AGENDA

Heavy-Duty Diesel Vehicle Inspection and Maintenance (IM) Working Group Conference Call
Thursday, August 15, 2019
10:30 am (US Central Time Zone)

Call Information
Call Number: 1-888-909-7654
Participant PIN: 504571#
Join WebEx:
https://nctcog.webex.com/nctcog/j.php?MTID=m3f9c73580bfba68c880665c3a755cd5f
(Meeting Number 803 319 652)

1. Welcome and Introductions .... Chris Klaus, NCTCOG
2. Real Emissions Assessment Logging (REAL) ... Tom Montes, Manager, Diesel OBD Section, California Air Resources Board
3. Heavy-Duty On-Road Vehicle IM Program ....Tom Durbin, UC Riverside
4. Cyber Security and Vehicle Diagnostics .... Mark Zachos, DG Technologies
5. Partner Updates:
    a. Arizona Department of Environmental Quality
    b. California Air Resources Board
    c. Clark County, Nevada
    d. Colorado Department of Public Health & Environment*
    e. Connecticut Department of Motor Vehicles
    f. DG Technologies
    g. Eastern Research Group
    h. Environmental Protection Agency
    i. Hong Kong Environmental Protection Department
    j. Houston Galveston Area Council
    k. Massachusetts Department of Environmental Protection
    l. Metropolitan Transportation Commission – San Francisco Bay Area
    m. New Jersey Motor Vehicle Commission
    n. New Jersey Department of Environmental Protection
    o. Oak Ridge National Laboratory
    p. Ontario Ministry of the Environment and Climate Change
    q. Oregon Department of Environmental Quality*
    r. Port of Los Angeles
    s. Rhode Island Department of Environmental Management
    t. Southwest Research Institute
    u. Texas A&M Transportation Institute
    v. Texas Commission on Environmental Quality
    w. Texas Department of Transportation
    x. Transport Scotland
    y. United Kingdom Department of Transport
    z. University of California, Riverside – Center for Environmental Research & Technology
    aa. University of Hong Kong
    bb. University of Leeds*
    cc. University of Tennessee
    dd. Utah
    ee. Vermont Air Pollution Control Program
    ff. Washington State Department of Ecology*

6. 2019 Meetings - November 21

7. Adjourn

More information found at www.nctcog.org/HDDVIMWorkingGroup.

- Heavy Duty Diesel I/M Survey
- Heavy-Duty Diesel Emissions Measurement Equipment Survey

CALIFORNIA
AIR RESOURCES BOARD

Heavy Duty On-Board Diagnostics Program: Real Emissions Assessment Logging (REAL)

Tom Montes
Manager, Diesel On-Board Diagnostics Section

August 15, 2019

Background

Light-duty OBD II integrated into I/M long ago

- Used in every State I/M program in the US
- 250M+ OBD II cars on the road in the US (1996MY+)
- 30,000+ OBD inspections per day just in CA

Light-duty experience was used to develop HD OBD regulation

Safeguards to ensure test integrity

- Identification of recent code clearing
- Permanent fault codes to verify faults have been properly repaired
- Tampered software
- Fraudulent inspection

Regulation protection to ensure I/M compatibility

- Rigorous production vehicle testing to verify standardization is met
- In-use testing to verify diagnostics calibrated and functioning correctly
- Mandatory recall for problems that prevent valid test results during inspection

CARB

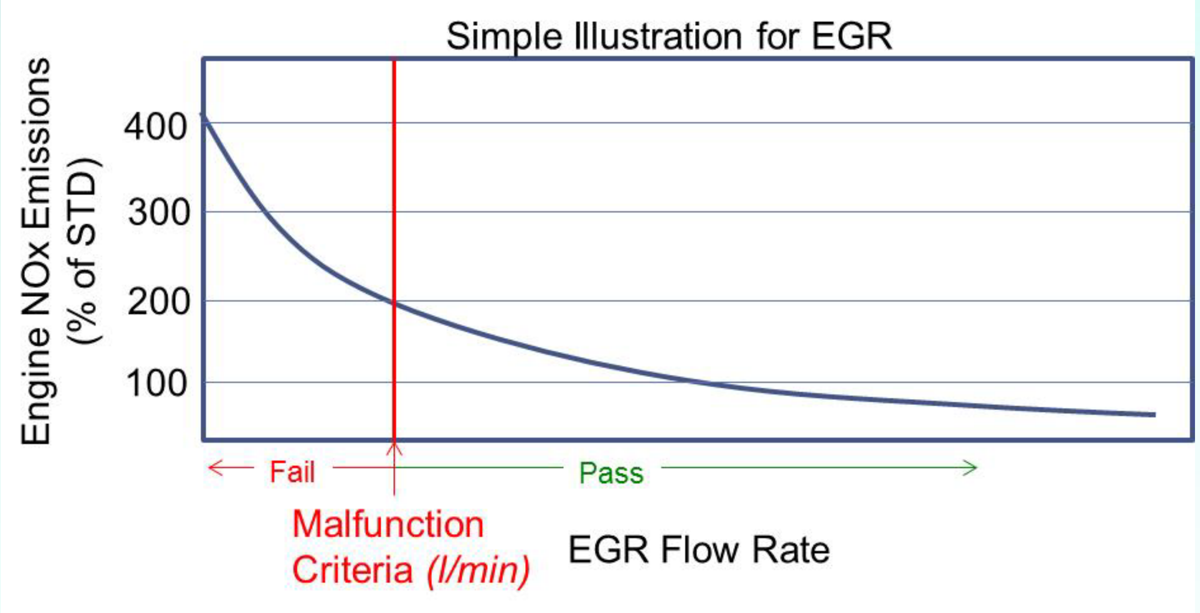
Background

Software routines ("diagnostics") in the on-board computer assess the performance of emission controls

- Uses existing sensors and controls to carry out the diagnostics under defined conditions
- ~200-400 individual diagnostics

***For major emission components only*, correlate emission levels in the lab => with something you can measure on the vehicle**

- OBD does NOT directly measure emissions (HC, CO, NOx, PM)



CARB

What is REAL?

Real Emissions Assessment Logging

Requires on-road vehicle manufacturers to track and report data characterizing NOx and GHG (CO2) emissions

HD OBD: Adopted by the Board November 2018

- Has not yet taken effect (starts in 2022 MY)

LD/MD OBD II: Adopted by the Board September 2015

- Implementation started in the 2019 MY

	Light Duty	Medium Duty	Heavy Duty
NOx Tracking	n/a	Diesel engines[2]	Diesel engines[2]
GHG Tracking	All engines[1]	All engines[1]	All engines[2]

[1] Phased in over 2019 – 2021 MYs. [2] Starting 2022 MY Note: Off-Road REAL being proposed

CARB

REAL Comes in Two Flavors

NOx Tracking

- Includes engine out and tailpipe NOx mass along with several engine activity parameters
- Puts data into a variety of bins, including recent and lifetime timeframes

GHG Tracking

- Includes broader range of engine activity parameters, hybrid-specific parameters, and active GHG technology tracking
- No bins, only recent and lifetime timeframes

…this presentation focuses on the NOx Tracking part of REAL

Why do we need REAL?

NOx tracking data will:

- Provide feedback on our regulatory programs
- Improve our emissions inventory
- Provide quick, real-world screening tool for flagging potential emissions issues

Relies on existing technology and hardware to estimate and track NOx emissions

Minimum NOx mass accuracy requirement:

- +/- 20% or +/- 0.1 g/bhp-hr
- Accuracy relative to lab on special hot-start test

REAL NOx Data is stored in arrays

Arrays

- Active 100 Hour array
- Stored 100 Hour array
- Lifetime array
- Lifetime Eng. Actv array

Parameters in each array

- NOx Mass - Engine Out (g)
- NOx Mass - Tailpipe (g)
- Engine Output Energy (kWh)
- Distance Traveled (km)
- Engine Run Time (hours)
- Fuel Consumption (liters)

Bins in each parameter

- Speed/power bins 1 to 14
- NTE bin
- Regen bin
- MIL-ON bin

NOx Data Arrays and Parameters

Parameter	Active 100 Hour Array	Stored 100 Hour Array	Lifetime Array	Lifetime Engine Activity Array
NOx mass – engine out (g)	x	x	x	n/a
NOx mass – tailpipe (g)	x	x	x	n/a
Engine output energy (kWh)	x	x	x	x
Distance traveled (km)	x	x	x	x
Engine run time (hours)	x	x	x	x
Vehicle fuel consumption (liters)	x	x	x	x

NOx Data Bins for Each Parameter in Each Array

Vehicle Speed (km/h)

% of Rated Power	0	> 0 ≤ 16	> 16 ≤ 40	> 40 ≤ 64	> 64
≤ 25%	Bin 2	Bin 3	Bin 4	Bin 5	Bin 6
> 25% ≤ 50%	Bin 2	Bin 7	Bin 8	Bin 9	Bin 10
> 50%	Bin 2	Bin 11	Bin 12	Bin 13	Bin 14

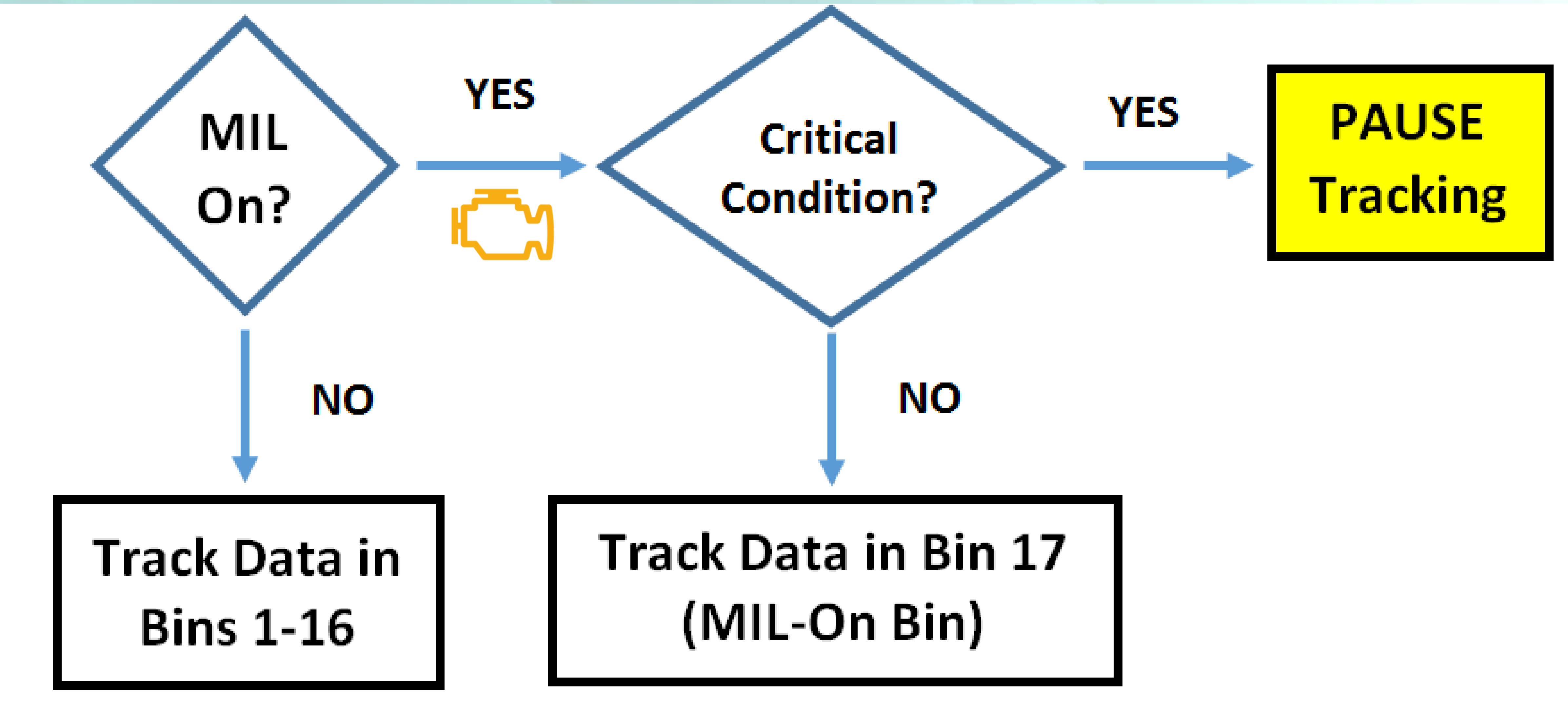
Total (Bin 1)

