Safety and security in automotive platforms with Red Hat & VicOne

VicOne's xCarbon lightweight, modularized, and configurable software-based intrusion detection or prevention system (IDS/IPS), pre-integrated on the safety-certified Red Hat In-Vehicle OS, work together to deliver a reference architecture that accelerates secure-by-design initiatives, compliance with cybersecurity standards, and enhances functional safety in SDV platforms.

Meeting the connected vehicle cybersecurity challenges

Automotive systems are evolving toward high-performance computing platforms. With competitive demands influencing the need for continuous innovation, features-on-demand, and modern automation—as well as interaction with the factory and the external world outside the connected vehicle—there is a heightened awareness for safety and cybersecurity protections. Software updates, delivered through over-the-air (OTA) network connections, must be safeguarded. There is also a greater need for the detection of, and protection from security threats within the operating system (OS) running the applications.

The automotive industry recognizes the imperative need to operate more efficiently, with greater resource management and cost effectiveness. This consideration involves taking advantage of modern, open technologies, and using the benefits of the local community and the broader ecosystem. It also means embracing open standards, open collaboration, adopting DevOps methodologies, and cloud-native technologies that allow the rapid, continuous innovation required for software-defined vehicles (SDVs).

A pre-integrated, safety-rich, and joint solution from Red Hat and VicOne

As automobile manufacturers speed up the delivery of modern vehicles featuring always-on network connectivity, it is imperative to protect the vehicles and their occupants from cybersecurity threats. And functional safety becomes even more critical as more advanced driver assistance systems (ADAS) capabilities are added. Red Hat and VicOne have partnered to craft an efficient, blueprint platform solution for OEM adoption in modern SDVs.

The combined, high performance solution additionally provides tremendous value to original equipment manufacturers (OEMs) and their Tier 1 suppliers:

- Red Hat provides a Linux-based in-vehicle OS with efficient resource use, mixed-criticality workload handling, and integration with modern DevOps development approaches and cloud-native toolchains.
- VicOne provides the xCarbon intrusion detection or prevention system, which delivers enhanced runtime security to better address cyber threats before they can propagate across networks, vehicle-to-X interfaces or cloud services. The integration of Red Hat In-Vehicle OS with xCarbon with Red Hat In-Vehicle OS can help OEMs and Tier 1s accelerate regulatory compliance as the attack surface grows in SDVs and connected cars.

Red Hat automotive solutions

Red Hat In-Vehicle Operating System (OS) and hybrid cloud platform portfolio offer automotive developers modern software solutions that provide reliable, predictable behavior for safety-critical systems, even under high load conditions, crucial for ISO 26262 compliance. Red Hat In-Vehicle OS has achieved functional safety certification, to level ASIL B of the ISO 26262 automotive standard,

as a Safety Element Out of Context (SEooC), ensuring safety and reusability throughout OEM production series and across models. Importantly, safety recertification is integrated into the OS development and validation process for maximum agility.

Red Hat has achieved this certification through an innovative container-based solution that ensures Freedom From Interference (FFI) for safety applications by isolating quality management (QM) applications and their resource requirements in a QM partition. While virtual machine (VM) isolation is also supported, this container-based approach provides efficient resource use and greater flexibility and serviceability in deployed applications.

In addition to these benefits, Red Hat In-Vehicle OS delivers real-time responsiveness, with the PREEMPT_RT support enabled by default, long-term lifecycle support, standard Linux security mechanisms along with regular security patches, and over-the-air (OTA) updates support with A/B and rollback for continuous innovation and serviceability.

