Truck Systems Cybersecurity

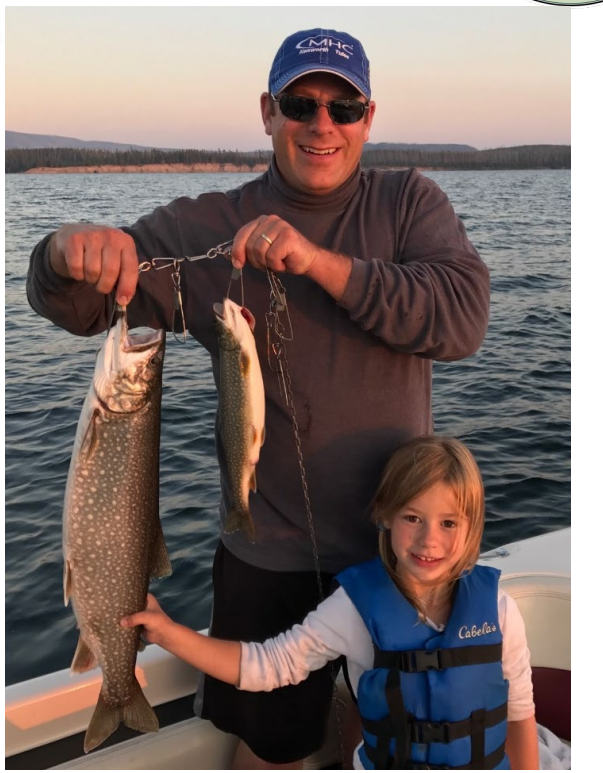
Jeremy S. Daily, Ph.D., P.E.

Jeremy.Daily@colostate.edu

Introduction and Overview

- Introduction to Trucks and Truck Systems
- Reading and Interpreting Schematics
- Vehicle Networking
- Diagnostics and Maintenance Systems
- RP1210 and DLL Shim Attacks

Jeremy S. Daily, Ph.D., P.E.



- U.S. Air Force (1995-2002)
  - Electronic Maintenance of Meteorological and Navigation Systems
  - Wright-Patterson Air Force Base, Dayton, OH
- Aerospace Engineer
  - Contractor for the Propulsion Directorate at WPAFB
- Ph.D. in Engineering from Wright State University (2006)
- Associate Professor of Mechanical Engineering at the University of Tulsa (2006)
- Founder of Synercon Technologies, LLC (2013)
  - Commercialized digital forensic technology developed at U. Tulsa.
  - Sold Synercon to the Dearborn Group in 2018.
- Co-Founded the CyberTruck Challenge (2017)
- Research Performer for NSF, DARPA, DOJ, and NMFTA
- Associate Professor of Systems Engineering at Colorado State University (2019)
- Hacked a ski boat to fish for lake trout with an auto-pilot trolling system

Let’s get started

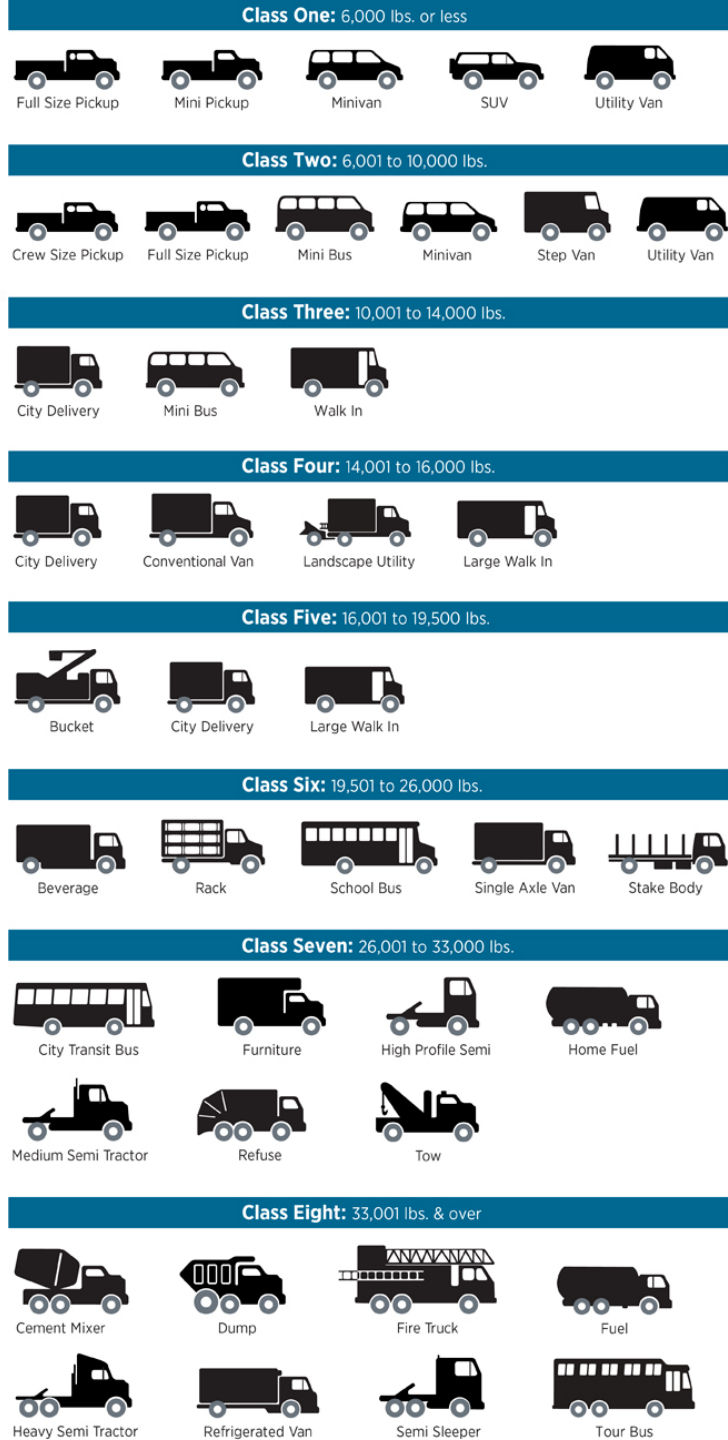
INTRODUCTION TO TRUCKS

What is a Truck?

- Generally called heavy vehicles
- Classifications based on Gross Vehicle Weight Rating

Gross Vehicle Weight Rating (lbs)	Federal Highway Administration	
	Vehicle Class	GVWR Catagory
<6,000	Class 1: <6,000 lbs	Light Duty <10,000 lbs
10,000	Class 2: 6,001–10,000lbs	
14,000	Class 3: 10,001–14,000 lbs	Medium Duty 10,001–26,000 lbs
16,000	Class 4: 14,001–16,000 lbs	
19,500	Class 5: 16,001–19,500 lbs	
26,000	Class 6: 19,501–26,000 lbs	
33,000	Class 7: 26,001–33,000 lbs	Heavy Duty >26,001 lbs
>33,000	Class 8: >33,001 lbs	

https://afdc.energy.gov/data/10381
https://afdc.energy.gov/data/10380



Comparison of Cars and Trucks

Cars

- Four Wheels
- Focused on Individual Consumer
- Vertically Integrated
- Proprietary CAN bus
- 11-bit CAN IDs
- Single dealer computer per brand
- SAE J2534 for diagnostic tool
- No communications to trailers
- Mostly Gasoline Powered
- Hydraulic Brakes

Trucks

- 4 to 18+ Wheels
- Focused on Utility or Fleet Customer
- Horizontally Integrated (more options)
- SAE J1939 Standardized CAN
- 29-bit CAN ID include Source Address
- Multiple vendors for ECU diagnostics
- ATA/TMC RP1210 for Diagnostic Tool
- SAE J560 has PLC4TRUCKS
- Mostly Diesel, needs DEF
- Air Brakes (needed for trailers)

Why are there computers on trucks?

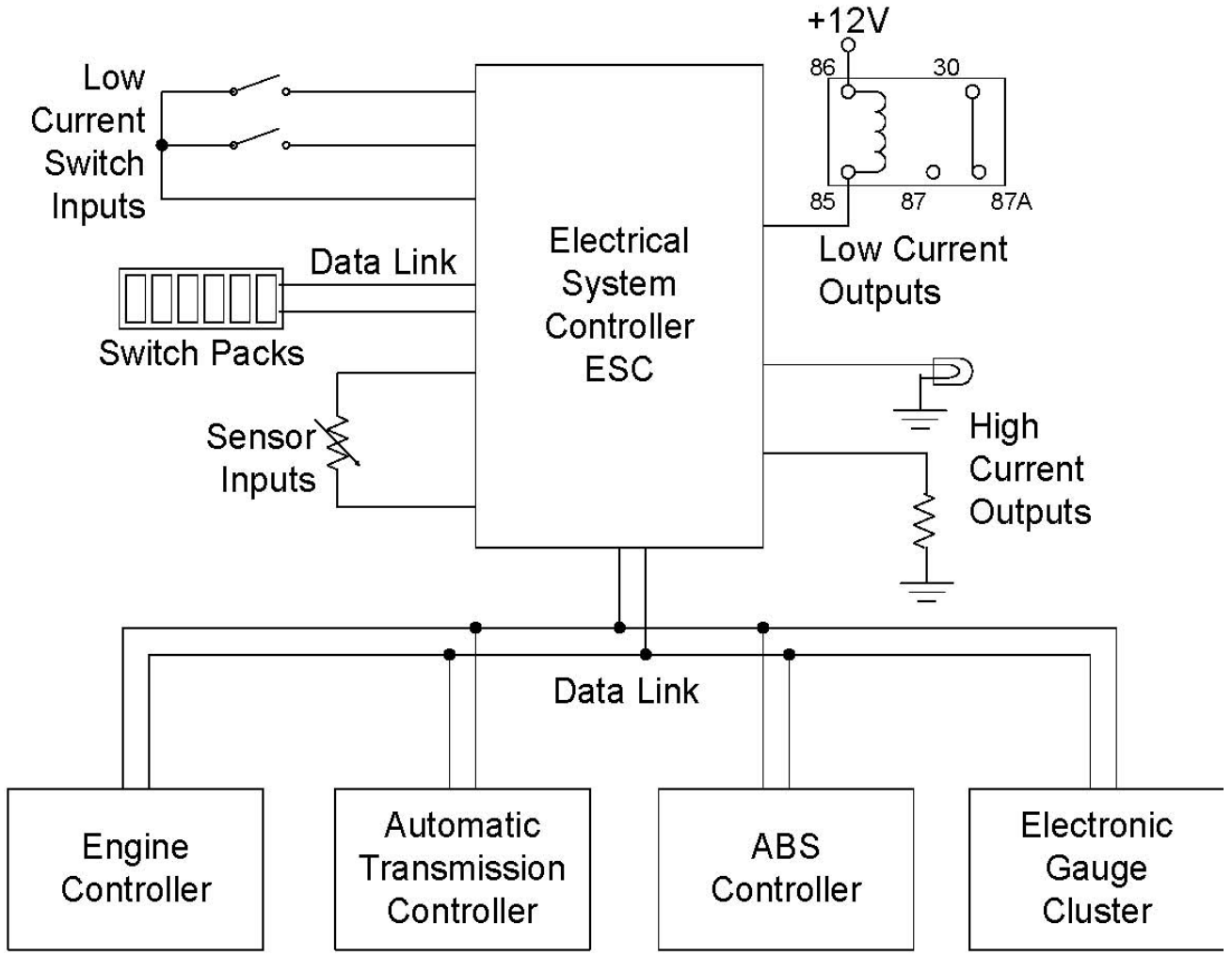
- Regulations to Reduce Emissions
  - Many software requirements are written by California Air Resource Board (CARB).
  - Computer control enables aftertreatment of exhaust
- Fuel Efficiency
  - Competitive Advantage
  - Fleet customers care about small improvements
- Automated Troubleshooting
  - Mechanics are now technicians

With all these computers, we need

HEAVY VEHICLE NETWORKING

Heavy Vehicle Networks

- Simplify Wiring
- Enables multiple systems on one bus
- Data sharing between ECUs
- External interface with 6 or 9-pin connector



Network Standards

- SAE J1708 and J1587
  - Based on a 9600 baud RS-485 connection
  - Similar to the serial port on a computer
  - Phased out, but still on the road (DDEC 4 and 5, Cat ADEM3)
- SAE J1939
  - Based on a 250,000 baud Controller Area Network (CAN) connection
  - CAN is used on passenger cars too.

J1708 Network Messages

- Speed signals are interpreted and broadcast as serial messages in frames.
- J1708 Frame:
- MID: Message Identifier
  - 128 (0x80) for Engine
  - 183 (0xB6) for Off-board Programming Station
- PID: Parameter Identification
  - 84 (0x54) for Road Speed
  - 190 (0xBE) for Engine Speed

MID	PID	DATA	Checksum

Interpreting J1708 Data

A.84 ROAD SPEED

Indicated vehicle velocity.

Parameter Data Length: 1 Character
Data Type: Unsigned Short Integer
Bit Resolution: 0.805 km/h (0.5 mph)
Maximum Range: 0.0 to 205.2 km/h (0.0 to 127.5 mph)
Transmission Update Period: 0.1 s
Message Priority: 1
Format:

PID	Data
84	a
a—	Road speed

Example Speed Data

- J1708 Hex Serial Data is found in a log file:

Line	Abs Time(Sec)	Rel Time (Sec)	Er	Tx	Description	MID	PID	DATA
24723	538.7992186	0.005920976	F	F	J1708 $80	80	54	37

- MID: Engine
- PID: Road Speed
  - Determine Decimal (55 in this case)
  - Multiply by 0.5 (27.5 in this case)
  - Append units from J1587: 27.5 mph

Converting Hex to Decimal

- Excel: =HEX2DEC(“37”)
- Windows Calculator
- Python:

```
>>> pgn = 0xFEF1
>>> pgn
65265
>>> "{:04X}“.format(pgn)
FEF1
>>> int("65265")
65265
>>> int("0xFEF1",16)
65265
>>>
```

Enter values as hex

Default display is a decimal

Use a format statement to display hex

Convert decimal strings to integers

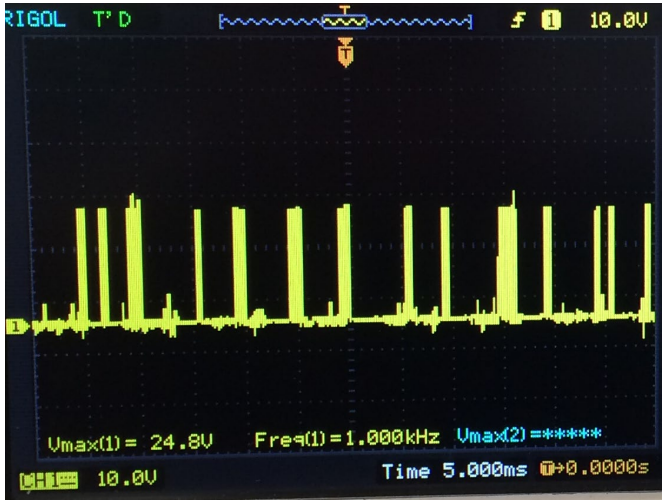
Convert hex strings to integers

Look at the struct library too!

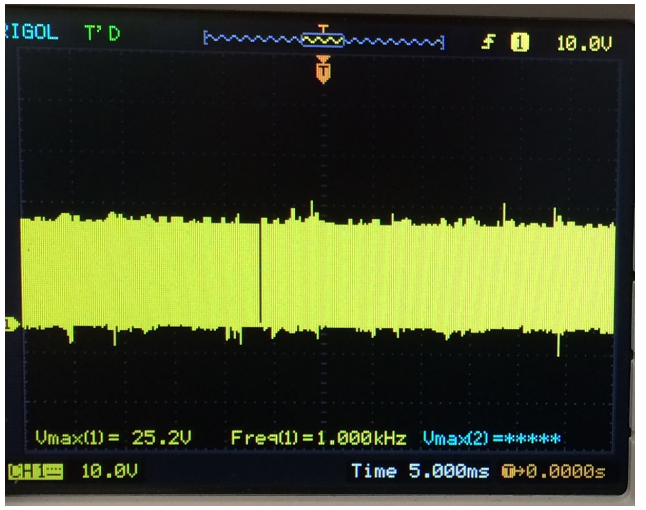
Controller Area Networks

- Serial bus introduced by Bosch in 1986
- A 2-wire bus with multi-master capability with Collision Detection, Arbitration, and Error Checking
  - Result: nearly 100% data integrity in harsh environments
- Trusting… all messages are inherently believed

Normal CAN



Flooded CAN

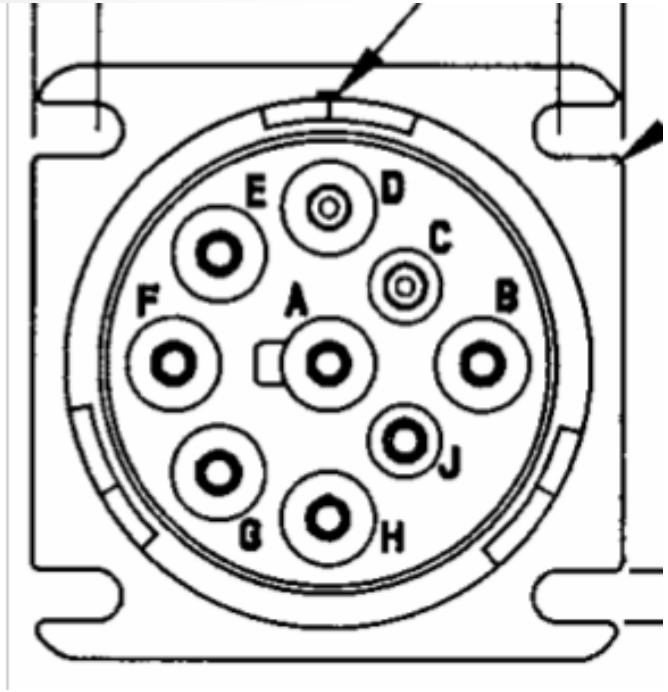


SAE J1939

- Built on CAN
  - Fast enough for real-time control
  - 250k (black connector)
  - 500k (green connector)
- Uses the message identifier to define purpose.
- Defines everything from physical connections to diagnostic applications.
- Provides the basis for understanding and interpreting some of the data.

J1939 Connector (9-Pin)

- Pin A: Battery (-)
- Pin B: Battery (+)
- Pin C: CAN High
- Pin D: CAN Low
- Pin E: CAN Shield
- Pin F: J1708 (+)
- Pin G: J1708 (-)
- Pin H: OEM Use or 2nd CAN High
- Pin J: OEM Use or 2nd CAN Low



- Check for +12 V on pin B with Pin A to ground
- Check for 60 Ohms between Pin C and D on J1939 enabled vehicles with vehicle off.

Pinouts

- https://www.dgtech.com/wp-content/uploads/2016/04/Pinouts_ICR.pdf

DG Technologies Product Pinouts and Industry Connectors Reference Guide

Including the J1939 Type-2 Connector, CAN-bus Troubleshooting, and 2013+ Volvo J1962 Connector

Industry Connectors

- DG Tech's Guide http://www.dgtech.com/product/dpa5/manual/DPA_Pinouts.pdf
- Deutsch Catalog from LADD distribution (pg 92 for CAN) https://laddinc.com/wp-content/uploads/2014/08/LADD-Catalog.pdf
- Digi-key for buying parts: http://www.digikey.com/Suppliers/us/Amphenol-Sine-Systems.page?lang=en

Model for Network Communication

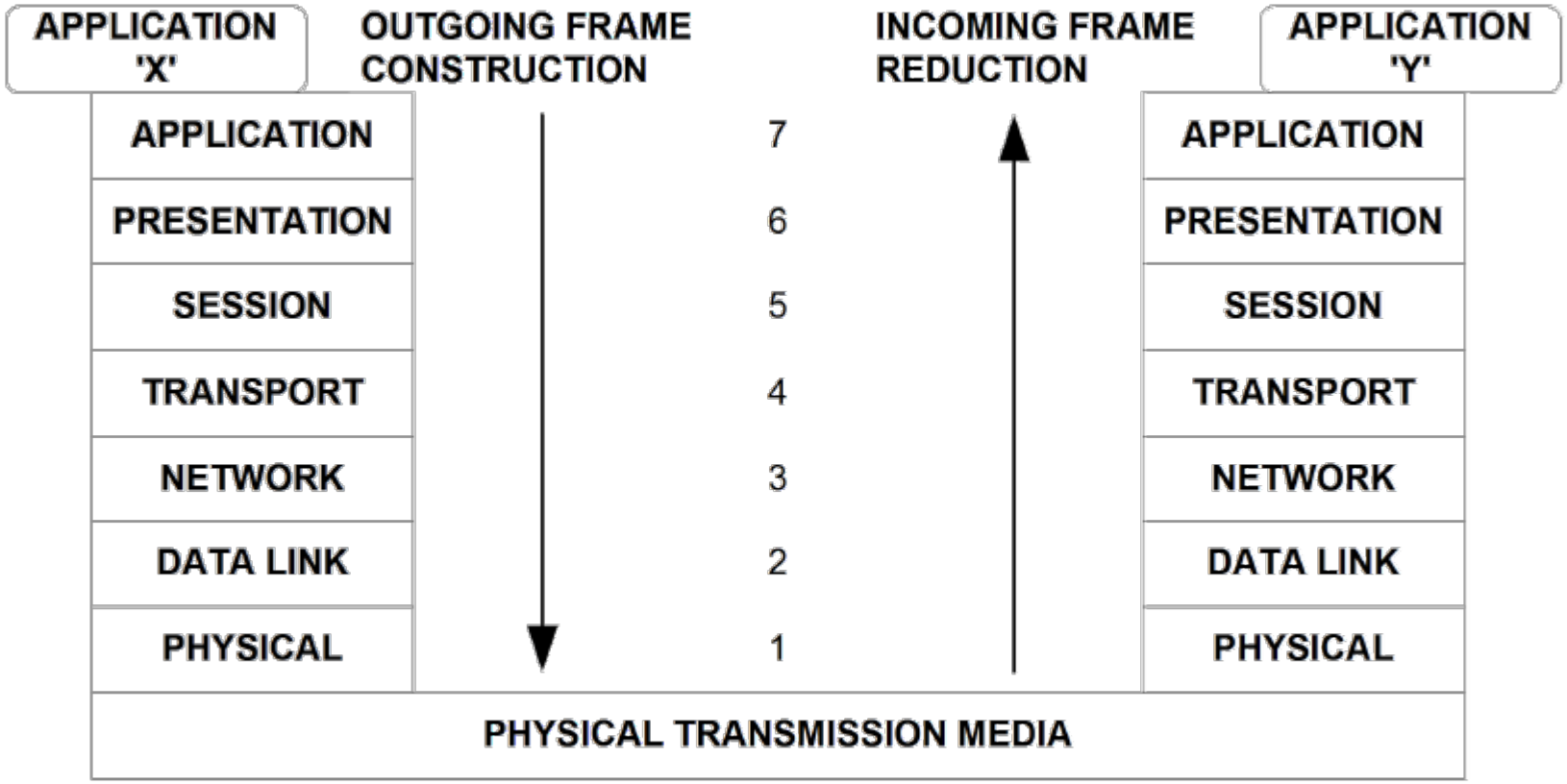
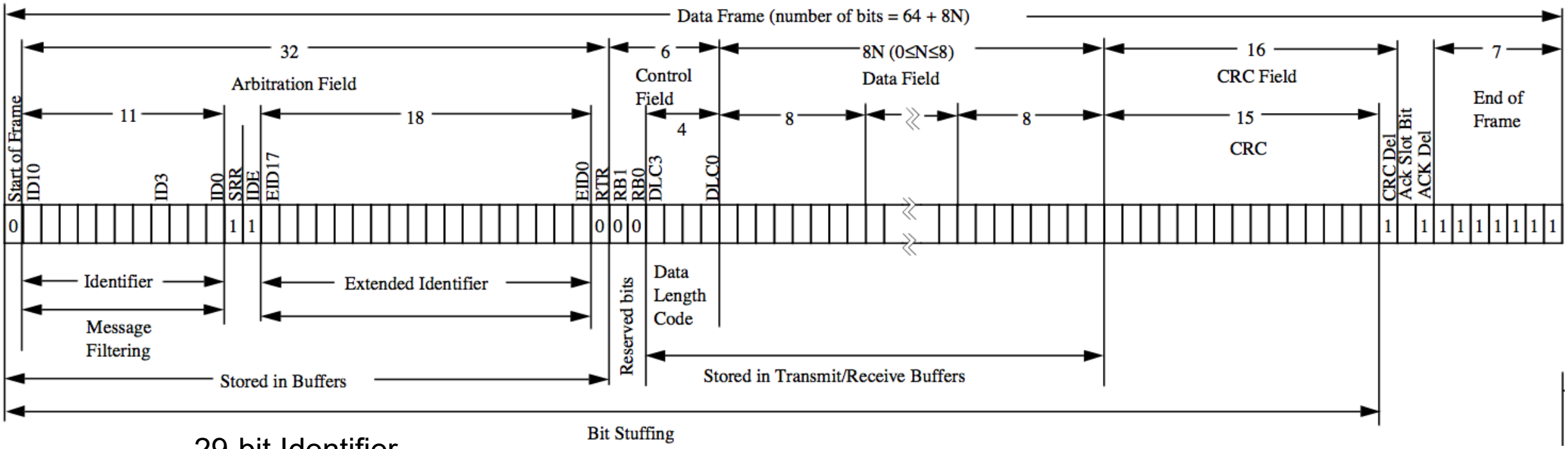


FIGURE 1 - THE OSI SEVEN LAYER MODEL

SAE J1939

- Arranged to reflect OSI model
  - J1939-1X: Physical connections
  - J1939-2X: Transport layer for long messages
  - J1939-7X: Application layer (bring meaning to data)
- Controller Applications (CA) are given source addresses
- Defines message transport protocol for up to 1785 bytes
- Defines source address claiming
  - Every CA is expected to have a unique address

Extended CAN Frame Structure



29-bit Identifier (Arbitration)

Control Field

Data Field

Error Checking

Data typically transferred up to 8 bytes at a time

Extended CAN Format for J1939

CAN EXTENDED FRAME FORMAT	SOF	IDENTIFIER 11 BITS											SRR	IDE	IDENTIFIER EXTENSION 18 BITS																RTR	...
J1939 FRAME FORMAT	SOF	PRIORITY			EDP	DP	PDU FORMAT (PF) 6 BITS (MSB)						SRR	IDE	PF (CONT.)		PDU SPECIFIC (PS) (DESTINATION ADDRESS, GROUP EXT. OR PROTIRETARY)								SOURCE ADDRESS								RTR	...
		3	2	1			8	7	6	5	4	3			2	1	8	7	6	5	4	3	2	1	8	7	6	5	4	3	2	1		
J1939 FRAME BIT POSITION	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	
CAN 29 BIT ID POSITION		28	27	26	25	24	23	22	21	20	19	18			17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0		

- SOF = Start of Frame
- EDP = Extended Data Page
- DP = Data Page
- PDU = Protocol Data Unit
- PF = PDU Format
- PG = Parameter Group
- SRR = Substitute Remote Request
- IDE = Identifier Extension Bit
- RTR = Remote transmission request

Source: SAE J1939-21

CAN Collisions and Arbitration

- Problem:
  - All have access to the bus at the same time
  - Multiple devices try to send data at once
- Solution:
  - CAN Arbitration where the highest Priority message comes through
  - Others wait and retry
- Arbitration
  - Message Identifier (MID) determines priority
  - 0 is dominant, so lowest MID wins

29-bit Identifier Example

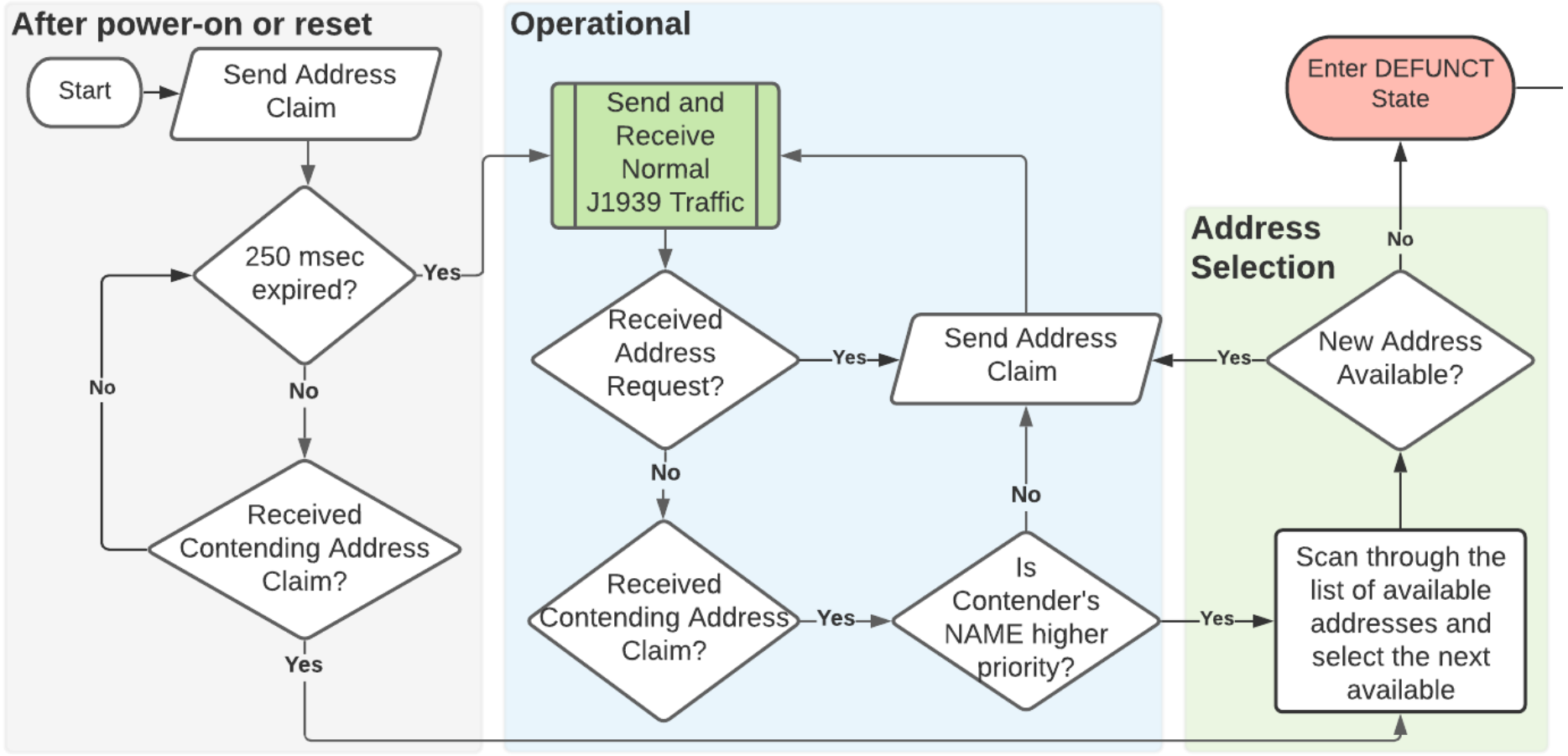
CAN Extended Frame Format		Identifier											SRR	IDE	Identifier Extension																		
J1939 Frame Bit Position	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
		Transmitted Parameter Group Number (PGN)																															
J1939 Frame Format	Start	Priority			EPD	DP	Protocol Data Unit Format (PF)								PDU Specific (PS) (Either a DA or GE)										Network Unique Source Address (SA)								RTR
29-bit Identifier Position		28	27	26	25	24	23	22	21	20	19	18			17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	
Decimal value for PGN							32768	16384	8192	4096	2048	1024			512	256	128	64	32	16	8	4	2	1									
Ex. 1: Transmission Control		0	0	0	0	0	0	0	0	0	0	0			0	1	0	0	0	0	0	0	0	0									
Ex. 2: Pending DTC		0	0	0	0	0	1	1	1	1	1	1			0	1	1	0	0	0	0	0	1	0									
Ex. 3: Immediate Fault Status		0	0	0	0	0	1	0	0	1	1	1			1	1	0	0	0	0	0	0	0	0									

CAN Extended Frame Format		Identifier											SRR	IDE	Identifier
J1939 Frame Bit Position	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
		Transmitted Parameter Group Number (PGN)																				
J1939 Frame Format	Start	Priority			EPD	DP	Protocol Data Unit Format (PF)								PDU Specific (PS) (Either a DA or							
29-bit Identifier Position		28	27	26	25	24	23	22	21	20	19	18			17	16	15	14	13	12	11	10
Decimal value for PGN							32768	16384	8192	4096	2048	1024			512	256	128	64	32	16	8	4
Ex. 1: Transmission Control		0	0	0	0	0	0	0	0	0	0	0			0	1	0	0	0	0	0	0
Ex. 2: Pending DTC		0	0	0	0	0	1	1	1	1	1	1			0	1	1	0	0	0	0	0
Ex. 3: Immediate Fault Status		0	0	0	0	0	1	0	0	1	1	1			1	1	0	0	0	0	0	0

Some messages have higher priority over others.

Source Address and Address Claiming

- See Digital Annex for a list of Source Addresses



Address NAME Field

Arbitrary Address Capable	Industry Group	Vehicle System Instance	Vehicle System	Reserved	Function	Function Instance	ECU Instance	Manufacturer Code	Identity Number
	SAE		SAE	SAE	SAE			SAE	
1 bit	3 bits	4 bits	7 bits	1 bit	8 bits	5 bits	3 bits	11 bits	21 bits

- From SAE J1939-81, the following NAME field is 64 Bits (8 bytes) long.
- Value is translated with little endian format (Intel), so the least significant byte is first.
- Example 1: Caterpillar C15 with ADEM4 ECU

```
can1  18EEFF00   [8]  D0 6B 01 01 00 00 00 80
```

- Example 2: Detroit Diesel CPC3Evo

```
can1  18EEFF00   [8]  00 00 C0 01 00 00 00 00
```

- Example 3: Allison Transmission

```
can1  18EEFF03   [8]  64 00 40 00 00 03 03 10
```

CAN ID has:
- Priority = 6,
- Parameter Group Number = 0xEE00,
- Destination Address = 0xFF (Global),
- Claimed Source Address = 0x00 (Engine #1)

Example 1: Caterpillar

```
can1  18EEFF00   [8]  D0 6B 01 01 00 00 00 80
```

- Byte 8 (0x80) = 0b1000 0000, which means:
  - it is arbitrary address capable,
  - the industry group is 0 (global), and
  - the vehicle system instance is zero.
- Byte 5 -7 (00 00 00), which means:
  - the vehicle system, function, and function instance are all zero, which is consistent with an engine controller
- Byte 4 (0x01), Bits 1-8 = MSB of Mfg Code
  Byte 3 (0x01), Bits 8-6 = LSB of Mfg Code
  - 0b0000 0001 0000 0001 = 0b1000 = 8 (dec)
- Byte 3 (0x01), bits 1-5 = MSB of Identity Field
  Byte 2 (0x6B) = 2nd byte of identity field
  Byte 1 (0xD0) = LSB of identity field
  - 0b0 0001 0110 1011 1101 0000 = 93,136 (dec)

Manufacturer ID Codes (Table B10)

The list of all Manufacturer Identifier code assignments.

