

# Education for Heavy Vehicle Security

---

Dr. Jeremy Daily

Associate Professor of Systems Engineering

[Jeremy.Daily@colostate.edu](mailto:Jeremy.Daily@colostate.edu)



SYSTEMS ENGINEERING  
COLORADO STATE UNIVERSITY

# Agenda

- Vehicle Network Security and J1939
- Student Projects
  - Advanced Protocol Attacks
  - Software Defined Truck
- PIVOT: Platform for Innovative Use of Vehicle Open Telematics
- CyberTruck Challenge





# Heavy Vehicle Networking using SAE J1939



Volvo SuperTruck 2018

# Presentation Goals

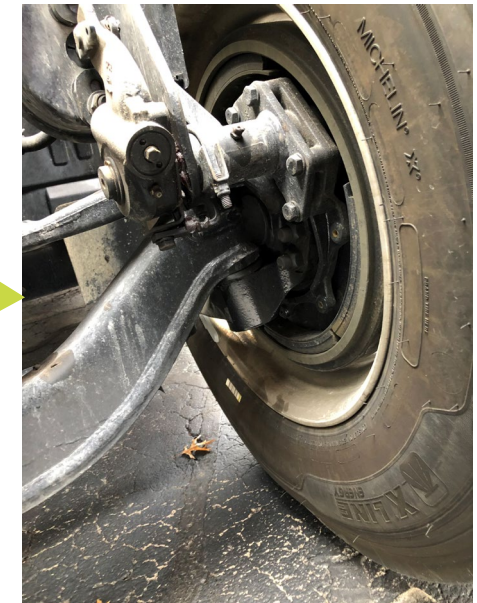
- Understand the need for in-vehicle communication using CAN and SAE J1939
- Connecting to J1939 Networks
- Interpret J1939 network traffic using the SAE Standard
- Recognize SAE J1939 Transport Protocols for larger messages
- Introduction to J1939 Address Claiming
- Realize J1939 is inherently an open (and potentially insecure) read-write bus





# Truck Systems

- Primary Functions
  - Go – Convert fuel into mechanical energy to accelerate heavy loads
  - Stop – Brake the tractor-trailer systems, often with anti-locking air brakes
  - Steer – Give the driver the ability to guide the vehicle
  - Haul – Support heavy loads and pull trailers
- Additional Functions
  - Protect – Restrain occupants in a crash. Assist drivers to avoid crashes.
  - House – Provide places to sleep while on a long haul
  - Entertain – Radio, CDs, Bluetooth, and Satellite options
  - Monitor – Telematics and fleet management
  - Diagnose – Provide information related to vehicle operation and potential faulty parts
  - Comply – US DOT regulation, EPA and emissions regulations





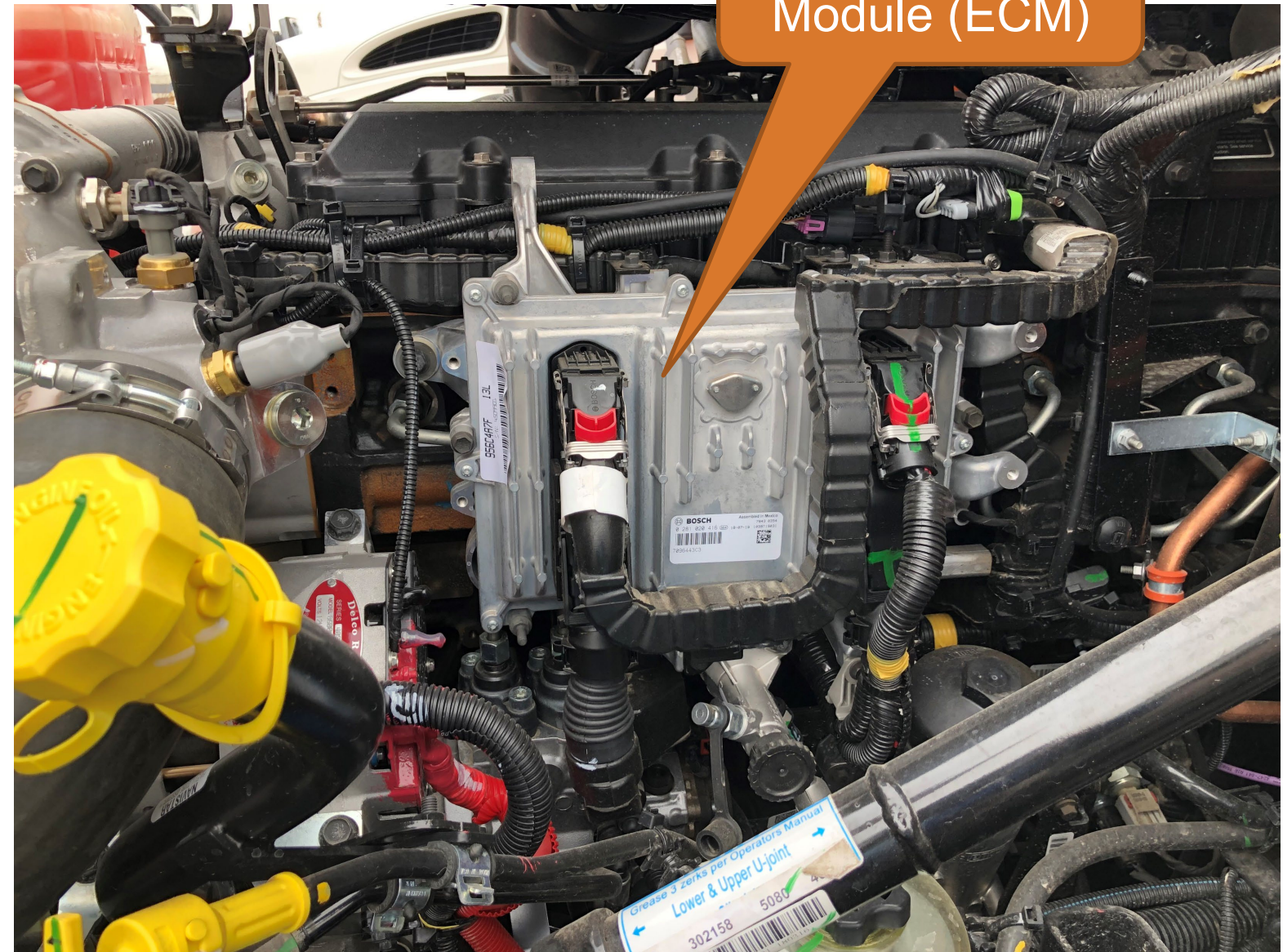
# Truck Engines

- Primary function to efficiently produce motive power

Also:

- Comply with emission requirements
- Aid diagnostics and troubleshooting
- Record driving and diagnostic events
- Provide additional power for
  - Compressed Air
  - Power take off (PTO) equipment
  - Electrical systems

**Computer controls are paramount to realize these functions**



The driver's side of a Navistar A26 Engine in an International LT truck.

