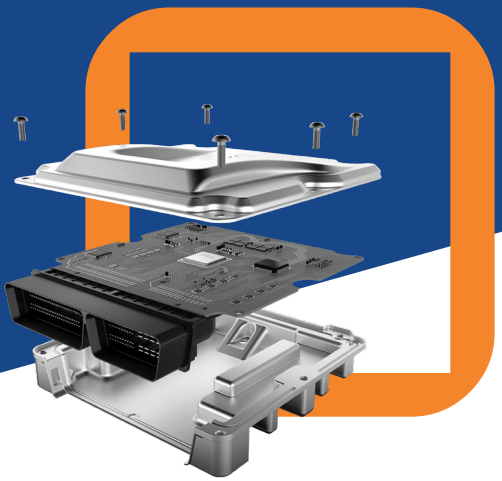
GUARDKNOX

GUARDKNOX
ZONAL E/E ARCHITECTURE

HIGHLIGHTS

- High-performance, flexible and scalable platforms available for design per OEM/Tier1 specifications
- Innovative hardware and software security by design architecture utilizing defense in depth ensuring high cybersecurity assurance for all layers and components
- Greater connectivity and versatile computing resources for current and next-gen vehicles.
- Customizable hardware – single platform fits many use case
- Post deployment hardware configuration – Hardware-OTA (HOTA)
- Patented Service-Oriented Architecture (SOA) for rapid application deployment, real-time customization, access control and service level partitioning
- Robust automotive cybersecurity solution as the platform for safety, security and over-the-air (OTA) updates



GuardKnox's solutions empower the auto industry with the **FREEDOM TO EVOLVE** to meet the challenges of rapid change and capability deployment

A COMPREHENSIVE VEHICLE SOLUTION: FROM AVIATION TO AUTOMOTIVE

GuardKnox's expertise started over two decades ago in defense aviation and secure avionics. The GuardKnox team brings invaluable expert knowledge in hardware and software-based automotive computing solutions for current and next generation vehicles.

GuardKnox is navigating and easing the steep learning curve for the development of cutting-edge platforms and vehicle architecture designs for the automotive industry and the greater automotive ecosystem.

As the world's first Cybertech Tier supplier, GuardKnox is providing optimized and high-performance cybersecure computing platforms and engineering services. The inherent flexibility enables a wide array of implementations from full hardware and software solutions to software only (integrated into existing hardware) or built-to-spec.

GUARDKNOX

GUARDKNOX DEMO AND USE CASES

DESIGNED WITH THE FUTURE IN MIND

GuardKnox's Platform functions as a Domain Controller or as a high-performance computing platform ECU, which provides a secure endpoint for data processing and storage and also supports secure cloud communication.

Safety and non-safety critical services and applications are hosted on a single system-on-chip (SoC) with secure separation, partitioning, and access control. This ensures that no vulnerability can be used as a stepping stone to penetrate safety critical systems.

Partitions provide the capability to run multiple operating systems in parallel, while supporting real-time OTA updating of all services and micro-services running on the platform. This creates the ability to implement a modular design, where each application/service can be tested and integrated independently of the others and the core system.

The Platform can utilize power efficient programmable logic (FPGA) and adaptable hardware to provide a variety of different computing resources which are adapted to optimize and accelerate many types of software application running in parallel, while ensuring acceleration adapts as applications change during the life cycle.

ZONAL GATEWAY ON A CHIP

- Single chip SoC which can act as a full zonal gateway
- Integrates into existing ECU - no need for extra zonal gateway
- Hardware level routing and acceleration
- Supports all interface types and OTA configuration on a hardware level (HOTA)

VEHICLE SERVER

- Modular through discrete elements or clustered devices
- Consolidation of critical and non-critical applications
- OTA capability for applications, operating systems (VM) and hardware configuration
- Asymmetric resource allocation & access (SOA or bus)
- Scaling up through clustering multiple computing elements running the same software stack
- Many options for modules connectivity (AXI, PCIe, Ethernet, Switched Ethernet, CAN-FD etc.)
- Agnostic to network topology

SOA IVI DOMAIN CONTROLLER

- Modular application deployment & integration. No need to recompile, integrate, or test entire software image
- Support for full services (partitions, processes) or micro services (containers)
- OTA on all services/software modules
- Vehicle App-store support
- Secure separation between safety and security critical domains from others through isolation and sandboxing

MODULAR ETHERNET BACKBONE

- Modular network through "plug & play" ECUs and sub-systems
- Decoupling of physical hardware from functionality (single firmware for any network configuration)
- Network and functionality disruption resilience
- High speed and high-performance scalable up to 100 Gbps
- Physical medium agnostic (copper or fiber)
- Automatic service discovery between all connected devices