GUARDKNOX CAPABILITIES AND SERVICES

CAPABILITIES

- **Gateways and Domain Controllers:** Vehicle network backbone. Connecting, segregating and orchestrating all cross-domain communications
- **Body Control Module:** Central hub for all body functionality and user input that effect vehicle interior. May also act as localized gateway
- **Telematics and IVI:** Domain controller platform that control various user interactive displays and HMI. Optimized to support graphical processing, AI and multiple operating systems running together.
- **EV Charging Gateway:** Secure endpoint for high performance data processing and storage while also supporting secure cloud communication, data analytics and AI. Enables compliance to ISO 15118 and DIN SPEC
- **Series Production ECUs**: Including prototype development and production until B-Sample
- **Application Hosting Domain Controller**

GUARDKNOX

GuardKnox provides optimized and cybersecure high-performance computing platforms to not only ensure security and safety, but serve as the foundational layer for added services, personalization and revenue generating opportunities.

GuardKnox offers a full hardware and software cybersecurity solution. GuardKnox's expertise and inherent flexibility facilitates a variety of implementations including software only (integrated into existing hardware) or built-to-spec.

CYBERSECURITY HOUSED WITHIN SOFTWARE ARCHITECTURE

LOCKDOWN SECURITY CORE

GuardKnox's patented Communication Lockdown™ Methodology is a formal, verifiable and certifiable security methodology that verifies all communication according to strict state machine-based model built by GuardKnox from CANDBs and function specification documents which are readily available from OEMs. The methodology verifies all data and communications on three layers (routing, content and context), including locking down any open fields or bits. The model can be certified for safety up to ASIL D and can adhere and comply to ISO26262, ISO15408 and GDPR.

EXPERT SERVICES

Engineering & Designing Next-Gen E/E Architecture

- **Hardware Engineering and Design:** High-performance, cybersecure and optimized architecture design. Full system cybersecurity.
- **Software Engineering and Design:** Hypervisor designed complete and customized software stack. Software architecture is designed to isolate security and safety critical systems.
- **Security Analysis and Consulting**
- **Pen-testing**

www.guardknox.com | info@guardknox.com | 2 Hahazon St. PO Box 320, Ramla, Israel 7210202

GUARDKNOX CAPABILITIES AND SERVICES

SERVICES-ORIENTED ARCHITECTURE (SOA)

SOA enables GuardKnox's patented architecture to allow unified communication as well as access control and service level portioning. SOA allows for multiple partitions hosting independent services and service/application managers with access control both on application/service level as well as on the hardware level. The unified communication infrastructure allows for distributed unified communication (CORBA model) with centralized policy over different hardware interfaces.

SOA utilizes a separation kernel for abstraction and concealment of communications across platforms – allowing for simplified and transparent interfaces to service providers. SOA also enables strong separation between services and applications on the virtual level as well as employing separation kernels. Additional capabilities include but are not limited to: separation via hypervisor, several computing zones, virtual ethernet, virtual CAN, network management, virtual ECUs, AUTOSAR classic and much more.

CYBERSECURITY HOUSED WITHIN HARDWARE ARCHITECTURE

Using programmable logic (FPGA), full hardware level separation is achieved between all physical interfaces. This leads to a dedicated communication path for each prior to reaching any software. Initial verification of data can be implemented in hardware.

Only after verifying hardware can data be passed to the software stack running on the CPU, providing an efficient and high-performance infrastructure for hardware level security analysis for communication. By providing hardware level separation, attacks can't spread and ensure that no one vulnerability is used as a stepping stone to penetrate safety-critical systems.

The use of an FPGA enables hardware and software adaptations for future requirements. Changes are implemented in the FPGA and do not require additional software, hardware or ECUs. A flexible and scalable hardware architecture enables consolidation of E/E architecture and an ethernet backbone based real-time communication and network management.

PATENTS

Patent 1- 9,899,563B2: GuardKnox Communication Lockdown Methodology and its implementation within a vehicle

Patent 2- 10,009,350BS: GuardKnox secure hardware architecture and the physical separation between vehicle networks, including Lockdown implementation in hardware

Patent 3 – 10,055,260B2: Service-Oriented Architecture (SOA) for vehicle ECUs, including Secure SOA and efficient implantation of in-vehicle SOA

Patent 4 – #10129259B2: Distributed Lockdown architecture within a vehicle, enabling multiple Lockdown devices to work together for improved security

Patent 5- # 10,191,777B2: Distributed SOA to enable services not solely related to a single ECU within a vehicle. Include services involving external parties and