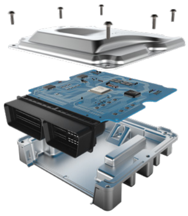
GUARDKNOX **SECURE NETWORK ORCHESTRATOR™ (SNO)** SOLUTION



HIGHLIGHTS

- Comprehensive robust automotive cybersecurity solution as the platform for safety and OTA updates
- Centralized and internal protection for multiple networks
- High performance, flexible and scalable protection available for design per OEM's/Tier 1s specifications
- Patented Communication Lockdown™ methodology for multi-layer protection against all types of known and unknown cyber attacks
- Patented Service Oriented Architecture (SOA) for access control and service level partitioning to secure further levels of connectivity & customization
- Cybersecurity as the foundational layer for added levels of connectivity, services, personalization and new revenue streams for OEMs

A COMPREHENSIVE VEHICLE CYBERSECURITY SOLUTION: THE FOUNDATION FOR CONNECTIVITY AND CUSTOMIZATION

As vehicle complexity and connectivity requirements increase, the need for post-production scalability and extensibility is rising. Furthermore, a secured end-point within the vehicle becomes increasingly vital to the automotive value chain as well

GuardKnox's Secure Network Orchestrator™ (SNO) product lines offers comprehensive vehicle cybersecurity protection against any type of known and unknown cyberattack. With a full software stack and hardware architecture, GuardKnox's patented technologies adhere to the most stringent security (ISO 15408) and safety (ISO 26262) standards. SNO™ solutions comply with GDPR.

VEHICLE-WIDE PROTECTION

GuardKnox's Internal SNO™ functions as a Central Gateway or Domain Controller and provides a secure endpoint for high performance data processing and storage which also supports secure cloud communication, data AI and analytics. The Internal SNO™ has a flexible configuration and enough spare resources (computing power, internal memory, external I/O interfaces) to support additional levels of connectivity, such as personalized application downloads, provided by OEMs and Tiers 1s.

The Internal SNO™ is a high-performance secure ECU that provides high assurance defense for all vehicle networks, enabling strong separation and lockdown of all communication traffic. Additionally, it is also possible to integrate the Internal SNO™ as a software stack and security core that is integrated into specific existing vehicle hardware, chosen by OEMs during production.

The Internal SNO™ Controller is completely autonomous, has high-performance data processing capabilities, does not require external connectivity, constant communication, cloud connectivity, or any on-going updates. The GuardKnox SNO™ eliminates the need for human intervention in the security mitigation process, and can defend against any kind of known or unknown cyber-attacks.

The Internal SNO™ scrutinizes all communication of all vehicle ECUs in real-time on a bit level from a central location. It is provided to OEMs as a complete software and hardware unit. As a complete unit (during production or retrofitted in the aftermarket), it integrates seamlessly into the vehicle, value chain and vehicle production process.

Component	Description
Processor	Dual ARMv7 Cortex-A9 32-bit microprocessor with built-in FPGA Or Quad ARMv8 Cortex-A53 64-bit microprocessor with built-in Dual ARMv7 Lockstep Cortex-R5 realtime safety microcontroller and built-in FPGA
Memory (RAM)	Up to 64GB
Storage (Flash)	Up to 256 GB SSD
Ports	Up to 10 x CAN 2.0B (up to 1 Mbps) Up to 10 x CAN-FD (up to 8 Mbps) Up to 15 x Ethernet 100 Mbps or Gigabit Ethernet Up to 10 x LIN interfaces
Data-at-Rest Encryption	AES128, AES256
Symmetric Encryption Support	AES128, AES256
Asymmetric Encryption	RSA (up to 4096 bit key), ECC (up to 256 bit key)
Cryptographic Signature	HMAC
Cryptographic Hash	SHA1, SHA2, SHA256
Encrypted Communication	TLS, SSL, DTLS
Wireless Communication	Bluetooth up to BLE 5 Cellular (2G, 3G, 4G) Wi-Fi (802.11g) and DSRC
Updates	Secure OTA Secure Boot
Standards Compliance	ISO 15408 certifiable up to EAL5 ISO 26262 certifiable up to ASIL D
Use Cases	Domain Controller Application Host – Domain Controller High-Speed Central Gateway Advanced Body Control Module
Third-Party Support & Integration (Optional)	DXC Technology (Security Operation Center & fleet management) Palo Alto Networks GlobalProtect™ Cloud Service (OTA updates) Custom integration (upon request)
Ability to provide a complete hardware and software design	Yes

FLEXIBLE, SCALABLE FUTURE-PROOF PROTECTION

The GuardKnox Internal SNO™ cybersecurity solution has a flexible configuration built around a multi-core CPU and an FPGA module with extensive embedded capabilities. The solution's flexible configuration enables OEMs to incorporate only the required GuardKnox security functionality into their vehicle design, such as a specific number and type of vehicular bus interfaces or specific types of encryption engines, etc. If additional security capabilities are required at a later date, such as additional bus interfaces, interface types, or additional types of encryption capabilities, etc., the OEM can activate the spare capacity in the existing FPGA of the Secure Network Orchestrator™ device without changing the footprint of the SNO™ or the BOM of the vehicle, resulting in extensive cost reductions.

PATENTED COMMUNICATION LOCKDOWN™ METHODOLOGY

GuardKnox's patented three-layer Communication Lockdown™ architecture enforces an ongoing, formally verified, and deterministic configuration of communication among the multiple bus networks embedded in the vehicle. The methodology enables a multi-platform and multi-service approach with the ability to host multiple operating systems and services on one ECU with secure separation and full permission control.

The three layers of the Communication Lockdown™ methodology are:

Routing Layer

Verifies that the message has arrived from a legal source

▶ Content Layer

Verifies that the content of the message, down to the bit level, is legal

▶ Contextual Layer

Verifies the message is legitimate in the specifically functional state of the vehicle (state machine)

PATENTED SERVICES-ORIENTED ARCHITECTURE (SOA)

SOA has a secure separation (both hardware and software) between all resources, application groups, and operating systems, simplifying edge computing capabilities by providing ample processing resources with maximal flexibility both in interface support and provision for future software extensions/additional service being added. SOA patented technology creates the secure environment which enables added services and applications by hosting downloads or upgrades on the SNO™ platform throughout the lifecycle of the vehicle. This enables mission critical and non-mission critical applications to run simultaneously without interference; if one application should be compromised, all others will not be affected. This in essence converts the driver of a vehicle to a subscriber of features and functions of the connected and/or autonomous vehicle.