MODULAR OPEN SYSTEMS APPROACH

Towards Deployment of a Zero-Trust Architecture (ZTA) for Automated Vehicles

Victor Murray, CISSP®
victor.murray@swri.org
Southwest Research Institute

Co-authors:
Scott Lathrop Ph.D., CISSP®, Raytheon BBN Technologies, Cambridge, MA
Dariusz Mikulski Ph.D., US Army DEVCOM Ground Vehicle Systems Center, Warren, MI

GVSETS GROUND VEHICLE SYSTEMS ENGINEERING & TECHNOLOGY SYMPOSIUM & MODERNIZATION UPDATE
NDIA Michigan

Agenda

- **Motivation**
- **Automated Vehicle Architecture**
  - Ground Vehicle Baseline
  - Add Control, Sensors, and Connectivity
- **Zero-Trust**
  - Introduction
  - NIST Approach – 7 tenants
  - Architecture
- **Work Completed**
  - CRASH
  - Ground Vehicles
- **Future Work and Key Takeaways**

Motivation: Automated Vehicles

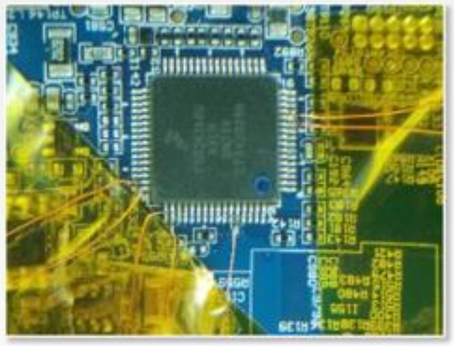
MODULAR OPEN SYSTEMS APPROACH

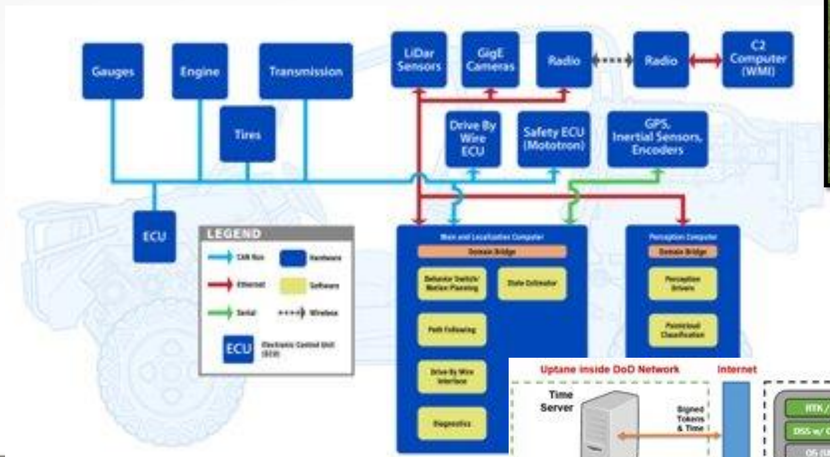
- Large AV development team
- Deployed autonomy solutions on over 20 types of vehicles

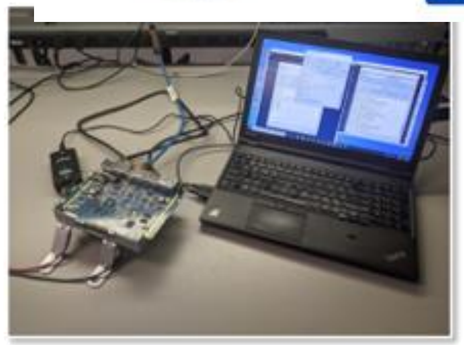
Initial focus on functionality, transitioned into deployment

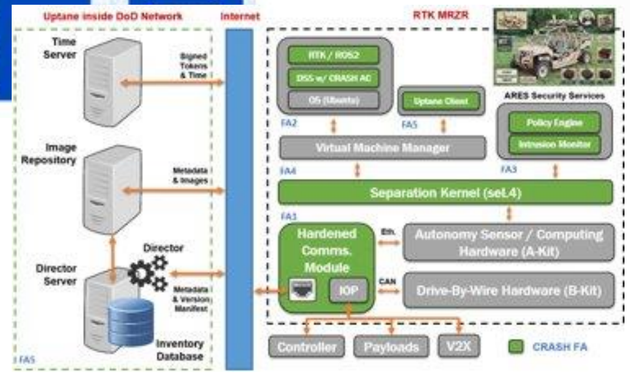
Motivation: Cybersecurity

- **Commercial Automotive (15 years)**
  - Pen Testing
  - Independent Analysis
- **AV Sensor Security**
  - Camera
  - Lidar
  - Radar
  - Ultrasonic
  - GNSS
- **Securing AV systems**
  - Software
  - Communication



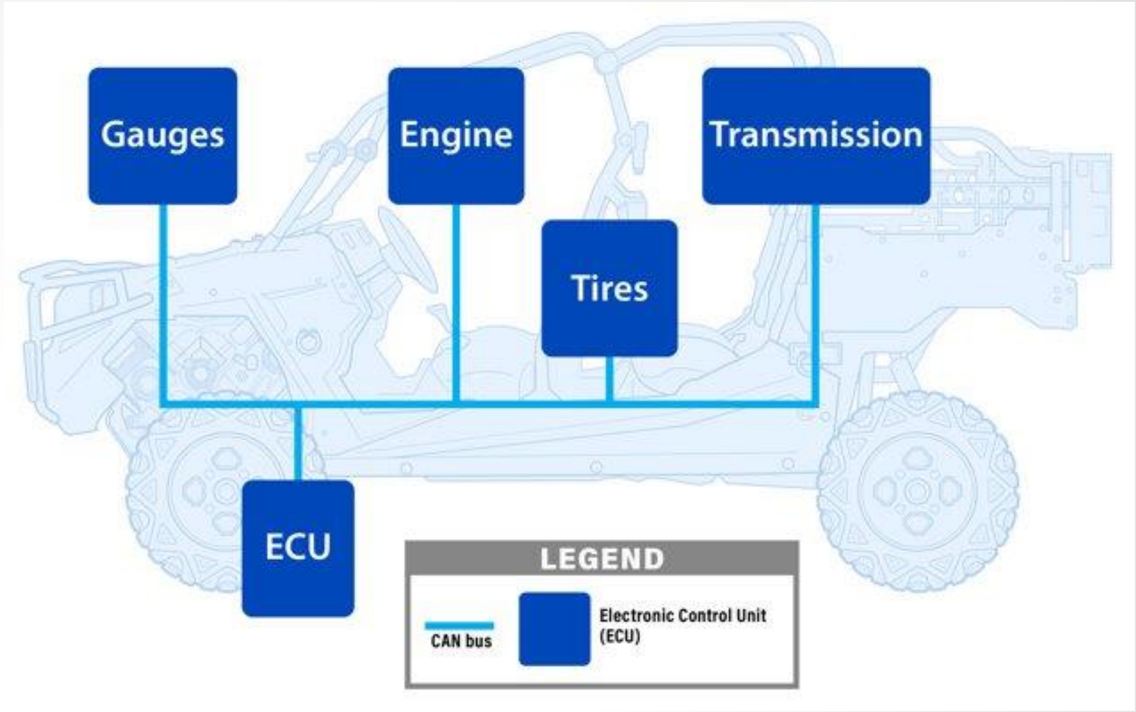






Ground Vehicle Baseline: ECU Communication

- **Controller Area Network (CAN)**
- **Local Interconnect Network (LIN)**
- **Automotive Ethernet**



Ground Vehicle Baseline ECU Network and Connections.

