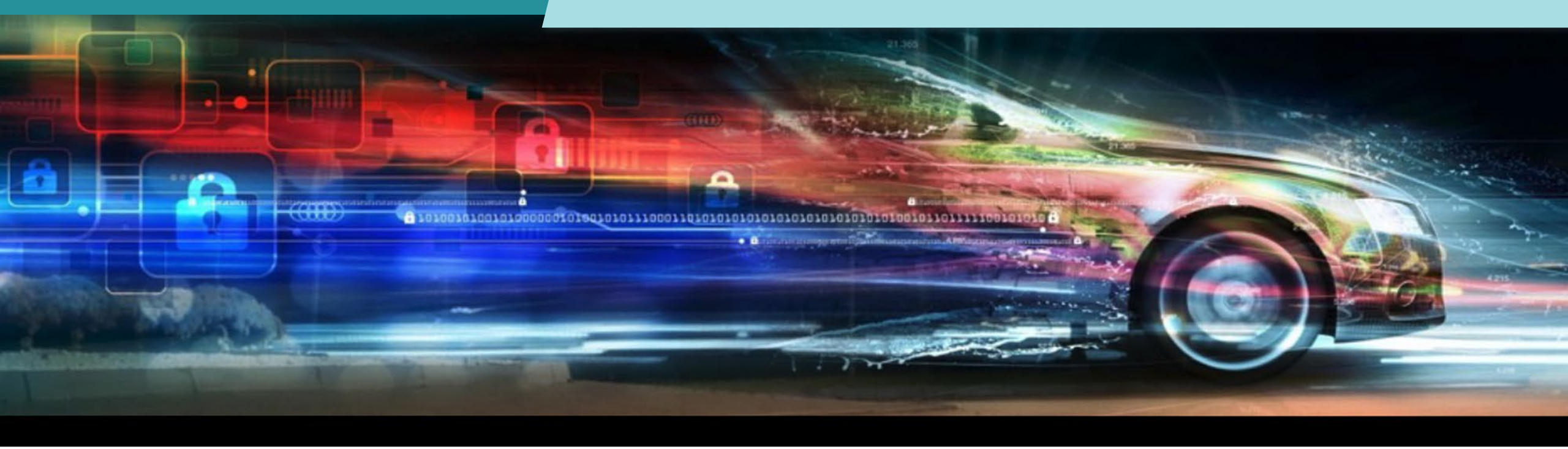


Welcome to Auto-ISAC!

Monthly Virtual Community Call

August 2, 2023

This Session will be recorded.

TLP:CLEAR

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Auto-ISAC Antitrust Statement

As Members of the Auto-ISAC, we strictly comply with EU and US antitrust laws. Please do not discuss anything that your company considers commercially sensitive and/or confidential such as pricing or future product plans. A violation of any of the above-mentioned issues will result in us having to quickly terminate the meeting.

Finally, please remember to keep these deliberations confidential. Please do not discuss the substance of these meetings outside of this group.

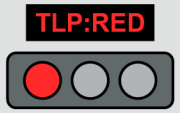
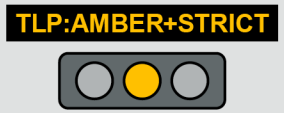
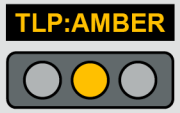
This meeting is being held at

TLP:CLEAR

Disclosure is not limited.

Traffic Light Protocol (TLP)

Version 2.0 Definitions

Color	When Should It Be Used?	How May It Be Shared?
 **Not for disclosure, restricted to participants only.**	Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. For the eyes and ears of individual recipients only, no further.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
 **Limited disclosure, restricted to participants' and its organization.**	Sources may use TLP:AMBER+STRICT when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organization.	Recipients may share TLP:AMBER+STRICT information only with members of their own organization on a need-to-know basis to protect their organization and prevent further harm.
 **Limited disclosure, restricted to participants' organization and its clients on a need-to-know basis.**	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Note that TLP:AMBER+STRICT should be used to restrict sharing to the recipient organization only.	Recipients may share TLP:AMBER information with members of their own organization and its clients on a need-to-know basis to protect their organization and its clients and prevent further harm.
 **Limited disclosure, restricted to the community.**	Sources may use TLP:GREEN when information is useful to increase awareness within their wider community.	Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. Unless otherwise specified, TLP:GREEN information may not be shared outside of the cybersecurity or cyber defense community.
 **Disclosure is not limited.**	Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Recipients may share this information without restriction. Information is subject to standard copyright rules.

Source: https://www.us-cert.gov/tlp

Agenda

Time (ET)	Topic
11:00	**Welcome** ➢ Why We're Here ➢ Expectations for This Community
11:05	**Auto-ISAC Update** ➢ Auto-ISAC Activities ➢ Heard Around the Community ➢ Intelligence Highlights
11:15	***DHS CISA Community Update*** ➢ **Jeff Terra, Consulting Support, Joint Cyber Defense Collaborative (JCDC), Cybersecurity and Infrastructure Security Agency (CISA)**
11:20	**Featured Speaker:** ➢ **Victor Murray, *Assistant Director, CISSP*, SwRI** ➢ **Title: *"Towards Deployment of a Zero-Trust Architecture (ZTA) For Automated Vehicles (AV)."***
11:45	**Around the Room** ➢ Sharing Around the Virtual Room
11:55	**Closing Remarks**

Welcome - Auto-ISAC Community Call!

Purpose: These monthly Auto-ISAC Community Meetings are an opportunity for you, our Members & connected vehicle ecosystem Partners, to:

- ✓ *Stay informed of Auto-ISAC activities*
- ✓ *Share information on key vehicle cybersecurity topics*
- ✓ *Learn about exciting initiatives within the automotive community from our featured speakers*

Participants: Auto-ISAC Members, Potential Members, Strategic Partners, Academia, Industry Stakeholders and Government – *the whole of the automotive industry*

Classification Level: TLP:GREEN - May be shared within the Auto-ISAC Community and "off the record"

How to Connect: For further info, questions or to add other POCs to the invite, please contact us!
(sharmilakhadka@automotiveisac.com)

Engaging in the Auto-ISAC Community

❖ Join

- ❖ If your organization is eligible, apply for Auto-ISAC Membership
- ❖ If you aren't eligible for Membership, connect with us as a Partner
- ❖ Get engaged – *"Cybersecurity is everyone's responsibility!"*

❖ Participate

- ❖ Participate in monthly virtual conference calls (1st Wednesday of month)
- ❖ If you have a topic of interest, let us know!
- ❖ Engage & ask questions!

30 *OEM Members*

21 *Navigator Partners*

❖ Share – *"If you see something, say something!"*

- ❖ Submit threat intelligence or other relevant information
- ❖ Send us information on potential vulnerabilities
- ❖ Contribute incident reports and lessons learned
- ❖ Provide best practices around mitigation techniques

46 *Supplier & Commercial Vehicle Members*

20 *Innovator Partners*

Membership represents **99%** *of cars and trucks on the road in North America*

Coordination with **26** *critical infrastructure ISACs through the National Council of ISACs (NCI)*

2023 Board of Directors

Thank you for your Leadership!

Josh Davis
***Chair** of the*
Board of the Directors
Toyota

Kevin Tierney
***Vice Chair** of the*
Board of the Directors
GM

Stephen Roberts
***Secretary** of the*
Board of the Directors
Honda

Tim Geiger
***Treasurer** of the*
Board of the Directors
Ford

Andreas Ebert
***Chair** of the EuSC*
Volkswagen

Andrew Hillery
***Chair** of the CAG*
Cummins

Ravi Puvvala
***Chair** of the SAG*
Fleet Defender

Monica Mitchell
Polaris

Bob Kaster
Bosch

Brian Witten
Aptiv

Auto-ISAC Member Roster

As of August 1, 2023

76 Members + 3 Pending

Aisin	Fleet Defender	Lucid Motors	Polaris
Allison Transmission	Flex	Luminar	Qualcomm
American Axle & Manufacturing	Ford	Magna	Renesas Electronics
Aptiv	Garrett	MARELLI	Rivian
AT&T	General Motors (Cruise-Affiliate)	Mazda	Stellantis
AVL List GmbH	Geotab	Mercedes-Benz	Subaru
Blackberry Limited	Harman	Mitsubishi Electric	Sumitomo Electric
BMW Group	Hitachi	Mitsubishi Motors	thyssenkrupp
BorgWarner	Honda	Mobis	Tokai Rika
Bosch (ETAS-Affiliate)	Hyundai	Motional	Toyota (Woven Planet-Affiliate)
Bose Automotive	Infineon	Navistar	Valeo
ChargePoint	Intel	Nexteer Automotive Corp	Veoneer
Continental (Argus-Affiliate)	John Deere Electronic	Nissan	Vitesco
Cummins (Meritor-Affiliate)	JTEKT	Nuro	Volkswagen (CARIAD-Affiliate)
Daimler Truck	Kia America, Inc.	Nuspire	Volvo Cars
Denso	Knorr Bremse	NXP	Volvo Group
e:fs TechHub GmbH	KTM	Oshkosh Corp	Waymo
Faurecia	Lear	PACCAR	Yamaha Motors
Ferrari	LG Electronics	Panasonic (Ficosa-Affiliate)	ZF

Pending: Amazon.com, CNH Industrial, Stoneridge

Auto-ISAC Business Updates and Events

**All times are in ET

- **Auto-ISAC Summit will be Tuesday, October 17th-18th, 2023 in Torrance, California. *Early bird registration discount pricing ends September 8th. Our discounted hotel room block ($219/night vs. $333 as of 7/31) closes when the block has been fully booked or September 21st.* You can find more information here: https://automotiveisac.com/2023-annual-summit.**

- **When booking summit travel, please consider joining these Members-only meetings in person**
  - **Monday, Oct 16th, Q3 2023 Pre-Summit Joint PWG + IT/OT Workshop – In Person Only**
  - **Thursday, Oct 19th, Member Advisory Forum - HYBRID**

- **Automotive Cybersecurity Training (ACT) Program: Registration for ACT Fundamental and Advanced Course Blocks opens August 7, 2023 on the Auto-ISAC website http://www.automotiveisac.com/act! Please send an email to ACT@automotiveisac.com with any questions you have regarding the ACT Program.**
  - **ACT Fundamental Course Block: Online, On-Demand, Anytime, Anywhere, and by Anyone**
    - **Cybersecurity Basics (32 hrs) | Security Engineering (28 hours) | Security Operations/Management (22.5 hours)**
  - **ACT Advanced Course Block: Collaborative, In-Person, and Hands-On**
    - **Sept 11 – 15, 2023: Advanced Engineering (40 hours)**
    - **Oct 02 – 06, 2023: Advanced Wireless (40 hours)**
    - **Nov 06 – 10, 2023: Advanced Guided Attacks (40 hours)**
    - **Nov 13 – Nov 17, 2023: Advanced EV/EV Infrastructure (36 hours)**

