GUARDKNOX DOMAIN CONTROLLER SOLUTION PLATFORM

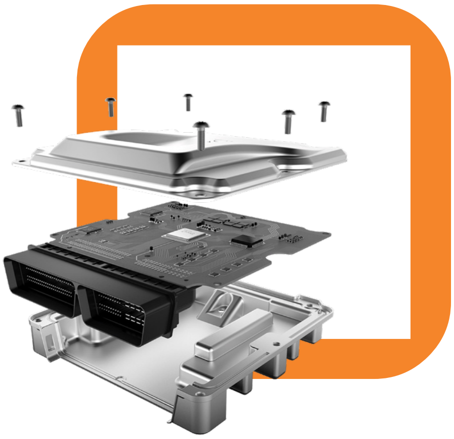
HIGHLIGHTS

- Uniform hardware and software ECU platform for Domain Controller architectures and multi Domain Controller ECUs
- Mixed criticality (up to ASIL D) and mixed security partitioning on a single chip, supporting domain applications with a wide spectrum of requirements
- Engineered to answer a wide range of domain-specific computing requirements and pain points
- Efficiently adapted to provide a solution for telematics domain controllers and ADAS domain controllers up to L2+
- Coupled with patented Secure Service Oriented Architecture (SOA) stack for access control and service level partitioning to secure further levels of connectivity & customization
- Unique hardware approach

A HIGH-PERFORMANCE VEHICLE PLATFORM: 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.

GuardKnox's Domain Controller Platform is designed to provide a uniform hardware and software ECU platform for Domain Controller E/E architectures. The platform can function as Gateway Domain Controller, Cockpit Domain Controller, or Body Domain Controller that provides a secure endpoint for data processing and storage , supports secure cloud communication, data AI and analytics.



The GuardKnox Domain Controller Platform 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 or 3rd party app stores, provided by OEMs and Tiers 1s.

The Domain Controller Platform is a high assurance ECU for E/E vehicle networks, enabling strong domain separation and Communication Lockdown™ of network traffic. It is also possible to integrate the software stack of the Domain Controller Platform into existing vehicle hardware, chosen by the customer or by the OEM during production.

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

The GuardKnox 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 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.

FREEDOM TO EVOLVE

Component	Description
Processor	Quad Core ARMv8 Cortex-A53 64-bit microprocessor with built-in Dual ARMv7 Lockstep Cortex-R5 realtime safety microcontroller and built-in FPGA Or Quad Core ARMv8 Cortex-A53 64-bit microprocessor with built-in triple ARMv7 Lockstep Cortex-M7 realtime safety microcontroller
Memory (RAM)	Up to 64GB
Storage (Flash)	Up to 256 GB
Interfaces	Up to 16 x CAN-FD Up to 14 x Ethernet Up to 20 x LIN
Symmetric Encryption Support	AES128, AES256
Asymmetric Encryption	RSA (up to 4096 bit key), ECC (up to 256 bit key)
Cryptographic Signature	HMAC, CMAC
Cryptographic Hash	SHA1, SHA2, SHA256
Encrypted Communication	TLS, DTLS
Wireless Communication	Bluetooth Cellular Wi-Fi
Updates	Secure OTA Secure Boot
Standards Compliance	Upcoming ISO 21434 certifiable ISO 26262 certifiable up to ASIL D
Use Cases	Gateway Domain Controller Cockpit Domain Controller Body / Comfort Domain Controller High-Speed Application Central Gateway
Third-Party Support & Integration (Optional)	DXC Technology (Security Operation Center & fleet management) Palo Alto Networks GlobalProtect™ Cloud Service (OTA updates) Custom integration (upon request)

FLEXIBLE, SCALABLE FUTURE-PROOF

The Domain Controller Platform consolidates an application domain, real-time domain, and extensive set of interfaces onto a single SoC. The solution's flexible configuration enables OEMs to incorporate only the required GuardKnox 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 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 (if applicable) of the Platform without changing the footprint 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 chip 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 Platform throughout the lifecycle of the vehicle. The mixed criticality environment 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.