Vehicle Cyber Security

Collaboration
SAE and ISO

SAE J3061 → **ISO/SAE 21434**

Cybersecurity Guidebook for Cyber-Physical Automotive Systems

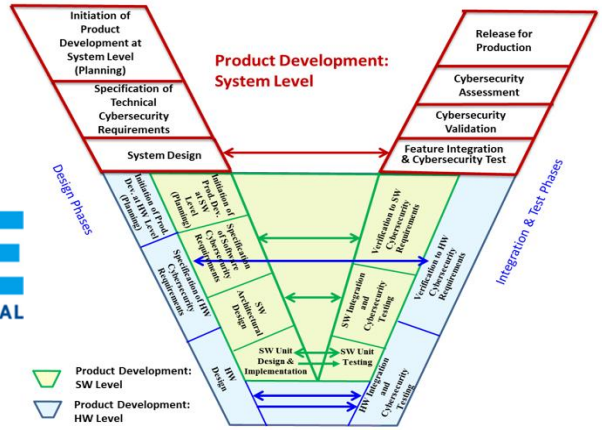
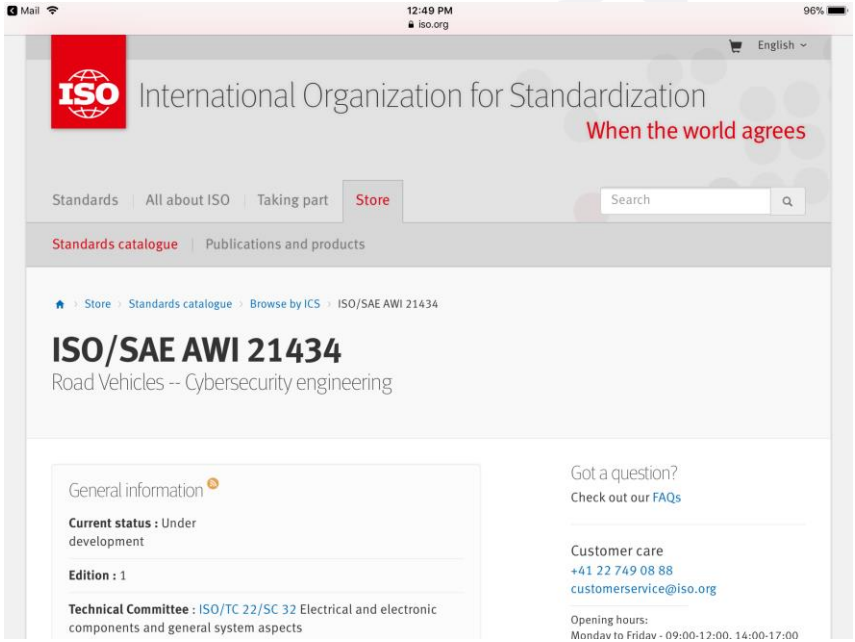
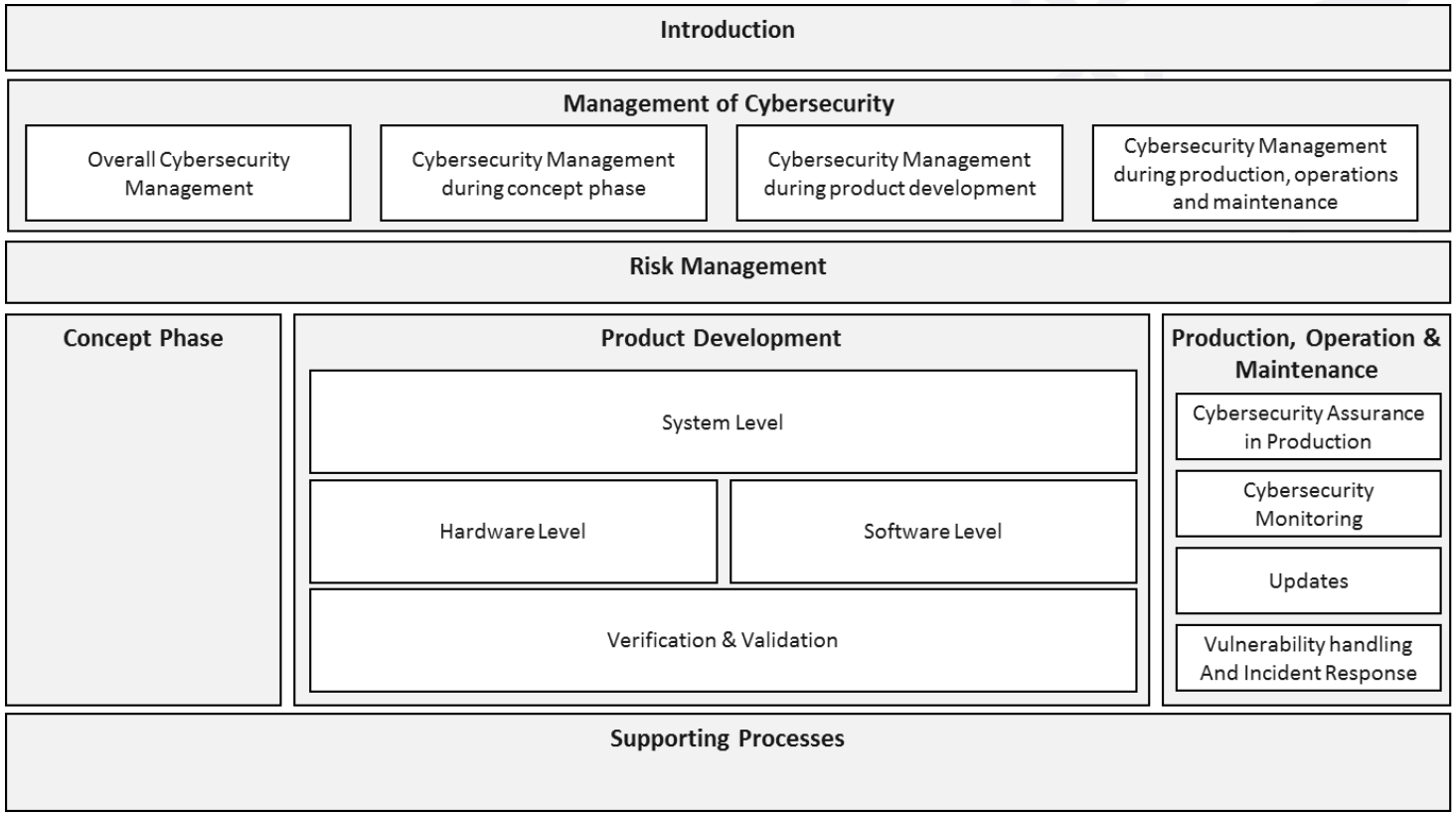