ACCELERATING CAST SECURITY

7th Annual Auto-ISAC Cybersecurity Summit

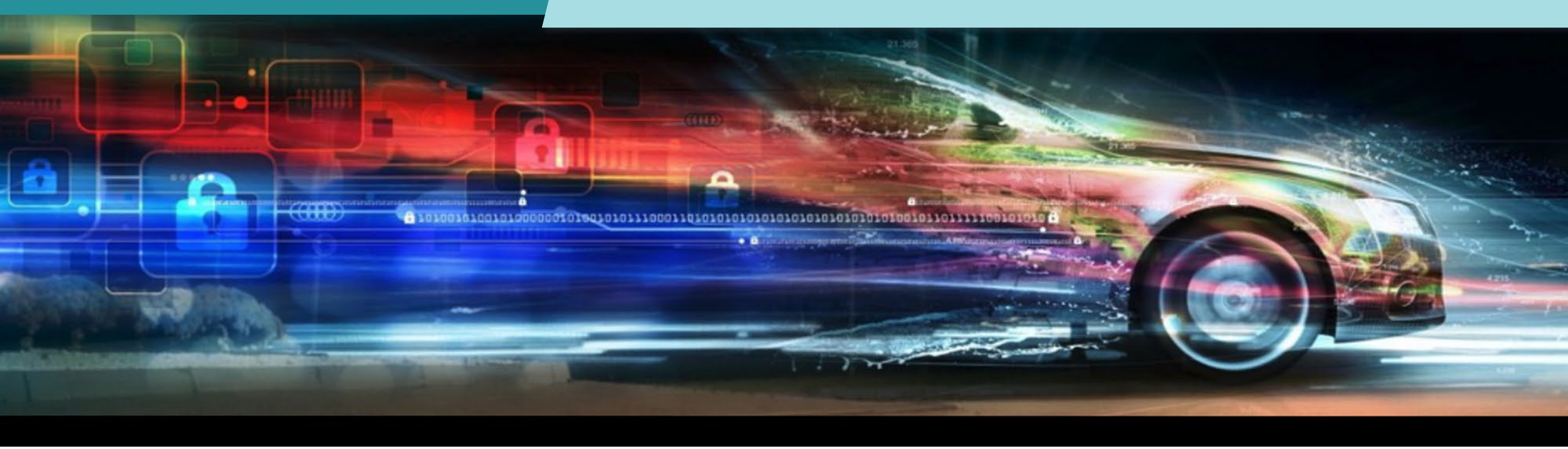
October 17-18, 2023

Torrance, CA

HONDA

The Power of Dreams

AUTO-ISAC



Auto-ISAC Intelligence Highlight

TLP:CLEAR

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Auto-ISAC Intelligence

- **Know what we track daily: subscribe to the DRIVEN; TLP:GREEN Auto-ISAC 2022 Threat Assessment released with Auto-ISAC Automotive Cyber Threat Ecosystem (1st Iteration) included.**
- **TLP:GREEN Generative AI in Automotive & Healthcare: Examining the Emerging Cyber Threat Landscape**
  - **Send feedback, contributions, or questions to analyst@automotiveisac.com**
- **Intelligence Notes**
  - **Geopolitical tensions involving Russia, China, North Korea, and Iran remain high with Russia-Ukraine in crisis. Threat of cyberattack spillover increases if: (1) the Russia-Ukraine war leads to kinetic clashes with the West (possible but unlikely), and (2) any other hotspots escalate into crises (possible) (Russia-Ukraine [1], China [2], North Korea [3] [4], Iran).**
    - **Note: Russia, China, North Korean, and Iran are constant cyberespionage threats regardless of tension.**
  - **Ransomware [5] Groups Targeting Automotive*: 8Base, Cl0p*, Akira, Rhysida, RA Group.**
  - **Continuing to monitor and internally discuss latest security research and CVEs regarding vehicle and EV charger cybersecurity; no malicious threats seen aside from technology-enabled vehicle theft.**
  - **Notable TTPs and Tools: Delivering malware via third-party cloud provider (Dark Reading); Exploitation of ICS Contec SolarView vulnerability (Vulncheck); Exploitation of unpatched zero-vulnerability CVE-2023-36884 in Windows/Office products (SecurityAffairs); Exploitation of MobileIron Zero-Day (BleepingComputer); Exploitation of insecure direct object reference (IDOR) vulnerabilities in web apps (CISA); WormGPT (Slashnext); PyLoose Cryptominer* (Wiz); Flipper Zero Third-Party Apps (BleepingComputer); Nitrogen (Sophos); Meduza Stealer (Uptycs).**

CISA Resource Highlights

- Joint Cyber Defense Collaborative

Jeff Terra
8/2/2023

CISA and Partners Release Joint Cybersecurity Advisory on Preventing Web Application Access Control Abuse

- The Australian Signals Directorate's Australian Cyber Security Centre (ACSC), the Cybersecurity and Infrastructure Security Agency (CISA), and the National Security Agency (NSA) are releasing a joint Cybersecurity Advisory (CSA).

- Preventing Web Application Access Control Abuse
  - Warning vendors, designers, developers, and end-user organizations of web applications about insecure direct object reference (IDOR) vulnerabilities.

- These vulnerabilities are frequently exploited by malicious actors in data breach incidents and have resulted in the compromise of personal, financial, and health information of millions of users and consumers.

CISA Releases Malware Analysis Reports on Barracuda Backdoors

- CISA has published three malware analysis reports on malware variants associated with exploitation of CVE-2023-2868.
- CVE-2023-2868 is a remote command injection vulnerability affecting Barracuda Email Security Gateway (ESG) Appliance, versions 5.1.3.001-9.2.0.006.
- It was exploited as a zero day as early as October 2022 to gain access to ESG appliances. According to industry reporting, the actors exploited the vulnerability to gain initial access to victim systems and then implanted backdoors to establish and maintain persistence.
- CISA analyzed backdoor malware variants obtained from an organization that had been compromised by threat actors exploiting the vulnerability.

CISA and FBI Release Cybersecurity Advisory on Enhanced Monitoring to Detect APT Activity Targeting Outlook Online

- CISA and FBI have released a joint Cybersecurity Advisory (CSA), Enhanced Monitoring to Detect APT Activity Targeting Outlook Online, to provide guidance to agencies and critical infrastructure organizations on enhancing monitoring in Microsoft Exchange Online environments.

- In June 2023, a Federal Civilian Executive Branch (FCEB) agency observed unexpected events in Microsoft 365 (M365) audit logs. As a response, Microsoft released this guidance:
  - Microsoft: Microsoft Mitigates China-based Threat Actor Storm-0558 Targeting of Customer Email
  - Microsoft: Mitigation for China-Based Threat Actor Activity
  - Microsoft: Analysis of Storm-0558 Techniques for Unauthorized Email Access

- The goal of this CSA is to enhance organizational cybersecurity posture and position organizations to detect similar malicious activity via implementing the listed logging recommendations.

Security/Software Updates

For July 2023:

- **Ivanti Releases Security Update: Endpoint Manager Mobile**
- Juniper Releases Multiple Security Updates: Junos OS
- Oracle Releases Security Updates
- Atlassian Releases Security Updates
- Fortinet Releases Security Updates: FortiOS and FortiProxy
- Adobe Releases Security Updates: ColdFusion and InDesign
- Microsoft Releases Security Updates: July 2023
- Mozilla Releases Security Advisories and Updates: Thunderbird, Firefox, and Firefox ESR
- CISCO Releases Security Updates: SD-WAN vManage API
- Apple Releases Security Updates: Multiple Products

- **Best practices:**
  - Leverage automatic updates for all operating systems and third-party software
  - Implement security configurations for all hardware and software assets
  - Remove unsupported or unauthorized hardware and software from systems

Please note all information provided is TLP Amber

CISA Releases Industrial Control Advisories

- These advisories provide timely information about current security issues, vulnerabilities, and exploits surrounding ICS.
- For the period of 7/1/23- 7/31/23 approximately 34 advisories have been issued.
- Affected systems include Mitsubishi Electric, PTC KepServerEx, Rockwell Automation ThinManager, Schneider Electric Eco Structure Products, GE Digital, Keysight Geolocation Server, Honeywell Experion, Siemens and many others.
- For current ICS advisories please check CISA.gov regularly

Please note all information provided is TLP Amber

KEVs Catalogue

CISA strongly urges all organizations to reduce their exposure to cyberattacks by prioritizing timely remediation of Catalog vulnerabilities as part of their vulnerability management practice.

CISA added 16 new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog in the month of July. These types of vulnerabilities are a frequent attack vector for malicious cyber actors and pose significant risk to the federal enterprise.

Please note all information provided is TLP Amber

Additional Resources from CISA

- CISA Homepage - https://www.cisa.gov/
- CISA NCAS – https://cisa.gov/resources-tools/all-resources-tools
- CISA Shields Up - https://www.cisa.gov/shields-up
- Free Cybersecurity Services and Tools - https://www.cisa.gov/free-cybersecurity-services-and-tools
- CISA News Room - https://www.cisa.gov/cisa/newsroom
- CISA Blog - https://www.cisa.gov/blog-list
- CISA Publications Library - https://www.cisa.gov/publications-library
- CISA Cyber Resource Hub - https://www.cisa.gov/cyber-resource-hub
- CISA Cybersecurity Directives - https://cyber.dhs.gov/directives/

JOINT CYBER DEFENSE
COLLABORATIVE

For more information:

cisa.gov

Questions?

Central@cisa.dhs.gov

1-888-282-0870

Jeff Terra
8/2/2023

Auto-ISAC Community Meeting

Why Do We Feature Speakers?

- These calls are an opportunity for information exchange & learning
- Goal is to educate & provide awareness around cybersecurity for the *connected vehicle*

What Does it Mean to Be Featured?

- Perspectives across our ecosystem are shared from Members, government, academia, researchers, industry, associations and others.
- Goal is to showcase a rich & balanced variety of topics and viewpoints
- *Featured speakers are not endorsed by Auto-ISAC nor do the speakers speak on behalf of Auto-ISAC*

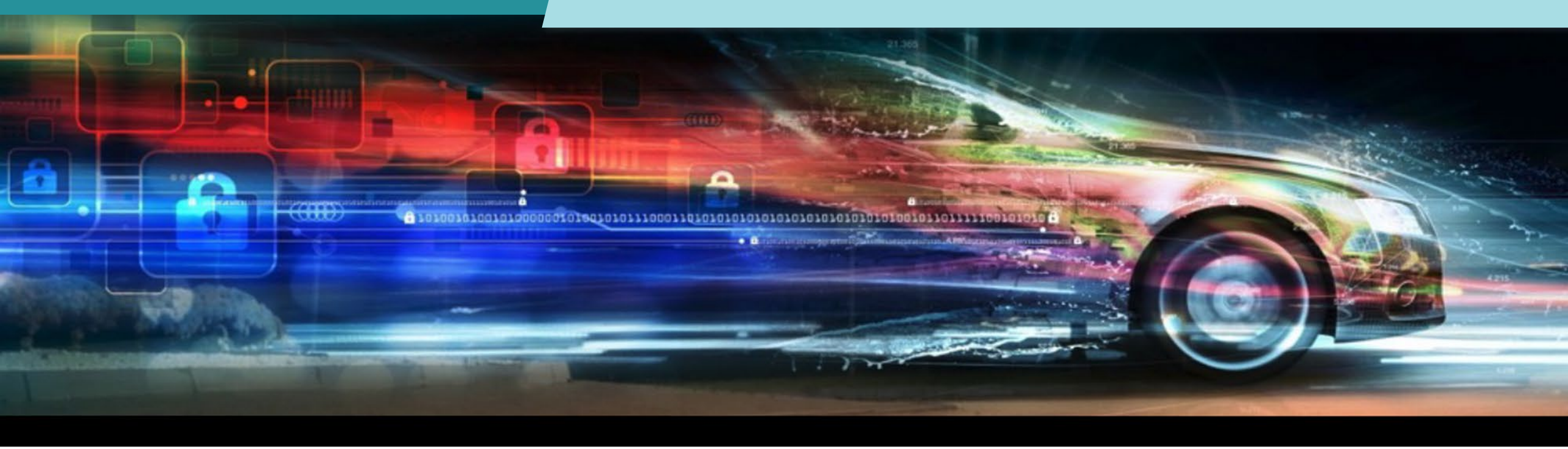
30+
Featured Speakers to date

How Can I Be Featured?

- If you have a topic of interest you would like to share with the broader Auto-ISAC Community, then we encourage you to contact us!

7 ***Best Practice Guides available on website***

2000+
Community Participants



Featured Speaker

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Victor Murray

Assistant Director, CISSP, SwRI

Mr. **Victor Murray** is an Assistant Director at Southwest Research Institute and is a Certified Information Systems Security Professional (CISSP).

He has over 15 years of experience leading the development and testing of embedded systems.

Mr. Murray has led many projects including penetration testing on electric vehicle battery management systems, applying cybersecurity best practices to automated ground vehicles, and developing automotive intrusion detection systems.