Return To Documentation Tab

R	Mfr ID	Manufacturer
	0	Reserved
	1	Bendix Commercial Vehicle Systems LLC (formerly Allied Signal Inc.)
	2	Allison Transmission, Inc.
	3	Ametek, US Gauge Division
	4	Ametek-Dixson
	5	AMP Inc.
	6	Berifors Electronics AB
	7	Case Corp.
	8	Caterpillar Inc.
	9	Chrysler Corp.
	10	Cummins Inc (formerly Cummins Engine Co)
	11	Dearborn Group Inc.
	12	Deere & Company, Precision Farming
	13	Delco Electronics
	14	Detroit Diesel Corporation
	15	DICKEY-john Corporation
	16	Eaton Corp

Example 2: Detroit Diesel

```
can1  18EEFF00   [8] 00 00 C0 01 00 00 00 00
```

- Byte 8 (0x00) = 0b0000 0000, which means:
  - it is NOT arbitrary address capable,
  - the industry group is 0 (global), and
  - the vehicle system instance is zero.
- Byte 5 -7 (00 00 00), which means:
  - the vehicle system, function, and function instance are all zero, which is consistent with an engine controller
- Byte 4 (0x01), Bits 1-8 = MSB of Mfg Code
  Byte 3 (0xC0), Bits 8-6 = LSB of Mfg Code
  - 0b0000 0001 1100 0000 = 0b1110 = 14 (dec)
- Byte 3 (0x01), bits 1-5 = MSB of Identity Field
  Byte 2 (0x00) = 2nd byte of identity field
  Byte 1 (0x00) = LSB of identity field
  - 0b0 0000 0000 0000 0000 0000 (likely not used)

Manufacturer ID Codes (Table B10)

The list of all Manufacturer Identifier code assignments.

Return To Documentation Tab

R	Mfr ID	Manufacturer
	0	Reserved
	1	Bendix Commercial Vehicle Systems LLC (formerly Allied Signal Inc.)
	2	Allison Transmission, Inc.
	3	Ametek, US Gauge Division
	4	Ametek-Dixson
	5	AMP Inc.
	6	Berifors Electronics AB
	7	Case Corp.
	8	Caterpillar Inc.
	9	Chrysler Corp.
	10	Cummins Inc (formerly Cummins Engine Co)
	11	Dearborn Group Inc.
	12	Deere & Company, Precision Farming
	13	Delco Electronics
	14	Detroit Diesel Corporation
	15	DICKEY-john Corporation
	16	Eaton Corp

Example 3: Allison Transmission

```
can1  18EEFF03 [8] 64 00 40 00 00 03 03 10
```

- Byte 8 (0x10) = 0b0001 0000, which means:
  - it is NOT arbitrary address capable,
  - the industry group is 1 (on-highway), and
  - the vehicle system instance is zero.
- Byte 7 (0x03), the vehicle system is the transmission
- Byte 6 (0x03), function is the transmission
- Byte 5 (0x00), the function and ECU instance is zero, which means it's the first instance.
- Byte 4 (0x00), Bits 1-8 = MSB of Mfg Code
  Byte 3 (0x40), Bits 8-6 = LSB of Mfg Code
  - 0b0000 0000 0100 0000 = 0b0010 = 2 (dec)
- Bytes 3-1 (0x00064) comprise the identity field

All Industry Groups Inclusive NAME Functions (Table B11)

The NAME Functions assigned to the lower 128 Function values. These lower 128 NAME Function values are independent of the Vehicle System or Industry Group, which means they can be used all eight Industry Groups. These should not be confused with the upper 128 NAME Functions of Industry Group 0 which is an Industry Group itself but applicable to all industries. The NAME fields are described in SAE J1939-81.

Return To Documentation Tab

Revised	Function ID	Function Description	Notes
	0	Engine	While the function identifies what is typically the mechanical power source of the machine, the reference tends to be to the management system that controls the torque vs speed vs command (typically throttle) of said power source.
	1	Auxiliary Power Unit (APU)	Power source for operating systems without the use of the prime 'drive' engine.
	2	Electric Propulsion Control	Control system which operates the drive mechanism when it is electrically powered, such as battery-motor, or engine-generator-motor hybrids
	3	Transmission	A mechanical system for alter the speed vs torque output of the engine to a level usable by another system on the machine. Although again the network reference is actually to the system which controls the operation of said transmission

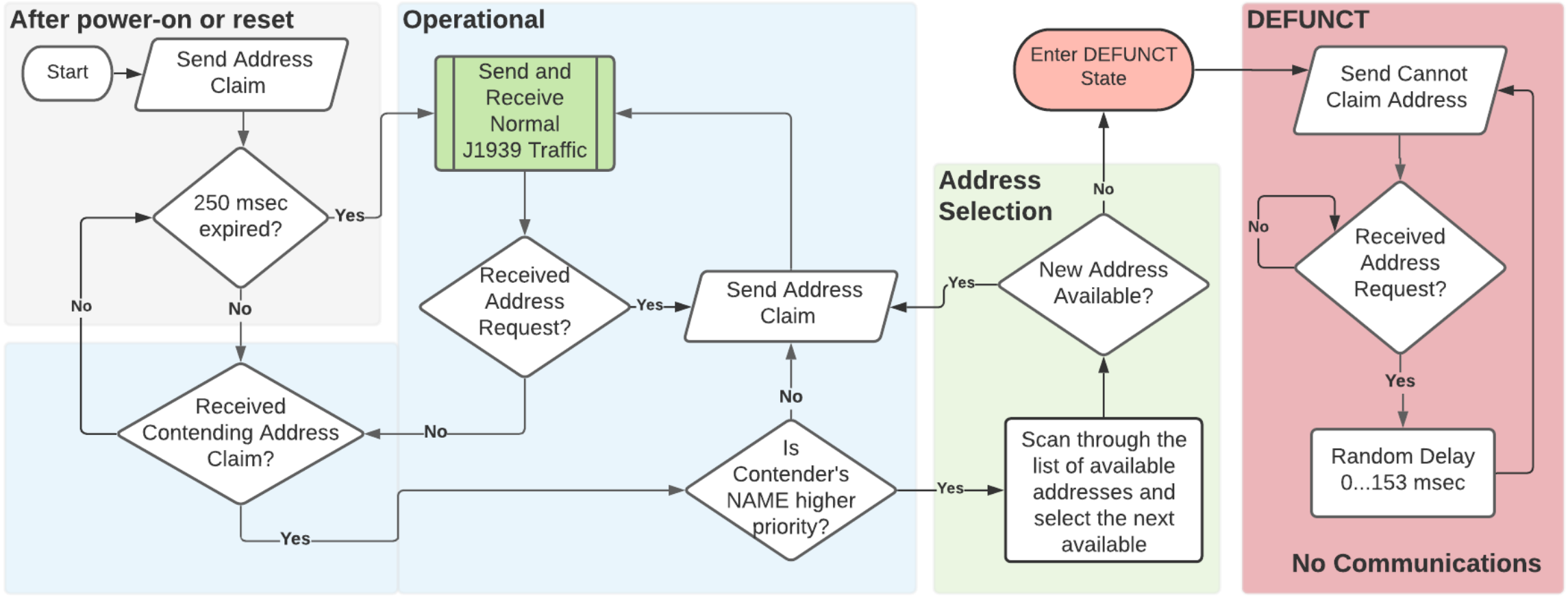
Manufacturer ID Codes (Table B10)

The list of all Manufacturer Identifier code assignments.

Return To Documentation Tab

R	Mfr ID	Manufacturer
	0	Reserved
	1	Bendix Commercial Vehicle Systems LLC (formerly Allied Signal Inc.)
	2	Allison Transmission, Inc.
	3	Ametek, US Gauge Division
	4	Ametek-Dixson

Address Claimed by Another ECU



Learn More about Hacking J1939 Address Claims

Murvay and Groza (2017):

http://www.aut.upt.ro/~pal-stefan.murvay/papers/security-shortcomings-countermeasures-SAE-J1939-commercial-vehicle-protocol.pdf

SystemsCyber on Github (Colorado State Univ.)

https://github.com/SystemsCyber/TruckCapeProjects/blob/master/Jupyter/06%20J1939%20Address%20Claim.ipynb

Campo, Mukherjee, and Daily (2021)

SAE International Journal of Commercial Vehicles
Manuscript Number: JCV-2021-0029R1
Real-time Network Defense of SAE J1939 Address Claim Attacks

Activity On Trucks

FILL OUT TRUCK INSPECTION WORKSHEET

Activity

TRACE SCHEMATICS

DDEC 6 CPC

- Identify and trace the following:
  - Accelerator Pedal Input
  - Diagnostic Port (i.e. J1939)
  - Engine CAN
  - Vehicle Speed Sensor

Challenge: How does the CPC know about Engine RPM?

Cummins CM2350

- https://quickserve.cummins.com
- Determine the engine components on CAN:
  - What pins are used for the VGT?
  - What pins are used for the Aftertreatment System?
  - How is engine speed determined?
    - What sensor?
    - What pins?
    - What signal?

Available on the NAS Resources

Deep Dive into

HOW EVENTS GET SET IN AN ENGINE CONTROL MODULE

Overview

- Vehicle Speed Data
- Synchronized Testing Results
  - Network Data, EDR Data, and GPS Data
  - Out-of-service brakes

We can’t work with this one

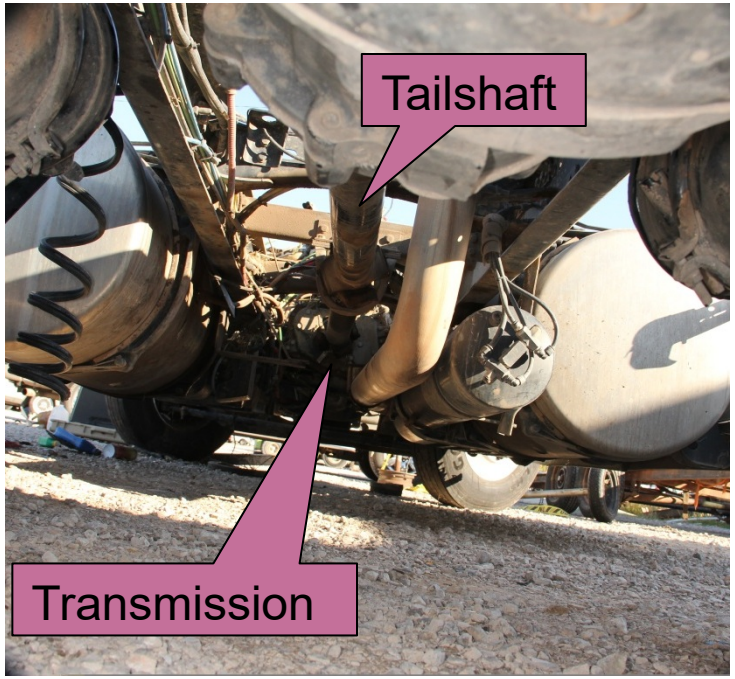
Missing Data??

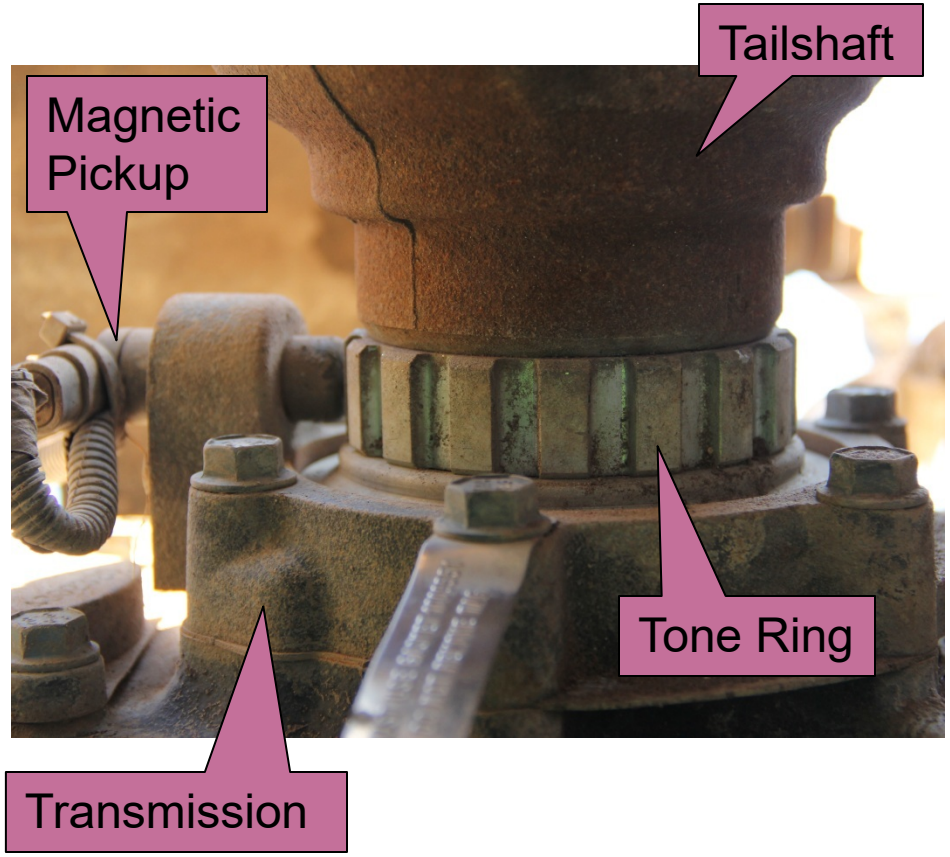
Pavement to EDR Data

Wheels Turn → VSS Signal Generated → ECM Calculates Speed → Data Transmitted on Network

Sensing Speed

- A magnetic pick-up uses variable reluctance to sense the rotation of the tailshaft.

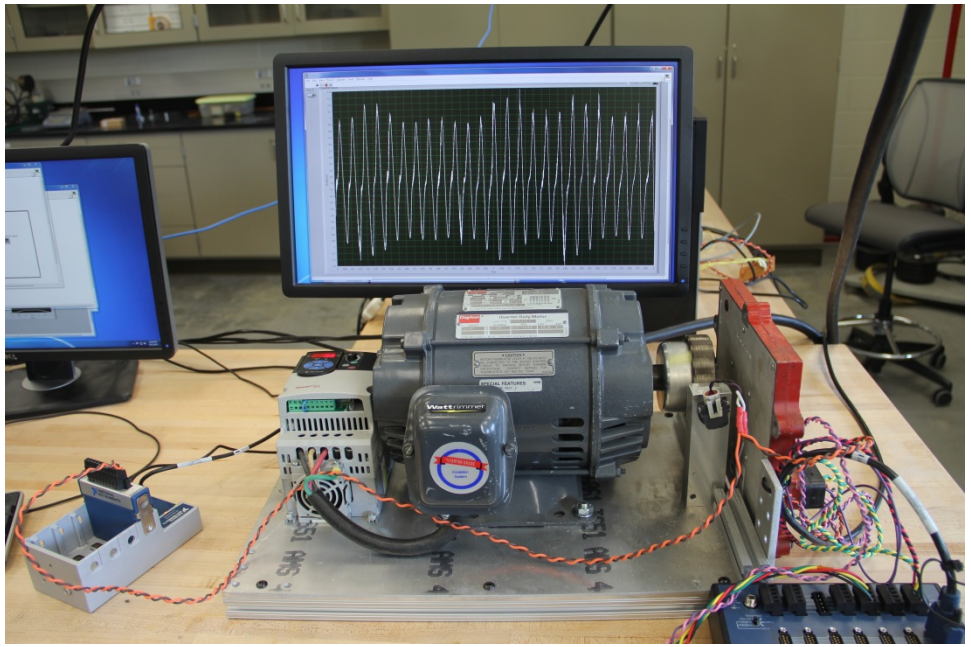




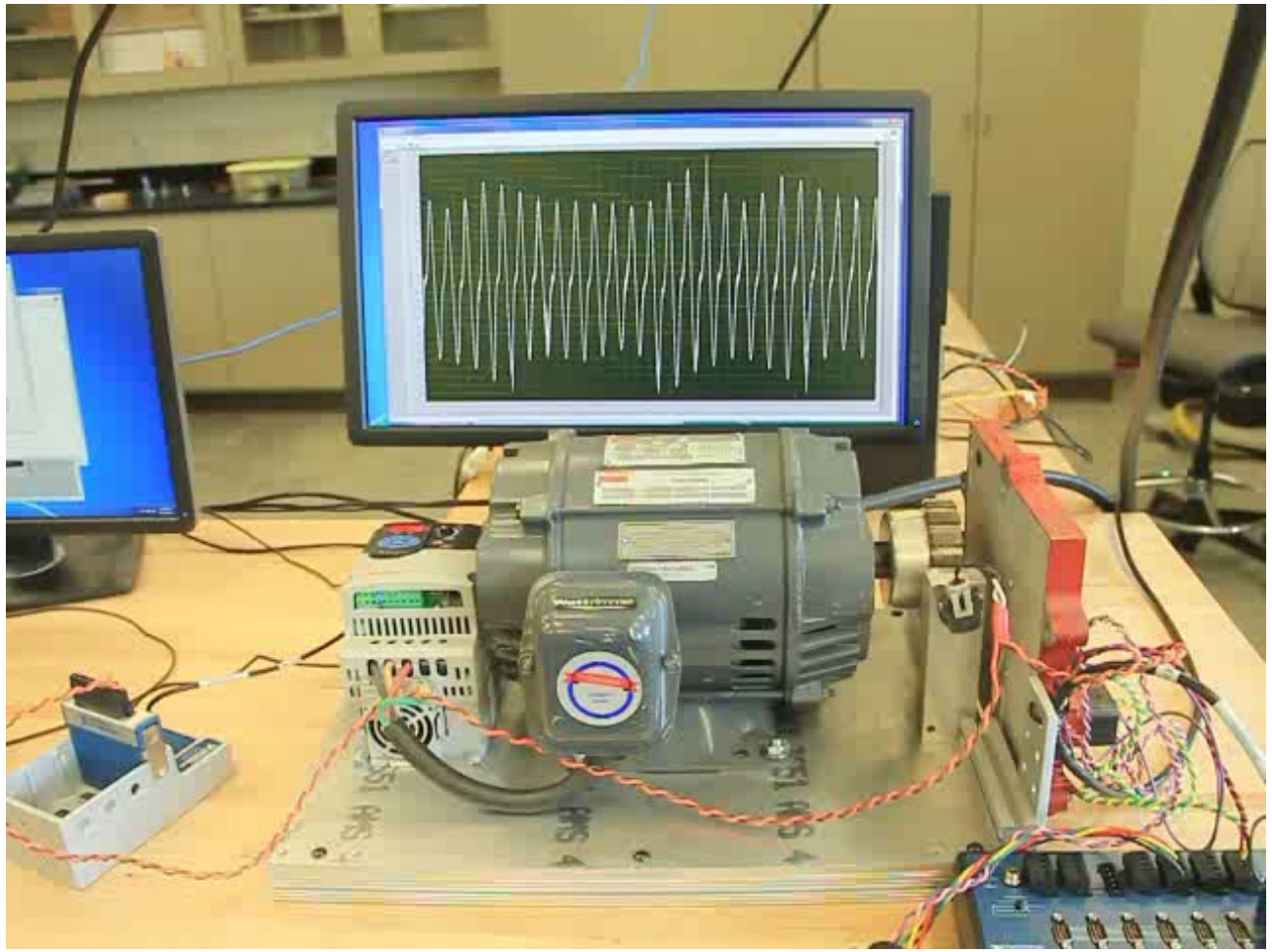

Vehicle Speed Sensor
16 Tooth Tone Ring

Pavement to EDR Data

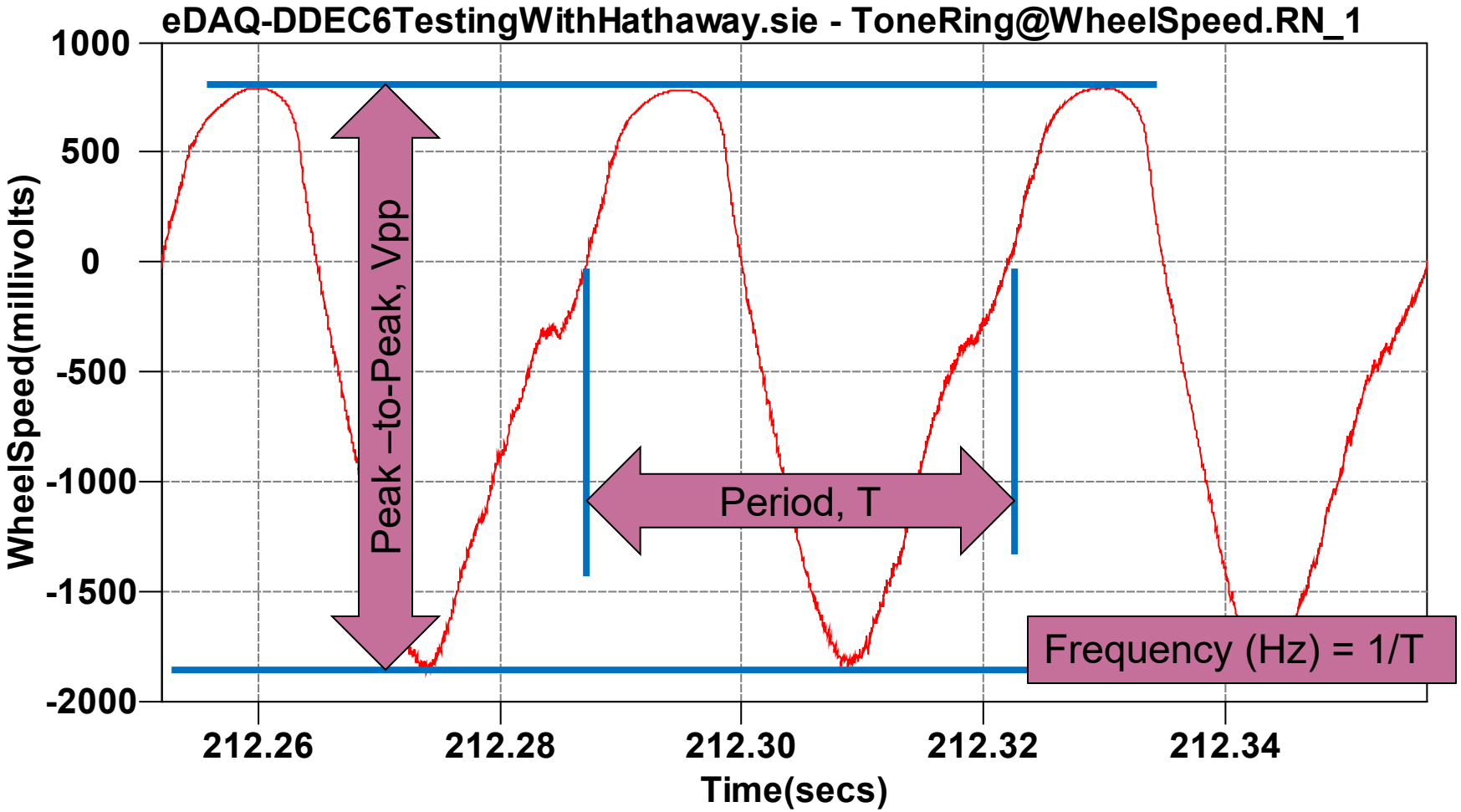
Wheels Turn → **VSS Signal Generated** → ECM Calculates Speed → Data Transmitted on Network



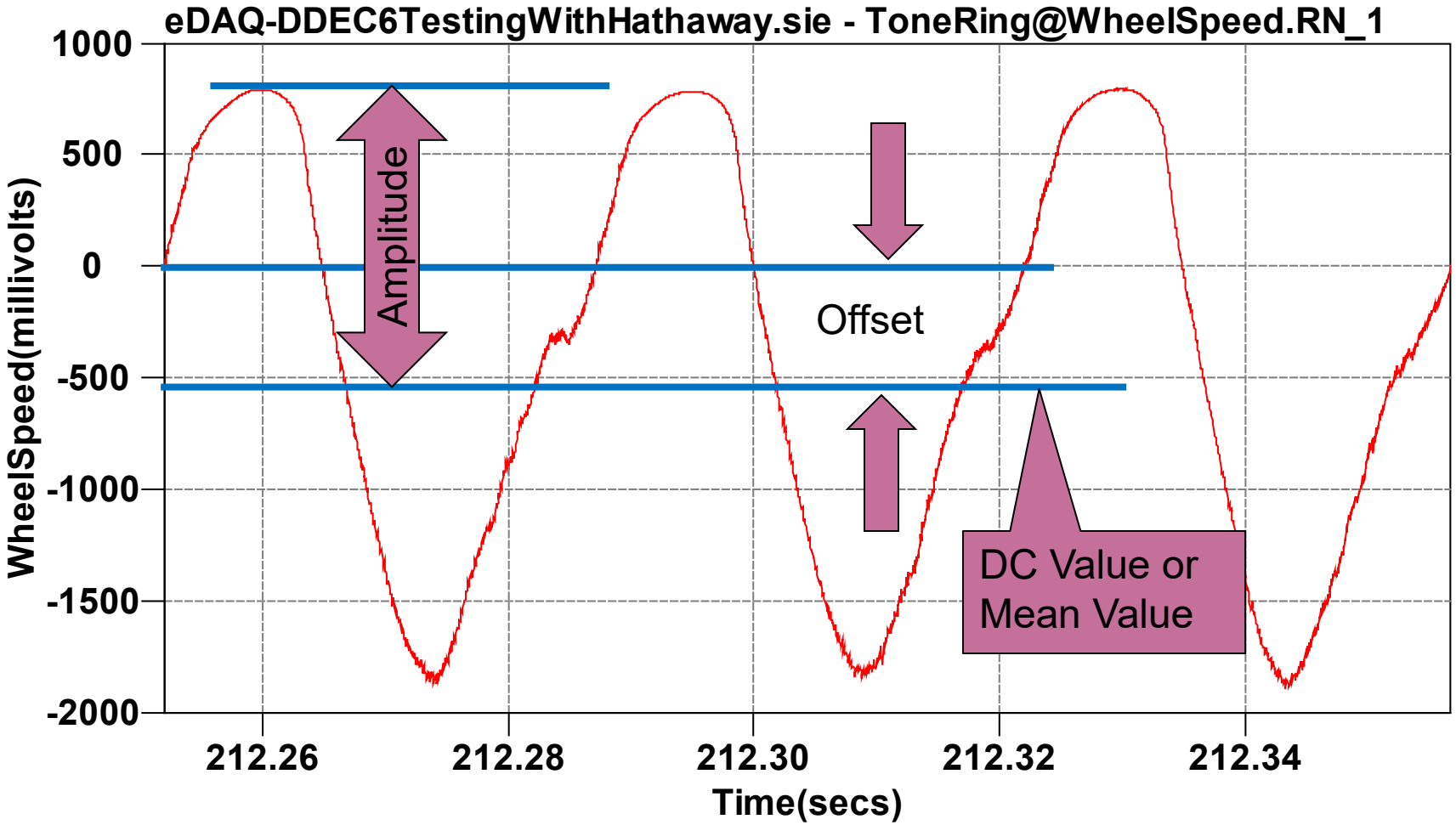
Speed Sensing In Action



Describing a Signal

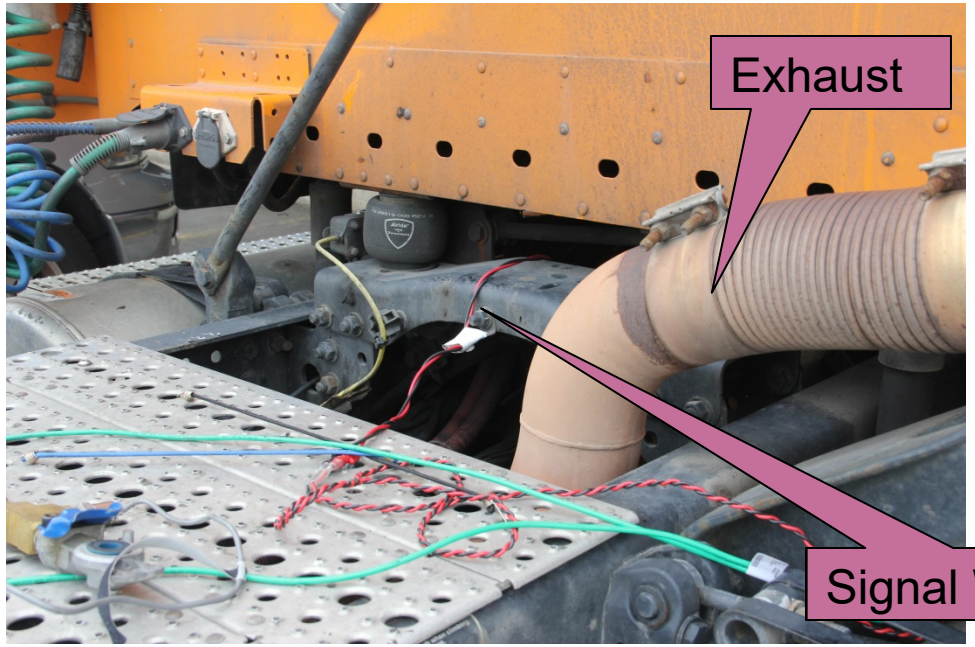


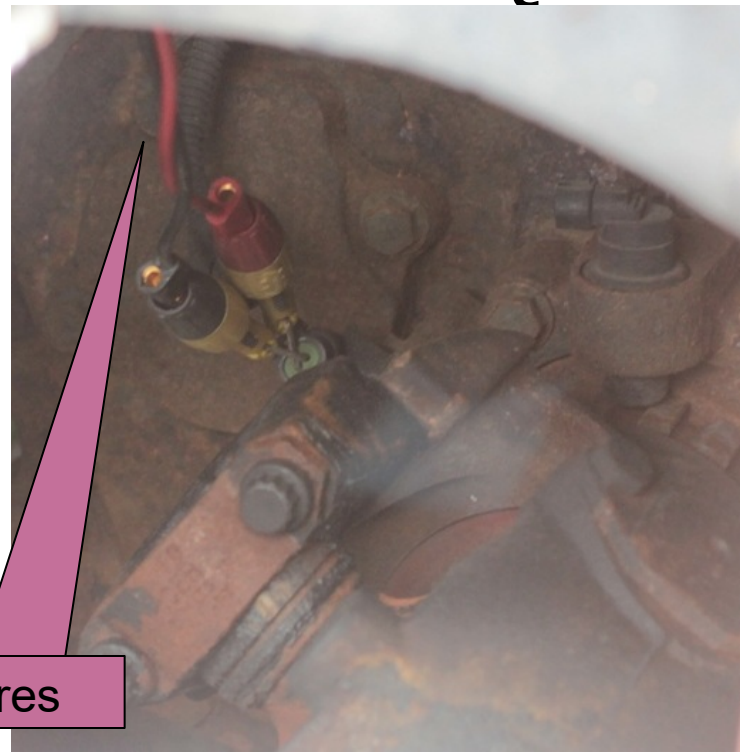
Describing a Signal (Cont.)



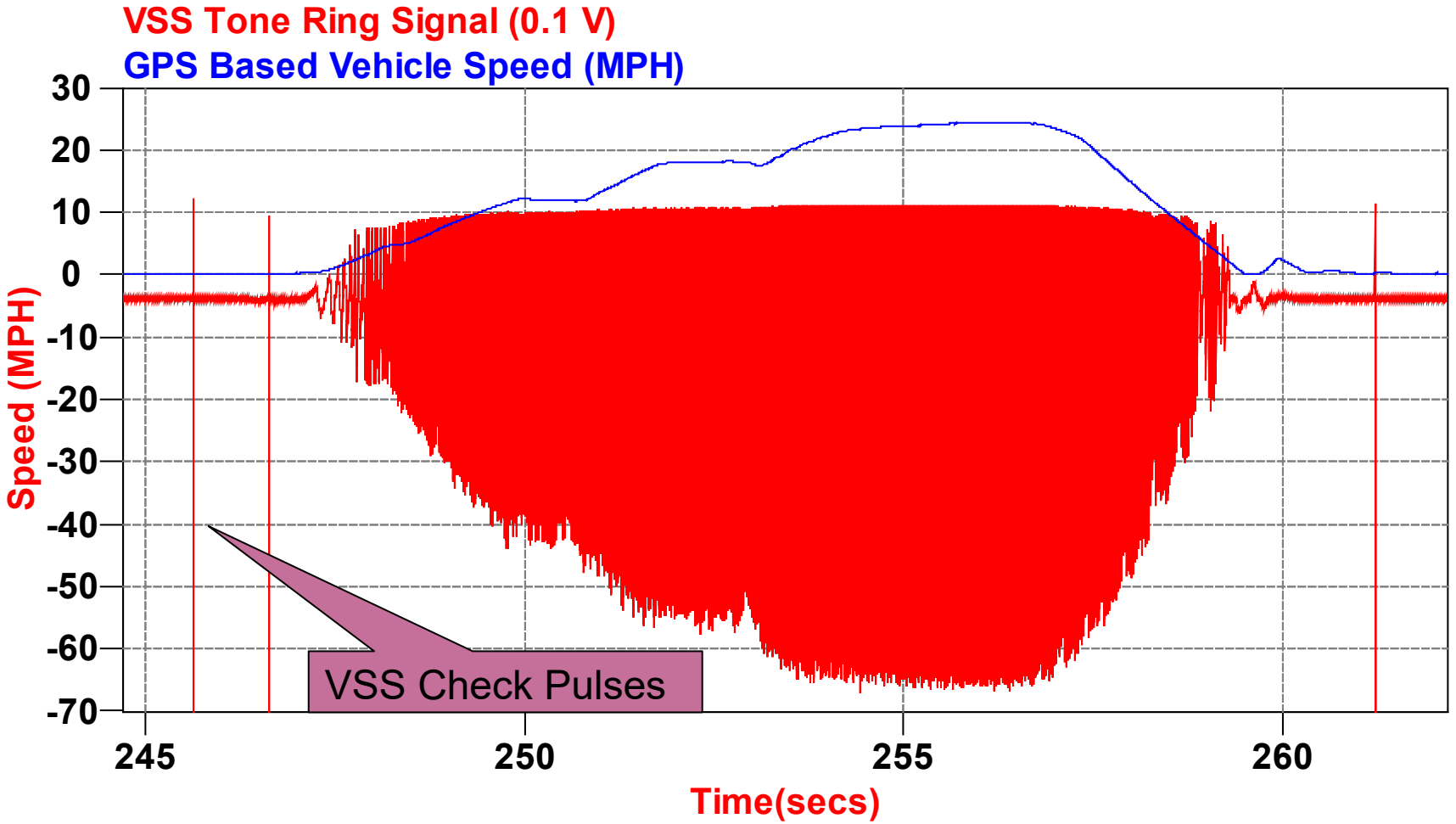
Actual Vehicle Speed Sensor Signals

- Wire pierce near the sensor
- Record with the Analog In feature of the eDAQ.