NTE Bin (Bin 15)

Regen Bin (Bin 16)

MIL-On Bin (Bin 17)

When to Pause NOx Tracking



Where is REAL Regulation Language?

Heavy-Duty OBD Regulation

- **Title 13, California Code of Regulations, Section 1971.1**
- (h)(5.3) NOx Tracking Requirements
- (h)(5.4)-(5.7) GHG Tracking Requirements

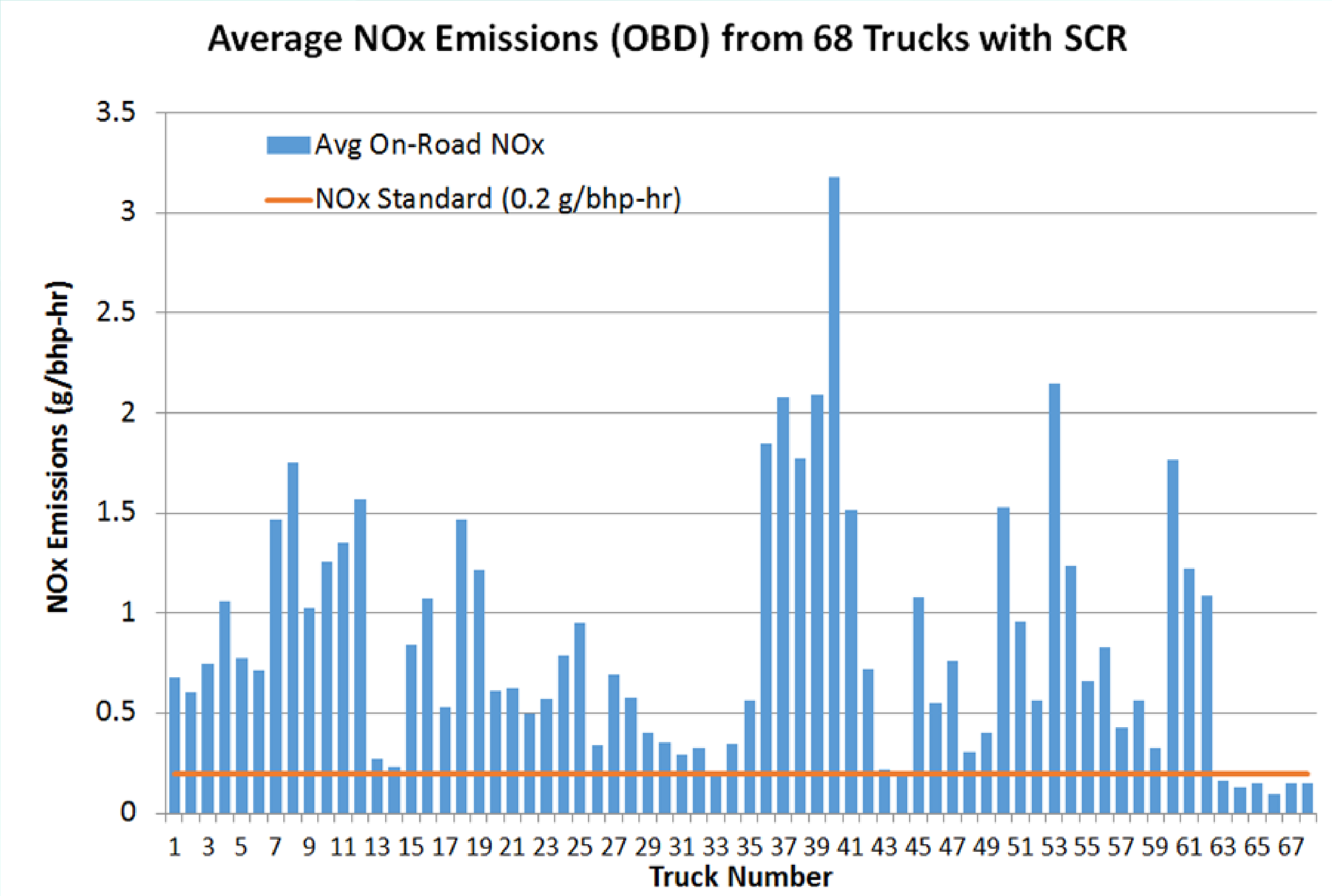
OBD II Regulation (Light/Medium Duty)

- **Title 13, California Code of Regulations, Section 1968.2**
- (g)(6.12) NOx Tracking Requirements
    - Adopted by the Board November 2018
- (g)(6.3)-(6.6), (6.8)-(6.11) GHG Tracking Requirements

In-Use NOx Performance

Real-World NOx from Trucks A Big Concern

- Project: logged OBD data from 68 trucks
- 1+ month activity each
- 2010 – 2015 MYs
- 4 engine manufacturers, many truck types & vocations

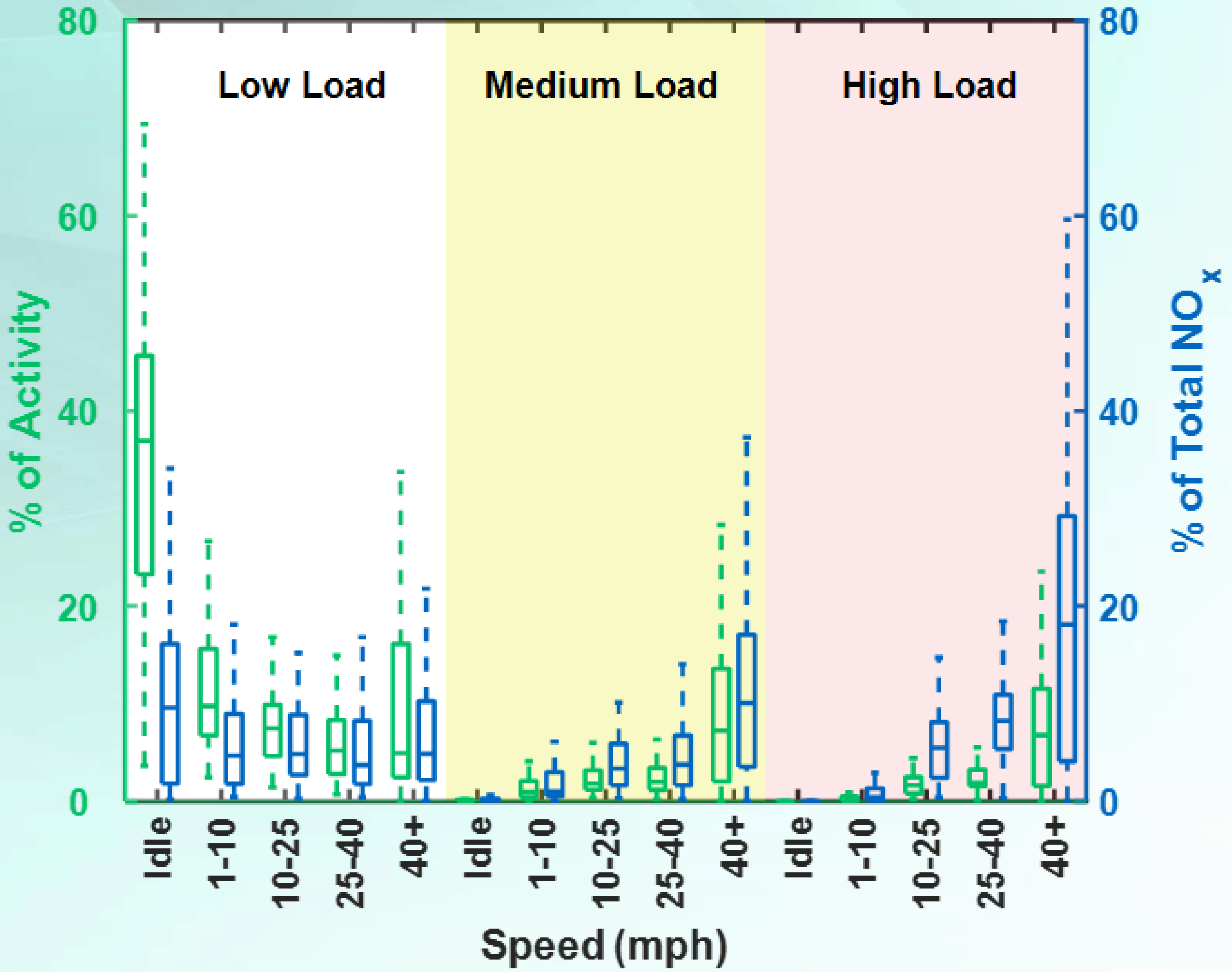


CARB

In-Use NOx Performance

Low load operation has significant activity and NOx mass emissions:

- 63% of total activity
- 34% of total NOx
- Idling: 34% of total activity
- Idling: 13% of total NOx