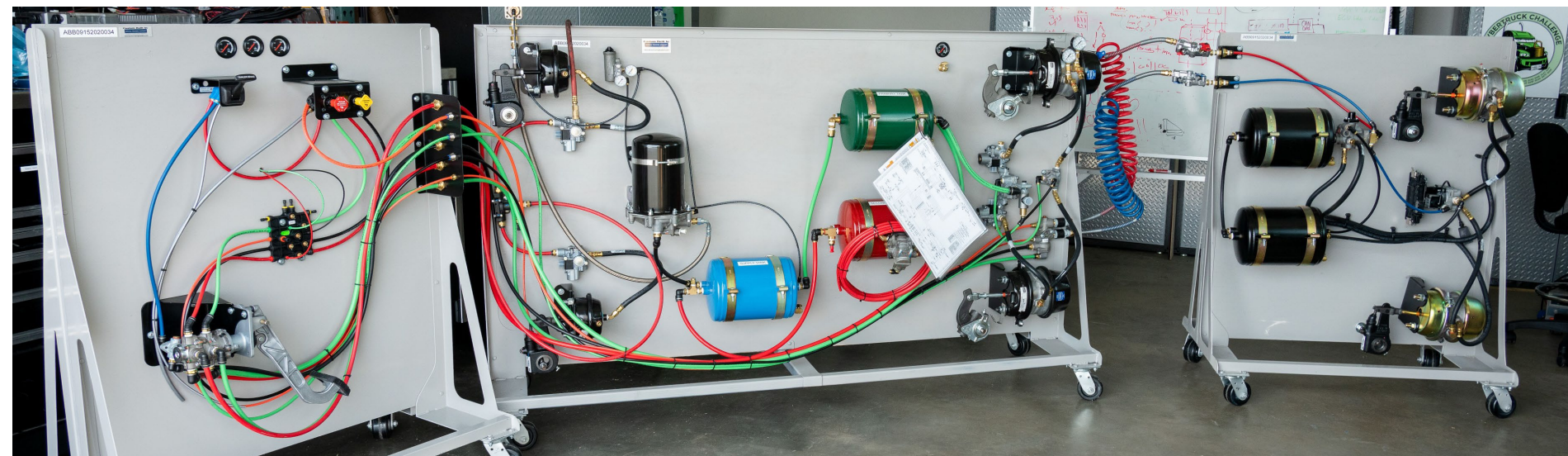


# Electronic Brake Controllers

1. Sense wheel speeds
2. Determine if wheel lock-up is impending
3. Modulate the air pressure to the brake chambers
4. Tell the engine to stop producing torque



[store.partshighway.com](http://store.partshighway.com)



# In-Vehicle Networking

How does the Brake Controller communicate with the Engine Controller?



# Controller Area Network (CAN) in Trucks

In the Diagnostic Port



Pin C: CAN-High  
Pin D: CAN-Low

Yellow: CAN-High  
Green: CAN-Low

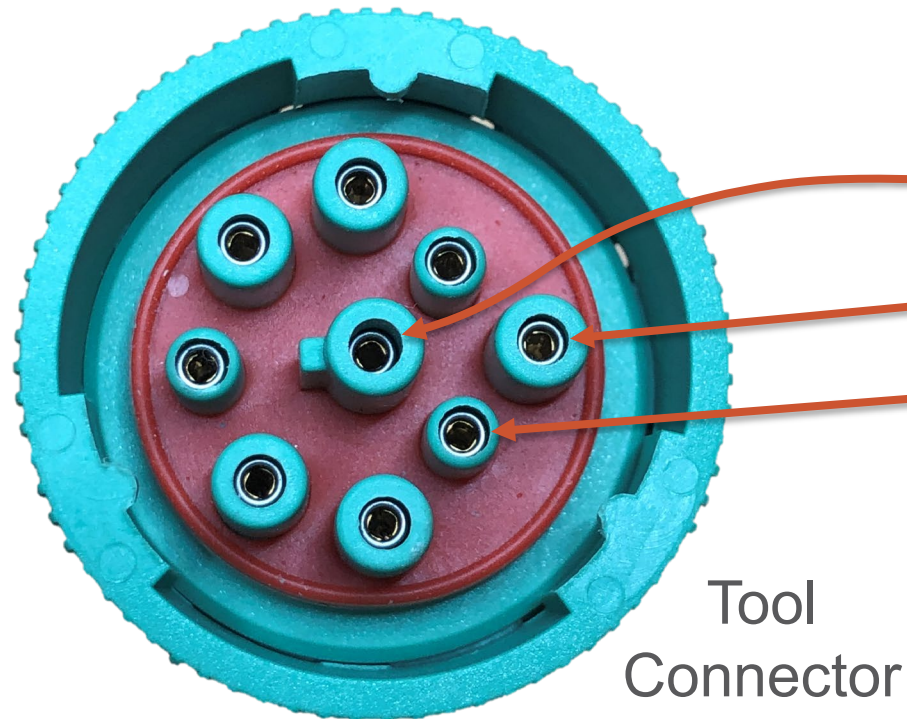
In the wiring harness



The CAN bus is typically a twisted-pair of copper wire connecting the ECUs.

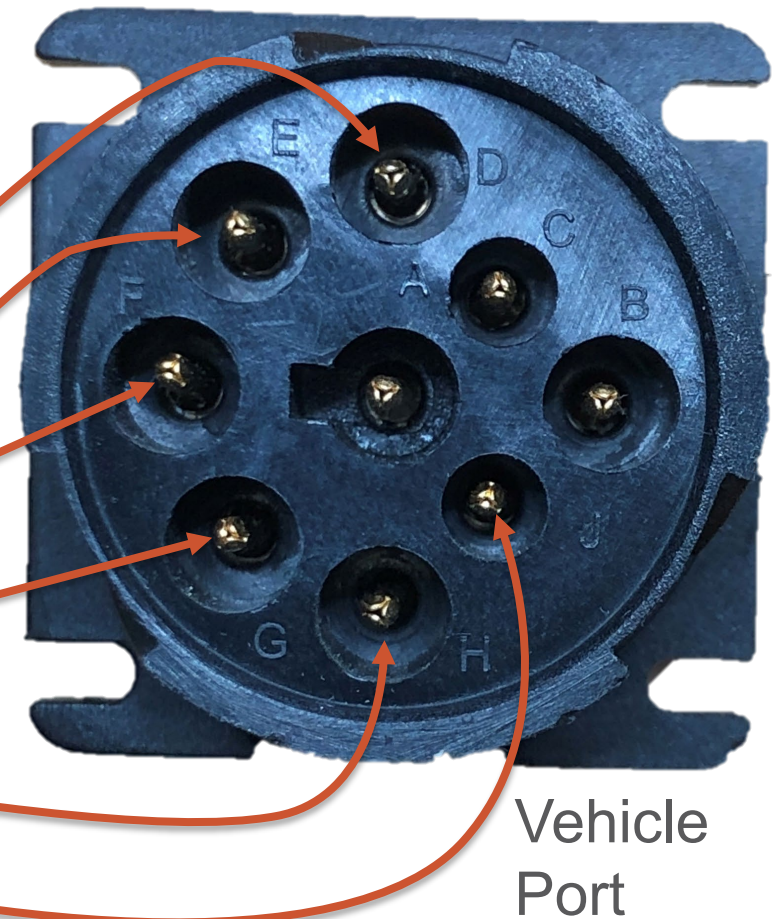
# Diagnostic Connector Pinouts – SAE J1939

Not all trucks are the same (Volvo uses J1962 connector)



250k - Black Connector  
500k - Green Connector  
Green goes into Black  
Black cannot plug into Green

Pin	Signal
A	Ground
B	Vbatt (+12V)
C	J1939 High
D	J1939 Low
E	Shield
F	J1708 A(+)
G	J1708 B(-)
H	CAN2 High
J	CAN2 Low