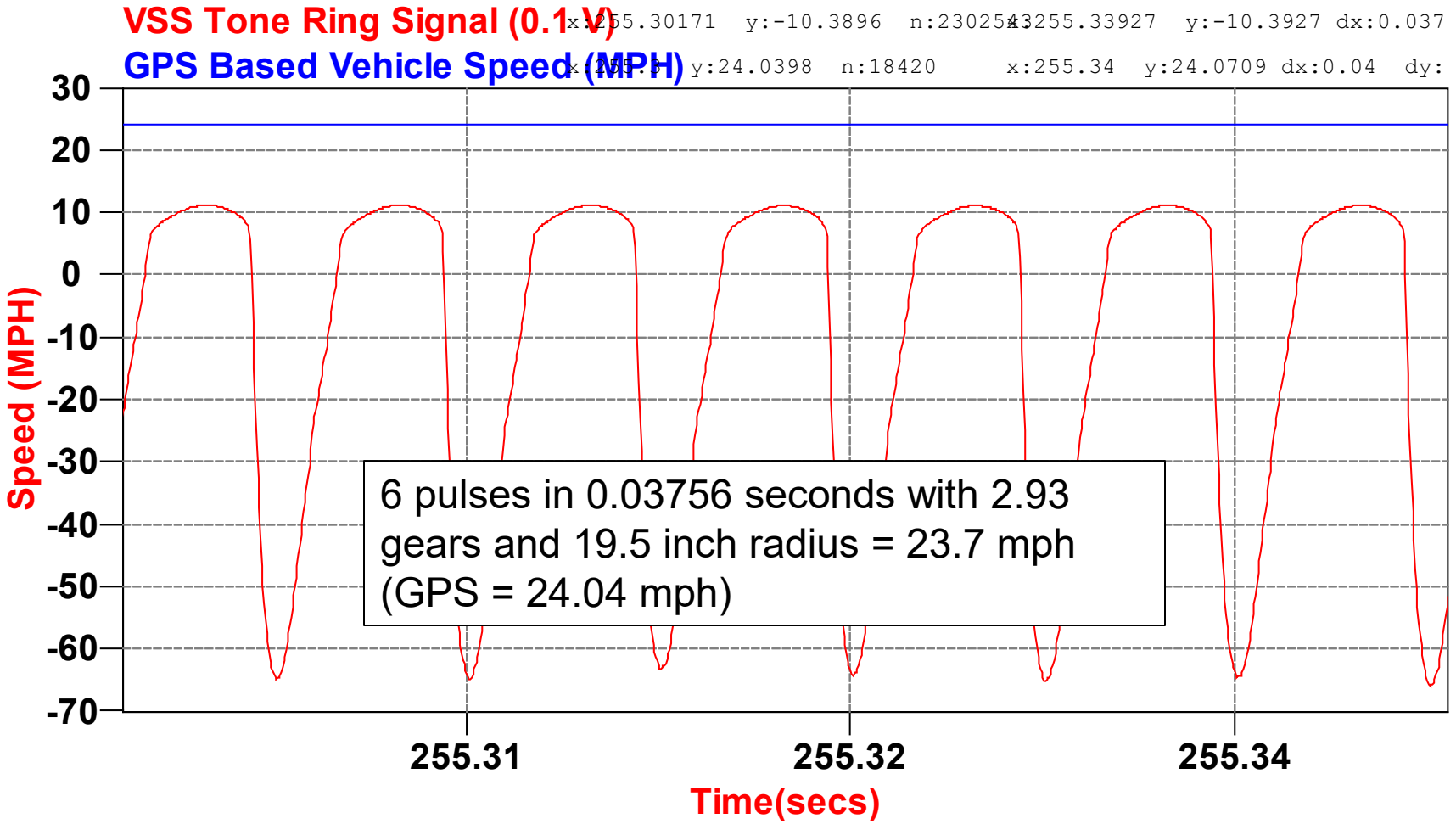




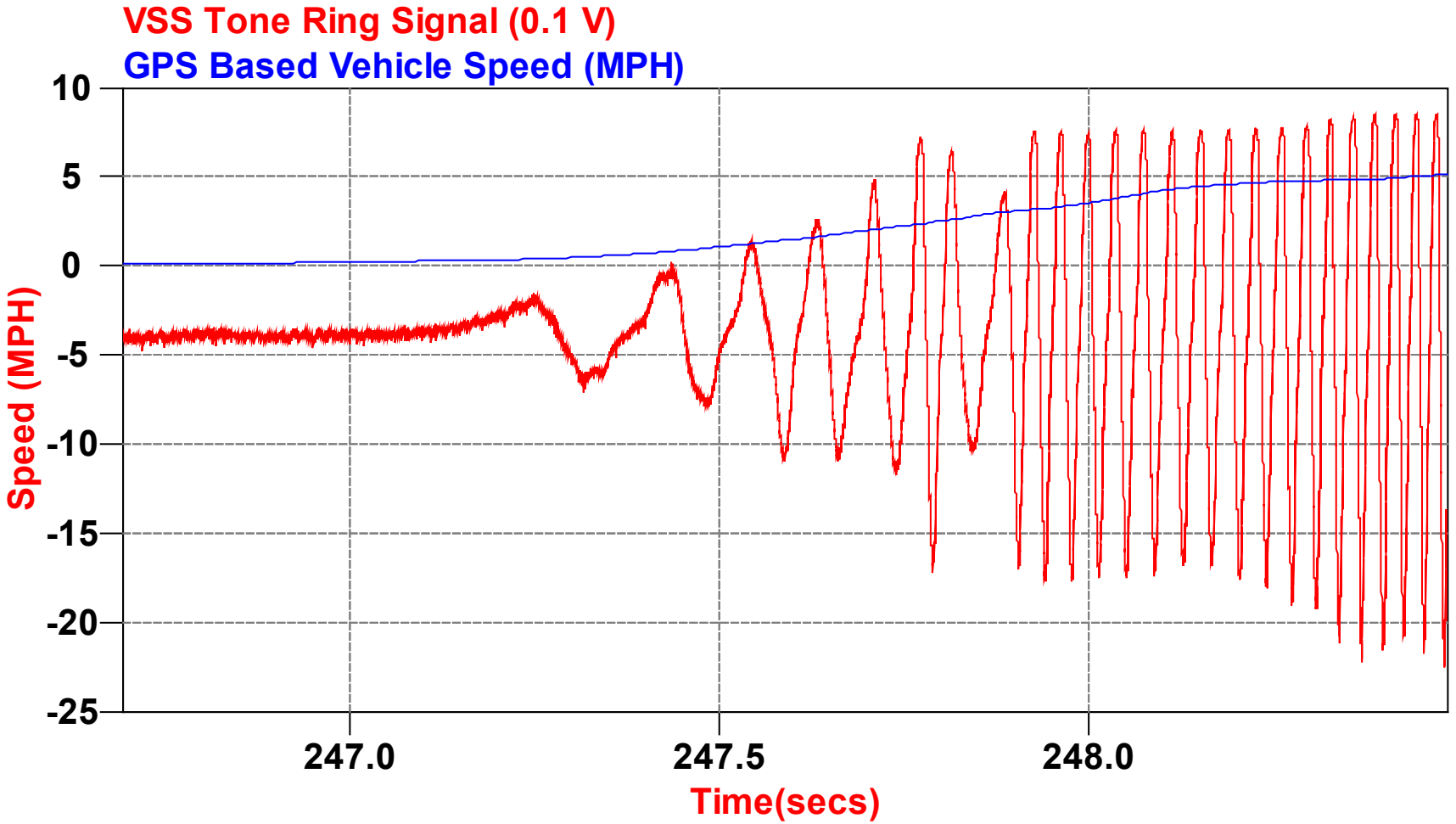
Example of Actual Speed Sensor Signal



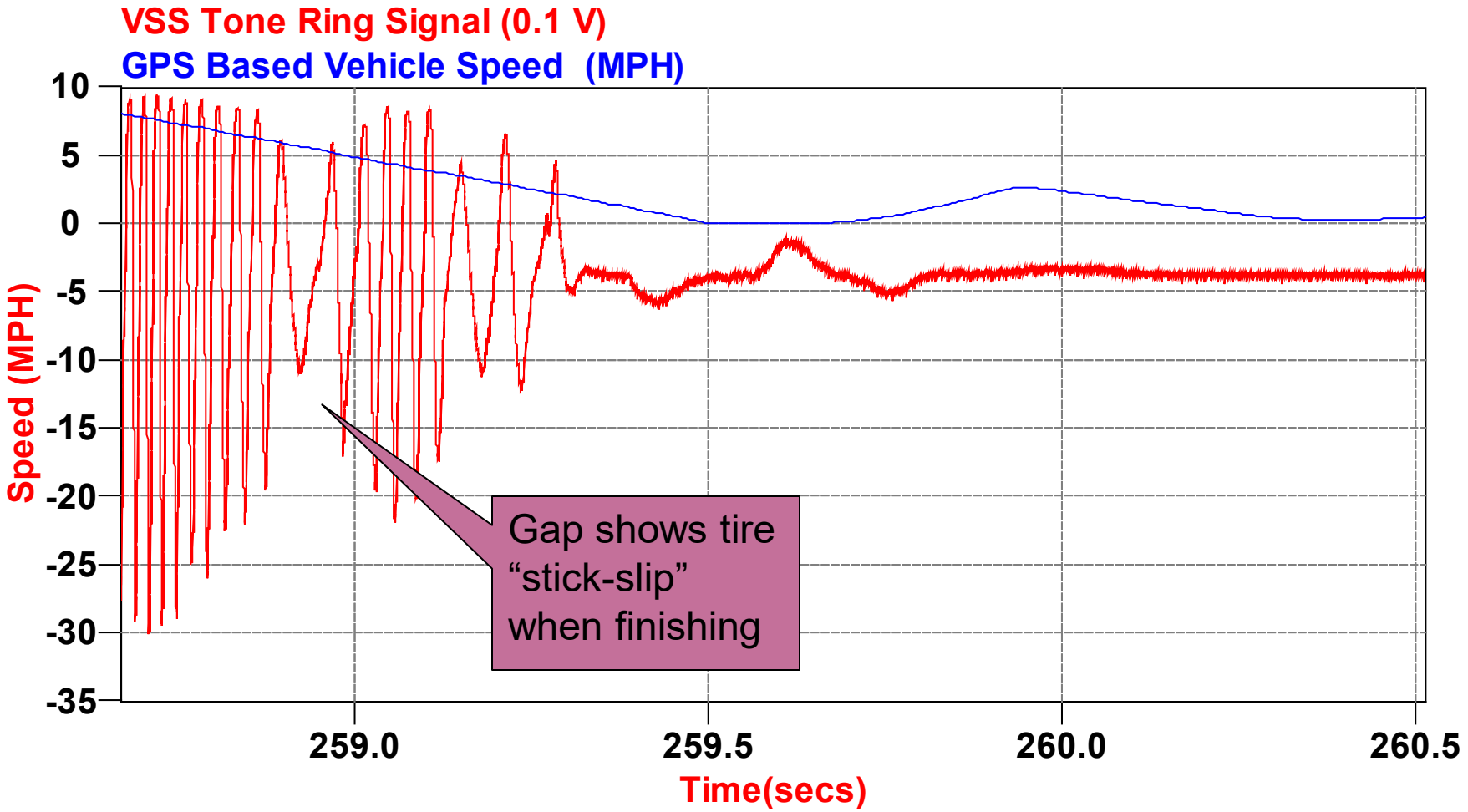
Example of Actual Speed Sensor Signal (Zoomed)



Example of Actual Speed Sensor Signal (Starting)



Example of Actual Speed Sensor Signal (Stopping)



Speed Sensing Observations

- Amplitude of the signal increases with speed.
- Frequency of the signal increases with speed.
- Peak to Peak may go from 10 mV to over 10 V.
- May not be referenced to common ground.

Pavement to EDR Data

Wheels Turn → VSS Signal Generated → **ECM Calculates Speed** → Data Transmitted on Network

Determining Speed

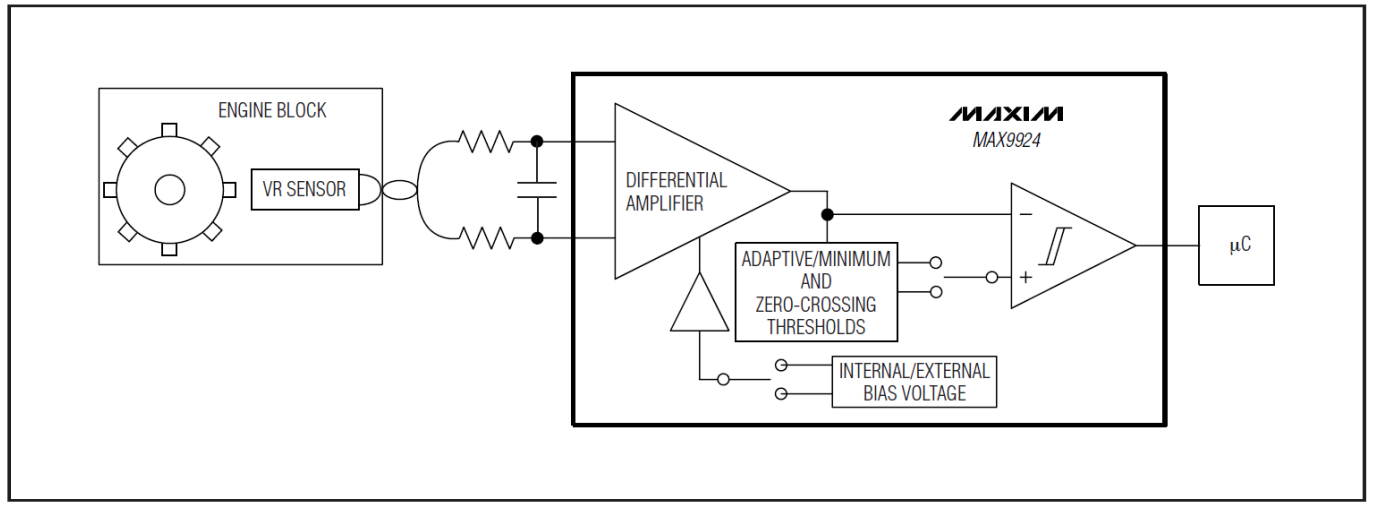
- A Signal Conditioning chip converts the analog signal into a pulse train.

Applications

Camshaft VRS Interfaces
Crankshaft VRS Interfaces
Vehicle Speed VRS Interfaces

µMAX is a registered trademark of Maxim Integrated Products, Inc.

Simplified Block Diagram



MAXIM Maxim Integrated Products 1

Determining Speed (Cont.)

- The ECM counts the number of pulses in a given unit of time, say 0.1 seconds.
- The number of pulses is converted to a distance using pulses per mile (ppm).
- Example: 60 pulses in 0.1 seconds.

$$\frac{60\ \text{pulses}}{0.1\ \text{sec}} \times \frac{\text{mile}}{29126\ \text{pulses}} \times \frac{3600\ \text{sec}}{1\ \text{hour}} = 74.1\ \text{mph}$$

Getting Pulses Per Mile

- Ask the Engine Control Module:
  - J1587 PID 228: Speed Sensor Calibration
  - Software output (DDDL shown here)

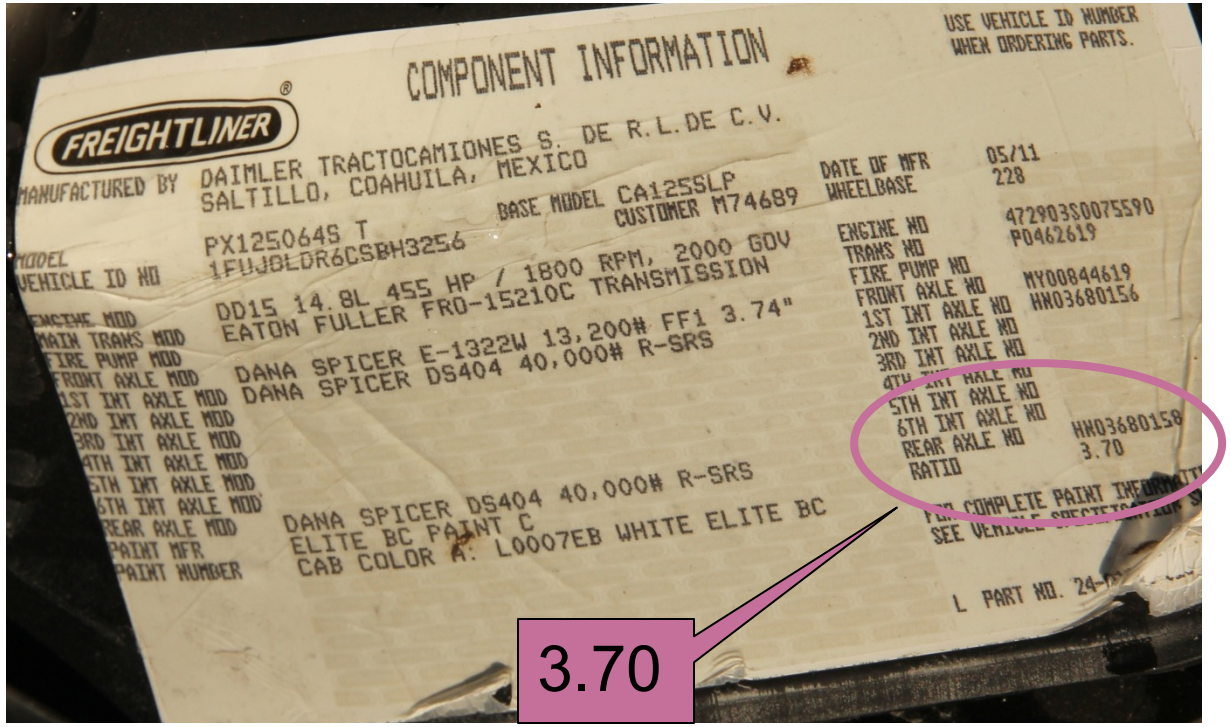
PGR008 Vehicle Speed Sensor

Anti Tamper	disabled
Axle Ratio	3.700
Number of Output Shaft Teeth	16
Second Highest Gear Ratio	1.000
Tire Revs per Unit Distance	492 1/mile
Top Gear Ratio	0.740
Two Spd Axle Second Axle Ratio	1.000
Vehicle Speed Sensor	magnetic pickup vehicle speed sensor
vss absolute diagnostic limit	99.92 mph
vss driving diagnostic limit	99.92 mph

  - 3.700 x 16 x 492 = 29126.4 ppm

Confirming Pulses Per Mile

- Physically Inspect the Vehicle
- Component Information (maybe in the glovebox)
- Tells what components to expect



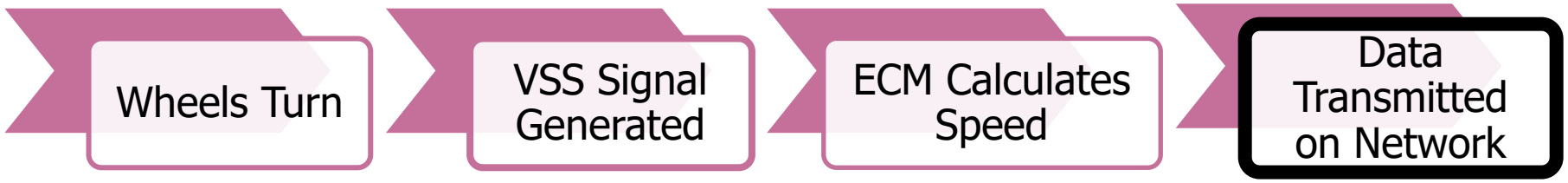
Axle Tag Shows Gear Ratio

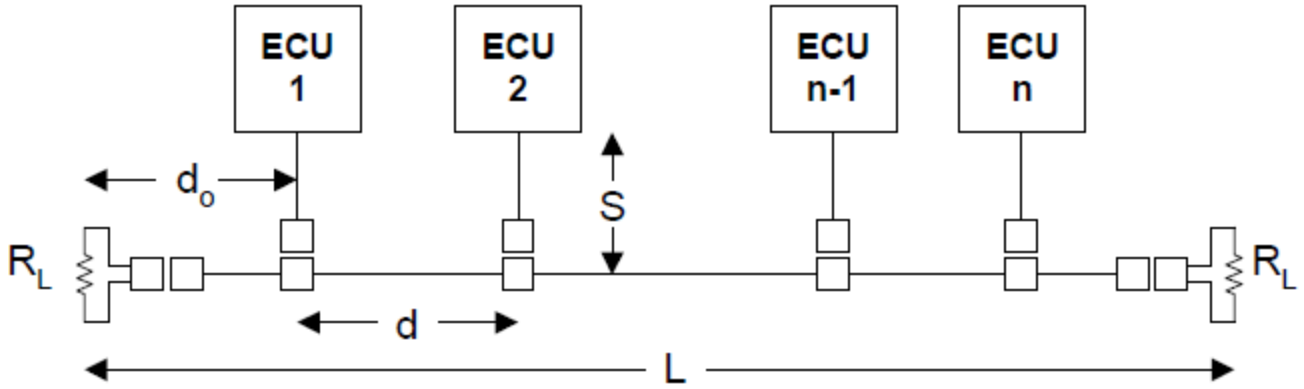
- Tag may not be readable.
- This one says RATIO 00370.
- Look for signs of repair.

Estimate Rolling Radius

- Method 1: Level and Tape Measure
  - Measure from center to ground of drive wheels
  - Typical ~19.5-21 inches
  - Circumference = 3.1415 x 2 x radius, which has units of inches per revolution
- Method 2: Mark the drive wheels and direct measure circumference
  - Put grease on the tread and measure the spacing of the grease mark on the pavement

Pavement to EDR Data





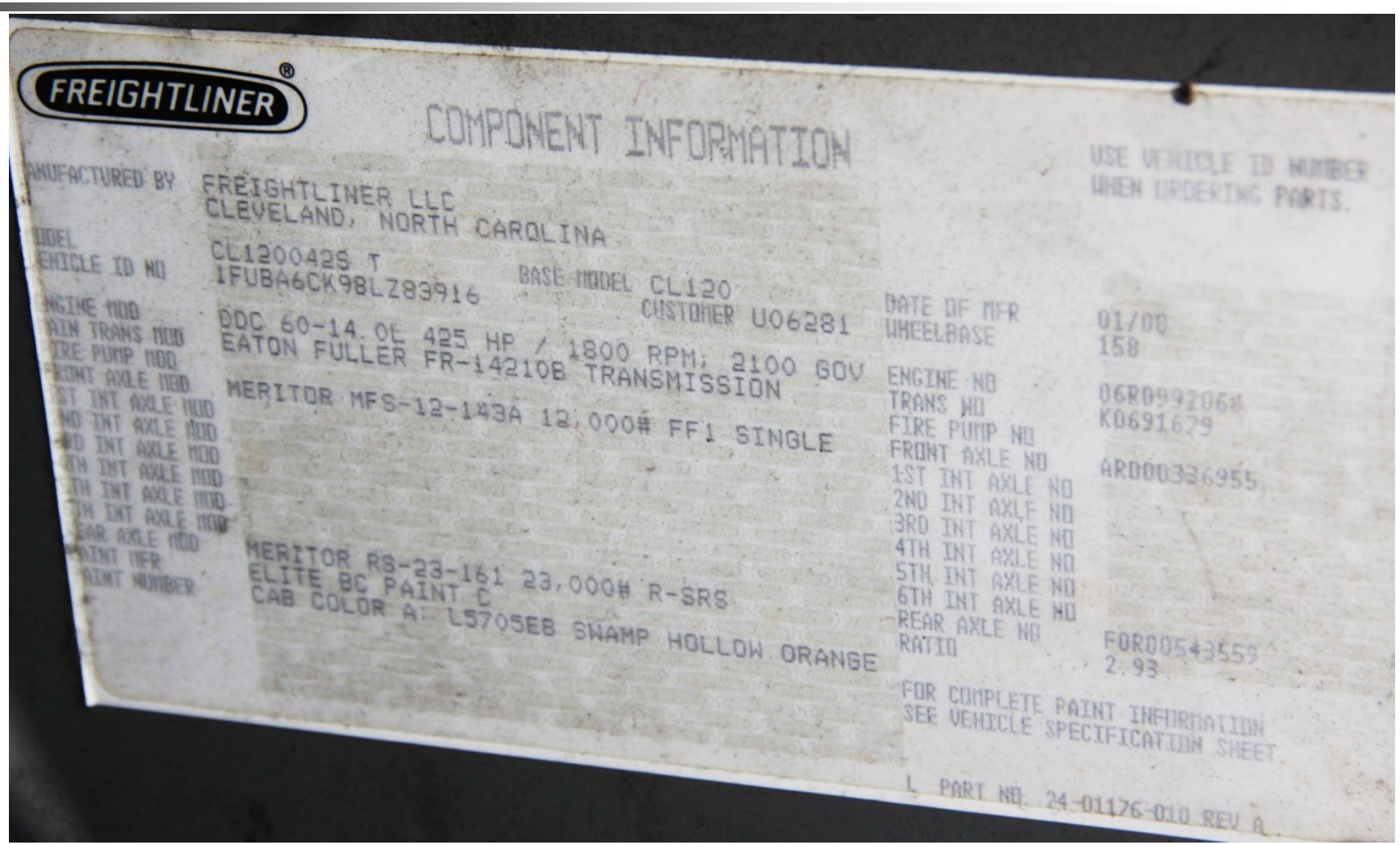
Data Acquisition and

APPLICATIONS TO HEAVY VEHICLES

Vehicle Description

- 2008 Freightliner
- Single Drive Axle
- DDEC VI equipped Detroit Diesel Series 60 Engine
- Eaton 10 Speed Manual
- 2.93:1 Rear Axle Ratio

Component Information



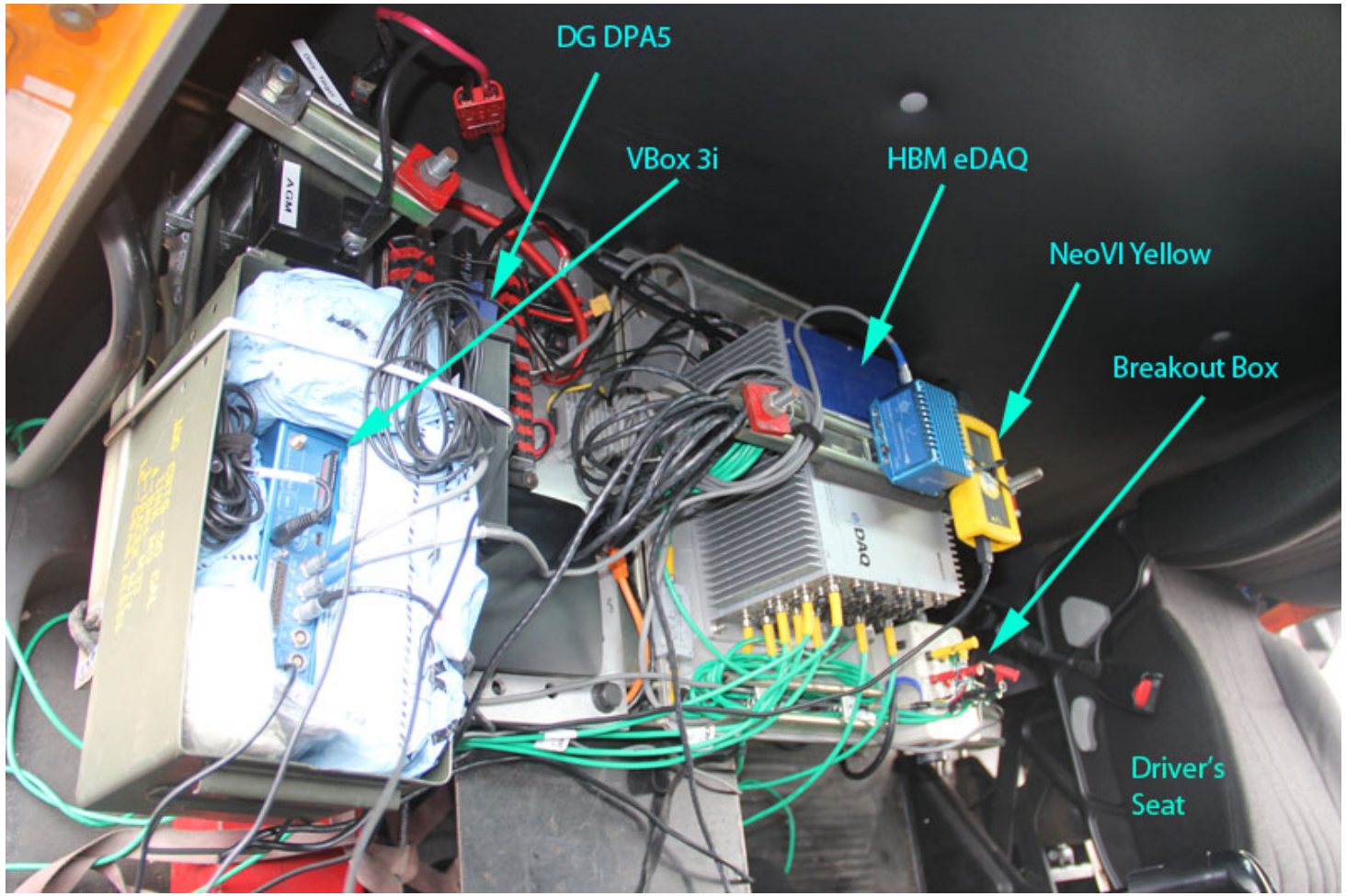
Procedure

- Training Facility Driving (i.e. Closed Course)
- Straight line runs with at least 2 hard brake events
- Multiple Configurations
  - Bobtail
  - Single Pup
  - Twin Pups
- Record while hitching and releasing pups

Correlated Data Gathering

- Simultaneously obtain
  - Tone Ring (VSS) Signals
  - J1939 Network Traffic (e.g. Wheel-based Vehicle Speed)
  - J1708 Network Traffic (e.g. Road Speed)
  - GPS Based Speeds (Vbox 3i and eGPS-200)
  - Tape Switch on Brake Pedal
  - Brake Chamber Pressures
- Perform multiple hard braking events
- Download HVEDR Data

Instrument Setup



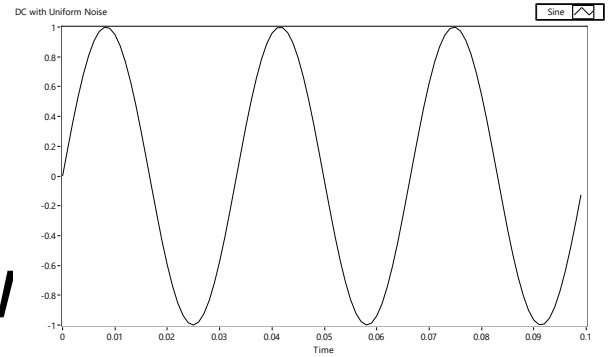
Instrument Setup (cont.)

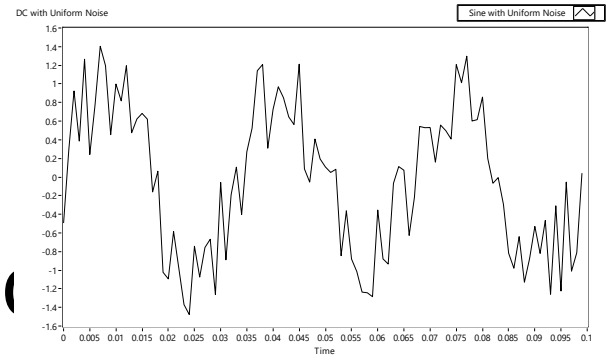
- Details on Instrumentation with links:

https://www.engr.colostate.edu/~jdaily/tucrrc/CorrelatedDDEC6DataSet.html

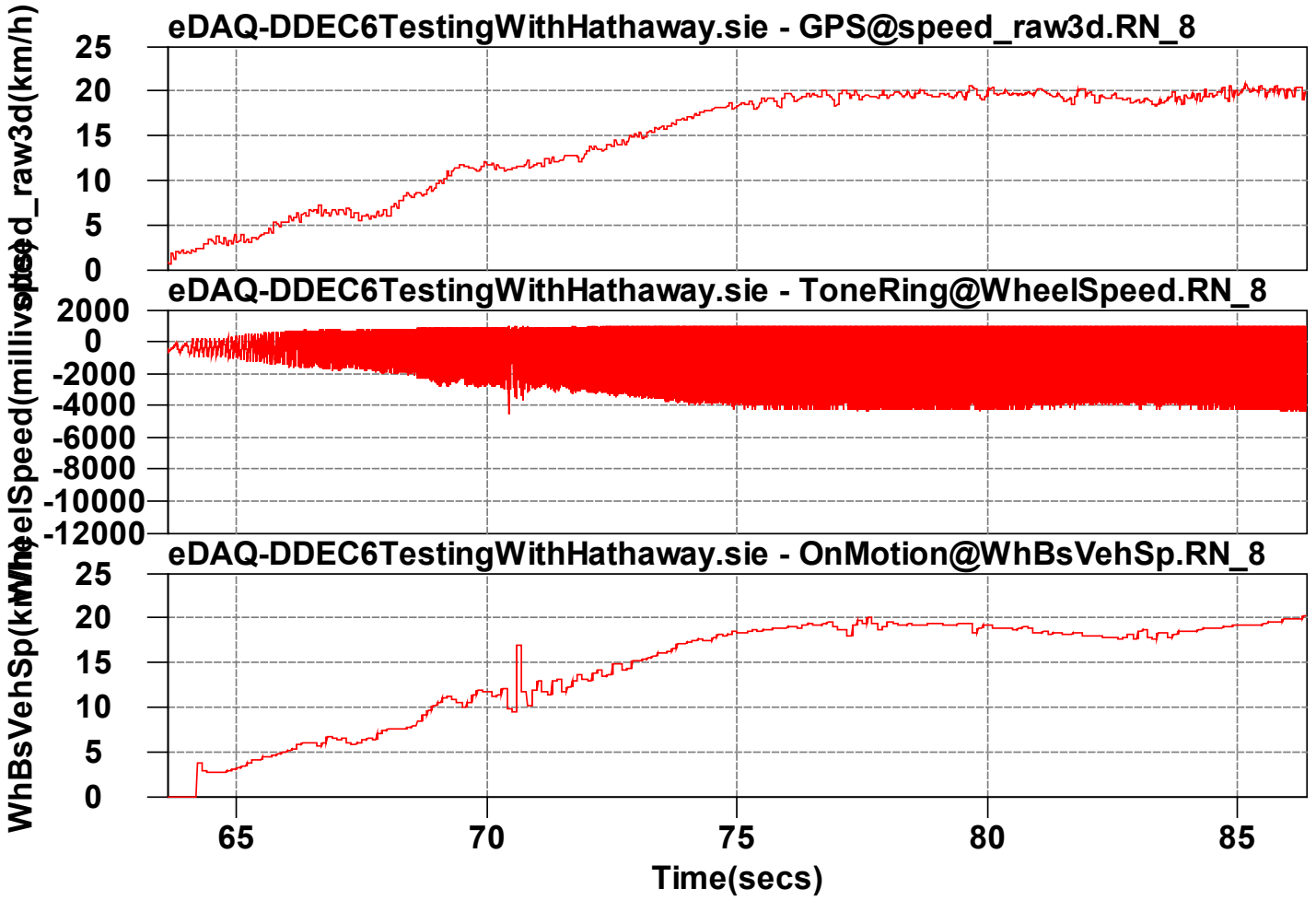
Speed Spikes and Noise

- Nice signals give predictable and reliable results.
  - Higher speeds
  - Lab Simulated Sine Waves
- Real Signals may not be nice at low
  - Compromised circuit
  - Drive train rattle
  - Vibration
- Longer sample times smooth out n



