SAE INTERNATIONAL

WCX WORLD CONGRESS EXPERIENCE™

APRIL 10-12, 2018 • COBO CENTER • DETROIT, MICHIGAN

sae.org/wcx

Cyber Security and Vehicle Diagnostics

Mark Zachos

DG Technologies

DG TECHNOLOGIES
Vehicle Network Solutions

Mail 10:47 AM nist.gov

NIST

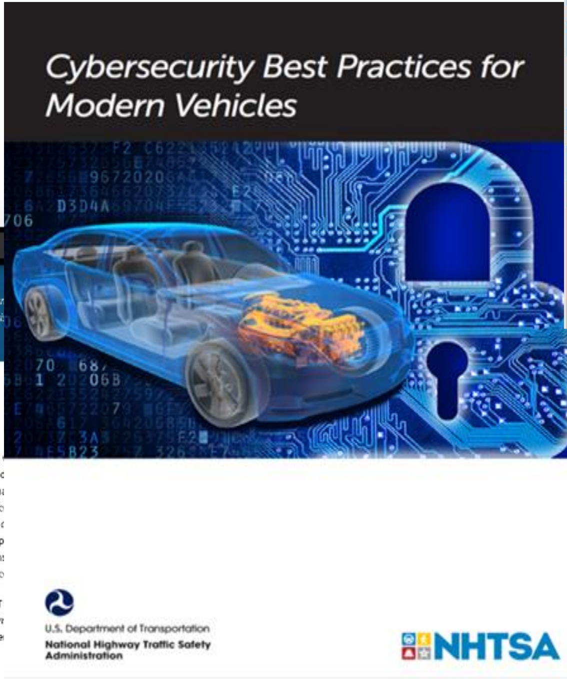
CYBERSECURITY FRAMEWORK

Helping organizations to better understand ar cybersecurity ri

- Framework +
- New to Framework +
- Perspectives +
- Online Learning +
- Evolution +
- Frequently Asked Questions +
- Events and Presentations
- Related Efforts (Roadmap)
- Informative References
- Resources +
- Newsroom +

LATEST UPDATES

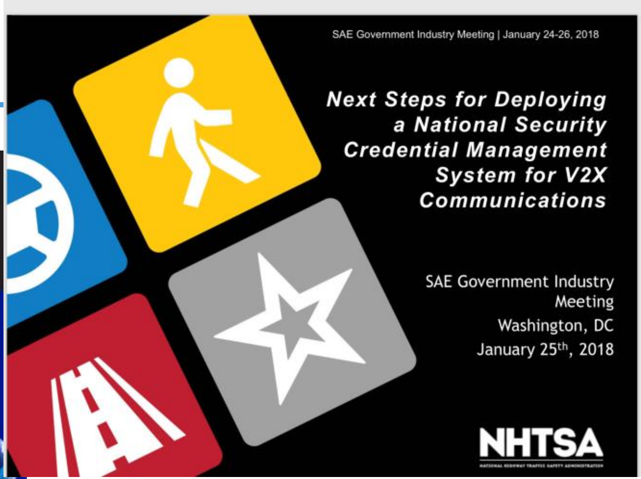
- Also, the next Baldrige Cybersecurity Excellence Builder Workshop, April 8, 8:30-3:30 pm, in Baltimore, MD. It's a practical, interactive workshop on using the Baldrige Cybersecurity



Cybersecurity Best Practices for Modern Vehicles

U.S. Department of Transportation
National Highway Traffic Safety Administration

NHTSA



SAE Government Industry Meeting | January 24-26, 2018

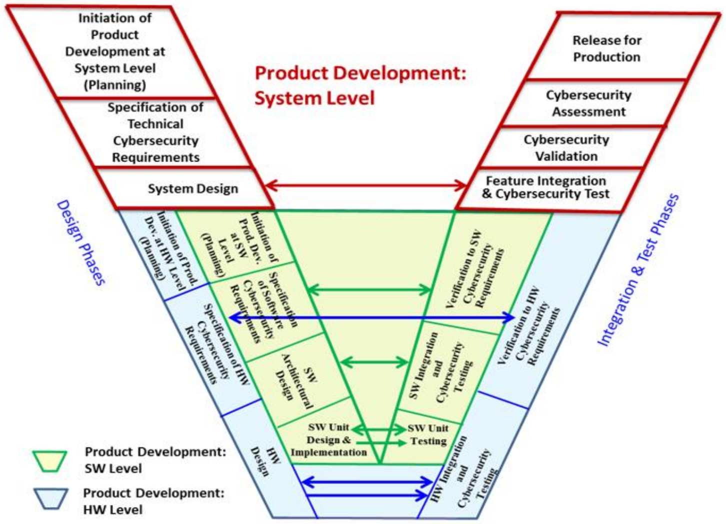
Next Steps for Deploying a National Security Credential Management System for V2X Communications

SAE Government Industry Meeting
Washington, DC
January 25th, 2018

NHTSA

SAE J3061 Cybersecurity Guidebook for Cyber-Physical Automotive Systems

- Published January 2016; drive to *a risk-based, process-driven approach to address the Cybersecurity threats the automotive environment* is experiencing.



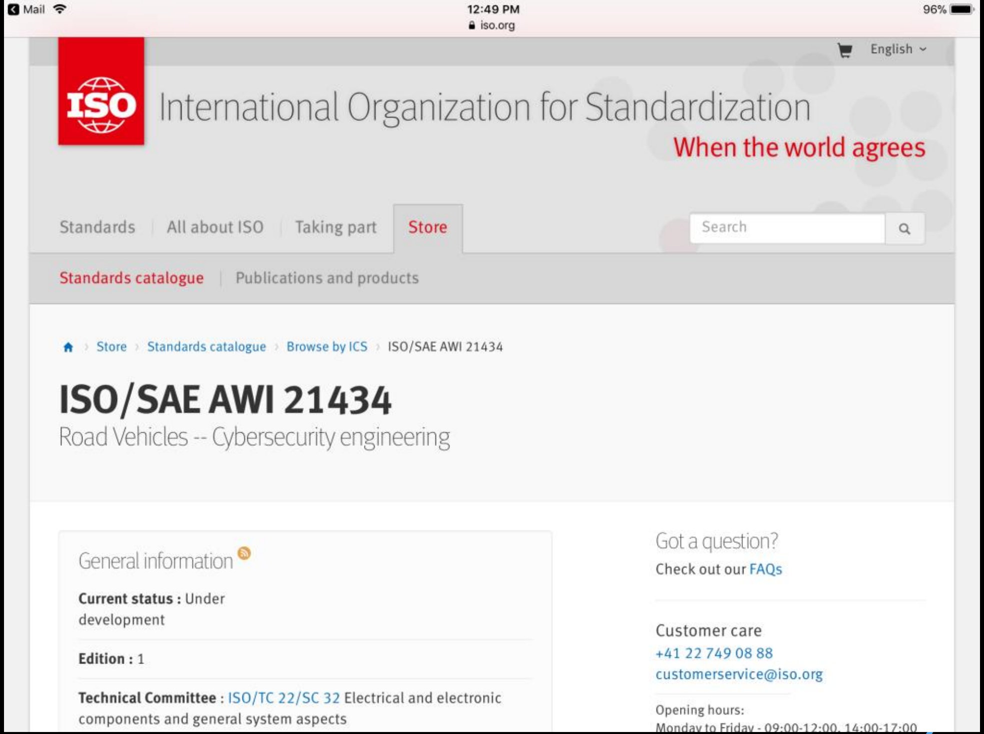
Initiation of Product Development at System Level (Planning)
Specification of Technical Cybersecurity Requirements
System Design
Product Development: System Level
Release for Production
Cybersecurity Assessment
Cybersecurity Validation
Feature Integration & Cybersecurity Test
Design Phases
Integration & Test Phases
Initiation of Prod. Dev. at HW Level (Planning)
Initiation of Prod. Dev. at SW Level (Planning)
Specification of Software Cybersecurity Requirements
Specification of HW Cybersecurity Requirements
SW Architectural Design
SW Unit Design & Implementation
HW Design
Verification to SW Cybersecurity Requirements
Verification to HW Cybersecurity Requirements
SW Integration and Cybersecurity Testing
SW Unit Testing
HW Integration and Cybersecurity Testing
Product Development: SW Level
Product Development: HW Level

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

- Provides guidance on how to *integrate cybersecurity* into their product development life-cycle
- Establishes the desired relationships between *cybersecurity and safety*
- J3061 provides a *foundation for further security standards* development and is the “go-to” resource throughout industry

SAE and ISO Collaboration

Enhancement of SAE J3061



Mail
12:49 PM
iso.org
96%
English
ISO
International Organization for Standardization
When the world agrees
Standards
All about ISO
Taking part
Store
Search
Standards catalogue
Publications and products
Store › Standards catalogue › Browse by ICS › ISO/SAE AWI 21434

ISO/SAE AWI 21434

Road Vehicles -- Cybersecurity engineering

General information

Current status : Under development

Edition : 1

Technical Committee : ISO/TC 22/SC 32 Electrical and electronic components and general system aspects

Got a question?