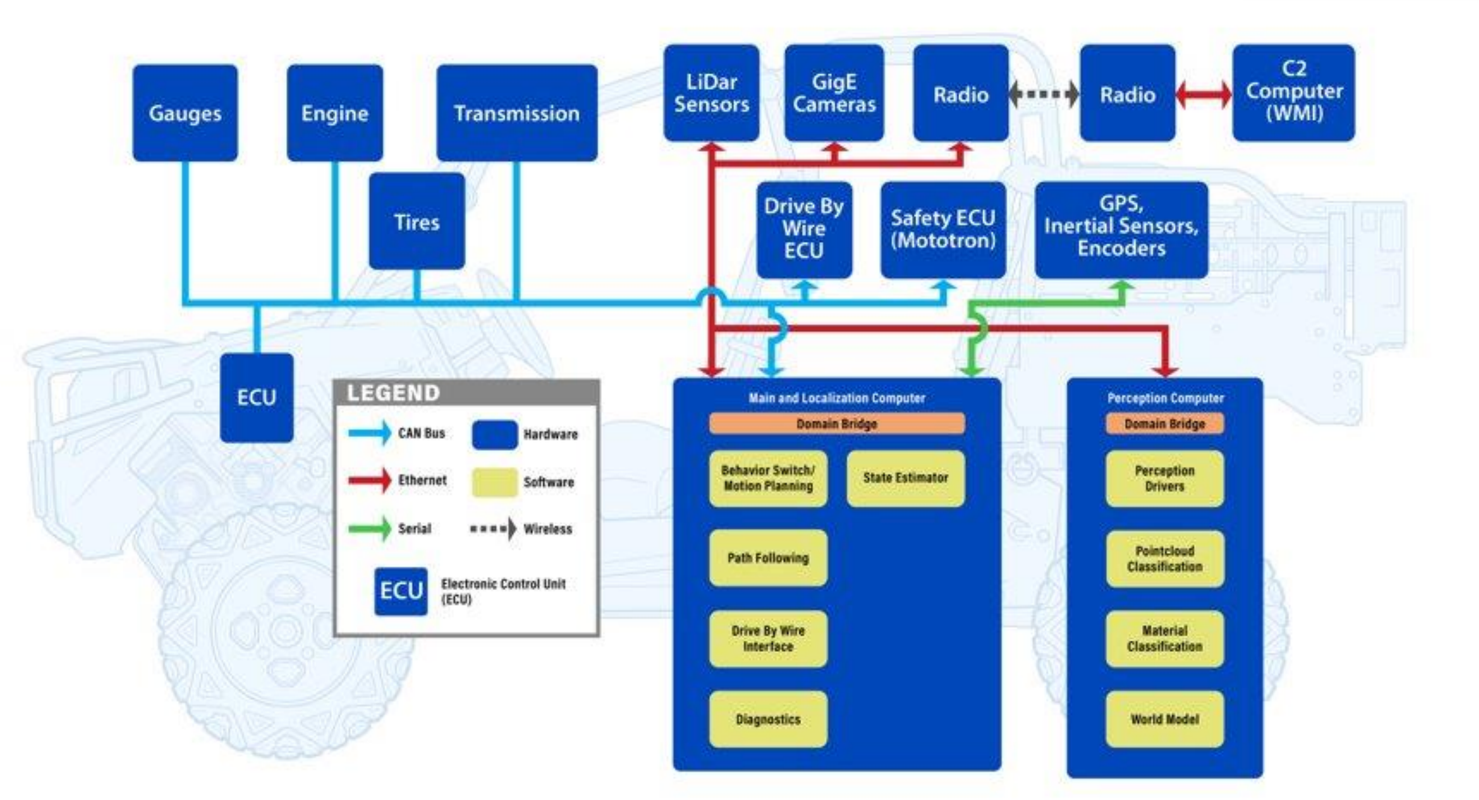
Automated Vehicles commonly built on top of non-automated vehicles

Automated Vehicle Add Ons

MODULAR OPEN SYSTEMS APPROACH

- Sensors
- Drive By Wire
- Control Computers
- Connectivity

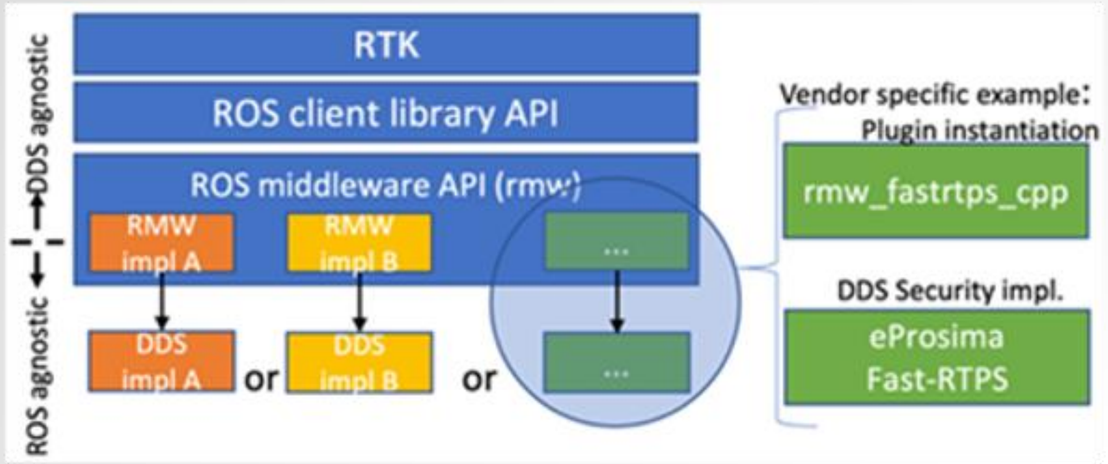
AV architecture with remote connectivity; sensors, drive-by-wire, and control computers; and ground vehicle baseline ECU



Architecture Used to Outline the ZTA for AV

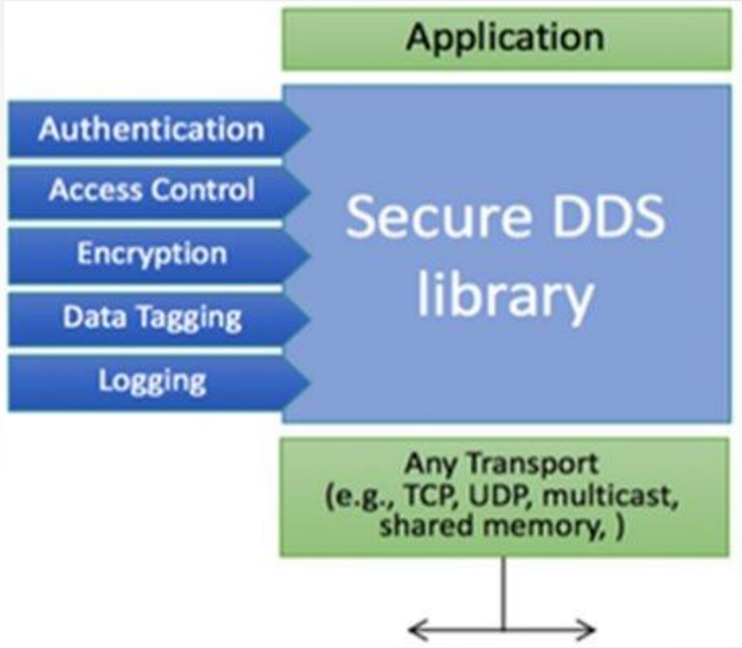
Automated Vehicle Control Software

MODULAR OPEN SYSTEMS APPROACH



In ROS2, Each DDS Provides ROS Middleware To Interface Between ROS And DDS.

- **Software Stack:**
  - Robotic Technology Kernal (RTK)
  - Robot Operating System 2 (ROS2)
  - Data Distribution Service (DDS)



DDS security layers Per OMG DDS Specification

Object Management Group, Inc. (OMG), "DDS Security Model," Object Management Group, Inc. (OMG), 2018.

Expand DDS Security

- Initial MARS work under ROS2 Foxy using CycloneDDS. Also looked at RTI Connext and FastRTPS.
- CRASH worked with ROS2 Humble and RTK23/ARCS and used both FastRTPS and CycloneDDS.
- Foxy and Humble default to FastRTPS.
- Galactic defaults to CycloneDDS.
- Turning on security for DDS was big part of CRASH.

- Zenoh is being analyzed. Not enough experience at this point.

Next: zero trust

Introduction to Zero Trust (ZT)

The National Institute of Standards and Technology (NIST) provides:

"Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. A zero trust architecture (ZTA) uses zero trust principles…. **ZT assumes there is no implicit trust** granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned)."


NIST
National Institute of Standards and Technology

NIST Special Publication 800-207

Zero Trust Architecture

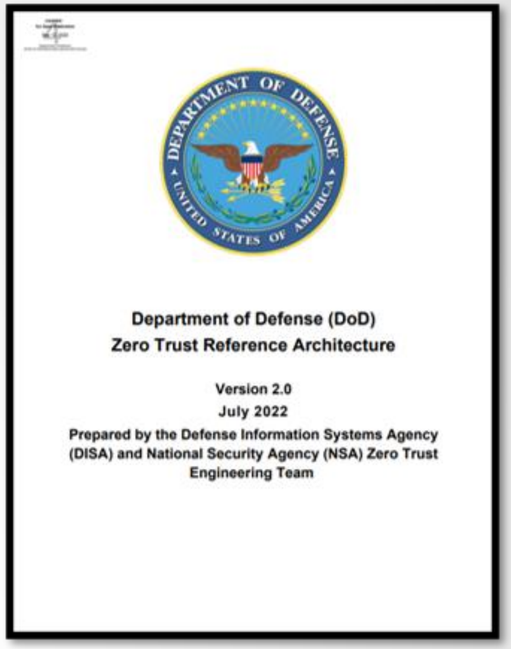
Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Assumes attacker already has access to your network


Department of Defense (DoD)
Zero Trust Reference Architecture

Version 2.0
July 2022
Prepared by the Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team

ZT commonly seen in company networks as requiring authentication for access to network assets

Authentication

Ethernet Communication

Authentication via DDS Security

CAN bus and Serial Communication

Authentication via Secure Onboard Communication (SecOC)

Wireless Communication

Authentication via Secure Shell (SSH)

Secure Boot and Software Validation

Authentication using Hashing Algorithms SHA-2 or SHA-3

Key Distribution, Management, and Revocation

Supports Secure Implementation of Authentication

NIST's 7 Tenets of Zero Trust

Tenet 1:

- **All data sources and computing services are considered resources.**

Tenet 2:

- **All communication is secured regardless of network location.**

Tenet 3:

- **Access to individual enterprise resources is granted on a per-session basis.**

Tenet 4:

- Access to resources is determined by dynamic policy...

Tenet 5:

- The enterprise monitors and measures the integrity and security posture of all owned and associated assets.

Tenet 6:

- **All resource authentication and authorization are dynamic and strictly enforced before access is allowed.**

Tenet 7:

- The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.

Monitoring and Policy Enforcement Engine

Network Monitoring

- ZTA networks are monitored by the Gateway to ensure devices maintain ZT policy compliance.