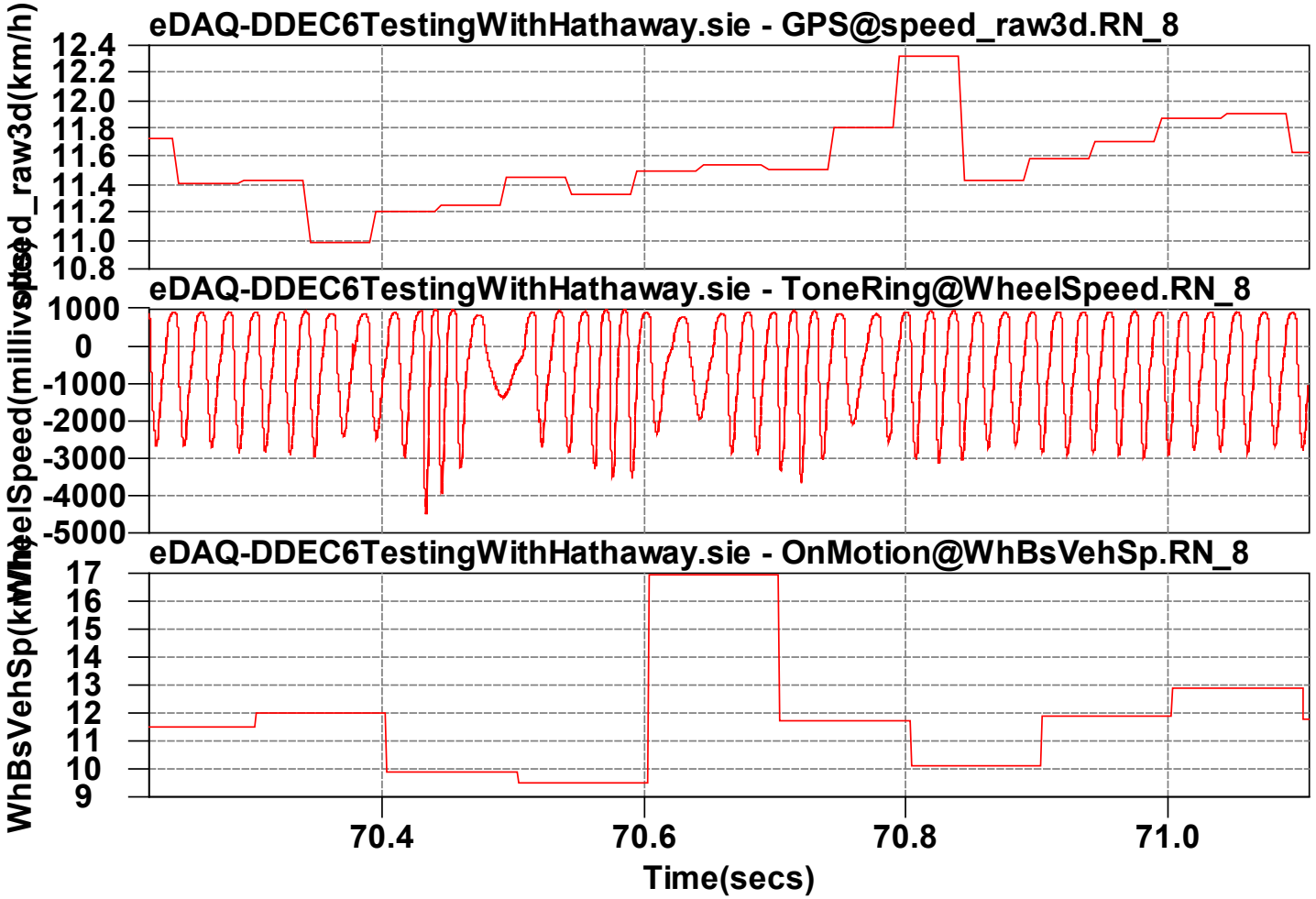


Speed Spikes at Shift Points



- External GPS
- Tone Ring Signal
- J1939 Speed

Speed Spikes at Shift Points

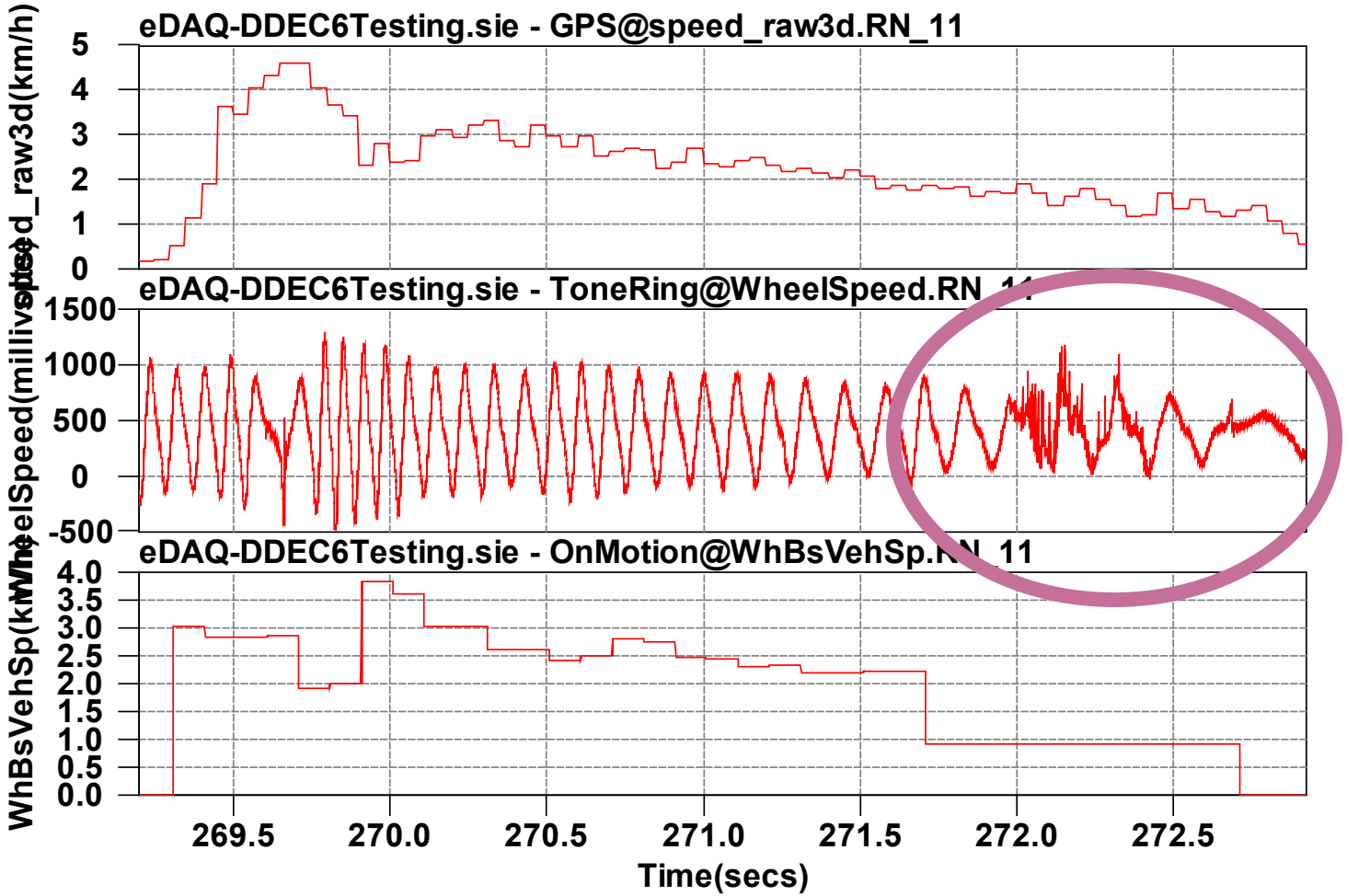


- External GPS
- Tone Ring Signal
- J1939 Speed

Signal Noise When Slow

- Some Event Records may show unphysical speed spikes (i.e. 0-55mph in 1 second).
- The speed sensing circuit automatically increases sensitivity with lower amplitudes
  - More susceptible to noise
- Can happen with impulses that cause drivetrain rattle

Tone Ring Noise From Trailer Connection

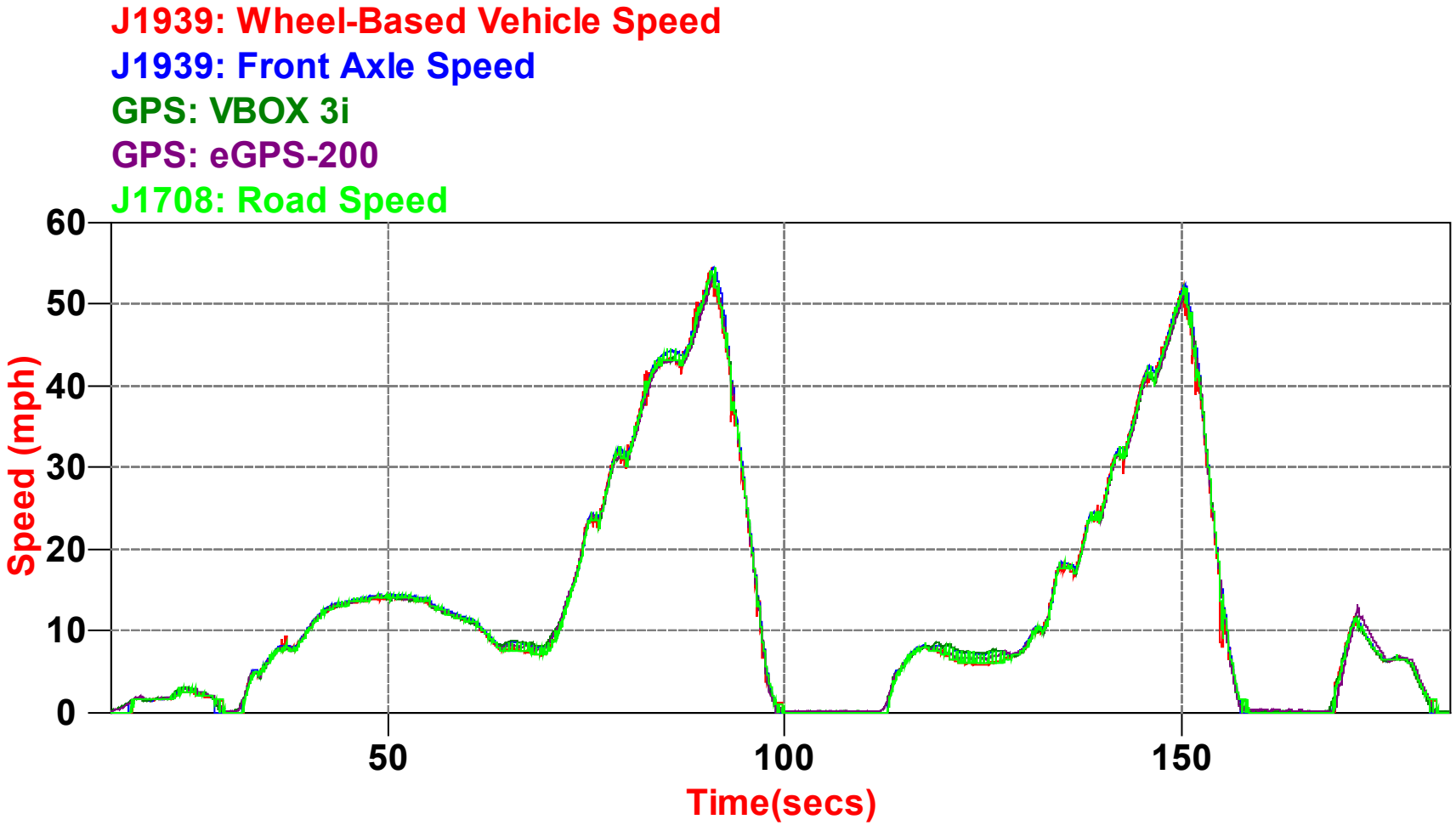


- External GPS
- Tone Ring Signal
- J1939 Speed

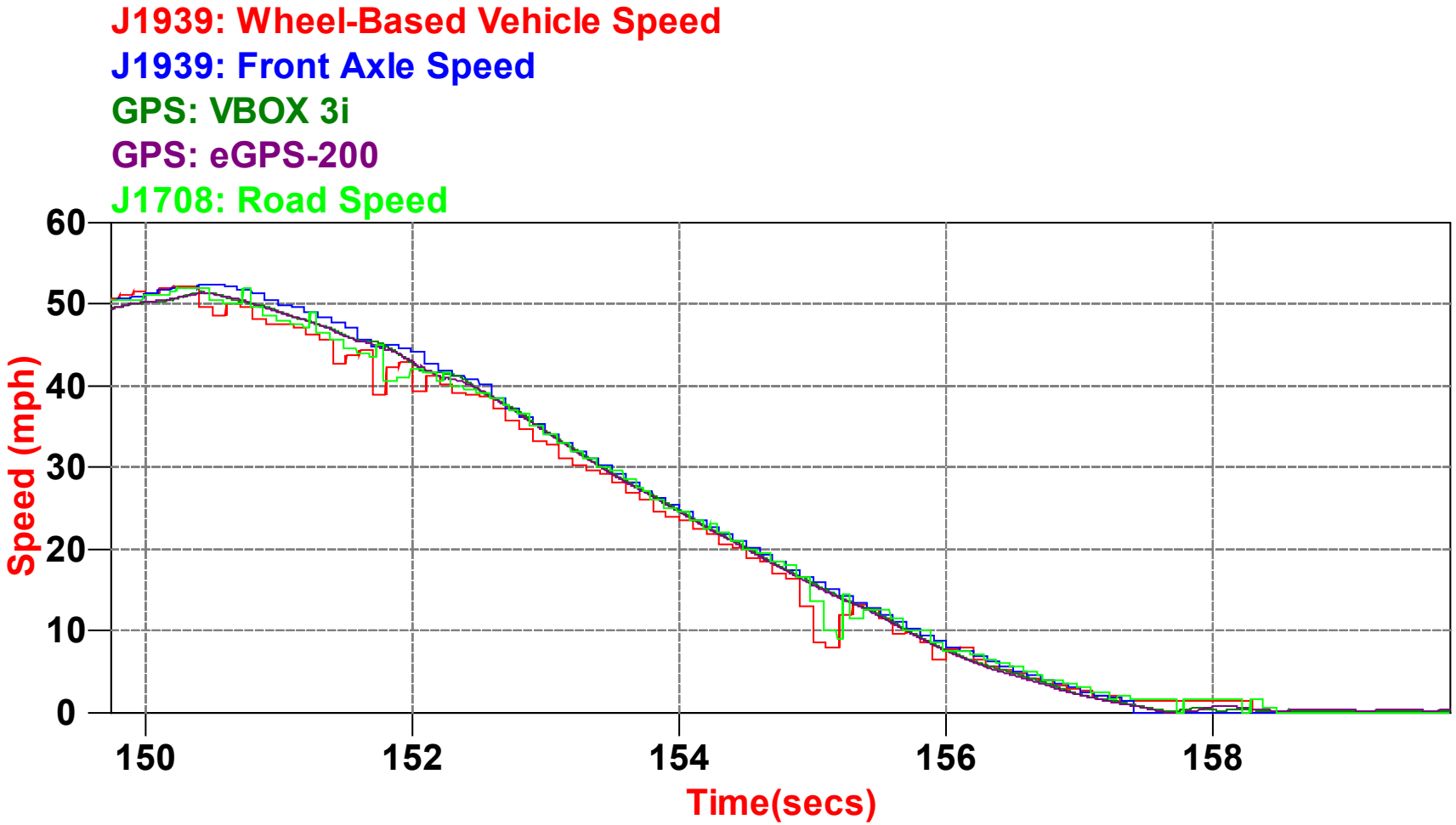
Speed Comparison

- eGPS-200 from eDAQ
- Vbox 3i GPS
- J1939 Network
  - Wheel-based Vehicle Speed (Tone Ring)
  - Front Axle Speed (Electronic Brake Controller)
- J1708 Network
  - Road Speed
- DDEC Reports

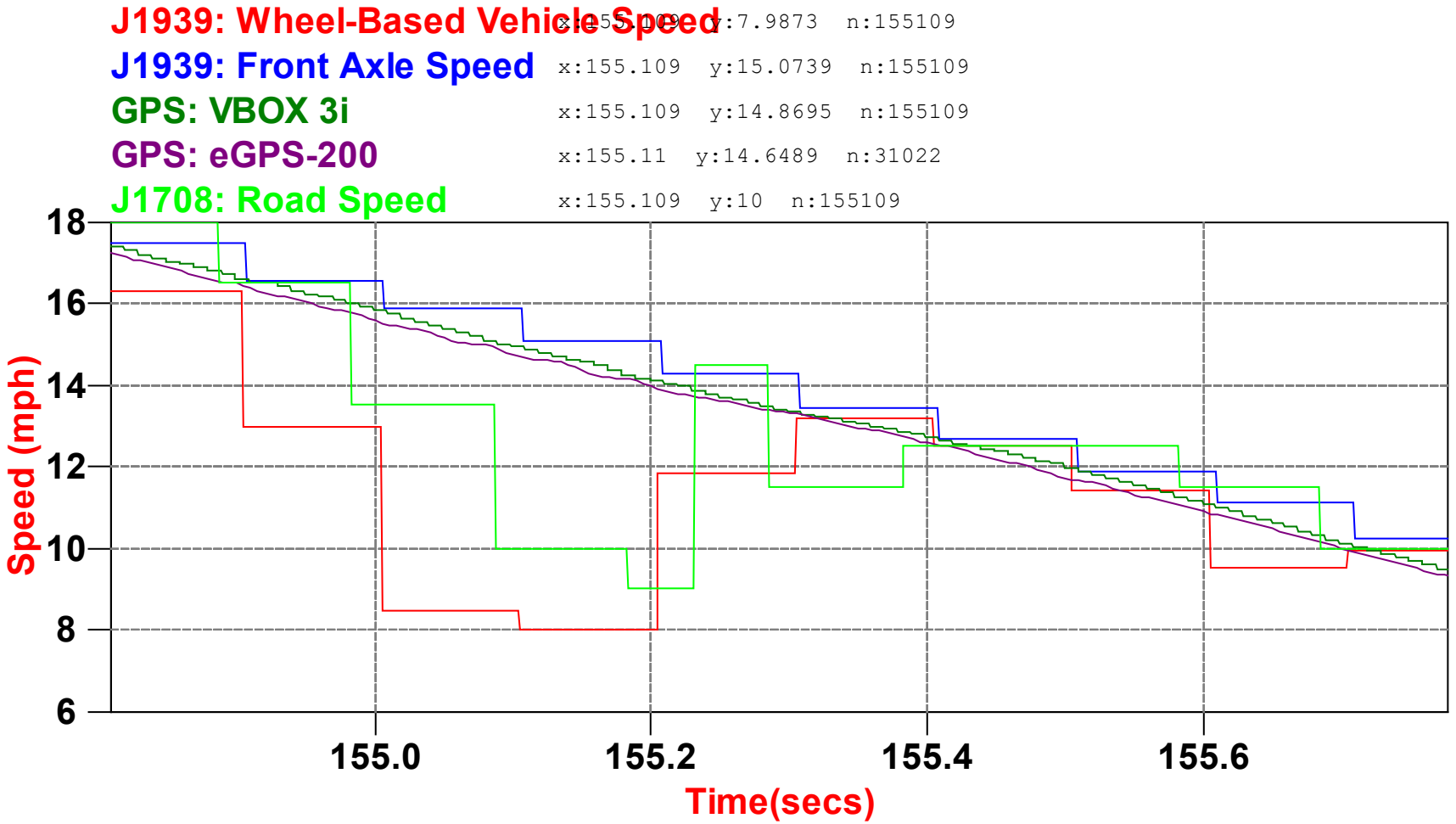
Speed Records



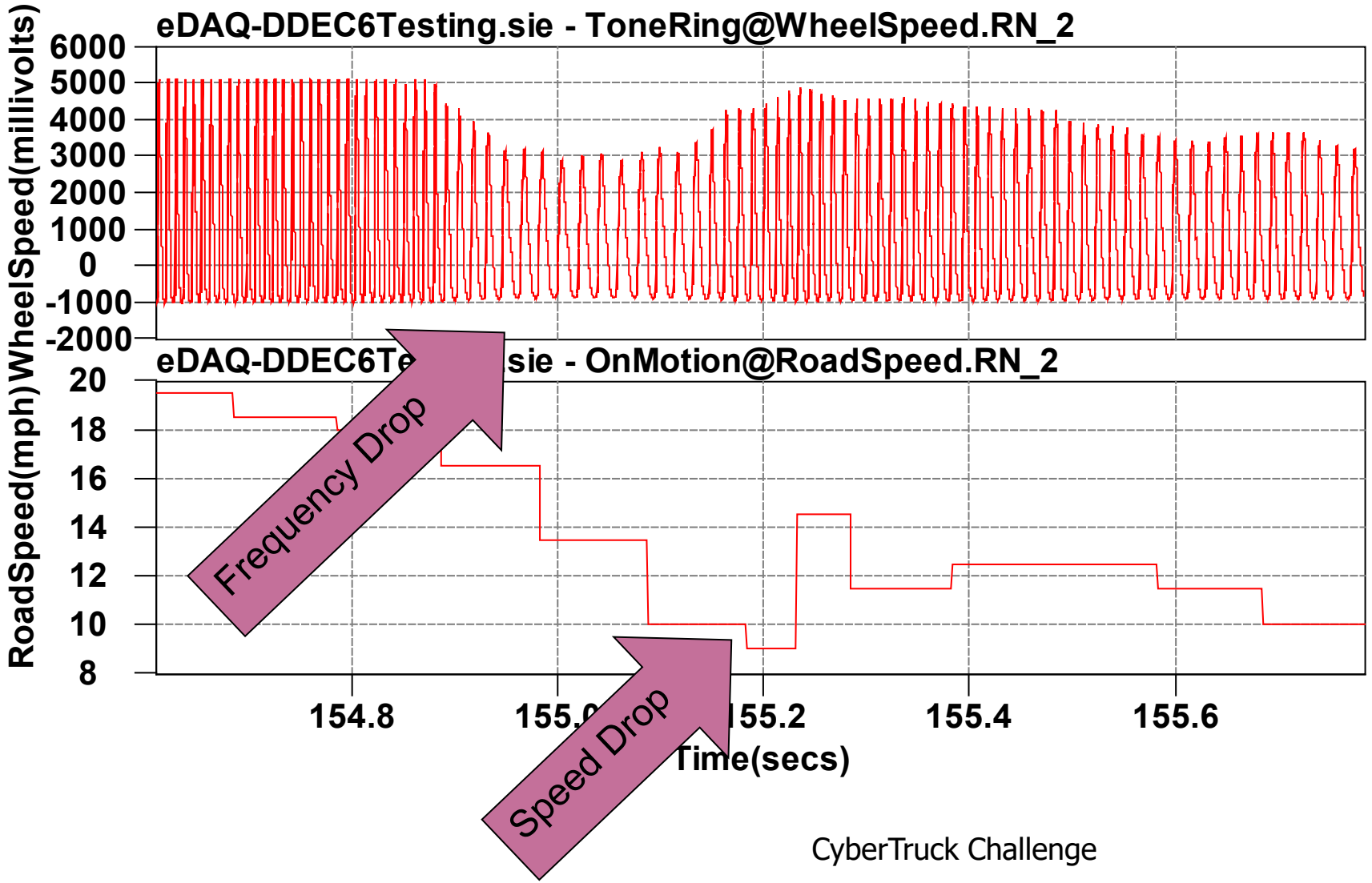
Speed Records Hard Brake



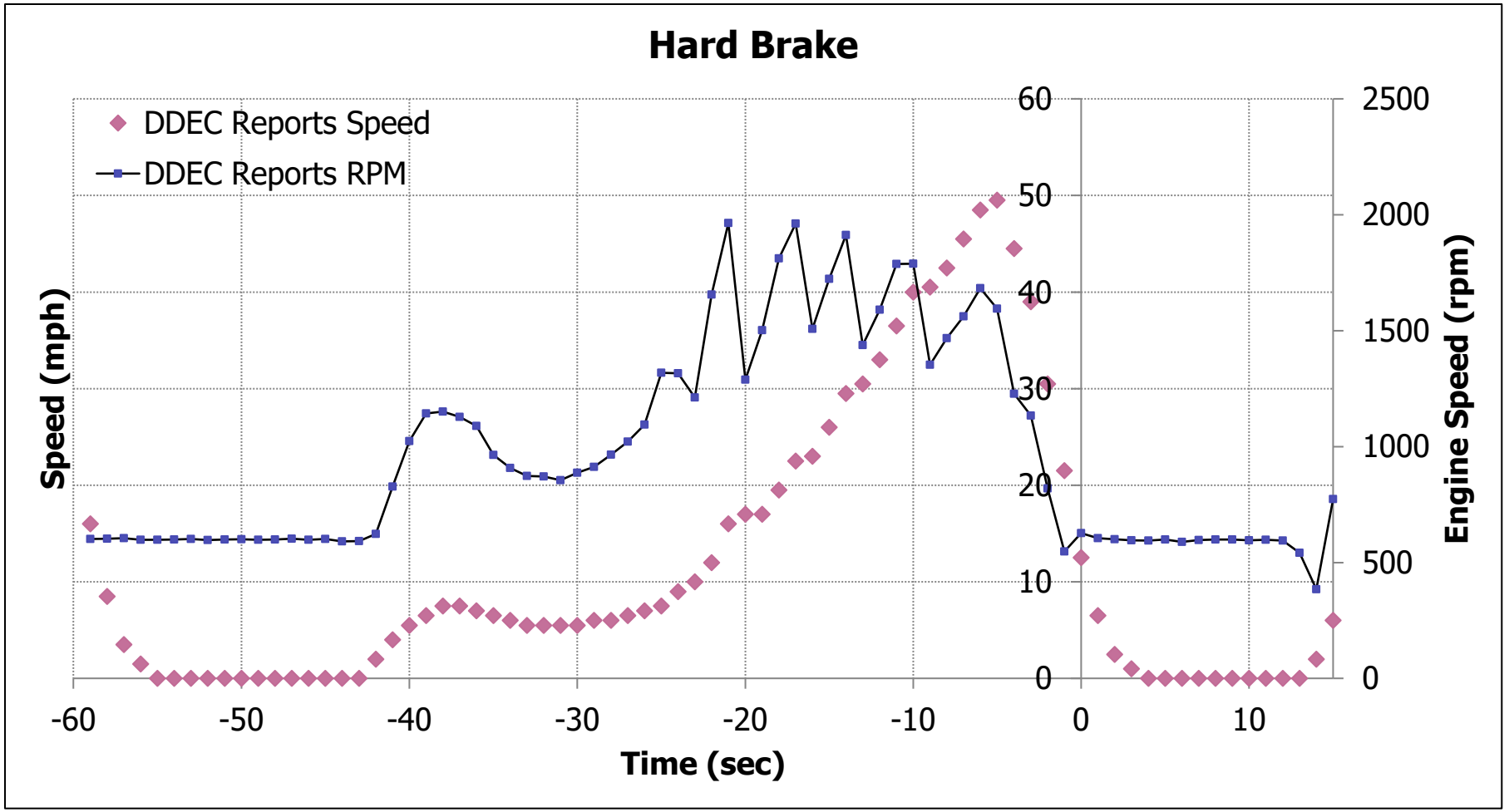
Zoom on Speed Feature



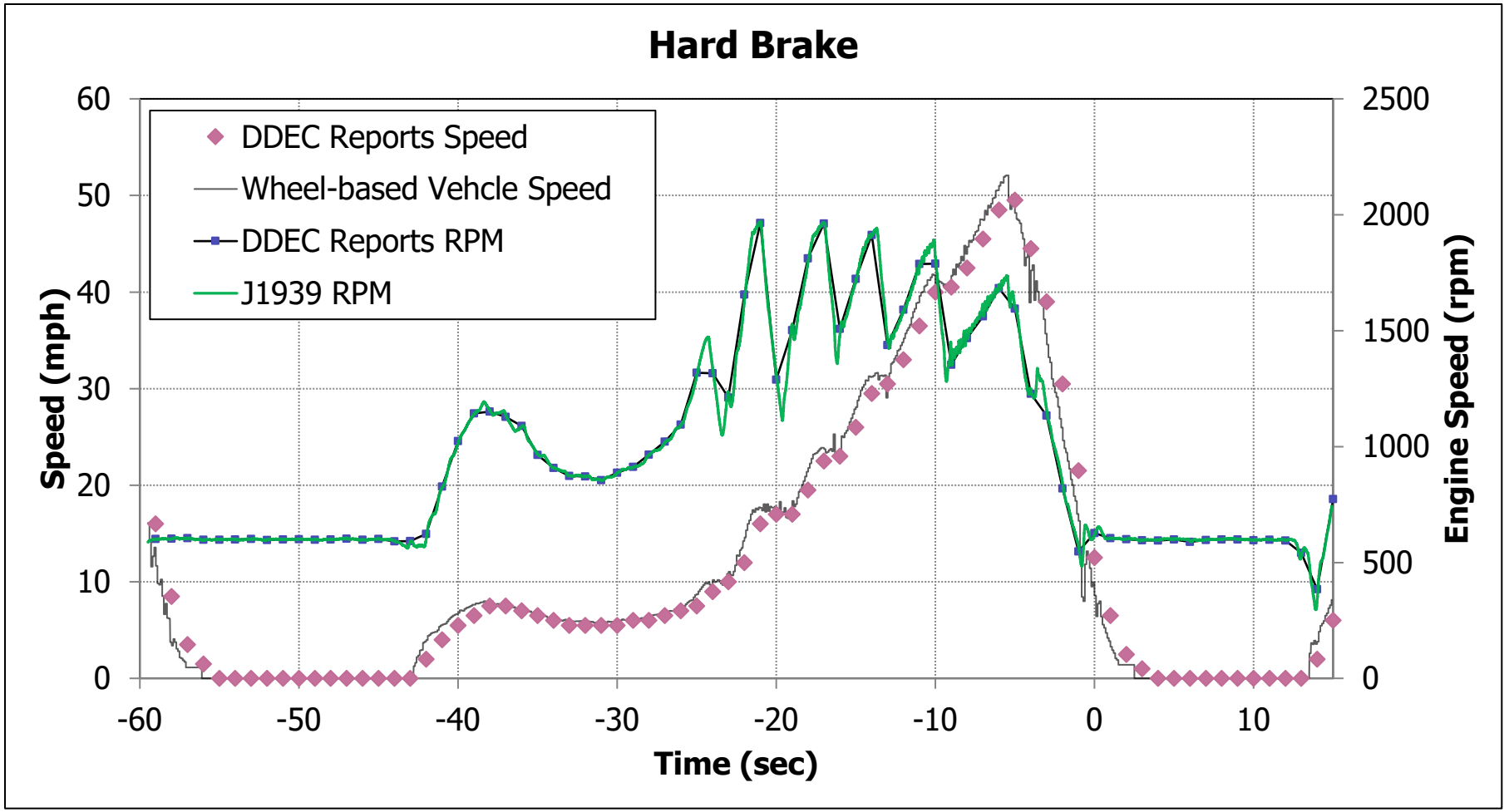
Compare Tone Ring Signal to ECM Calculated Speed



DDEC Reports Data



Merge DDEC Data with Network Data

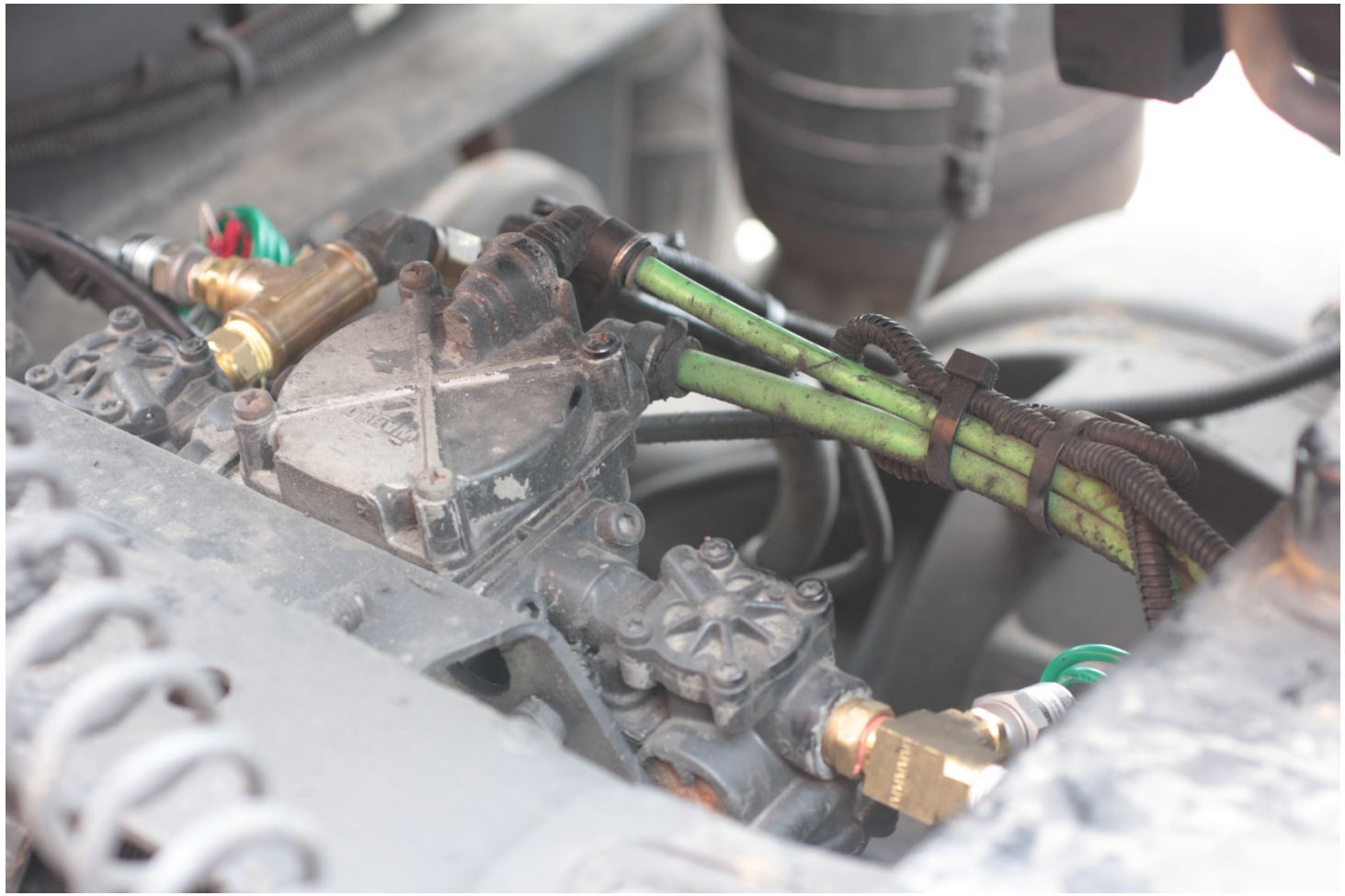


Speed Data Observations

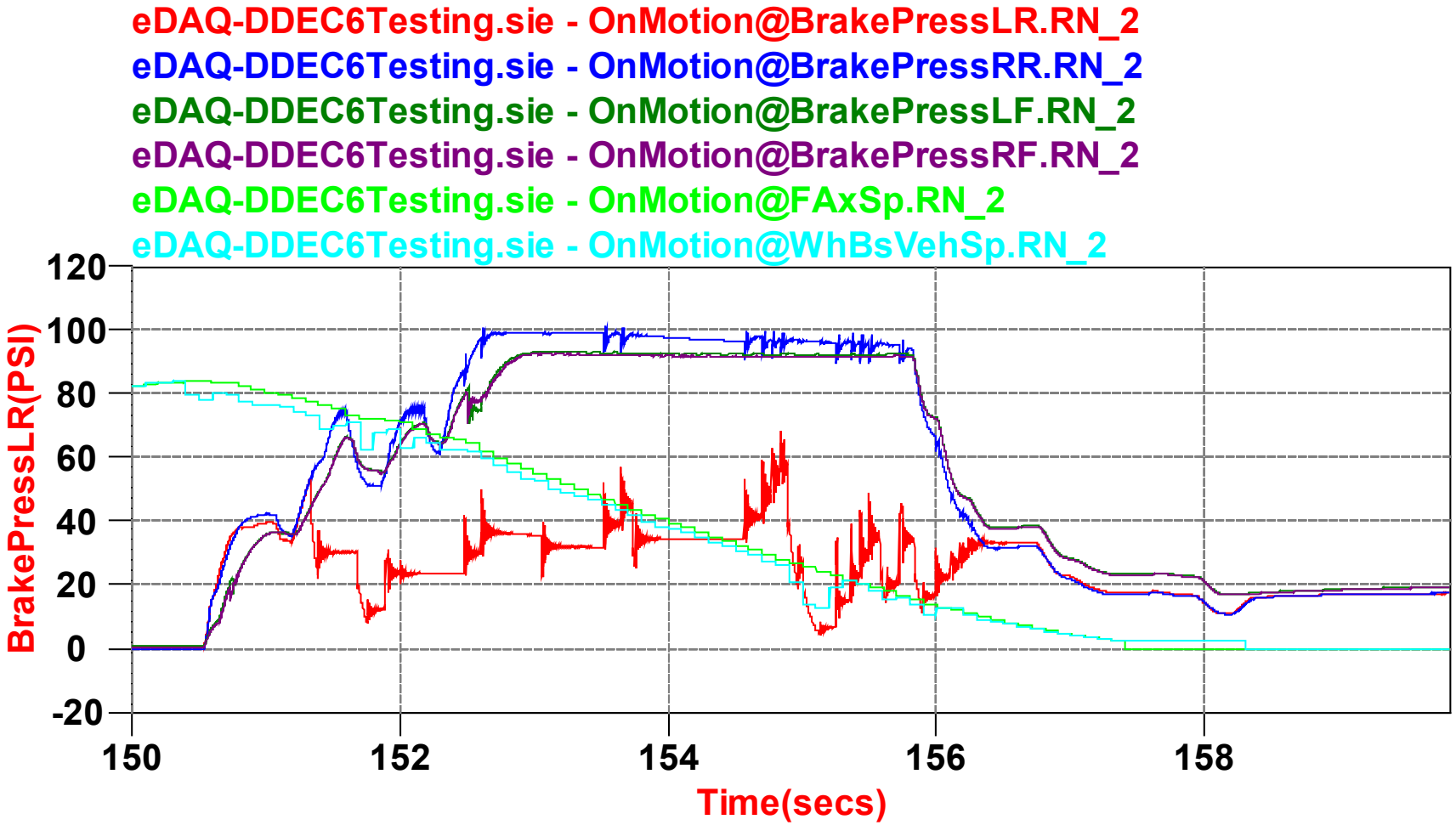
- Network speed data are about 0.1 second be hind tone ring signal.
- GPS units tracked each other around 0.2 mph difference
- Front Axle Speed over reported speed
  - Likely reduced rolling radius from treadware
  - From the Electronic Brake controller
- Road Speed (J1708) and Wheel-based Vehicle Speed (J1939) show drops in speed
  - Tire slip from braking
  - Used the same tone ring sensor