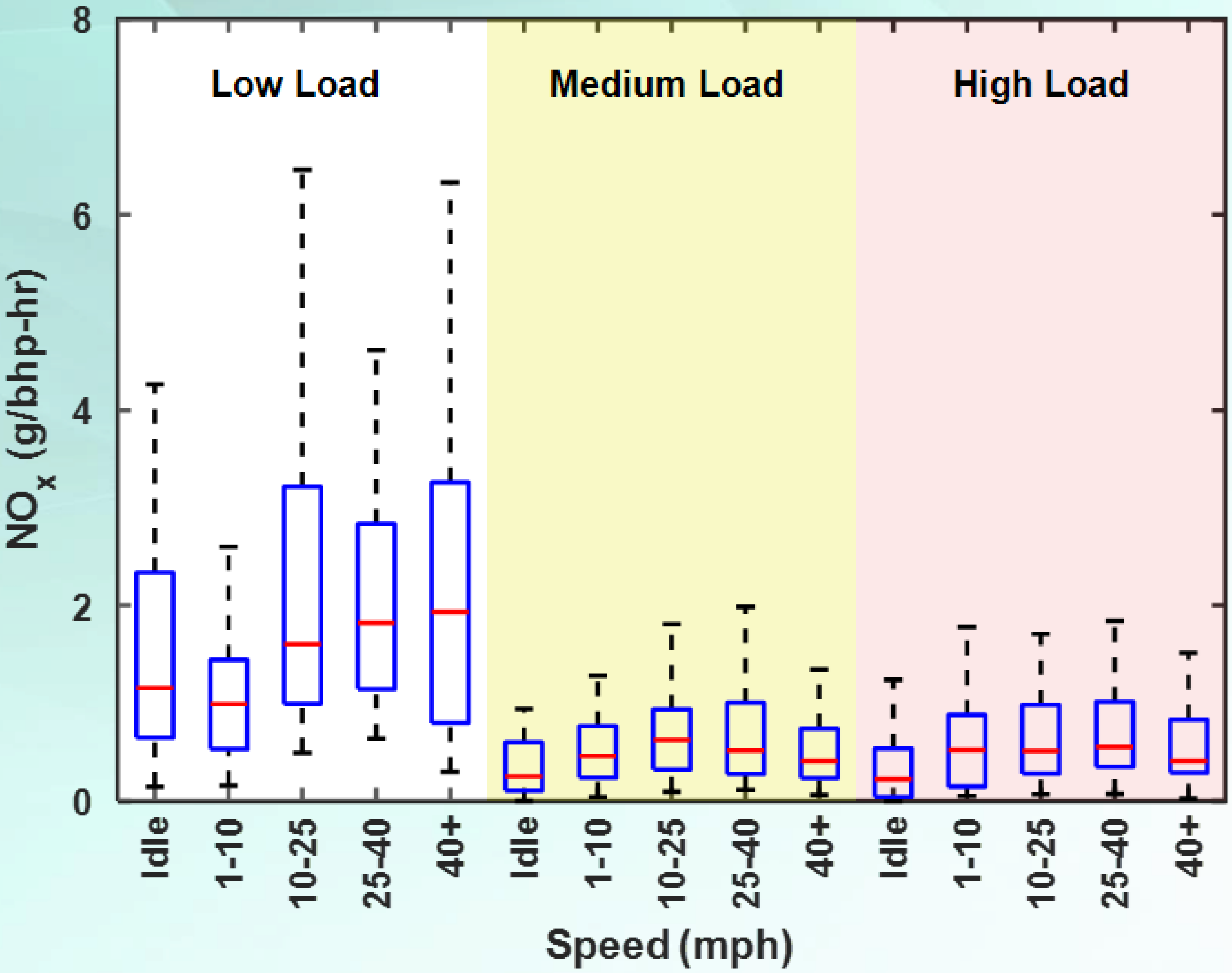


CARB

In-Use NOx Performance

- Low load operation had much higher NOx rate likely due in part to low brake work

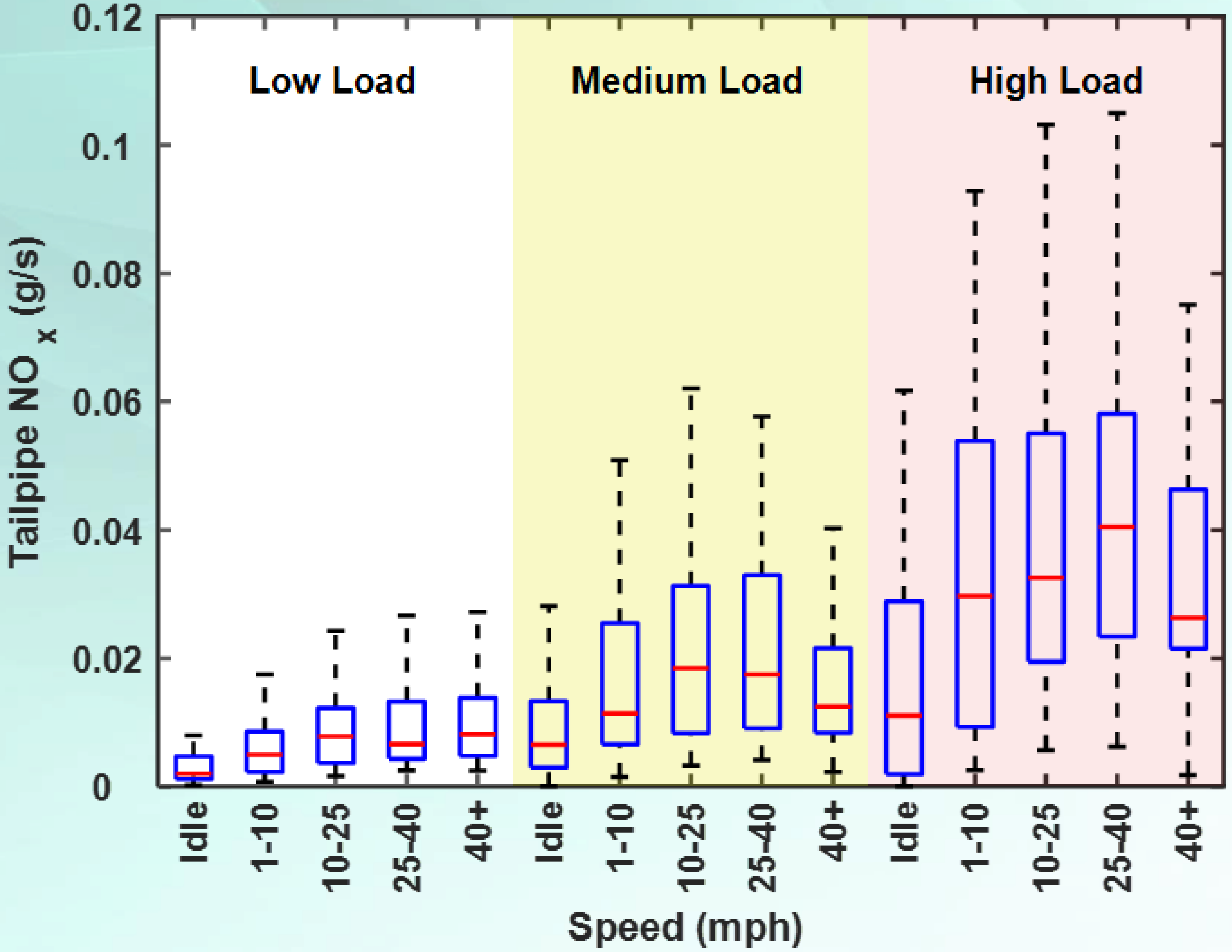
- Vehicle speed had moderate effects on brake-specific NOx emission factors



CARB

In-Use NOx Performance

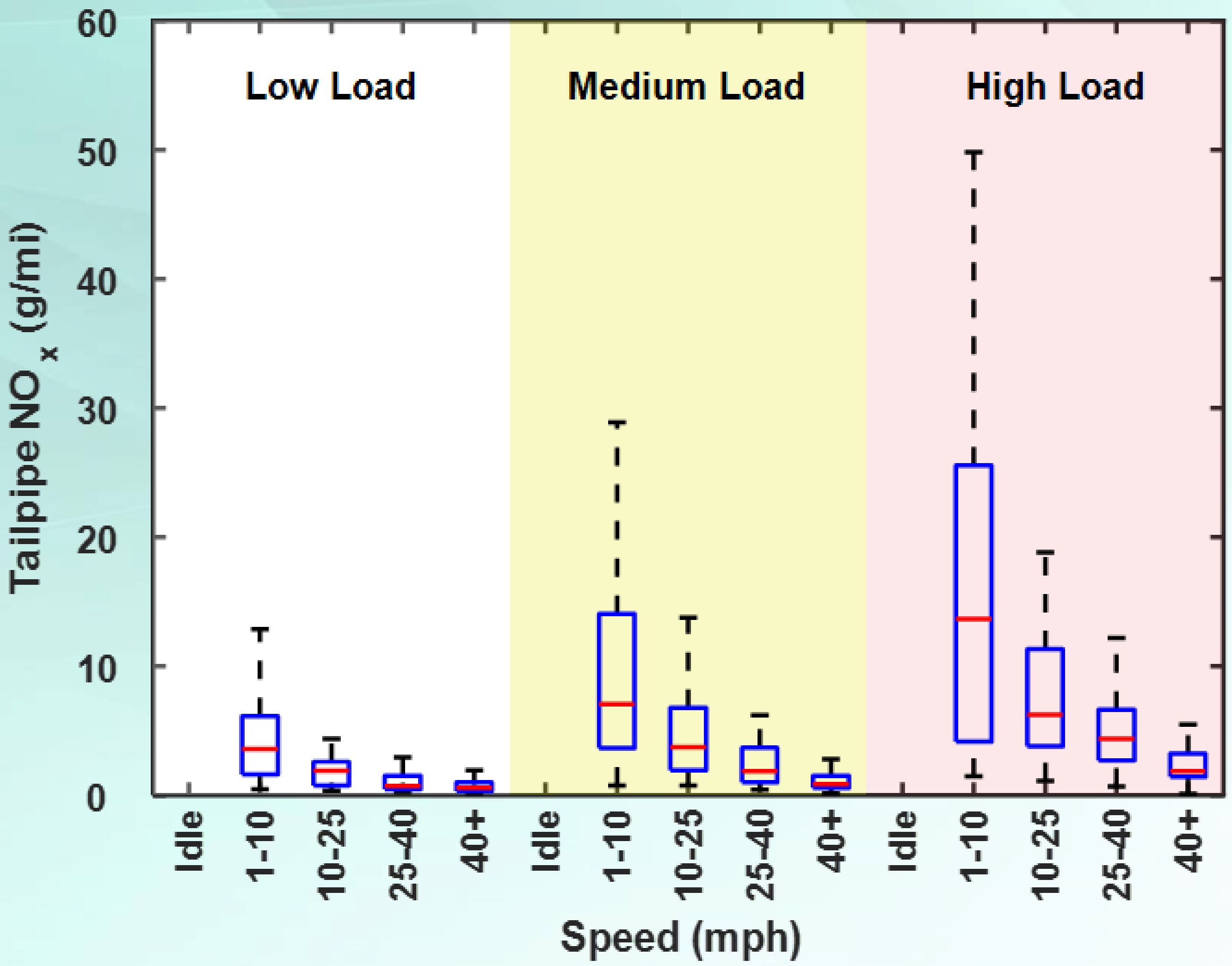
- Time-based NOx increases with vehicle speed and engine power



