2023 NDIA MICHIGAN CHAPTER
GROUND VEHICLE SYSTEMS ENGINEERING
AND TECHNOLOGY SYMPOSIUM
MODULAR OPEN SYSTEMS ARCHITECTURE (MOSA) TECHNICAL SESSION
AUGUST 15-17, 2023 - NOVI, MICHIGAN

ADVANCED MODULAR VEHICLE ARCHITECTURES AND CYBER RESILIANCE IN THE SOFTWARE DEFINED VEHICLE

Jamey Cates, P.E.[1], Karl Nielson[2], Joe Stempnik, [3]

[1]GuardKnox Cyber Technologies, Livonia, MI
[2]Army CCDC/GSCE, Warren, MI
[3]Army CCDC/RTCS, Warren, MI

ABSTRACT

Automotive electrical/electronic (E/E) architectures are continuously evolving to meet the technological challenges of the highly connected, software-defined vehicle. Advances are being made in µController/µProcessor compute hardware, software, and cyber security methodologies, to provide enhanced security, safety, flexibility and functionality.

These advancements will mature through millions of miles of road/lab testing and reach TRLs suitable for use by the Army to implement safe and secure cyber-resilient platforms for manned and unmanned ground vehicle systems.

This paper will describe three specific advances that will benefit Army vehicle programs of the future: Software that leverages the Modular Open Systems Approach (MOSA) as a secure and flexible Service Oriented Architecture (SOA) framework; Hardware-based Communication Engines for high bandwidth/low latency network communications; and a Hardware Security Module (HSM) that enhances the cyber-resilience of the next generation of the Army's neXtECU module.

Citation: J. Cates (GuardKnox), K Nielson, J. Stempnik, "Advanced Modular Vehicle Architectures and Cyber Resilience in the Software Defined Vehicle," In Proceedings of the Ground Vehicle Systems Engineering and Technology Symposium (GVSETS), NDIA, Novi, MI, Aug. 15-17, 2023.

1. Introduction

Current automotive architectures can consist of up to 150 functionally specific ECUs, dozens of sensors and miles of wiring. In order to meet the rising demand for increased functionality, safety, security and connectivity associated with next-gen autonomous, software defined vehicles, automakers have historically just added more ECUs. These ECUs usually provide a single or limited number of functions and bring additional components and wiring along with them, but cannot keep pace with growing requirements. The result is rising complexity and cost and is no longer viable since the vehicle network is saturated, has insufficient bandwidth and too much wiring to handle additional ECUs. As such, modular, high performance hardware platforms and software stacks are being developed that operate in a more centralized manner and offer exponentially more functionality and flexibility:

- Secure, high performance vehicle computers (HPCs), ECUs, Gateways, Domain and Zonal controllers, based on advanced silicon platforms like System on Chip (SoC)s and Field Programmable Gate Arrays (FPGA)s offer more flexibility and can handle multiple functions which are abstracted and performed within hardware.

- Modular, Service Oriented Architecture (SOA) software stacks decouple underlying hardware from application software, increase flexibility and leverage hypervisors and separation kernels to allow mixed-criticality applications to run on a single platform.

- Secure, hardware-based, high bandwidth/low latency network communications facilitated by single chip communication engines.

