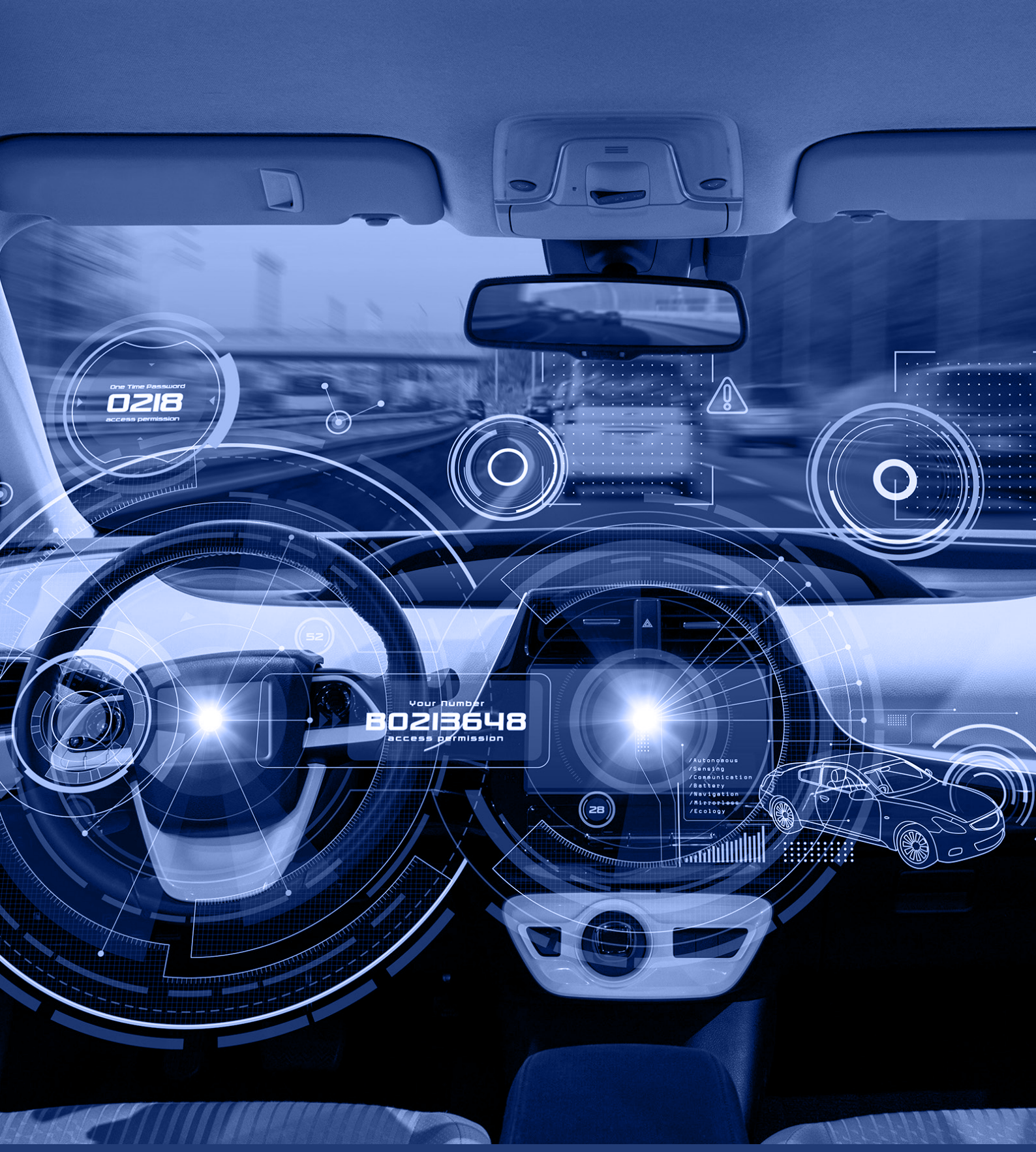


CREATING A SERVICE-ORIENTED ARCHITECTURE FOR

CONNECTED AND AUTONOMOUS VEHICLES

SYNOPSIS

This paper is intended to give a technical overview of GuardKnox's Service-Oriented Architecture (SOA) and how this patented methodology, with its hardware and software implementation, can serve the next-generation of connected and autonomous vehicles.