Check out our FAQs

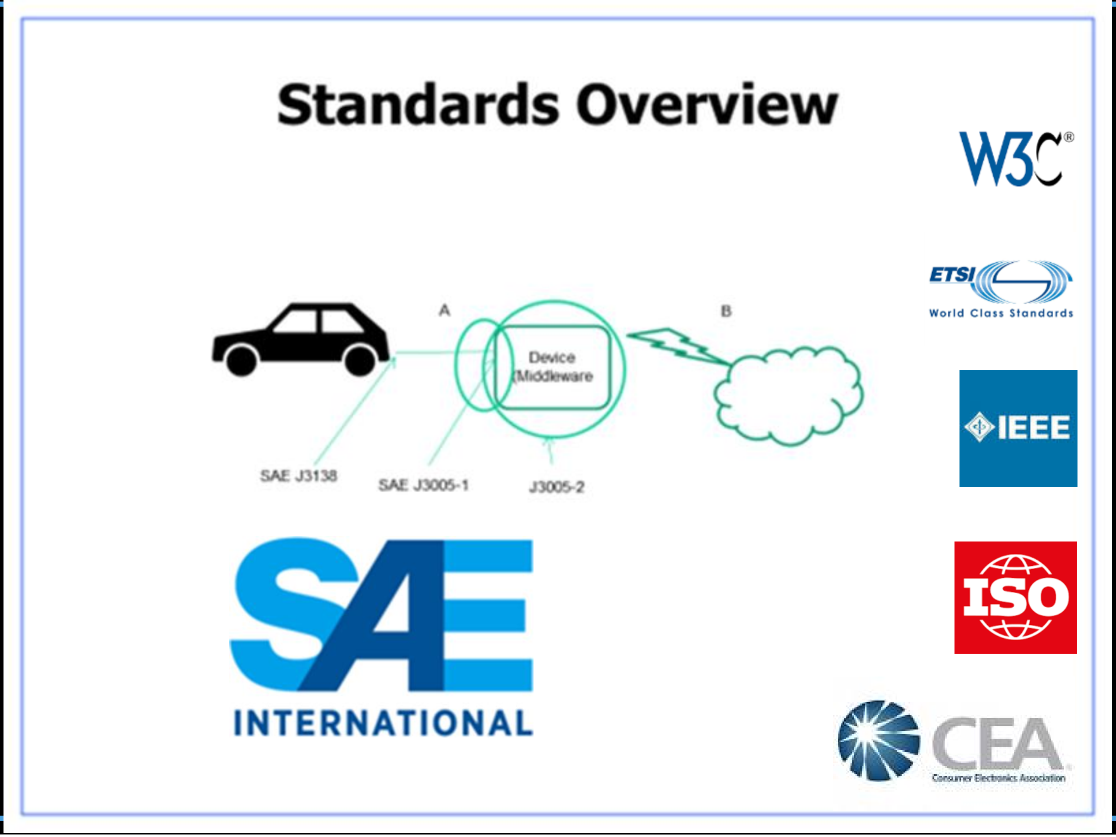
Customer care

+41 22 749 08 88

customerservice@iso.org

Opening hours:

Monday to Friday - 09:00-12:00, 14:00-17:00



Standards Overview

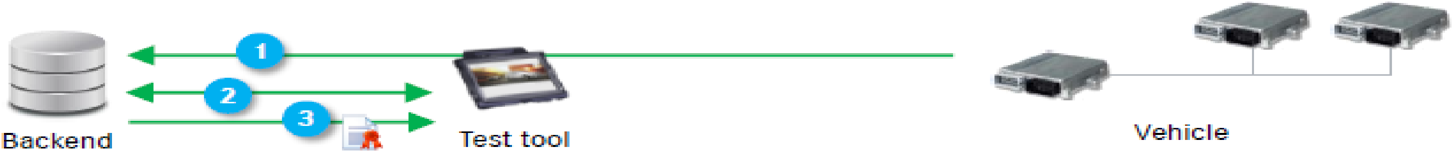
ISO TC22/SC31/WG2/PT2

Draft document being developed for submission as a NWIP

ISO International Organization for Standardization

Tester Authentication & Rights Management

Obtaining certificates from a backend



1. **Optional** (see notes): test tool needs to provide data from the vehicle (e.g. challenge for current diagnostic session)
2. Test tool authenticates itself against the backend using a secure channel
3. Backend provides certificate

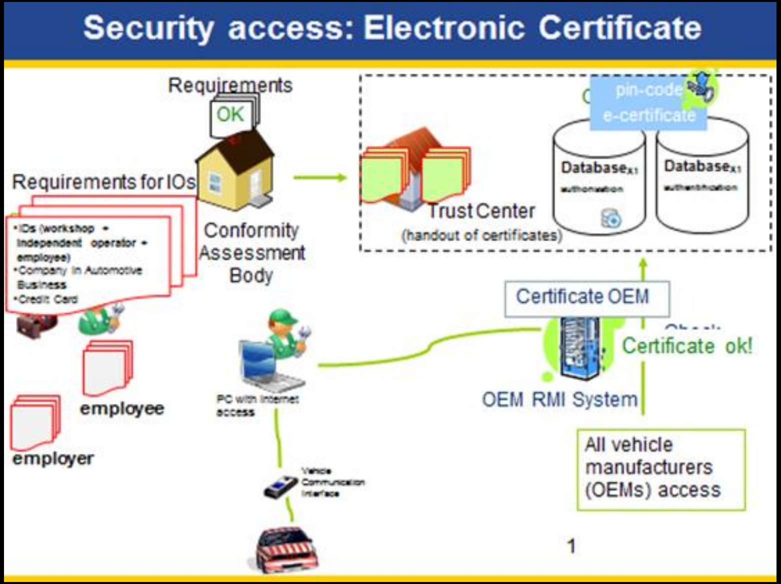
New SAE J3005-2 *draft*

Permanently or Semi-Permanently Installed Diagnostic Communication Devices- *Security Guidelines*

- Best practices for OBD-II interface and telematic devices for handling cyber security issues.
  - Design and implement a secure firmware/software update process
  - Secure product interfaces with authentication, integrity protection and encryption
  - Obtain an independent security assessment of your product
  - Secure the companion mobile applications and/or gateways that connect with your products (e.g., encryption/ privileges/authentication)
  - Implement a secure root of trust for root chains and private keys on the device

SAE J3146 – *draft*

Industry practices related to securing the diagnostics interface to a vehicle (e.g. EU SERMI)


Security access: Electronic Certificate
Requirements
OK
Requirements for IOs
• IOs (workshop + independent operator + employee)
• Company in Automotive Business
• Credit Card
Conformity Assessment Body
Trust Center
(handout of certificates)
pin-code
e-certificate
Database$_{x1}$
authorisation
Database$_{x1}$
authentification
Certificate OEM
Certificate ok!
OEM RMI System
employee
employer
PC with Internet access
Vehicle Communication Interface
All vehicle manufacturers (OEMs) access
1

Secure Over The Air (SOTA) ECU software updates

SAE INTERNATIONAL®

ASAM

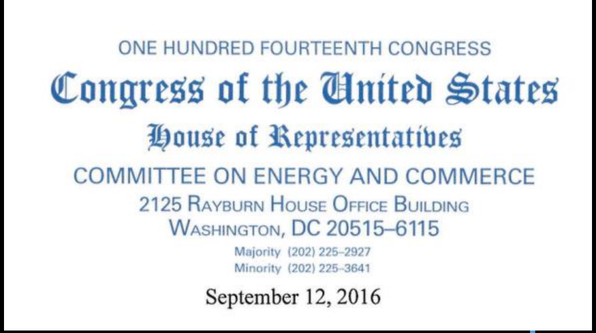
UPTANE

GENIVI®

US-NHTSA focus on OBD-II Security

- *September 12:* Letter from House Committee on Energy and Commerce to NHTSA RE: OBD-II Security

  "…request that NHTSA convene an industry-wide effort to develop a plan of action for addressing the risk posed by the existence of the OBD-II port in the modern vehicle ecosystem."



