Automotive Security through New Communication Lockdown Utilizing Programmable Logic Solutions

Authors:

Dan Isaacs
Director Automotive Business Unit
Xilinx
dani@xilinx.com

Jillian Goldberg
VP Marketing
GuardKnox
jillian.goldberg@guardknox.com

Dionis Teshler
CTO and Co-Founder
GuardKnox
dionis@guardknox.com

Tal Nisan
Software Architect
GuardKnox
tal.nisan@guardknox.com

INTRODUCTION

In today's connected world, ensuring a vehicle's security must be addressed through a comprehensive understanding of all networked communication channels internal and external to the vehicle. This article presents an innovative methodology, Communication Lockdown, including Network Orchestration, from development to production, as implemented in a centralized communication gateway based on Xilinx's configurable Zynq® SoC programmable technology. This includes a description of the methodology, advantages and differentiating values of the technologies involved.

PROBLEM STATEMENT

As vehicles drive towards autonomy, they multiply in complexity, becoming far more connected. Today's vehicles are highly sophisticated local area networks on wheels that controls numerous complex systems via hundreds of micro-processors, up to 150 ECUs [1] (automotive computers), and numerous sensors, interconnected by a high-speed, high-availability internal communications network.

The automotive industry is moving towards a service-oriented vehicle, where the passengers (or drivers) and their needs are the focal point rather than the vehicle itself. This concept is focused on the ability to continuously and securely change vehicle capabilities, instantaneously, on-demand and over-the-air (OTA) from future OEM app stores.

Automotive cyber security for modern connected and autonomous vehicles require a solution that is:

1) Cyber-secure: In today's vehicles, safety and security are inherently the same. Modern vehicles host hundreds of sensors and ECUs powered by more than 100 million lines [2] of software code. Cameras and sensing devices stream gigabytes of data in real time. A typical vehicle might also host several different types of local area networks such as CAN bus, Ethernet, and LIN. Manufacturers source hardware and software from different suppliers. No single player controls, or is familiar with, all of the possible attack vectors within any vehicle. As such, vehicles constitute a massive attack surface that could be used to exploit sensitive data, financial information and much more.

2) Flexible and Scalable: Current and next generation automotive architecture will be based on high speed communication and high-performance computing. This will

[1] Techopedia. "Your Car, Your Computer: ECUs and the Controller Area Network" https://www.techopedia.com/your-car-your-computer-ecus-and-the-controller-area-network/2/32218

[2] MIT Technology Review. "Many Cars Have a Hundred Million Lines of Code" https://www.technologyreview.com/s/508231/many-cars-have-a-hundred-million-lines-of-code/

require the handling and securing of multi gigabit data channels and the running of dozens of applications per ECU. This task cannot be achieved with current architectures based on micro-controllers which are not optimized or flexible to cover evolving requirements. Cybersecurity solutions require both hardware and software flexibility and scalability to provide ample processing resources and provision for future software extensions/additional services. Having extra computing power and storage management from the onset will not require costly and resource-intensive changes to vehicular hardware architecture as the connected and autonomous industry develops and matures.

3) Interoperable: Mission and non-mission critical operating systems and applications need to run simultaneously on one ECU without interference. Additionally, a compartmentalization is needed to ensure that if one application should be compromised, all others will be unaffected.

4) Service-Oriented: The automotive industry is moving towards OEM future app stores for vehicle customization, requiring a multi-platform and multi-service approach with the ability to host multiple operating systems and services with secure separation between all resources, applications and operating systems.

5) Personalized: In-vehicle safety is critical for the automotive industry as additional levels of connectivity, especially for vehicular personalization, are added. Cybersecurity needs to serve as the foundational platform for added connectivity, services, and customization to create new markets and added revenue streams for OEMs.

Car manufacturers and Tier 1 suppliers have traditionally been turning to IT experts for in vehicle solutions. Unfortunately, IT cyber solutions may not be applicable to the automotive industry as vehicles are moving platforms with a finite set of messages compared to static computers with an infinite set of messages. In addition, cybersecurity within vehicles is an extension of safety, therefore the reliability of automotive cybersecurity solutions must be as close to 100% as possible. Furthermore, there is no room for false positives in such systems.