CARB

In-Use NOx Performance

- Highly useful for emissions inventory modeling
- Distance-based NOx increases with engine load but decreases with vehicle speed
- Acceleration events from stop have high NOx



CARB

What REAL Does Not Do

1.) Is does not Illuminate the MIL

2.) It does not fail a vehicle in I/M

3.) It does not form the basis for a compliance or enforcement action

Thomas.montes@arb.ca.gov
626-575-6777

CARB OBD Program Website:
www.arb.ca.gov/msprog/obdprog/obdprog.htm

Heavy-Duty On-Road Vehicle Inspection and Maintenance Program

Heavy-Duty Diesel Vehicle Inspection and Maintenance Workgroup

August 15, 2019

Presented By:

Thomas Durbin, Yu (Jade) Jiang, Kent Johnson, Georgios Karavalakis, Jiacheng (Joey) Yang, Edward O'Neil, and Wayne Miller
University of California, Riverside
Bourns College of Engineering
Center for Environmental Research and Technology

Mark Carlock, consultant, West Covina, CA
Nigel Clark & David McCain, University of West Virginia, Morgantown, WV
Yi Tan, Hung-Li Chang, and Seungju Yoon,
California Air Resources Board, Sacramento, CA

UCR UNIVERSITY OF CALIFORNIA, RIVERSIDE

Background

- HD vehicles estimated to represent 24% of NOx and 10% of PM from mobile sources by 2025 based on EMFAC2017.
- California has an existing heavy-duty vehicle Inspection program (HDVIP) and a Periodic Smoke Inspection Program (PSIP)
  - Snap-acceleration opacity testing (SAE J1667)
  - Vehicle and emission control label (ECL) inspections
  - No significant controls for NOx emissions
  - Not necessarily adequate for newer HD vehicles that are equipped with exhaust aftertreatment.
- California needs a more comprehensive HD I/M program.
  - Ensure in-use engines continue to meet emissions performance requirements and to deal with post-2007 trucks.

Objective

- The objective of this study is to evaluate and assess alternatives approaches and technologies for a more comprehensive HD I/M program that could be implemented in California.
- Funding from California Air Resources Board.
- Final report to be released March 2019.
  - CARB chairman series talk March 27, 2019

Pilot Program

- Vehicles having the check engine light on & needing repair or maintenance in target areas were found at two repair facilities
  - Characterize emissions before and after repair using a repair grade heavy-duty chassis dynamometer
    - 30 mph, 50 mph, idle, and high idle
  - MAHA I/M grade gaseous and PM analyzers, and opacity
  - OBD scans pre- and post-repair
- Additional instruments
  - parSYNC Plus, NTK NCEM, TSI NPET, Pegasor PPS-M, Testo PEPA
  - HEAT EDAR system and ARB PEAQS system
- Target 50 vehicles
  - 20% MY2010-2012; 80% MY2013 and newer

Pilot I/M Program – Test Matrix

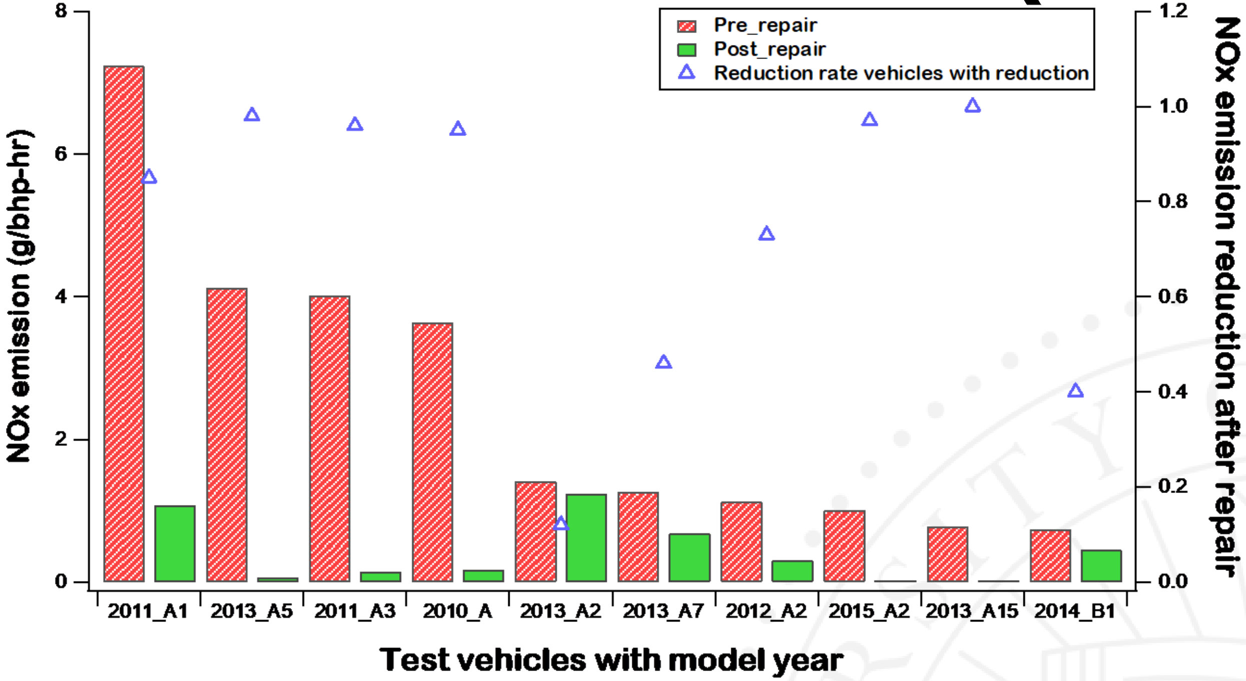
No.	Part/Repair	Targeted # of Test Vehicles	# Identified Test Vehicles
1	DPF filter cleaning*	3	3
2	DPF filter	6	3
3	exhaust pressure sensor	2	2
4	oxidation catalyst	2	0
5	injector doser	4	5.5
6	EGR valve/cooler/system	4	4.5
7	DEF filter, fluid & parts	2	5
8	turbocharger	2	2
9	boost pressure sensor	2	0
10	inlet or outlet NOx sensor	2	7.5
11	charge air cooler	2	0
12	ammonia sensor	2	1
13	SCR	2	3
14	temperature sensor	6	2
15	fuel injector	2	1
16	fuel system components	2	3
17	Engine control module (ECM)	2	3
18	lambda(O2) sensor	2	0
19	crankcase filter		2
20	crankcase pressure sensor		1
21	crank position sensor		1
22	air filter	1	1
	aborted vehicles		3 (Count as half vehicle)
	total number of vehicles	50	50.5

Two vehicles with Navistar non-SCR equipped engines excluded from subsequent analysis

Pilot I/M Program – Chassis Dyno Testing

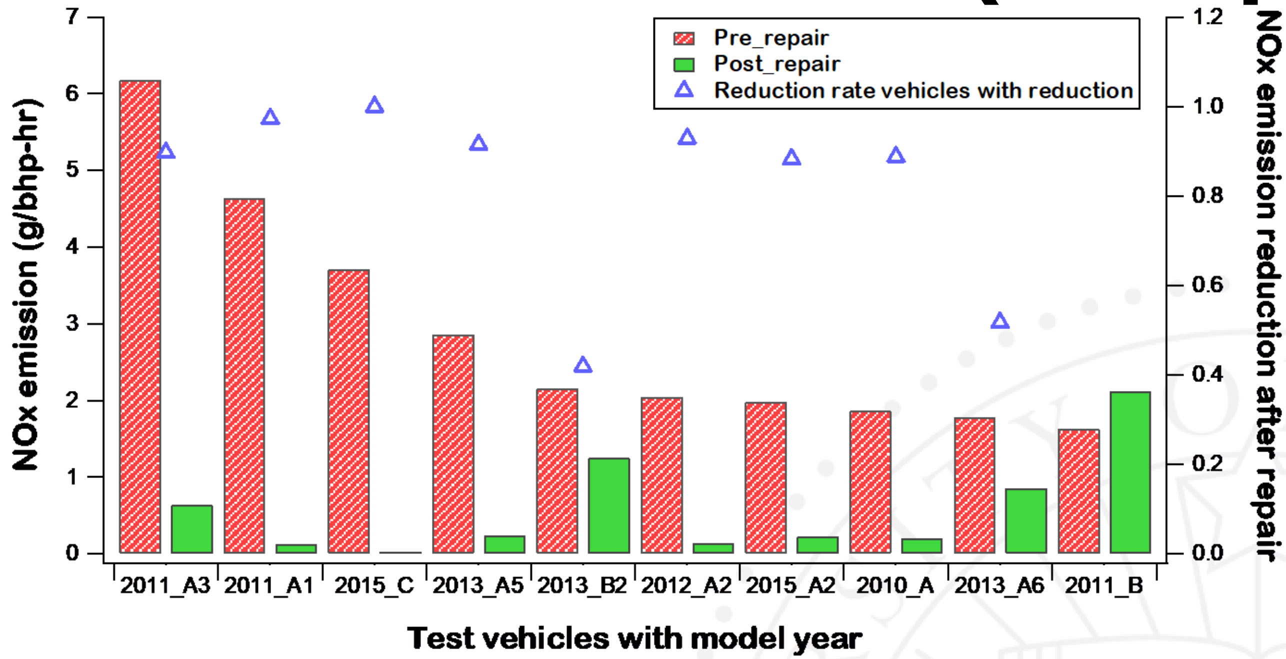
Test Sequence	
~3 -5 minute warm up @ 60 mph til NOx stable, followed by lug down test	
Dyno 50 mph @ 200 hp	
1 minute @ 50 mph	Collect Emissions
Dyno 30 mph @ 100 hp	
1 minute @ 30 mph	Collect Emissions
2 minutes Idle @ 600 rpm	Collect Emissions
1 minute High Idle @ 1800 rpm	Collect Emissions
Opacity	Triplicate tests

NOx Emissions Results (30 mph)



Vehicle NO	Repair
2011_A1	Replaced DPF and injector doser, clean DPF
2013_A5	Exhaust pressure sensor
2011_A3	Injector doser, Intake NOx sensor, clean DPF
2010_A	Injector doser, turbocharger
2013_A2	Outlet NOx sensor, Injector Doser
2013_A7	Short w/ coolant temperature sensor, thermostat
2012_A2	Clean DPF
2015_A2	DEF harness
2013_A15	Corrected/Cleaned DEF pump/harness connections
2014_B1	Turbo speed sensor

NOx Emissions Results (50 mph)



Vehicle NO	Repair
2011_A3	Injector doser, Intake NOx sensor, clean DPF
2011_A1	DPF, injector doser, DPF cleaning
2015_C	EGR cooler, valve assembly, & actuator
2013_A5	Exhaust Pressure Sensor
2013_B2	differential pressure sensor
2012_A2	Clean DPF
2015_A2	DEF harness
2010_A	Injector doser, turbocharger
2013_A6	Clean DPF/Engine Oil Cooler
2011_B	DEF lines at dosing valve, manual regen

