Over-the-Air Software and Data Management With Multi-Layer Security

Increasing Cybersecurity Threats

With predictions of over 100 million connected vehicles on the road by 2030, automotive cybersecurity protection is more important than ever. And as connected vehicles evolve and become more advanced—requiring hundreds of millions of lines of software code to operate and power advanced features—the number of cybersecurity threats will continue to grow. A multi-layer, defense-in-depth security approach combined with real-time data collection and the efficient and reliable delivery of over-the-air (OTA) software updates will be essential for automakers to address cybersecurity threats, reduce operational expenses, and deliver new advanced driver assistance systems, vehicle-to-everything, and autonomous driving innovations.

Robust Multi-Layer Cybersecurity Protection

Combining Airbiquity's OTAmatic® OTA software update, data management, and upgradeable edge analytics module features with SafeRide's vSentry™ multi-layer cybersecurity solution provides automakers and automotive suppliers with a robust end-to-end and future-proof cybersecurity system for connected vehicles. When the vSentry anomally detection module running in OTAmatic's data agent detects a vehicle cyberattack an alert is sent to the OTAmatic cloud which then transmits and installs the specified vehicle software update to remedy the vulnerability and restore protection of the vehicle asset and its occupants.

Airbiquity
OTAmatic®

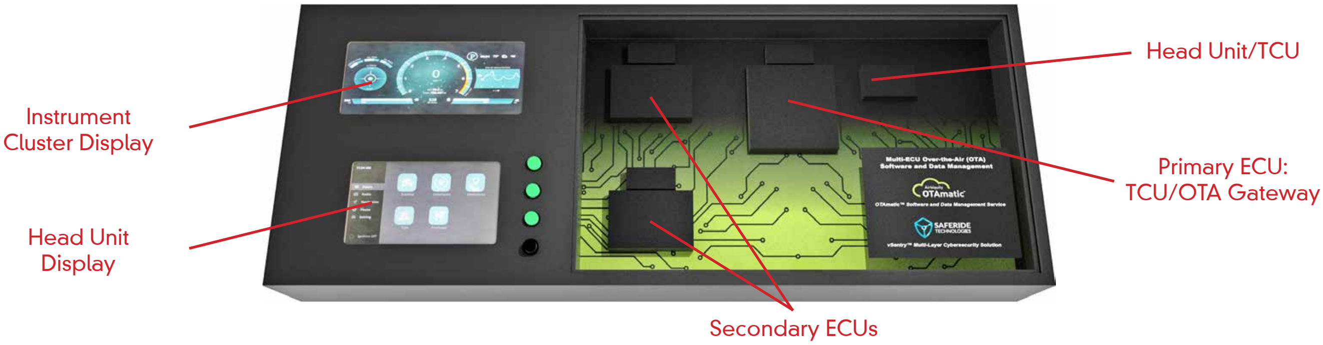
OTAmatic
OTA Software and Data Management

OTAmatic securely orchestrates and automates connected vehicle software update and data management campaigns from the cloud. OTAmatic provides a sophisticated back-end service delivery management capability with highly refined vehicle and device targeting, discrete policy and privacy controls, customizable consumer communications, and solution deployment flexibility. OTAmatic also features an edge analytics framework supporting upgradable data analytics modules and enhanced multi-layer cybersecurity protection via integration of the compromise-resilient Uptane Security Framework.

SAFERIDE
TECHNOLOGIES

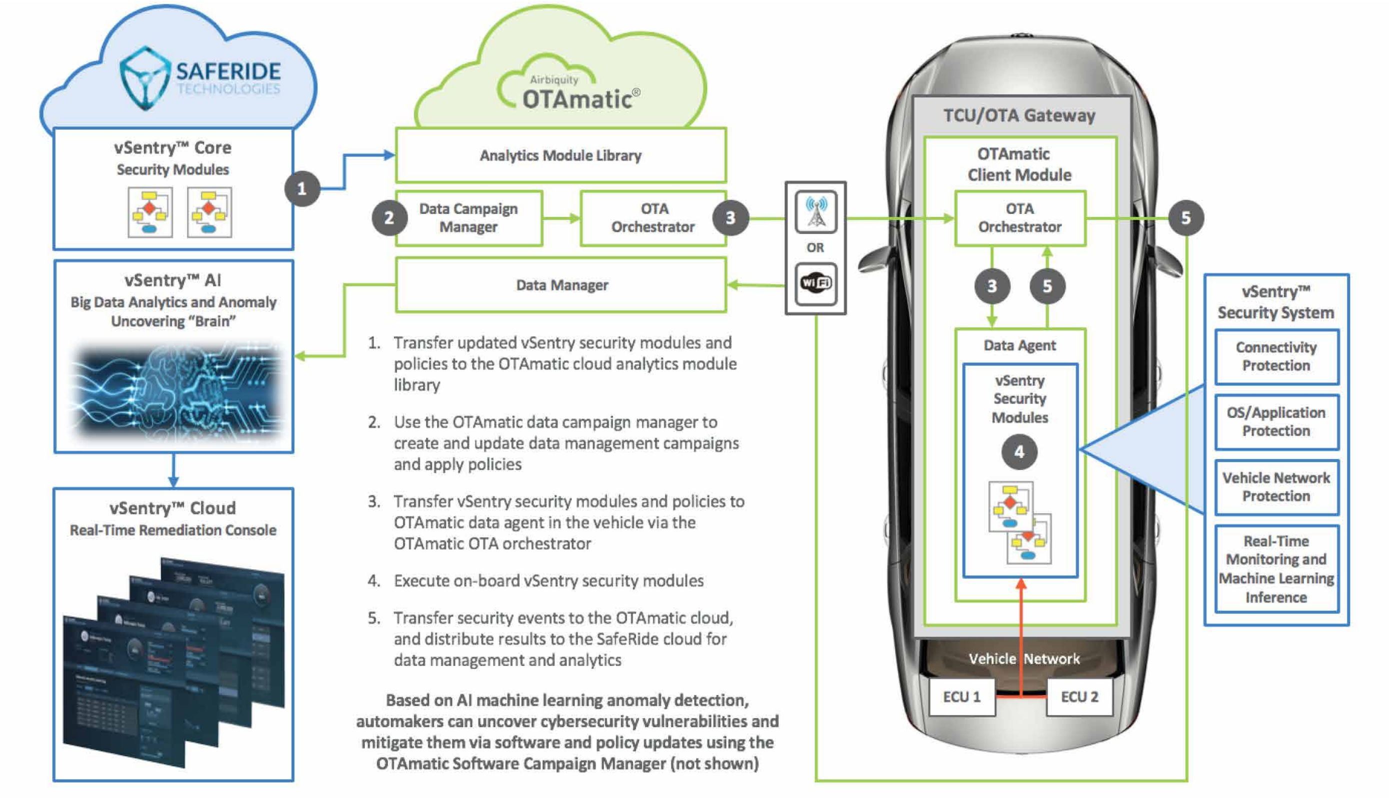
vSentry™
Multi-Layer Cybersecurity Solution