INNOVATION ADDRESSING AUTOMOTIVE CYBERSECURITY CHALLENGES

Overview - Expertise / Capabilities

GuardKnox Cyber Technologies Ltd[3]. is an automotive cybersecurity company which provides secured ECU's, domain controllers, and gateways to the automotive industry with a hardware and software cybersecurity solution to protect vehicles including passenger cars, commercial vehicles, mass transportation and more. GuardKnox

[3] [3] www.guardknox.com

solutions are based on the secure network orchestrator or SNO™ technology[4] that can be centralized or localized. SNO features include in-vehicle network defence, high-performance gateway, application host domain computer, advanced body control and security for all external communication coming into the vehicle and from the vehicle externally.
Applications include:

- EV Charging ECU - a secure in-vehicle charging platform for V2G communications and
- Secured High-Performance ECU's - high-performance, scalable, and secured ECU's due to manufacturers' specification.

Applications include EV Charging ECU- providing a secure in-vehicle charging platform for V2G communications and Secured High-Performance ECU's- design high-performance, scalable and secured ECU's.

The GuardKnox platform also hosts service-oriented architecture, or SOA [5, 6] allows unified communication as well as access control and service level partitioning to ensure further levels of connectivity, customization, and additional revenue streams across the automotive value chain. These systems can also serve as platforms within the vehicle for secured data processing and storage.

The Communication Lockdown approach to cybersecurity is uniquely differentiated as it is not a learning or IT-based solution. Computer industry solutions such as Intrusion Detection/Intrusion Prevention Systems (IDS/IPS) and/or firewalls are seemingly obvious choices to protect computers-on-wheels, but they are ill-equipped to meet the cybersecurity needs of the automotive industry as they:

- Cannot offer a real-time/immediate response to new threats or morphing malware
- Require time to analyse specific new threats and to develop and deploy software updates
- Do not offer support for an external Security Operations Center (SOC) to continuously monitor vehicles and communicate with owners and drivers

[4] https://www.guardknox.com/products/

[5] GuardKnox Secure Hardware Architecture Patent "Hardware Components Configured for Secure Physical Separation of Communication Networks in A Vehicle and Methods of Use Thereof" http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=4&f=G&l=50&co1=AND&d=PTXT&s1=guardknox&OS=guardknox&RS=guardknox

[6] GuardKnox Services Oriented Architecture (SOA) Patent "Specially Programmed Computing Systems with Associated Devices Configured to Implement Centralized Services Based on Services Oriented Architecture and Methods of Use Thereof": http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.htm&r=1&f=G&l=50&s1=10,055,260.PN.&OS=PN/10,055,260&RS=PN/10,055,260

These challenges are overcome through a patented cybersecurity "lockdown" approach that is successfully used by Israel's F-35I and F-16I fighter jets and missile defence systems. By enforcing a formally verified and deterministic configuration of communication among the various networks of the vehicle, the Communication Lockdown methodology eliminates all known and unknown cybersecurity risks by approving or discarding all inbound and internal vehicle communications in real-time.

Table 1: Different Approaches to Automotive Cybersecurity

Capability	Communication Lockdown	Firewall	IDS/IPS	Anti-Virus
Security Mechanism	- Formally verifiable state machine - Agnostic to attacks - Certifiable (safety and security) - Approved configuration lockdown	- Static ruleset firewall - Needs updating as new attacks materialize	- Heuristic detection of attacks (anomalies) - Reliability can't be proven	- Local Anti-Virus - Signature updates required
Defense Capability	- All vehicle networks - Prevention on bit level	- Several car networks	- No prevention	- 1 ECU
Reliability	- 99.99999% - with deterministic mathematical model That can be verified, tested, and certified - Zero false positives	- Can be tested by automotive standards but can't be qualified	- 98% Detection rate - Up to 5% False positive rate	- Reliability can't be proven
Maintenance	- No cloud connectivity required - No on-going updates required	- Requires cloud connectivity and regular updates	- Requires online cloud connectivity and continuous updates	- Updates for every change of the ECU

