Darren Shelcusky

Senior Consultant

Product Cybersecurity

4-Jun-2024

Security Use Cases for Software Defined Vehicles (SDVs)

SDVs rely heavily on software and electronics to manage and control many vehicle features

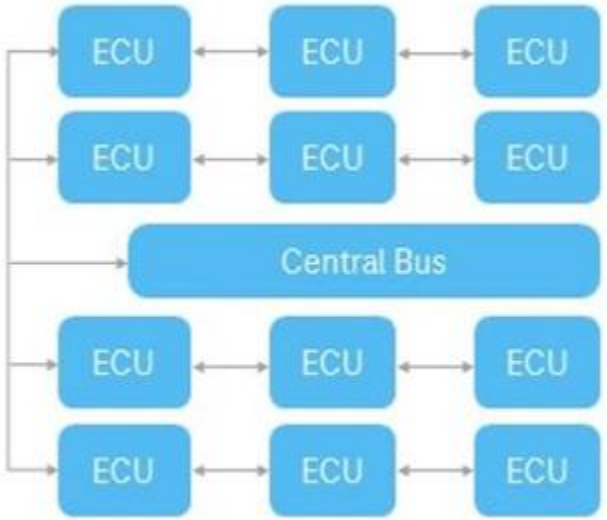
What Are Software Defined Vehicles (SDVs)?

- An overused **buzzword**
- Provides the capability to
  - Introduce new vehicle and consumer features
  - Update existing features
  - Evolve a vehicle during its lifetime
- Have two key elements
  - Software running in the vehicle and connected ecosystem
  - The underlying tech stack and architecture

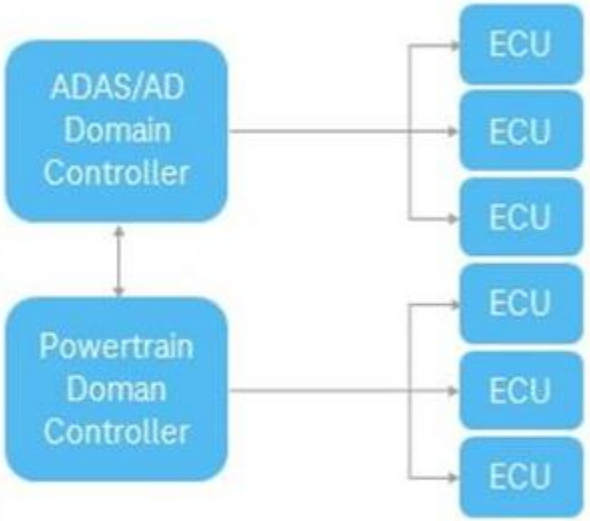
A software-defined vehicle can be improved by software updates as opposed to changing physical parts

Evolving In-Vehicle Architectures

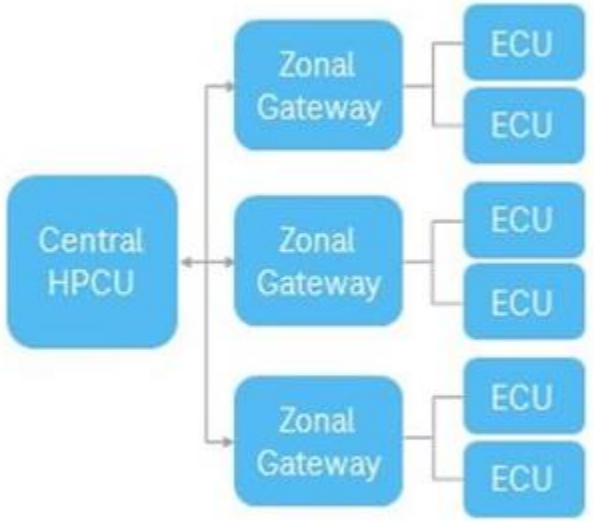
Distributed



Domains



Centralized



Many erroneously view the centralized computing architecture as the only valid SDV architecture