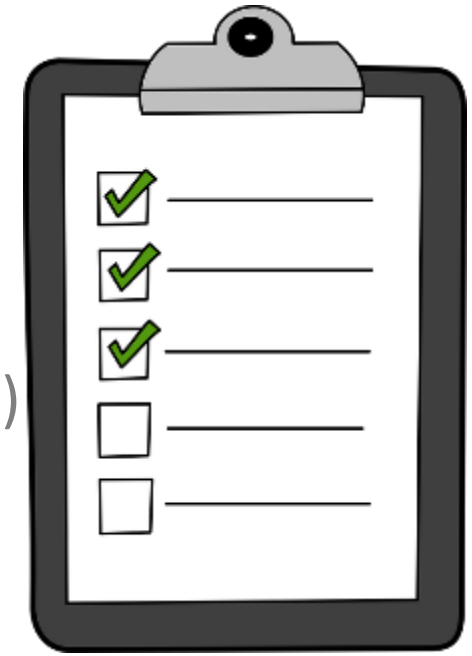
Towards Deployment of a Zero-Trust Architecture(ZTA) For Automated Vehicles (AV)

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

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

Agenda

- Motivation
- Automated Vehicle Architecture
  - Ground Vehicle Baseline
  - Add Control and Sensors
  - Add Remote Connectivity
- Introduction to Zero-Trust
- Zero-Trust Architecture (ZTA) For Automated Vehicles (AV)
  - Authentication
  - Monitoring and Policy Enforcement Engine
- Implementing ZTA on CRASH
- Implementing ZTA on Ground Vehicles
- Future Work
- Key Takeaways



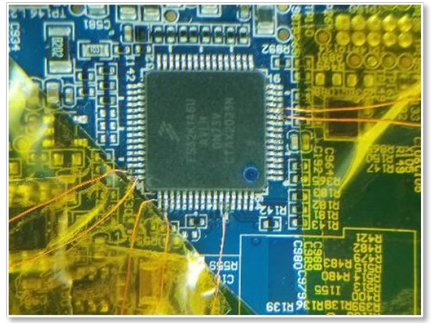
Motivation

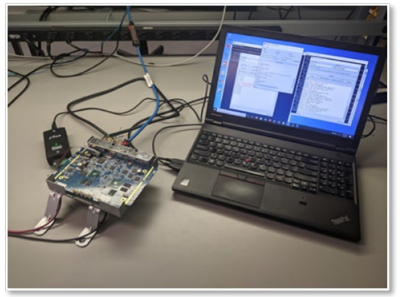
- Large AV development team
- Deployed autonomy solutions on over 20 types of vehicles

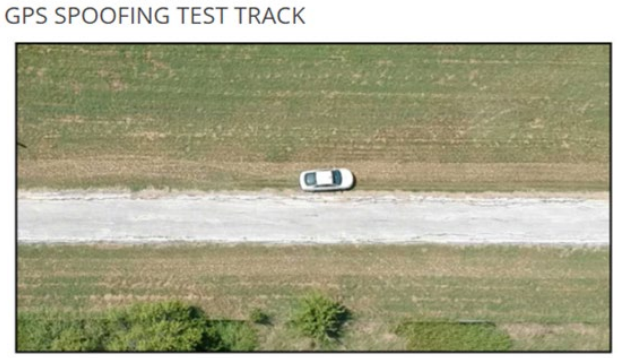
Initial focus on functionality, transitioned into deployment.

Motivation

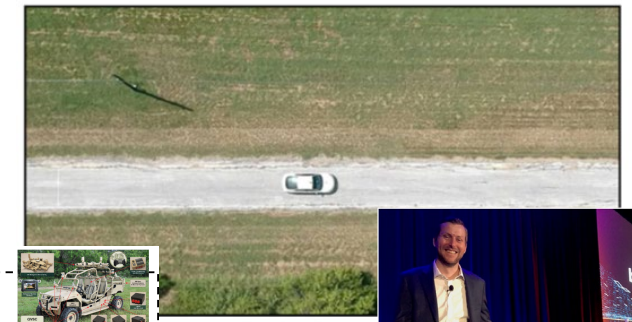
- Commercial Automotive (15 years)
  - Pen Testing
  - Independent Analysis
- AV Sensor Security
  - Camera, lidar, radar, ultrasonic, GNSS
- Securing AV systems
  - Software
  - Communication



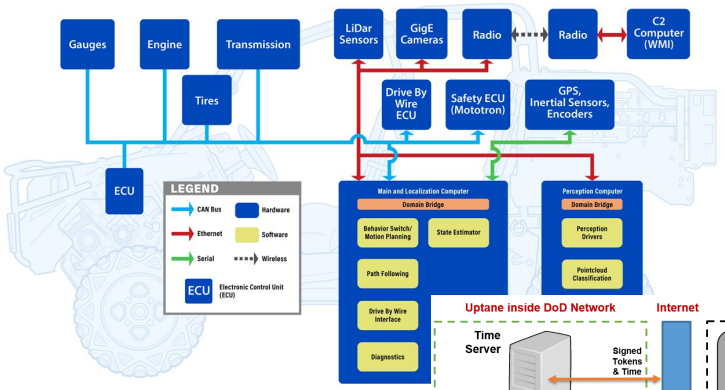


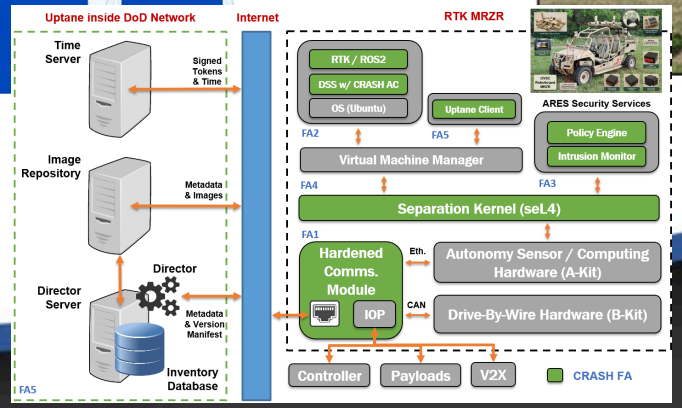


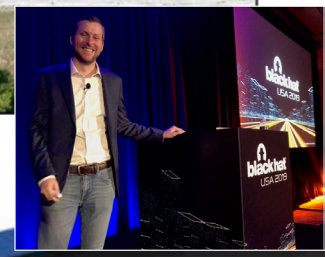
Altered GPS



Normal





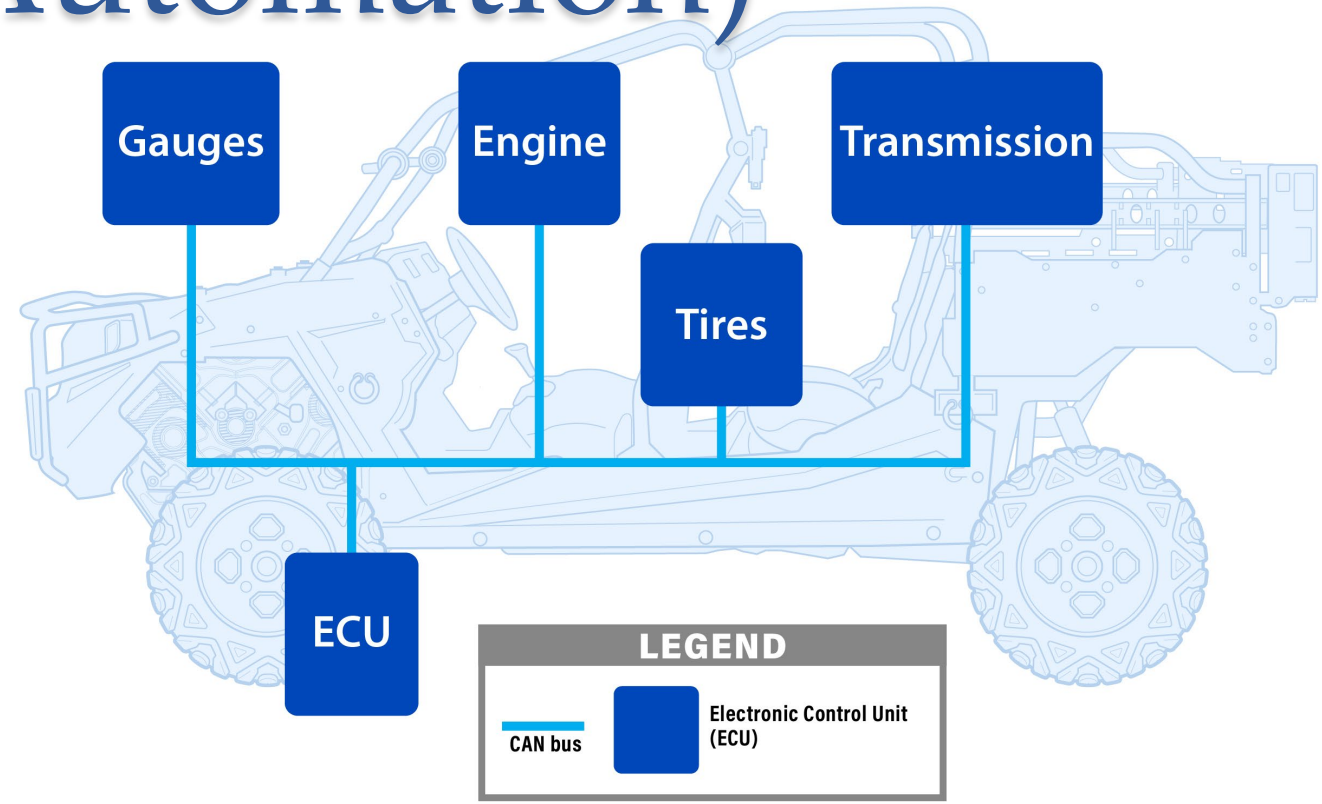


Ground Vehicle Baseline (No Automation)

ECU communication:

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

AV commonly built on top of non-automated vehicles.

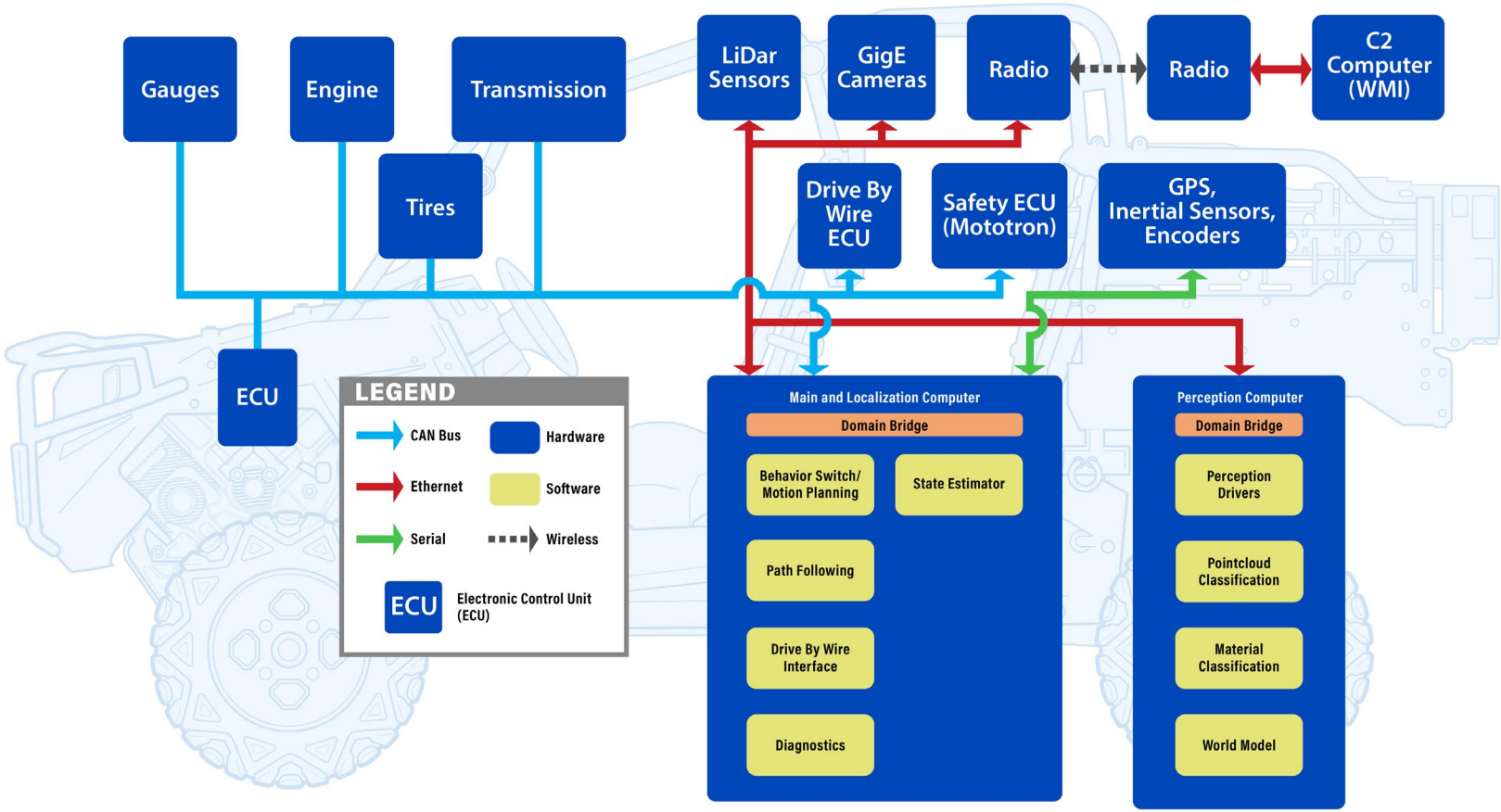


Ground vehicle baseline ECU network and connections.