Capability	Communication Lockdown	Firewall	IDS/IPS	Anti-Virus
Physical Separation	- Hardware, software and firmware level separation between networks	- None	- None	- None
Integration	- Minimal integration - Transparent to other ECUs	- Requires integration into 3rd party (Tier1) ECU	- Requires integration into multiple 3rd party (Tier1) ECUs	- Requires integration into ECU and development environment
Scalability	- Full services and application secure hosting platform - Full support for virtualization and service oriented environment	- Fixed functionality - Requires integration into each environment	- Fixed functionality - Requires integration into each environment	- Need to recompile and re-certify the ECU
Cost Effective Hardware	- No need to modify vehicular hardware architecture for additional software extensions/applications	- None	- None	- None
Compliance to Standards	- Safety: ISO 26262 - Security: Common Criteria (ISO 15408)	- None	- None	- None
Physical Security	- Tamper proof: erases information upon tamper attempt	- None	- None	- None
Fit to Automotive value chain	- Full fit to tiered hardware value chain, no integration	- Requires software integration	- Extensive integration	- Extensive integration

Target Areas for the Communication Lockdown based technology include:

1) Automotive OEMs: where the systems would be provided directly to the OEM, where connected vehicles need security, without compromising the safety and integrity of the vehicle. Specific product implemented depends on the OEM's concern:
   a) Preserving the holistic security for the vehicle and all of its components.
   b) Dedicated ECUs or a single interface, such as telematics or infotainment.

The technology can be implemented during production or retrofitted after production or in the aftermarket.

2) Tier 1 Suppliers: Tier 1 suppliers are responsible for building the in-vehicle ECUs. The ECUs may possess many cybersecurity vulnerabilities due to the number of networks and other ECUs communicating within a vehicle. By implementing Communication Lockdown technology into their ECUs, these vulnerabilities can be addressed. This applies to aftermarket products that need protection and seamless integration as well.

3) Telematics Providers - Fleet Tracking: Telematics and in particular trucking telematics is considered one of the biggest growth industries. Telematics and fleet management solutions enable commercial trucking OEMs and large fleets to monitor and better understand their usage through location providing services. These behave the same as a car ECU but are referred to as a TGU, or Telematics Gateway Unit within a commercial vehicle. A Communication Lockdown-based solution protects the TGU and ensures both secure functioning of the vehicle from any external cyber threats as well as securing the data obtained from the device.

Solution

Application Illustrating Innovation – "Communication Lockdown"