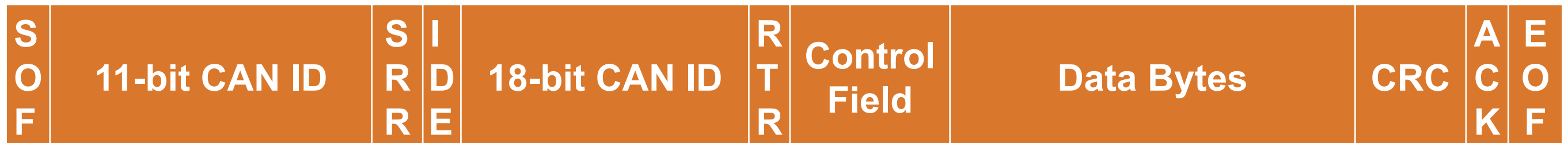




# Controller Area Network

- Introduced by Bosch in the 1980s
- Multi-master priority-based bus access with non-destructive message arbitration
- Utilizes a 15-bit cyclic redundancy check (CRC) to reliably detect transmission errors
- Reliable delivery is built in with an acknowledgement bit at the end of the frame
- Low latency with up to 8 bytes of data per frame (Classic CAN)
- Bit rates up to 1 Mbit/second
  - CAN-FD promises 8 Mbit/sec
- Required on all passenger cars for emission compliance starting in 2008 (Standard 11-bit CAN ID)
- Utilized by SAE J1939 as the foundational networking protocol in the 1990s ()

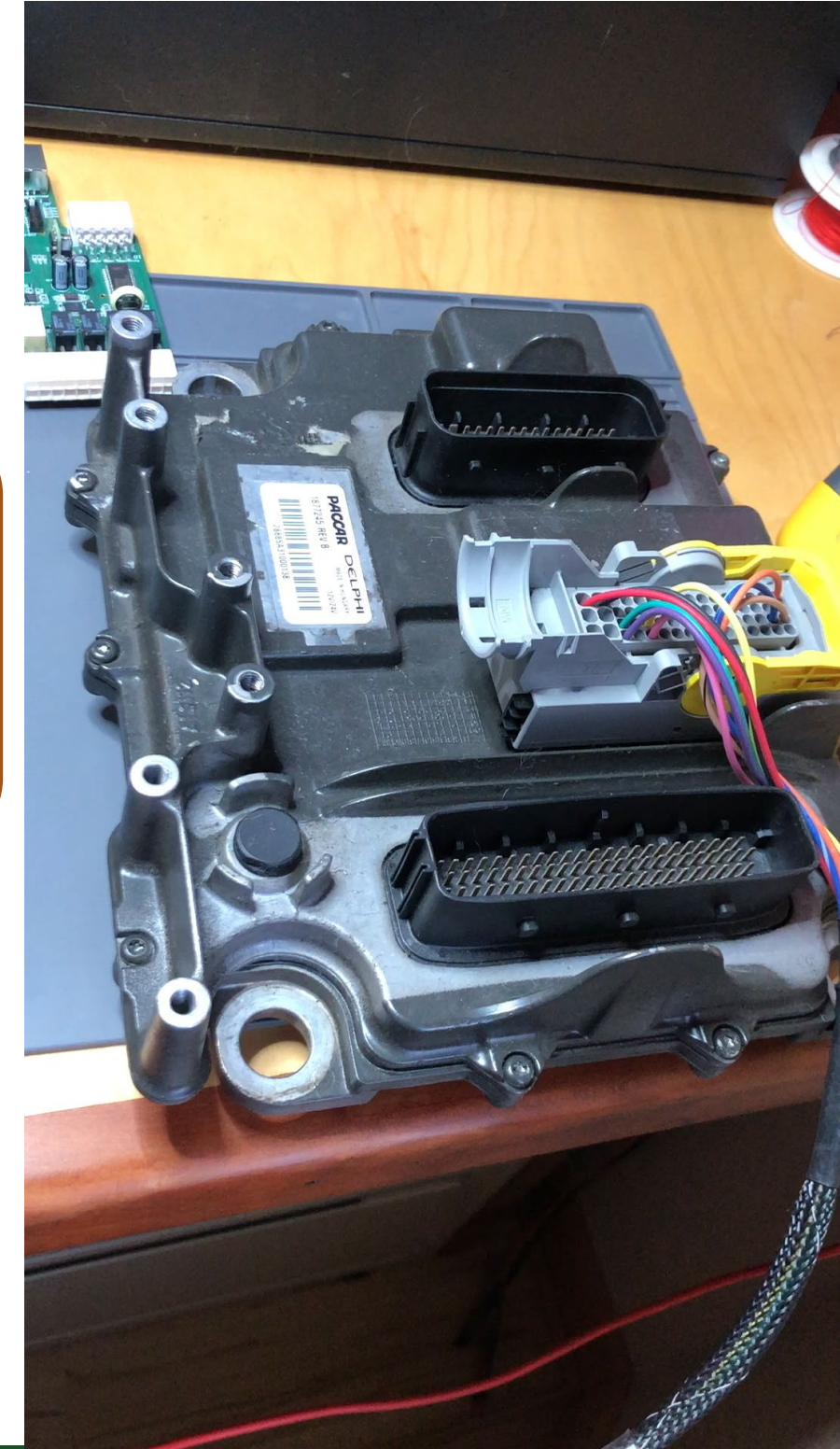
## Extended 29-bit CAN Frame



# CAN Signaling: Measurement Example

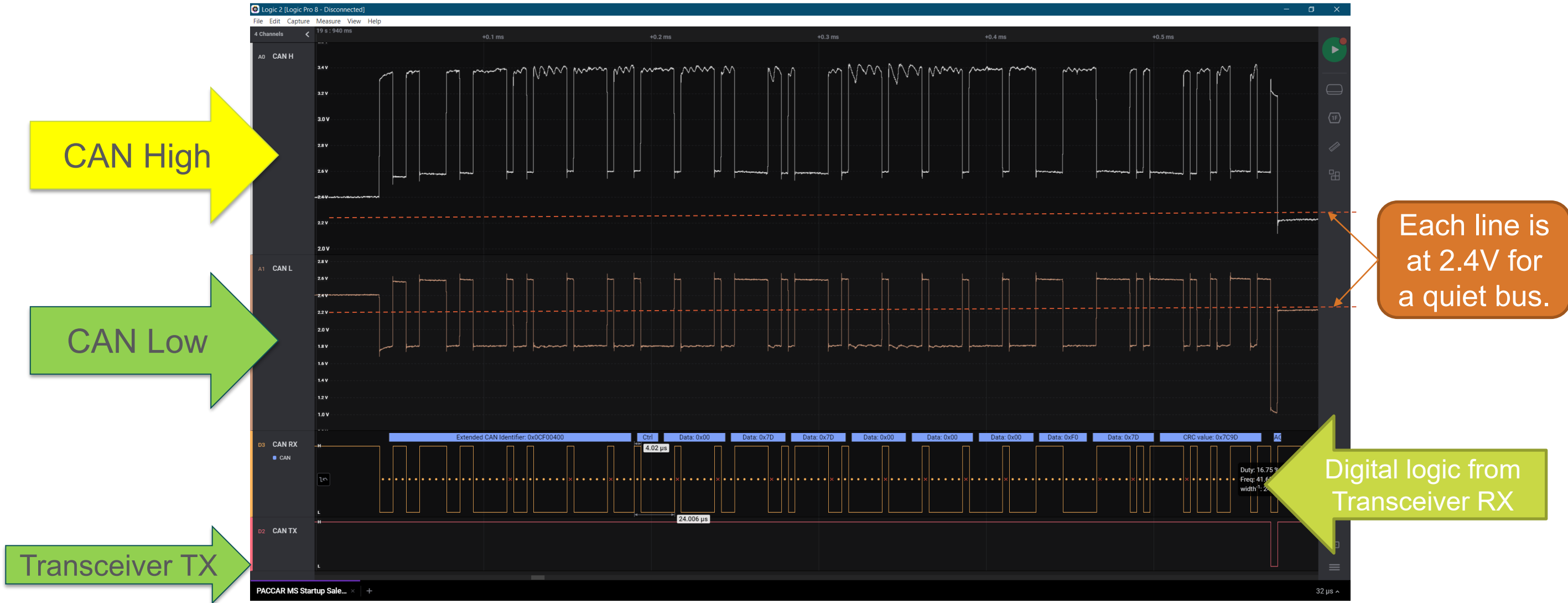
- PACCAR MX Engine Control Module (ECM)
- Synercon Technologies Smart Sensor Simulator
  - Completes the CAN network circuit
  - Provides connectivity for the ECM
- DG Technologies J1939 Breakout Box
- Raspberry Pi with a CAN-FD Hat
  - Runs embedded Linux with SocketCAN
  - Records CAN traffic using `can-utils candump` command
- Fluke Scope Meter as an Oscilloscope
  - Measures voltage traces between CAN High and CAN Low
- Saleae Logic Probe
  - Analog Voltage measurements (duplicating the oscilloscope)
  - Digital measurements from the CAN Transceiver
  - CAN signal decoding features
  - PC application interface