The paper opens with the origins of service-oriented architecture and the challenge posed by the multiplicity of vehicle computer networks and increased complexity of automotive software that cause millions of vehicles to be recalled each year. GuardKnox's patented approach for using the SOA methodology to utilize any ECU, Domain Controller or Gateway as a platform on which Tier 1 vendors and OEMs develop their services is introduced. The paper then explains how partitioning of the SOA concept works to enable the reuse of code, precisely allocate resources, and reduce cyber risks. The paper then touches upon GuardKnox's patented three-layer Communication Lockdown™ methodology and concludes with a look at how GuardKnox's SOA centralizes security for all vehicle applications, improves and simplifies interaction between ECUs, increases reliability and safety, and enables new revenues from app stores and add-ons.

THE ORIGINS OF SERVICE-ORIENTED ARCHITECTURE

Service-Oriented Architecture is an IT design philosophy that was developed in the late 1990s. It offered a solution for coping with the massive amounts of unwieldy code that needed to be processed during the migration of business applications to the Internet. Applications were broken down into specific functional components or "services" so that they could be remotely accessed and updated independently of the vendors that implemented them or the clients that used them.

Today's connected vehicles face a similar challenge. With a modern vehicle on average containing 100 million lines of code spread across nearly 150 ECUs on 7 customized networks, mobile computing systems are stretched to their limits. All of this complexity comes at a high cost: software issues in 2018 required the recall of millions of vehicles and cost the car industry over $17 billion.

In the coming years, the difficulties in updating and integrating computer code in vehicles will become insurmountable: autonomous vehicles will require an additional 200 million lines of code to handle vehicle-to-vehicle communication, vehicle-to-infrastructure communications and customizable or usability-related features. Scaling up becomes a major challenge in vehicle electronics and network design.

The only option for the mobile computing industry is to adopt a service-oriented architecture (SOA) methodology so that common system functions are formed into discrete, reusable "services" or standalone code components.

THIS WILL ENABLE OEMS AND TIER 1 PROVIDERS TO:

- Eliminate thousands of lines of redundant code
- Speed up software creation, integration and testing
- Enable the secure exchange of services
- Improve vehicle cybersecurity
- Standardize computing platforms and reduce vehicle costs
- Allow for reuse of well tested and field proven software components
- Ease safety certification

TECHNOLOGY REQUIREMENTS FOR IMPLEMENTING SOA

A completely new approach is required in which any ECU, Domain Controller or Gateway becomes a platform or repository on which Tier 1 vendors and OEMs develop their services using standardized protocols that facilitate communications and enable easy data transfer, irrespective of the underlying hardware, topology and protocols that are used to create the services. This will ease integration, make it significantly less labor-intensive, and nearly eliminate the development risks and software errors associated with the fragmented approach of today's vehicles.

The backbone ECU should be designed for real-time performance and high robustness to handle the variety of services designed by OEMs, Tier 1 and third-party vendors. The ECU should also offer the requisite levels of safety and performance required to support services used by the drivetrain, accessories, keyless entry, instrumentation, infotainment and Advanced Driver Assistance System (ADAS). This approach can offer scalability for the continuously changing needs of individual existing services as well as offer the capacity to easily add new functionality and customization.

Another advantage of SOA is that it allows for built-in security (such as seamless encryption) & application containment so that they can be monitored and not able to destabilize the entire system.