Clearly defines:

- Network users (subjects) and resources (topics and data sources).
- Allowed network traffic including packet info, who sends it, who receives it, and allowable bounds as applicable.

Tenet 1:
- All data sources and computing services are considered resources.

Tenet 2:
- All communication is secured regardless of network location.

Tenet 3:
- Access to individual enterprise resources is granted on a per-session basis.

Tenet 4:
- **Access to resources is determined by dynamic policy...**

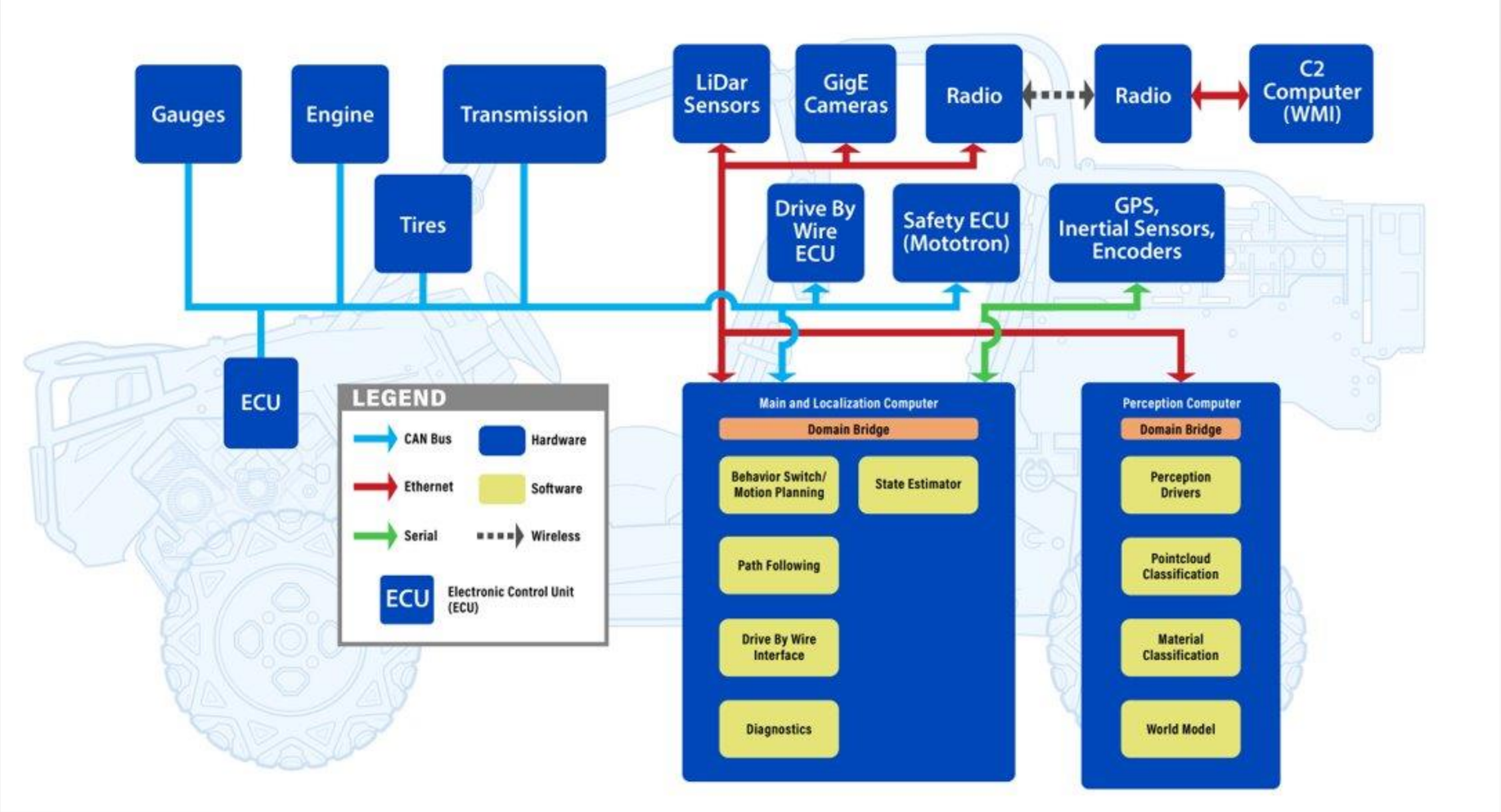
Tenet 5:
- **The enterprise monitors and measures the integrity and security posture of all owned and associated assets.**

Tenet 6:
- All resource authentication and authorization are dynamic and strictly enforced before access is allowed.

Tenet 7:
- **The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.**

Automated Vehicle

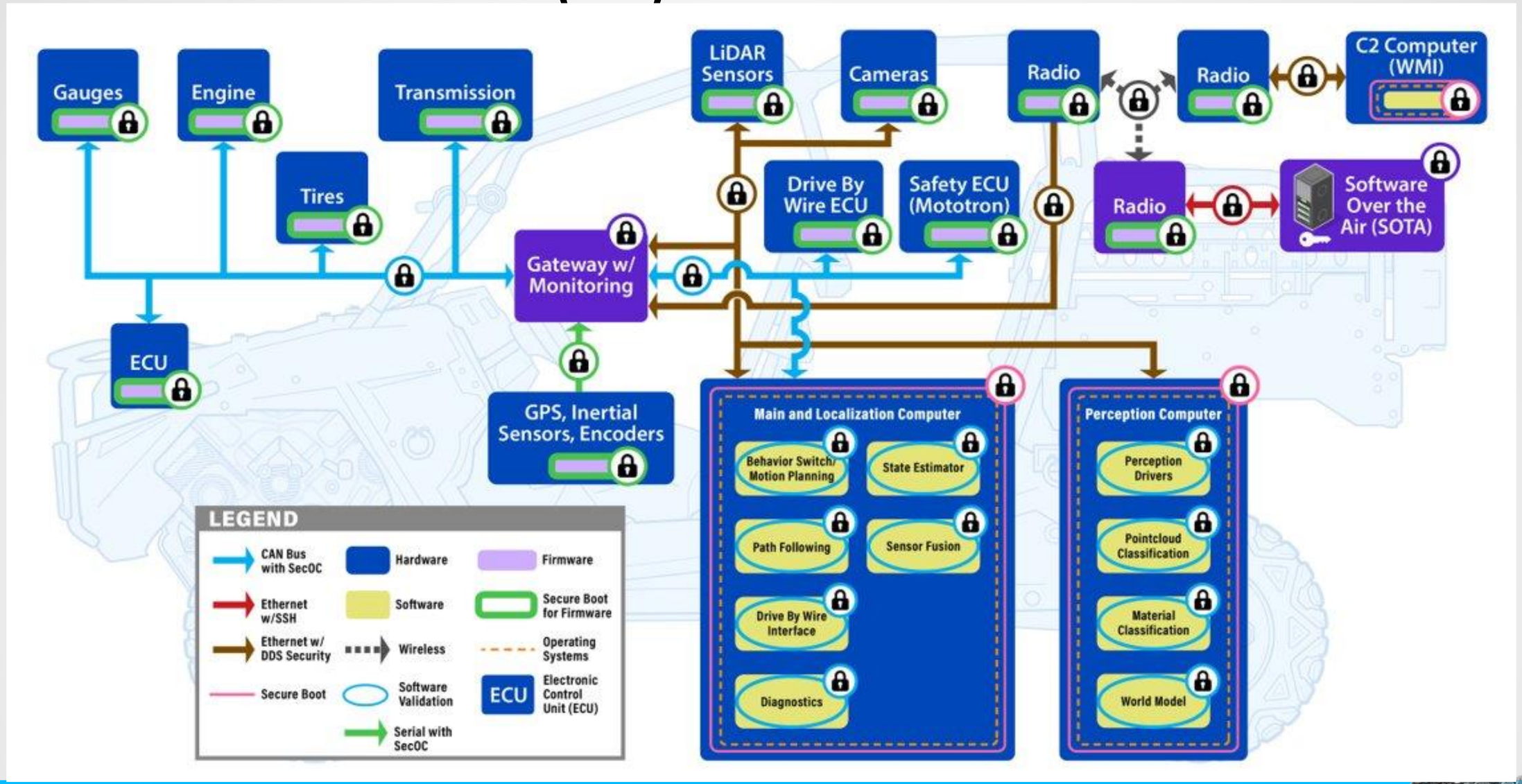
MODULAR OPEN SYSTEMS APPROACH



AV architecture with remote connectivity; sensors, drive-by-wire, and control computers; and ground vehicle baseline ECU. This architecture is used to outline the ZTA for AV.