Figure 5 - Relationships between product development at the system, hardware, and software levels



ISO/SAE 21434 Overview



Vehicle Cyber Security

ISO/SAE 21434

Dividing Up the Beast

Layers of Vehicle Security

OEM and Fleet Specific

IEEE 1609.x, ISO 2007x, **SAE J1939-91B**
DSRC, V2X, ITS, ExVe, SOTA

SAE J1939-31 and **SAE J1939-91A**
Network Architecture Recommendations

AUTOSAR SecOC, **SAE J1939-91C**
In-Vehicle and ECU Secure Data Transfer

ISO 14229-1 and SAE J3101
ECU Protected Boot, Secure Flash,
Authorization and Authentication

Foundation Level Vehicle Security Recommendations:
SAE J3005, SAE J3061, ISO 15765-5, SAE J3138, **SAE J1939-91A**
Diagnostics Interface Security

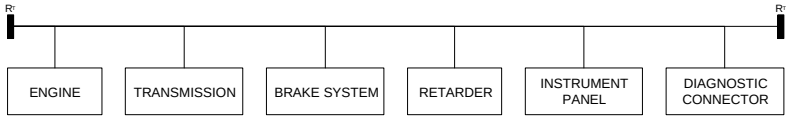
ISO/SAE 21434

SAE J1939-91 Network Security

The document is divided into **3 Parts: A, B and C**

RATIONALE:

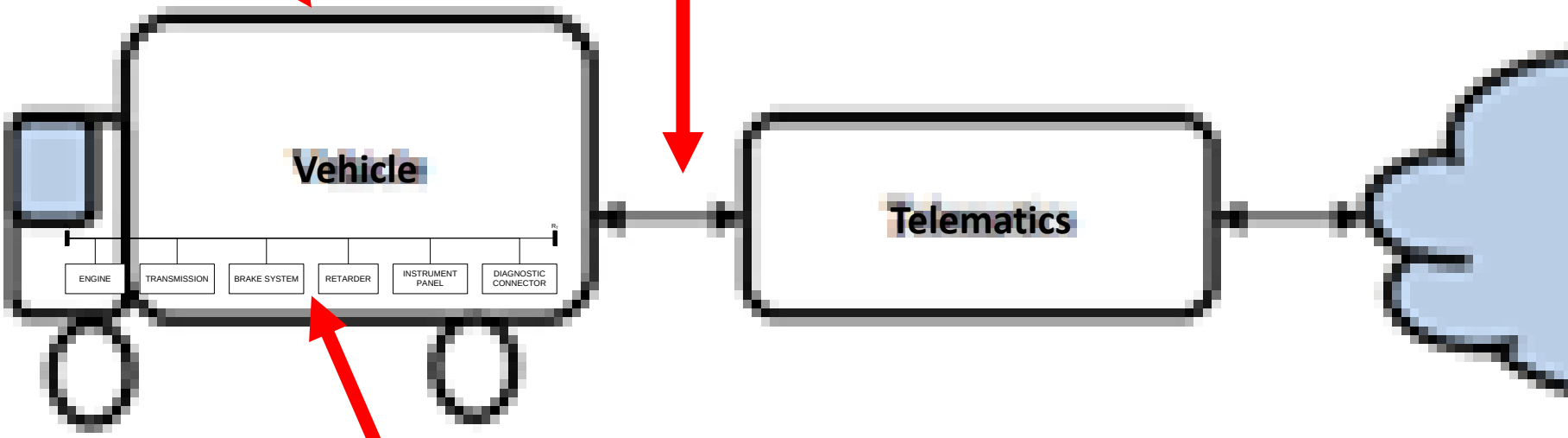
- PROVIDE GUIDELINES FOR SECURING COMMUNICATIONS WITH VEHICLES UTILIZING THE SAE J1939 NETWORK.



SAE J1939 Network Security

J1939-91 Scope

J1939-91A J1939-91B



J1939-91C

SCOPE – J1939-91Part "A"

Foundation Layer Security

J1939-91A defines the recommendations for security of the vehicle side of the J1939-13 connector.

- Recommendations for vehicle communications functions with a device which is connected to J1939-13 interface - diagnostics interface security. [Similar to SAE J3138 diagnostics link security and SAE J3005-2 "dongle" device security]
- General requirements for "Imposter Reporting" for devices that may spoof J1939 Source Addresses.

Layer 1 Security
Individual ECU

ISO 14229-1 and SAE J3101 ✓

- ECU Protected Boot, Secure Flash
- Authorization and Authentication

SCOPE – J1939-91Part "C"

In-Vehicle Network Security

J1939-91C defines recommendations for:

- Secure on-board communications between ECUs
- Update General Vehicle Network Gateway recommendations and network topology reference related to J1939-31

Scope being Drafted

Committee NWIP Draft

ASAM collaboration
→ Proposal draft?

