GUARDKNOX SECURE SOA FRAMEWORK

INTRO

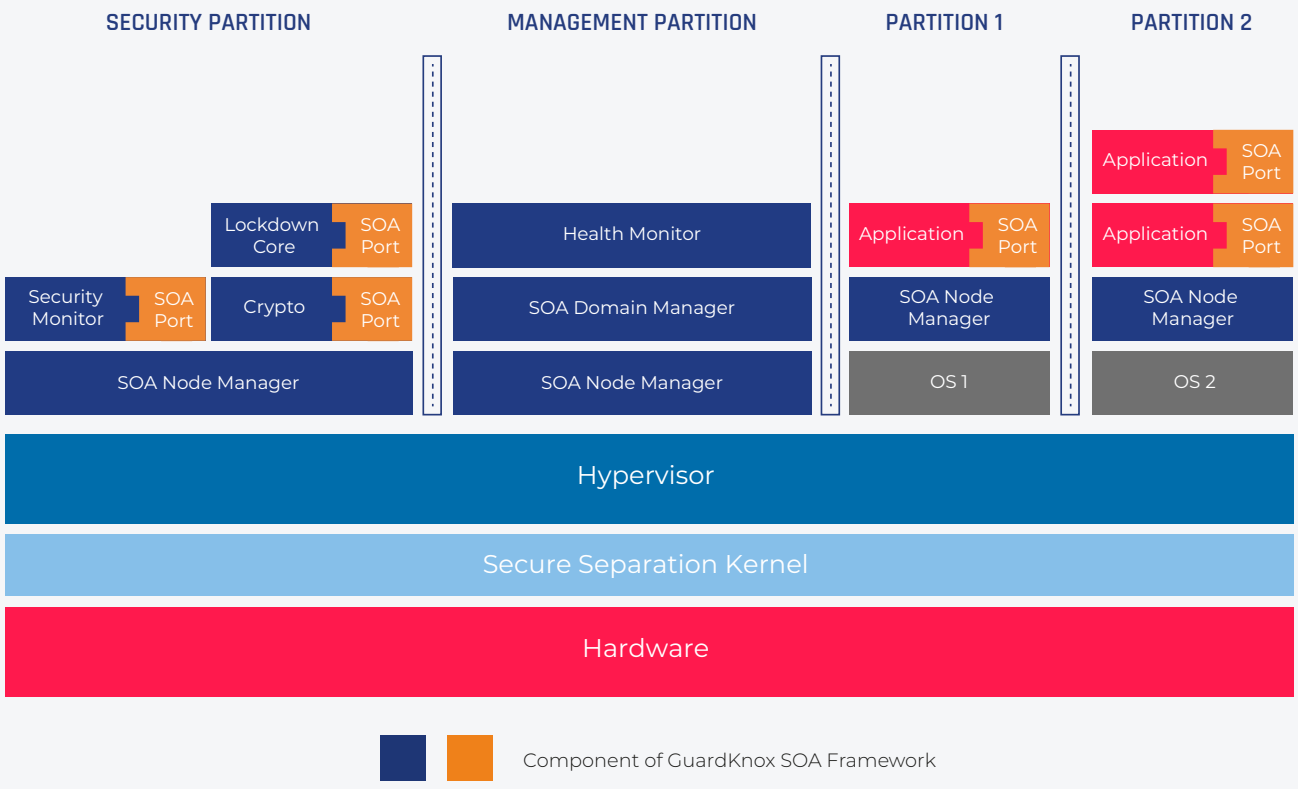
The development, deployment, testing, and maintenance of software in today's automotive industry is inflexible and unnecessarily demanding. Vehicle SW is built from monolithic blocks of code structured to define each and every function in the car as a self-contained service. This means for every change, minor or major, extensive testing is required resulting in a 3-6 month wait to deploy updates.

GuardKnox's Secure SOA Framework is a software middleware to help automotive software architects and developers streamline and automate the development and deployment of automotive software. It consists of a number of components that act as middleware between the Operating System (OS) of an ECU or partition and applications that provide or consume services (functions) on the same hardware, other hardware in the vehicle, or in the cloud.

GuardKnox's Secure SOA Framework decouples the SWC (Software Component) from the underlying runtime environment and HW, allowing for true software portability. The framework delivers software more efficiently, optimizes compute resources, and increases reliability, significantly reduces time to market to just weeks and enables next generation capabilities-as-a-service for automotive.

KEY BENEFITS

- **Decreases time to market** for new APP/SWC deployment from 3-6 months to several weeks.
- **Standard development process** across the supply chain allowing architects to uniformly define interfaces and services to distribute business logic development across multiple suppliers.
- **Automatic life cycle management** of applications running on top of the framework.
- **True portability of applications** and SWCs in a "lift and shift" approach.
- **Open architecture**, extensible and modular, not limited to particular protocols or solutions to enable complete automatic application lifecycle management.
- **Software Defined Vehicle (SDV) platform** provides rapid introduction for new features and capabilities (personalization and retrofits).