What is on the wire?  
Let's monitor the  
yellow CAN-H and  
green CAN-L lines.



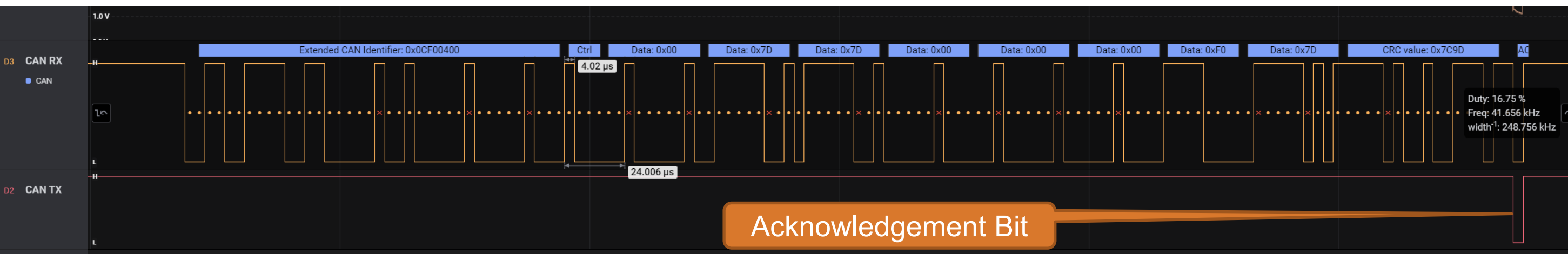


# CAN Signaling: Single Frame



# CAN Measurements Observations

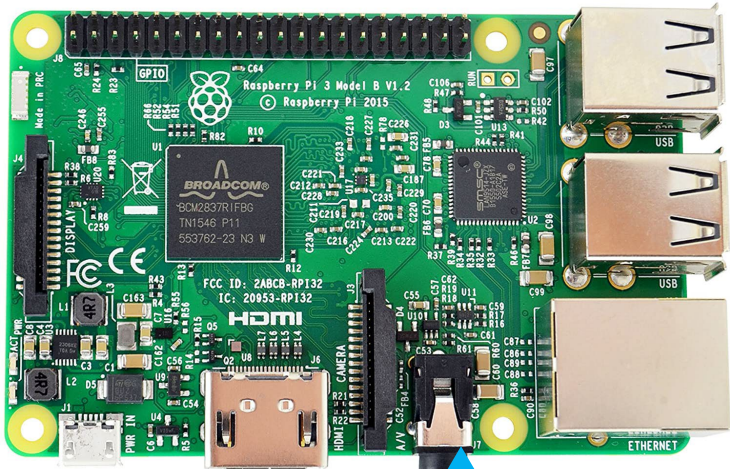
- A bit time is about 4 microseconds. This is 1/250000.
- Data that has all zeros still has extra bits in the field. These are called stuff bits.
- Stuff bits are inserted after 5 sequential bits of the same value.
- At the end of the message, A bit is seen on the TX line, which indicates an acknowledgement the message was received.
- The total message length is about 500us.
- Signaling is non-return-to-zero (NRZ).



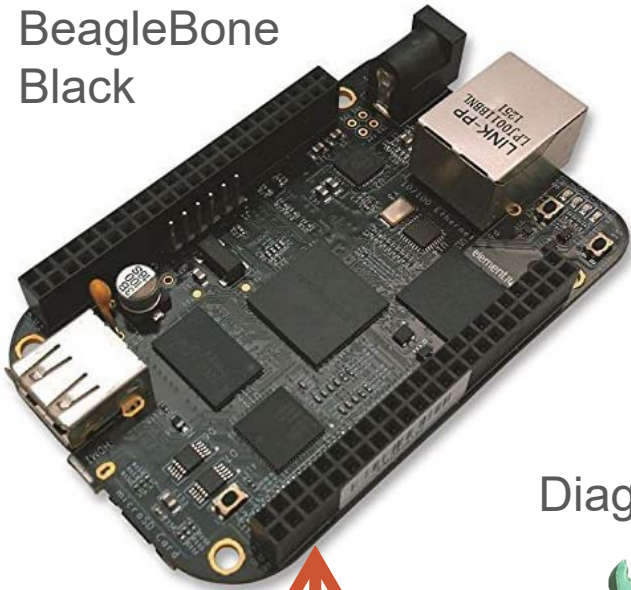


# CAN Enabled Embedded Linux Hardware

Raspberry Pi



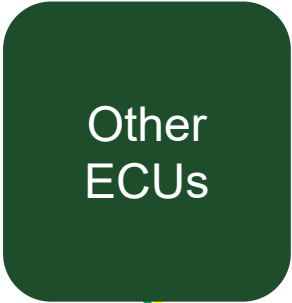
BeagleBone Black



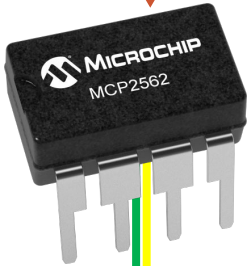
CAN Controller



Other ECUs



CAN Transceiver



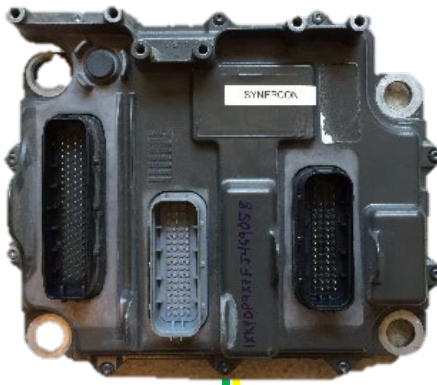
Diagnostics Port



Brake Controller



Engine Control Module



120 Ω

120 Ω

# Connecting to a Truck and Reading Data

- Check the bitrate of the physical channel:
  - `ip -details -statistics link show can1`
- Change bitrate to match system:
  - `sudo ip link set can1 down`
  - `sudo ip link set can1 type can bitrate 500000`
  - `sudo ip link set can1 up`
- Log the can data to a file:
  - `candump -l -e any`







# Creating Meaning from Messages

How do we get engineering values from J1939 Protocol Data Units?

# SAE J1939 is Built on CAN

The main features that define J1939 are:

- A standardized meaning for 29-bit arbitration identifiers.
- A mechanism for sending messages larger than 8 bytes (up to 1785 bytes) using the transport protocol.
- The ability for a controller application to negotiate a unique source address.