ONE HUNDRED FOURTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115

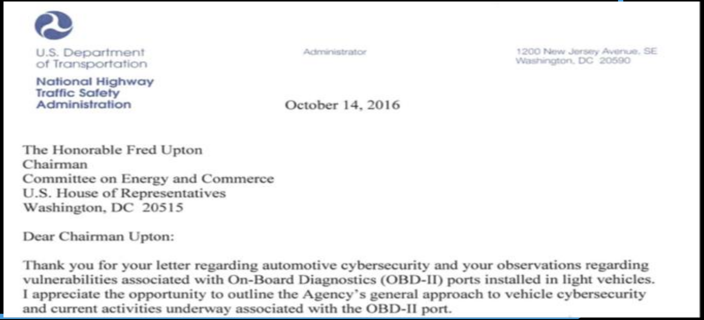
Majority (202) 225–2927
Minority (202) 225–3641

September 12, 2016

- *September 28:* NHTSA requests SAE to take the lead and convene industry group to examine issue

- *October 14:* NHTSA response to House Committee highlights SAE role:

  "At NHTSA's urging, SAE International has started a working group that is looking to explore ways to harden the OBD-II port. This group is making good progress and the Agency remains hopeful that the group will move expeditiously to develop a set of recommendations."



U.S. Department
of Transportation

National Highway
Traffic Safety
Administration

Administrator

1200 New Jersey Avenue, SE
Washington, DC 20590

October 14, 2016

The Honorable Fred Upton
Chairman
Committee on Energy and Commerce
U.S. House of Representatives
Washington, DC 20515

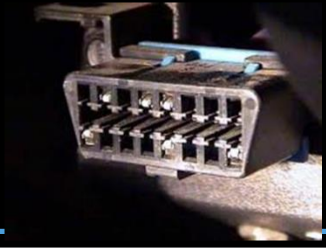
Dear Chairman Upton:

Thank you for your letter regarding automotive cybersecurity and your observations regarding vulnerabilities associated with On-Board Diagnostics (OBD-II) ports installed in light vehicles. I appreciate the opportunity to outline the Agency's general approach to vehicle cybersecurity and current activities underway associated with the OBD-II port.

SAE Data Link Connector (DLC) Vehicle Security

Recommend Practice SAE J3138 *draft*

- Definition of “Hardened OBD-II Port”
- Firewall function recommendations for the DLC
- ECU security recommendations for data link connections
- *Still allow required communications per vehicle emissions regulations*



SAE J3138

The vehicle should be in a “safe state” prior to an intrusive OBD Service Request operation

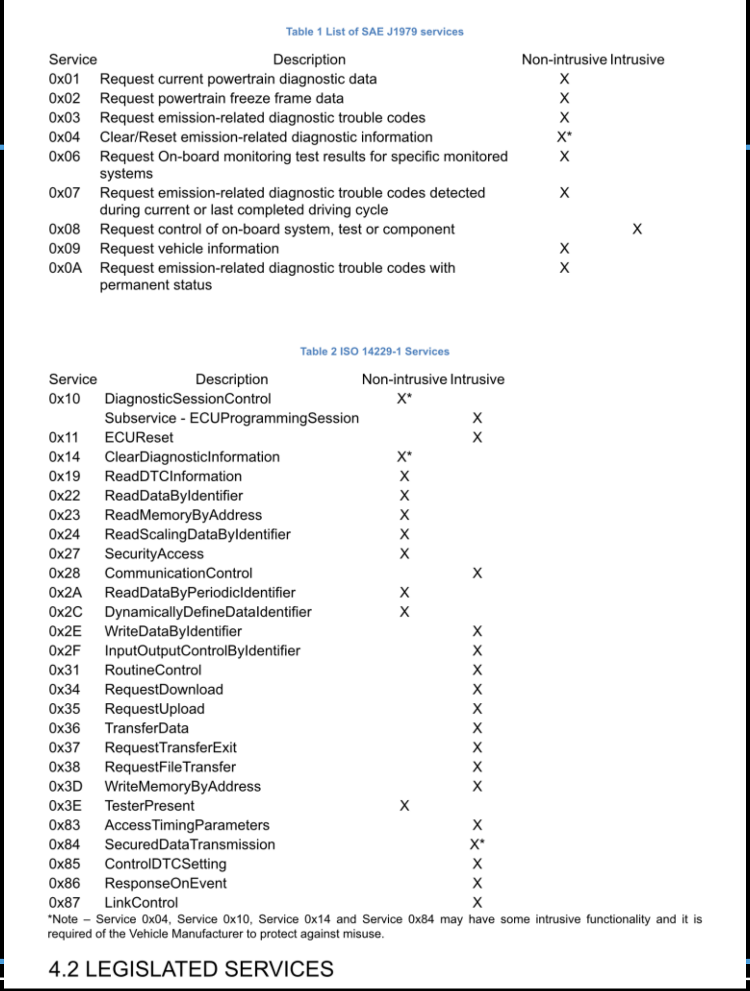


Table 1 List of SAE J1979 services

Service	Description	Non-intrusive	Intrusive
0x01	Request current powertrain diagnostic data	X	
0x02	Request powertrain freeze frame data	X	
0x03	Request emission-related diagnostic trouble codes	X	
0x04	Clear/Reset emission-related diagnostic information	X*	
0x06	Request On-board monitoring test results for specific monitored systems	X	
0x07	Request emission-related diagnostic trouble codes detected during current or last completed driving cycle	X	
0x08	Request control of on-board system, test or component		X
0x09	Request vehicle information	X	
0x0A	Request emission-related diagnostic trouble codes with permanent status	X	

Table 2 ISO 14229-1 Services

Service	Description	Non-intrusive	Intrusive
0x10	DiagnosticSessionControl	X*	
	Subservice - ECUProgrammingSession		X
0x11	ECUReset		X
0x14	ClearDiagnosticInformation	X*	
0x19	ReadDTCInformation	X	
0x22	ReadDataByIdentifier	X	
0x23	ReadMemoryByAddress	X	
0x24	ReadScalingDataByIdentifier	X	
0x27	SecurityAccess	X	
0x28	CommunicationControl		X
0x2A	ReadDataByPeriodicIdentifier	X	
0x2C	DynamicallyDefineDataIdentifier	X	
0x2E	WriteDataByIdentifier		X
0x2F	InputOutputControlByIdentifier		X
0x31	RoutineControl		X
0x34	RequestDownload		X
0x35	RequestUpload		X
0x36	TransferData		X
0x37	RequestTransferExit		X
0x38	RequestFileTransfer		X
0x3D	WriteMemoryByAddress		X
0x3E	TesterPresent	X	
0x83	AccessTimingParameters		X
0x84	SecuredDataTransmission		X*
0x85	ControlDTCSetting		X
0x86	ResponseOnEvent		X
0x87	LinkControl		X

*Note – Service 0x04, Service 0x10, Service 0x14 and Service 0x84 may have some intrusive functionality and it is required of the Vehicle Manufacturer to protect against misuse.

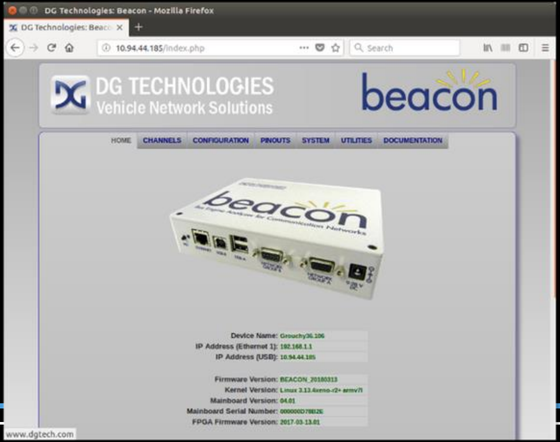
4.2 LEGISLATED SERVICES

SAE J3138 Validation Testing

- **SAE J3138 specifies that the vehicle to be in a “Safe State” (e.g. stopped) for OBD-II communications.**
- **Validation Test**
  - Before starting OBD-II test the tools checks that vehicle speed is zero
  - If not zero, the test aborts the test sequence
- **However, a defect/malicious actor could try to trick the test**
  - – By injecting a false vehicle speed of zero before the actual vehicle speed message
  - – Thereby tricking (spoofing) the test to continue