Automated Vehicle

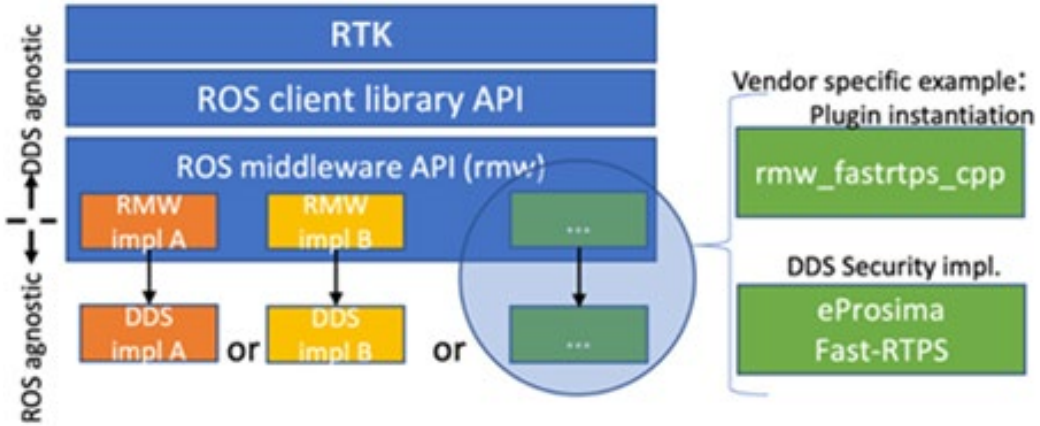
Add:

- Sensors
- Drive By Wire
- Control Computers
- Connectivity

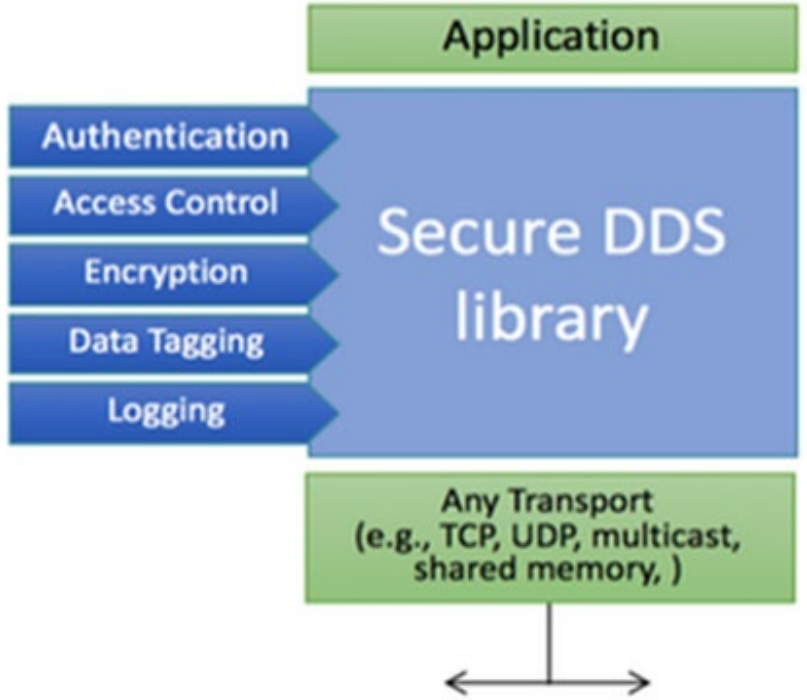


AV architecture with remote connectivity; sensors, drive-by-wire, and control computers; and ground vehicle baseline ECU. This architecture is used to outline the ZTA for AV.

Control Software



In ROS2, each DDS provides the ROS middleware to interface between ROS and DDS.



DDS security layers per the OMG DDS specification.

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

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

Next: zero trust

Introduction to Zero Trust

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

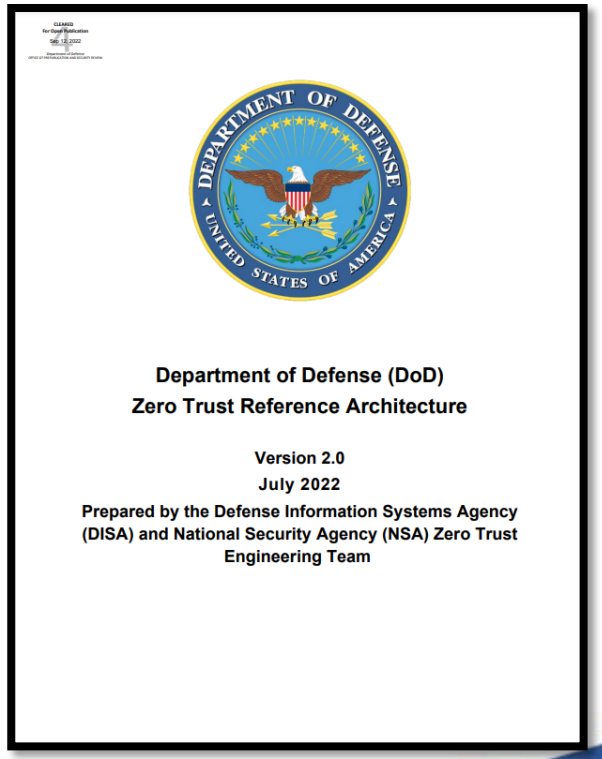
Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

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 an 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.

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

The ZTA for AV is correlates directly to the principles outlined in **NIST SP 800-207.**

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.

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

Distilling down:

1. Authentication
2. Monitoring and Policy Enforcement Engine

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.

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.

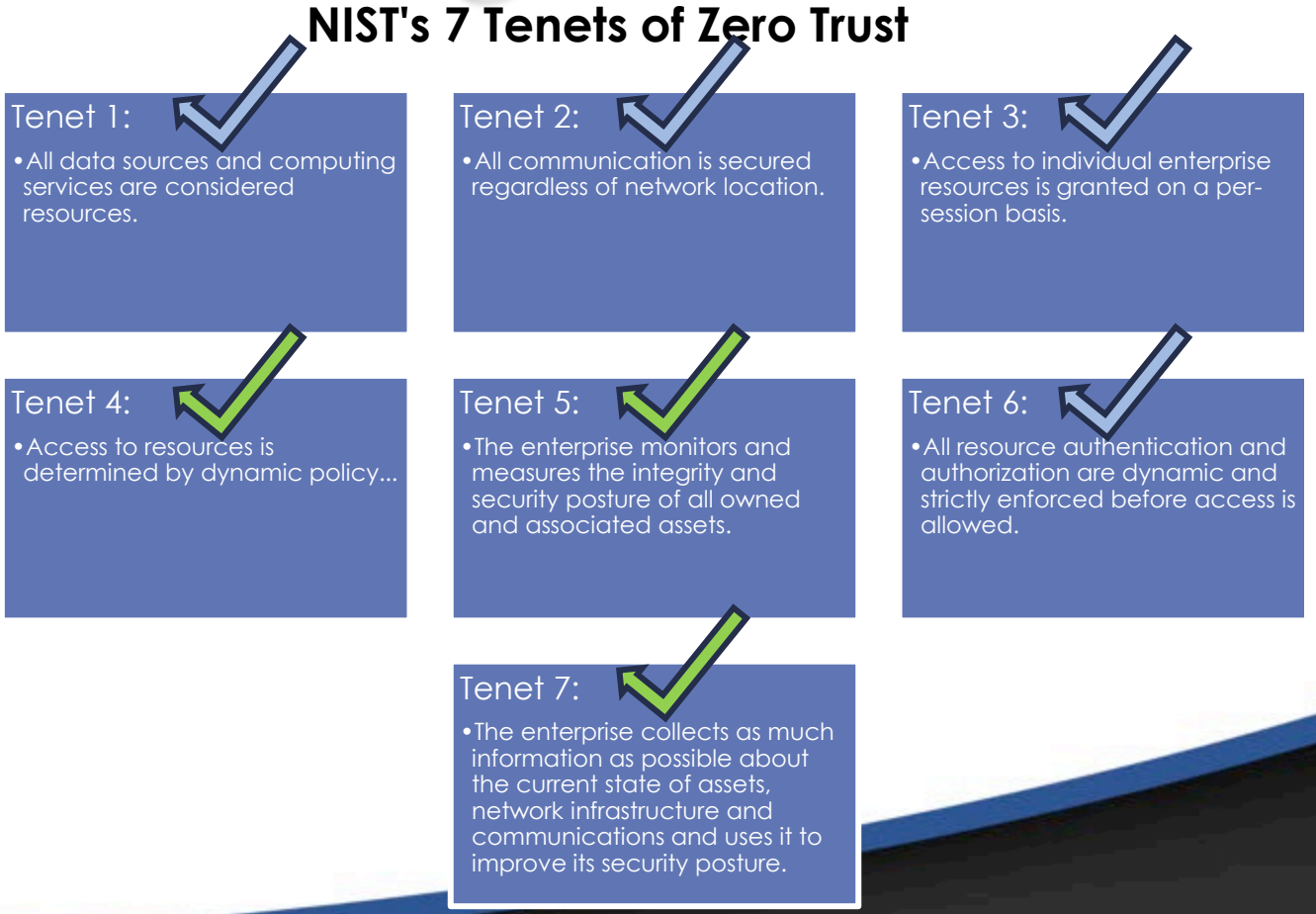
Monitoring and Policy Enforcement Engine

Network Monitoring

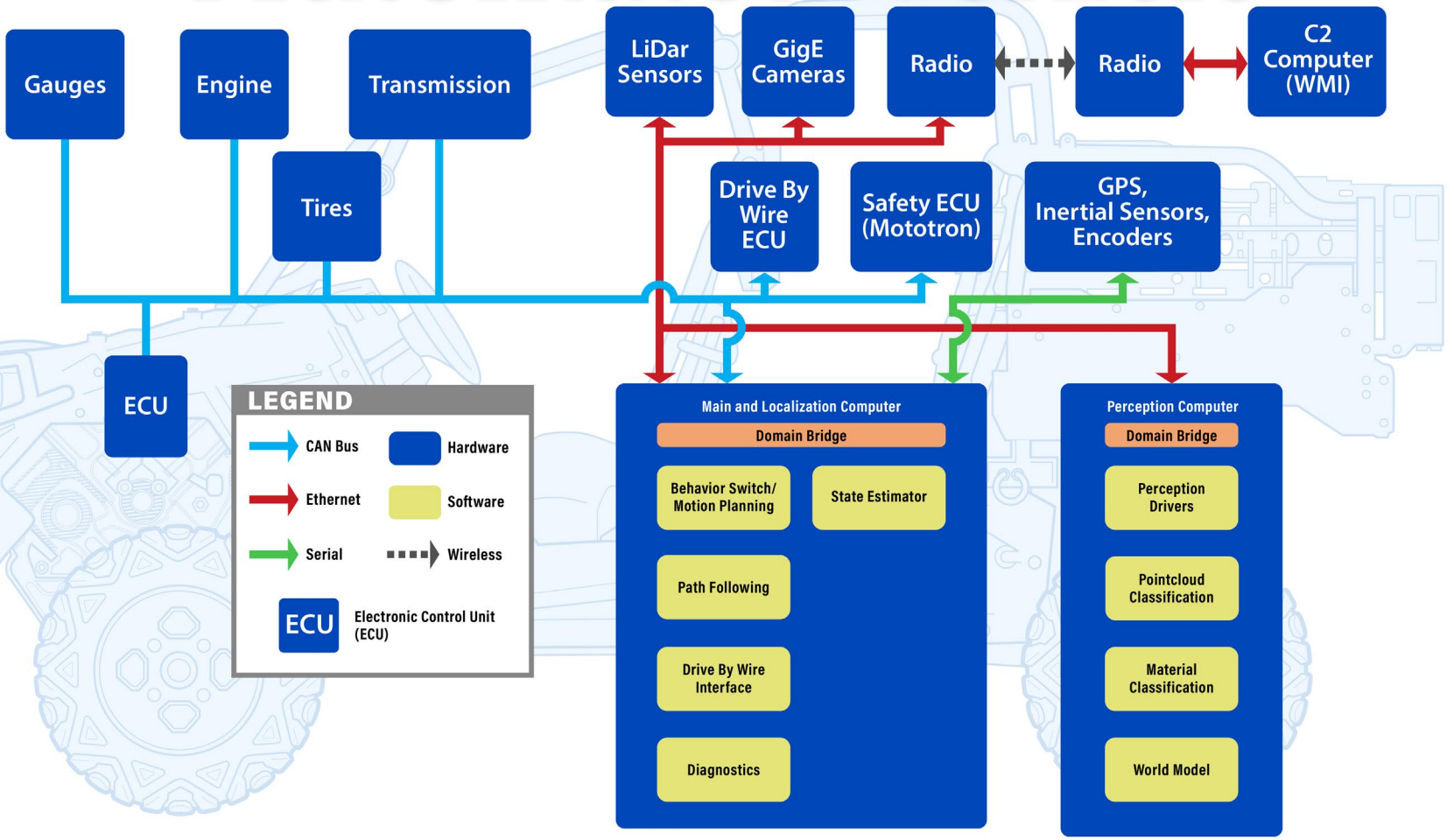
- ZTA networks are monitored by the Gateway to ensure devices maintain ZT policy compliance.