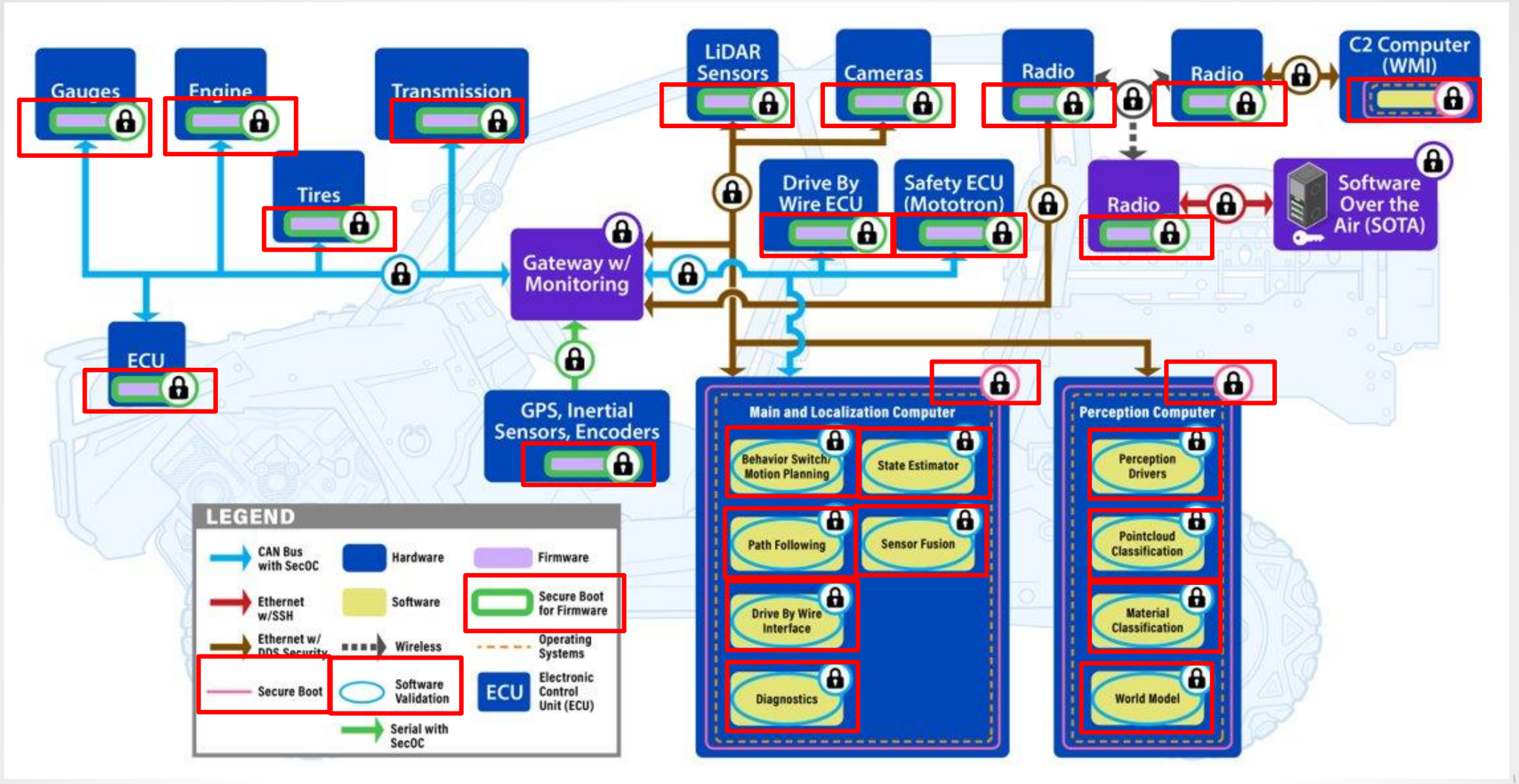
Zero Trust Architecture (ZTA) for Automated Vehicles (AV)

MODULAR OPEN SYSTEMS APPROACH



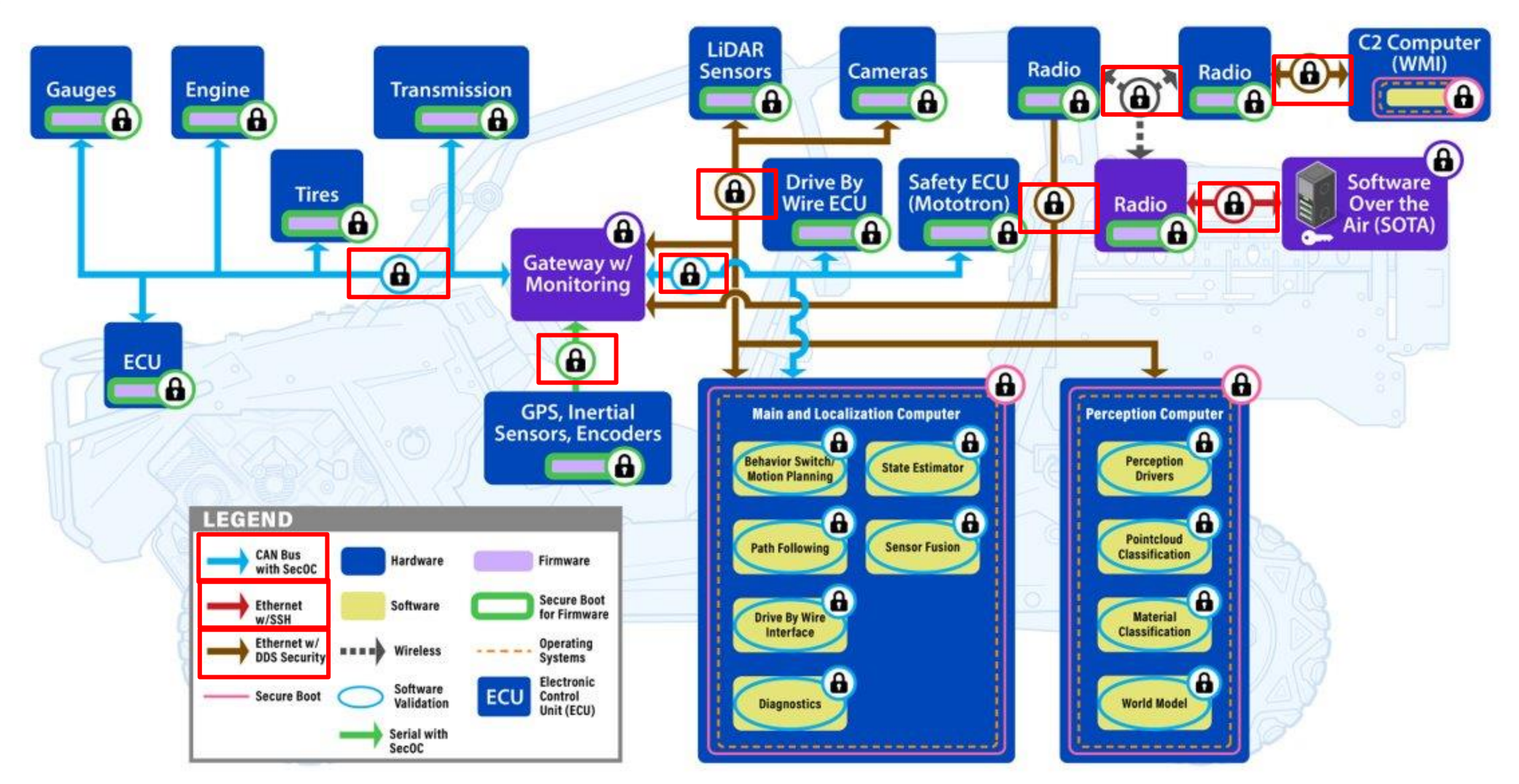
ZTA for AV-Authentication of Software and Firmware

MODULAR OPEN SYSTEMS APPROACH



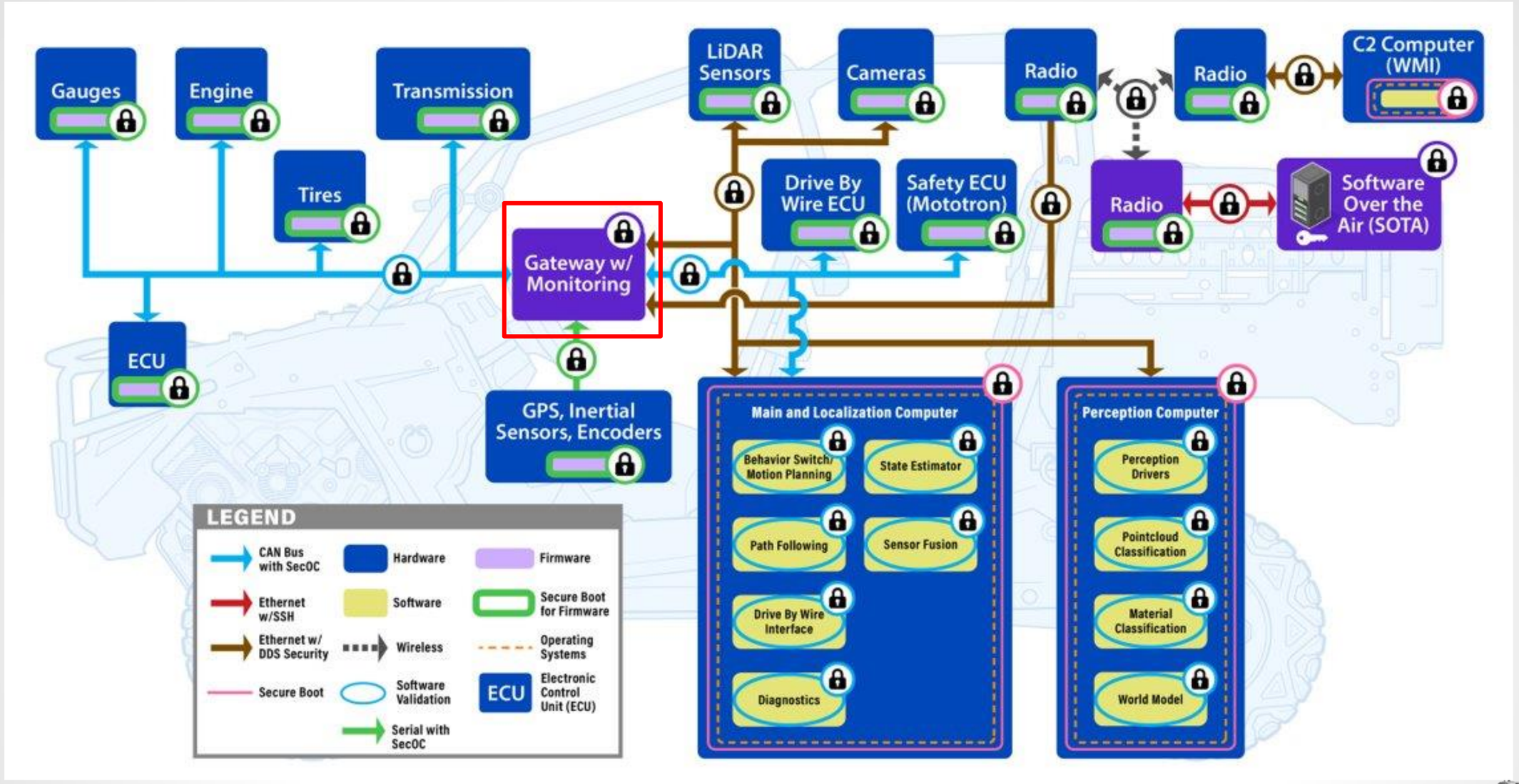
ZTA for AV-Authentication of Network Communication