	<b>SURFACE VEHICLE RECOMMENDED PRACTICE</b>		<b>J1939 JUN2012</b>
		Issued	2000-04
		Revised	2012-06
		Superseding J1939 APR2011	
Serial Control and Communications Heavy Duty Vehicle Network - Top Level Document			



# J1939 Network Layers

Layer	Name	Standard	Description and Purpose
7	Application	SAE J1939-71 (Applications) SAE J1939-73 (Diagnostics)	Defines how to interpret and compose J1939 messages with engineering values
6	Presentation	Not Used These services are built into the Data Link Layer.	
5	Session		
4	Transport		
3	Network	J1939-31	Clarifies the concept of a gateway between two separate networks.
2	Data Link	J1939-21	Describes how to make a J1939 PDU. Includes details on sending messages up to 1785 bytes long.
1	Physical	J1939-1X	Defined connectors, transceivers, wiring, pinouts, and signaling.

# SAE J1939 Standards Organization

- Follows the OSI 7-layer model for naming, e.g.:
  - J1939-7X are for application layers
  - J1939-1X are for physical layers
- The standard collection adds much more definition to the CAN communications
- Includes additional “Layers”
  - J1939-8X Network Management
  - J1939-9X Network Security
- J1939 is large and not free
- J1939 Accommodates Extensions
  - PGN 0xEF00 is Proprietary A
  - PGN 0xFFXX is Proprietary B
  - PGN 0xDA00 is ISO-15765 (UDS)
- A Digital Annex (J1939DA) has the applications defined in an Excel spreadsheet

## Recommendation:

- Acquire the Digital Annex first.
- Read J1939-21 for details on the PDU

### SAE J1939 Standards Collection

The J1939 Standards subscription is the easiest and most cost-effective way to access SAE's family of standards relating to the Controller Area Network (CAN) for heavy-duty vehicles.

The SAE J1939 standards in this collection define a high-speed CAN (ISO 11898-1) communication network that supports real-time, closed-loop control functions, simple information exchanges, and diagnostic data exchanges between electronic control units throughout the vehicle. It is considered the CAN solution of choice for applications in the construction, fire/rescue, forestry, materials handling, and on-highway sectors.

[Learn more about J1939 Standards](#)


**How to Purchase:** Flexible purchase options and volume discounts are available for single and multiple users. Please contact the SAE Sales Team directly at:

SAE Sales Team  
[customersales@sae.org](mailto:customersales@sae.org)  
1-888-875-3976 (U.S. and Canada)  
1-724-772-4086 (Outside the U.S.)

[https://www.sae.org/publications/collections/content/j1939\\_dl/](https://www.sae.org/publications/collections/content/j1939_dl/)

### SAE MOBILUS

This product is available for a free 30-day trial. [Take the Free Trial »](#)

 Subscription  
**\$1,160.00**

[Add to Cart](#)



# Data Decoding and Encoding: Meaning for Bits and Bytes

- Common data sizes
  - Bit Mapped, like Switch States, (2-bits)
  - Single Byte Data (8-bits)
  - 2-byte Data (16 bits)
  - 4-byte Data (32 bits)
  - ASCII data (variable)
- Exceptions:
  - Field data, engine maps
  - Suspect Parameter Numbers (19 bits)
  - Failure Mode Indicators (5 bits)
  - Others...
- Scale, Limits, Offsets, Transfer (SLOTs)

Identifier	SLOT Name	SLOT Type	Scaling	Range	Offset	Length
1	SAEpr11	Pressure	5 kPa/bit	0 to 1,250 kPa	0	1 byte
2	SAEpr13	Pressure	8 kPa/bit	0 to 2,000 kPa	0	1 byte
3	SAEtm11	Time	1 h/bit	0 to 250 h	0	1 byte
4	SAEtm10	Time	1 h/bit	-125 to 125 h	-125 h	1 byte
5	SAEtm12	Time	1 h/bit	-32,127 to 32,128 h	-32,127 h	2 bytes
6	SAEtm06	Time	1 s/bit	0 to 4,211,081,215 s	0	4 bytes
7	SAEad01	Angle/Direction	0.0000001 deg/bit	-210 to 211.1081215 deg	-210 deg	4 bytes
⋮	⋮	⋮	⋮	⋮	⋮	⋮



# J1939 Transport Protocol

How can we send messages larger than 8 bytes in a CAN frame?



# J1939 Transport Protocol

- Data more than 8 bytes in length requires multiple CAN frames to send the data.
- Two Approaches that follow PDU formats
  - Request to Send/Clear to Send (RTS/CTS) – point-to-point messaging
  - Broadcast Announce Message (BAM) – global address
  - Approach is determined with the first byte of the Connection Management Message
    - If 32 (0x20), then BAM
    - If 16 (0x10), then RTS
    - If 17 (0x11), then CTS
- Three Parameter Groups to track
  - Transport Protocol – Connection Management (TP.CM), PGN 60416 (0xEC00)
  - Transport Protocol – Data Transfer (TP.DT), PGN 60160 (0xEB00)
  - PGN of the data being transported

Details are in  
SAE J1939-21

# J1939 Transport Protocol VIN Example

The following data were on J1939:

- |   | <u>CAN ID: CAN Data (in hex)</u>  |
|---|-----------------------------------|
| • | 1CECFF00: 20 12 00 03 FF EC FE 00 |
| • | 1CEBFF00: 01 31 58 4B 59 44 50 39 |
| • | 1CEBFF00: 02 58 37 46 4A 34 36 39 |
| • | 1CEBFF00: 03 30 35 38 2A FF FF FF |

- Parse the CAN ID into J1939 parameters:
  - 0x1C000000 -> Priority = 7 (lowest)
  - 0x00EC0000 -> PGN = 60416 (TP.CM)
  - 0x00EB0000 -> PGN = 60160 (TP.DT)
  - 0x0000FF00 -> Destination = 255 (Global)
  - 0x00000000 -> Source Address = 0 (Engine 1)

# J1939 Transport Protocol VIN Example (cont.)

- Transport Protocol – Connection Management

- 1CECFF00: 20 12 00 03 FF EC FE 00

- 20 – Control Byte = BAM
- 12 00 – Message size (18 bytes)
- 03 – Number of packets (3)
- EC FE 00 – PGN of message (0x00FEEC = 65260 Vehicle Identification)

- **Connection Mode: BAM**

- Byte 1: Control byte = 32 (0x20), Broadcast Announce Message (BAM)
- Bytes 2,3: Total message size, number of bytes (Big Endian or reverse byte order)
- Byte 4: Total number of packets
- Byte 5: Reserved (0xFF)
- Bytes 6,7,8: Parameter Group Number of the packeted message (Big Endian)

- Note: The destination on a BAM is often 255 for all the nodes.



# J1939 Transport Protocol VIN Example (cont.)

- Transport Protocol – Data Transfer

- 1CEBFF00: 01 31 58 4B 59 44 50 39
- 1CEBFF00: 02 58 37 46 4A 34 36 39
- 1CEBFF00: 03 30 35 38 2A FF FF FF
  - NN – Sequence Number (01 to FF)
  - Data totaling the number of bytes in TC.CM
  - FF FF FF – Filler for an 8-byte message
- A maximum of 255 messages with 7 bytes each means a total of  $255 \times 7 = 1785$  bytes maximum for each J1939 transport protocol message.