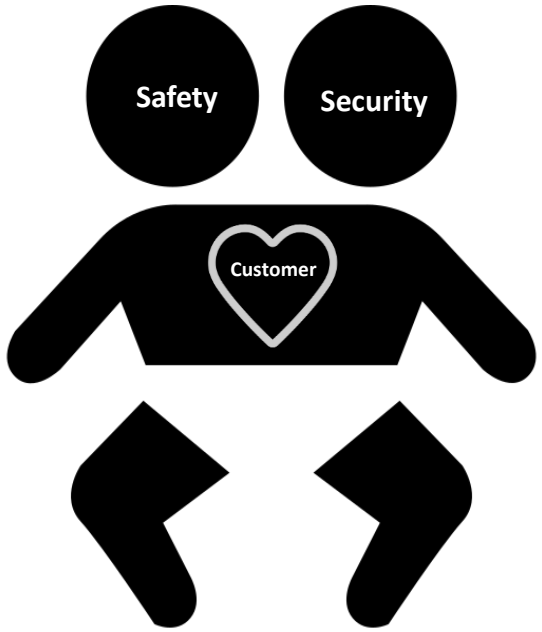
All of these architectures exist today and must be addressed

Use Case - Secrets Management

- **Secrets management** is foundational in increasing the security of software-defined vehicles
- During vehicle **manufacturing and servicing** various cryptographic keys and secrets are generated and programmed into different vehicle components
- These secrets play a vital role in securing a vehicles software and communication channels

HSM's safeguard vehicle systems with various cryptographic technologies

Use Case - Safety and Security

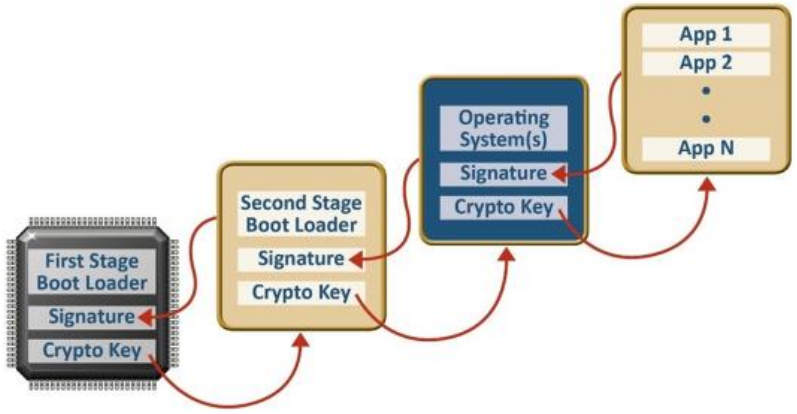


Safety and security are like conjoined twins that share a single heart who cannot be separated

- Protecting a vehicle's software from cyber threats is crucial and **requires continuous updates** and vigilance from OEMs and service providers
- Security employs a preventative approach, which is required for the **ongoing assurance of vehicle safety during its lifetime**

Safety and security must be preserved in SDVs as features become primarily software-defined

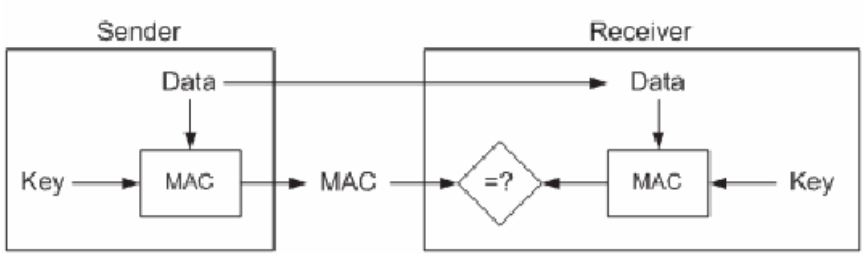
Use Case – Authentic Software



- Secure boot provides **detection of inauthentic software** when booting a vehicle ECU
- Secure boot addresses these questions
  - "How do I know the software is authentic?"
  - "How do I know the software is unaltered?"
- Secure boot requires a root-of-trust or a trust anchor which is rooted in an immutable part of the ECU hardware
- Secure Boot requires a **secure development process**, if your software signing keys leak then someone can sign their software using the key stored in the SDV