GUARDKNOX'S PATENTED APPROACH TO SOA

GuardKnox has pioneered a patented approach for vehicle networks that uses the SOA methodology to enable any ECU, Domain Controller or Gateway to serve as a vehicle-wide computing platform. By integrating SOA capabilities into ECU's, GuardKnox can maximize the functionality, security and safety of connected and autonomous vehicles while lowering the complexity of developing software and services that customize vehicles and generate new revenue streams for OEMs and third-parties.

FLEXIBLE SOA IMPLEMENTATION

The GuardKnox Platform has a wide offering of products that can be easily implemented alongside a vehicle-based Service Oriented Architecture

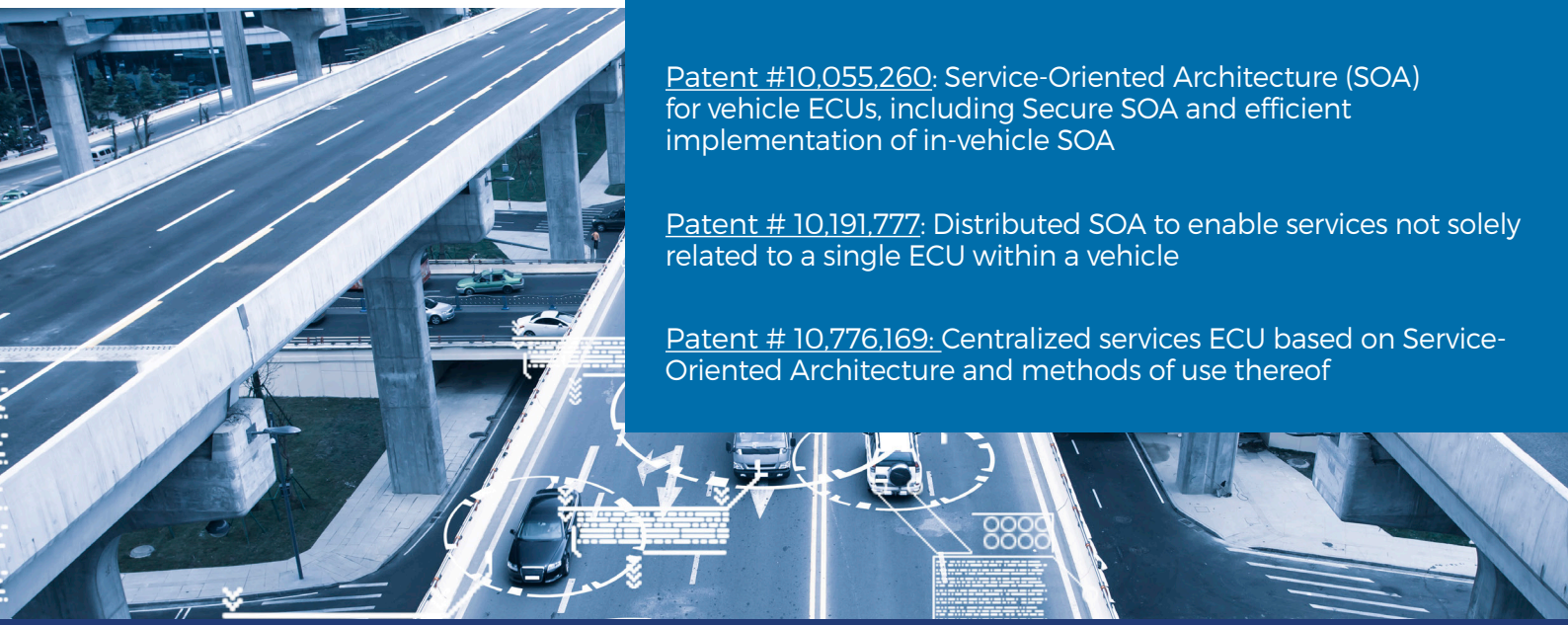
- Domain Controller
- Vehicle Server ECU
- Zonal Gateway on a Chip
- Secure Service-Oriented Architecture (SOA) Modular Stack
- Aftermarket Tailored Solution
- Built to Spec Solution