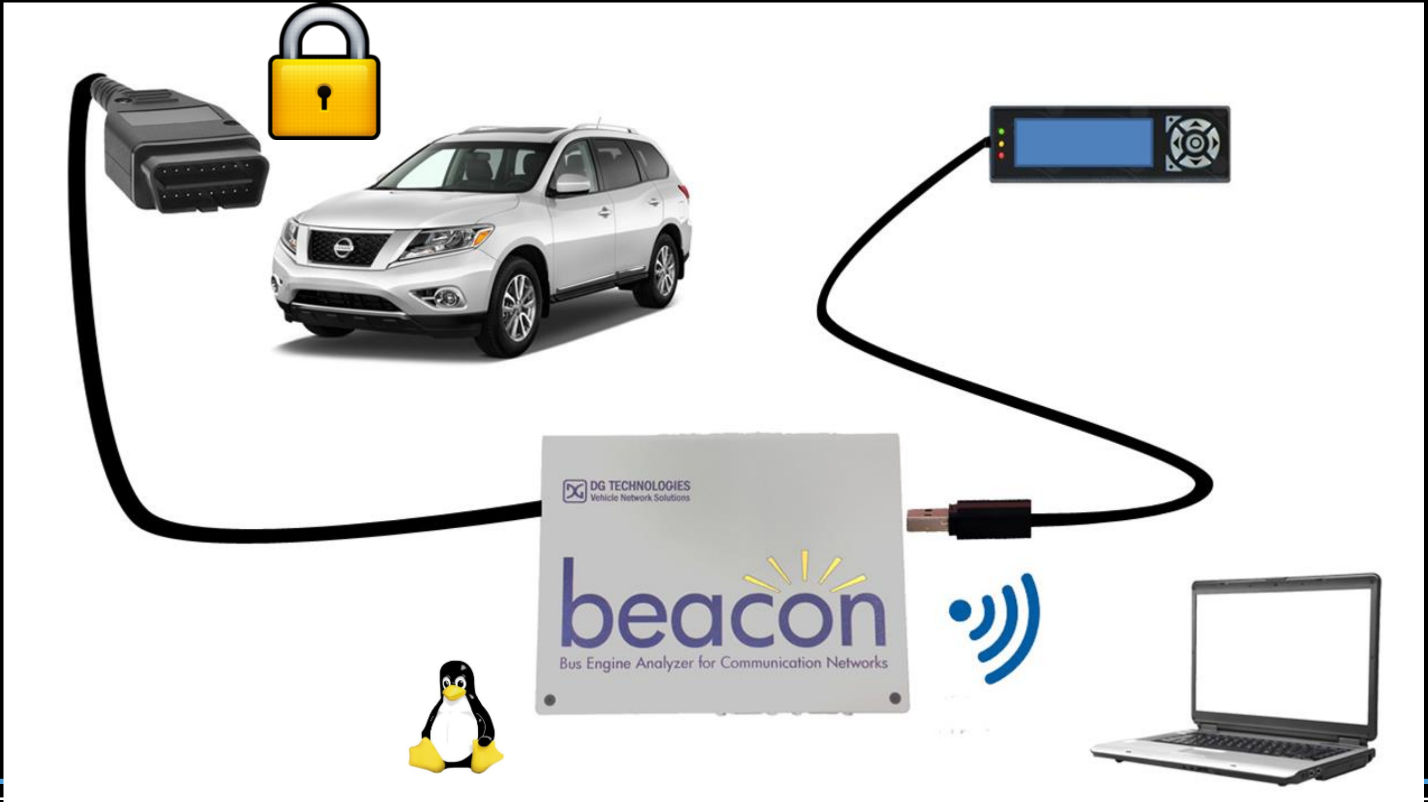
BEACON J3138 Test Utility

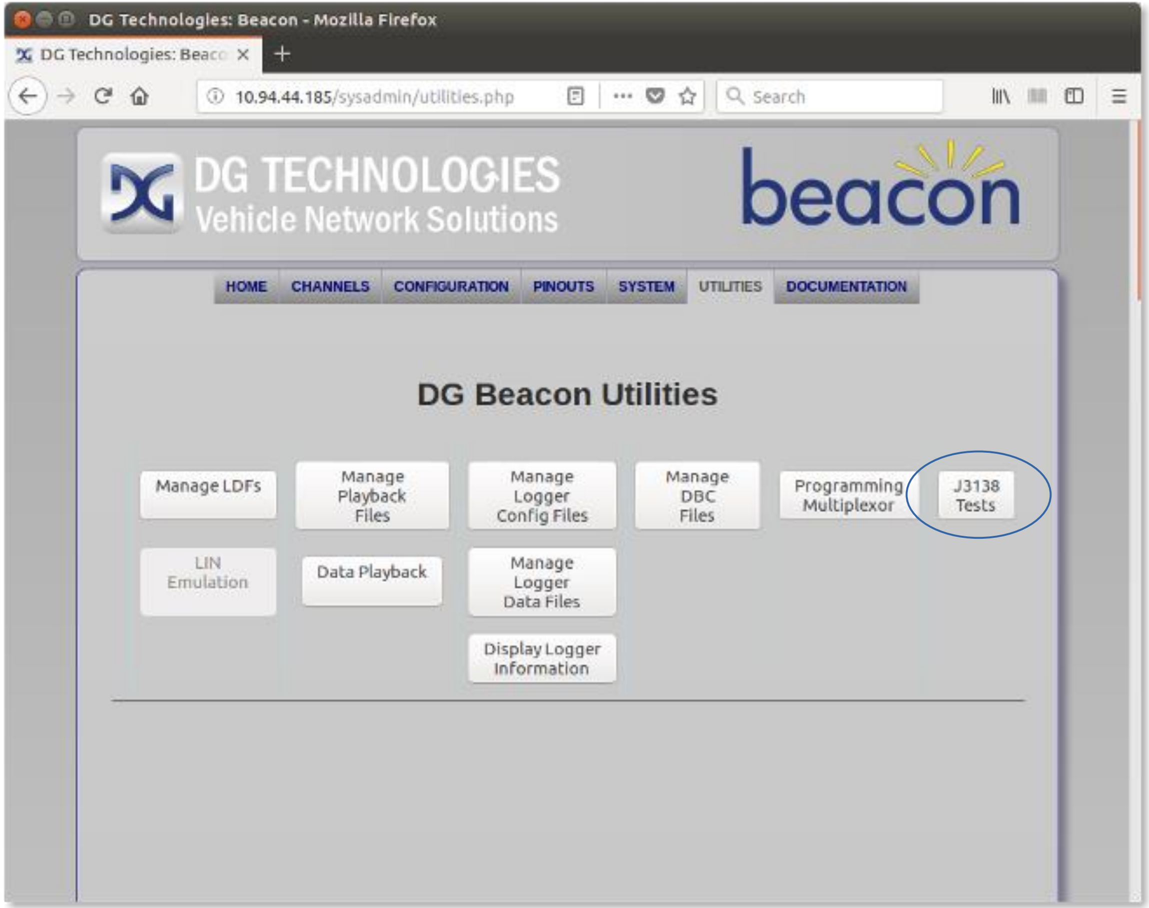
- The DG BEACON J3138 test utility allows the user to easily build and execute test sessions through a web page interface
- The user can easily construct OBD-II request and response messages
- The user can add padding and extra data bytes to the message definition



Device Name: Grouchy36.106
IP Address (Ethernet 1): 192.168.1.1
IP Address (USB): 10.94.44.185

Firmware Version: BEACON_20180313
Kernel Version: Linux 3.13.4xeno-r2+ armv7l
Mainboard Version: 04.01
Mainboard Serial Number: 000000D78B26
FPGA Firmware Version: 2017-03-13.01


DG TECHNOLOGIES
Vehicle Network Solutions
beacon
Bus Engine Analyzer for Communication Networks