Layer 4 Security

Connected Vehicle Security

Scope of SAE J1939-91B: Bi-Directional secure Over The Air (OTA) communications via a telematics interface to the vehicle

ASAM collaboration
→ Proposal draft?

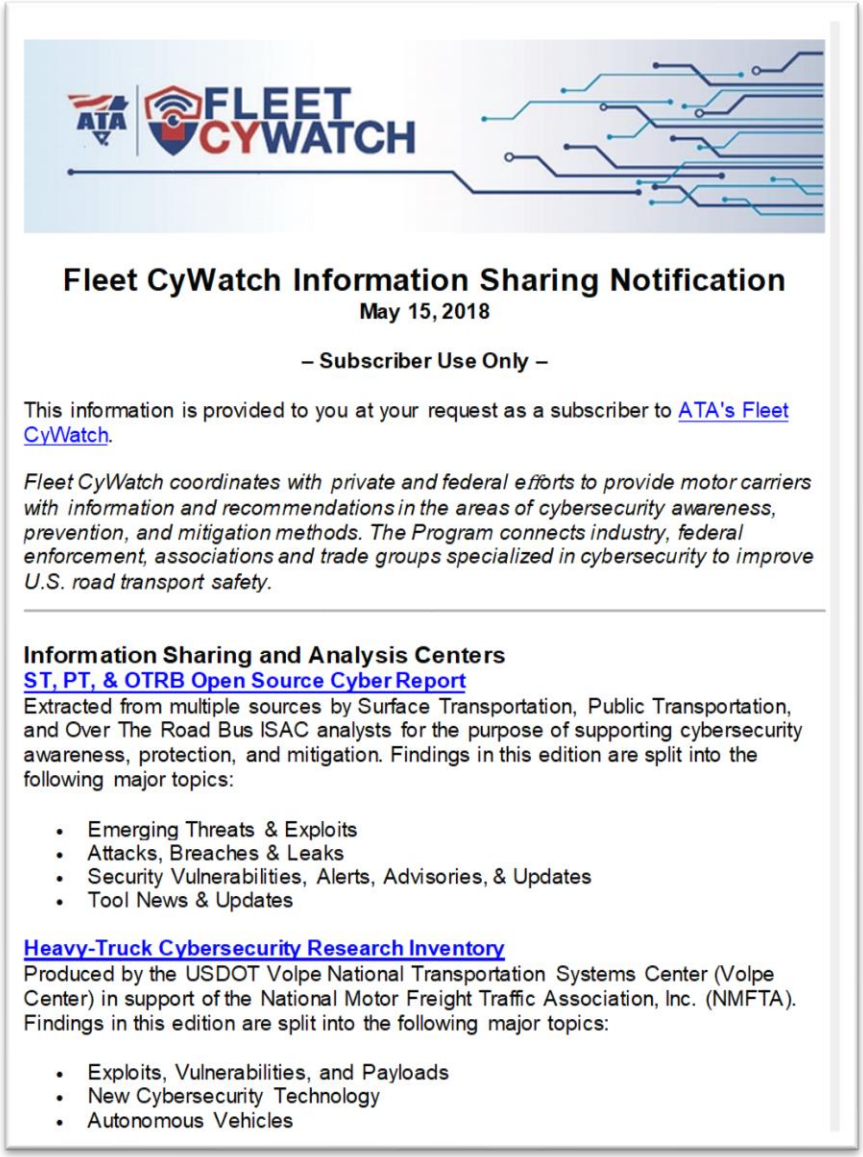
- Extended Vehicle (ExVe) Systems and Intelligent Transportation Systems (ITS) ✓
  - IEEE 1609.x (DSRC)
  - ISO 20077, ISO 20078, ISO 20080, etc.
  - ISO/SAE 21434
  - ISO TC204 work items (ITS)

