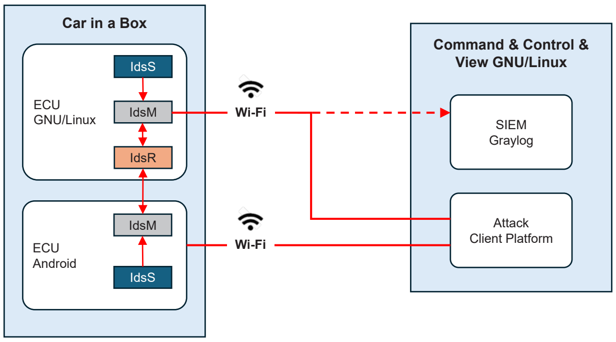
SYSGO Demo Description



Host-based Intrusion Detection Security System (H-IDS) for Software-Defined Vehicles

Our demo shows SYSGO's Host-based Intrusion Detection Security System (H-IDS) — a fully operational Cybersecurity solution designed for modern, connected Automotive architectures. The demonstration illustrates how real-world vehicle networks and ECUs can be monitored, protected, and analyzed in real time to detect and respond to intrusion attempts.

DEMO KEY FEATURES

AUTOSAR IDS compliance: Seamless integration with contemporary Automotive E/E architectures, adhering to the AUTOSAR intrusion detection specification.

QM-qualified: Developed using quality management processes that support robust development and production deployment.

Threat-aware design: Built on insights from AUTO-ISAC threat intelligence and the MITRE ATT&CK framework, covering common attack vectors.

Flexible runtime support: Compatible with Linux and Android Automotive, enabling consolidation of mixed-criticality workloads.

Realistic attack scenarios: Based on a simplified but representative in-vehicle architecture, the demo shows how security events unfold and how the H-IDS detects anomalies.

SIEM integration: Alerts and events are visualized in real time through integration with Graylog, demonstrating actionable incident data aggregation and analysis.

CUSTOMER BENEFITS

Safety & Security

- Compliant with emerging Automotive Cybersecurity standards (e.g., ISO 21434) to support long-term vehicle platform resilience
- Early detection of cyber-attacks at the ECU and application level, enabling fast response and containment
- Protection against common attack vectors, leveraging AUTO-ISAC threat intelligence and the MITRE ATT&CK framework
- Isolation of mixed-criticality workloads, ensuring that Security incidents in non-critical domains cannot compromise Safety-critical functions

Real-Time Monitoring & Diagnostics

- Immediate visibility of abnormal system behavior, enabling predictive maintenance and reduced downtime
- Actionable event correlation across ECUs and domains, supporting faster root-cause analysis
- Demonstrated real-world attack scenarios help OEMs and Tier-1s validate readiness against real threats

Operational Efficiency

- Reduced integration effort thanks to AUTOSAR-aligned interfaces and support for Linux and Android Automotive environments
- Centralized monitoring via SIEM (Graylog) provides engineers and security teams with clear, aggregated insights on events and anomalies
- Lower cost of ownership by enabling a scalable, host-based intrusion detection approach rather than specialized hardware add-ons

Future-Proof Architecture

- Designed for software-defined vehicles, supporting continuous updates and long-term maintainability
- Compatible with evolving E/E vehicle architectures, including high-performance zonal and centralized platforms
- Runs on top of SYSGO's certifiable PikeOS RTOS & Hypervisor platform, enabling a pathway to functional Safety and Security certification where required

Founded in 1991, SYSGO became a trusted advisor for Embedded Operating Systems and is the European leader in hypervisor-based OS technology offering worldwide product life cycle support. We are well positioned to meet customer needs in all industries and offer tailor-made solutions with highest expectations in Safety & Security. More information at → www.sysgo.com/automotive

SYSGO Headquarters
+49 6136 9948 500

SYSGO France
+33 1 30 09 12 70

SYSGO Czech Republic
+420 222 138 111

sales@sysgo.com

www.sysgo.com