SafeRide Technologies is the provider of vSentry—the industry leading multi-layer cybersecurity solution for connected and autonomous vehicles. vSentry monitors all external communication to the vehicle, in-vehicle network traffic, and ECU software in real-time - and provides a zero false-positive firewall, Intrusion Detection and Prevention System (IDPS), and access control to all resources. SafeRide's vXRay™ advanced AI machine learning and deep learning technology uncovers zero-day vulnerabilities and allows for remediation by updating real-time access control policies over-the-air.


Head Unit/TCU
Instrument Cluster Display
Primary ECU: TCU/OTA Gateway
Head Unit Display
Multi-ECU Over-the-Air (OTA) Software and Data Management
OTAmatic
SAFERIDE TECHNOLOGIES
vSentry™ Multi-Layer Cybersecurity Solution
Secondary ECUs

Airbiquity-SafeRide OTA Software and Data Management with Multi-Layer Security Demonstrator

Airbiquity-SafeRide OTA Software and Data Management with Multi-Layer Security — Functional View —



1. Transfer updated vSentry security modules and policies to the OTAmatic cloud analytics module library
2. Use the OTAmatic data campaign manager to create and update data management campaigns and apply policies
3. Transfer vSentry security modules and policies to OTAmatic data agent in the vehicle via the OTAmatic OTA orchestrator
4. Execute on-board vSentry security modules
5. Transfer security events to the OTAmatic cloud, and distribute results to the SafeRide cloud for data management and analytics

Based on AI machine learning anomaly detection, automakers can uncover cybersecurity vulnerabilities and mitigate them via software and policy updates using the OTAmatic Software Campaign Manager (not shown)

- Single and Multi-ECU Software Updates
  - Unified Diagnostic Services (UDS) Updates for Secondary and Legacy ECUs
- Multiple Software Update Installations
  - Firmware, System, Application, and HMI
- Dynamic and Flexible Data Management Framework
  - Definable Collection: Frequency, Triggers, Logs, DTCs
  - Multiple Bus Support: CAN, Ethernet, MOST, FlexRay
  - Upgradeable In-Vehicle Edge Analytics
  - Data Transfer from Car to Cloud to Analytic Resources
- Advanced OTA Software Update Orchestration
  - Pre-Conditions, Priorities, and Dependencies
  - Fault and Error Detection, Recovery and Rollback
- Campaign Specific Consumer Notifications
  - In-Vehicle Displays and Smartphone Application HMI
- Back-End Service Management Portal
  - Step-by-Step Campaign Configuration Process
- Real-Time In-Vehicle Software Protection
  - IDPS Protects Memory and Peripherals and Ensures System Integrity
  - Protects Kernel, Applications, and Secures Initialization
  - Prevents Reverse Engineering and Debugging
  - Prevents Malicious Code Execution
- External and Internal Network Protection
  - Firewall Enforces Perimeter Access Control
  - Firewall Enforces CAN Bus Access Control
  - IDPS Detects and Prevents Infiltration and Data Exfiltration
- Defense In-Depth Security Approach
  - Standards-Based Certification, Authentication, and Encryption: PKI, PSK, TLS 1.2
  - Compromise-Resilient Uptane Security Framework
- Comprehensive Campaign Reporting
  - Summary and Campaign Specific Results
  - Analytics Module Performance Metrics

For Additional Information

Airbiquity

Email sales@airbiquity.com

SAFERIDE TECHNOLOGIES

www.saferide.io