- Decoded value from ASCII:
- 31 58 4B 59 44 50 39 58 37  
46 4A 34 36 39 30 35 38 2A
- 1 X K Y D P 9 X 7  
F J 4 6 9 0 5 8 \*
- Or 1XKYDP9X7FJ469058
- (VIN is usually 17 characters, so the \* is dropped)



# RP1210 Programming

Using Diagnostic Service Tools to Connect to the Network

# RP1210 Vehicle Diagnostics Adapters

- Truck owners want only one hardware device to work with all their ECUs and diagnostics software
- American Trucking Association (ATA) and their Technology Maintenance Council (TMC) published Recommended Practice (RP) number 1210 to define a Windows API for vehicle diagnostic adapters (VDAs)



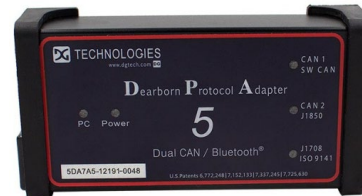
[This Photo](#) by Unknown Author is licensed under [CC BY](#)



J1939  
J1708



Nexiq USB Link 2



DG DPA 5 Pro



Noregon DLA +

USB  
Bluetooth  
WiFi



Service  
Computer



# RP1210 Function Prototypes

Function Name	Description
RP1210_ClientConnect (...)	Load the routines for a particular protocol on the correct channel
RP1210_SendCommand(...)	Send command to change the behavior or property of the VDA
RP1210_SendMessage (...)	Send a message through the VDA to the vehicle network
RP1210_ReadMessage (...)	Read a message from the vehicle network
RP1210_ClientDisconnect (...)	Disconnect the client and close the driver

- The message structure depends on the type of client
  - J1939
  - CAN
  - J1708

RP1210 Log files are helpful to understand diagnostic communication.

<https://www.atabusinesssolutions.com/Shopping/Product/viewproduct/2675472/TMC%20Individual%20RPs>

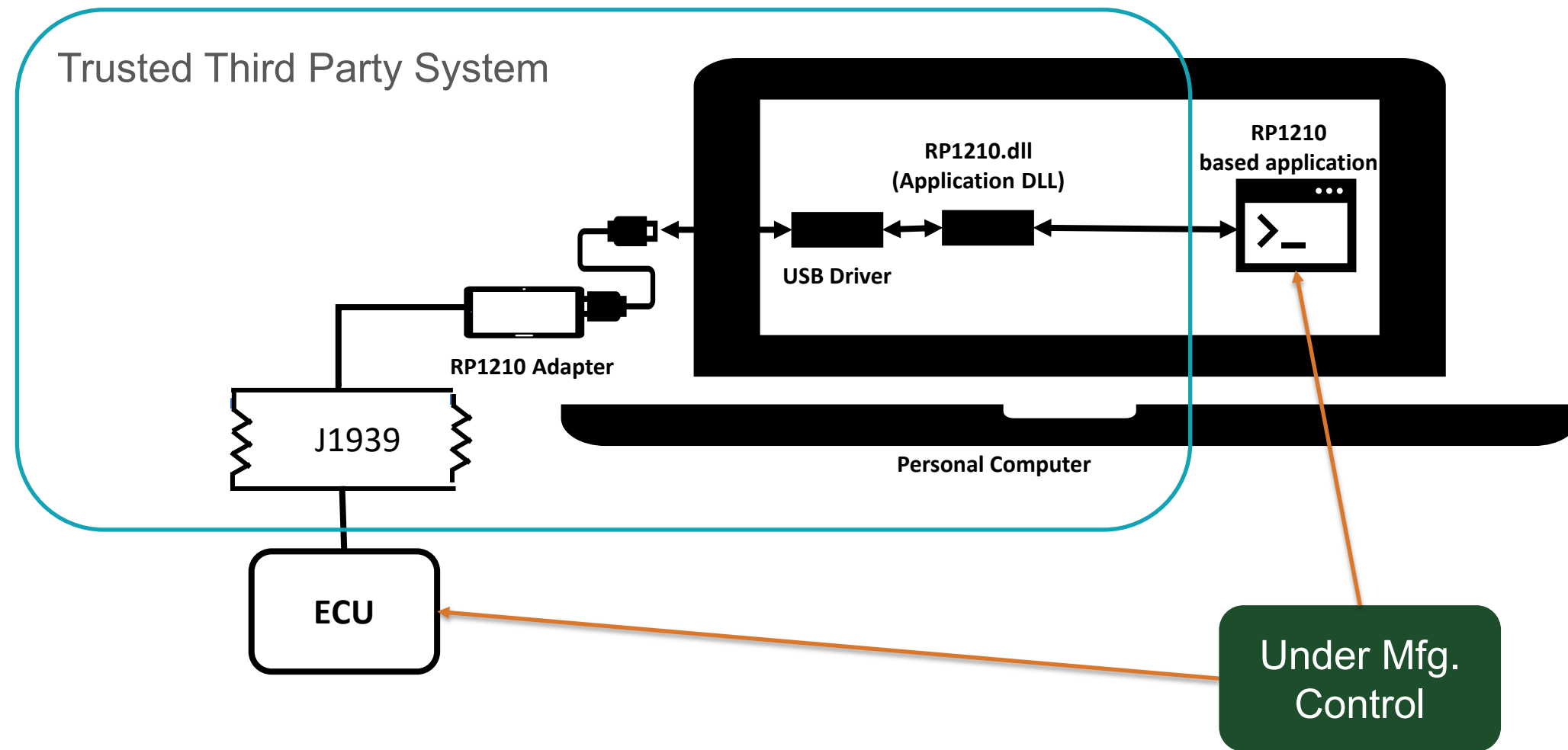
# RP1210 Log File Example

## DG Technologies DPA5

```
FT:0011,AT:0030  XX,CC,00,02,001,J1939:Baud=Auto,0,0,0
Exe Name: C:\PROGRAM FILES (X86)\CUMMINS\POWERSPEC5\POWERSPEC.EXE :Thu Jan 13 13:05:10 2022
FT:0000,AT:0000  02,SC,00,17,45,35,30,30,30,30,30,00,00,00,00,00,00,00,00,00,00,00
FT:0000,AT:0000  02,SC,00,1,18,00
FT:0001,AT:0001  02,SC,00,7,4,0d,00,ef,00,ff,00,fa
FT:0000,AT:0000  02,SC,00,1,18,01
FT:0252,AT:0252  02,SC,00,10,19,fa,d6,eb,56,01,00,81,00,00,00
FT:0000,AT:0000  02,SM,00,15,0,0,00,ef,00,06,fa,00,81,02,01,01,ff,01,ff,00,00,
FT:0265,AT:0013  02,RM,19,4104,1,00,01,9b,da,00,ef,00,00,00,fa,81,01,02,00,01,70,01,05,30,
FT:0000,AT:0000  02,SM,00,15,0,0,00,ef,00,06,fa,00,81,00,03,00,00,01,01,00,00,
FT:0027,AT:0027  02,RM,23,4104,1,00,01,9b,f3,00,ef,00,00,00,fa,81,00,03,01,01,01,02,01,00,7f,04,28,31,
```