VicOne's xCarbon cybersecurity solution

VicOne's xCarbon helps secure the over-the-air (OTA) software updates to automotive systems, improves protections for containerized workloads in SDVs and enables lifecycle cybersecurity with minimal performance overhead in terms of central processing unit (CPU) and memory usage. xCarbon is a lightweight, modularized, and configurable software-based intrusion detection or prevention system (IDS/IPS), proven at running on resource-constrained electronic control units (ECUs). The VicOne solution empowers OEMs and Tier 1 suppliers by enabling specific detection functions to meet E/E architecture needs, and it frictionlessly fits into various types of hardware, ranging from low-end microcontroller units (MCUs) to high-end high-performance computers (HPCs).

xCarbon allows OEMs to bring vehicle security operations center (VSOC) capabilities into vehicles by using edge AI, enhancing threat detection coverage from a single ECU to the entire vehicle. By sending only critical security events to a public cloud environment, users may see a significant reduction in data transfer and cloud processing costs. xCarbon also allows OEM and suppliers to comply with the ISO/SAE 21434 clause 13 13.3 requirements for cybersecurity incident response.

Pre-integrated solution to safeguard containers

The blueprint is depicted in the diagram. VicOne and Red Hat illustrate how container application lockdown prevents unauthorized or malicious program execution, while adaptive container escape detection continuously monitors abnormal behavior, learns from escape attempts, and applies expert rules to block similar threats.

Lockdown of applications: Reduces security risks in containerized environments by limiting privileges, ensuring image integrity, isolating networks, controlling resources, and monitoring activities to stop unauthorized or malicious programs.

Adaptive container escape detection: Counters escape attempts through continuous monitoring, identifying unusual attacker patterns, extracting attack signatures, and applying expert rules to prevent similar threats.

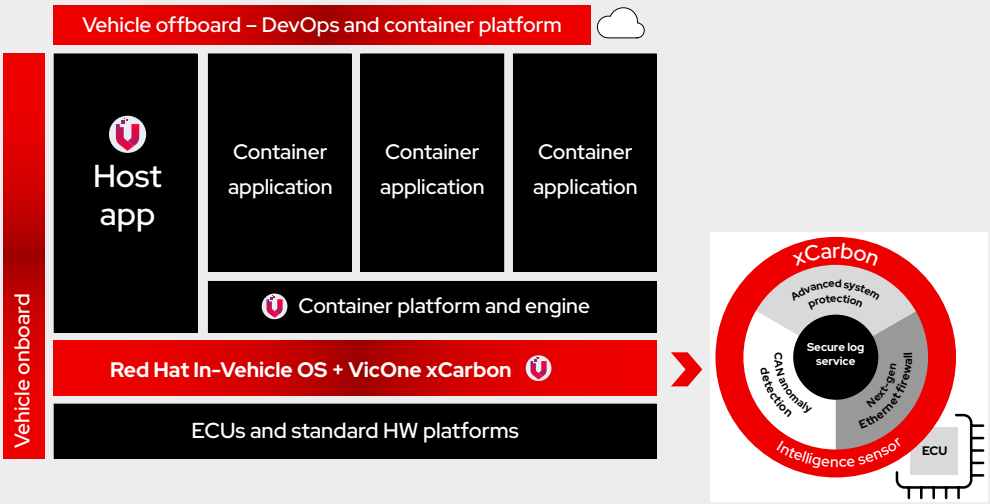

Figure 1. Proactive runtime security for Linux-based SDVs with VicOne xCarbon and Red Hat In-Vehicle OS

Discover the pre-integration stack advantage

Manufacturers must embrace open source, open collaboration and continuous innovation to accelerate the SDV transformation. It is paramount to protect OTA updates, and detect and prevent security attacks, while ensuring functional safety. By combining VicOne's cybersecurity expertise, pre-integrated on the safety-certified Red Hat In-Vehicle OS, automotive manufacturers get to production sooner, with lower risk, while meeting the safety and security requirements end customers rely on.

Learn more

Red Hat automotive solutions

VicOne automotive solutions

About Red Hat

Red Hat helps customers standardize across environments, develop cloud-native applications, and integrate, automate, secure, and manage complex environments with award-winning support, training, and consulting services.

facebook.com/redhatinc
@RedHat
linkedin.com/company/red-hat

North America
1 888 REDHAT1
www.redhat.com

Europe, Middle East, and Africa
00800 7334 2835
europe@redhat.com

Asia Pacific
+65 6490 4200
apac@redhat.com

Latin America
+54 11 4329 7300
info-latam@redhat.com

redhat.com
#2876406_1025