DG Technologies: Beacon - Mozilla Firefox

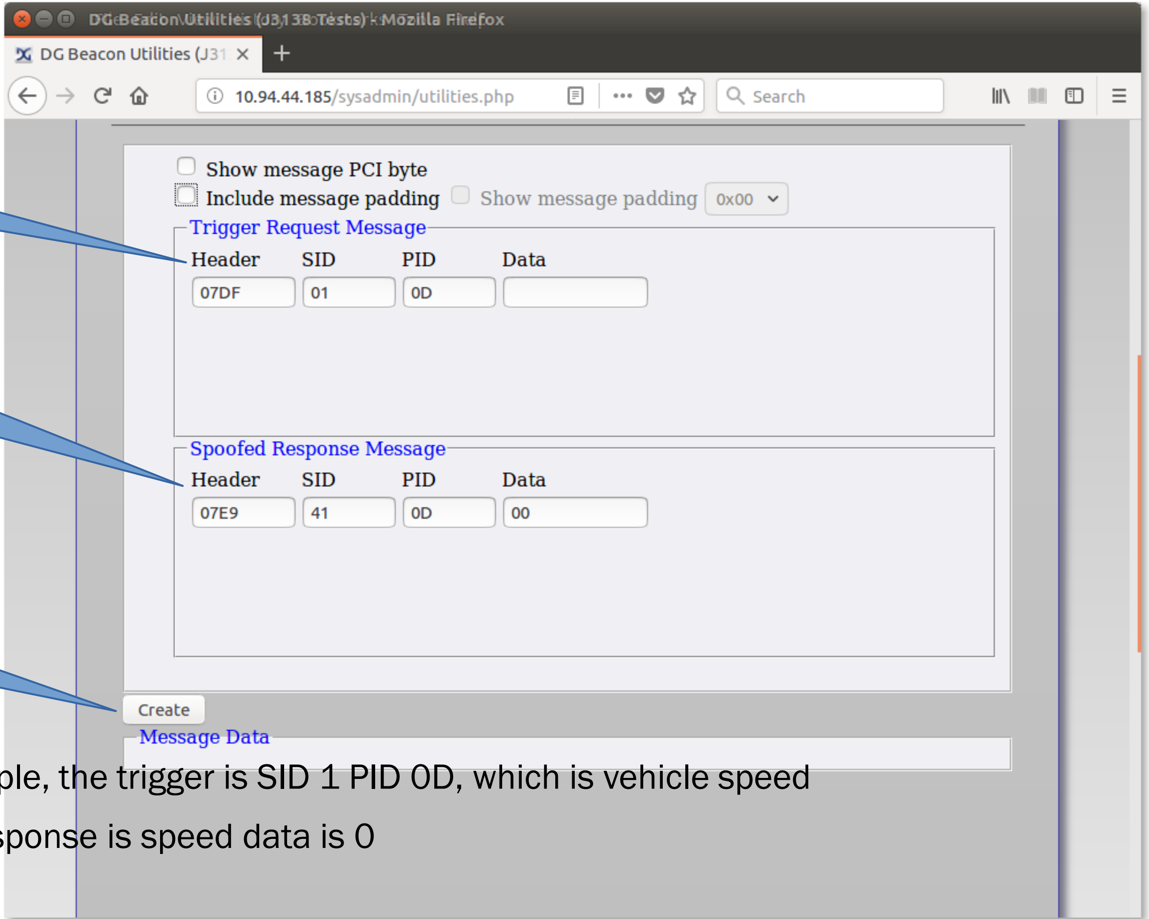
10.94.44.185/sysadmin/utilities.php

DG Beacon Utilities

Define Trigger

Define Response

Create Test



DG Beacon Utilities (J3138 Tests) - Mozilla Firefox
DG Beacon Utilities (J31
10.94.44.185/sysadmin/utilities.php
Search

□ Show message PCI byte

□ Include message padding □ Show message padding 0x00

Trigger Request Message

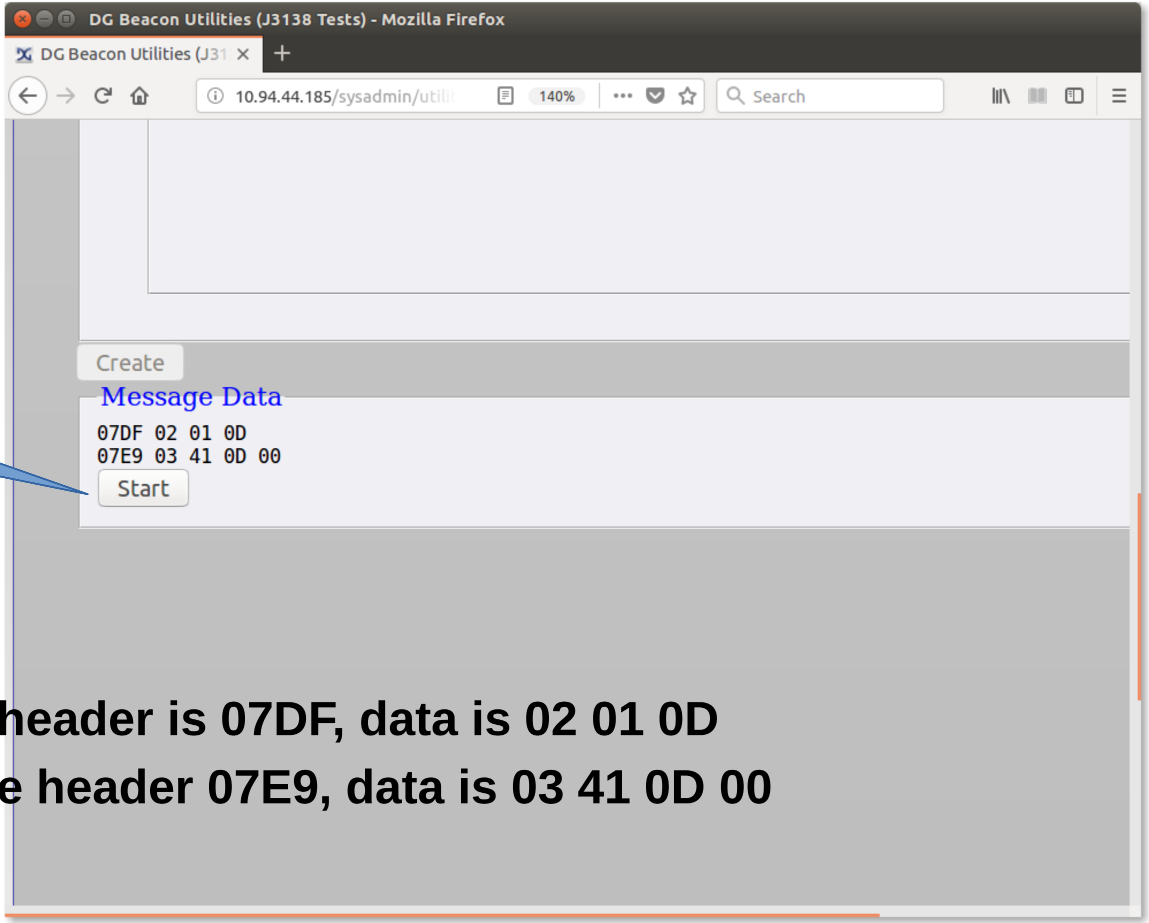
Header	SID	PID	Data
07DF	01	0D	

Spoofed Response Message

Header	SID	PID	Data
07E9	41	0D	00

- In this example, the trigger is SID 1 PID 0D, which is vehicle speed
- The false response is speed data is 0

Start Test

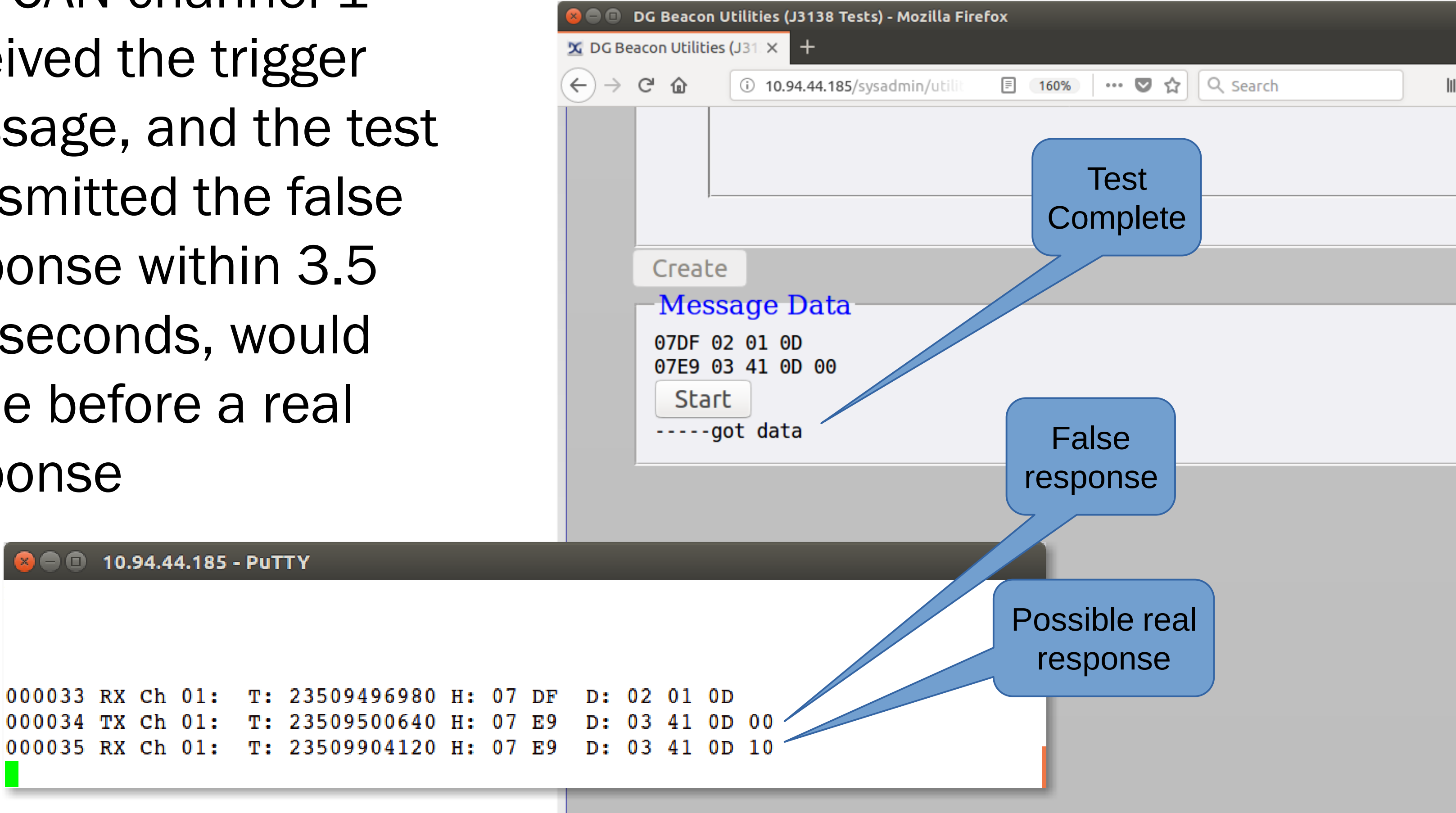

DG Beacon Utilities (J3138 Tests) - Mozilla Firefox
DG Beacon Utilities (J31
10.94.44.185/sysadmin/utilit
140%
Search
Create
Start

