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

HIGHLIGHTS

- Comprehensive robust automotive cybersecurity solution as the platform for safety and OTA updates
- Localized and external protection for a single network (ECU)
- 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 and provide holistic automotive cybersecurity that easily fits the automotive tiered value chain while alleviating the difficulties of software only integration.

LOCALIZED, SINGLE INTERFACE (ECU) PROTECTION

GuardKnox's External SNO™ secures a single ECU with external connectivity and functions as a local domain controller. The External-Local 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 GuardKnox External SNO™ can be connected to any single ECU with external connectivity while simultaneously providing extensive connectivity protection.

Ideal for telematics, infotainment, OBD, fleet management systems and other externally connected ECUs, it is integrated during production of the ECU or is installed or retrofitted by Tier 1s as an extension between the ECU and the rest of the vehicle

The External SNO™ 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 is provided to OEMs and Tier 1s as a complete software and hardware unit.

EXTERNAL SNO™ CONTROLLER SPECIFICATIONS

Component	Description
Processor	ARMv7 Cortex-M4 32-bit microcontroller
Memory (RAM)	Typically up to 256 KB
Storage (Flash)	Typically up to 1MB
Ports	Up to 1 x CAN 2.0B (up to 1 Mbps) Up to 1 x CAN-FD (up to 8 Mbps) Up to 1 x Ethernet 100 Mbps or Gigabit Ethernet Up to 1 x LIN interface
CAN 2.0B (up to 1 Mbps)	Typically up to two interfaces per module
CAN-FD (up to 8 Mbps)	
Ethernet 100Mbps	
Other capabilities	LIN
Secure Boot	Encrypted and signed image
Data-at-Rest Encryption	AES128, AES256
Symmetric encryption support	AES128, AES256
Asymmetric encryption	RSA (up to 4096bit key size), ECC (up to 256bit)
Cryptographic signature	HMAC
Cryptographic Hash	SHA1, SHA2, SHA256
Support for encrypted communication over TLS, SSL, DTLS	Yes
Ability to provide a complete hardware and software design	Yes

FLEXIBLE, SCALABLE FUTURE-PROOF PROTECTION

The GuardKnox External 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.