Air Pressure Transducer (Front Axle)

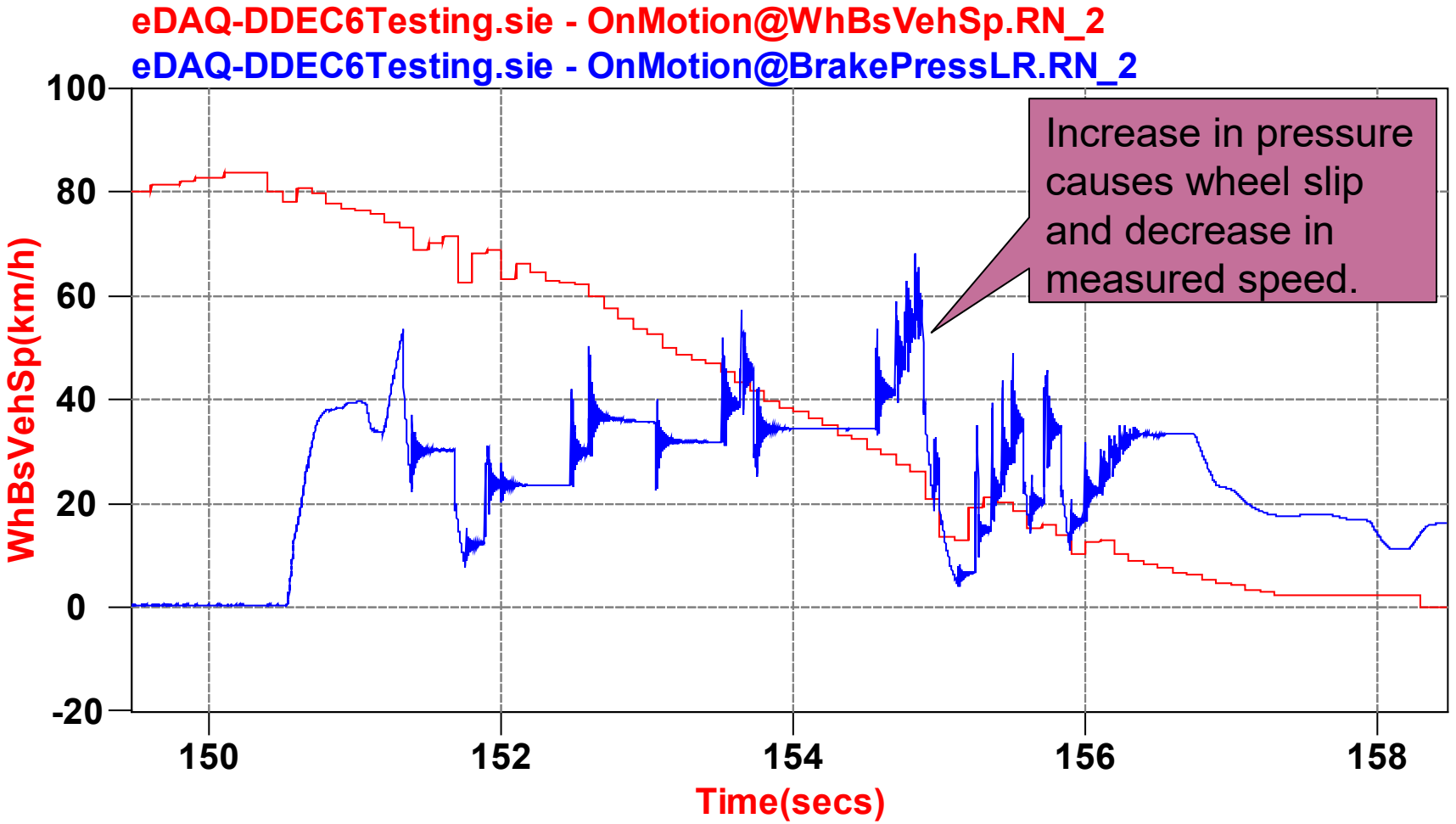
Air Pressure Transducer (Rear Axle)



Air Pressure for ABS Braking



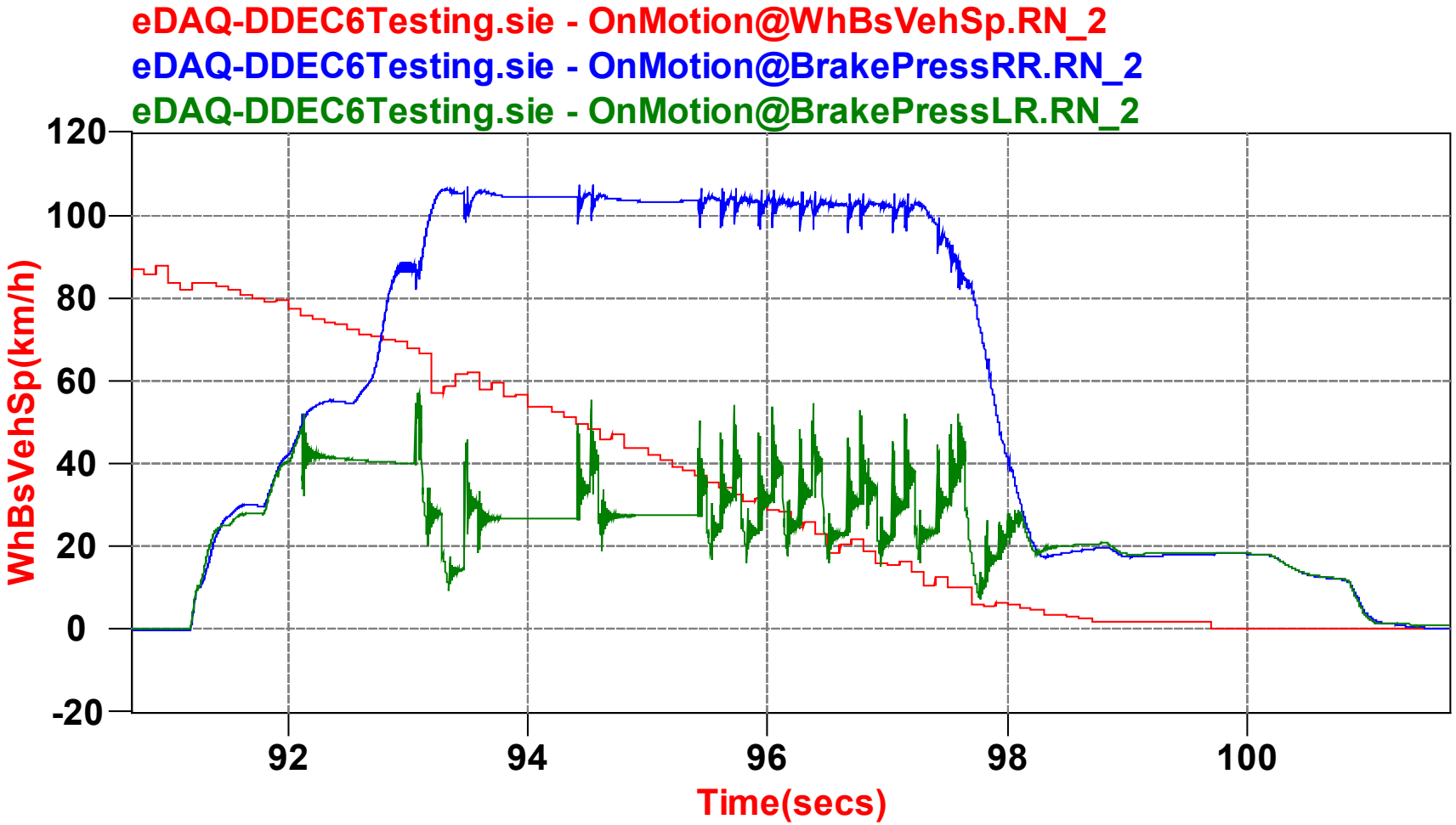
Left Rear Brake Pressure with Wheel-Based Speed



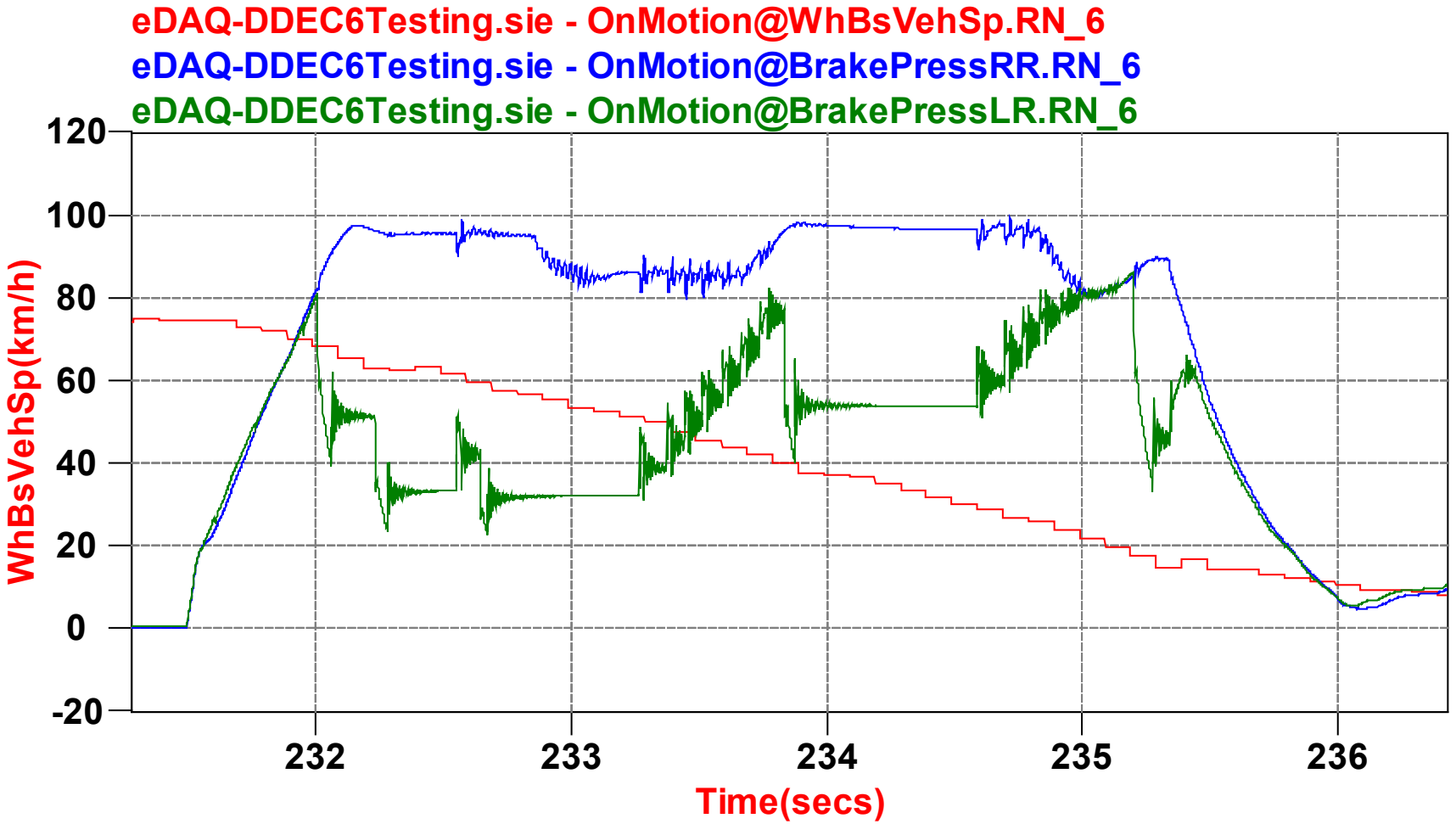
Bobtail Braking Results

- J1939 brake switch status lags tape switch by 0.07 seconds.
  - 15 psi builds in that time.
  - 40 psi (average operational pressure) lags by 0.25 psi
- Data show the pressure modulation from the ABS system.
- Front axle pressures tracked each other.
  - No modulation needed.

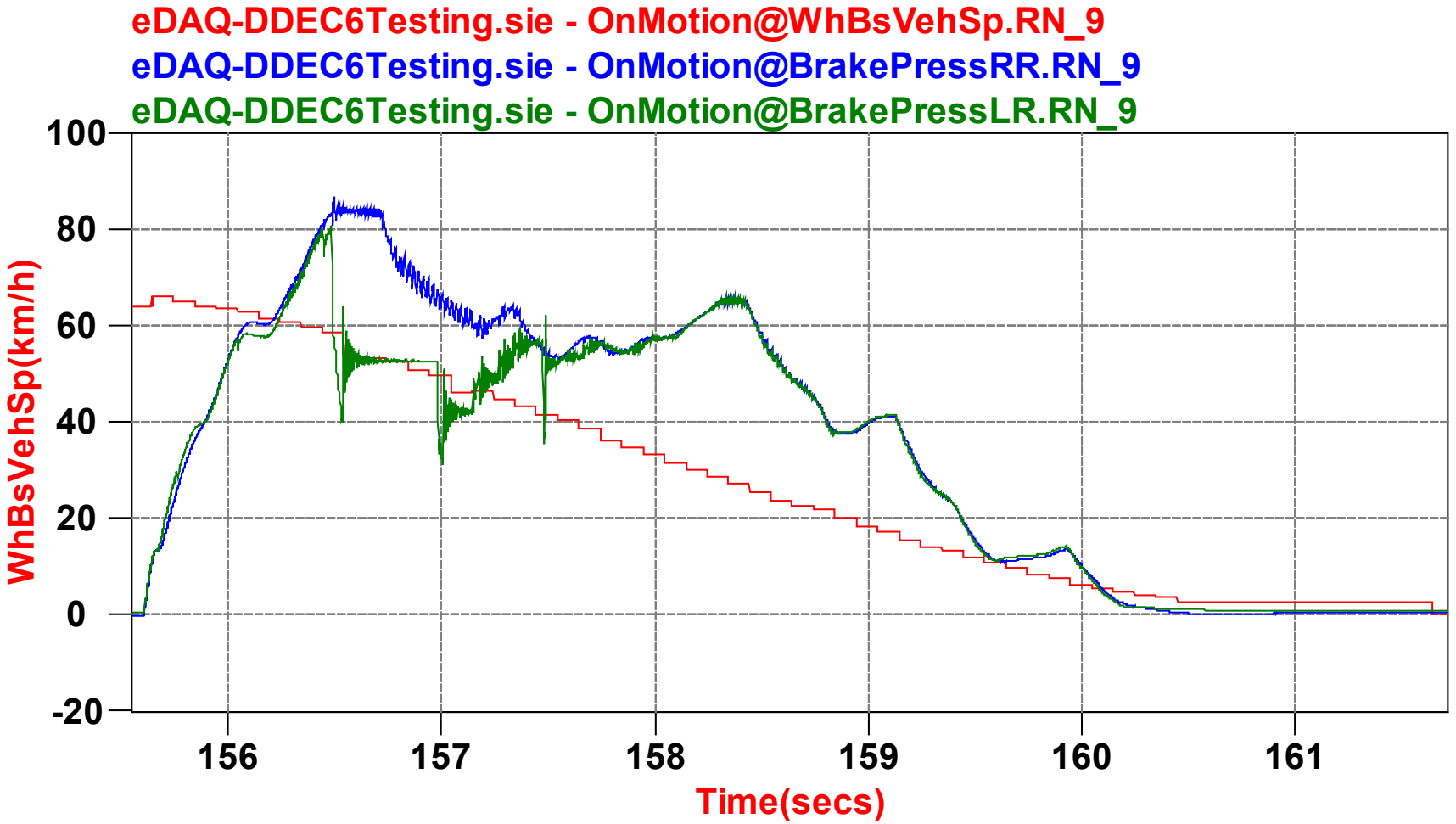
Rear Brake Pressures: Bobtail



Rear Brake Pressures: Single Pup



Rear Brake Pressures: Two Pups



Push Rod Stroke - OK

Push Rod Stroke – (Bad)

Remove Emergency Brake Line

This fell to the ground…

A Dime to Block the Line

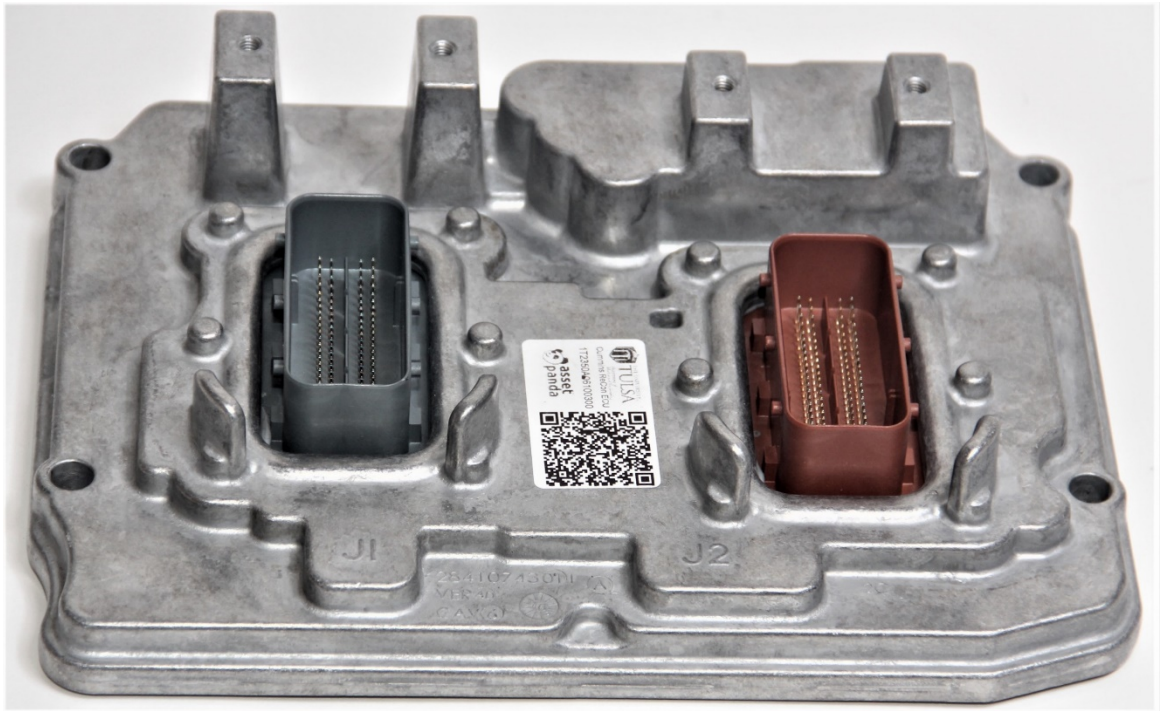
Observations

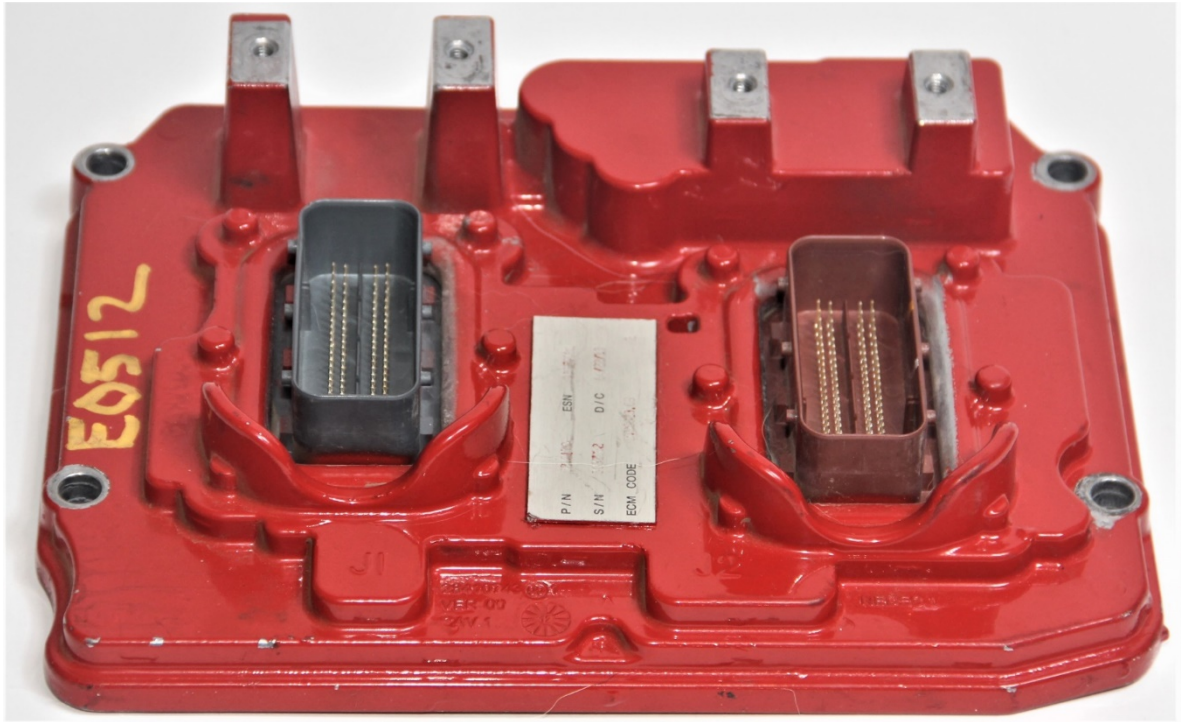
- When the dime was removed no pressure would hold when the parking brake was
- Dime prevented an air leak from a defective chamber
  - Service brake worked to depress the spring to release the brake
- Pressures were high/normal in the brake line
  - No Pressure modulation since no wheel slip.
- Push rod stroke was almost double on the defective brake
- No pushrod stroke when parking brake was set

When something goes wrong, we need to know about it.

HEAVY VEHICLE DIAGNOSTICS

Cummins PowerSpec and Insite





Cummins

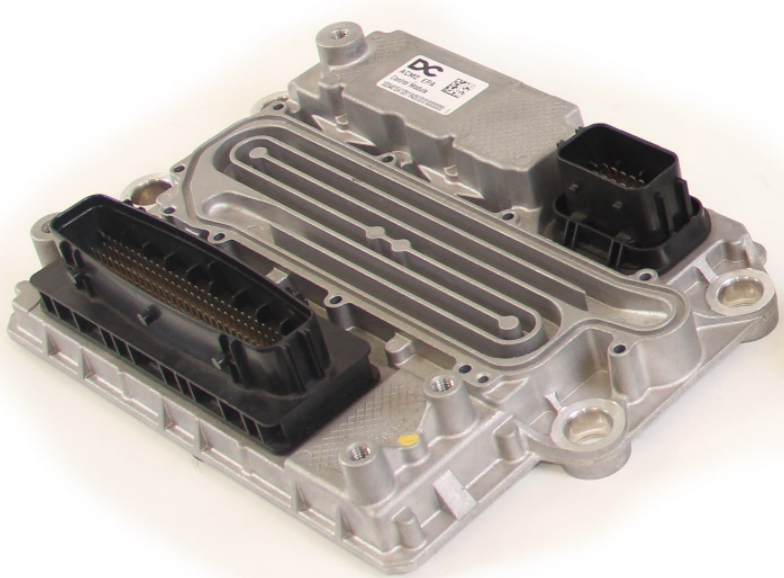
PowerSpec

- Sudden Decel Data
- Save directly to PDF
- Attribution is through Engine Hours and Mileage
- Free (with registration)

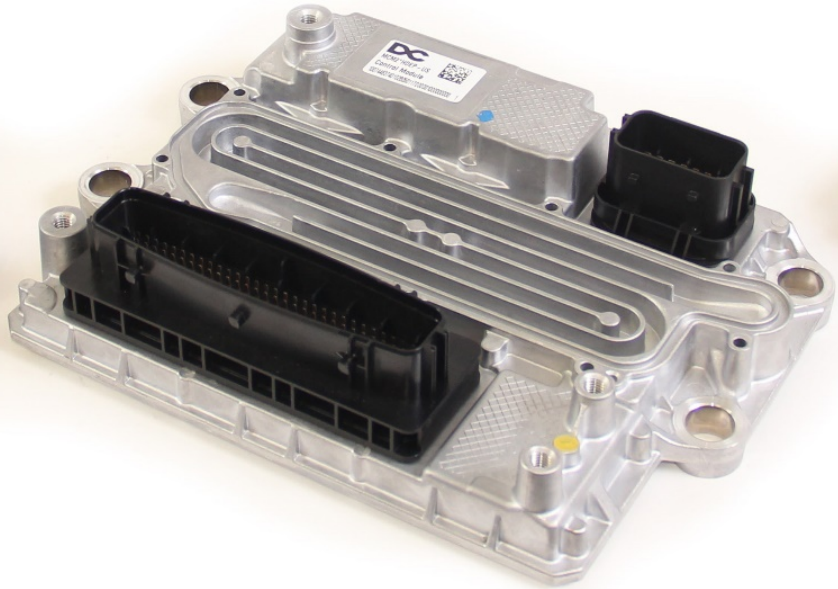
Insite

- Fault Code Freeze Frames
- Fault Schematics
- Audit Logs
- Produces a “Work Order” image
- Reflash firmware
- Subscription

Detroit Diesel Electronic Controls (DDEC)



Aftertreatment Control Module (ACM)



Motor Control Module (MCM)

Common Powertrain Controller (CPC)

Detroit Diesel Software

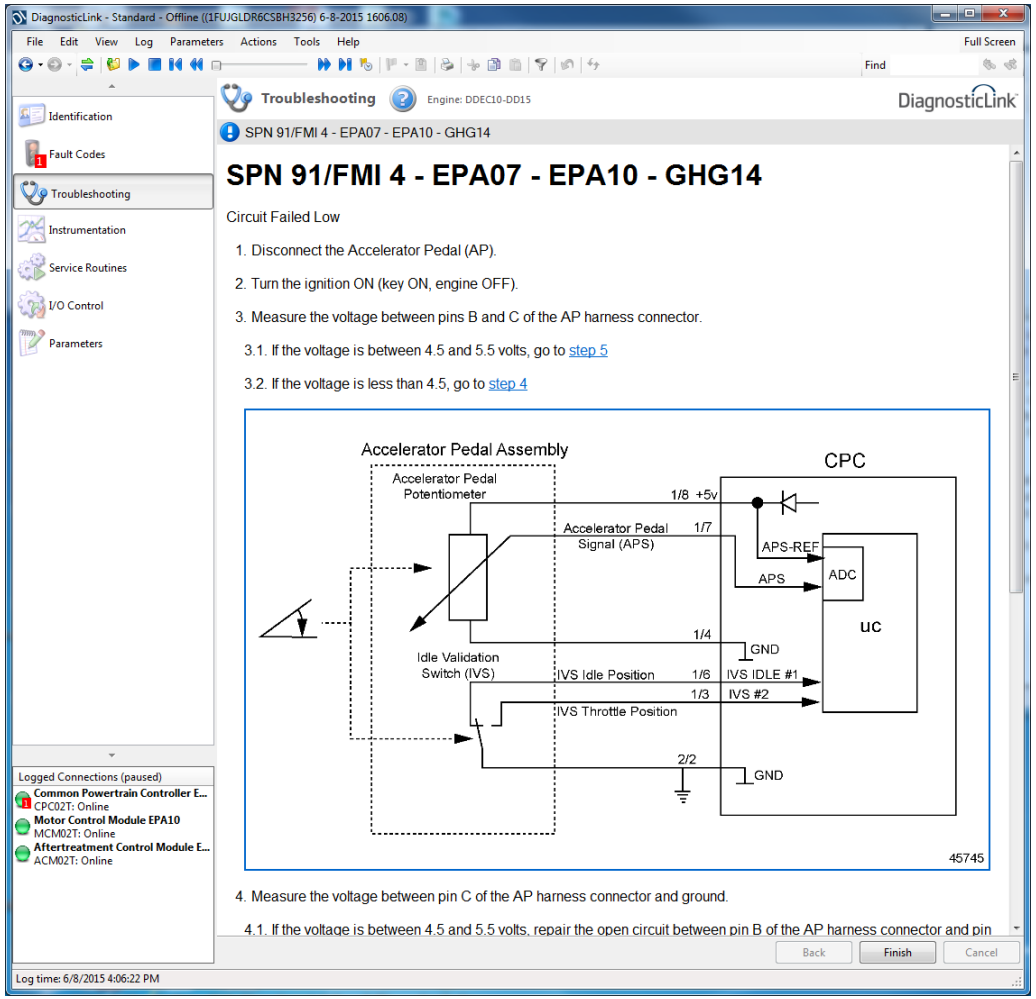
DDEC Reports

- Incident Data
- .XTR files
- Fleet Management
- Free

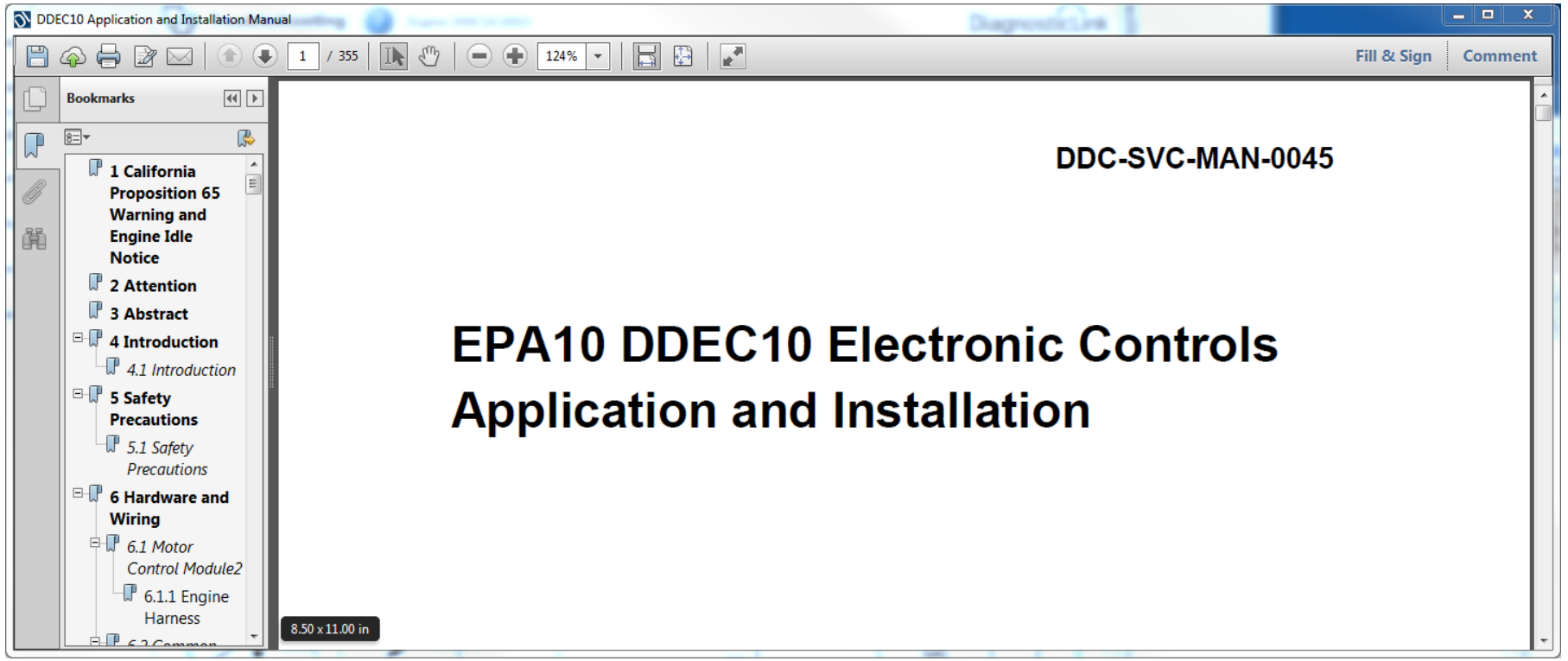
Diagnostic Link (DDDL)

- Fault Code Data
- Schematics
- Audit Logs
- Session Log Files
- Turn on DDEC Reports Data Pages for New Cascadia
- Subscription