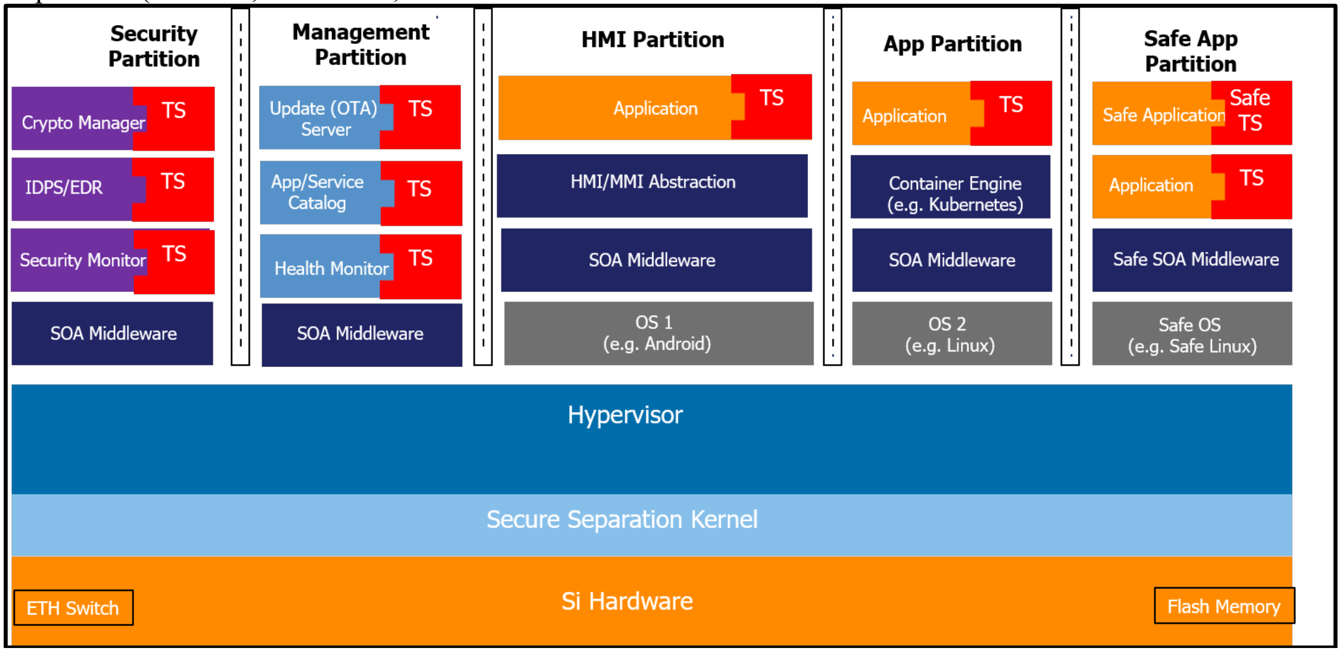
- Advanced cybersecurity software stacks, cryptographic libraries, and processes combining hardware and software (e.g., Hardware Security Modules (HSMs), Public Key Infrastructure / Service (PKI/PKS), Intrusion Detection/Prevention (IDPS), etc.) that minimize data and mission safety and security risks.

These advancements are working their way into military vehicle design in part because of the adoption of a Modular Open Systems Approach (MOSA). MOSA will ensure that each discrete component (software, hardware, sensors or interfaces) can function agnostically to surrounding sub-systems and receive maintenance and upgrades without requiring changes to the vehicle or other sub-systems. This will result in more robust and flexible platforms for the next-gen fleet of military vehicles.

2. SOA

In order to support the dynamic functionality required by future vehicles, a service-oriented architecture (SOA) framework is required. One of the first implementations of SOA was the development of the Software Communications Architecture (SCA) framework open standard architecture for Software Defined Radios (SDRs), developed to standardize communications between different branches of the military.

Automotive SOA is based on IT architectures, using software applications to provide services to other components through a communication protocol over a network (communication bus). In figure 1 below, the management partition provides services such as software distribution and updates (OTA), services management (cataloging) and health monitoring.



SOA offers the benefits of MOSA:

- Provides a framework based on modular component-based software design acting as middleware between the base software (operating system) and applications.

- Allows maximum modularity of individual software components (SWCs) for dynamic management and decoupling from runtime environment and hardware.

- Provides a virtual communication infrastructure for cross-platform data abstraction adaptable for specific customer requirements/target environment.

- Outlines a complete toolchain for model-based design of SWCs/interfaces, automatic code generation, and a unified language between architects and developers.

- Enables automatic software lifecycle management on ECU and vehicle – automatically deploy, initialize, start, stop, update, teardown and remove SWCs.

- Facilitates flexible, unified communication between SWCs and services, with easily modified underlying transport middleware (allows multiple communication busses to coexist).