The policy 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.

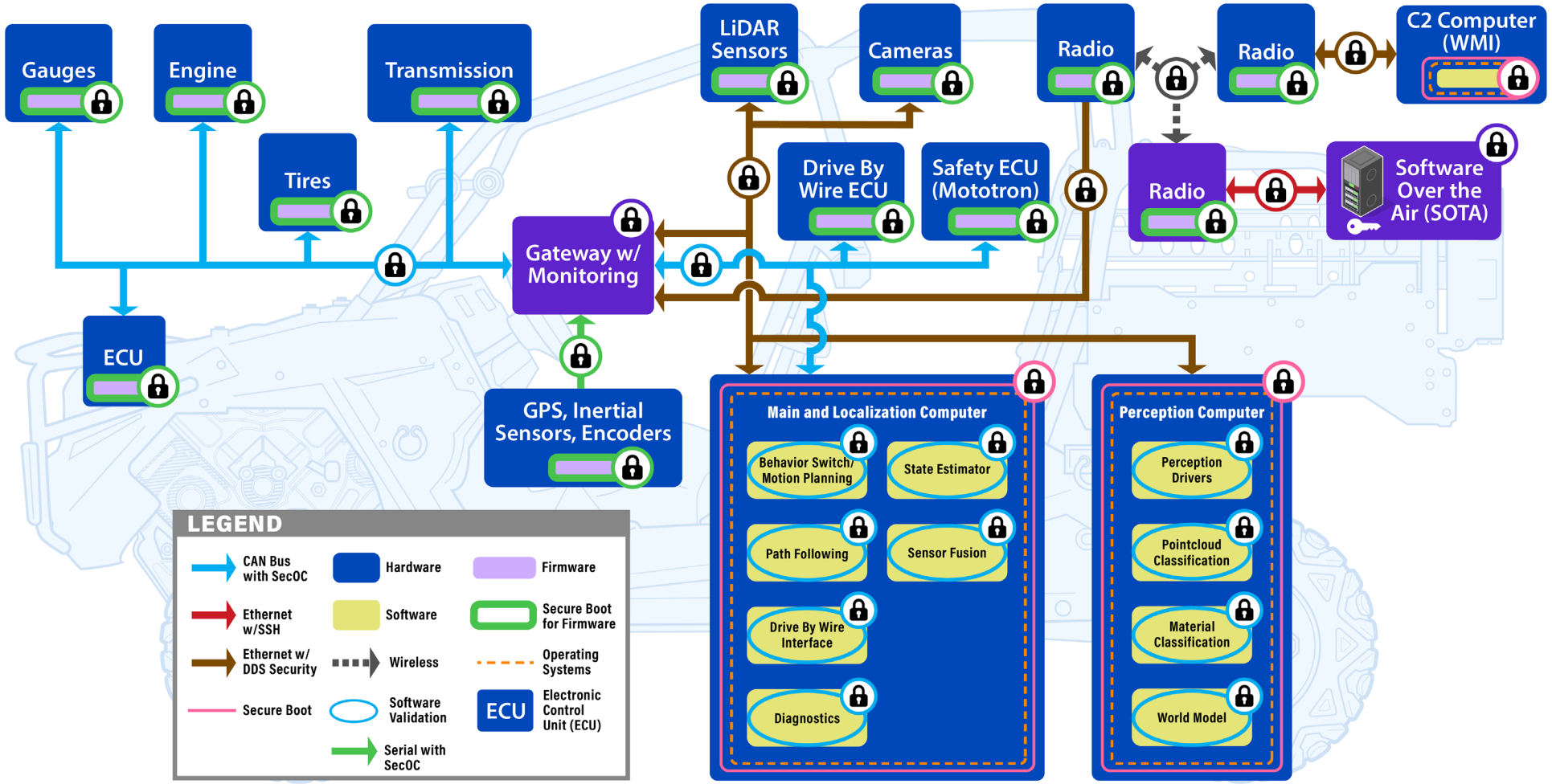


Automated Vehicle

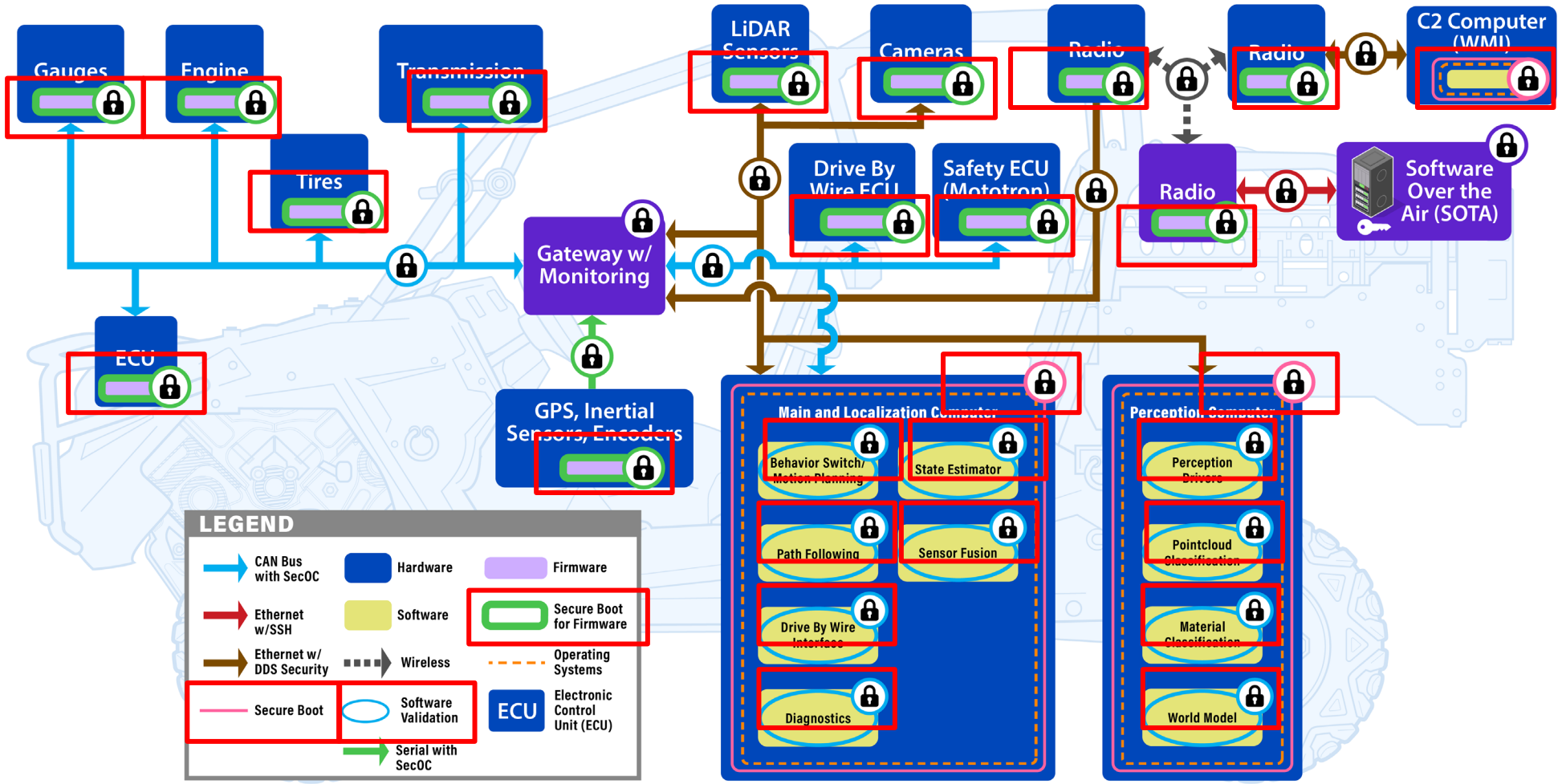


AV architecture with remote connectivity; sensors, drive-by-wire, and control computers; and ground vehicle baseline ECU. This architecture is used to outline the ZTA for AV.

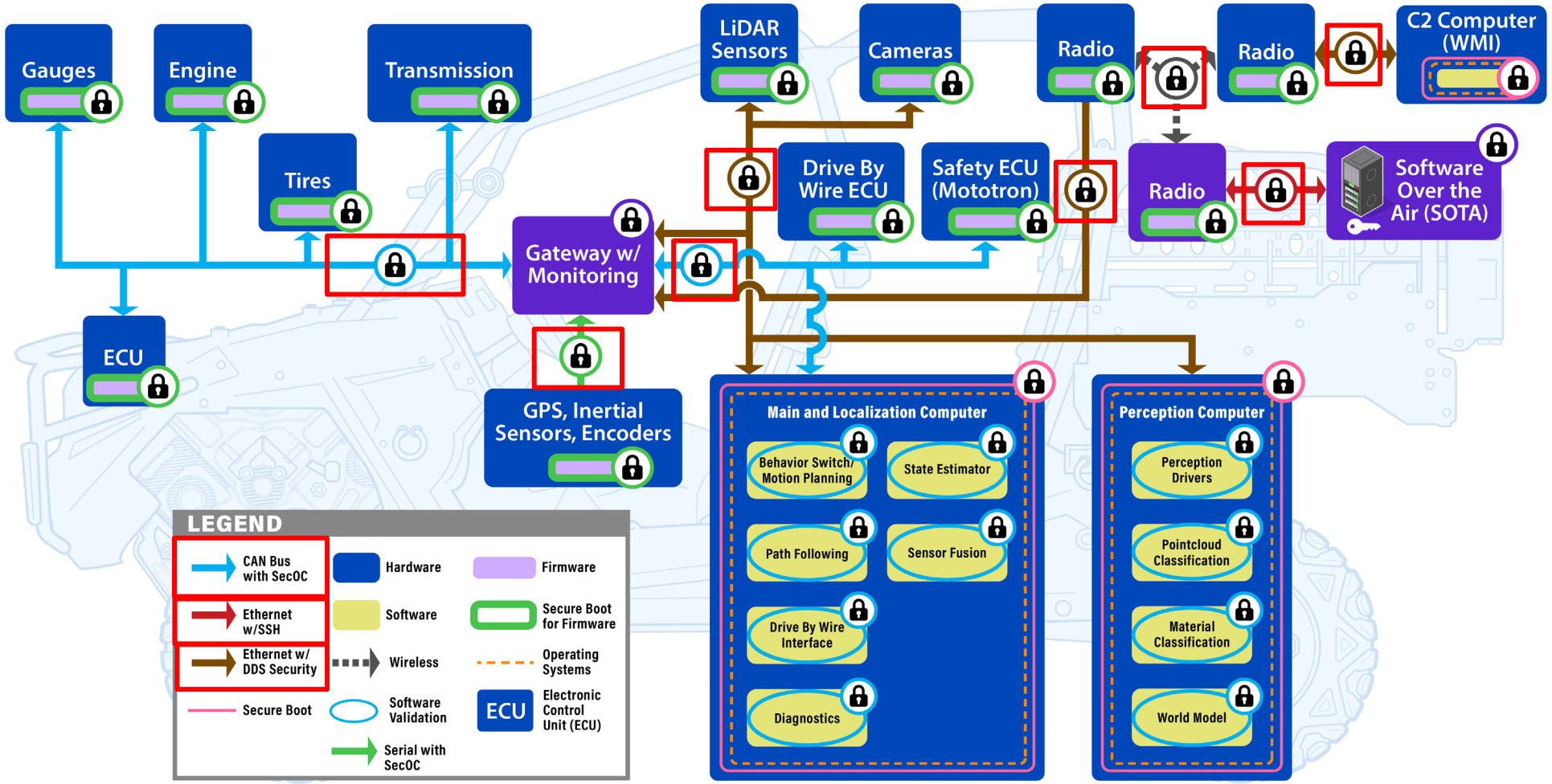
Zero-Trust Architecture (ZTA) for Automated Vehicles (AV)