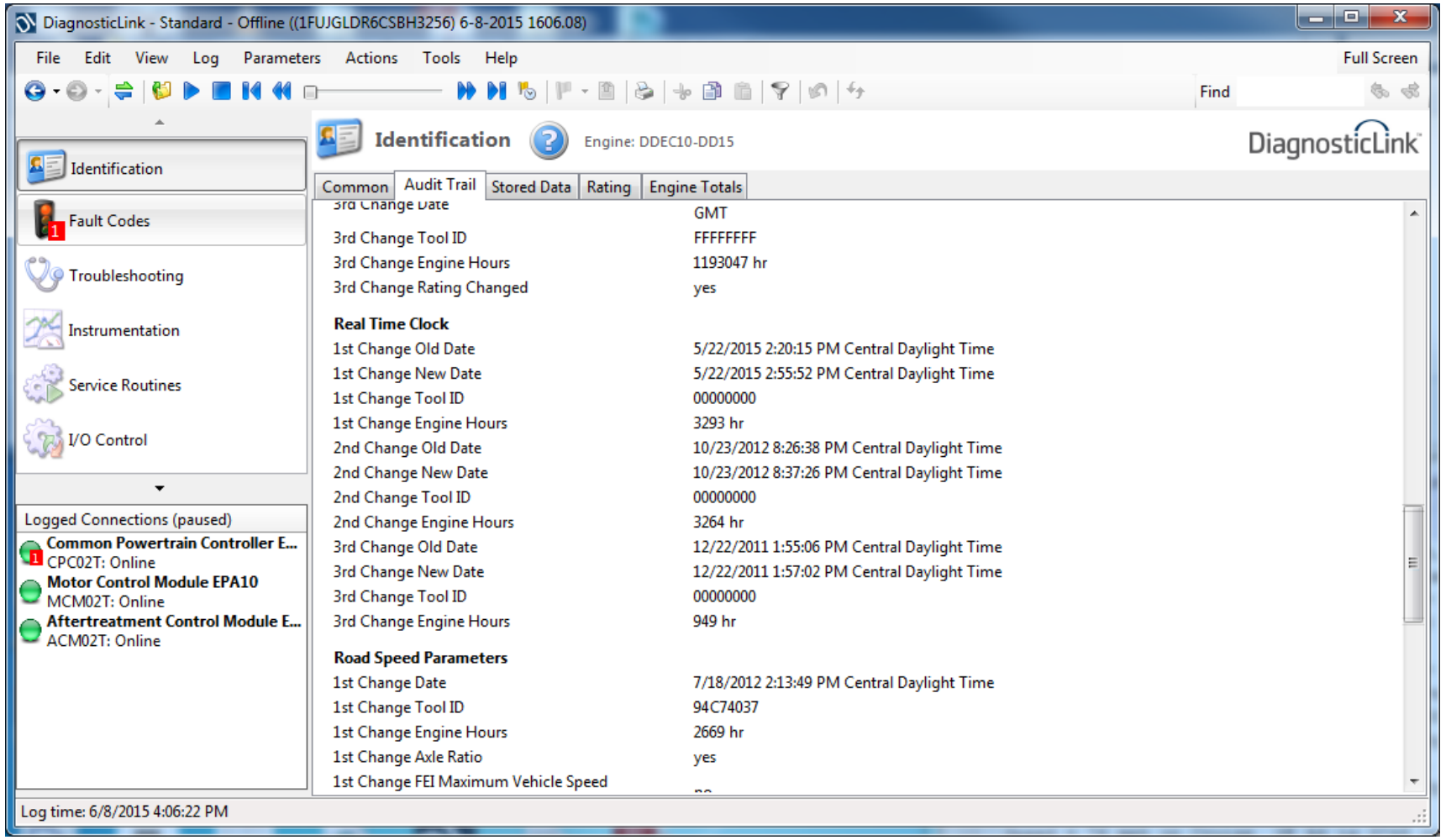
Fault Code Schematics in DDDL



Service Manuals

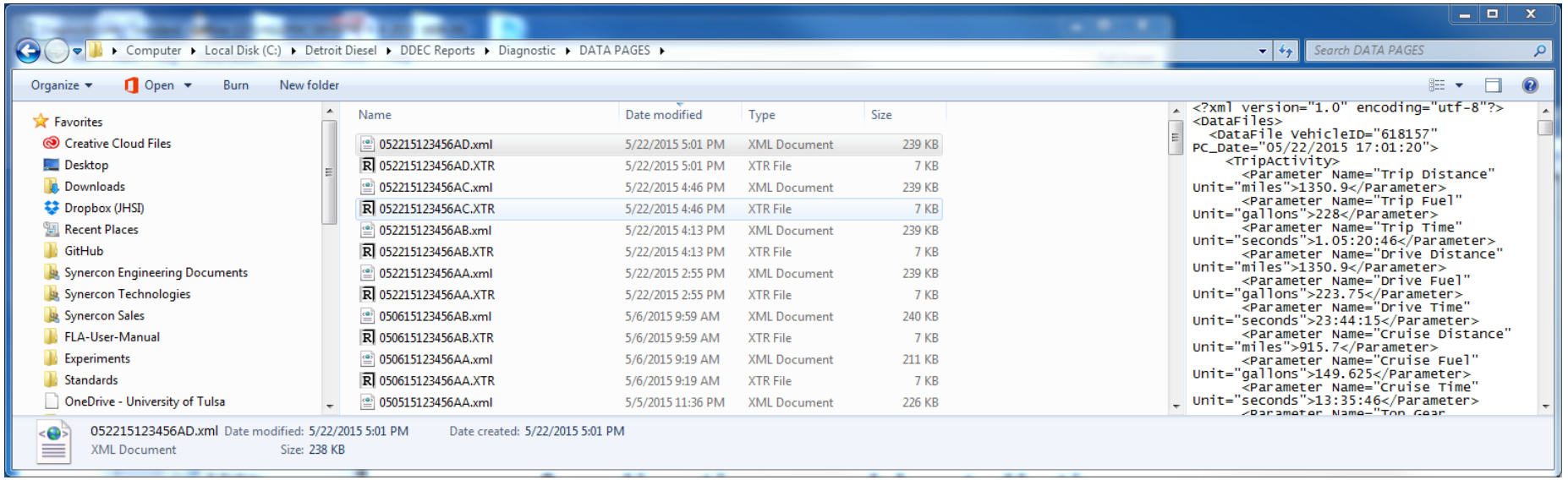


Audit Logs


DiagnosticLink - Standard - Offline ((1FUJGLDR6CSBH3256) 6-8-2015 1606.08)
File Edit View Log Parameters Actions Tools Help
Full Screen
Find
Identification
Fault Codes
Troubleshooting
Instrumentation
Service Routines
I/O Control
Logged Connections (paused)
Common Powertrain Controller E...
CPC02T: Online
Motor Control Module EPA10
MCM02T: Online
Aftertreatment Control Module E...
ACM02T: Online
Identification
Engine: DDEC10-DD15
DiagnosticLink
Common
Audit Trail
Stored Data
Rating
Engine Totals
3rd Change Date GMT
3rd Change Tool ID FFFFFFFF
3rd Change Engine Hours 1193047 hr
3rd Change Rating Changed yes
Real Time Clock
1st Change Old Date 5/22/2015 2:20:15 PM Central Daylight Time
1st Change New Date 5/22/2015 2:55:52 PM Central Daylight Time
1st Change Tool ID 00000000
1st Change Engine Hours 3293 hr
2nd Change Old Date 10/23/2012 8:26:38 PM Central Daylight Time
2nd Change New Date 10/23/2012 8:37:26 PM Central Daylight Time
2nd Change Tool ID 00000000
2nd Change Engine Hours 3264 hr
3rd Change Old Date 12/22/2011 1:55:06 PM Central Daylight Time
3rd Change New Date 12/22/2011 1:57:02 PM Central Daylight Time
3rd Change Tool ID 00000000
3rd Change Engine Hours 949 hr
Road Speed Parameters
1st Change Date 7/18/2012 2:13:49 PM Central Daylight Time
1st Change Tool ID 94C74037
1st Change Engine Hours 2669 hr
1st Change Axle Ratio yes
1st Change FEI Maximum Vehicle Speed
Log time: 6/8/2015 4:06:22 PM

DDEC Reports .XTR

- C:\Detroit Diesel\DDEC Reports\Diagnostic\DATA PAGES
- CSV and XML exporter

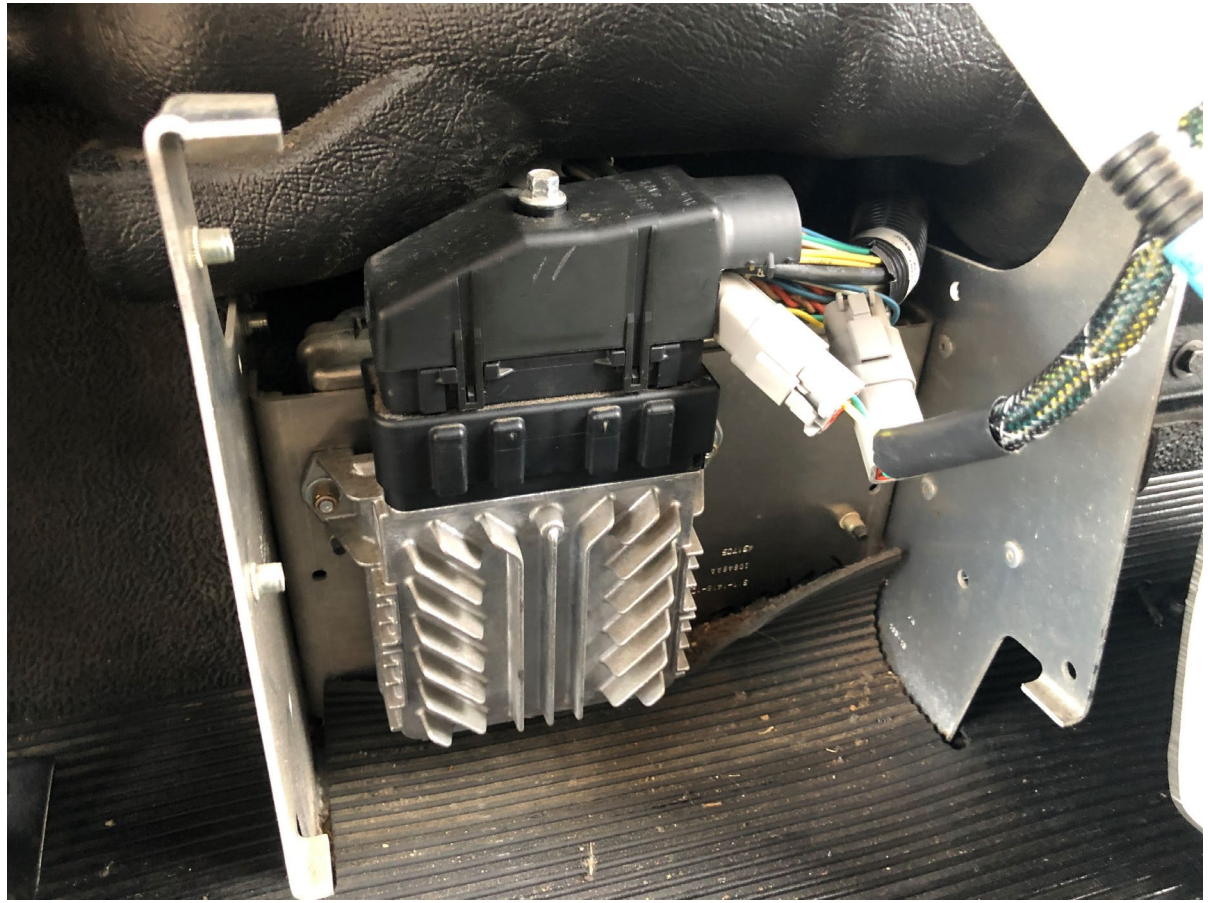


Bendix Brake Controller

Bendix® ACom® PRO™ Diagnostics

Diagnostics at your fingertips to quickly troubleshoot, repair, and recalibrate Bendix systems & components.

Allison Transmissions



Other Diagnostic Software

- Wabco Toolbox
- Navistar Service Maxx for the MaxxForce engines
- PACCAR DAVIE for the MX-13 engine
- Premium Tech Tool for Mack and Volvo

There are many others… ask around and visit service shops.

Almost all use RP1210 and J1939 for the tool interface.

Use different software with just one device.

INTRODUCTION TO RP1210

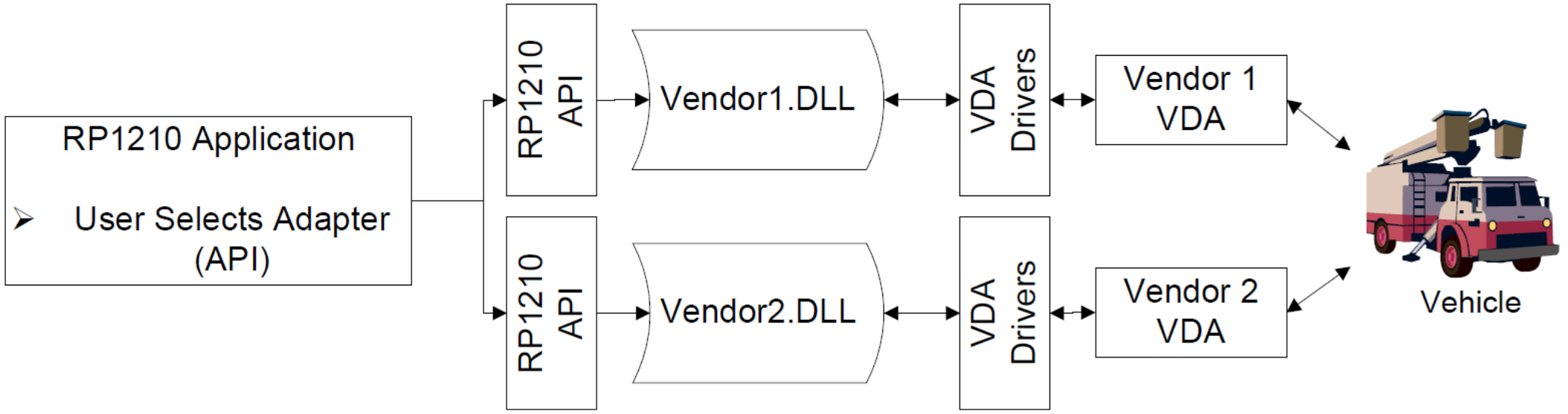
Recommended Practice for Windows Based Diagnostics

- OEMs can write software to an API
- Vehicle Diagnostic Adapters (VDAs) convert Vehicle Networks to PC

5. High-Level RP1210 Interface Conceptual and Design

The following is a diagram of how the RP1210 model is implemented.

- The RP1210 software developer is interested in only the “RP1210 Application” box.
- The RP1210 VDA manufacturer is responsible for the RP1210 API, the DLL (which is responsible for changing the vehicle protocol into API command/responses), the VDA Drivers, and the physical interface device (VDA).



RP1210 Function Calls

Function Name	Description
`GetPrivateProfileString (…)`	Parse the INI files for vendor, device, protocols supported information.
`LoadLibrary (…)`	Open the VDA API's DLL.
`GetProcAddress(…)`	Get pointers to the RP1210 functions within the VDA API's DLL.
`RP1210_ClientConnect (…)`	Get a "logical" connection to the vehicle data bus.
`RP1210_SendCommand(…)`	Allow messages to pass through the API.
`RP1210_SendMessage (…)`	Send a message.
`RP1210_ReadMessage (…)`	Read a message.
`RP1210_ClientDisconnect (…)`	Close the logical connection to the data bus.
`FreeLibrary(…)`	Close the VDA API's DLL.

CSU_RP1210

- Python Application to use RP1210
  - Must use 32-bit Python 3 (suggest to add to path)

https://github.com/SystemsCyber/CSU-RP1210

Demo Code:

Hands on: Extract Component ID from modules by requesting PGN ***65259*** (0xFEEB)

What does it mean to

THINK LIKE A HACKER

"Calculus is the Mathematics of Philosophers,
Cryptography is the Mathematics of Kings"

What is a “Hacker?”

A technically inclined person who is really curious about how things work but doesn’t have the manual (or doesn’t use it).

Most engineers are hackers to some extent.

- Hacker + complicated kids toy = dad at Christmas
- Hacker + patent attorney = inventor
- Hacker + business opportunity = entrepreneur
- Hacker + university = researcher
- Hacker + prankster = drain on society
- Hacker + gangster = digital theft and black markets
- Hacker + evil empire = national security threat

Outcome depends on the context of the “Hack” and the ethics of the “hacker”

The Hacker Tools

- Fuzzing or Black Box Approach
  - Buffer Overflows
  - Low Cost and Minimal Effort
- Static Analysis
  - Decompiled Code
  - Detailed Discovery
  - Time Consuming
- Dynamic Analysis
  - Debuggers
  - System Controls
  - Development Tools

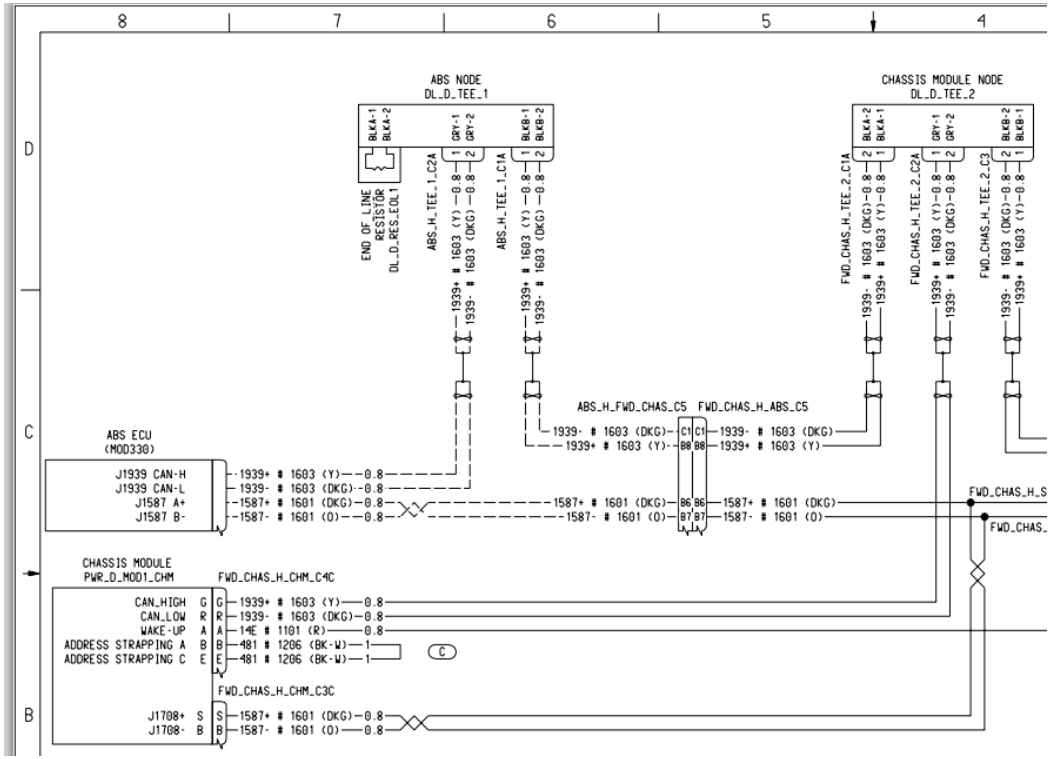
OllyDbg

Let’s look at Demonstrations of Methods and Potential

SECURITY VULNERABILITIES

Door Lock Control with Access to the CAN Bus

Trucks Have Easy Access to Wiring



Assume anyone can get physical access to the network.

Network Analysis of Seed/Key Exchange

- Example of a black box approach
- ECM has the Seed
- PC Software Has the Key
- Extract key information from PC.
  - Record J1939 network traffic to a log
  - Filter and discover J1939 ID 0x18DA00F1 and 0x18DAF100
  - PGNs are used for ISO-CAN over J1939

ISO 15765-3: Unified Diagnostic Services on CAN

Line	Abs Tim	PT	B1	B2	B3	B4	B5	B6	B7	B8
5836	63.73227	18DA00F1	2	10	3	0	0	0	0	0
5839	63.74426	18DAF100	6	50	3	0	14	0	C8	0F
6406	64.72396	18DA00F1	3	22	F1	0	0	0	0	0
6412	64.74421	18DAF100	7	62	F1	0	2	1	0E	3
7043	65.8583	18DA00F1	2	27	5	0	0	0	0	0
7050	65.874	18DAF100	4	67	5	81	B7	1	0E	3
7625	66.88428	18DA00F1	4	27	6	16	98	0	0	0
7639	66.904	18DAF100	2	67	6	81	B7	1	0E	3
8252	67.96437	18DA00F1	10	0D	2E	F1	5C	0	0	0

- SecurityAccess (27 hex) service
  - Subfunction 05 hex: requestSeed
  - Subfunction 06 hex: sendKey
- First Byte = Message length -> 2 byte seed/key

Test setup to get the seed/key pairing

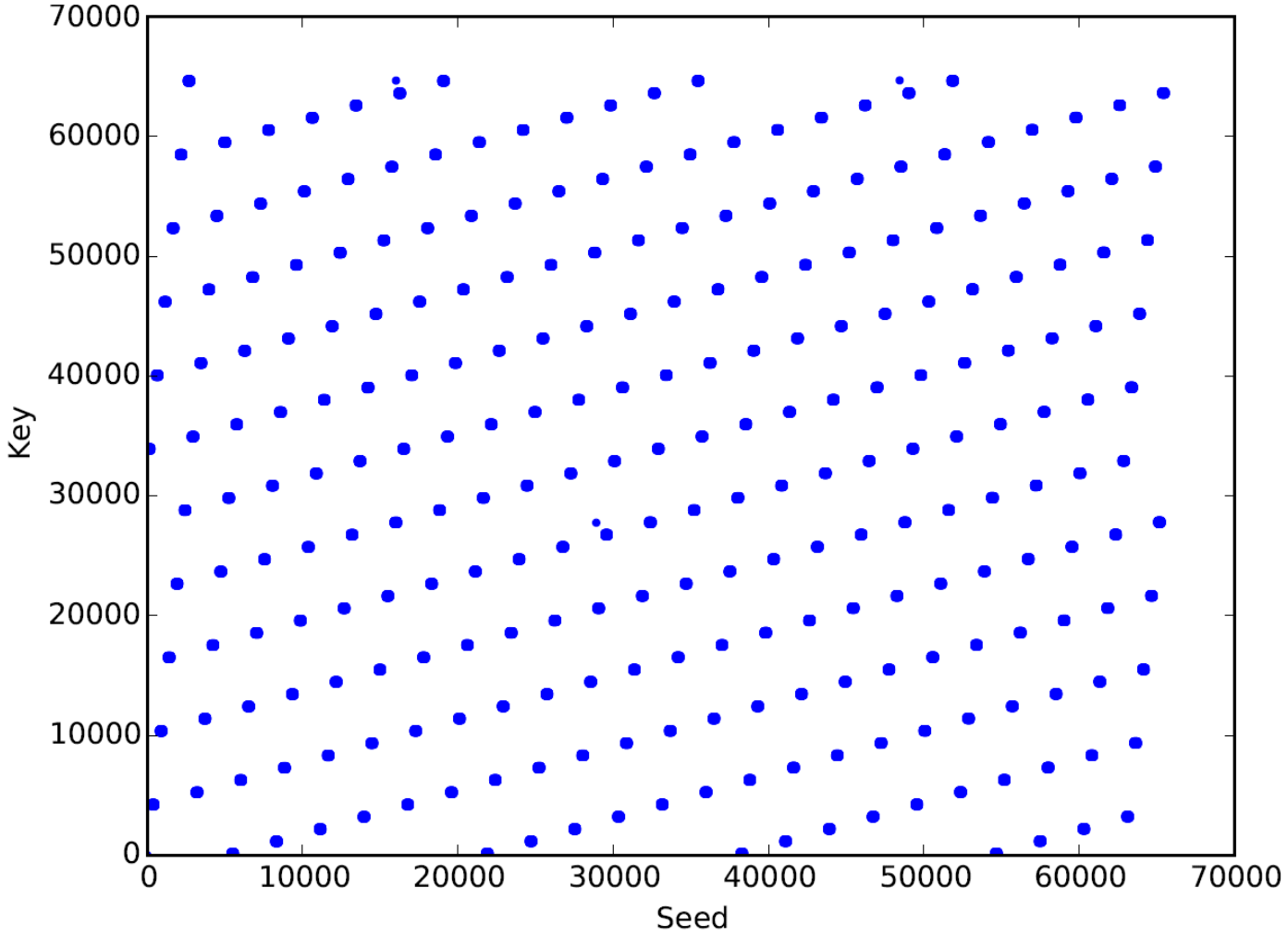
- Beagle Bone Black
  - ARM Linux with SocketCAN
  - Built in CAN Controllers
  - Added MCP2561 CAN Transceiver
  - Python Program to emulate ECM
- CAN Network
- Diagnostic Software with RP1210 device
  - Perpetual Polling Loop -> no PC code needed.

Code Emulating the ECM

```
if can_id == 0x98da00f1:
    if can_data[0:3] == b'\x02\x27\x05': #Received Seed Request
        print("RequestSeed from the PC")
        seed = seedSpace[i]
        i+=1
        #Send Seed Value:
        s1.send(build_can_frame(0x98daf100, b'\x04\x67\x05'
            +struct.pack('<H',seed)+b'\x00\x00\x00'))
        print("Sent Seed value of ", end="")
        print(seed)
        print(time.time())
    elif can_data[0:3] == b'\x04\x27\x06': #Received Key
        print("PC sent Key:", end="")
        key = struct.unpack('<H',can_data[3:5])[0]
        print(key)
        seedKeyPairs[seed]=key
        with open("SeedKeyPairs.json", 'w') as outfile:
            json.dump(seedKeyPairs, outfile)
```

Results for the Seed/Key Exchange

- 11 seconds per pair
- 8 Days
- 65536 Seed/Key Pairs
- 16384 unique values
- 14-Bit Linear Feedback Shift Register?

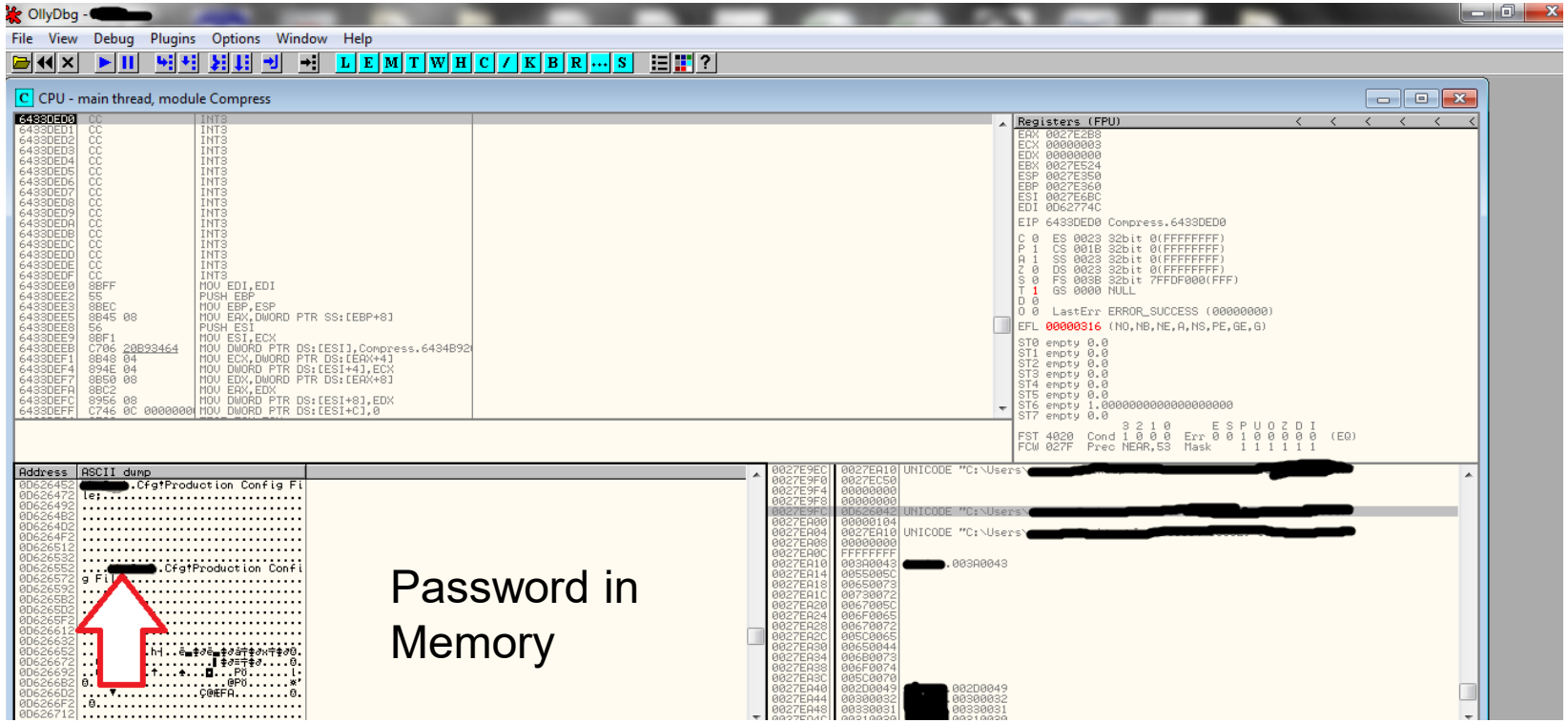


Seed/Key Exchange Conclusion

- 16 bit Seed/Key space is small
  - Brute force attacks are feasible
- Downloadable PC software contains the “secret” for the ECM.
- Complete black box approach
  - No need to know the internal algorithms or processes
  - 192k Lookup Table

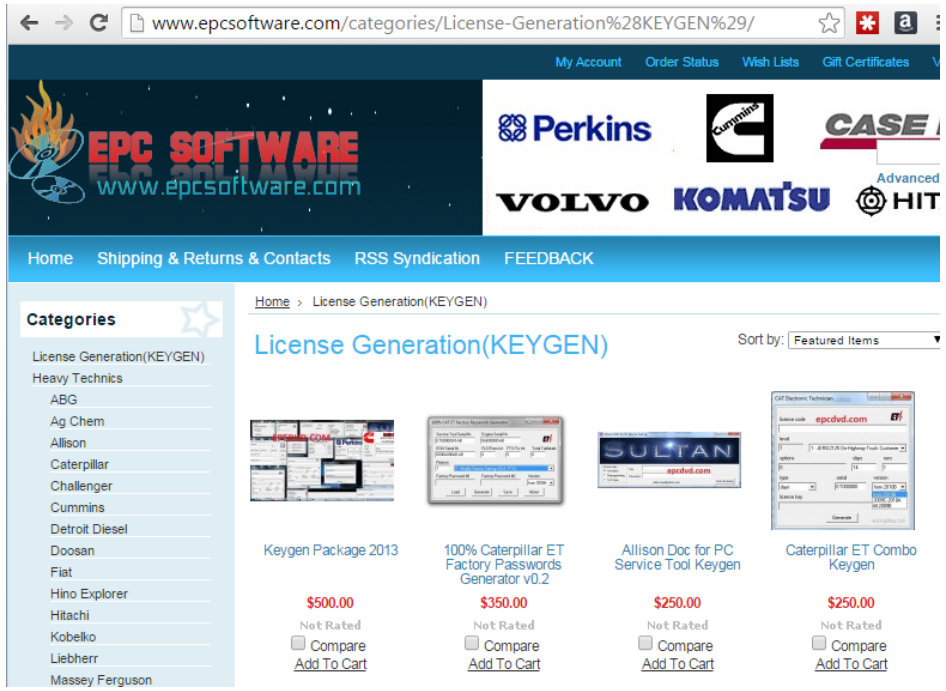
Dynamic Code Analysis

- Use a debugger to examine PC processes and memory during a file save process.



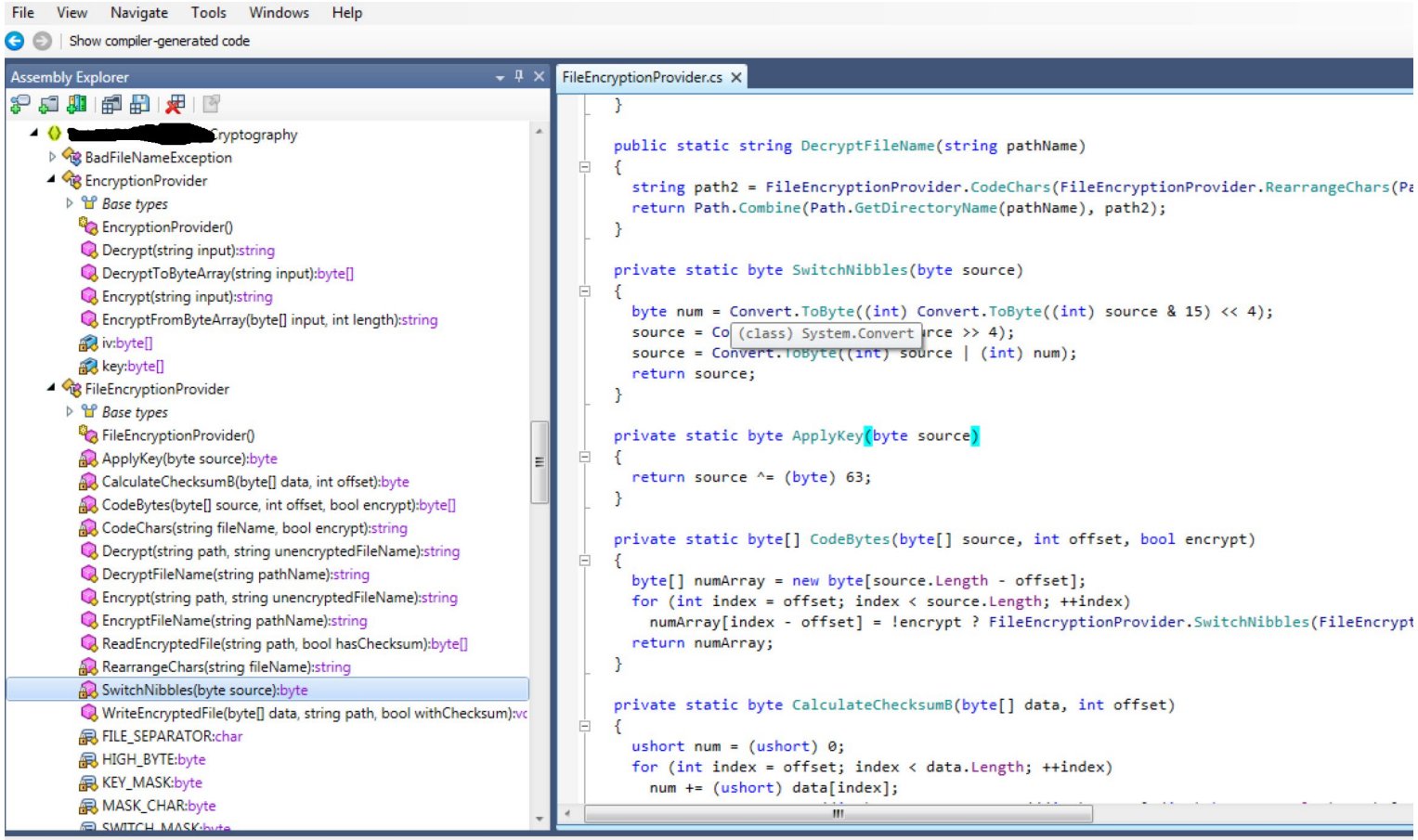
Ramifications from Dynamic Analysis

- Audit Logs can be removed from engine image records.
- Maintenance software can be unlocked.
- Limitations:
  - PC side only.
  - Record is intact on ECU.



Static Analysis

- Use a decompiler on maintenance software



Example Static Analysis Discoveries

- Encryption Scheme:
  - XOR each byte with decimal 63, then switch the nibbles of the byte.
- XOR encryption dates back to Julius Caesar
- Code written in Microsoft .NET framework is byte compiled source code
  - Provides easy source code navigation from distributed products.

Strong Encryption Example

- Data translator tool
  - Defines location and meaning of bytes in a network stream.
  - XML File is Encrypted with Advanced Encryption Standard (AES).
  - Encrypted Data is meaningless without a key.

Key Storage Issues

- AES symmetric key is stored in source code

```
namespace [redacted].TemplateSupportLib
{
  public class ReportTemplateDocument : ITemplateLoader
  {
    private static byte[] encryptKey = new byte[32]
    {
      (byte) 185,
      (byte) 63,
      (byte) 32,
      (byte) 122,
      (byte) 254,
      (byte) 183,
      (byte) 58,
      (byte) 247,
      (byte) 119,
      (byte) 25,
      (byte) 50,
      (byte) 74,
      (byte) 216,
      (byte) 87
```

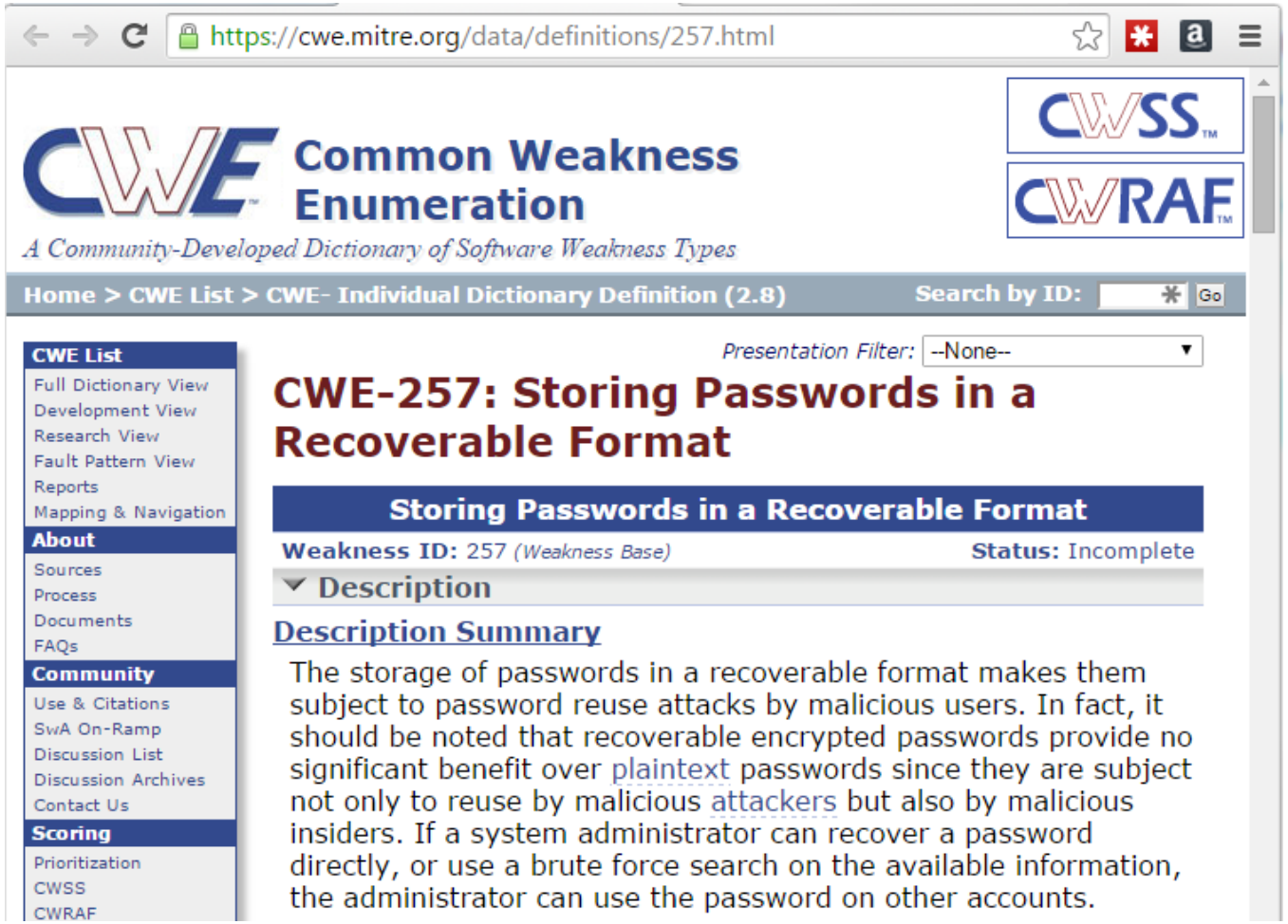
Decrypted Data Translation

```
PublicKeyToken=32f6138b2445373d" name="SingleParameterControl80" children="Controls">
    <Property name="AppKinds">OffHighway, Marine</Property>
    <Property name="Size">300, 15</Property>
    <Property name="ViewKinds">All</Property>
    <Property name="Caption">Battery</Property>
    <Property name="Unit" />
    <Property name="Name">SingleParameterControl80</Property>
    <Property name="ParameterQualifier">Battery Time 2</Property>
    <Property name="EcuKinds">All</Property>
    <Property name="Location">470, 350</Property>
    <Property name="ForeColor">ControlText</Property>
    <Property name="Font">Courier New, 9pt</Property>
</Object>
```

Social Engineering

- True Story: Having trouble with my maintenance software, so I bought pizza for the local service shop and talked to the manger. He placed a call for me to the support line. A support tech with a European accent answers and the manager provides a dealer code and my username over the speakerphone. The support tech fixes the issue with the login. Then…
- Support tech says, “Do you need your password?”
- I say, “No, thank you. I know it.”
- He says, “Your password is psd#5689.”
- I say, “Well, I probably shouldn’t use that one for my bank account anymore.”