Message Data

```
07DF 02 01 0D
07E9 03 41 0D 00
```

- Request header is 07DF, data is 02 01 0D
- Response header 07E9, data is 03 41 0D 00

The log below shows that CAN channel 1 received the trigger message, and the test transmitted the false response within 3.5 milliseconds, would come before a real response


DG Beacon Utilities (J3138 Tests) - Mozilla Firefox
DG Beacon Utilities (J31
10.94.44.185/sysadmin/utilit
160%
Search
Create
Start
10.94.44.185 - PuTTY

Message Data

```
07DF 02 01 0D
07E9 03 41 0D 00
```

```
-----got data
```

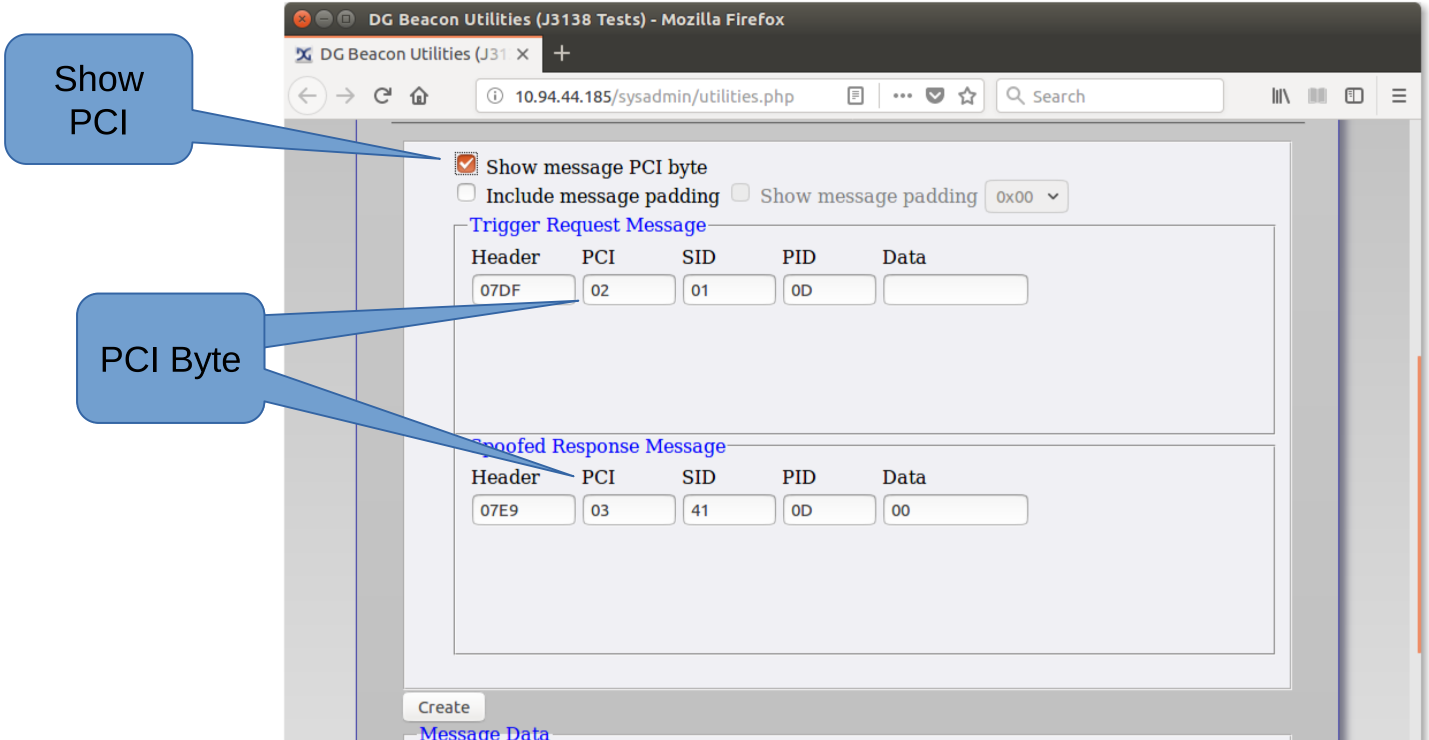
```
000033 RX Ch 01:  T: 23509496980 H: 07 DF  D: 02 01 0D
000034 TX Ch 01:  T: 23509500640 H: 07 E9  D: 03 41 0D 00
000035 RX Ch 01:  T: 23509904120 H: 07 E9  D: 03 41 0D 10
```

Test Complete

False response

Possible real response

- Click start again to start the test again
- Click J3138 button to start over and define a new test
- User can show and change PCI byte



Show PCI

PCI Byte

DG Beacon Utilities (J3138 Tests) - Mozilla Firefox

☑ Show message PCI byte

☐ Include message padding ☐ Show message padding 0x00

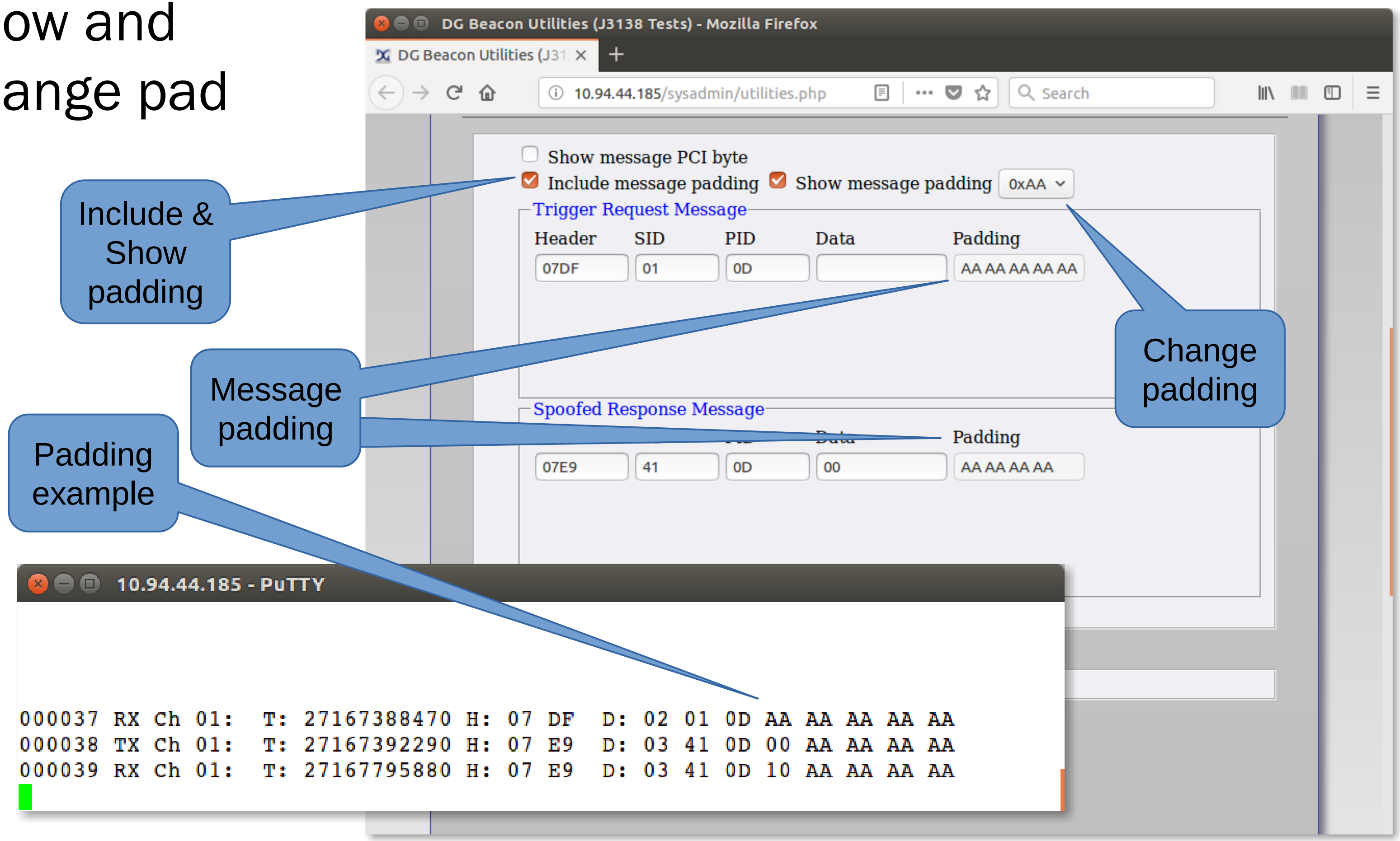
Trigger Request Message

Header	PCI	SID	PID	Data
07DF	02	01	0D	

Spoofed Response Message

Header	PCI	SID	PID	Data
07E9	03	41	0D	00

User can show and change pad



DG Beacon Utilities (J3138 Tests) - Mozilla Firefox
DG Beacon Utilities (J31
10.94.44.185/sysadmin/utilities.php
Search
10.94.44.185 - PuTTY