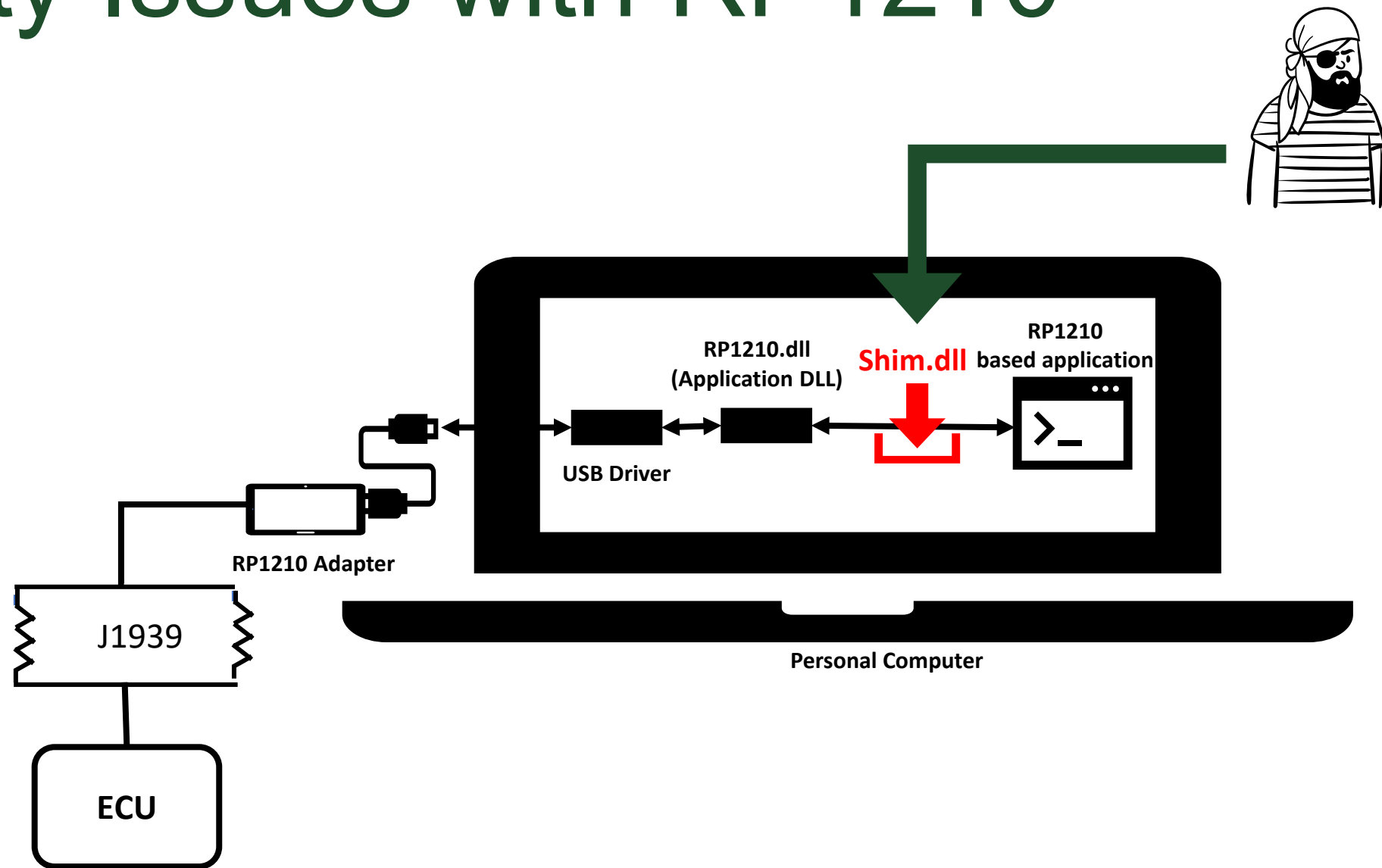
CC – Client Connect	SM – Send Message
SC – Send Command	RM – Read Message

# Security Issues with RP1210





# Security Issues with RP1210



```

short FUNCTION_MODIFIER RP1210_ReadMessage (short nClientID,
                                             char far *buf,
                                             short nBufferSize,
                                             short nBlockOnRead)
{
    int writeSize;
    if(xx_DLL.functions.readMessage)
    {
        status = xx_DLL.functions.readMessage( nClientID,
                                                buf,
                                                nBufferSize,
                                                nBlockOnRead);
    }
    else
    {
        status = -1;
    }

    if (status > 0)
    {
        size_t i = 0
        //Total Vehicle Distance -- byte manipulations
        if ((buf[4] == 0xE0) && (buf[5] == 0xFE) && (buf[6] == 0x00)) {
            buf[14] = 0x60; //SPN 245
            buf[15] = 0xFE;
            buf[16] = 0xFF;
            buf[17] = 0xFA;
        }
        return(status);
    }
}

```

*Fake Data*

# Manipulating Engine Hours with a Shim.dll

Data can be changed  
in the device buffers.

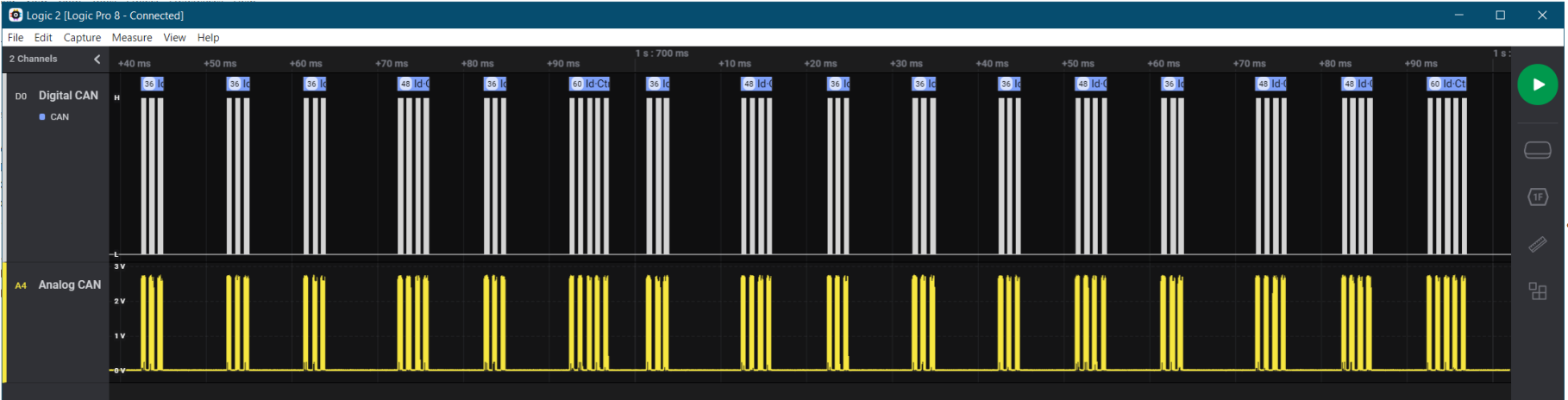


# Cybersecurity Considerations for J1939

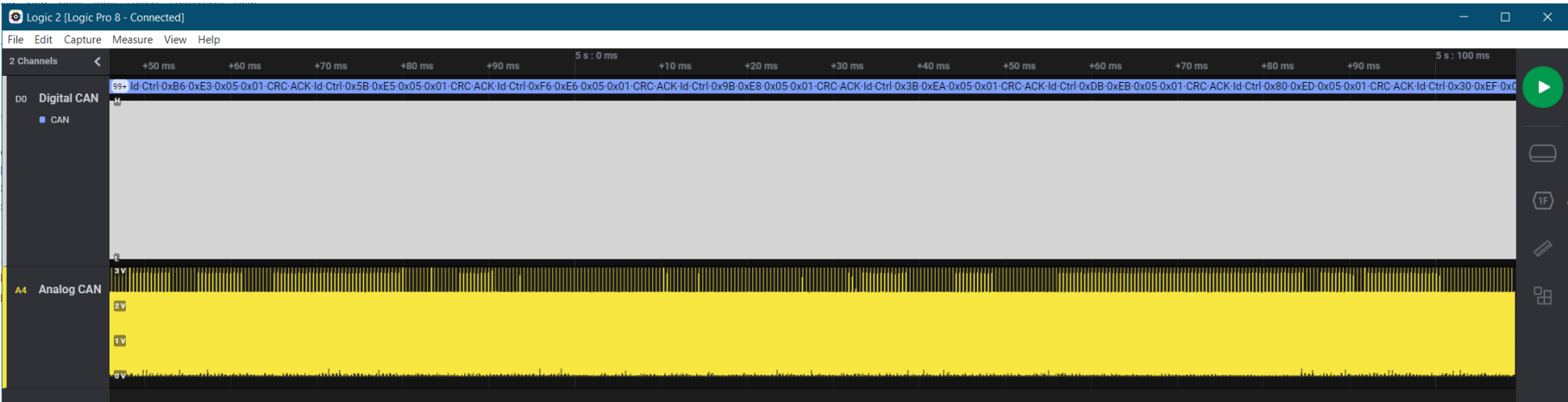
What can go wrong if a hacker gets access to the network?