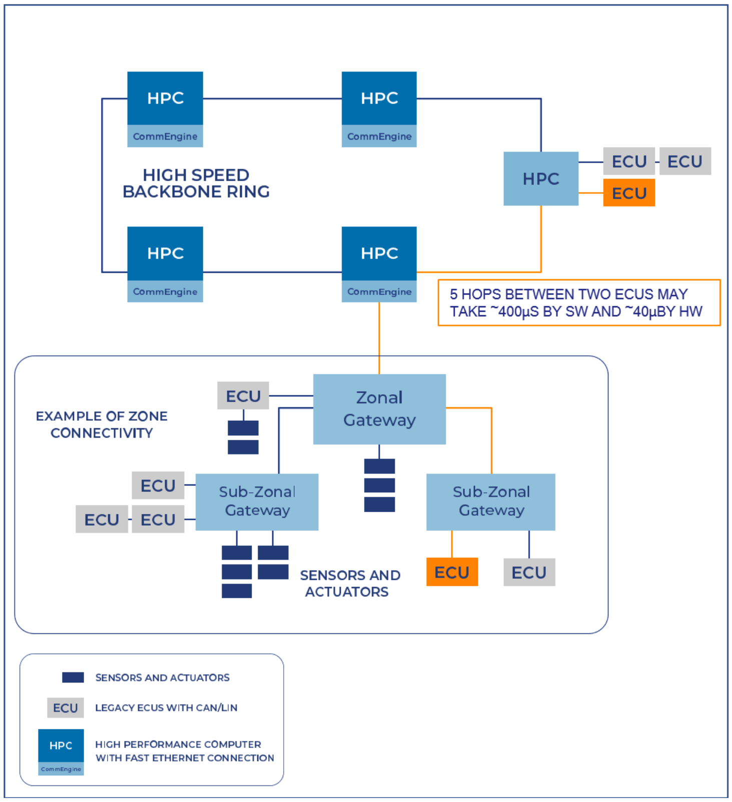
- Is scalable from single ECU to multiple ECUs and infrastructure outside of vehicle and cloud.

3. Communication Engine

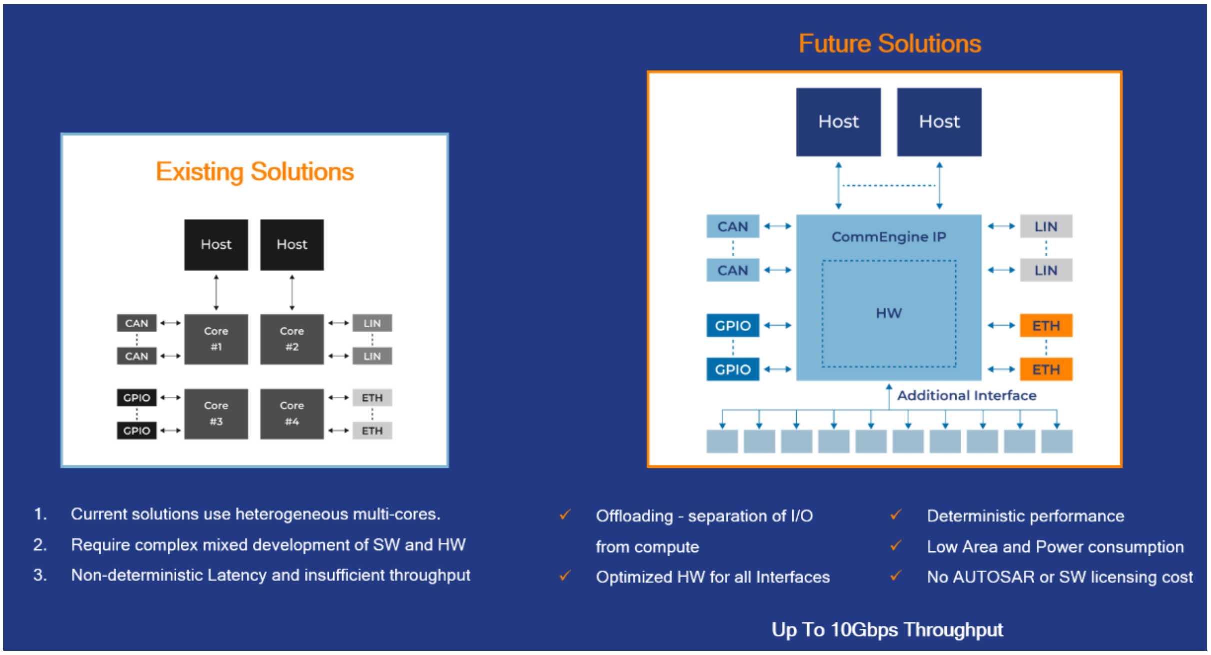
Automotive E/E topologies are moving toward architectures where domain-centered and zone-centered configurations are used to consolidate the functionality of several ECUs.