MODULAR OPEN SYSTEMS APPROACH



ZTA for AV-Monitoring and Policy Enforcement

MODULAR OPEN SYSTEMS APPROACH



Current State of ZTA

Many pieces implemented in varying degrees.

Highlight two projects: CRASH and Ground Vehicle

Implementing Zero Trust on CRASH

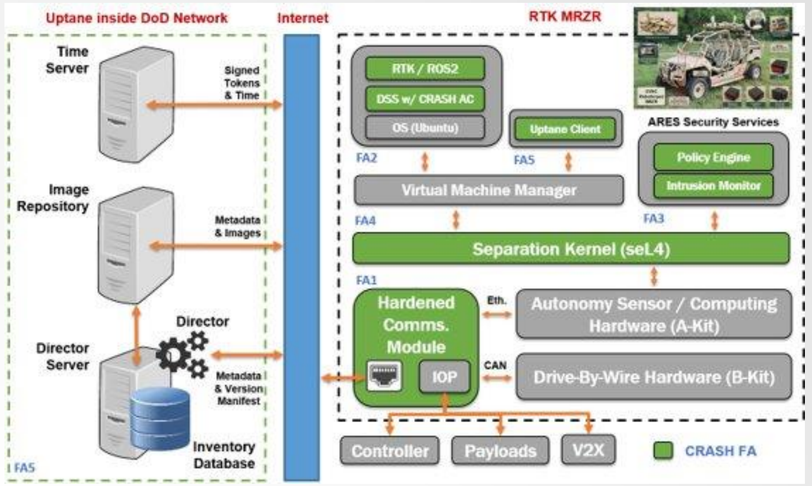
MODULAR OPEN SYSTEMS APPROACH

CRASH's Five Focus Areas:

1. Hardened Communication Interfaces
2. ★ Robust Access Control
3. Anomaly Detection Engine
4. Secure-RTK on seL4
5. ★ Secure Software Update

```
<?xml version="1.0" encoding="UTF-8"?>
<policy version="0.2.0"
 xmlns:xi="http://www.w3.org/2001/XInclude">
 <enclaves>
  <enclave path="/lesson_4/gui_monitor">
   <profiles>
    <profile ns="/cyber_training" node="gui_monitor">
     <xi:include href="common/node.xml"
      xpointer="xpointer(/profile/*)"/>
     <topics subscribe="ALLOW">
      <topic>planner_command</topic>
      <topic>planner_pose</topic>
     </topics>
    </profile>
   </profiles>
  </enclave>
 </enclaves>
</policy>
```

Example DDS Security Access Control Policy



Overview of five (5) focus areas (FA) for CRASH

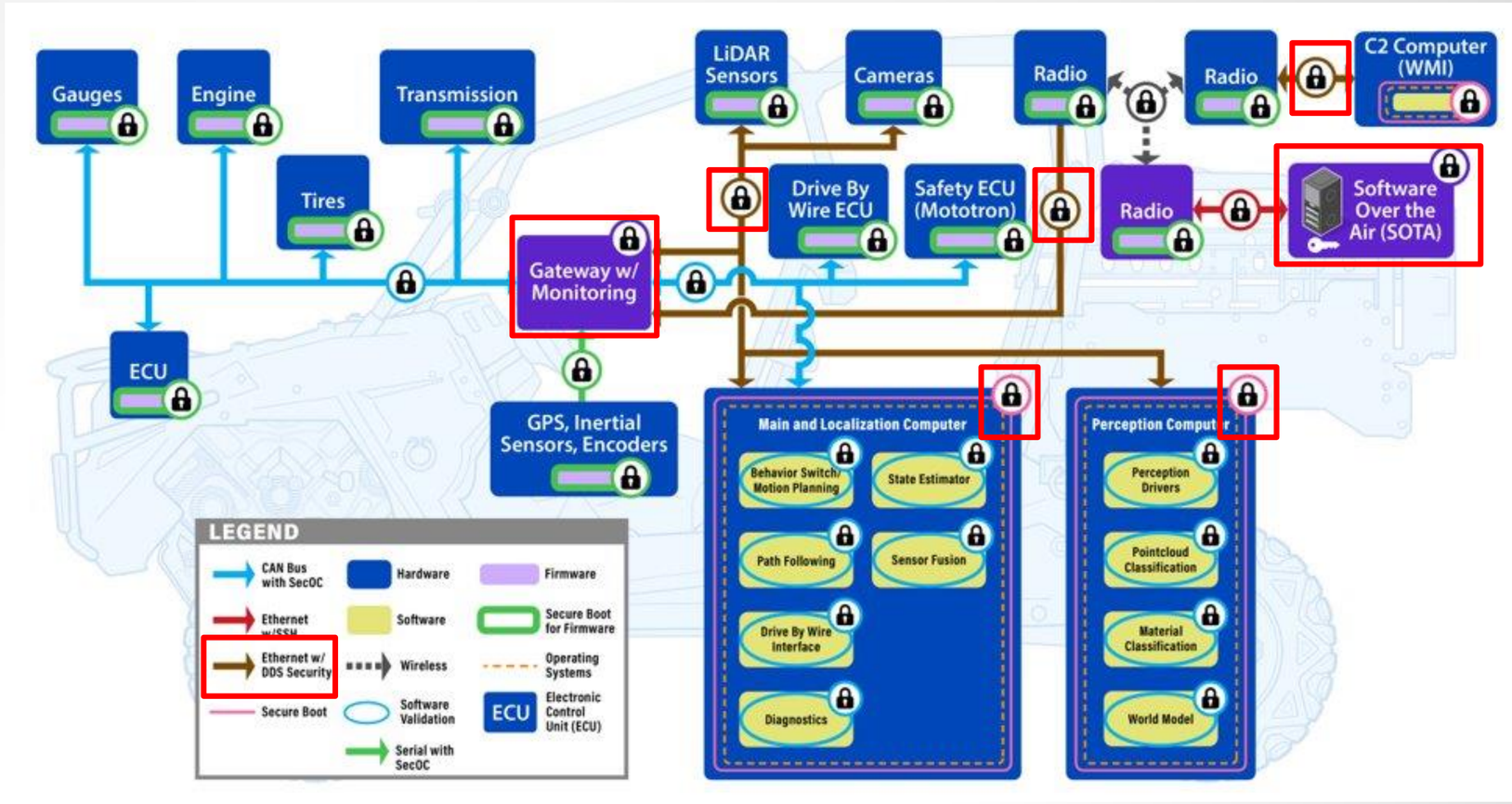
Secure Software Updates & Market Roles

CRASH Progress Towards ZTA

MODULAR OPEN SYSTEMS APPROACH

CRASH's Five Focus Areas:

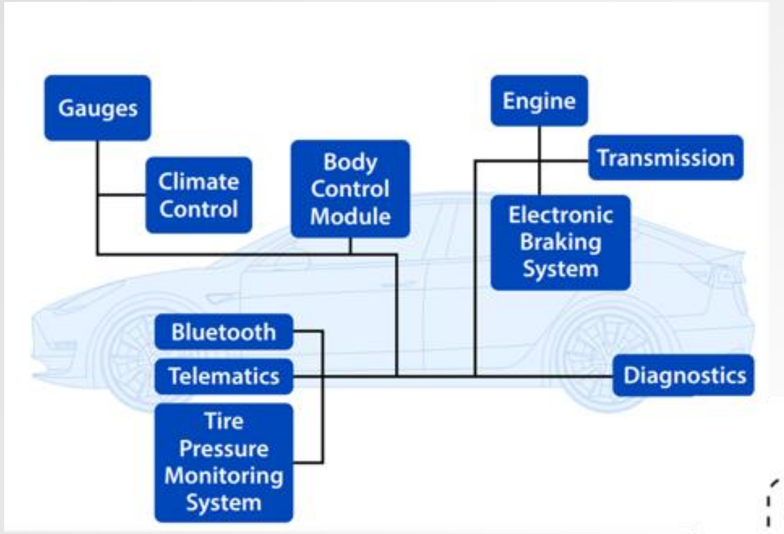
1. Hardened Communication Interfaces
2. Robust Access Control
3. Anomaly Detection Engine
4. Secure-RTK on seL4
5. Secure Software Update