GUARDKNOX SECURE SOA FRAMEWORK

The SOA Domain Manager is responsible for the "SOA Domain" (virtual application space) managing the lifecycle of SWC and their services. The Domain includes multiple runtime environments for applications, each one called a "Node". The Domain Manager also decides in which Node to deploy every SWC.

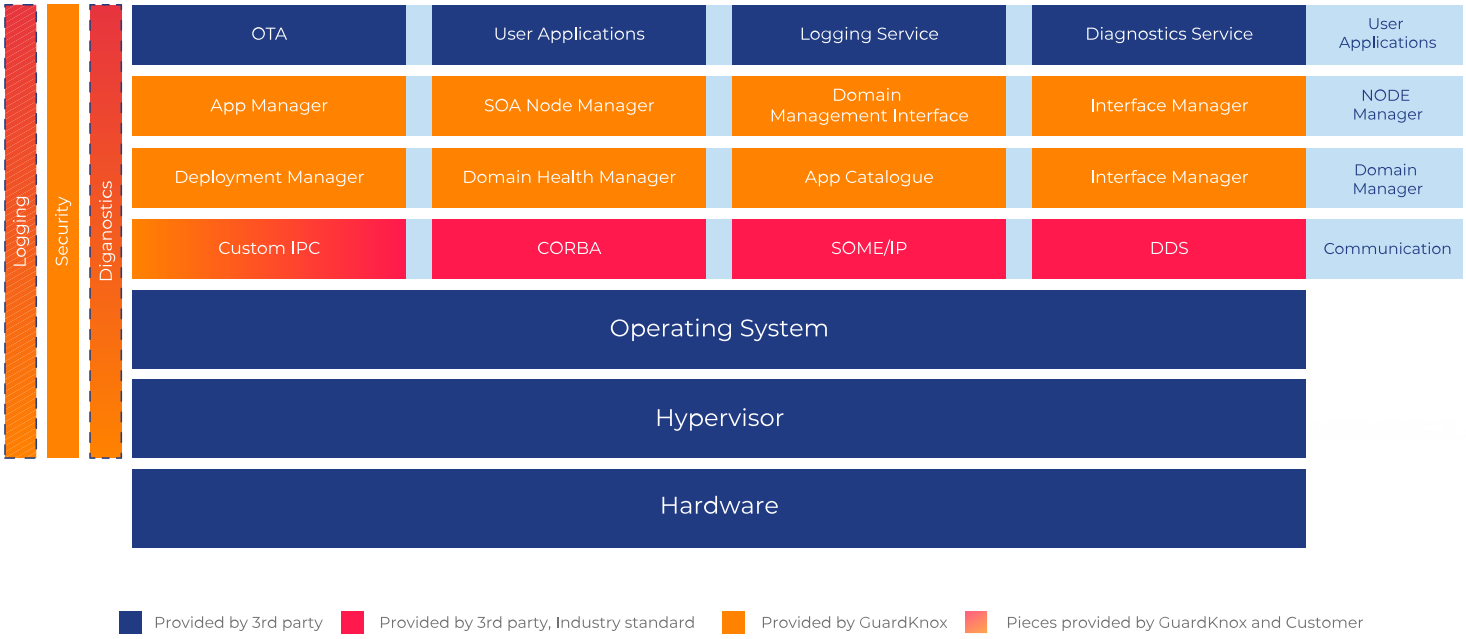
The SOA Node Manager is respectively responsible for a single "Node" (single runtime environment) and is adapted to execute control operations specifically in this "Node". It is managed by the Domain Manager which isn't specific to any runtime environment.

The SOA Port is an interface (defined in OMG IDL) realizing a communication broker connecting the SWC to a particular ESB using a user defined transport middleware. It allows for any SWC to create service-based communication ports and define them in a standardized format, regardless of the actual transport implementation. It also provides security, access control, QoS and other communication related capabilities.

KEY FEATURES

SEE ALL OUR PRODUCTS

- Open and extensible framework - add capabilities on top of the framework
- Automatic management of software lifecycle within the ECU – deploy, initialize, start, stop, teardown and remove SWCs.
- Virtual communication infrastructure – full support for multiple service-oriented communication ESBs – CORBA, DDS, SOME/IP and user defined IPC.
- Commercial OTA platform integration support (Uptane integration supported natively).
- Secure by design - security and access control mechanisms integrated in the framework.
- Support for management of safety critical applications and communication up to ASIL B. (and ASIL D under certain conditions.)
- Included modelling and supporting toolchain for design, code generation and simulation.



Contact info@guardknox.com for more information