GUARDKNOX'S SOA PATENTS

Patent #10,055,260: Service-Oriented Architecture (SOA) for vehicle ECUs, including Secure SOA and efficient implementation of in-vehicle SOA

Patent # 10,191,777: Distributed SOA to enable services not solely related to a single ECU within a vehicle

Patent # 10,776,169: Centralized services ECU based on Service-Oriented Architecture and methods of use thereof

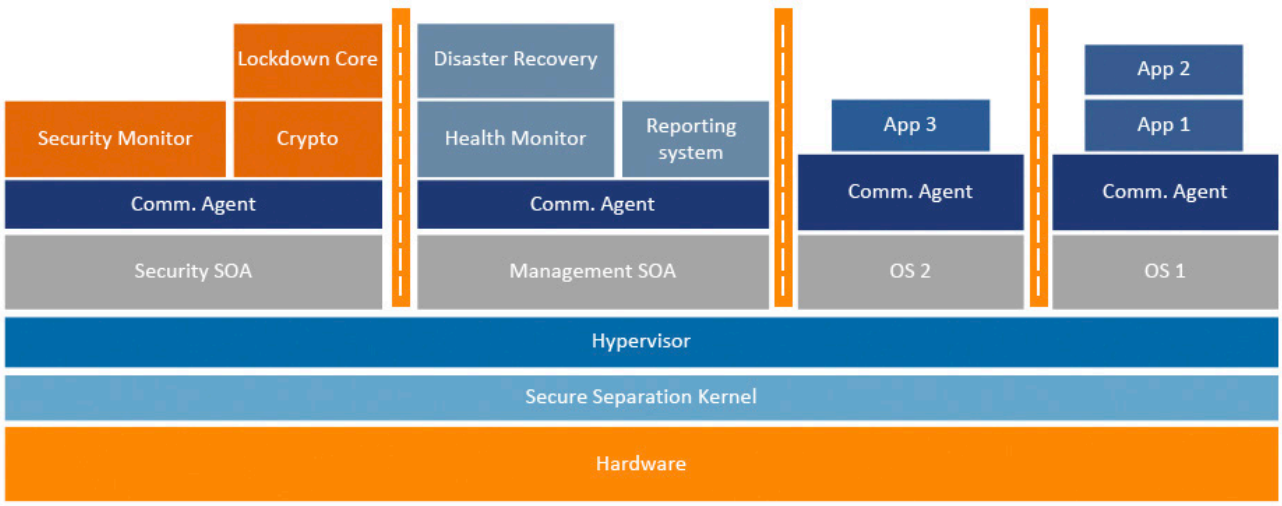


ENHANCED SAFETY AND PERFORMANCE WITH PARTITIONS AND ACCESS CONTROL

The GuardKnox SOA Platform provides a real-time safe and secure environment for the operation of multiple services within a client-server framework. The use of partitions isolates each discrete service component in order to:

- Precisely allocate computing resources as needed
- Guarantee a predetermined level of service and performance for each application
- Reduce cyber risks by separating safety-critical clients/networks from non-safety-critical clients/networks
- Integrate generic service API over legacy interfaces
- Easily add or modify services via over-the-air (OTA) software updates