Include & Show padding

Message padding

Padding example

Change padding

□ Show message PCI byte

☑ Include message padding ☑ Show message padding 0xAA

Trigger Request Message

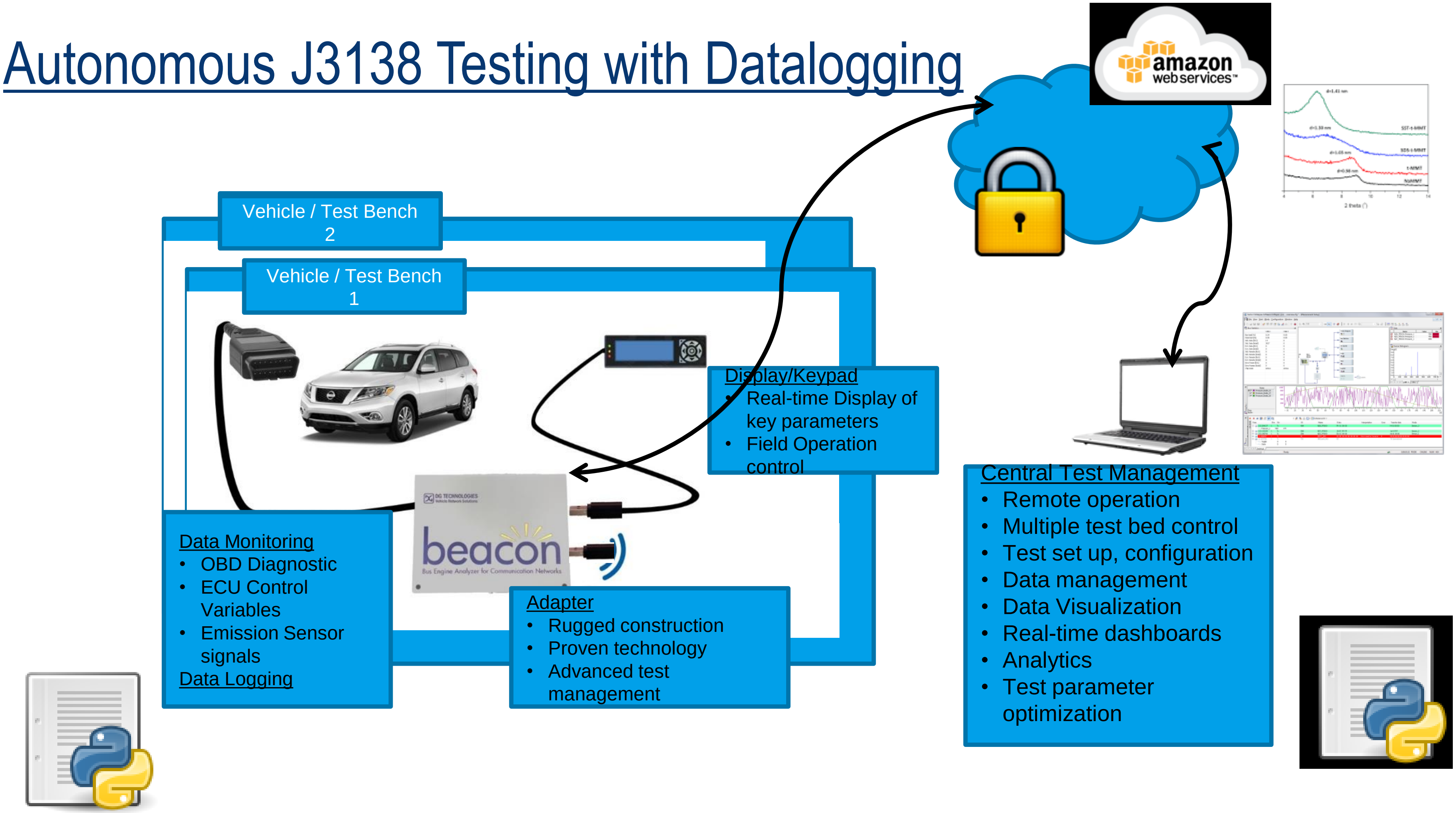
Header	SID	PID	Data	Padding
07DF	01	0D		AA AA AA AA AA

Spoofed Response Message

		PID	Data	Padding
07E9	41	0D	00	AA AA AA AA

```
000037 RX Ch 01:  T: 27167388470 H: 07 DF  D: 02 01 0D AA AA AA AA AA
000038 TX Ch 01:  T: 27167392290 H: 07 E9  D: 03 41 0D 00 AA AA AA AA
000039 RX Ch 01:  T: 27167795880 H: 07 E9  D: 03 41 0D 10 AA AA AA AA
```

Autonomous J3138 Testing with Datalogging



Vehicle / Test Bench 2

Vehicle / Test Bench 1

Display/Keypad
- Real-time Display of key parameters
- Field Operation control

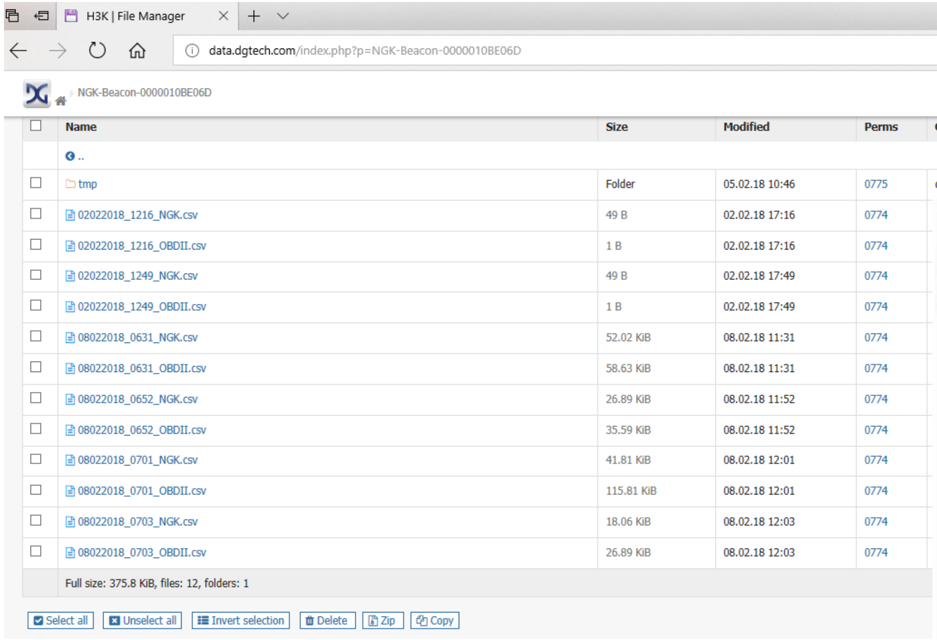
Data Monitoring
- OBD Diagnostic
- ECU Control Variables
- Emission Sensor signals

Data Logging

Adapter
- Rugged construction
- Proven technology
- Advanced test management

Central Test Management
- Remote operation
- Multiple test bed control
- Test set up, configuration
- Data management
- Data Visualization
- Real-time dashboards
- Analytics
- Test parameter optimization