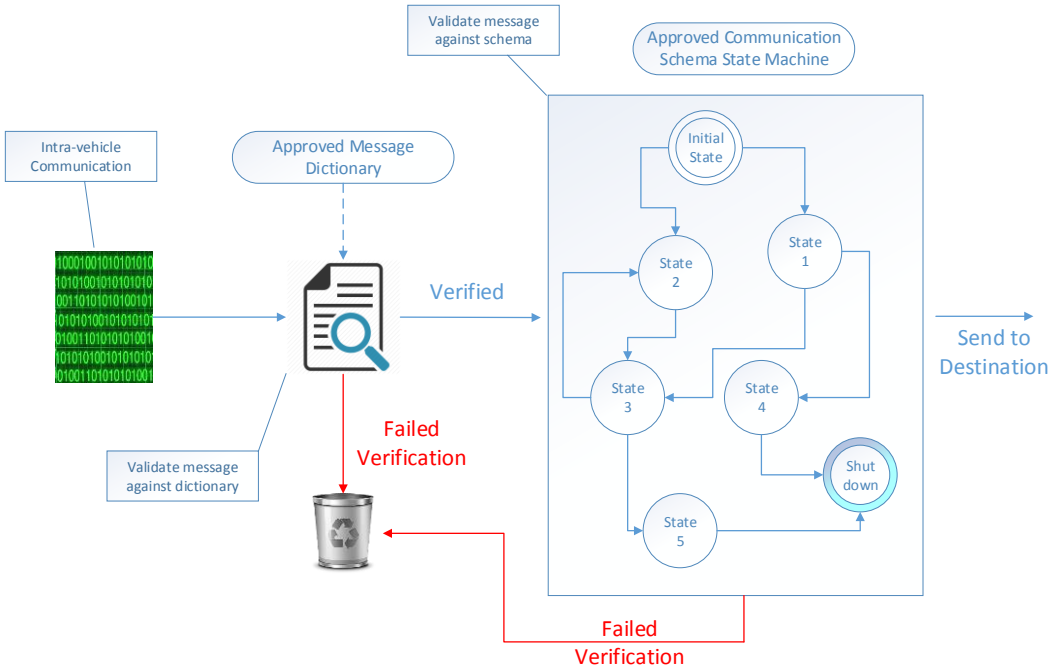

Figure 1: Communication Lockdown with State Machine

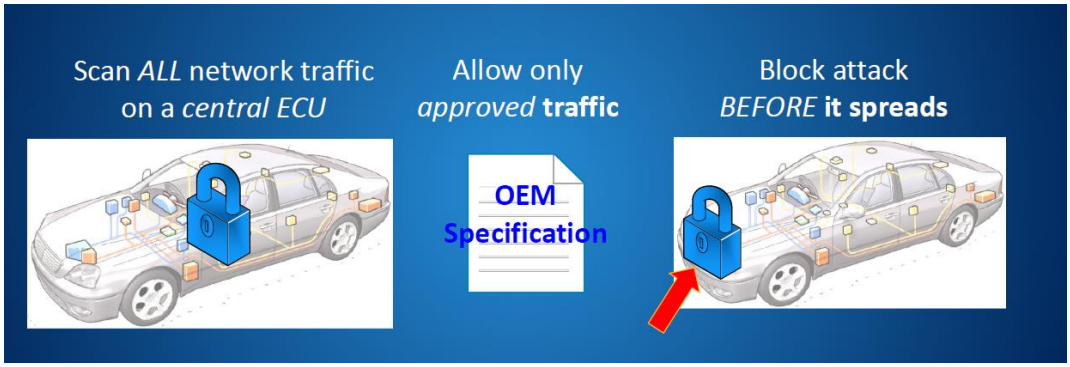

Figure 2: Communication Lockdown

Description of Methodology "Communication Lockdown" with Network Orchestration

The Communication Lockdown methodology delivers an innovative approach to automotive security, permitting authorized communication while being impervious to any type of inappropriate transmission, including all cyber-attacks. This includes but is not limited to DoS attacks.

The methodology detects and prevents the injection and the spread of malicious

messages between the various ECUs used to control the vehicle. All incoming messages are inspected, and only approved/legal messages can continue to their destination. Since communication lockdown looks at the approved frequency and the size of the messages, this effectively limits the case of bus overload. This is furthermore achieved even more effectively in hardware using field-programmable gate array (FPGA) logic since it is able to deal with a higher bandwidth communication than solely reaching it in software. All cyberattack attempts—in which illegal or improper messages are discarded—can be logged and reported over a wireless vehicular communication channel to a remote OEM SOC for further technical and statistical analysis, including fleet information, geographies and trends.

Intrinsic to the Communication Lockdown methodology is the ability to use the OEM Technical Specifications, specifically the communication matrix, where the bus message database and the functional specifications are used, to create a communication schema that models the proper behavior of all vehicular data.

The Communication Lockdown methodology is agnostic to attacks since it does not look for them. Instead it only models the "correct" behavior. In this approach of not looking for attacks from a defense methodology standpoint, you do not care about the incoming attacks since they are not being looked for. In Communication Lockdown the communication is efficiently modeled and verified to comply with the vehicle specification. This enables full autonomy after installation and operates deterministically without the need for frequent software or firmware updates—unlike Intrusion Detection/Intrusion Prevention Systems (IDS/IPS) or firewalls.

Three Layers of Communication Security

The effectiveness of the Communication Lockdown methodology is based on the patented ability to inspect and verify messages on multiple layers. This ensures that if an external message from the vehicle's ecosystem is compromised, the internal vehicle network remains fully protected from the spread or propagation of malicious code.

