

GUARDKNOX SECURE NETWORK ORCHESTRATOR™ (SNO) SOLUTION



- Comprehensive robust automotive cybersecurity solutions as the platform for added connectivity, safety, services, OTA updates and vehicle customization
- Centralized and internal protection for multiple networks (ECUs)
- High performance, flexible, scalable, future-proof protection designed for integration by OEMs and aftermarket providers
- Patented Communication Lockdown™ methodology for multi-layer protection against all types of known and unknown cyber attacks
- Patented Service Oriented Architecture (SOA) - allows unified communication as well as access control and service level partitioning to secure further levels of connectivity, customization, and additional revenue streams across the automotive value chain
- Ability and flexibility to provide complete solution (including all HW/SW requirements) design per OEM's and/or Tier 1's specification – including secure EV ECUs

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



The Internal-Central SNO™ Gateway/Domain Controller locks down all ECUs and inter-network communication.

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 (General Data Protection Regulation) and provide holistic automotive cybersecurity that easily fits the automotive tiered value chain while alleviating the difficulties of software only integration.

The GuardKnox Internal-Central SNO™ Gateway/Domain Controller is the only solution that adjusts to end-users wants and needs as they evolve over the vehicle life span.

VEHICLE-WIDE AND LOCALIZED, SINGLE INTERFACE (ECU) PROTECTION

GuardKnox's unique value proposition brings solutions to the automotive industry that provide a secure endpoint for high performance data processing and storage which also support secure cloud communication, data AI and analytics.

GuardKnox's Internal-Central SNO™ is implemented through the Gateway/Domain Controller during production, or retrofitted in the aftermarket, allowing the automotive industry to add robust security in a cost-effective manner. The Internal-Central 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 – supporting end-users trends of increased data consumption.



GuardKnox's Internal-Central SNO™ is a high-performance secure ECU that provides high assurance defense for vehicle networks, enabling strong separation and lockdown of all communication traffic. The Internal-Central SNO™ Gateway/Domain Controller 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 hardware and software unit. As a complete unit, it integrates seamlessly into the vehicle, value chain and vehicle production process. Additionally, it is also possible to integrate the Internal-Central SNO™ as a software stack and security core that is integrated into specific existing vehicle hardware, chosen by OEMs during production.

FLEXIBLE, SCALABLE FUTURE-PROOF PROTECTION

The GuardKnox Internal-Central 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™ ARCHITECTURE

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.

This approach allows unified communications as well as customizable access control and service level partitioning for all internal and external vehicle communications.

The three layers of Communication Lockdown™ architecture are:

Routing Layer

The routing layer creates a physical separation between different networks using the FPGA and enables the GuardKnox SNO™ to differentiate messages by their origin. For example, if a message from the ECU of the right mirror tries to go to the ECU of power train, it will be discarded and reported.

Content Layer

The content layer is used to lock all bits in each field of all messages for the entire vehicle. GuardKnox uses the CAN dB file as a source map for the bit in each message and populates open fields or bits with values that are agreed upon with the OEM. If a hacker has changed one bit in the content layer, the message will be discarded and reported.

Contextual Layer

The content layer is used to create a state machine topped by a configuration file (a communication schema) that is build out of the two documents mentioned above. This state machine compares and enforce the real performance of the vehicle in the real world to what the network is doing or thinks it is doing.

PATENTED SERVICES-ORIENTED ARCHITECTURE (SOA)

GuardKnox's patented Service Oriented Architecture enables additional levels of connectivity and customization through access control and service level partitioning to maintain vehicle integrity while increasing end user personalization. GuardKnox's already patented Communication Lockdown™ 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. 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.

GuardKnox 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.

GuardKnox sees cybersecurity as the foundational layer for added levels of connectivity and personalization in connected and autonomous vehicles: enabling not only increased revenue streams per initial vehicle sale but also the end-user customization of the vehicle necessary to meet changing individual needs in a cost-effective manner.

The GuardKnox Internal-Central SNO™ Gateway/Domain Controller is completely autonomous, have high-performance data processing capabilities, do 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.

CENTRAL-INTERNAL SNO™ GATEWAY/DOMAIN CONTROLLER SPECIFICATIONS

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	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

Though every care has been taken to ensure the accuracy of this document, GuardKnox Cyber Technologies Ltd. cannot accept responsibility for any errors or omissions or for any loss occasioned to any person, whether legal or natural, from acting, or refraining from action, as a result of the information contained herein. Information in this document is subject to change at any time without obligation to notify any person of such changes.

GuardKnox Cyber Technologies Ltd. may have patents or patent pending applications, trademarks copyrights or other intellectual property rights covering subject matter in this document. The furnishing of this document does not give the recipient or reader any license to these patents, trademarks copyrights or other intellectual property rights.

No part of this document may be communicated, distributed, reproduced or transmitted in any form or by any means, electronic or mechanical or otherwise, for any purpose, without the prior written permission of GuardKnox Cyber Technologies Ltd.

The document is subject to revision without further notice.

All brand names and product names mentioned in this document are trademarks or registered trademarks of their respective owners.