In zonal routers, a combination of microcontroller and Ethernet switches are used. However, such designs quickly lead to timing and routing problems and advanced communication engines are being developed to address the resulting routing complexity.

Zonal Architectures require signals or messages to pass through several “hops”, with latencies compounding. The resulting end-to-end latencies can therefore quickly exceed the limits set by the system, further complicated by unpredictable fluctuations (figure 2 below).



The communication engine solution must therefore address several different dimensions of these growing communication needs. It must securely route information quickly, with deterministic, extremely low latency, independent of any other message traffic. State of the art solutions will need to have latencies in the microsecond range vs. the current status quo in the millisecond range. It must also be flexible enough to function across multiple interfaces and support payload-level custom logic (figure 3 below).



Future Solutions

Existing Solutions

1. Current solutions use heterogeneous multi-cores.
2. Require complex mixed development of SW and HW
3. Non-deterministic Latency and insufficient throughput

- ✓ Offloading - separation of I/O from compute
- ✓ Optimized HW for all Interfaces
- ✓ Deterministic performance
- ✓ Low Area and Power consumption
- ✓ No AUTOSAR or SW licensing cost

Up To 10Gbps Throughput

4. neXtECU HSM

Vehicle Cybersecurity is focused on protecting data and data management assets – not only from theft but also misuse. In general, Cybersecurity is concerned with the security mechanisms used to protect the data and also the assurance that those mechanisms protect as intended.

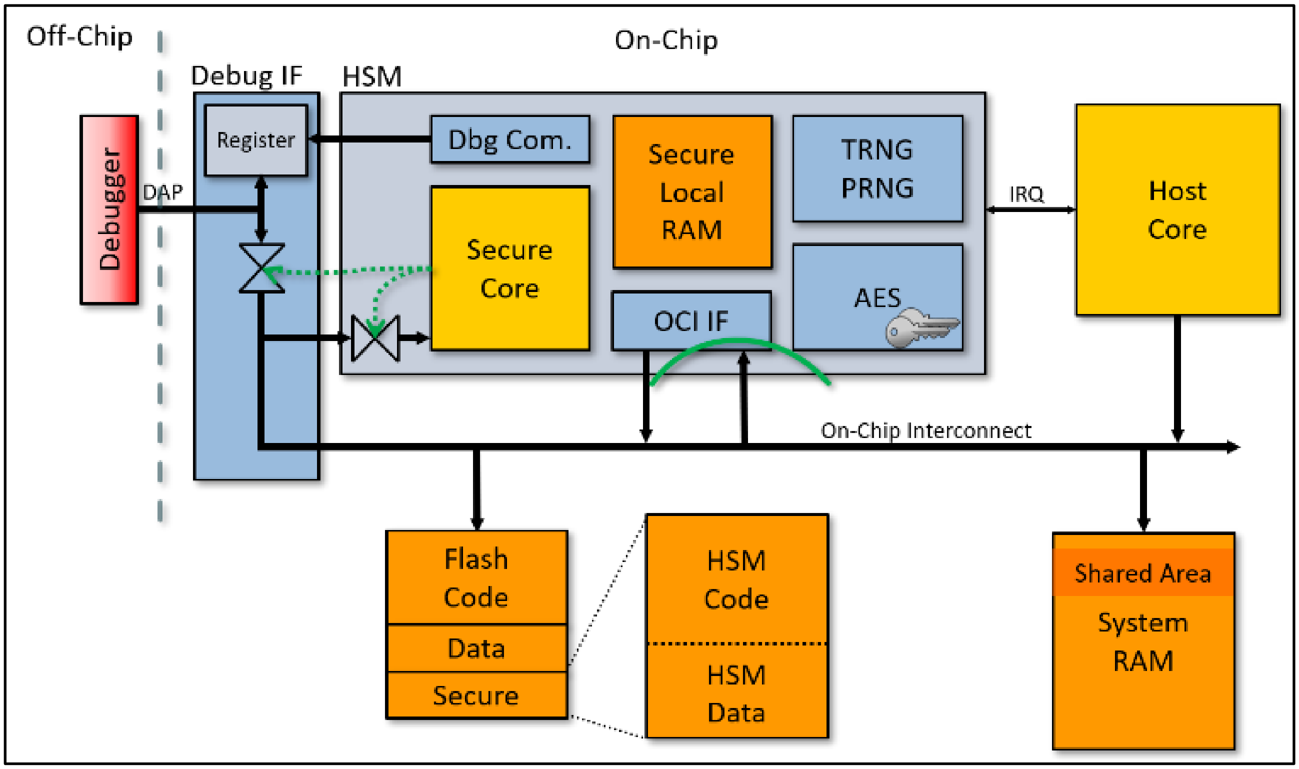
Since modern vehicles are defined by their software and have dozens to hundreds of ECUs with hundreds of millions of lines of code, the performance and functionality requirements are daunting, as are the security and safety risks. Some of the greatest advances in vehicle connectivity are quickly becoming the biggest vulnerabilities in the system and therefore leading to serious threats.