All incoming messages are inspected on three layers:

Routing Layer

- The origin and destination of each incoming message (type) is checked by the Communication Lockdown™ schema to ensure that they are permissible or "legal". For example, messages from the infotainment subsystem to the powertrain components (steering, brakes, etc.) are prohibited and would therefore be discarded.

Content Layer

- The content of each incoming message is checked down to the bit level for compliance with the permissible format as defined in the OEM's Technical Specifications. Messages that do not conform to the defined format are dropped.

Contextual Layer

- The content of each incoming message is checked for legitimacy in the specific functional state of the vehicle, subsystem, ECU, etc. Messages from specific origins to specific destinations are permitted or discarded depending on the contextual/functional state of the vehicle. For example, messages received from the OBD-II maintenance connector during the vehicle movement on the road (speed > X Kmph) will be discarded.

Communication Lockdown Methodology Unique Benefits:

DETERMINSTIC

The Communication Lockdown approach is a fully deterministic cyber security methodology. The closed-system approach is not to look for attacks, but rather to ensure that the vehicle continues to function in the way it was designed.

UPDATEABLE

Using automatic tools to create layered protection, a fully deterministic, yet updateable mathematical model that can be formally verified is generated.

FORMALLY VERIFIED

On three different layers, down to the bit level. Additionally, open fields are also 'locked down' to ensure stringent security.

FINITE STATE-MACHINE

This model includes a state machine, which enforces predetermined states, with a dedicated ruleset generation tool. Only allowed communications, as detailed by OEM technical specifications and bus network communication matrices, are approved.

STAND ALONE SOLUTION

There is no need for cloud connectivity nor for ongoing updates. No malware can sneak in and corrupt the safety requirements of the vehicle. The Communication Lockdown methodology delivers the requirements of the Safety Critical Subsystem of the connected car.

SECURED CLOUD CONNECTIVITY

The Communication Lockdown model behaves as a secured landing point within the vehicle for cloud connectivity which enables secured OTA and data transfer, among other things. The mechanism supports mutual authentication and encryption between the backend, the cloud and the vehicle, therefore enabling secured cloud connectivity when needed as opposed to resource-intensive and vulnerable continuous connectivity.

CAN BE INTEGRATED WITH ANY SOC

Supports any SOC to monitor, log and report any and all activities.

Software - Service Oriented Architecture (SOA)

SOA partitioning [7] utilizes the patented architecture allowing for unified communication as well as access control and service level partitioning. Using a separation kernel allows for abstraction and concealment of communications across the platform, this allows for simplified and transparent interface to service providers. Service providers include but not limited to:

- Another process
- Different partition
- Reside on a different operating system
- Reside on a different processor

Furthermore, CORBA brokers may be used in order to standardize service access across the platform.