System Administrators with passwords?

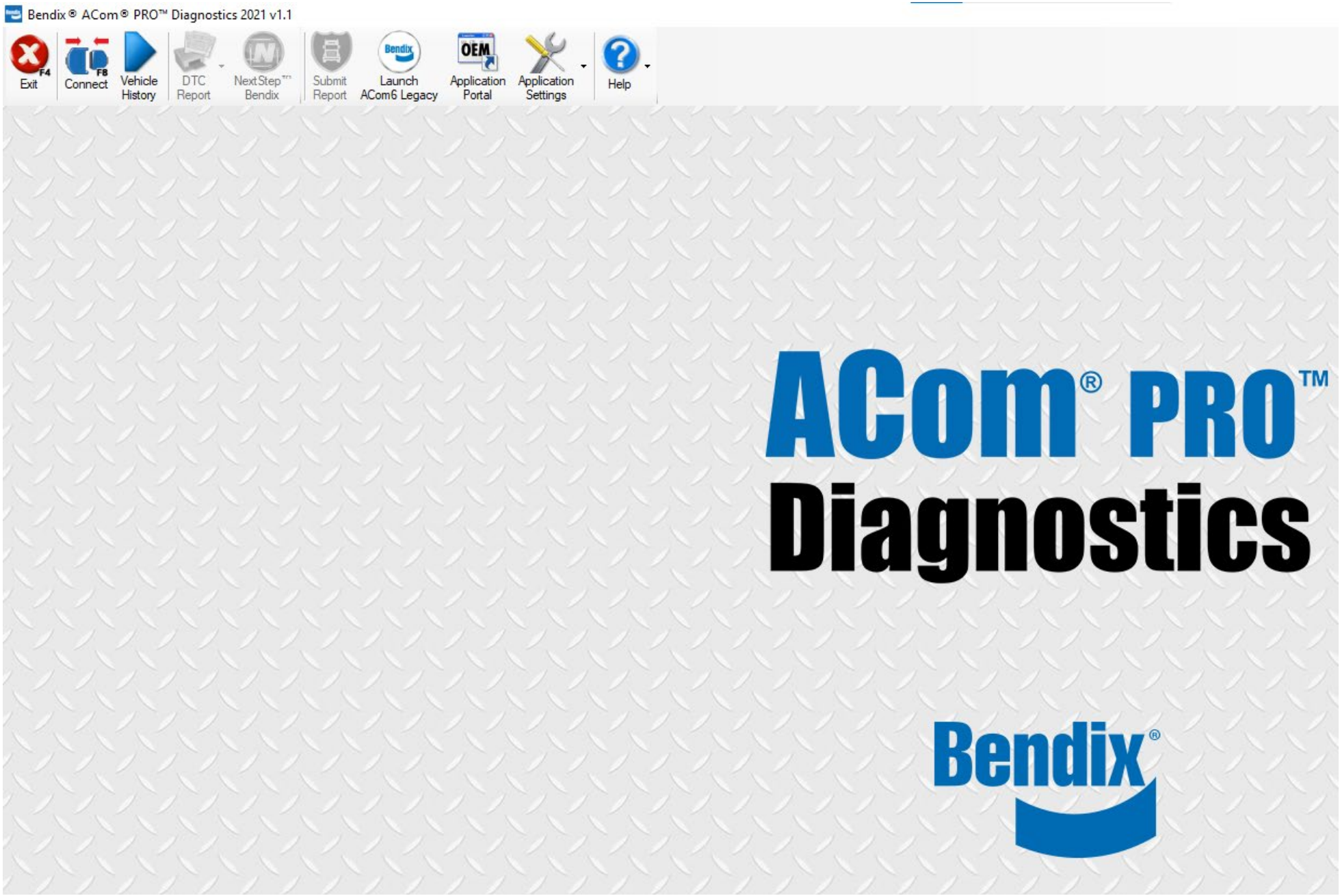


File Obfuscation Example

- Bendix logx files are actually zip files.

1. Open ACOM
2. Connect to a Brake ECU
3. Send (Save) Report
4. Convert .logx file to .zip
5. Analyze CAN traffic and more…

The backend server trusts the .logx file…


Bendix® ACom® PRO™ Diagnostics 2021 v1.1
Exit
Connect
Vehicle History
DTC Report
NextStep™ Bendix
Submit Report
Launch ACom6 Legacy
Application Portal
Application Settings
Help
ACom® PRO™
Diagnostics
Bendix®

Bendix ® ACom ® PRO™ Diagnostics 2021 v1.1

Exit (F4) | Disconnect (F8) | Record | DTC Report | NextStep™ Bendix | Data Monitor | Consumable Fluids | Bendix Diagnostics | Bus Statistics | Submit Report | Launch ACom6 Legacy | Application Portal | Application Settings | Help

Acquiring vehicle information ...

Vehicle

Bendix EC-60 Premium ABS

Vehicle Information

VIN: Not Available

Manufacturer: Not Available

Model Year: Not Available

Status	Component	Description	Lookup Code	...	Count
Active	EC-60 Premium ABS	Miscellaneous - Stop Lamp Switch Not Detected (Flash Code 12-1)	SPN 1045	7	N/A
Active	EC-60 Premium ABS	Miscellaneous - Reserved (Flash Code 12-18)	SPN 611	14	N/A
Active	EC-60 Premium ABS	J1939 Serial Communication: J1939 Retarder (Flash Code 11-2)	SPN 639	14	N/A
Active	EC-60 Premium ABS	J1939 Serial Communication (Flash Code 11-10 or 11-11 or 11-12 or 11-13 or 11-3 or 11-4 or 11-5 or 11-6 or 11-7 or 11-8 or 11-9)	SPN 639	2	N/A
Active	EC-60 Premium ABS	Steer Axle Left WSS: Open or shorted (Flash Code 2-3)	SPN 789	2	N/A
Active	EC-60 Premium ABS	Steer Axle Right WSS: Open or shorted (Flash Code 3-3)	SPN 790	2	N/A
Active	EC-60 Premium ABS	Drive Axle Left WSS: Open or shorted (Flash Code 4-3)	SPN 791	2	N/A

Clear Faults

Malfunction Indicator | Red Stop | Amber Warning | Protect

Wheel Speeds

Left: Front 0.0 mph; Rear #1 0.0 mph; Rear #2 0.0 mph

Right: Front 0.0 mph; Rear #1 0.0 mph; Rear #2 0.0 mph

Odometer 0.0 mi

PROTECT STOP WARNING

ABS ATC

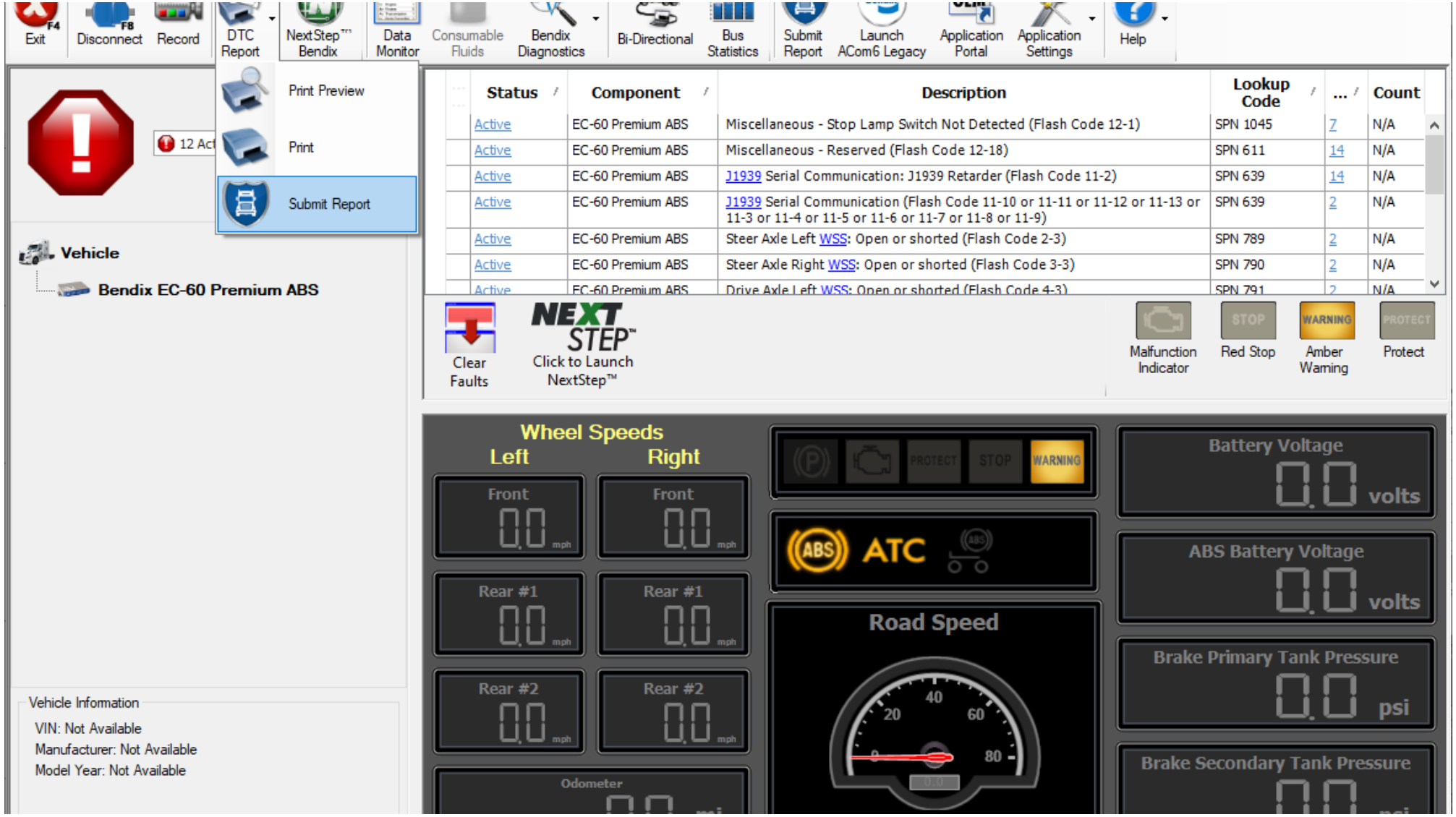
Road Speed

Battery Voltage 0.0 volts

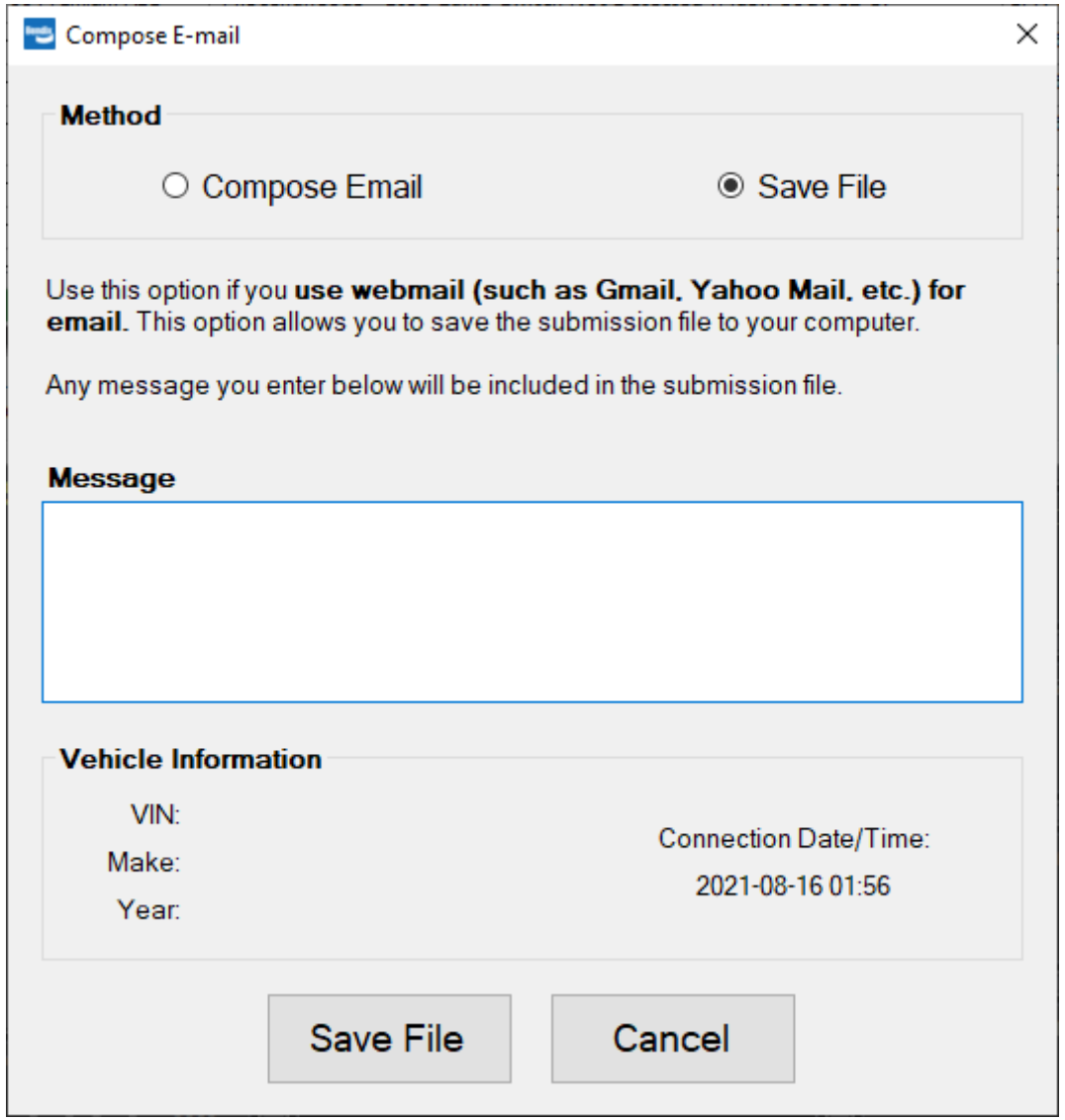
ABS Battery Voltage 0.0 volts

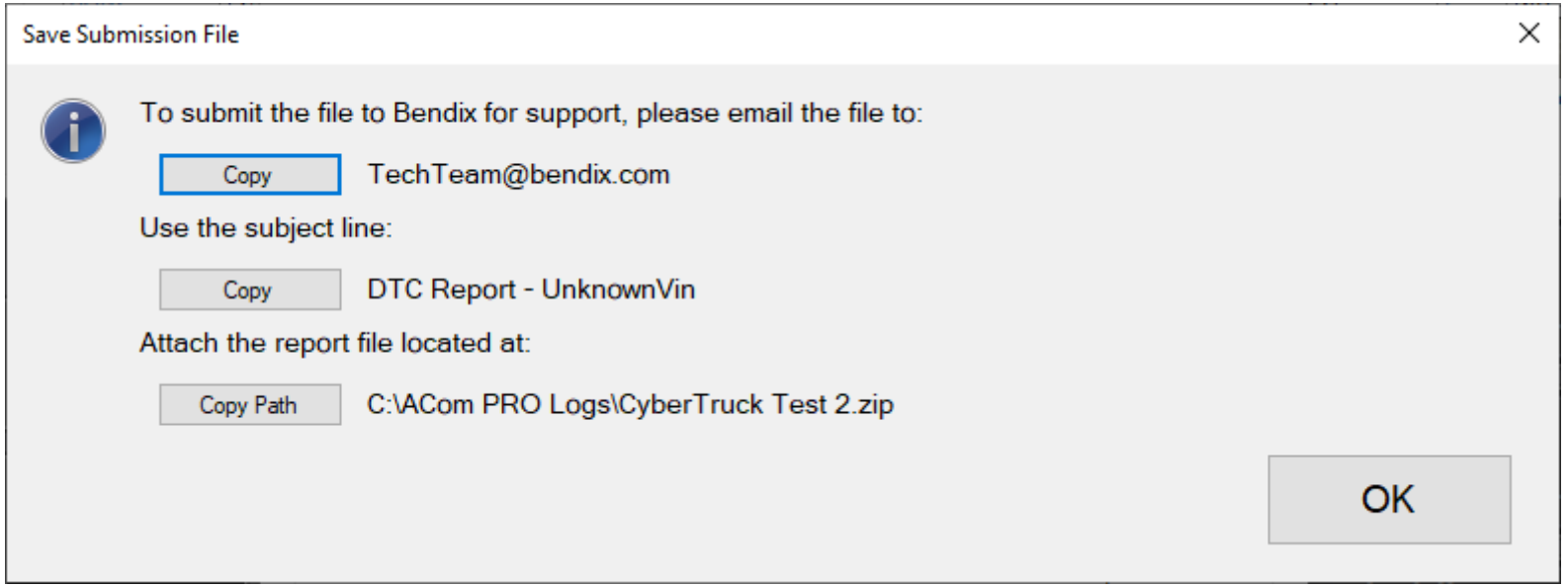
Brake Primary Tank Pressure 0.0 psi

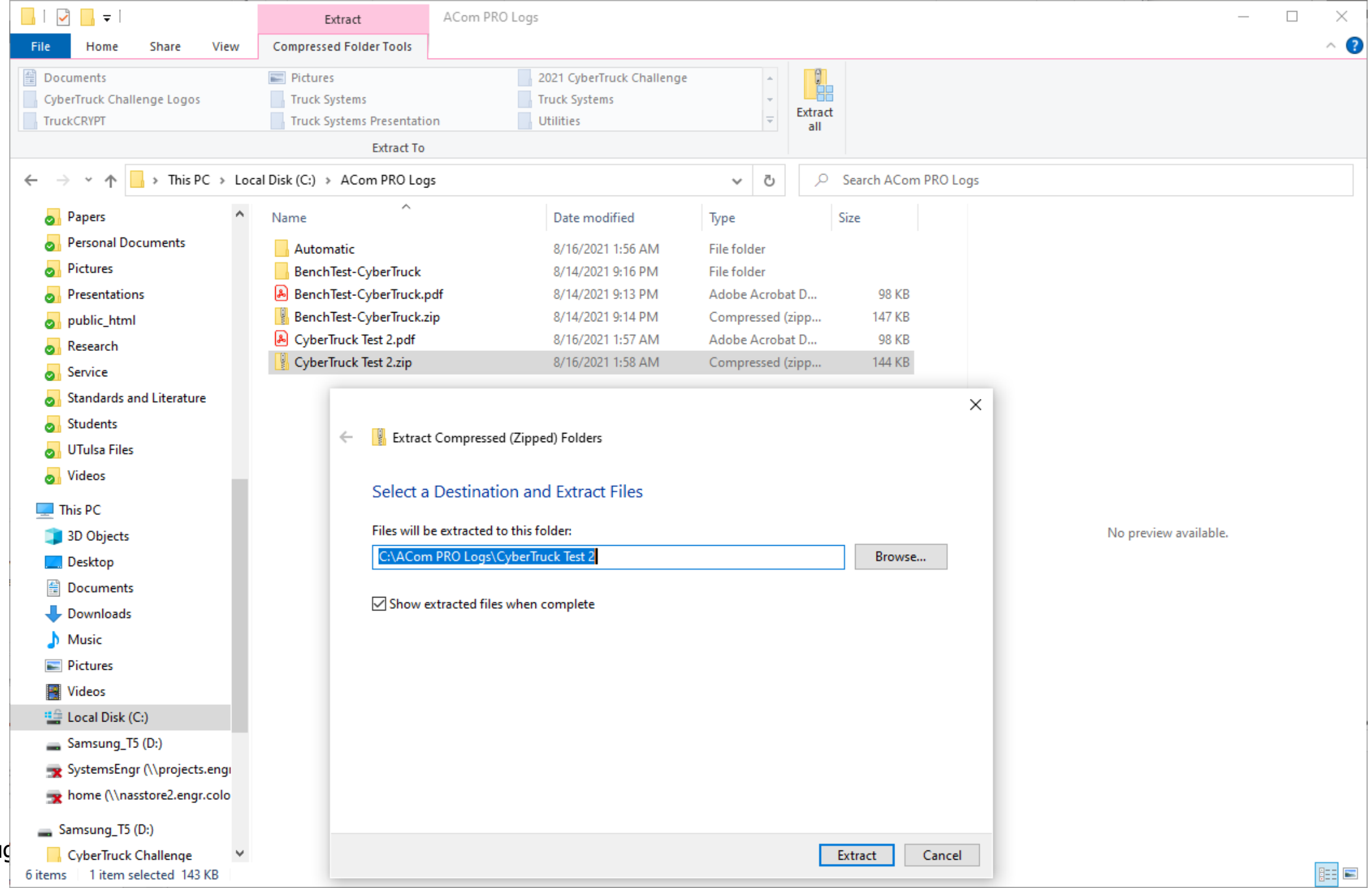
Brake Secondary Tank Pressure 0.0 psi

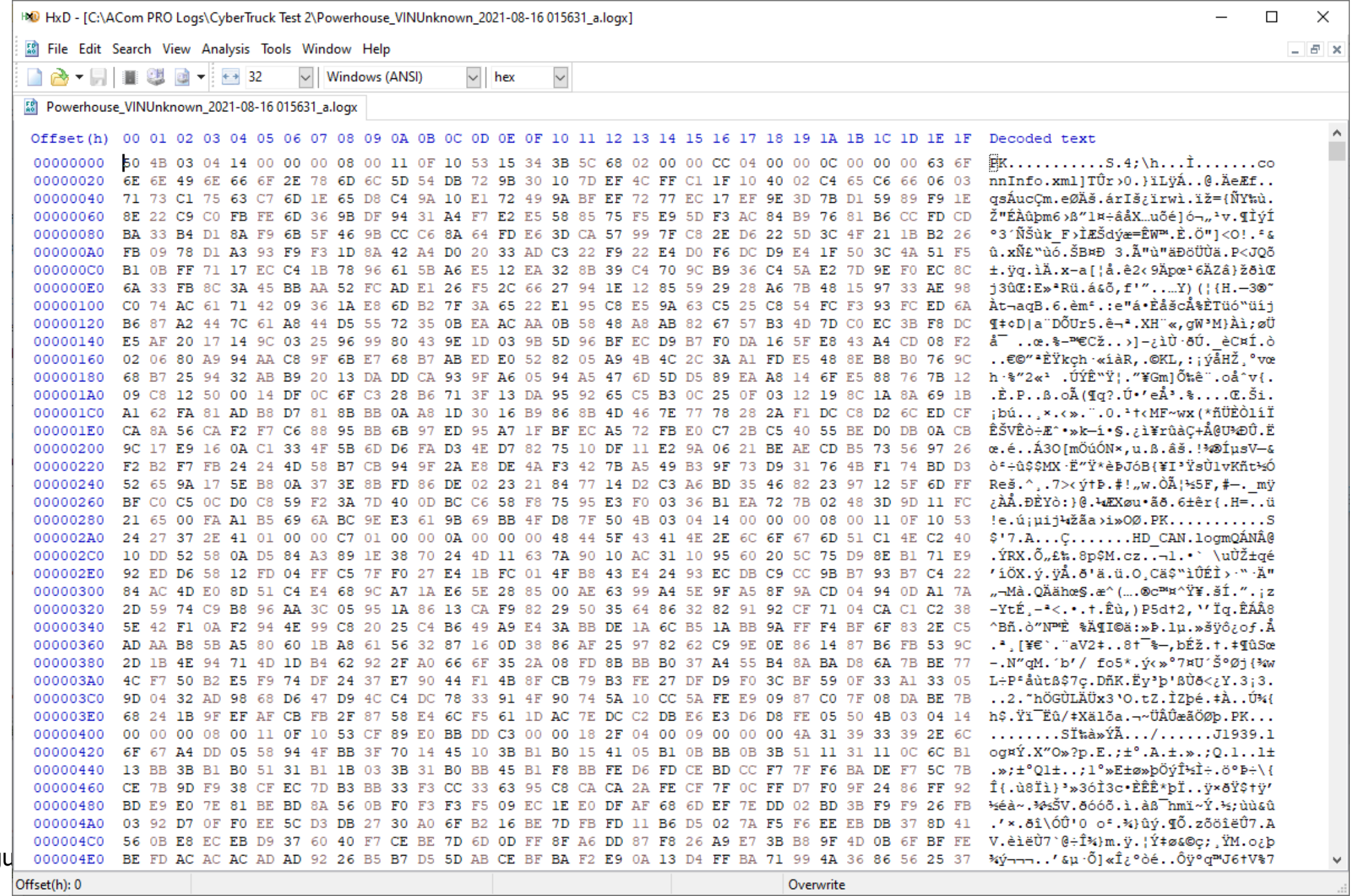


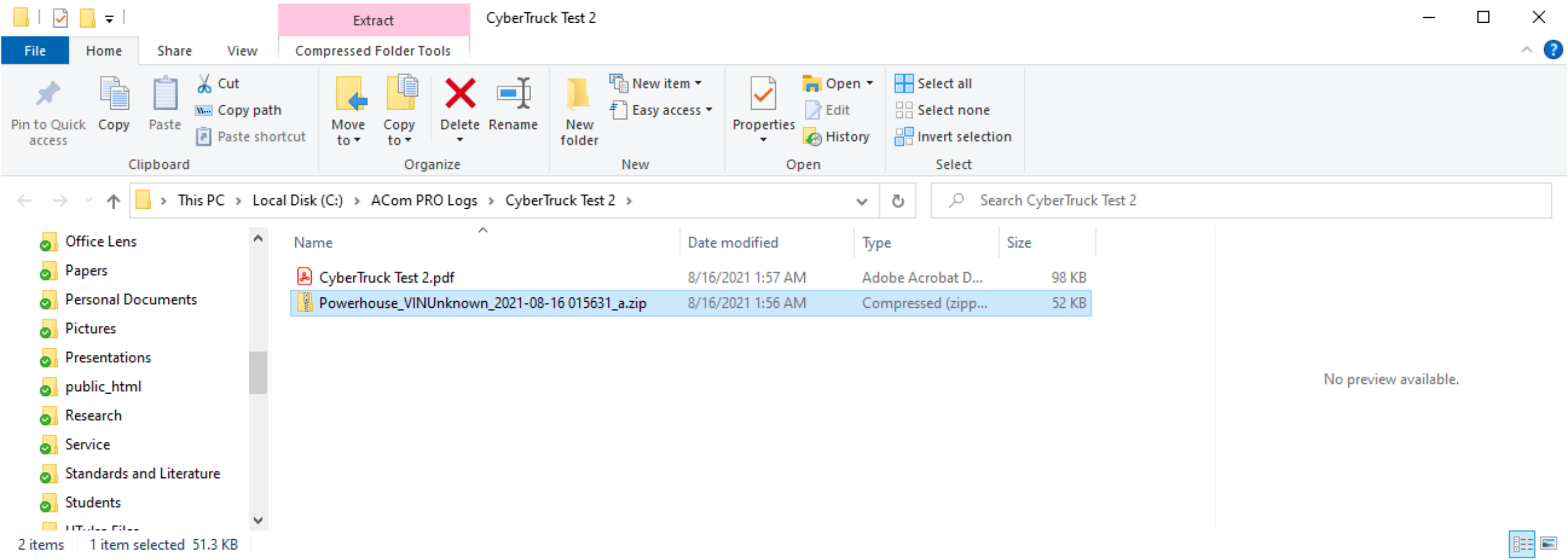
Submit report

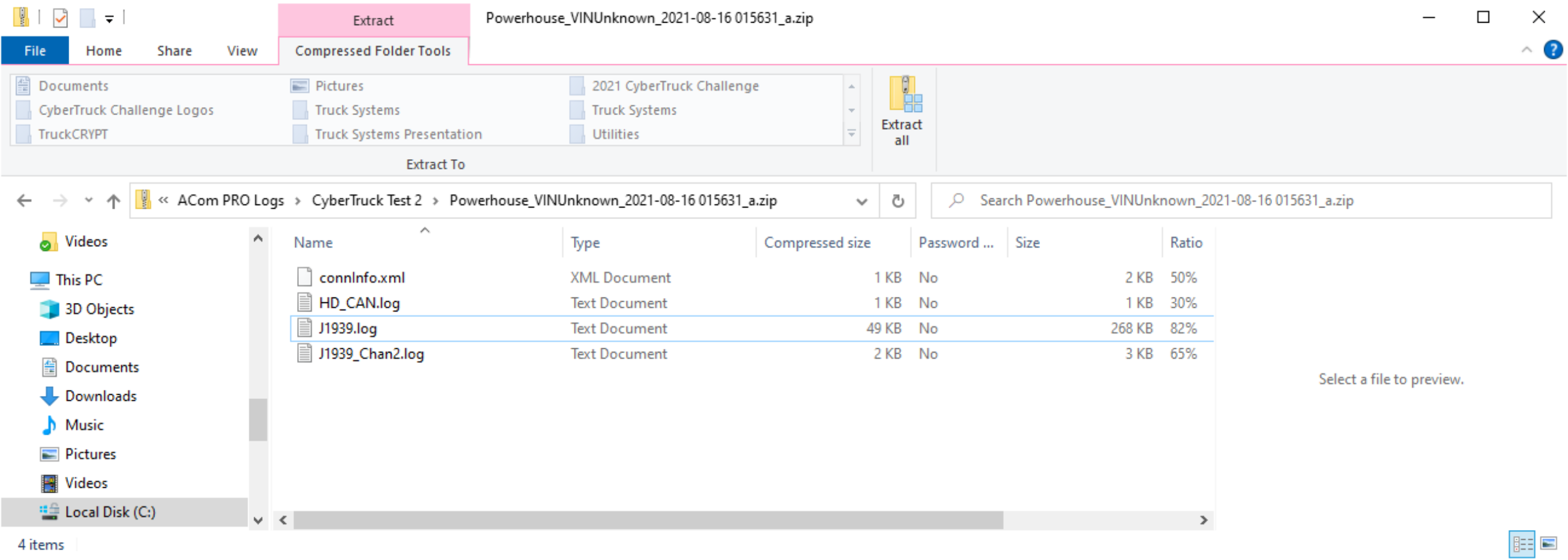

Compose E-mail
Method
Compose Email
Save File
Use this option if you use webmail (such as Gmail, Yahoo Mail, etc.) for email. This option allows you to save the submission file to your computer.
Any message you enter below will be included in the submission file.
Message
Vehicle Information
VIN:
Make:
Year:
Connection Date/Time:
2021-08-16 01:56
Save File
Cancel


Save Submission File
To submit the file to Bendix for support, please email the file to:
Copy
TechTeam@bendix.com
Use the subject line:
Copy
DTC Report - UnknownVin
Attach the report file located at:
Copy Path
C:\ACom PRO Logs\CyberTruck Test 2.zip
OK


Extract
ACom PRO Logs
File
Home
Share
View
Compressed Folder Tools
Documents
CyberTruck Challenge Logos
TruckCRYPT
Pictures
Truck Systems
Truck Systems Presentation
2021 CyberTruck Challenge
Truck Systems
Utilities
Extract all
Extract To
This PC › Local Disk (C:) › ACom PRO Logs
Search ACom PRO Logs
Papers
Personal Documents
Pictures
Presentations
public_html
Research
Service
Standards and Literature
Students
UTulsa Files
Videos
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Samsung_T5 (D:)
SystemsEngr (\\projects.engr
home (\\nasstore2.engr.colo
Samsung_T5 (D:)
CyberTruck Challenge
Name
Date modified
Type
Size
Automatic 8/16/2021 1:56 AM File folder
BenchTest-CyberTruck 8/14/2021 9:16 PM File folder
BenchTest-CyberTruck.pdf 8/14/2021 9:13 PM Adobe Acrobat D... 98 KB
BenchTest-CyberTruck.zip 8/14/2021 9:14 PM Compressed (zipp... 147 KB
CyberTruck Test 2.pdf 8/16/2021 1:57 AM Adobe Acrobat D... 98 KB
CyberTruck Test 2.zip 8/16/2021 1:58 AM Compressed (zipp... 144 KB
Extract Compressed (Zipped) Folders
Select a Destination and Extract Files
Files will be extracted to this folder:
C:\ACom PRO Logs\CyberTruck Test 2
Browse...
Show extracted files when complete
Extract
Cancel
No preview available.
6 items
1 item selected 143 KB