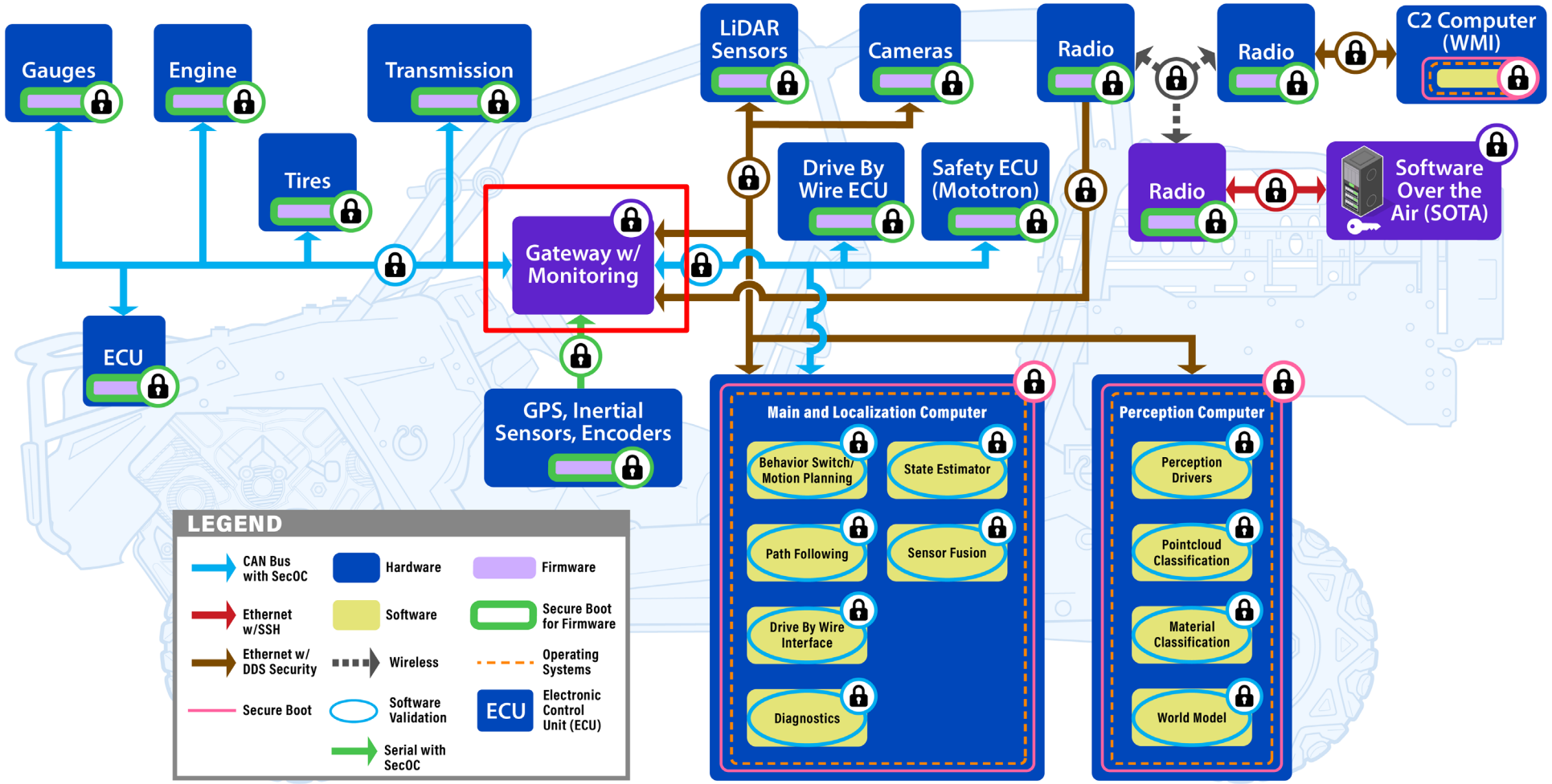
ZTA for AV – Authentication of Software and Firmware



ZTA for AV – Authentication of Network Communication



ZTA for AV – Monitoring and Policy Enforcement



Current State of ZTA

- Many pieces implemented in varying degrees.

Implementing Zero Trust on CRASH

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

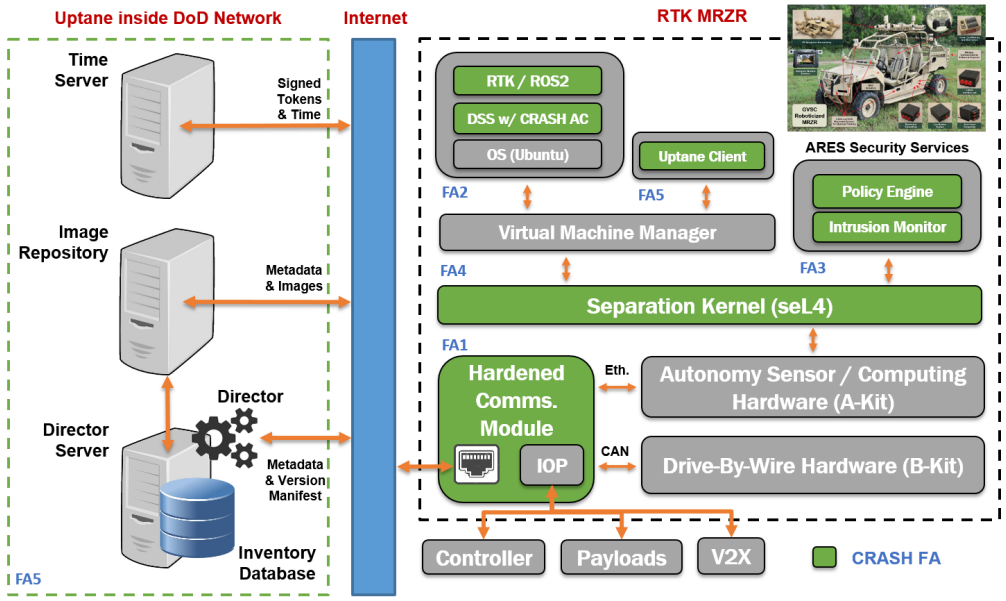
Remote Connectivity:

