE MONITORING SUPPORT

Sustained compliance confidence across the vehicle lifecycle.

- Continuous monitoring for new CVEs
- SBOM diff comparisons between builds
- Integration with GitHub, GitLab, Bitbucket

A STRONGER CYBERSECURITY POSITION

RunSafe provides technical evidence and reporting that supports these elements.

Component	Supported by RunSafe
Item Definition	✓
TARA (Threat Analysis & Risk Assessment)	✓
Cybersecurity Concept	✓
Cybersecurity Requirements & Architecture	✓
Verification & Validation Evidence	✓
Residual Risk & Cybersecurity Case	✓
SBOM & Vulnerability Status	✓
Post-Development Monitoring & Response Plan	✓

WHY RUNSAFE?

RunSafe helps automotive manufacturers and suppliers turn SBOMs into defensible cybersecurity evidence. By identifying vulnerabilities, prioritizing exploitability, and reducing real-world risk, we enable measurable compliance support for ISO 21434 and R155 — strengthening certification readiness and lifecycle assurance across the vehicle ecosystem.

ABOUT RUNSAFE SECURITY, INC.

RunSafe Security proactively protects embedded software for both commercial and defense deployments across critical infrastructure, with comprehensive risk identification, protection, and monitoring, ensuring robust, continuous security without affecting performance. Headquartered in McLean, Virginia, with an office in Huntsville, Alabama, RunSafe Security's customers span the aerospace, defense, energy, industrial, and national security verticals. Learn more at: **RunSafeSecurity.com.**