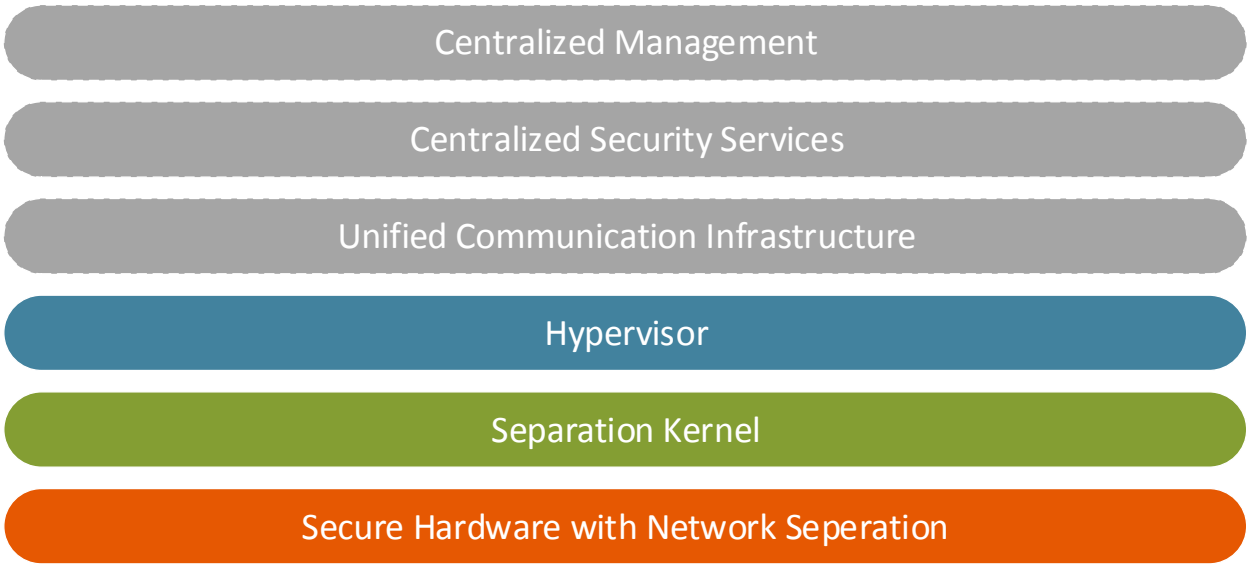

Figure 3: Services Oriented Architecture

[7] GuardKnox Distributed SOA Patent "Specially Programmed Computing Systems with Associated Devices Configured to Implement Centralized Services ECU Based on Services Oriented Architecture and Methods of Use Thereof "http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=3&f=G&l=50&co1=AND&d=PG01&s1=GuardKnox&OS=GuardKnox&RS=GuardKnox"

SOA Unique Benefits[8]:

REUSABLE CYBERSECURITY SERVICES

Including firewalls, remote server management, cryptography or the Communication Lockdown framework

INCREASED CONNECTIVITY

Hosting services and downloadable applications for customization

NEW REVENUE STREAMS

Supporting an app store [9] for downloadable personalized apps and features

SCALABILITY

Flexible hardware architecture for future unforeseen needs and data requirements

INTEROPERABILITY

Ability to host and communicate with all operating systems, whether mission critical or not and containing the failure of a single app/service so that others are unaffected.

Hardware – physical separation of safety critical networks in distributed environment

At the core of the hardware architecture is the physical separation of critical networks by isolating the communication interfaces. In order to pass data to one another, the communication interfaces have to go through a security mechanism. The platform can ensure data paths are enforced by physical means and not only by traditional software permissions. Custom IP cores can also be used and placed along those paths to further boost security assurance.

Distributed Systems: The patent on distributed systems ensures that multiple units (SNO's) within a vehicle work together in a cohesive manner in which they are not independent entities. This therefore enables multiple lockdown devices to operate together in a vehicle (e.g., internal and external ones). Since each device is only seeing a part of the network traffic, they can cooperate and exchange metadata about the traffic they see and approved/blocked. Thus, making the overall model more accurate.

[8] GuardKnox Services Oriented Architecture (SOA)https://www.guardknox.com/services-oriented-architecture-automotive-services/

[9] Goldberg, Jillian (2017,11). Turning Drivers to Subscribers. https://blog.guardknox.com/connected-vehicle-vulnerabilities-turning-drivers-to-subscribers