SOA IMPLEMENTATION

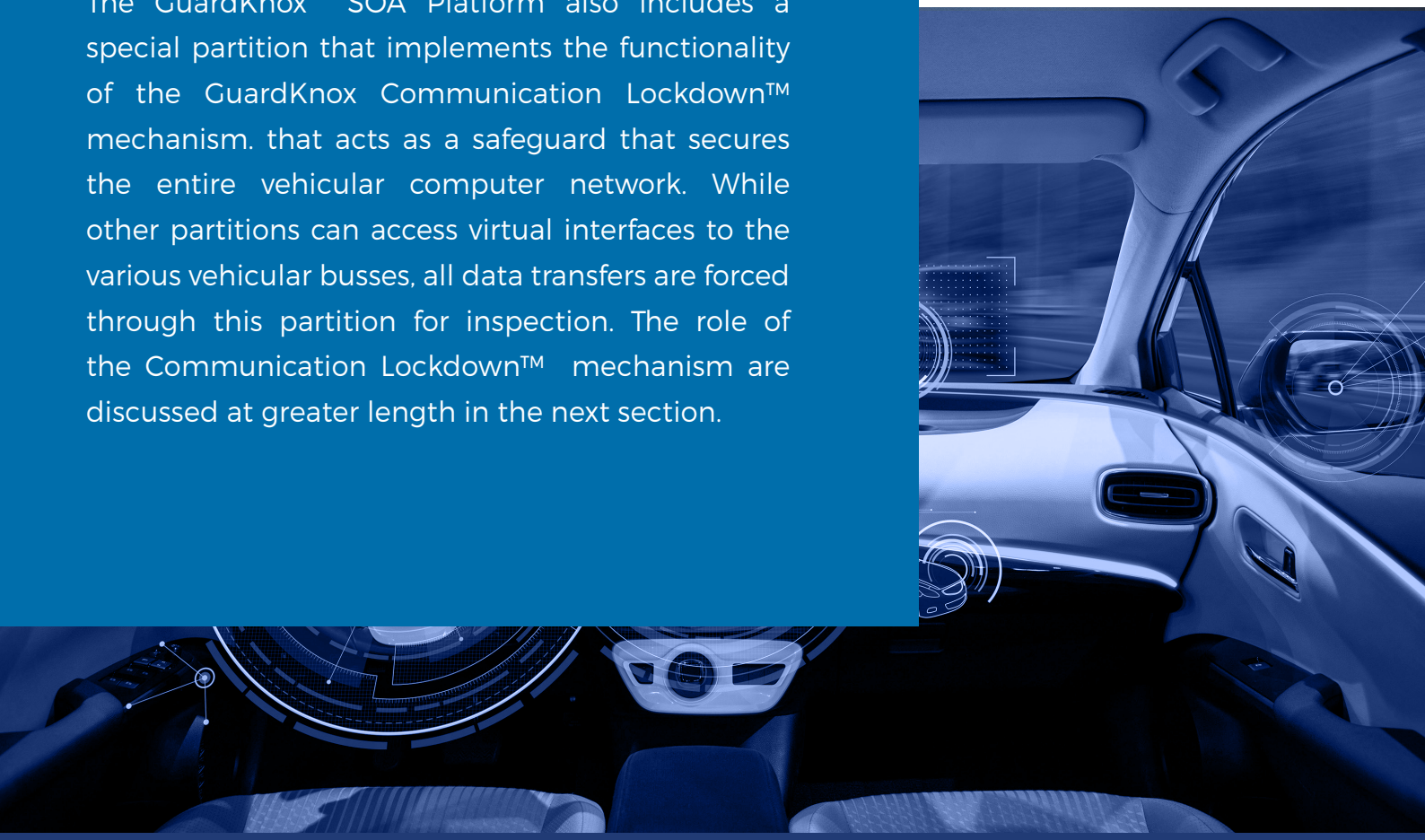


Each virtual partition can host an Operating System (OS) by utilizing a hypervisor. Applications are bound to resource allocation and access permissions and thus cannot modify the underlying OS or configuration parameters. This prevents unauthorized access to other areas within the vehicle network and greatly limits the potential for putting the vehicle at risk. By using different partitions, the GuardKnox Service-Oriented Architecture can consolidate functionality, optimize the use of computing resources and simplify the integration of third-party applications and services.