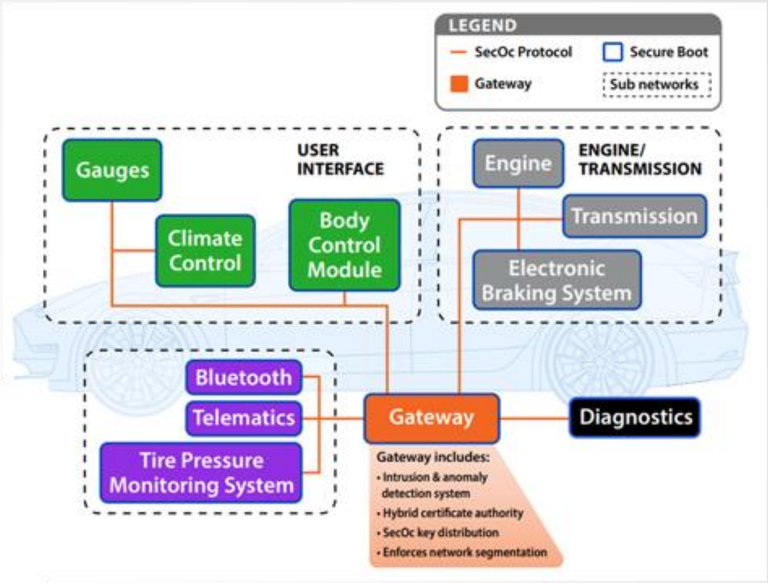
Next: ZT for Ground Vehicles

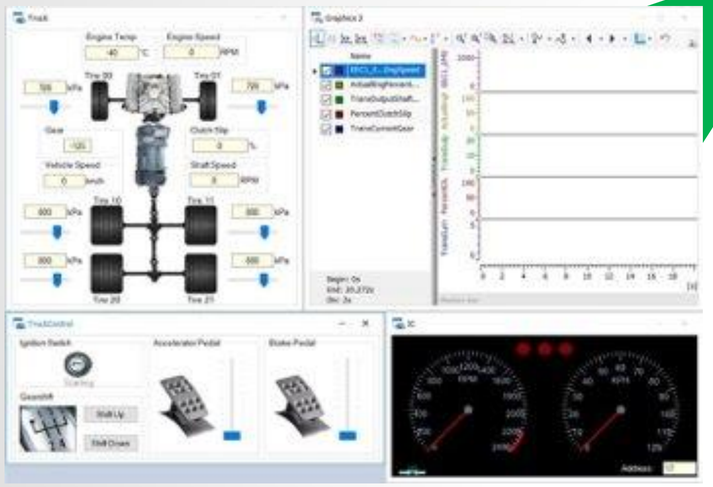
Zero Trust for Ground Vehicles

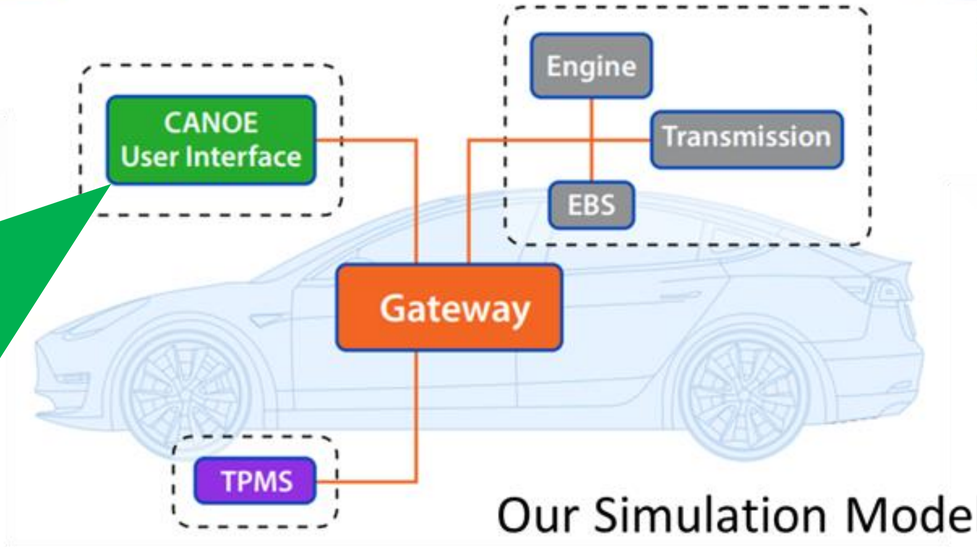
MODULAR OPEN SYSTEMS APPROACH



Zero Trust





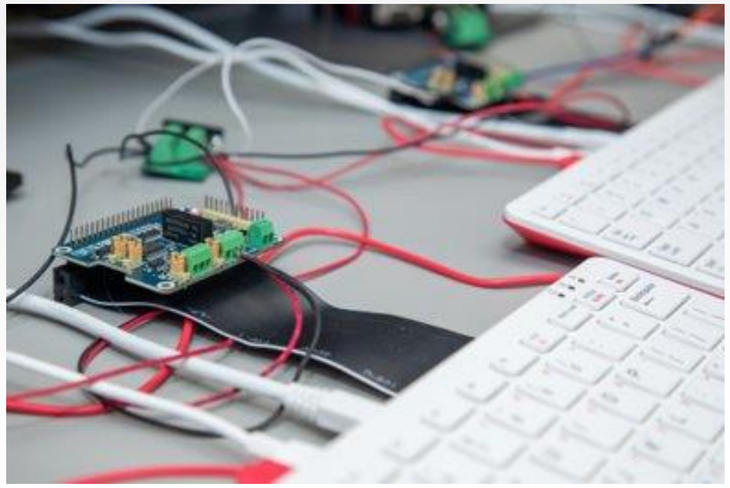


Our Simulation Model

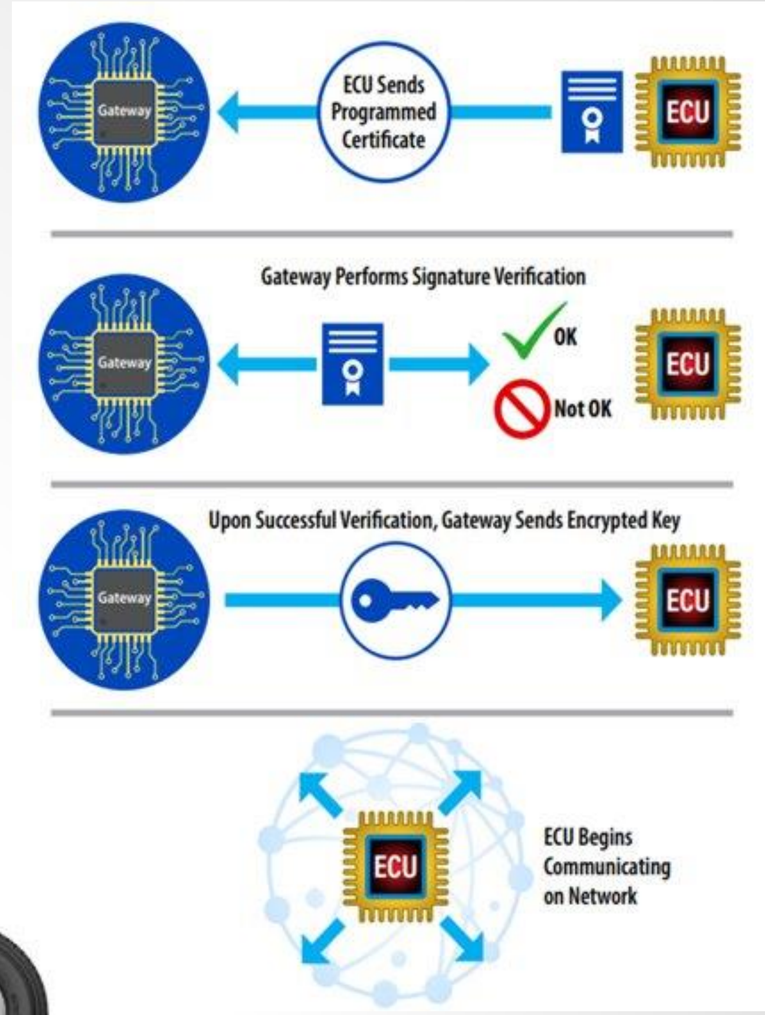
Ground Vehicle: ZTA Components

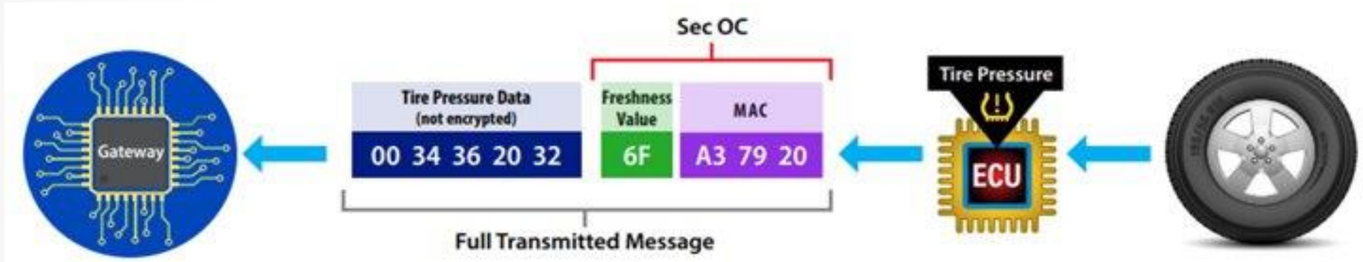
MODULAR OPEN SYSTEMS APPROACH

- **Secure Boot**
  - Digital Signature
  - Public Key
  - Verified at power on
  - SecOC public/private key