Layer 5: ATA's ✓ Fleet CyWatch

Information Sharing Notification (ISN)

- Surface Transportation ISAC
- Public Transportation ISAC
- Over The Road Bus ISAC
- Auto-ISAC
- Homeland Security
  - Critical Infrastructure
  - Highway & Motor Carrier
  - NCCIC Portal
- Federal Bureau of Investigation
  - FBI CyWatch Alerts
  - IC3 Updates
- Industry Best Practices
  - NIST Cyber Framework
  - NHTSA & FMCSA Cybersecurity
  - SAE Standards & Guidebooks
  - DHS TSA Programs
- TMC RP Developments & Events
- NMFTA Research & Events

Direct link to reporting cybercrime



Fleet CyWatch Information Sharing Notification
May 15, 2018

– Subscriber Use Only –

This information is provided to you at your request as a subscriber to ATA's Fleet CyWatch.

Fleet CyWatch coordinates with private and federal efforts to provide motor carriers with information and recommendations in the areas of cybersecurity awareness, prevention, and mitigation methods. The Program connects industry, federal enforcement, associations and trade groups specialized in cybersecurity to improve U.S. road transport safety.

Information Sharing and Analysis Centers
ST, PT, & OTRB Open Source Cyber Report
Extracted from multiple sources by Surface Transportation, Public Transportation, and Over The Road Bus ISAC analysts for the purpose of supporting cybersecurity awareness, protection, and mitigation. Findings in this edition are split into the following major topics:

- Emerging Threats & Exploits
- Attacks, Breaches & Leaks
- Security Vulnerabilities, Alerts, Advisories, & Updates
- Tool News & Updates

Heavy-Truck Cybersecurity Research Inventory
Produced by the USDOT Volpe National Transportation Systems Center (Volpe Center) in support of the National Motor Freight Traffic Association, Inc. (NMFTA). Findings in this edition are split into the following major topics:

- Exploits, Vulnerabilities, and Payloads
- New Cybersecurity Technology
- Autonomous Vehicles

Standardize PKI Management Process Needed

SAE INTERNATIONAL

NWIP Coming Soon

M city UNIVERSITY OF MICHIGAN

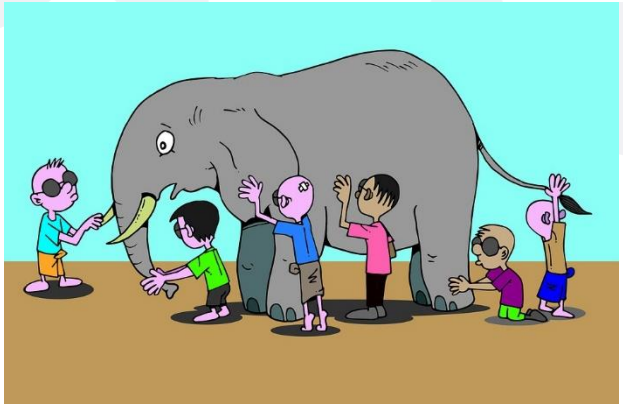
SAE and ASAM collaboration on J1939-91

- **Will ASAM draft a proposal for "Part B"?**
  - **Secure Telematics**
- **Will ASAM draft a proposal for "Part C"?**
  - **Secure ECU to ECU**

- Response by Dec. 1st to ideation@asam.net from ASAM Members with a commitment of a certain number of person days
- Interest group prepares a draft of a ASAM proposal document until end of January with the help of a document owner from ASAM
- Then a Joint ASAM/SAE proposal workshop will be held on Feb.18th at Santa Fe, NM
- Afterwards, the TSC will vote on the project and budget

Questions or Comments?

Mark Zachos
DG Technologies
mzachos@dgtech.com



Chairman:

- SAE J1939 Network Security Task Force
- SAE Data Link Security Committee
- ATA/TMC Cyber Security Issues Task Force

Head of US Delegation

- ISO TC22/SC31