- Encryption
- Hashing
- Rekeying

```
<?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

Secure Software Updates & Market Roles

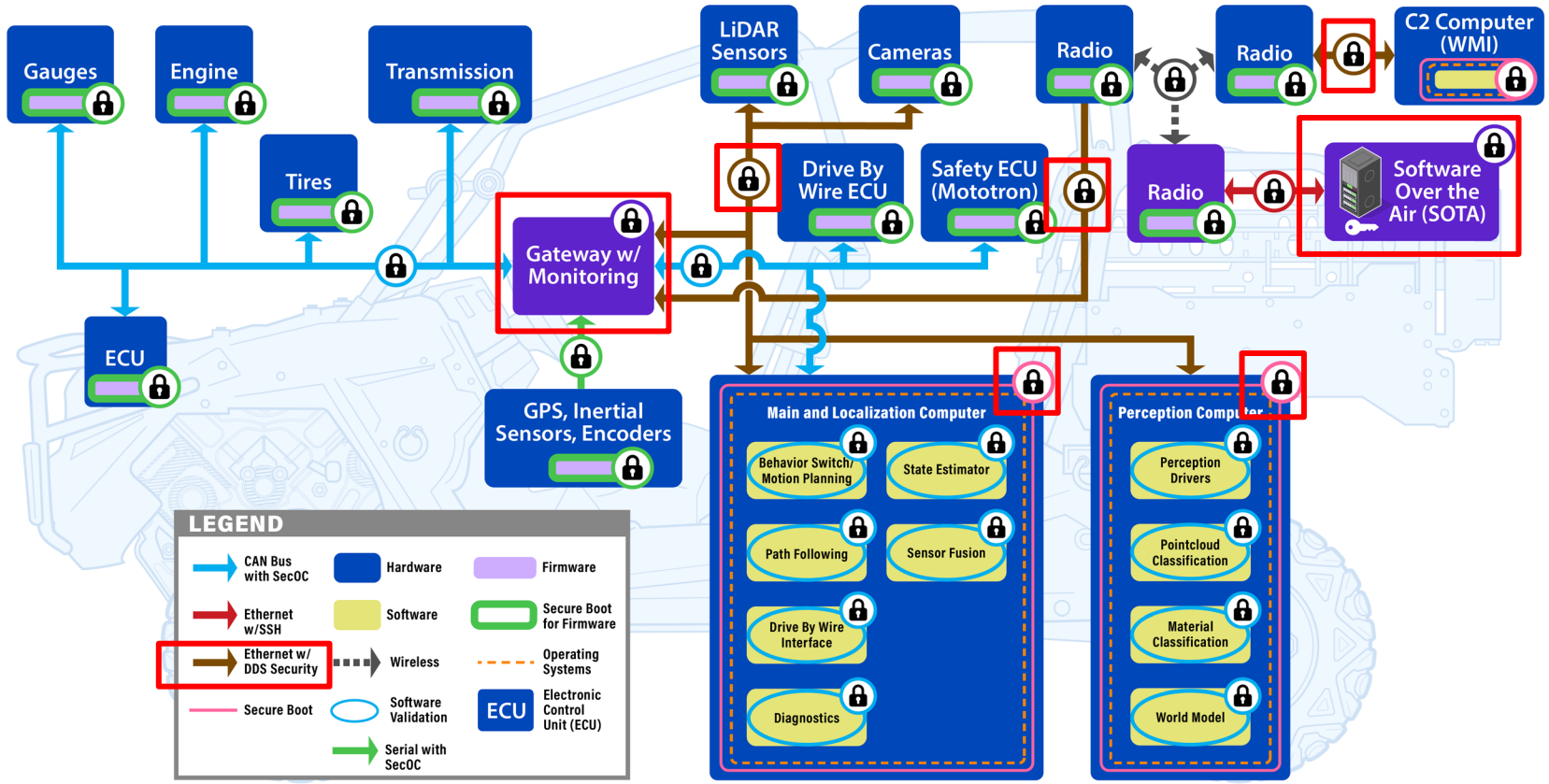


Overview of five (5) focus areas (FA) for CRASH

Implementing Zero Trust on CRASH

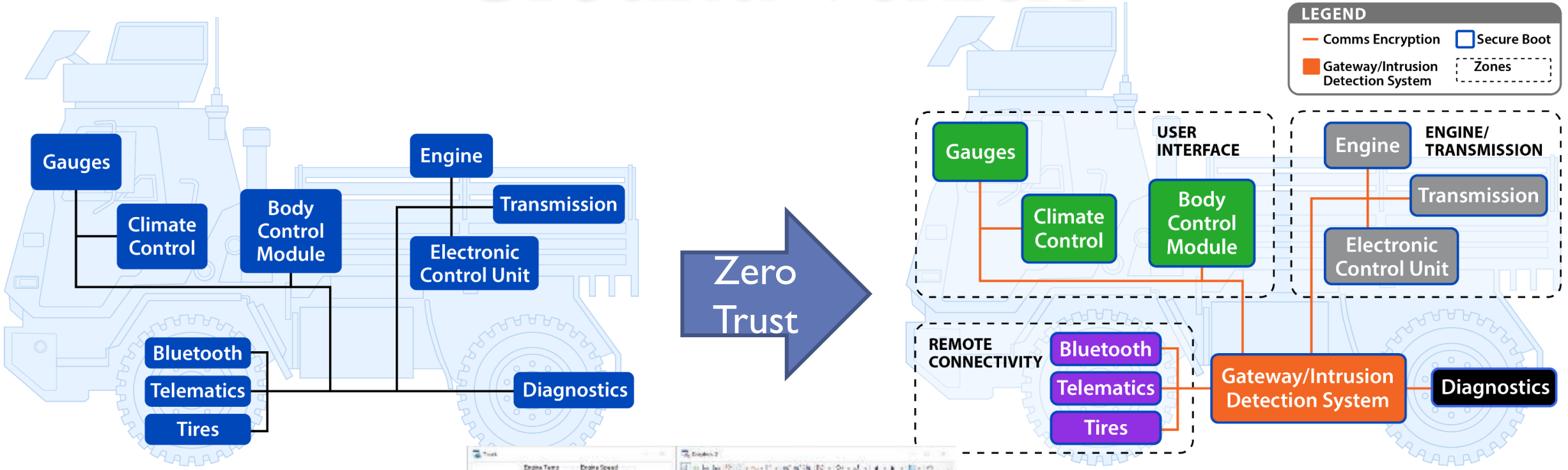
CRASH's Five Focus Areas:

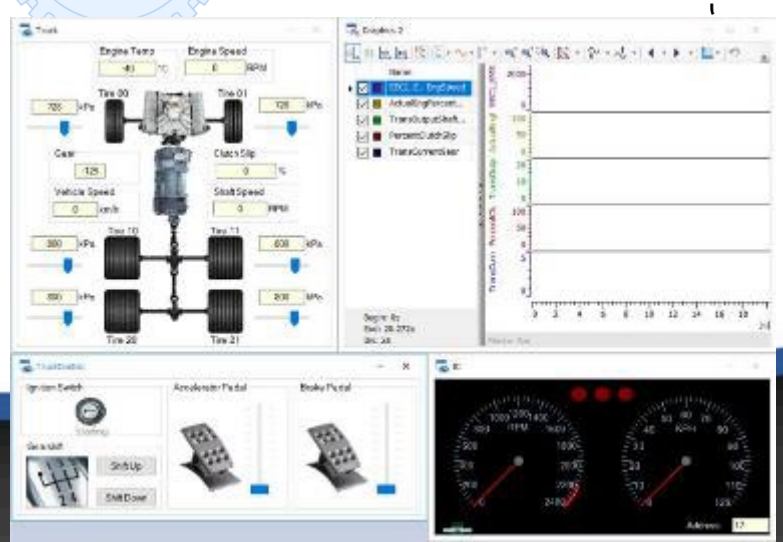
1. Hardened Communication Interfaces
2. ★ Robust Access Control
3. Anomaly Detection Engine
4. Secure-RTK on seL4
5. ★ Secure Software Update



Next: ZT for Ground Vehicles

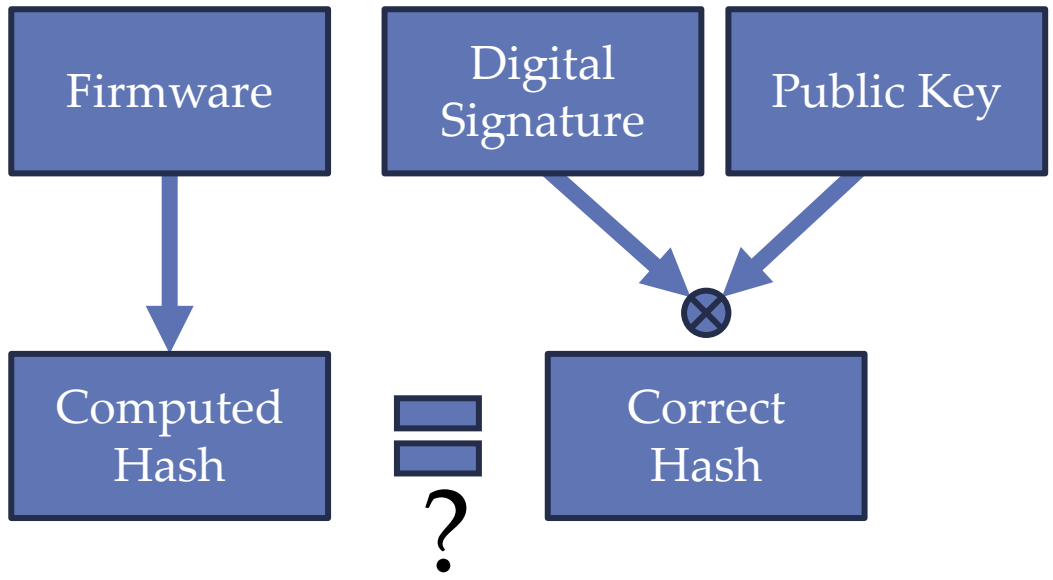
Ground Vehicle





Ground Vehicle

- Secure Boot
  - Digital Signature
  - Public Key
  - Verified at power on



Ground Vehicle

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

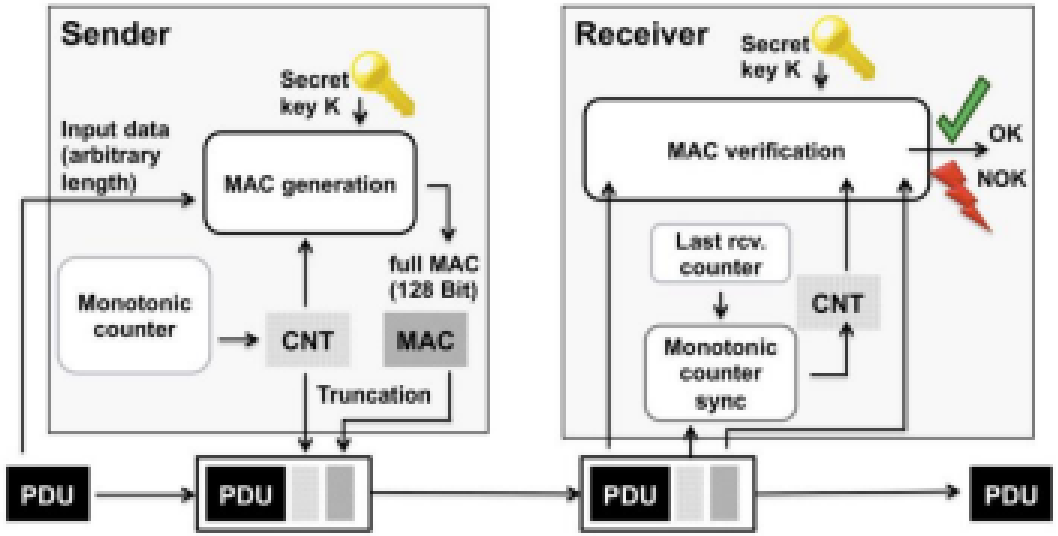
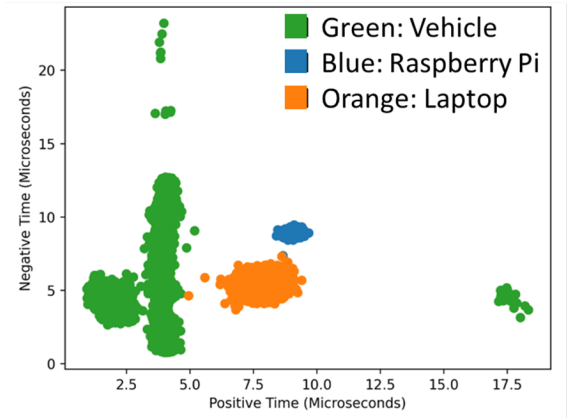
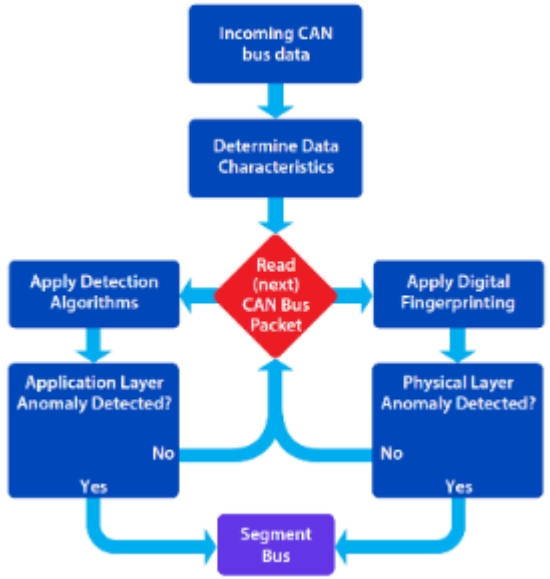


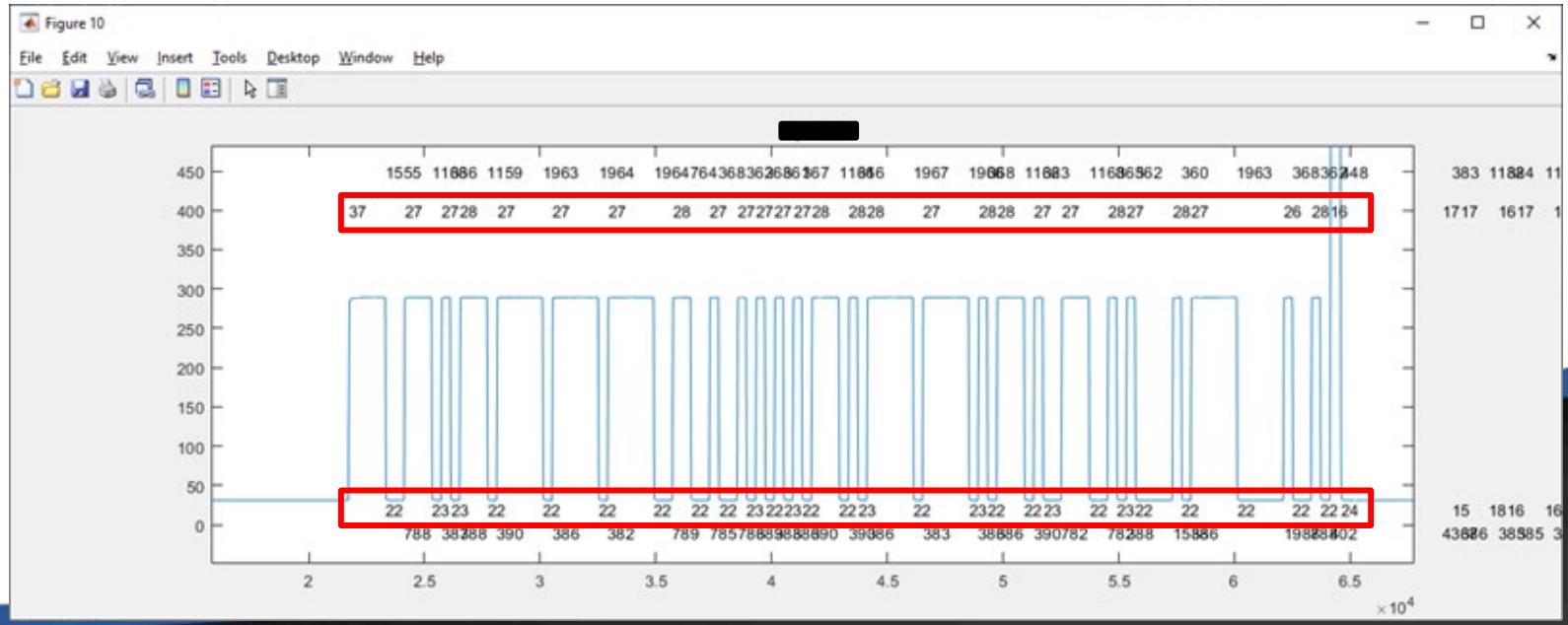
Image Source: autosar.org

Ground Vehicle

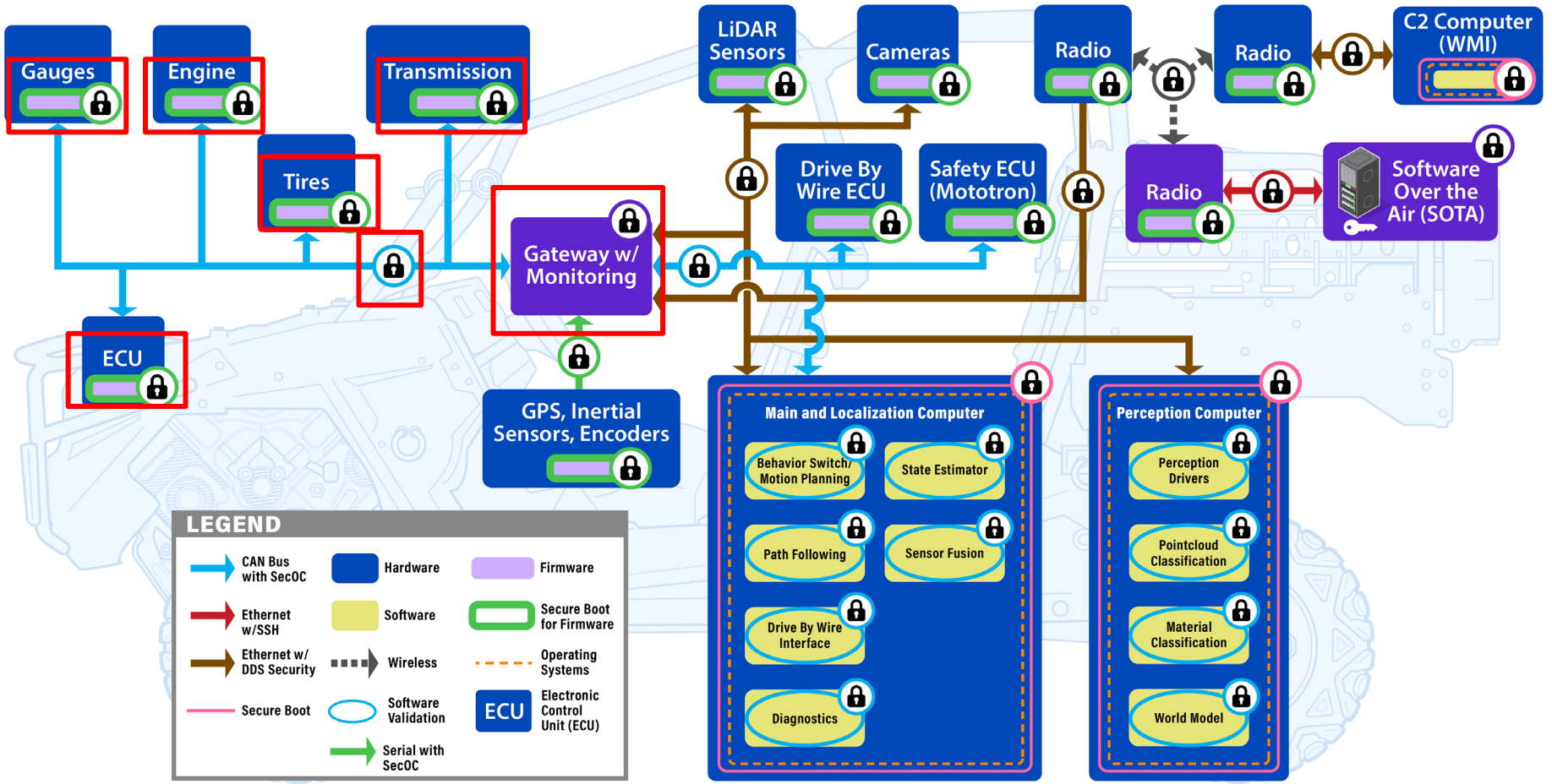
- Anomaly Detection
  - Monitor MAC error codes
    - Receiving ECUs report errors
    - Gateway logs
  - Packet Monitoring
    - Signature-based: Uses characteristics of previously identified malicious packets to uncover anomalies
    - Anomaly-based: Examines behavioral characteristics of traffic
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







Ground Vehicle



Next: Future work

Future Work

Authentication Updates:

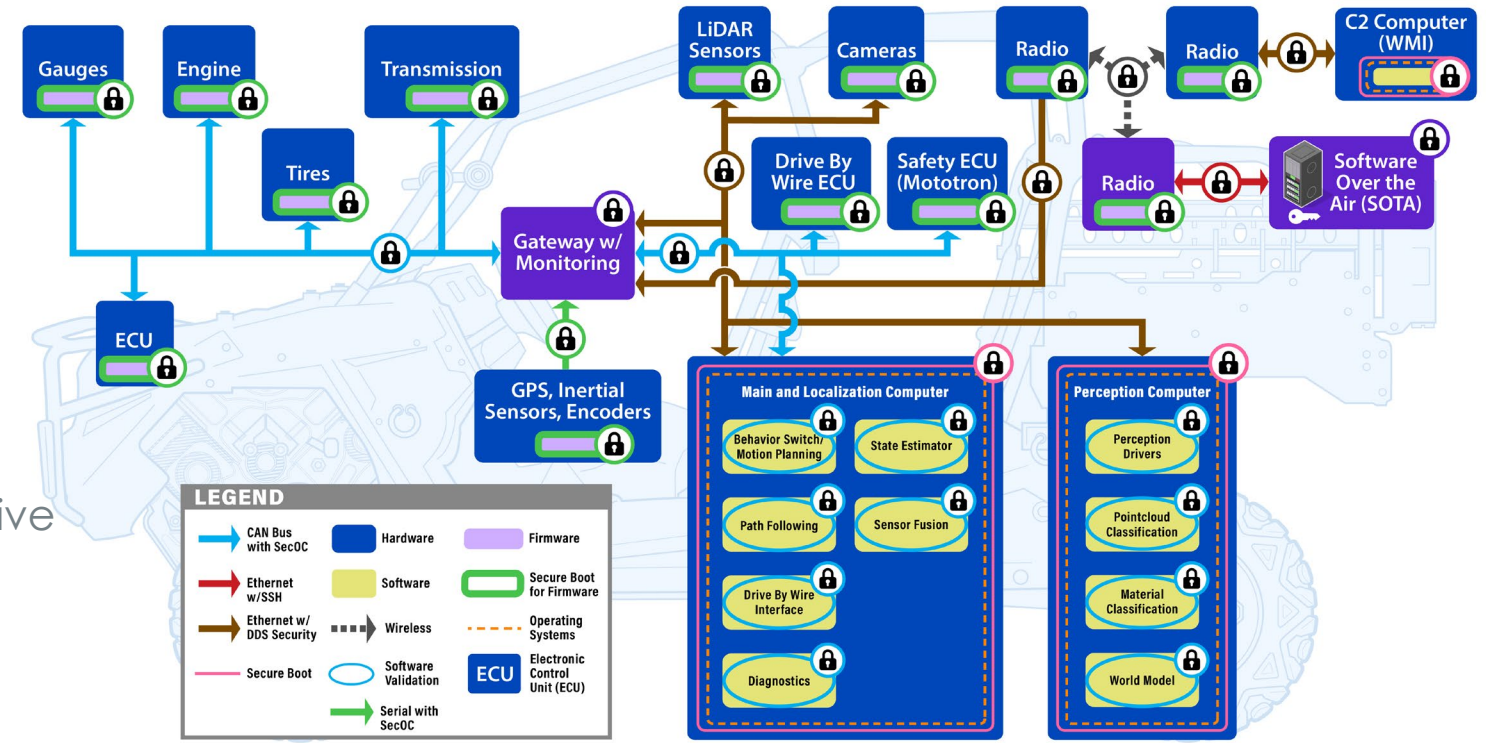
- Third Party ECUs
  - For AV ECUs, no DDS security
- DDS Security to Full AV
- Software Validation for AV codebase
- SecOC public/private key
- Key Distribution and Management

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?

Open Discussion

Any questions about the Auto-ISAC or future topics for discussion?

How to Get Involved: Membership

If you are an OEM, supplier or commercial vehicle, Carrier or Fleet, please join the Auto-ISAC!

- Real-time Intelligence Sharing
- Intelligence Summaries
- Regular intelligence meetings
- Crisis Notifications
- Member Contact Directory
- Development of Best Practice Guides
- Exchanges and Workshops
- Tabletop exercises
- Webinars and Presentations
- Annual Auto-ISAC Summit Event

To learn more about Auto-ISAC Membership and Partnership, please contact melissacromack@automotiveisac.com.

Auto-ISAC Partnership Programs

Strategic Partnership

- **For-profit** companies such as "Solutions Providers" that sell connected vehicle cybersecurity products & services.
- **Examples:** *Hacker ONE, Upstream, IOActive, Karamba, Grimm*

1. **Must be approved** by Executive Director and the Membership & Benefit Standing Committee (MBSC).
2. Formal agreements: **NDA, SPA, SoW, CoC** required.
3. **In-kind contributions** allowed. Currently no fee.
4. **Does not** overtly sell or promote product or service.
5. Commits to **support the Auto-ISAC's mission.**
6. Engages with the automotive ecosystem, **supporting & educating Auto-ISAC Members and its Community.**
7. **Develops value added Partnership Projects** to engage with the Auto-ISAC, its Member, and Community.
8. **Summit Sponsorship** allowed for promotion. Summit Booth **priority**.
9. Engagement **must provide Member awareness, education, training, and information sharing**
10. **Builds relationships, shares, and participates** in information sharing Auto-ISAC activities.
11. Supports our mission through **educational webinars and sharing of information.**

Community Partnership

- **Community Partners** are companies, individuals, or organizations with a complementary mission to the Auto-ISAC, with the interest in engaging with the automotive ecosystem, supporting, and educating Members and the community.