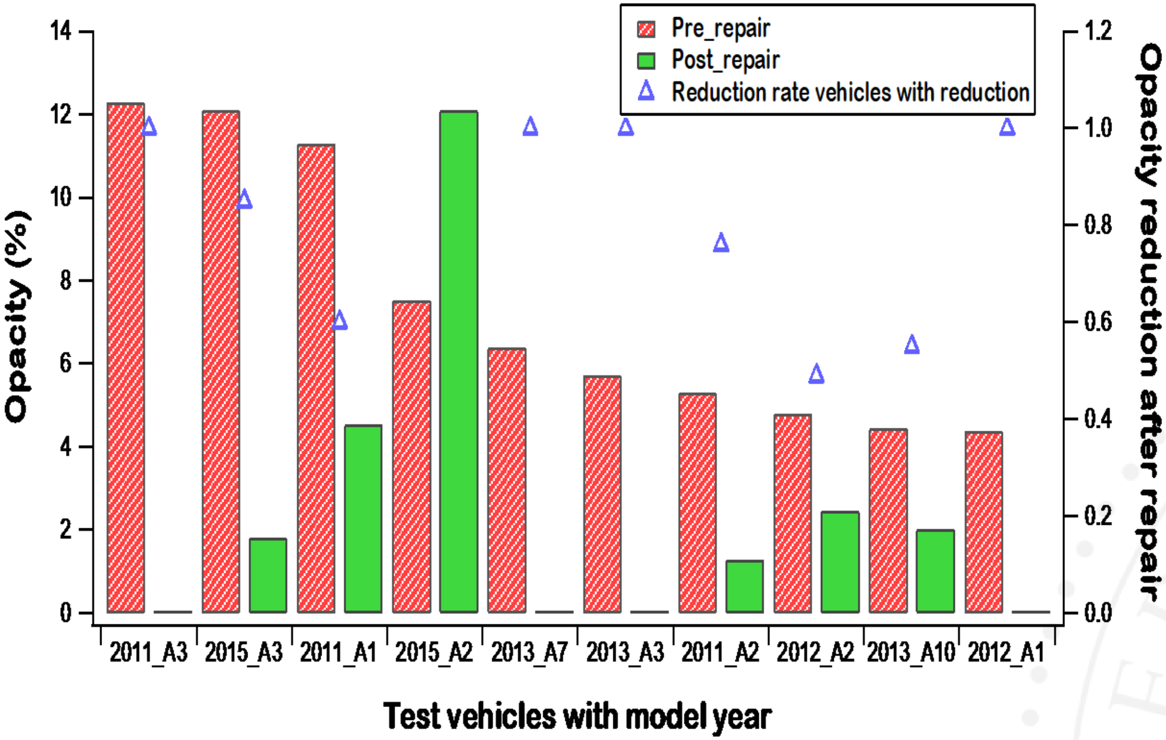
Summary NOx Emissions Results

- Pre-repair NOx for a number of vehicles were higher than 0.20 g/bhp-hr for both the 30 and 50 mph tests
- The results showed that NOx reductions for the SCR-equipped trucks were greater than 80% for 45% of the 30 mph tests and 31% of the 50 mph tests after repair.
- The highest emitters showed greater than 80% NOx reductions under all test conditions.
- Fleet average NOx reduction for check engine light on and DM1 MIL on.
- Mini-PEMS show potential to identify high emitters.

Table ES-2 NOx Emission Reductions from Pilot Study

Failure Category	Pollutant	Emission Reduction (30 mph)	Emission Reductions (50 mph)
Check Engine Lights	NOx	75%	46%
DM1 MIL on	NOx	81%	53%

Opacity Results



Vehicle NO	Repair
2011_A3	Injector doser, Intake NOx sensor, clean DPF
2015_A3	DEF harness
2011_A1	Replaced DPF and injector doser, clean DPF
2015_A2	DEF harness
2013_A7	Short w/ coolant temperature sensor, thermostat
2013_A3	Intake NOx sensor & engine harness
2011_A2	Outlet NOx sensor
2012_A2	Clean DPF
2013_A10	update ECM
2012_A1	Burned DEF system relays, DEF filter

- The pre-repair opacity values were 5% or less for all but 7 SCR-equipped vehicles.
- All 7 SCR-equipped vehicles with pre-repair opacity readings above 5% were ultimately reduced to below the 5% level.

Summary PM Emissions Results

- Opacity measurements showed the most consistent PM reductions.
- The pre-repair opacity values were 5% or less for all but 7 SCR-equipped vehicles.
- Of the 7 SCR-equipped vehicles with pre-repair opacity readings that were above 5%, all 7 vehicles were ultimately reduced to below the 5% level.
- Fleet average opacity reduced by 43%.
- Solid PN/PM measurements showed improved sensitivity (Pegasor, TSI NPET, Testo), but not necessarily consistency between the methods.

Summary

- An OBD based pilot program showed reductions in NOx and Opacity.
  - Fleet average NOx emission reductions ranged from 46 to 81%
  - Fleet average opacity reductions were 43%
- Comprehensive HD I/M may utilize several tiers of enforcement
  - OBD is primary method (possibly using telematics)
  - OBD coupled with RSD/PEAQS
  - OBD + RSD/PEAQS + mini-PEMS validation
- Results suggest a HD I/M program will provide significant and tangible emission benefits and can facilitate California's ability to meet federal ambient air quality standards, and CARB's overall air quality, sustainable freight, and climate goals.

Cyber Security and Vehicle Diagnostics

Mark Zachos
President – DG Technologies
Chairman – SAE J1939 Security Task Force
Chairman – SAE Vehicle DLC Security Committee
Chairman – ISO TC22/SC31 US TAG

Vehicle Cyber Security

Collaboration
SAE and ISO

SAE J3061 → **ISO/SAE 21434**

Cybersecurity Guidebook for Cyber-Physical Automotive Systems

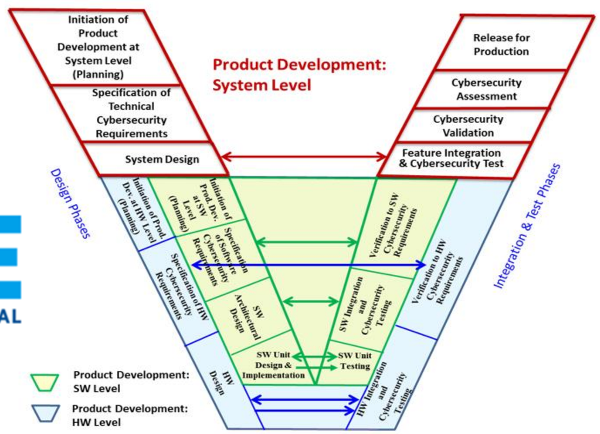
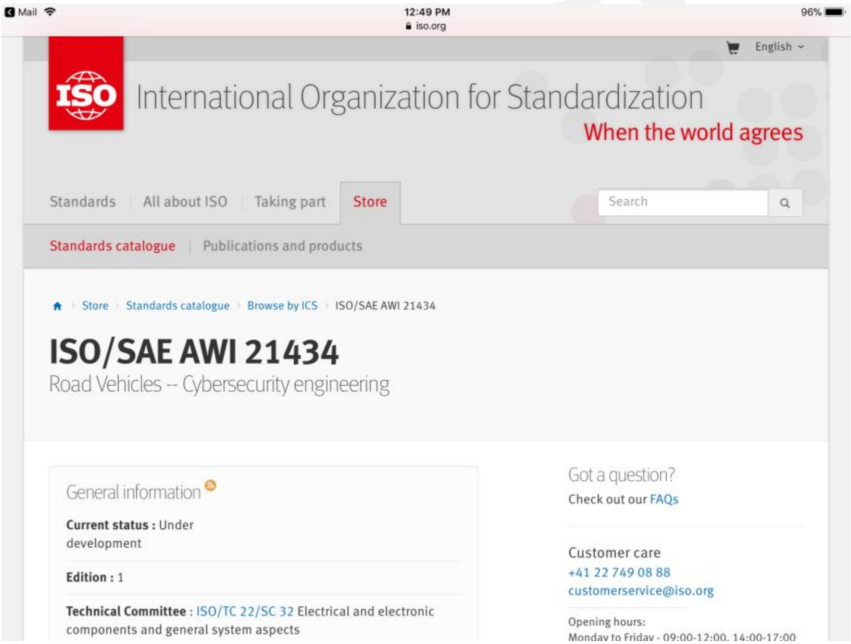
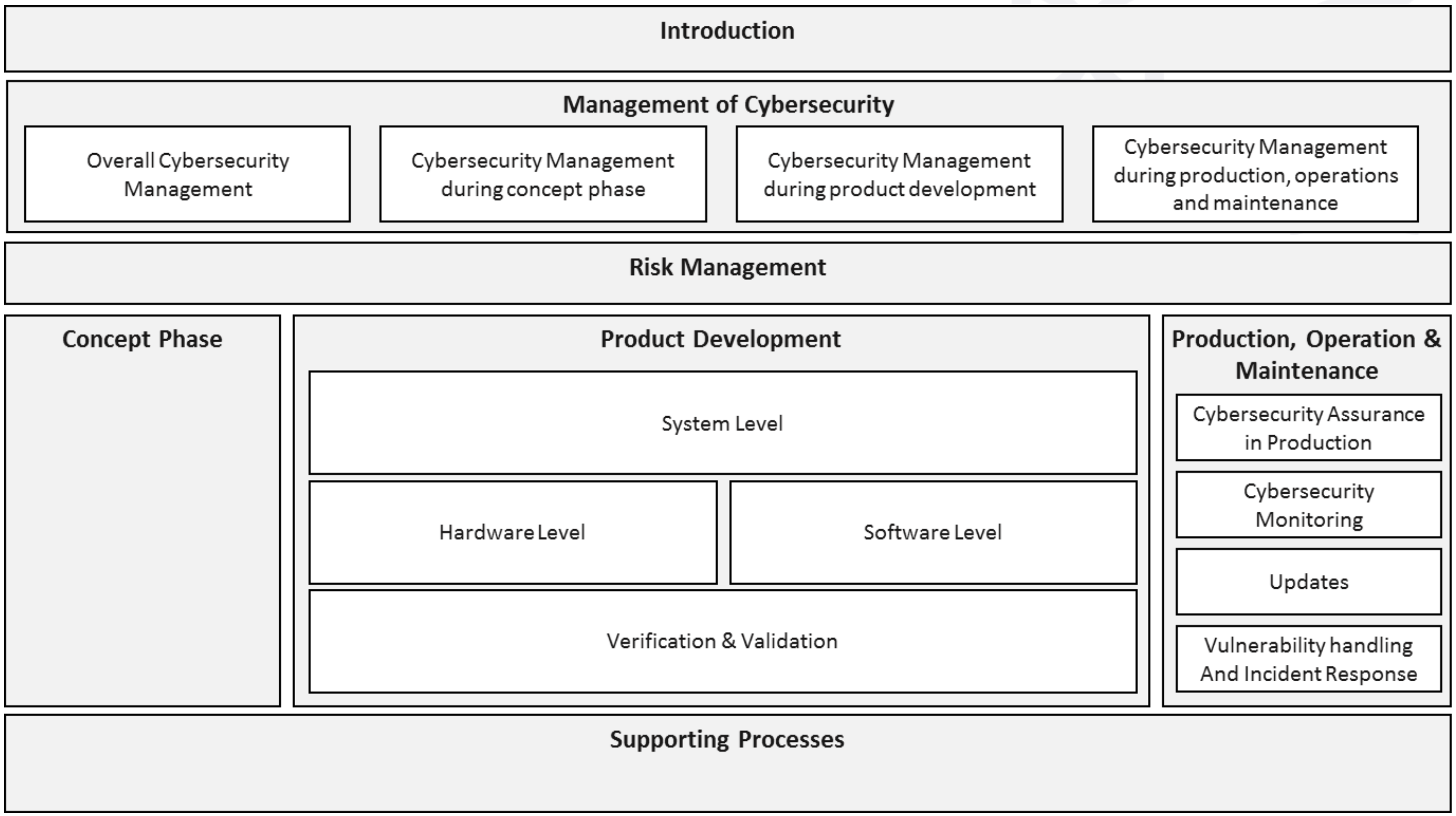