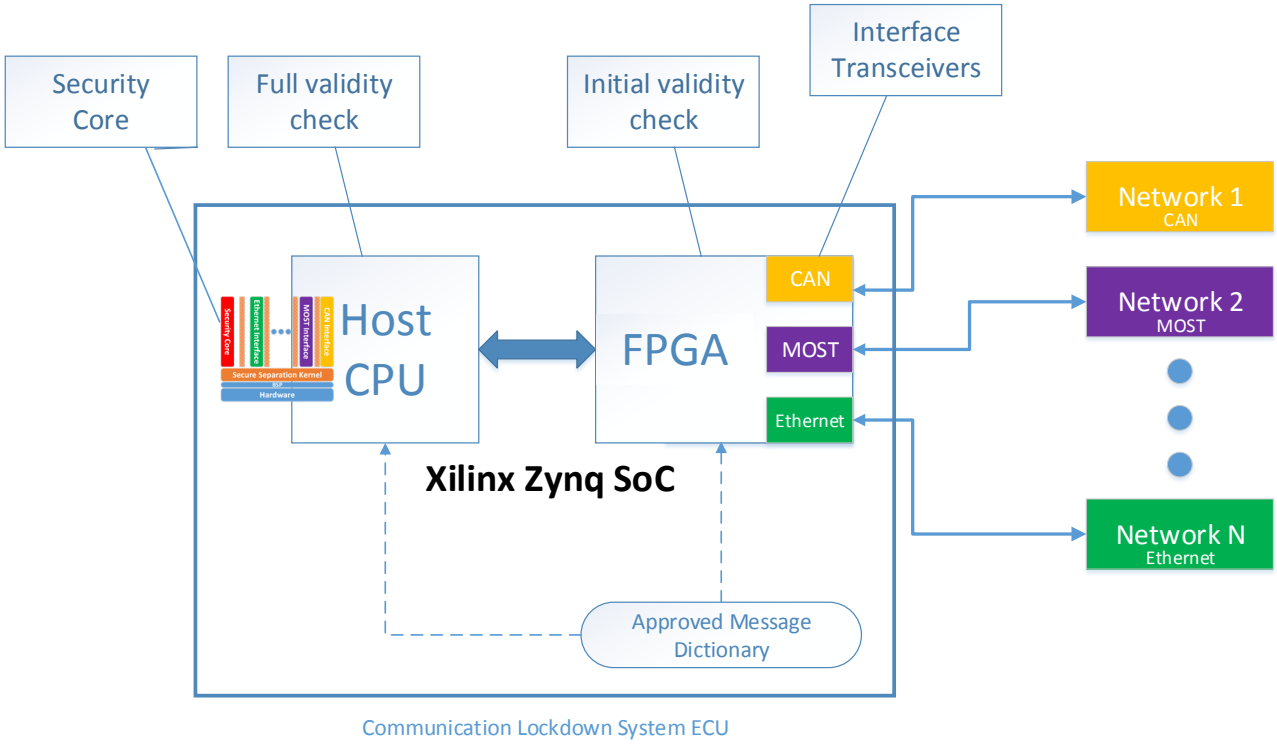

Figure 4: Communication Lockdown System ECU

Secure Updates

Secure delivery, authentication of sender and verification of data integrity, bug fixes, improved user experience as well as new functionality can be introduced safely and securely to address current and future needs, increasing the value of the product to the customer, while reducing development and integration costs.

The firmware image (both hardware and software) can be encrypted and signed at the vendor's site and delivered to devices securely at all times and by any means.

Xilinx Zynq SoC decrypts and authenticates the firmware image prior or during first boot ensuring no unauthorized hardware configuration or software can be loaded and executed on the device.

Role of Data Analytics and Machine Learning

Utilizing FPGA has other performance related benefits as well, advance Artificial Intelligence (AI) and analytics can be implemented in hardware.

Preprocessing can be done on the endpoint (in this case the G platform SNO™) in order to save bandwidth by offloading and distilling data to only what is necessary for the cloud application.

The platform also enables secure end-to-end connection to a cloud infrastructure. Afterwards, the cloud can be used for use cases such:

- Predictive Maintenance
- Fleet health monitoring

Xilinx Programmable Technology

Flexibility and scalability are key advantages that programmable technology provides. Zynq programmable SoC and FPGA technology includes dedicated automotive, and mil qualified device families. These support a wide variety of industry standard interfaces for interoperability with other devices, including virtually any type and combination of interfaces through use of the programmable fabric and configurable IO. In the context of security and flexibility, security accelerators can be implemented in the programmable logic. Cryptography can be managed with keys embedded in hardware (also creating secure memory from FPGA) and further enhanced using the integrated Physical Unclonable Function (PUF) technology in the Zynq MPSoC family of devices[10].From an isolation point of view, true hardware separation is utilized – where the communication interfaces can be passed through security mechanism(s), such as watchdogs, isolation of data and control paths and other mechanisms in order to pass data to one another.