As such, more advanced methodologies are being developed to address hardware security directly – i.e., on-silicon Hardware Trust Anchors (HTAs). The most common are Secure Hardware Extensions (SHEs), Trusted Platform Modules (TPMs) and Hardware Security Modules (HSMs).

HSMs are the method of choice for vehicle security due their extended capabilities and ability to be customized for specific applications and OEM requirements e.g. SecureBoot, SecureReflash and SecureCommunications. They are fully programmable and accessible to on-board applications in the ECU. A typical HSM has the elements shown in figure 4 below and provides the following capabilities:

- Automotive HSMs are an embedded peripheral of the Microcontroller Unit (MCU), as opposed to a network-attached enterprise HSM
- HSM firmware typically supports cryptographic key provisioning
- HSM firmware allows direct access to application host memory
- HSMs generally provide the broadest scope and are typically the most flexible and powerful approach to hardware security – some are faster than a computer CPU when performing cryptographic operations due to cryptographic acceleration hardware.

- HSMs provide enhanced security and acceleration of encryption or decryption.
- Some HSMs can run their own operating system and execute custom programs.
- HSMs are generic devices that conform to APIs and are therefore accessible to any application that wants to use their services.



The US Army's Combat Capabilities Development Command (CCDC) Ground Vehicle Systems Center (GVSC) Ground Systems Cyber Engineering's (GSCE) Vehicle Systems Security (VSS) program is directly supporting Next Generation Combat Vehicle (NGCV) development by demonstrating an enhanced combat vehicle cybersecurity methodology and architecture.

GuardKnox was engaged by GSCE to develop an HSM security stack that will leverage the HSM resident on the microcontroller of the next-gen neXtECU control module in development by the Army's Real Time Controls Team (RTC).

The primary HSM security goal is to provide a trust base for cryptography to be used by, and provide protection for, applications on the MCU within the neXtECU. The objective of the HSM software development will be to provide the following functionality to the MCU:

- Cryptographic Operations and Key Storage including authentication and encryption methods
- Secure Boot
- Secure Software Update Process

The project resulted in the successful development and deployment of a full-functional HSM stack and is in ongoing development and testing on the neXtECU module.

5. REFERENCES

(Note: Use IEEE style)

[1] Statement of Work: "W15QKN-1709-1025 Hardware Security Module (HSM) Prototype."

[2] NCMS Advanced Cybersecurity Technologies to Improve Fleet Maintenance and Vehicle Safety Final Report