The use of whitelist access control ensures that individual services receive only their predefined sub-services and can be enhanced by hardware modules that accelerate some of the core functionality and security capabilities of the GuardKnox Service-Oriented Architecture such as the Hardware Security Module (HSM), the Trusted Platform Module (TPM) module or a cryptographic coprocessor without making any changes to the services themselves.

A SPECIAL PARTITION FOR CYBERSECURITY

The GuardKnox SOA Platform also includes a special partition that implements the functionality of the GuardKnox Communication Lockdown™ mechanism. that acts as a safeguard that secures the entire vehicular computer network. While other partitions can access virtual interfaces to the various vehicular busses, all data transfers are forced through this partition for inspection. The role of the Communication Lockdown™ mechanism are discussed at greater length in the next section.



THE ROLE OF COMMUNICATION LOCKDOWN™

In addition to simplifying the vehicle's computing architecture, a unique feature of the GuardKnox SOA Platform is its patented Communication Lockdown™ approach for providing holistic vehicle cybersecurity. Using the vehicle's communications matrix and OEM's specifications of the vehicle, GuardKnox builds a state machine that is used to inspect activity on three layers:

ROUTING LAYER

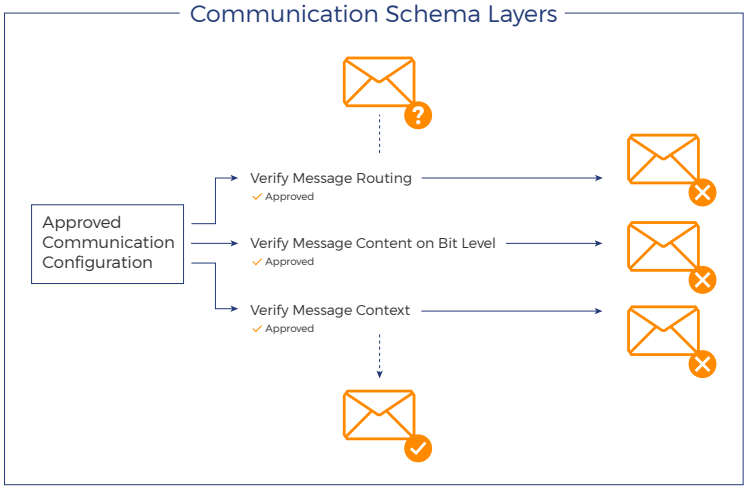
verifying that messages originate on the appropriate network or sub-segment

CONTENT LAYER

verifying that message content is permissible down to the bit level

CONTEXTUAL LAYER

verifying that each message is legitimate within the context of the vehicle's specific functional state (e.g., opening the sunroof at 100 km/h (54 mi/h))



Approving or discarding messages

The three layers of inspection ensure that if the external vehicle network is compromised by a message from the vehicle's external connectivity, the internal vehicle network remains fully protected from the propagation of malicious activity.

The Communication Lockdown™ methodology is completely agnostic to all types of known, unknown and future cyber attacks since the proper behavior of all messages has been fully modeled by the GuardKnox communications schema and certified by the OEM.

This also enables the GuardKnox solution to become fully autonomous after installation and to operate deterministically without the need for frequent software or firmware updates—unlike traditional Intrusion Detection/Intrusion Prevention Systems (IDS/IPS) or firewalls.

If the OEM changes the vehicle's Technical Specifications or its configuration, a new Communication Lockdown™ schema can be generated, certified and installed via secure OTA update or via a wired connection (such as the standardized OBD-II port).

THE BENEFITS OF THE GUARDKNOX SOA APPROACH

CENTRALIZED REUSABLE SERVICES

The GuardKnox Service-Oriented Architecture uses a central repository of software services that can be accessed by a variety of subsystems. These services or software models include but are not limited to:

ENCRYPTION such as symmetric cryptography services (e.g. AES, DES), asymmetric cryptography services (e.g. RSA, ECC), certificate storage and key management.