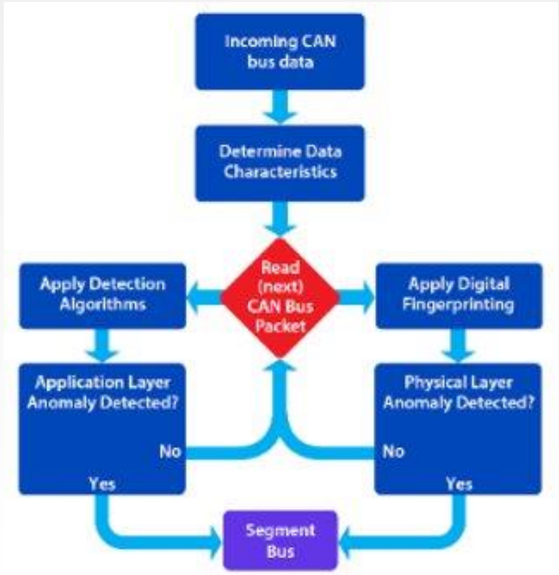
- **AUTOSAR SecOC**
  - Secure Onboard Communication
  - MAC using AES
  - Freshness Value
  - Public/Private Key for dynamically sharing AES key (in progress).

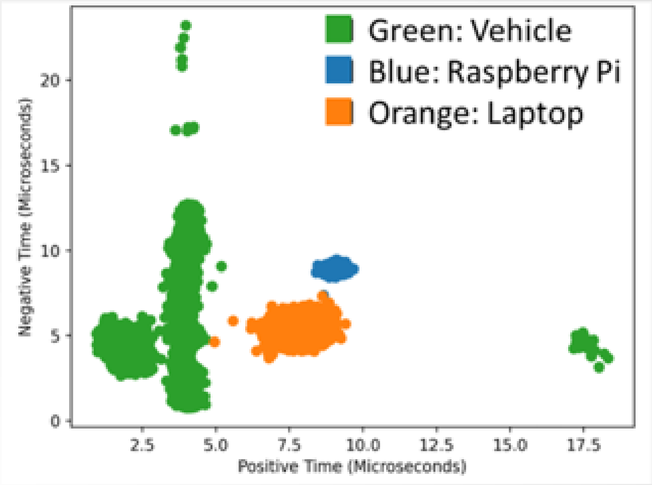


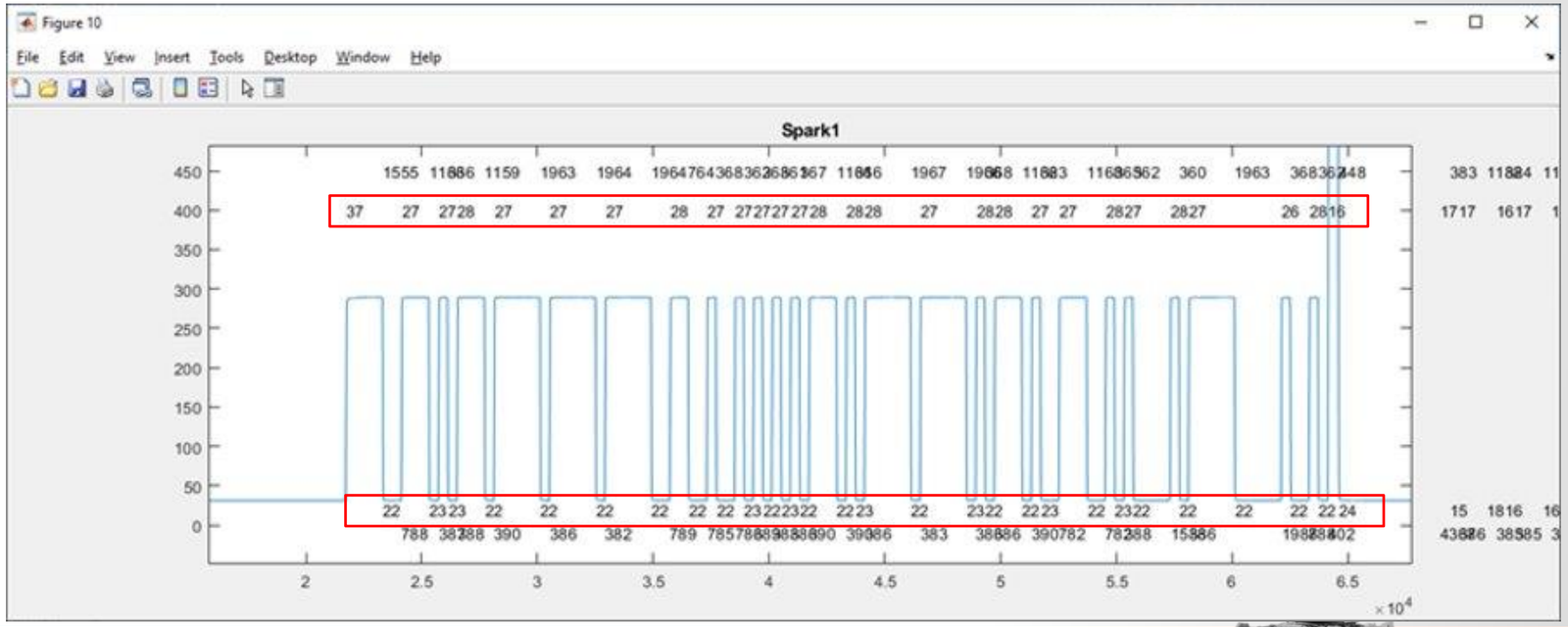


Ground Vehicle: Monitoring

- **Anomaly Detection**
  - Monitor MAC error codes
    - Receiving ECUs report errors
    - Gateway logs
  - Packet Monitoring
    - Signature-based: Uses characteristics of previously identified malicious packets to uncover anomalies
    - Anomaly-based: Examines behavioral characteristics of traffic
  - Physical Layer Monitoring

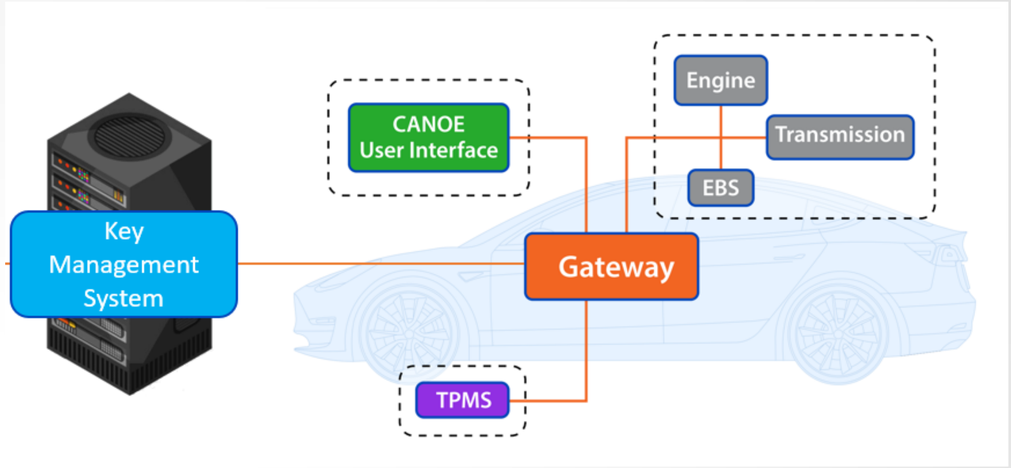




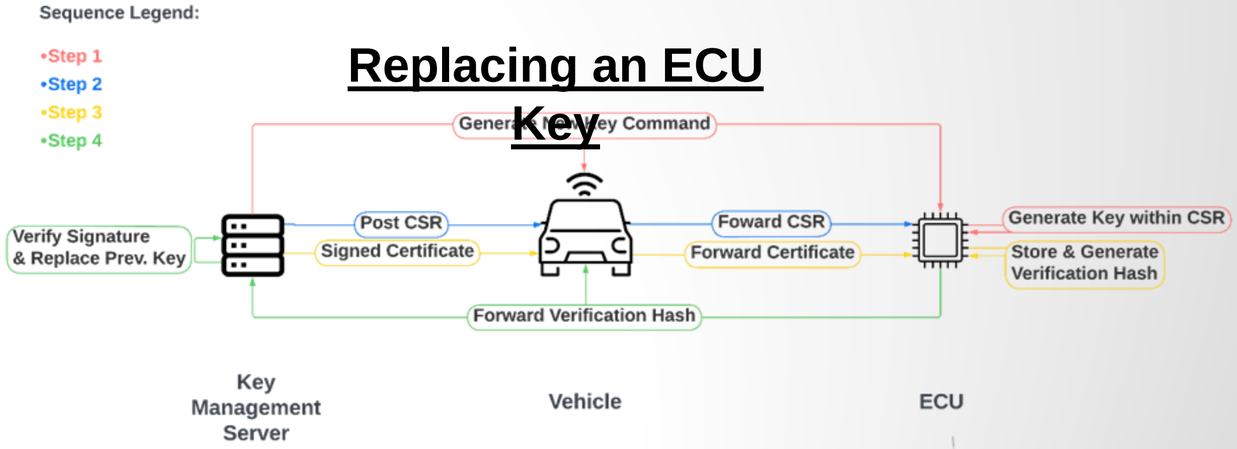


Internal Research:
Key Management for Embedded Systems

- Key management involves:
  - Secure generation
  - Authentication
  - Exchanging
  - Storing
  - Replacing
  - Terminating keys