Additionally, a certifiable methodology for isolation of separate areas on a single device can be achieved through use of Isolation Design Flow (IDF) and Vivado® Isolation Verifier (VIV) / Isolation Verification Tools (IVT). Designs placed into these regions are physically isolated. The areas can be changed at any time without impacting other isolated regions.

System responsibility can be distributed between the processing system (i.e., software) and the programmable logic (i.e., hardware). Unique to programmable technology, both the software and the hardware can be reconfigured, either in total or partially (with DFX during runtime), utilizing the reconfigurable nature of the device. This essentially provides new functionality and updates to existing functionality via OTA SW and OTA Silicon, including systems already deployed in-field.

Application	Standard
Automotive	ISO 26262
Industrial and Medical	IEC 61508, IEC 62061 and IEC 13849
Aerospace & Defense	DO-254/DO178b

Table 2: Functional Safety Standards

Functional Safety Standards Supported

Security and Functional Safety should be designed in from the start.

[10] Physical Unclonable Function (PUF) technology in the Zynq MPSoC family of devices: https://scholar.uwindsor.ca/cgi/viewcontent.cgi?article=8596&context=etd

System Features

The Zynq MP SoC architecture (Figure 5) includes a high bandwidth interconnect between the Processing System, Programmable Logic allows for tight integration and flexible partitioning between both hardware and software.

Optimization of algorithms running on the processing system can be achieved by offloading and accelerating the algorithms using the inherent parallelism of the programmable logic fabric while providing the processing power scalability and flexibility essential for these programmable platforms across the Zynq SOC device family.

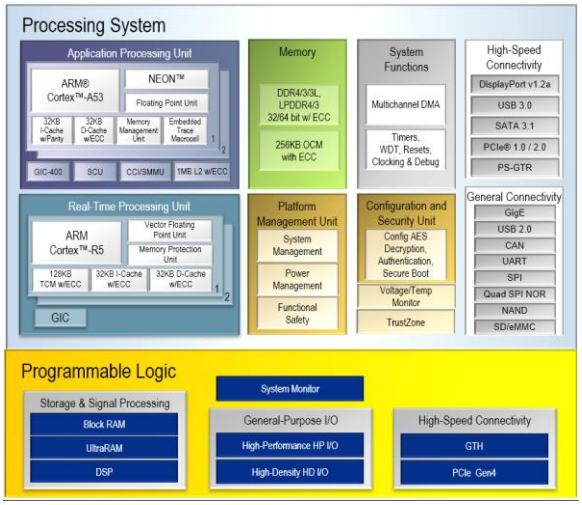

Figure 5: Zynq US+ MPSoC Partitioning: Processing System and Programable Logic

Scalability of the processing system and soft processor instantiations or programmable accelerators implemented in the programmable logic can be applied where required.

Extending this compute capability, is the focus on Machine Learning and AI Engines[11]. Optimized resource and power efficient neural networks can be implemented in the Programmable Logic to augment compute in Automotive solutions [12] and other applications and markets.

Future Direction

The Communication Lockdown methodology as described in this article extends beyond the automotive industry and is applicable to any kind of closed system. This includes but is not limited to

- Industry 4.0
- Smart-grid applications
- Critical infrastructure
- Medical devices.

In addition, GuardKnox is an active member of the *ISO/SAE joint working group, ISO-TC22-SC32-WG11.* This working group's mission is to create a new standard, ISO-SAE 21434: Road vehicles – Cybersecurity Engineering[13].

[11] Xilinx AI Engines and Their Applications https://www.xilinx.com/support/documentation/white_papers/wp506-ai-engine.pdf

[12] Power efficient neural networks Augmenting compute in Automotive solutions: https://www.itu.int/en/journal/001/Documents/itu2017-2.pdf

[13] Goldberg, Jillian (2018, 04) Setting the Standard for Automotive Cybersecurity https://blog.guardknox.com/setting-standard-automotive-cyber-security

- Return to IIC Journal of Innovation landing page for more articles and past editions.