OTA (OVER-THE-AIR) UPDATE MANAGEMENT of software and firmware update services for multiple ECUs, OTA package delivery, authentication and external ECU flashing

HEALTH MONITORING such as starting, stopping and restarting services as needed

By implementing these functions as SOA services rather than separate applications, GuardKnox enables Tier 1 suppliers to more efficiently and rapidly develop their products and services.

In addition, OEMs need to perform a single testing and integration process that is considerably less expensive.

SERVICES FROM MUTLIPLE DEVICES TO OTHER ECUS

The Service-Oriented Architecture enables the improved delivery of services from local devices to multiple ECUs within the vehicle. These include signals to the vehicle instrumentation or messaging system, accepting inputs from the touch screen to various vehicle systems, transmitting location-related data from the GPS/navigation system, displaying alerts, warnings and failure messages, as well as resetting alerts and warnings.

Implementing these function as SOA services simplifies and improves the human-machine in interface (HMI) and the overall driver experience, enables more flexibility in implementing changes to vehicle functionality, and prioritizes access of resources for car subsystems.

FLEXIBLE DELIVERY OF CRITICAL VEHICLE-WIDE SERVICES

The architecture of the GuardKnox SOA Platform allows the flexible delivery of critical services with system-wide significance, such as the Communication Lockdown™ mechanism. Other critical services could include a centralized firewall, IDS/IPS, etc. Implementing these functions as SOA services eases the process of changing these services or adding new ones—and dramatically eases the debug and testing process.

IMPROVED VEHICLE RELIABILITY & SAFETY

The GuardKnox Service-Oriented Architecture by having common functionality, implemented, tested and certified only once.

The SOA approach eases the ISO certification for functional safety of electrical systems (ISO 26262) and cyber security (ISO15408) and the upcoming ISO 21434. The separation between the modules in the SOA design enables an entire ECU to be certified for safety without certifying any services that are not safety- or security-critical.

NEW REVENUES FROM APP STORES & ADD-ONS

Just as the app store concept revolutionized the mobile phone market user experience and generated new revenues, so too the automotive app store market will revolutionize the car market, improve driver experience and create vast new potential source of revenues for OEMs and Tier 1 vendors.

Automotive app stores are already a reality. OEMs such as Porsche, Mercedes, BMW and Volvo have their own app stores or distribute apps through Google and Apple. While Tesla seeks to retain control of its apps and services and has not shared a public SDK, an aftermarket Tesla app store has been launched.

Together, all of these initiatives are starting to turn drivers into subscribers who seek to continually enhance their driving experience. With customizable apps for navigation, infotainment, telematics. and roadside assistance, OEMs and Tier 1 vendors are continuing to develop apps to further customize the driving experience, including customized vehicle handling (breaking, acceleration, suspension, steering) for driving in different road or weather conditions, or to reflect the needs of different drivers or owners.

THE GUARDKNOX SERVICE-ORIENTED ARCHITECTURE CAN SERVE AS A KEY ENABLER FOR INTEGRATING THESE CAPABILITIES:

- Offers a centralized repository of functionality that accelerates and eases the creation of applications
- Manages and secures application installation and updates
- Protects the vehicle and other vehicle applications from unauthorized access or manipulation

CONCLUSION

The GuardKnox Service-Oriented Architecture brings a new paradigm to the connected and autonomous vehicles and provides a highly flexible and extensible platform that will:

- Provide a centralized security services for other applications
- Simplify vehicle networks and eliminate duplication of software components and libraries
- Reduce the costs of physical hardware due to consolidation and functionality offloading
- Accelerate the time-to-market for new vehicle platforms and services/apps
- Reduce vehicle recalls due to software and integration issues
- Create new revenue streams for OEMs and Tier 1s through continuous driver customizations

In short, the GuardKnox Service-Oriented Architecture will enable OEM and Tier 1 vendors to do more with less while enabling the next-generation of connected and autonomous vehicles.

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