Secure boot is a foundational technology in SDVs

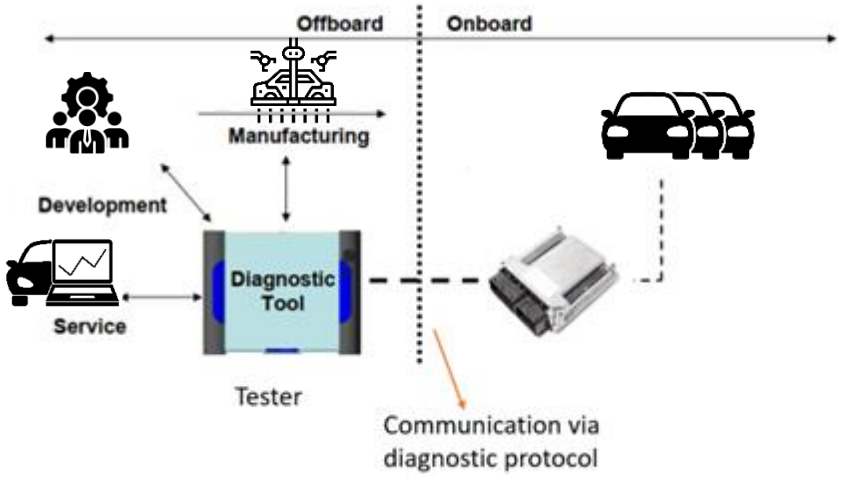
Use Case – Secure Data Transmission



- Secure messaging is an approach designed to **protect sensitive data**
- Message authentication ensures that the transmitted data **has not been tampered with**
- This includes both off board and on-board messages
- SDVs rely on networks for communication and updates and **network security is crucial**

Secure messaging is a foundational technology in SDVs

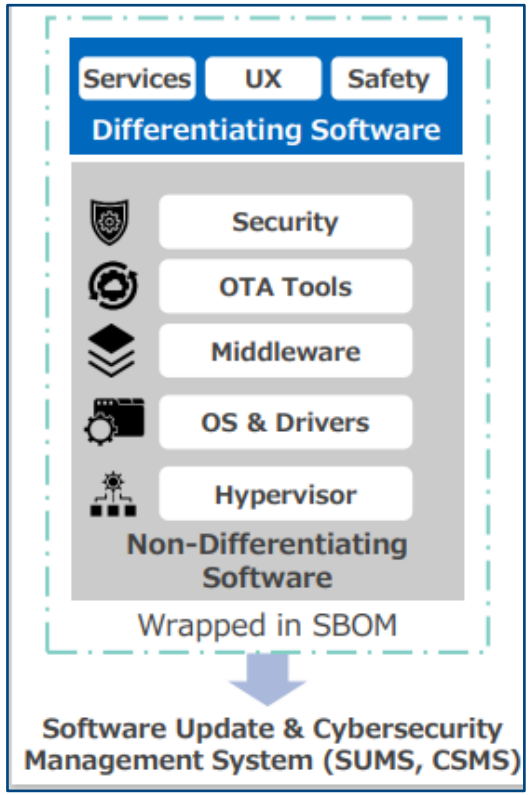
Use Case – Secure Vehicle Servicing



- **Unified Diagnostics Service 29** includes bidirectional authentication with **PKI-based Certificate Exchange** providing a standardized method for secure communication and access control within automotive ECUs
- This advanced software and electronics **can make repairs more complex and costly**
- Zero Trust security model ensures that **access is exclusively given** to authorized users

UDS Service 29 is a cornerstone for ensuring secure access to vehicle diagnostics and servicing capabilities

Use Case: SBOMS



Graphic:SBD

- SDVs are increasingly reliant on accurate SBOMs to **ensure that cybersecurity verifications were completed**
- As R156 expands to more models and regions, simplifying reuse will gain in importance
- Requires industry consortiums and tool supplier partner to optimize deployment of SBOM processes and solutions and for automotive applications

SBOMs provide a common language for communication of software content

Additional SDV Use Cases

- Remote diagnostics
- Fleet applications
- Patch security vulnerabilities
- Anomaly detection
- Update existing features
- Provision and managing secrets
- Secure messaging
- EOL testing
- Fraud prevention (counterfeit parts)

- IDPS (Intrusion Detection and prevention)
- Apps and content streaming in infotainment systems
- Emergency services
- HD maps with linked context for autonomous driving
- Electric vehicles services
- Personalization and user experience
- Energy Management

Most automotive innovations rely heavily on software

Where Are SDVs Driving the Industry?

- Move to **zero trust architectures** where everything is untrusted, and each component verifies that others are trustworthy, and interaction operates on a **least privileged basis**
- Increased **transparency of SBOMs,** because if there is not transparency into software security then the industry is at risk
- A move towards **software/component certification**; R155 type approval today is for a vehicle type approval which includes software/components reused on many products in many markets

Thank You

Contact Information

dshelcu1@ford.com

darren.shelcusky@gmail.com

https://www.linkedin.com/in/darren-shelcusky-b215164/