HxD - [C:\ACom PRO Logs\CyberTruck Test 2\Powerhouse_VINUnknown_2021-08-16 015631_a.logx]
File Edit Search View Analysis Tools Window Help
32
Windows (ANSI)
hex
Powerhouse_VINUnknown_2021-08-16 015631_a.logx
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F Decoded text
00000000 50 4B 03 04 14 00 00 00 08 00 11 0F 10 53 15 34 3B 5C 68 02 00 00 CC 04 00 00 0C 00 00 00 63 6F PK.....S.4;\h...Ì.....co
00000020 6E 6E 49 6E 66 6F 2E 78 6D 6C 5D 54 DB 72 9B 30 10 7D EF 4C FF C1 1F 10 40 02 C4 65 C6 66 06 03 nnInfo.xml]TÛr›0.}ïLÿÁ..@.ÄeÆf..
00000040 71 73 C1 75 63 C7 6D 1E 65 D8 C4 9A 10 E1 72 49 9A BF EF 72 77 EC 17 EF 9E 3D 7B D1 59 89 F9 1E qsÁucÇm.eØÄš.árIš¿ïrwì.ïž={ÑY‰ù.
00000060 8E 22 C9 C0 FB FE 6D 36 9B DF 94 31 A4 F7 E2 E5 58 85 75 F5 E9 5D F3 AC 84 B9 76 81 B6 CC FD CD Ž"ÉÀûþm6›ß"1¤÷âåX…uõé]ó¬„¹v.¶ÌýÍ
00000080 BA 33 B4 D1 8A F9 6B 5F 46 9B CC C6 8A 64 FD E6 3D CA 57 99 7F C8 2E D6 22 5D 3C 4F 21 1B B2 26 °3´ÑŠùk_F›ÌÆŠdýæ=ÊW™.È.Ö"]<O!.²&
000000A0 FB 09 78 D1 A3 93 F9 F3 1D 8A 42 A4 D0 20 33 AD C3 22 F9 22 E4 D0 F6 DC D9 E4 1F 50 3C 4A 51 F5 û.xÑ£"ùó.ŠB¤Ð 3.Ã"ù"äÐöÜÙä.P<JQõ
000000C0 B1 0B FF 71 17 EC C4 1B 78 96 61 5B A6 E5 12 EA 32 8B 39 C4 70 9C B9 36 C4 5A E2 7D 9E F0 EC 8C ±.ÿq.ìÄ.x–a[¦å.ê2‹9Äpœ¹6ÄZâ}žðìŒ
000000E0 6A 33 FB 8C 3A 45 BB AA 52 FC AD E1 26 F5 2C 66 27 94 1E 12 85 59 29 28 A6 7B 48 15 97 33 AE 98 j3ûŒ:E»ªRü.á&õ,f'"...Y)(¦{H.—3®˜
00000100 C0 74 AC 61 71 42 09 36 1A E8 6D B2 7F 3A 65 22 E1 95 C8 E5 9A 63 C5 25 C8 54 FC F3 93 FC ED 6A Àt¬aqB.6.èm².:e"á•ÈåšcÅ%ÈTüó"üíj
00000120 B6 87 A2 44 7C 61 A8 44 D5 55 72 35 0B EA AC AA 0B 58 48 A8 AB 82 67 57 B3 4D 7D C0 EC 3B F8 DC ¶‡¢D|a¨DÕUr5.ê¬ª.XH¨«‚gW³M}Àì;øÜ
00000140 E5 AF 20 17 14 9C 03 25 96 99 80 43 9E 1D 03 9B 5D 96 BF EC D9 B7 F0 DA 16 5F E8 43 A4 CD 08 F2 å¯ ..œ.%–™€Cž..›]–¿ìÙ·ðÚ._èC¤Í.ò
00000160 02 06 80 A9 94 AA C8 9F 6B E7 68 B7 AB ED E0 52 82 05 A9 4B 4C 2C 3A A1 FD E5 48 8E B8 B0 76 9C ..€©"ªÈŸkçh·«íàR‚.©KL,:¡ýåHŽ¸°vœ
00000180 68 B7 25 94 32 AB B9 20 13 DA DD CA 93 9F A6 05 94 A5 47 6D 5D D5 89 EA A8 14 6F E5 88 76 7B 12 h·%"2«¹ .ÚÝÊ"Ÿ¦.”¥Gm]Õ‰ê¨.oå^v{.
000001A0 09 C8 12 50 00 14 DF 0C 6F C3 28 B6 71 3F 13 DA 95 92 65 C5 B3 0C 25 0F 03 12 19 8C 1A 8A 69 1B .È.P..ß.oÃ(¶q?.Ú•'eÅ³.%....Œ.Ši.
000001C0 A1 62 FA 81 AD B8 D7 81 8B BB 0A A8 1D 30 16 B9 86 8B 4D 46 7E 77 78 28 2A F1 DC C8 D2 6C ED CF ¡bú..‹»¨.0.¹†‹MF~wx(*ñÜÈÒlíÏ
000001E0 CA 8A 56 CA F2 F7 C6 88 95 BB 6B 97 ED 95 A7 1F BF EC A5 72 FB E0 C7 2B C5 40 55 BE D0 DB 0A CB ÊŠVÊò÷Æˆ•»k—í•§.¿ì¥rûàÇ+Å@U¾ÐÛ.Ë
00000200 9C 17 E9 16 0A C1 33 4F 5B 6D D6 FA D3 4E D7 82 75 10 DF 11 E2 9A 06 21 BE AE CD B5 73 56 97 26 œ.é..Á3O[mÖúÓN×‚u.ß.âš.!¾®ÍµsV—&
00000220 F2 B2 F7 FB 24 24 4D 58 B7 CB 94 9F 2A E8 DE 4A F3 42 7B A5 49 B3 9F 73 D9 31 76 4B F1 74 BD D3 ò²÷û$$MX·Ë”Ÿ*èÞJóB{¥I³ŸsÙ1vKñt½Ó
00000240 52 65 9A 17 5E B8 0A 37 3E 8B FD 86 DE 02 23 21 84 77 14 D2 C3 A6 BD 35 46 82 23 97 12 5F 6D FF Reš.^¸.7>‹ý†Þ.#!„w.ÒÃ¦½5F‚#—._mÿ
00000260 BF C0 C5 0C D0 C8 59 F2 3A 7D 40 0D BC C6 58 F8 75 95 E3 F0 03 36 B1 EA 72 7B 02 48 3D 9D 11 FC ¿ÀÅ.ÐÈYò:}@.¼ÆXøu•ãð.6±êr{.H=..ü
00000280 21 65 00 FA A1 B5 69 6A BC 9E E3 61 9B 69 BB 4F D8 7F 50 4B 03 04 14 00 00 00 08 00 11 0F 10 53 !e.ú¡µij¼žãa›i»OØ.PK.....S
000002A0 24 27 37 2E 41 01 00 00 C7 01 00 00 0A 00 00 00 48 44 5F 43 41 4E 2E 6C 6F 67 6D 51 C1 4E C2 40 $'7.A...Ç.....HD_CAN.logmQÁNÂ@
000002C0 10 DD 52 58 0A D5 84 A3 89 1E 38 70 24 4D 11 63 7A 90 10 AC 31 10 95 60 20 5C 75 D9 8E B1 71 E9 .ÝRX.Õ„£‰.8p$M.cz..¬1.•` \uÙŽ±qé
000002E0 92 ED D6 58 12 FD 04 FF C5 7F F0 27 E4 1B FC 01 4F B8 43 E4 24 93 EC DB C9 CC 9B B7 93 B7 C4 22 'íÖX.ý.ÿÅ.ð'ä.ü.O¸Cä$"ìÛÉÌ›·"·Ä"
00000300 84 AC 4D E0 8D 51 C4 E4 68 9C A7 1A E6 5E 28 85 00 AE 63 99 A4 5E 9F A5 8F 9A CD 04 94 0D A1 7A „¬Mà.QÄähœ§.æ^(….®c™¤^Ÿ¥.šÍ.”.¡z
00000320 2D 59 74 C9 B8 96 AA 3C 05 95 1A 86 13 CA F9 82 29 50 35 64 86 32 82 91 92 CF 71 04 CA C1 C2 38 -YtÉ¸–ª<.•.†.Êù‚)P5d†2‚‘'Ïq.ÊÁÂ8
00000340 5E 42 F1 0A F2 94 4E 99 C8 20 25 C4 B6 49 A9 E4 3A BB DE 1A 6C B5 1A BB 9A FF F4 BF 6F 83 2E C5 ^Bñ.ò”N™È %Ä¶I©ä:»Þ.lµ.»šÿô¿of‚.Å
00000360 AD AA B8 5B A5 80 60 1B A8 61 56 32 87 16 0D 38 86 AF 25 97 82 62 C9 9E 0E 86 14 87 B6 FB 53 9C .ª¸[¥€`.¨aV2‡..8†¯%—‚bÉž.†.‡¶ûSœ
00000380 2D 1B 4E 94 71 4D 1D B4 62 92 2F A0 66 6F 35 2A 08 FD 8B BB B0 37 A4 55 B4 8A BA D8 6A 7B BE 77 -.N”qM.´b’/ fo5*.ý‹»°7¤U´Š°Øj{¾w
000003A0 4C F7 50 B2 E5 F9 74 DF 24 37 E7 90 44 F1 4B 8F CB 79 B3 FE 27 DF D9 F0 3C BF 59 0F 33 A1 33 05 L÷P²åùtß$7ç.DñK.Ëy³þ'ßÙð<¿Y.3¡3.
000003C0 9D 04 32 AD 98 68 D6 47 D9 4C C4 DC 78 33 91 4F 90 74 5A 10 CC 5A FE E9 09 87 C0 7F 08 DA BE 7B ..2.˜hÖGÙLÄÜx3'O.tZ.ÌZþé.‡À..Ú¾{
000003E0 68 24 1B 9F EF AF CB FB 2F 87 58 E4 6C F5 61 1D AC 7E DC C2 DB E6 E3 D6 D8 FE 05 50 4B 03 04 14 h$.Ÿï¯Ëû/‡Xälõa.¬~ÜÂÛæãÖØþ.PK...
00000400 00 00 00 08 00 11 0F 10 53 CF 89 E0 BB DD C3 00 00 18 2F 04 00 09 00 00 00 4A 31 39 33 39 2E 6C ....SÏ‰à»ÝÃ.../.....J1939.l
00000420 6F 67 A4 DD 05 58 94 4F BB 3F 70 14 45 10 3B B1 B0 15 41 05 B1 0B BB 0B 3B 51 11 31 11 0C 6C B1 og¤Ý.X”O»?p.E.;±°.A.±.».;Q.1..l±
00000440 13 BB 3B B1 B0 51 31 B1 1B 03 3B 31 B0 BB 45 B1 F8 BB FE D6 FD CE BD CC F7 7F F6 BA DE F7 5C 7B .»;±°Q1±..;1°»E±ø»þÖýÎ½Ì÷.ö°Þ÷\{
00000460 CE 7B 9D F9 38 CF EC 7D B3 BB 33 F3 CC 33 63 95 C8 CA CA 2A FE CF 7F 0C FF D7 F0 9F 24 86 FF 92 Î{.ù8Ïì}³»3óÌ3c•ÈÊÊ*þÏ..ÿ×ðŸ$†ÿ’
00000480 BD E9 E0 7E 81 BE BD 8A 56 0B F0 F3 F3 F5 09 EC 1E E0 DF AF 68 6D EF 7E DD 02 BD 3B F9 F9 26 FB ½éà~.¾½ŠV.ðóóõ.ì.àß¯hmï~Ý.½;ùù&û
000004A0 03 92 D7 0F F0 EE 5C D3 DB 27 30 A0 6F B2 16 BE 7D FB FD 11 B6 D5 02 7A F5 F6 EE EB DB 37 8D 41 .’×.ðî\ÓÛ'0 o².¾}ûý.¶Õ.zõöîëÛ7.A
000004C0 56 0B E8 EC EB D9 37 60 40 F7 CE BE 7D 6D 0D FF 8F A6 DD 87 F8 26 A9 E7 3B B8 9F 4D 0B 6F BF FE V.èìëÙ7`@÷Î¾}m.ÿ.¦Ý‡ø&©ç;¸ŸM.o¿þ
000004E0 BE FD AC AC AC AD AD 92 26 B5 B7 D5 5D AB CE BF BA F2 E9 0A 13 D4 FF BA 71 99 4A 36 86 56 25 37 ¾ý¬¬¬..’&µ·Õ]«Î¿°òé..Ôÿ°q™J6†V%7
Offset(h): 0
Overwrite


Extract
CyberTruck Test 2
File
Home
Share
View
Compressed Folder Tools
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New folder
New item
Easy access
New
Properties
Open
Edit
History
Open
Select all
Select none
Invert selection
Select
This PC
Local Disk (C:)
ACom PRO Logs
CyberTruck Test 2
Search CyberTruck Test 2
Office Lens
Papers
Personal Documents
Pictures
Presentations
public_html
Research
Service
Standards and Literature
Students
Name
Date modified
Type
Size
CyberTruck Test 2.pdf
8/16/2021 1:57 AM
Adobe Acrobat D...
98 KB
Powerhouse_VINUnknown_2021-08-16 015631_a.zip
8/16/2021 1:56 AM
Compressed (zipp...
52 KB
No preview available.
2 items
1 item selected 51.3 KB

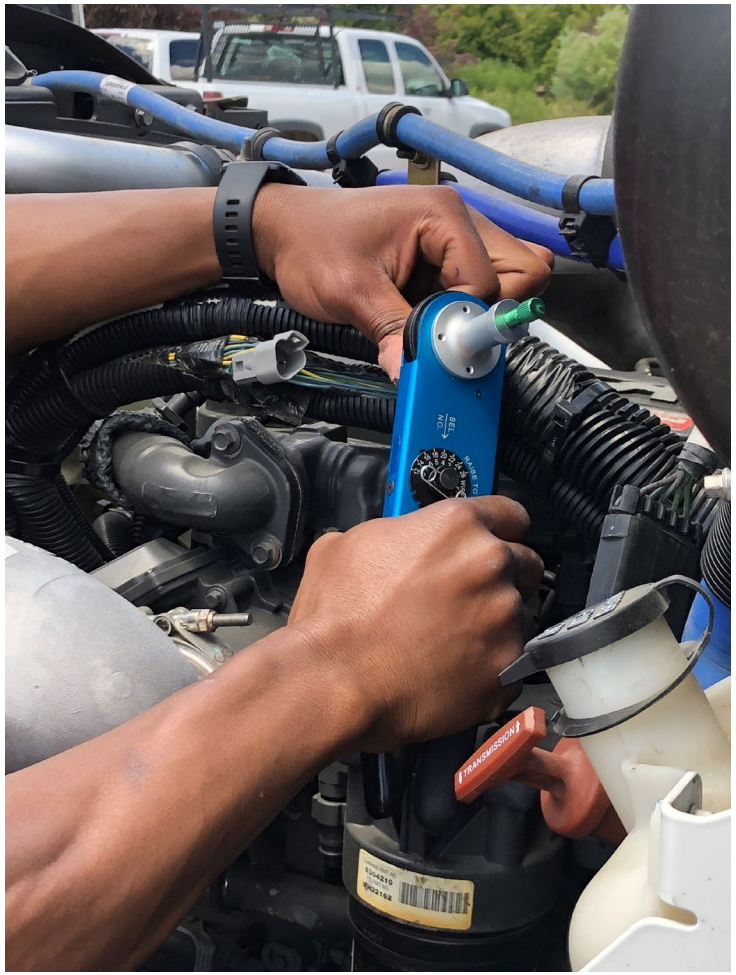

Extract
Powerhouse_VINUnknown_2021-08-16 015631_a.zip
File
Home
Share
View
Compressed Folder Tools
Documents
CyberTruck Challenge Logos
TruckCRYPT
Pictures
Truck Systems
Truck Systems Presentation
2021 CyberTruck Challenge
Truck Systems
Utilities
Extract To
Extract all
« ACom PRO Logs › CyberTruck Test 2 › Powerhouse_VINUnknown_2021-08-16 015631_a.zip
Search Powerhouse_VINUnknown_2021-08-16 015631_a.zip
Videos
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Name
Type
Compressed size
Password ...
Size
Ratio
connInfo.xml
XML Document
1 KB
No
2 KB
50%
HD_CAN.log
Text Document
1 KB
No
1 KB
30%
J1939.log
Text Document
49 KB
No
268 KB
82%
J1939_Chan2.log
Text Document
2 KB
No
3 KB
65%
Select a file to preview.
4 items

Diagnostics Files

- Companies want to collect data
  - Trust data sources from trusted applications
- Can you exploit a zip file?
- Are there virus scans or protections when parsing the logx (zip)?

Challenge: Can you manipulate the data in the file to affect the forensic record (Bendix Data Recorder?)

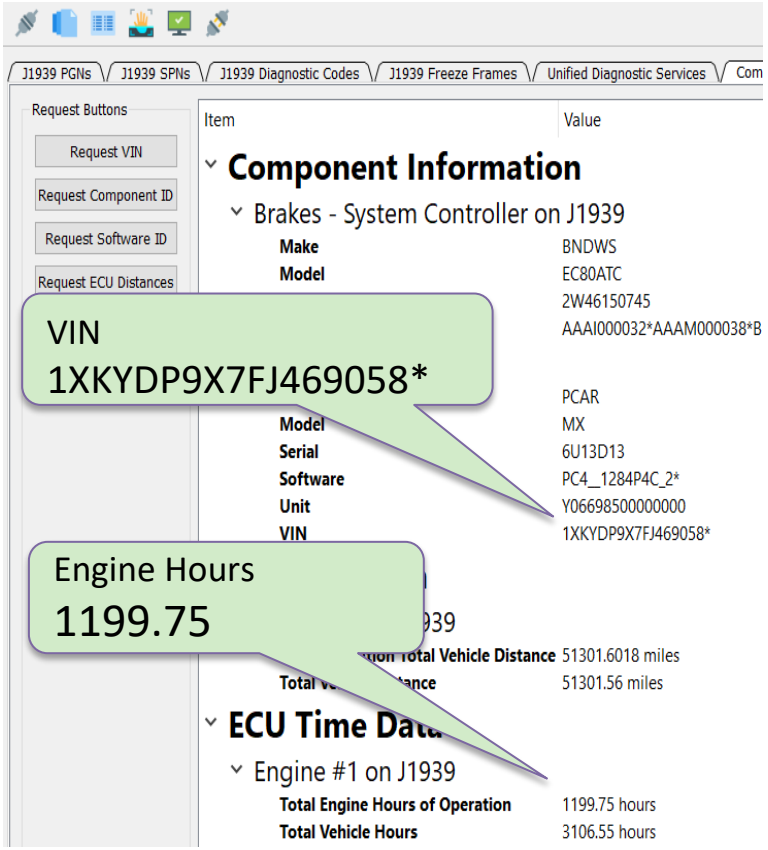
Middleperson Attacks



Installed "Gateway" Devices Splitting the Network

Microprocessors with 2 CAN channels can pass CAN data back and forth.

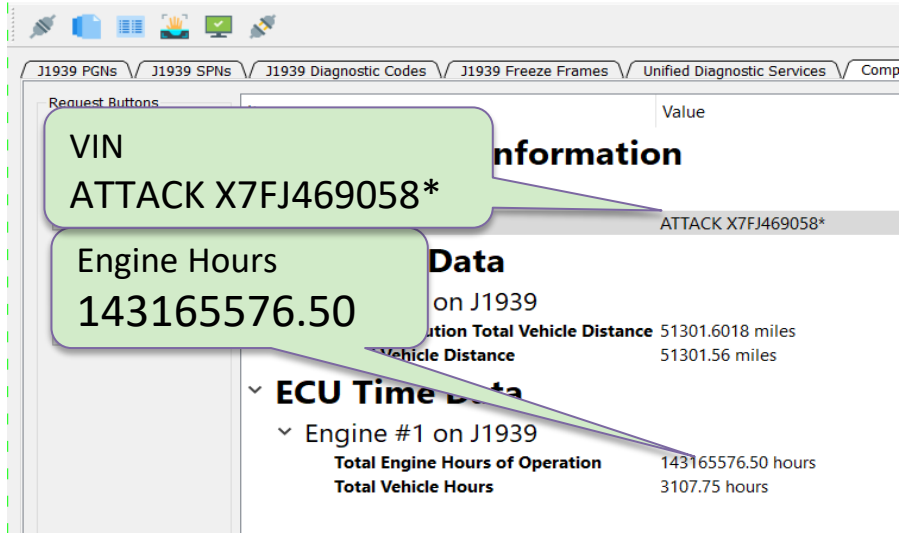
Manipulated VIN and Engine Hours



Normal VIN

Use a middleperson node to lie to the diagnostics software.

After a middle person attack



The middle person doesn’t need to be wired in.

RP1210 SHIM DLL

TMC RP1210 Standard

TMC = Truck Maintenance Council

RP = Recommended Practice

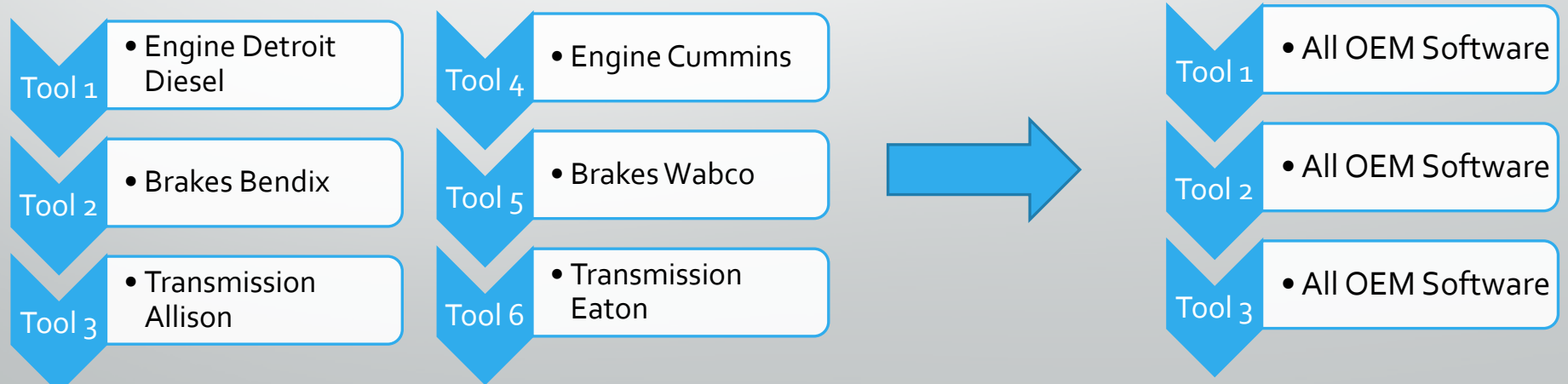
1210 = Standard Number

Standardize communication between Windows applications and diagnostic tools that support the heavy duty vehicle market.

Angela Adelsberger
DG Technologies

History

- Trucking industry customers pick and choose what modules they want on their vehicle. This is very different from automotive market.
- Why was API was developed? Heavy duty repair shops were not happy about having to buy multiple tools to support multiple OEM pieces of software that were tied to different diagnostic tools. They wanted to buy one tool to support all their OEM software.



Development of RP1210

- Truck repair / fleets approached TMC about this problem and a common API was developed for OEMs to start using.
- April 1997 RP1210 was approved.
- Initial protocols supported CAN, J1939, J1708, J1850
- Current revision is RP1210(D)
  - Changes made to address things such as CAN Auto Baud and add additional protocols

RP1210 DLL Exports

RP1210 Original Exports	Exports Added Later On
• RP1210_ClientConnect • RP1210_ClientDisconnect • RP1210_SendMessage • RP1210_ReadMessage • RP1210_SendCommand • RP1210_ReadVersion • RP1210_GetErrorMsg	• RP1210_ReadDetailedVersion • RP1210_GetHardwareStatus • RP1210_GetErrorMsg • RP1210_GetLastErrorMsg • RP1210_Ioctl • RP1210_GetHardwareStatusEx

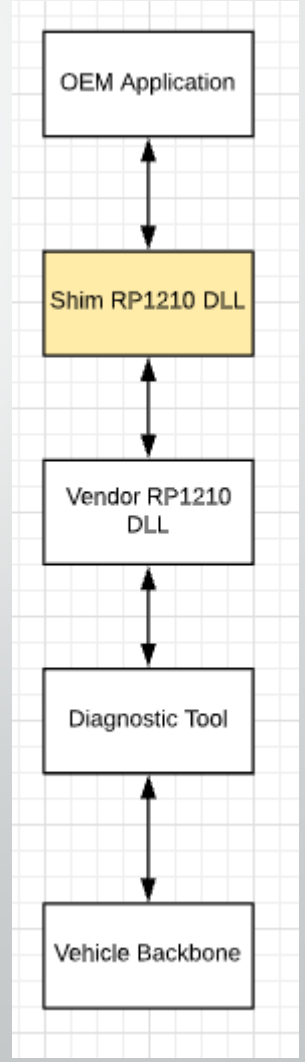
OEM Application to Vendor DLL

- [Windows]\RP121032.ini
  - Contains list of vendor ini & dlls that support the RP1210 API
  - Name must be unique and max of 8 bytes
- [Windows]\Vendor1.ini
  - Contains devices and protocols that the vendor supports
  - OEM software populates a list of devices / maybe protocols for user to select from based on this file
- [Windows\System32]\Vendor1.dll
  - RP1210 dll that is loaded by OEM software

```
[RP1210Support]
APIImplementations=Vendor1,Vendor2,Vendor3,Vendor4
```

Vulnerabilities of RP1210

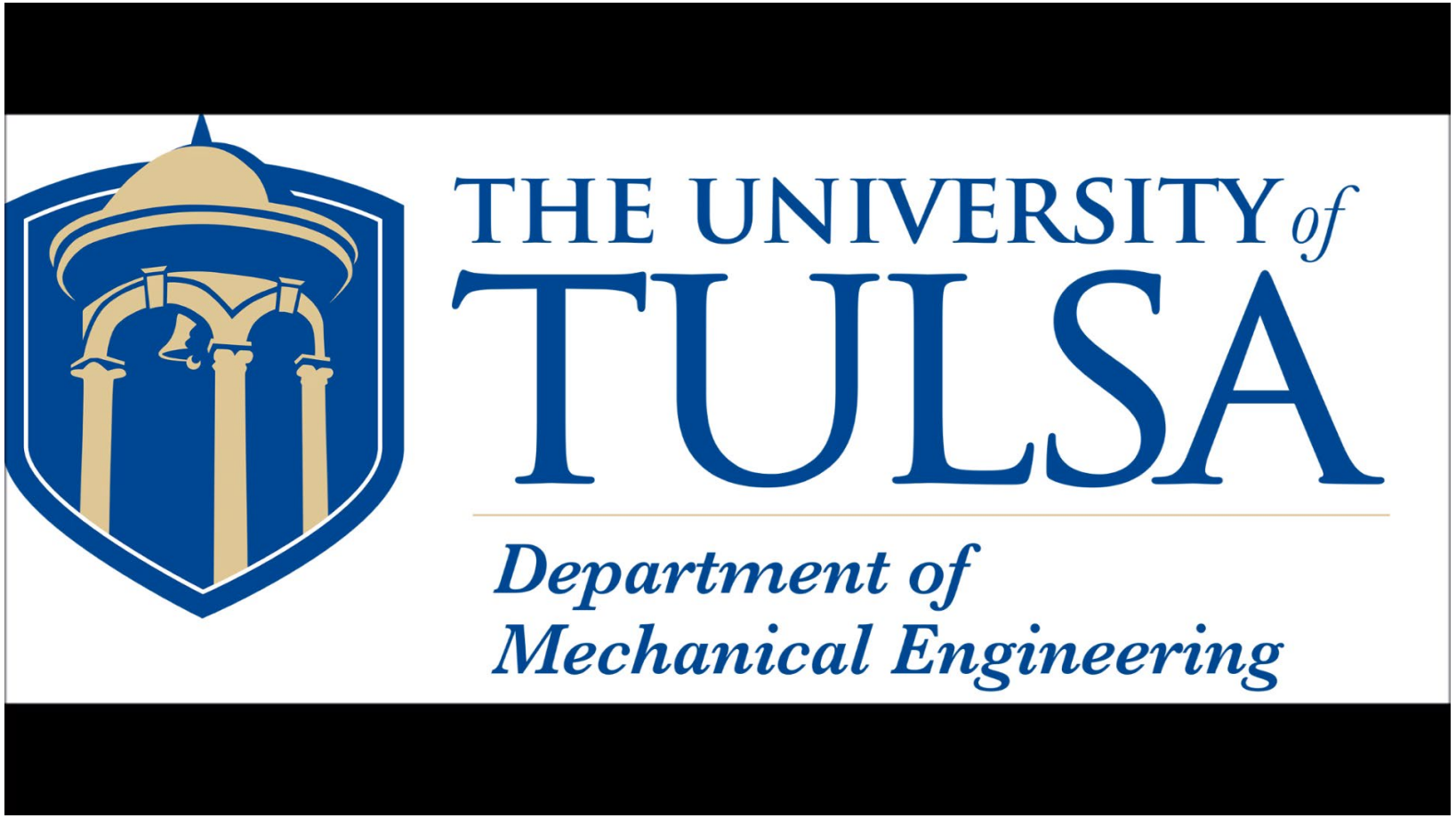
- Because this is a common API that all tools use you run the risk of another DLL impersonating a vendor's DLL.
  - Data Manipulation
  - Logging of Information Without User's Knowledge



RP1210 Shim Challenge

- Act as a shim DLL for a RP1210 application
- Update the code provided to you to log information between the application and vendor tool
- Manipulate the data of a message being returned to the application (do we want to specify what PGN / Data bytes we want changed?)

Cars and Trucks Sometimes Crash



Why did these trucks crash?

- Real reason: we pulled them together with cables.
- Thought experiment:
  - One of the drivers was tired and fell asleep at the wheel.
  - Drifted left of center and had a head on crash.
  - Investigation showed the driver falsified his logs.
  - Driver was actually on his 15th hour of driving that day

- How does the government respond to this (repeated) scenario?

FEDERAL REGISTER

Vol. 80 Wednesday,
No. 241 December 16, 2015

Part II

Department of Transportation

Federal Motor Carrier Safety Administration

49 CFR Parts 385, 386, 390, and 395
Electronic Logging Devices and Hours of Service Supporting Documents; Final Rule

a.k.a. the
"ELD Mandate"

49 CFR
Parts 385, 386, 390, and 395

"SUMMARY: The Federal Motor Carrier Safety Administration (FMCSA) amends the Federal Motor Carrier Safety Regulations (FMCSRs) to establish:

- Minimum performance and design standards for hours-of-service (HOS) electronic logging devices (ELDs);
- requirements for the **mandatory use** of these devices by drivers currently required to prepare HOS records of duty status (RODS);
- requirements concerning HOS supporting documents;
- and measures to address concerns about harassment resulting from the mandatory use of ELDs.

The requirements for ELDs will improve compliance with the HOS rules."

ELD Self Certification and Integration

1. Scope and Description

(a) This appendix specifies the minimal requirements for an electronic logging device (ELD) necessary for an ELD provider to build and **certify** that its technology is compliant with this appendix.

1.4. System Design

(a) An ELD is integrally synchronized with the engine of the CMV such that driving time can be automatically recorded for the driver operating the CMV and using the ELD.

Bridging the Air Gap Defenses

- Adding Internet Connectivity
- Adding Bluetooth and USB 2.0

In consideration of the comments, FMCSA revised the data transfer options, by establishing two options for electronic data transfer (option one is a telematics-type ELD with a minimum capability of electronically transferring data via wireless Web service, and email; option two is a "local connectivity" type ELD with a minimum capability of electronically transferring data via USB 2.0 and Bluetooth). Additionally, both types of ELDs must be capable of displaying a

1. Comments to the 2014 SNPRM

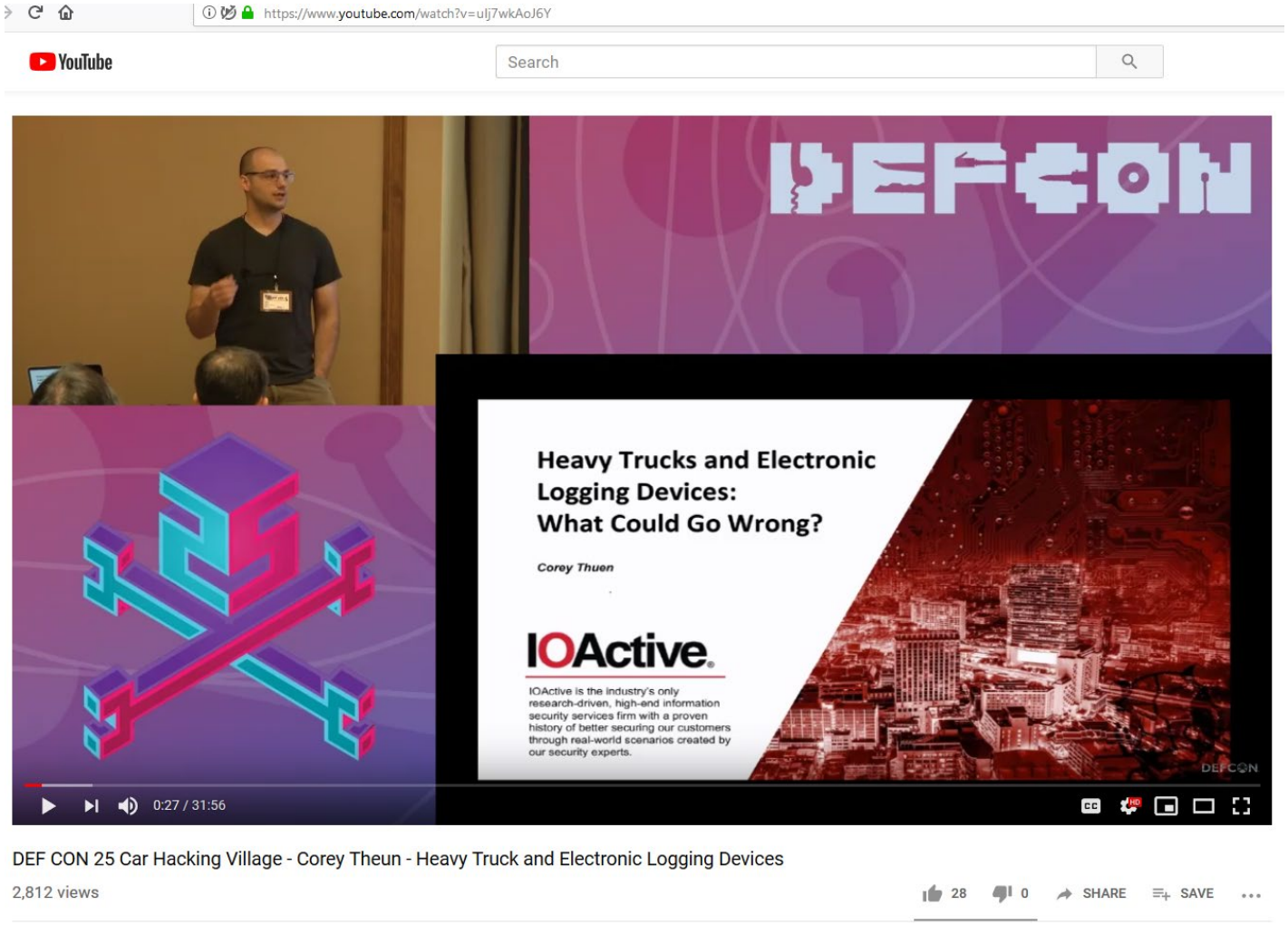
Proposed section 4.10.1 provided that ELDs must transmit records electronically in accordance with a specified file format and must be capable of a one-way transfer of these records to authorized safety officials upon request. Proposed section 4.10.1.1 described the standards for transferring ELD data to FMCSA via Web services.

BigRoad stated that section 4.10.1.1 describes how an ELD provider must obtain a public/private key pair compliant with NIST SP 800 32. Using a private key in this scenario is not ideal since it would have to be stored on every ELD that might create the email and is therefore exploitable via memory inspection or code disassembly.

2. FMCSA Response

All required security measures for data transfer with the Agency, public or private, will require strict adherence to NIST for all data in transit or 'handshakes' between Government and private systems. DOT guidelines follow NIST 820. The exact Public Key Infrastructure (PKI) for ELD data transfers will be distributed once ELD providers register and certify ELDs.

Mandated Electronic Logging Devices (ELDs) May Not Be Secure



https://www.youtube.com/watch?v=ulj7wkAoJ6Y

What can we do?

- ELDs are required on most trucks from year 2000 to present.
- Air gap defenses no longer exist.
- Older vehicles may have single CAN bus (SAE J1939) for all ECUs.
- There is a race to the bottom… What is the cheapest ELD that we can buy?

BYOD

How to pick a secure ELD?

Conspicuously Absent

- The checklist discusses data protections, but not equipment (i.e. truck) protections
- Could include the following item in the checklist:

  Have the vendor demonstrate protections from affecting the CAN bus in an unintended manner.

- Problem: How can we protect the CAN bus when we are forced to expose it to aftermarket or third-party devices on legacy systems?

BTW: this applies to insurance incentives to install dongles too.

Conclusion

There are many attack surfaces.

Have fun and go hack a truck!

P.S. You are under an NDA…
hack to help improve the industry.