Figure 5 - Relationships between product development at the system, hardware, and software levels



ISO/SAE 21434 Overview



Vehicle Cyber Security

ISO/SAE 21434

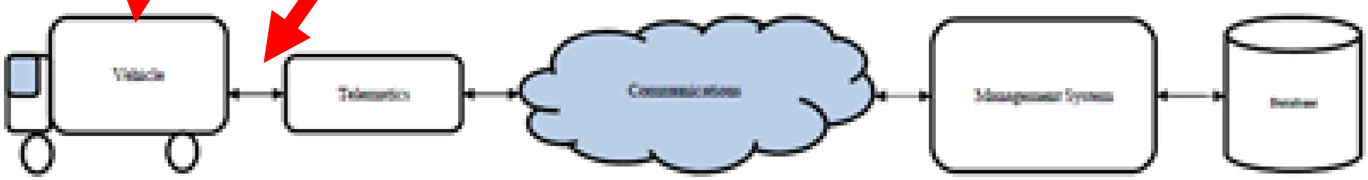
Dividing Up the Beast

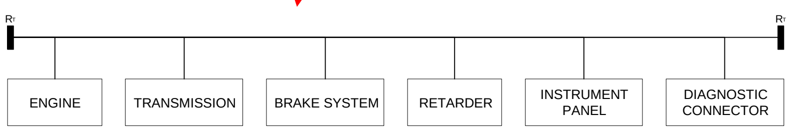
SAE J1939-91 Network Security

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

RATIONALE:

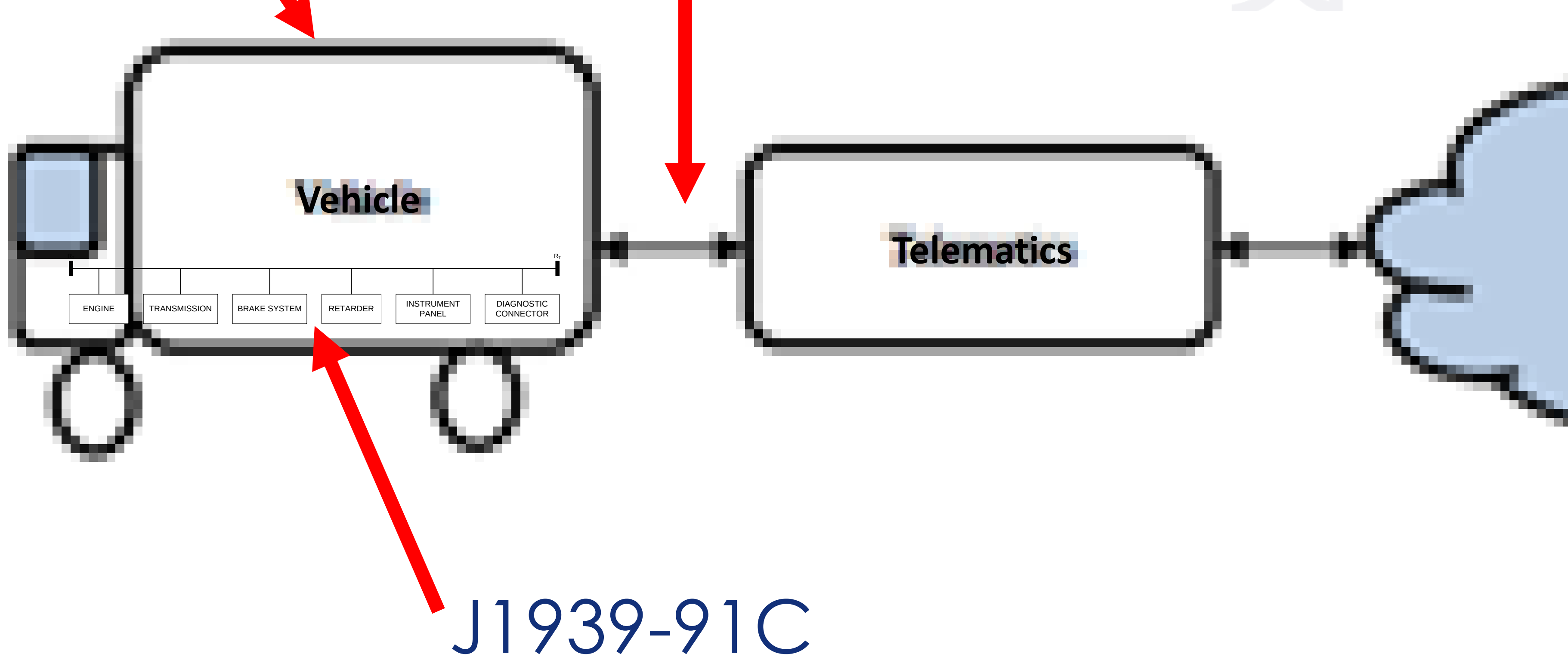
- PROVIDE GUIDELINES FOR SECURING COMMUNICATIONS WITH VEHICLES UTILIZING THE SAE J1939 NETWORK.





SAE J1939 Network Security

J1939-91 Scope



Layers of Vehicle Security

OEM and Fleet Specific

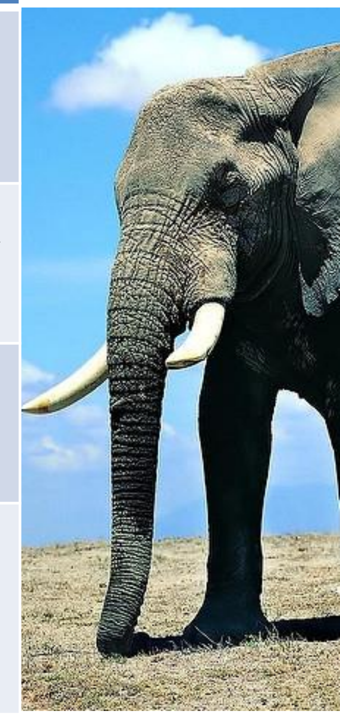
IEEE 1609.x, ISO 2007x, **SAE J1939-91B**
SAE J3201, SAE J3005-2

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 J3005-1, SAE J3061, ISO 15765-5, SAE J3138, **SAE J1939-91A**
Diagnostics Interface Security



ISO/SAE 21434

SCOPE – J1939-91Part "A"
Foundation Layer Security

J1939-91A defines 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 "dongle" device security]

✓ – General requirements for "Imposter Reporting" for devices that may spoof J1939 Source Addresses.

– Update General Vehicle Network Gateway recommendations and network topology reference related to J1939-31 (TBD)

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

Committee NWIP Draft

J1939-91C defines recommendations for:

- Secure on-board communications between ECUs

Scope being Drafted

Layer 4 Security

Connected Vehicle Security

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

Potential NMFTA, IEEE, TMC and ISO collaboration
→ Drafting NWIP

- 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

ATA FLEET CYWATCH

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

Public Key Infrastructure (PKI) System Security Practices

- Comprehensive security technology and policies
- using cryptography and standards to enable users to:
- Identify (authenticate) themselves to network services.
- Digitally sign email and other electronic docs and services.
- Encrypt email and other documents to prevent unauthorized access.

NIST publication SP 800-32
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-32.pdf

SAE J3101 - Hardware Protected Security for Ground Vehicles

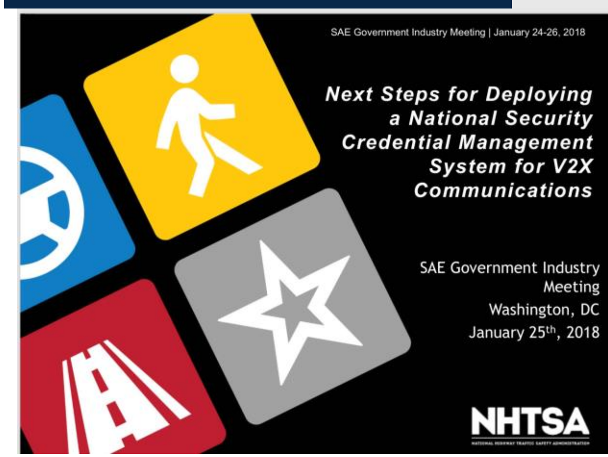
- Specifically crafted for embedded use in Ground Vehicle applications
- Lists core requirements derived from reviewed use cases
  - • ***Hardware Protected Keystore*** • Cryptographic Algorithms • Cryptoagility • Random Number Generator • Nonvolatile Critical Security Parameters • Interface Control • Secure Execution Environment • Self Test

Hardware Protected Keystore

Fundamentally security is about storing a digital key

- Hardware protected Security stores keys beyond the reach of normal operation
- Not just secure storage a Keystore is a fully functional storage module
- Specifically for keys • Only for Keys • Symmetric Keys and Asymmetric Keys
- Key Installation, Generation, access control, validity, Erasure etc.
- Objective is to prevent keys from ever being disclosed in the clear outside the Hardware Protected Security Environment

Standardize PKI Management Process Needed

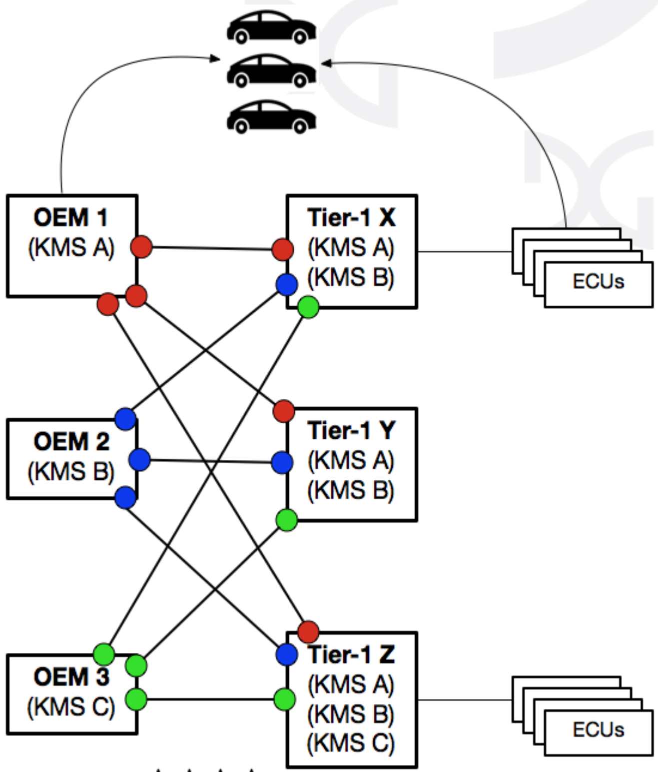


NEW

SAE J3201 being drafted

OASIS KMIP 2.0

Research Project => Proposed SAE Standard



Non-Interoperable, OEM-specific automotive KMS systems today - high number of integration points

SAE J3201 draft

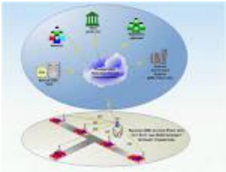
Guideline for Automotive Secure Key Management and Credential Distribution

- Defines architecture, design, and implementation requirements for vehicle key management security.
- Best practice guidance on generation, handling, and storing of credentials within car maker and suppliers.
- Best practice guidance on overall key management system cooperation between all stakeholders.
- Best practice guidance on overall key management system architecture and design, backup strategies, and recovery strategies.