J3138 Autonomous Datalogger Cloud Data Example



□	Name	Size	Modified	Perms	Owner	Actions
	..					
□	tmp	Folder	05.02.18 10:46	0775	datasync:datasync	
□	02022018_1216_NGK.csv	49 B	02.02.18 17:16	0774		
□	02022018_1216_OBDII.csv	1 B	02.02.18 17:16	0774		
□	02022018_1249_NGK.csv	49 B	02.02.18 17:49	0774		
□	02022018_1249_OBDII.csv	1 B	02.02.18 17:49	0774		
□	08022018_0631_NGK.csv	52.02 KiB	08.02.18 11:31	0774		
□	08022018_0631_OBDII.csv	58.63 KiB	08.02.18 11:31	0774		
□	08022018_0652_NGK.csv	26.89 KiB	08.02.18 11:52	0774		
□	08022018_0652_OBDII.csv	35.59 KiB	08.02.18 11:52	0774		
□	08022018_0701_NGK.csv	41.81 KiB	08.02.18 12:01	0774		
□	08022018_0701_OBDII.csv	115.81 KiB	08.02.18 12:01	0774		
□	08022018_0703_NGK.csv	18.06 KiB	08.02.18 12:03	0774		
□	08022018_0703_OBDII.csv	26.89 KiB	08.02.18 12:03	0774		

Full size: 375.8 KiB, files: 12, folders: 1

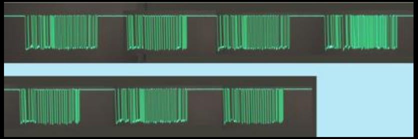
Select all
Unselect all
Invert selection
Delete
Zip
Copy

Speed Change #1

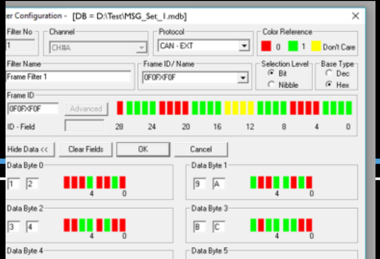
Incident Engine Hours: 33276.1 Hours **Incident Time:** Wednesday, 20 Mar 2013 at 08:53:22 (ECM Time) Time Stamp
Incident Engine Hours Hex: 52 27 0a 08 **Incident Time Hex:** a2 08 11 35
Oldest Incident Sample Timestamp: Wednesday, 20 Mar 2013 at 08:52:21 (ECM Time) Time Stamp **Incident Odometer:** 954760.6 Miles
Oldest Incident Sample Timestamp Hex: 57 09 11 35 **Incident Odometer Hex:** 55 a5 91 08

Additional Cyber Test Utilities

- **Denial of Service (DOS)**
  - Overloading CANbus(s) with message traffic



- **Fuzzing**
  - Allows the user to check the performance of an ECU or network in the presence of repeated and varied malformed CAN Bus messages
    - Data value fuzzing (e.g. Boofuzz)
    - Hardware fuzzing: Creation of malformed CAN Bus messages (incorrect data bits, incorrect stuff bits, incorrect CRC)



er Configuration - [DB = D:\Test\MSG_Set_I.mdb]

Filter No: 1

Channel: CH#A

Protocol: CAN - EXT

Color Reference: 🟥 0 🟩 1 🟨 Don't Care

Filter Name: Frame Filter 1

Frame ID/ Name: 0F0FXF0F

Selection Level: ● Bit ○ Nibble

Base Type: ○ Dec ● Hex

Frame ID: 0F0FXF0F

Data Byte 0: 1 2

Data Byte 1: 9 A

Data Byte 2: 3 4

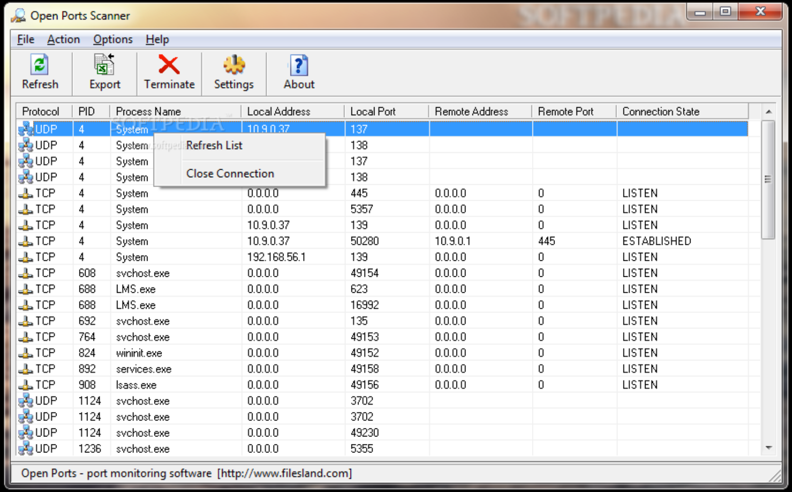
Data Byte 3: B C

Data Byte 4

Data Byte 5

Detection of unspecified Diagnostics Services ("open port scan")

- Polling ECUs with UDS SID requests and recording responses



Protocol	PID	Process Name	Local Address	Local Port	Remote Address	Remote Port	Connection State
UDP	4	System	10.9.0.37	137			
UDP	4	System		138			
UDP	4	System		137			
UDP	4	System		138			
TCP	4	System	0.0.0.0	445	0.0.0.0	0	LISTEN
TCP	4	System	0.0.0.0	5357	0.0.0.0	0	LISTEN
TCP	4	System	10.9.0.37	139	0.0.0.0	0	LISTEN
TCP	4	System	10.9.0.37	50280	10.9.0.1	445	ESTABLISHED
TCP	4	System	192.168.56.1	139	0.0.0.0	0	LISTEN
TCP	608	svchost.exe	0.0.0.0	49154	0.0.0.0	0	LISTEN
TCP	688	LMS.exe	0.0.0.0	623	0.0.0.0	0	LISTEN
TCP	688	LMS.exe	0.0.0.0	16992	0.0.0.0	0	LISTEN
TCP	692	svchost.exe	0.0.0.0	135	0.0.0.0	0	LISTEN
TCP	764	svchost.exe	0.0.0.0	49153	0.0.0.0	0	LISTEN
TCP	824	wininit.exe	0.0.0.0	49152	0.0.0.0	0	LISTEN
TCP	892	services.exe	0.0.0.0	49158	0.0.0.0	0	LISTEN
TCP	908	lsass.exe	0.0.0.0	49156	0.0.0.0	0	LISTEN
UDP	1124	svchost.exe	0.0.0.0	3702			
UDP	1124	svchost.exe	0.0.0.0	3702			
UDP	1124	svchost.exe	0.0.0.0	49230			
UDP	1236	svchost.exe	0.0.0.0	5355			

Open Ports - port monitoring software [http://www.filesland.com]

Additional integrated test system support

- Professional Cyber Security Test Tools

SPIRENT

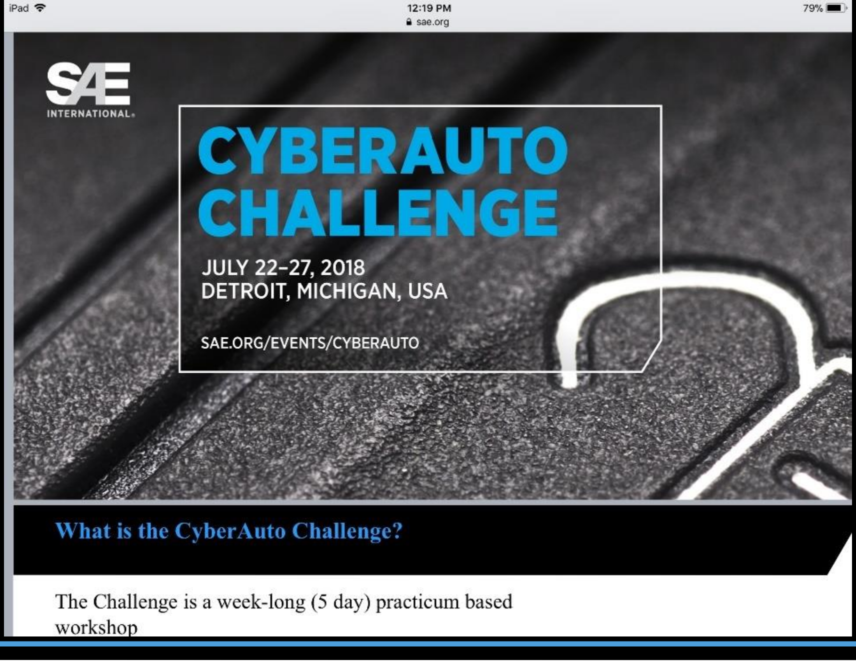
- Or, roll your own with opensource, SocketCAN interface

metasploit®

python™

GitHub

J3138 vehicle speed “spoof” test



CYBERAUTO CHALLENGE

JULY 22–27, 2018
DETROIT, MICHIGAN, USA

SAE.ORG/EVENTS/CYBERAUTO

What is the CyberAuto Challenge?

The Challenge is a week-long (5 day) practicum based workshop

SAE INTERNATIONAL

WCX WORLD CONGRESS EXPERIENCE™

APRIL 10-12, 2018 • COBO CENTER • DETROIT, MICHIGAN

sae.org/wcx

Thank you!

Mark Zachos
mzachos@dgtech.com

DG TECHNOLOGIES
Vehicle Network Solutions