- Includes ***Industry Associations, Government Partners, Academia, Research Institution, Standards Organizations, Non- Profit, Technical Experts, Auto-ISAC Sponsors*.**
- **Examples:** *Autos Innovate, ATA, ACEA, JAMA, MEMA,CLEPA, CISA, DHS, FBI, NHTSA, NCI, UDM etc.*

1. **No formal agreement** required.
2. **No approval** required.
3. Added to **Auto-ISAC Community Distro** List to stay engaged in Community events and activities.
4. Participate in **Auto-ISAC Monthly Community Calls.**
5. Learn **what is trending** in the ISACs and hear from key leaders during the **special topic of interest** presentation.
6. Added to **Auto-ISAC DRIVEN** list to receive our **daily cyber automotive newsletter.**
7. Part of the Network with **Automotive Community and the extended automotive ecosystem.**
8. Invitation to **attend and support** our yearly Summit.

Current Partnerships

Many organizations engaging

Thanks for your Support to our Many Partners

Community Partners

INNOVATOR
Strategic Partnership (20)

ArmorText
BlockHarbor
Cybellum
Deloitte
FEV
GRIMM
HackerOne
Irdeto
Itemis
Karamba Security
KELA
Pen Testing Partners
Red Balloon Security
Regulus Cyber
Saferide
Security Scorecard
Trustonic
Upstream
VicOne
Vultara

NAVIGATOR
Support Partnership

AAA
ACEA
ACM
American Trucking Associations (ATA)
ASC
ATIS
Auto Alliance
EMA
Global Automakers
IARA
IIC
JAMA
MEMA
NADA
NAFA
NMFTA
RVIA
SAE
TIA
Transport Canada

COLLABORATOR
Coordination Partnership

AUTOSAR
Billington Cybersecurity
Cal-CSIC
Computest
Cyber Truck Challenge
DHS CSVI
DHS HQ
DOT-PIF
FASTR
FBI
GAO
ISAO
Macomb Business/MADCAT
Merit (training, np)
MITRE
National White Collar Crime Center
NCFTA
NDIA
NHTSA
NIST
Northern California Regional Intelligence Center (NCRIC)
NTIA
OASIS
ODNI
Ohio Turnpike & Infrastructure Commission
SANS
The University of Warwick
TSA
University of Tulsa
USSC
VOLPE
W3C/MIT
Walsh College

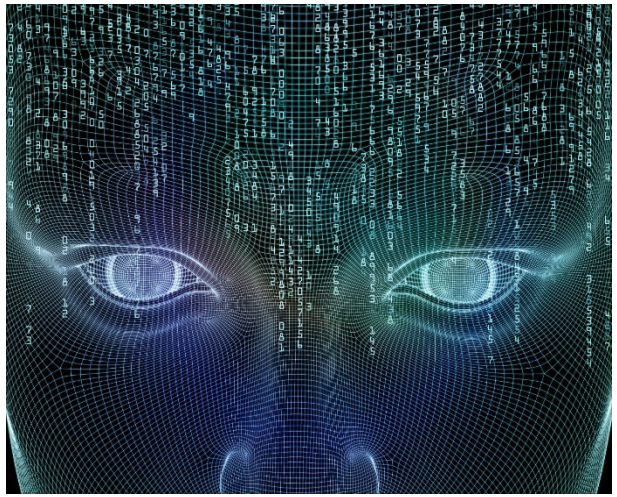
BENEFACTOR
Sponsorship Partnership

2022 Summit Sponsors-

Argus
BGNetworks
Bosch
Blackberry
Block Harbor
BlueVoyant
Booz Allen Hamilton
C2A
Cybellum
CyberGRX
Cyware
Deloitte
Denso
Finite State
Fortress
Itemis
Keysight Technologies
Micron
NXP
Okta
Sandia
Securonix
Tanium
UL
Upstream
VicOne

Auto-ISAC Benefits

- Focused Intelligence Information/Briefings
- Cybersecurity intelligence sharing
- Vulnerability resolution
- Member to Member Sharing
- Distribute Information Gathering Costs across the Sector
- Non-attribution and Anonymity of Submissions
- Information source for the entire organization
- Risk mitigation for automotive industry
- Comparative advantage in risk mitigation
- Security and Resiliency



Building Resiliency Across the Auto Industry

Thank You


THANK
YOU
GRAZIE
MERCI
MULTUMESC
MAAKE
TERMA KASIH
RAIBH MAITH AGAT
JUSPAXAR
OBRIGADO
MATONDO
KIITOS
SALAMAT
MOCHCHAKKERAM
KIA ORA
MULTUMESC
CHOKRANE
SALAMAT
CAM ON BAN
MERCI
RAIBH MAITH AGAT
OBRIGADO
MOCHCHAKKERAM
ASANTE
UA TSAUG RAU KOJ
MOCHCHAKKERAM
CHOKRANE
MATUR NUWUN
MATONDO
CHOKRANE
UA TSAUG RAU KOJ
DANK JE
RAIBH MAITH AGAT
SPASIBO
MAAKE
OBRIGADO
SPASIBO
WELALIN
ARIGATO
MOCHCHAKKERAM
OBRIGADO
KIITOS
DANKON
NIRRINGRAZZJAK
MOCHCHAKKERAM
MULTUMESC
VINAKA
KIITOS
OBRIGADO
DANK JE
NIRRINGRAZZJAK
MAMANA

Our Contact Info

Faye Francy
Executive Director

AUTO-ISAC
Automotive Information Sharing and Analysis Center

20 F Street Northwest
Suite 700
Washington, DC 20001
703-861-5417
fayefrancy@automotiveisac.com

AUTO-ISAC
Automotive Information Sharing and Analysis Center

AUTOMOTIVEISAC.COM