Vehicle data access vs. vehicle security

- Insurance “telematics”
- Other “telematics”
- “Prognostics”
- Modification of powertrain components (“tuning”)
- Malicious attacks (“hacking”)

Vehicle DLC Use Cases



Remote OBD

PEMS

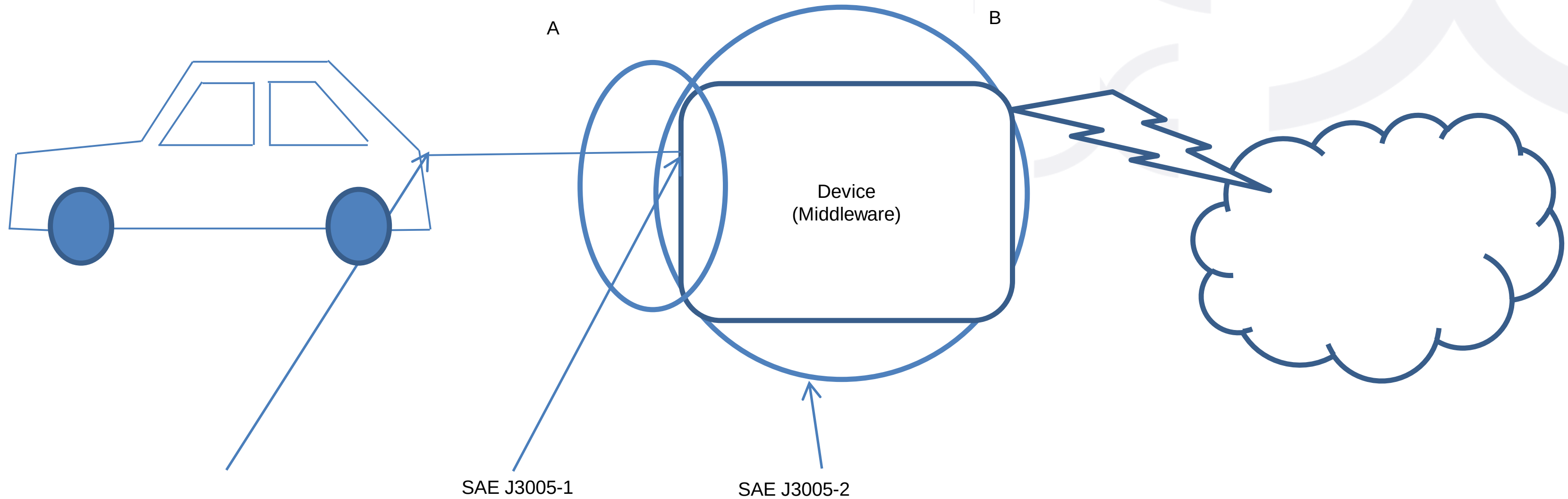
Split-cables

WLAN interfaces

Insurance devices

GPS

Passenger Vehicle DLC Security



SAE J3138

Diagram Courtesy SAE J3005-2/J. Pauli, Technology Specialist, Volvo Group Trucks Technology

SAE J3138

SAE J3138 initiated to address the risk to the modern vehicle ecosystem posed by the SAE J1962 Connector

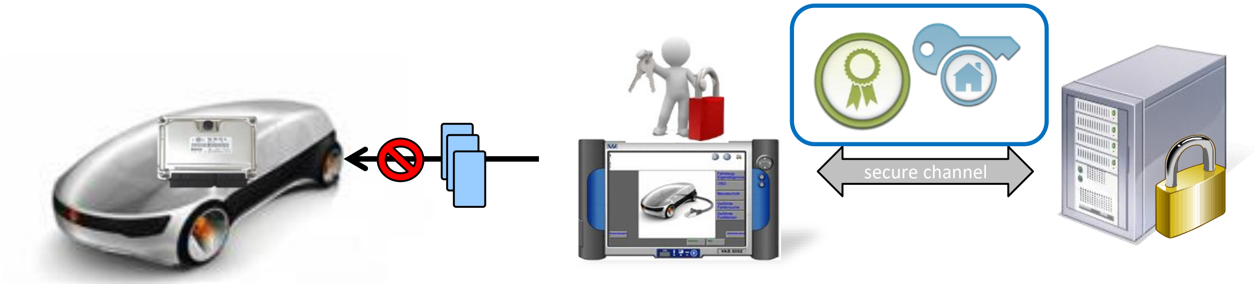
- Recommendations are aimed at all future vehicle applications requiring standardized communication access through this connector
- Addresses all vehicle diagnostic network configurations
  - Full gateway
  - Partial gateway
  - No gateway

SAE J3138

Main premise – ensure that the vehicle is in an OEM-determined “safe state” before allowing any intrusive diagnostic function request is allowed

- Secondary concern addressed – ensure that current tool/maintenance access is not interfered with.
- Document balloted, passed and published June 2018
- Next version is at “Work in Progress” stage, addressing future cybersecurity items.

Concept for a long-term solution
first step: protection of diagnostics access



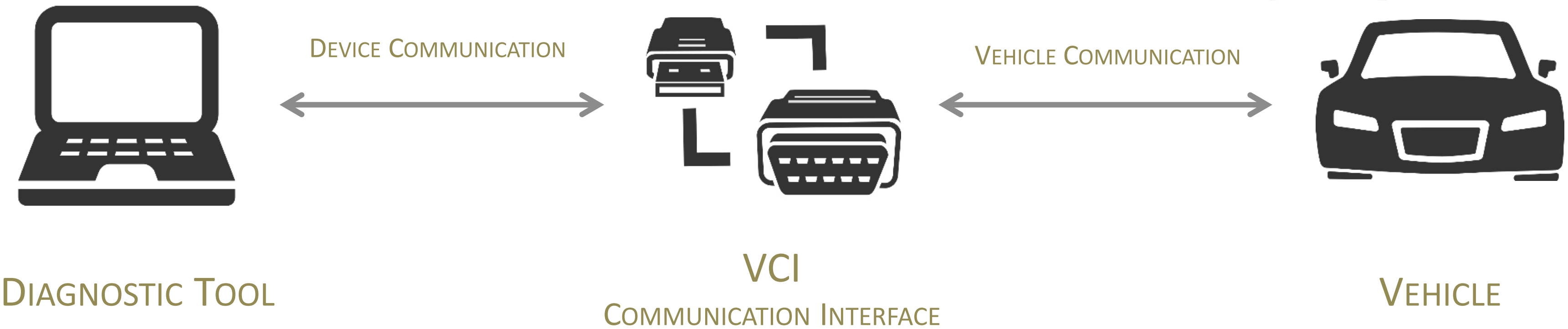
Electronic Control Unit (ECU)
- signature verification and public key

Diagnostic system
- private key and certificate signing request
- routing of security token
- Individual-ID: (VIN, ECU-ID, Project-ID)

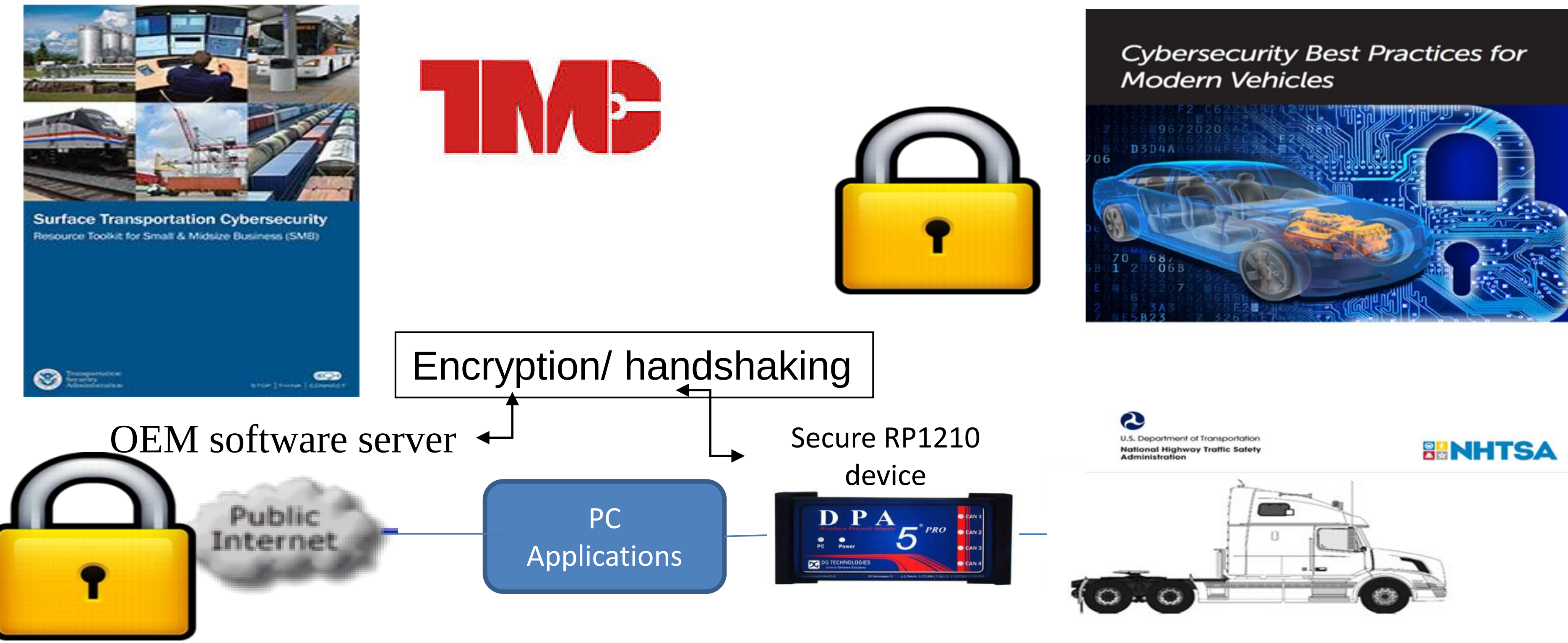
IT-Backend
- creation of security token
- identity and access management
- Log saves all events, accesses, and errors