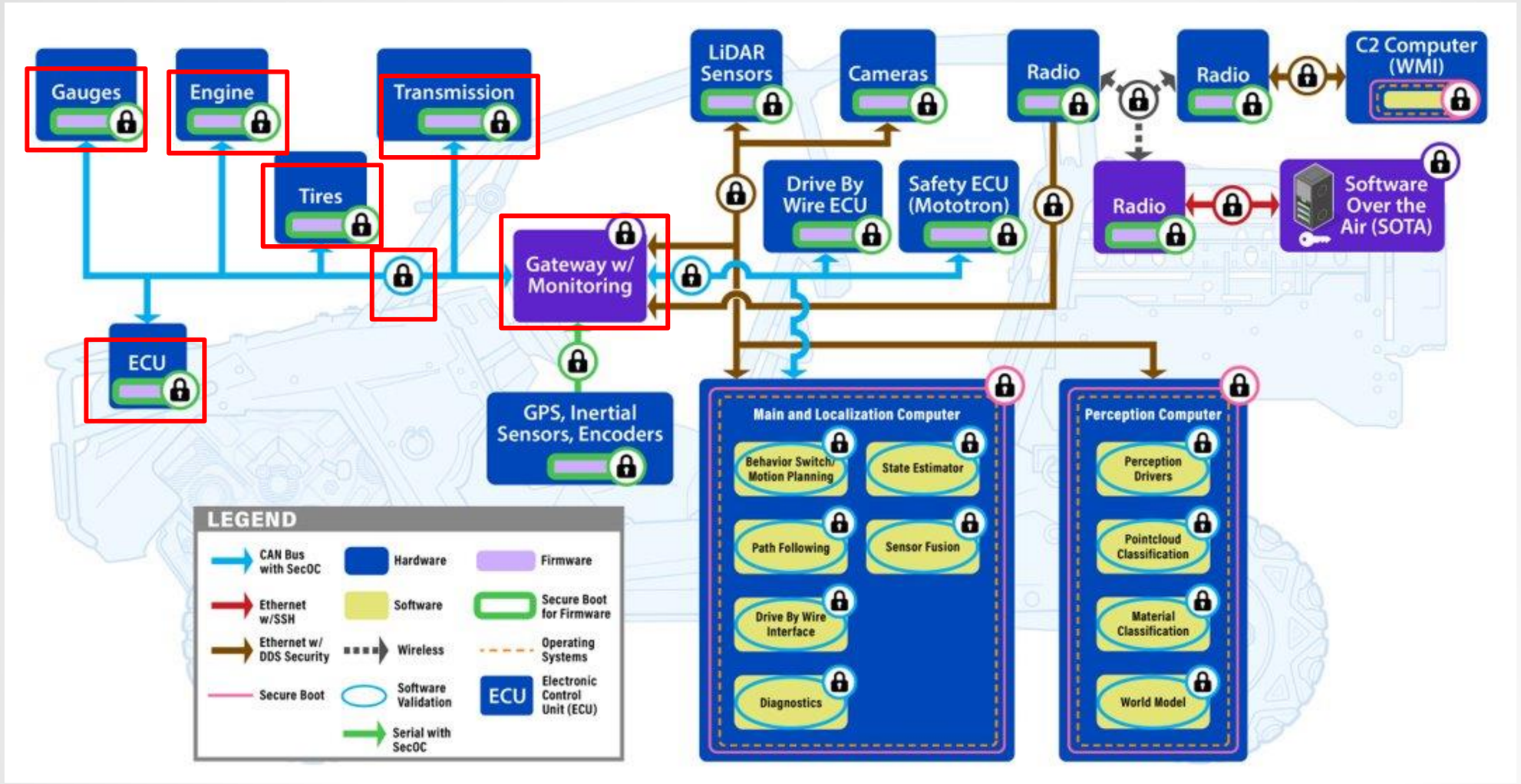


- Research highlights:
  - Key management administrator dashboard
  - Integration with Hardware Security Module (HSM)
  - Integration with Secure On-Board Communication (SecOC) and Uptane Secure OTA Updates



Ground Vehicle

MODULAR OPEN SYSTEMS APPROACH



Next: Future work

Future Work

Authentication Updates:

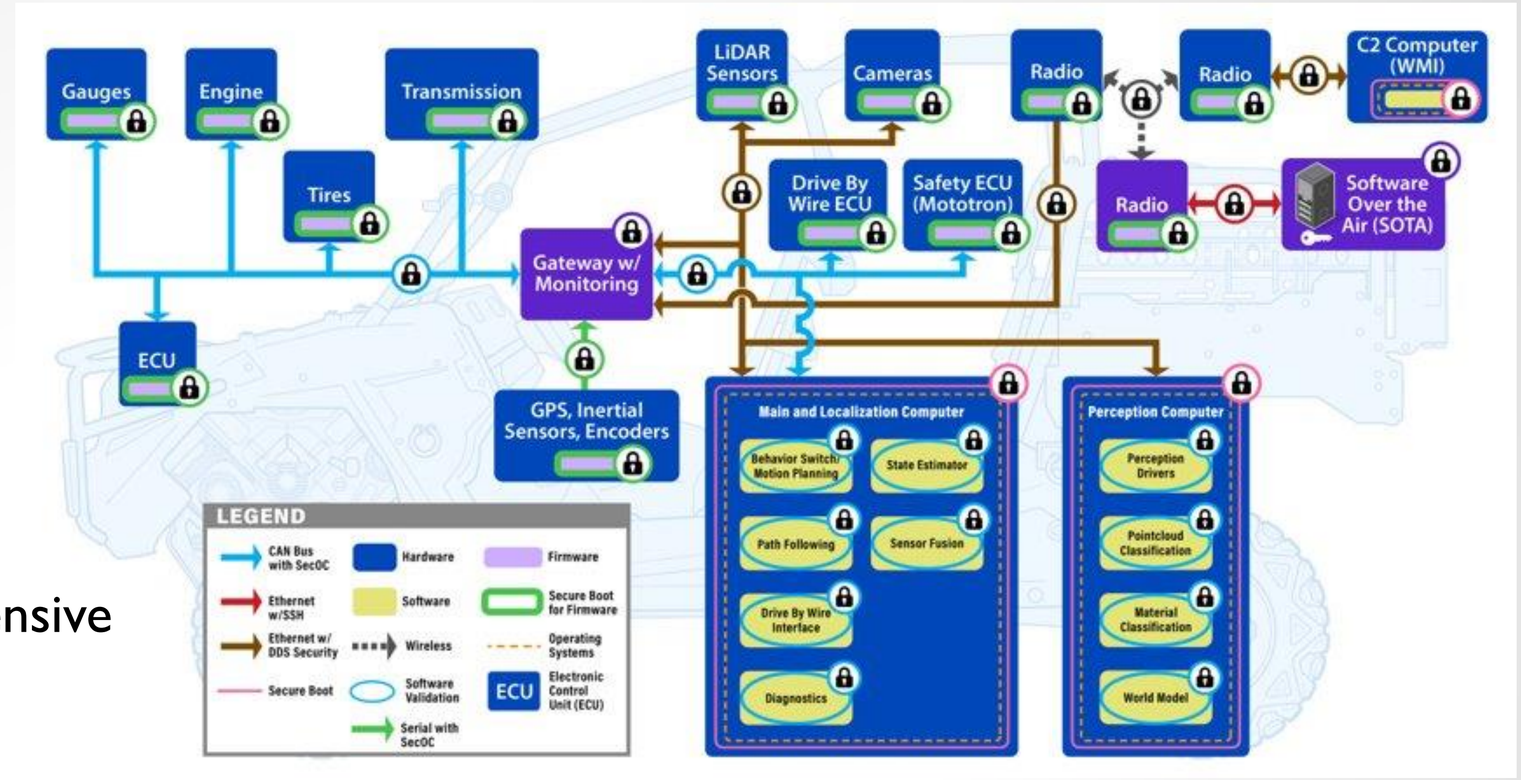
- Third Party ECUs
  - For AV ECUs, no DDS security
- DDS Security to Full AV
- Software Validation for AV codebase
- Full Vehicle Key Distribution and Management

Policy Enforcement Monitoring:

- Expand policy to be more comprehensive
  - Notify servers if major issue.
  - Drive to solution when problem detected

Monitoring Updates:

- Full AV Monitoring



Key Takeaways

- Presented ZTA for AV focusing on authentication, monitoring and policy enforcement.
- No requirement to implement all security features.
- Risk based approach rather than all or nothing:
  - Remote connectivity top priority.
  - Safety systems next.

- Features implemented to date have substantially increased AV security.
- Fielding implementation requires several groups:
  - OEMS
  - Suppliers
  - Testers
  - Research

Questions?