Diagnostics

Today's setup



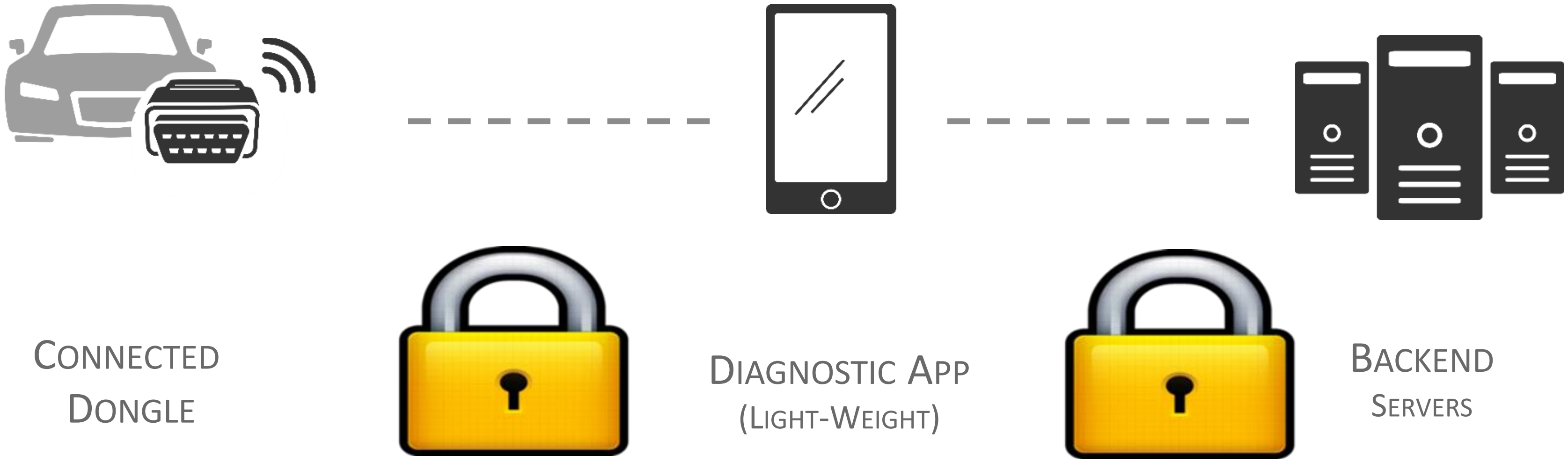
Secure Vehicle Diagnostics



SAE INTERNATIONAL

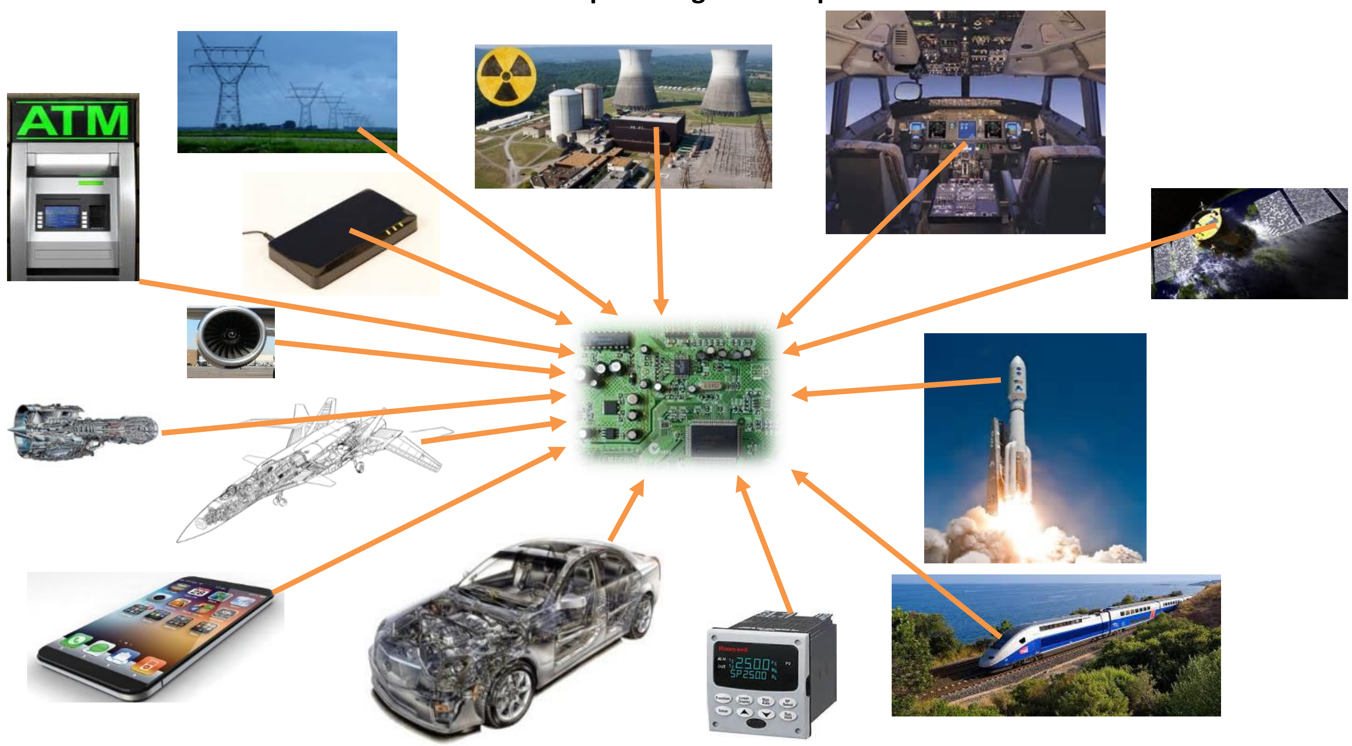
Diagnostic Components

For the next generation

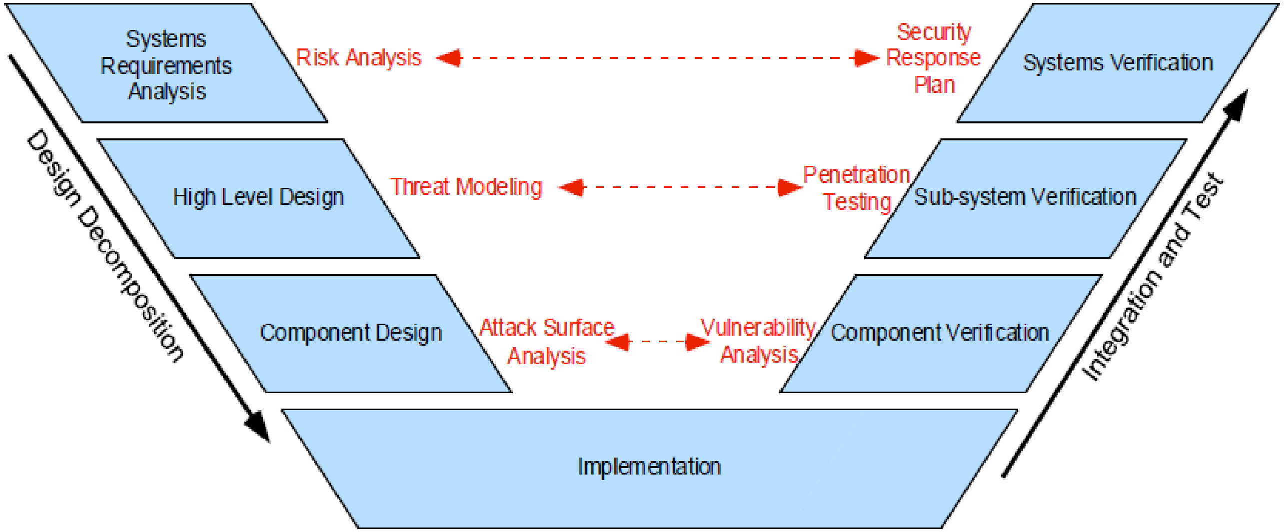


Cyber Physical Systems (CPS)

Cyber Physical Systems are defined as technologies that combine the cyber and physical worlds that can respond in real time to their environments. Cyber physical systems includes electronic parts, assemblies, systems, and system elements that operate as a single, self-contained device or within an interconnected network providing shared operations.



Systems Engineering for CPS Security



Driving to a High-Level Common Industry Approach

What is Hardware Assurance (HwA)?

- Definition 1 – The Goal - the level of confidence that microelectronics (also known as microcircuits, semiconductors, and integrated circuits, including its embedded software and/or intellectual property) function as intended and are free of known vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system's hardware and/or its embedded software and/or intellectual property, throughout the life cycle.
- Definition 2 – The Process - the process, practice or methodology that can be employed to achieve the goal of Hardware Assurance

Hardware may be extremely difficult and costly to "fix"

Source: Defense Acquisition Guidelines (DAG) Chapter 9 (Program Protection Planning) Section 3.2.4

SAE INTERNATIONAL

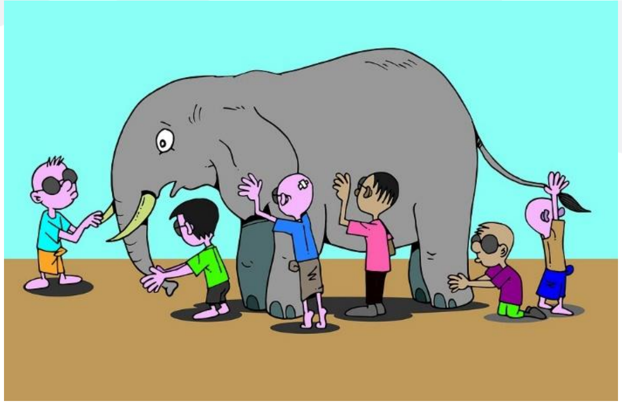
What is Software Assurance (SwA)?

- **Definition 1** - Software assurance (SwA) is the level of confidence that software functions as intended and is free of known vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software, throughout the life cycle [Public Law 112-239-Jan 2013 see Section 933]
- **Definition 2** - The process, practice or methodology that can be employed to achieve the goal of Hardware Assurance
- ***Efforts are required to define "level of confidence" and "free of vulnerabilities"***

Source: Defense Acquisition Guidelines (DAG) Chapter 9 (Program Protection Planning) Section 3.2.4

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

SAE INTERNATIONAL

TMC