# Denial Of Service

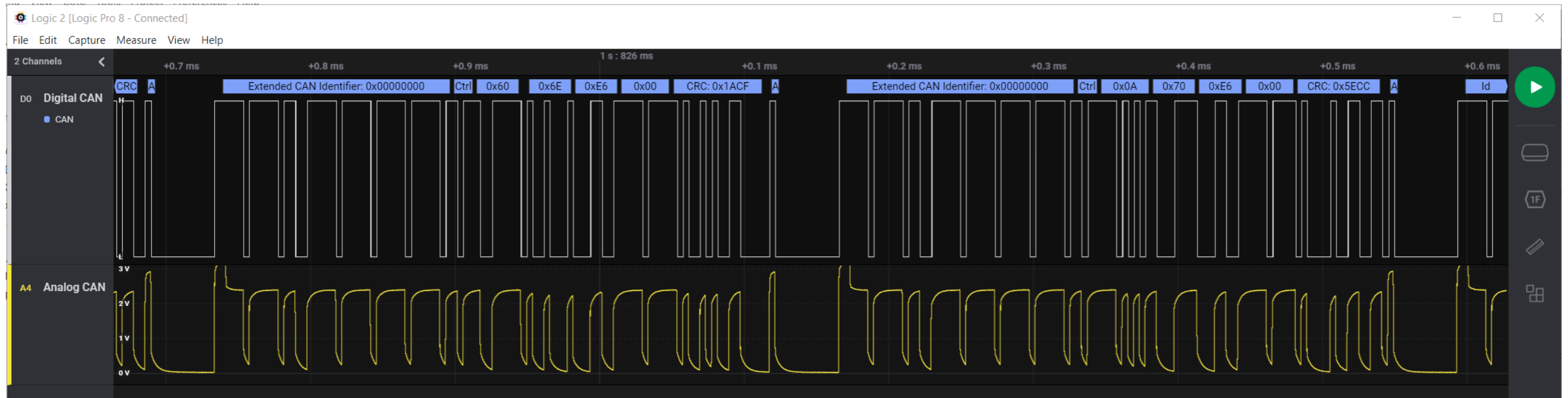


Normal J1939



Flooded J1939

# Denial of Service

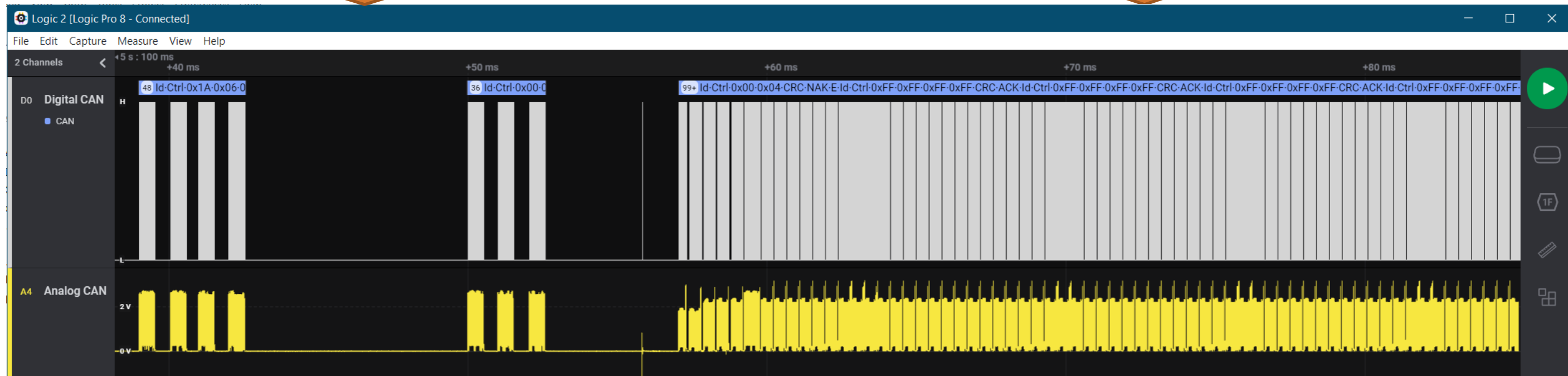


- By repeating high priority messages (ID = 0), no other legitimate message can get access to the network.
- This will shut down communications and potentially stall a truck.
- There are no native protections against this in J1939; avoid connecting unknown new devices to J1939.

# Spoofing Messages and Commands

Normal J1939

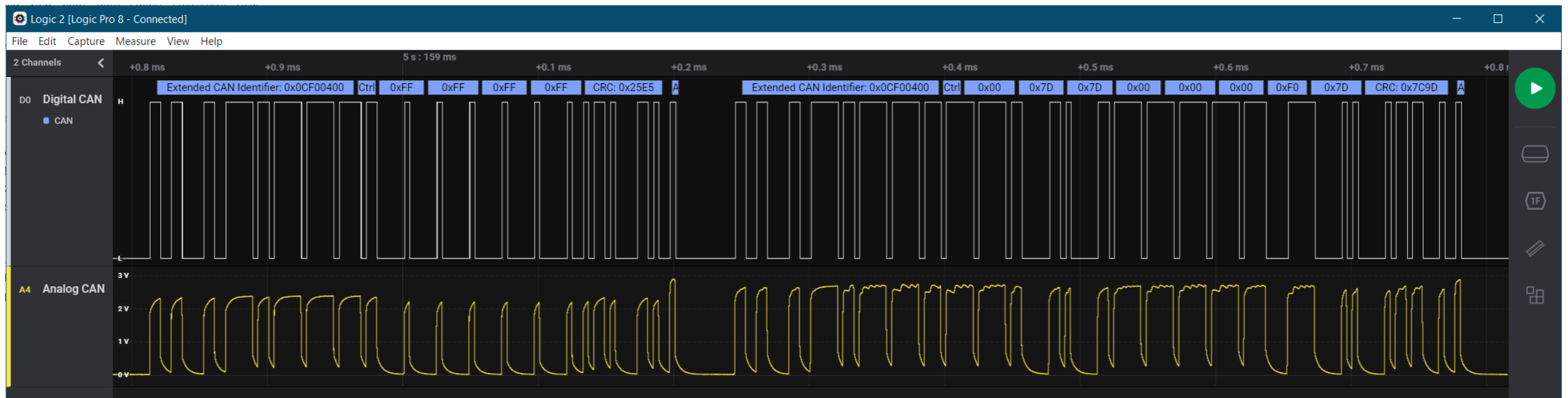
Spoofed J1939



# Spoofing Messages and Commands

- Two messages with the same IDs will be interpreted the same way
  - One message is legitimate (right)
  - The other is spoofed (left)

The network doesn't know which message is legitimate







The operator reported that the vehicle suddenly stopped working when they were sitting in traffic. There was no sign of overheating or mechanical failure

# Student Projects

J1939 Decoder (based on the NMFTA pretty-j1939 work)

J1939 Transport Protocol Vulnerabilities

Software Defined Truck

Testbed Development

# Transport Layer Vulnerabilities in SAE J1939 Protocol

---

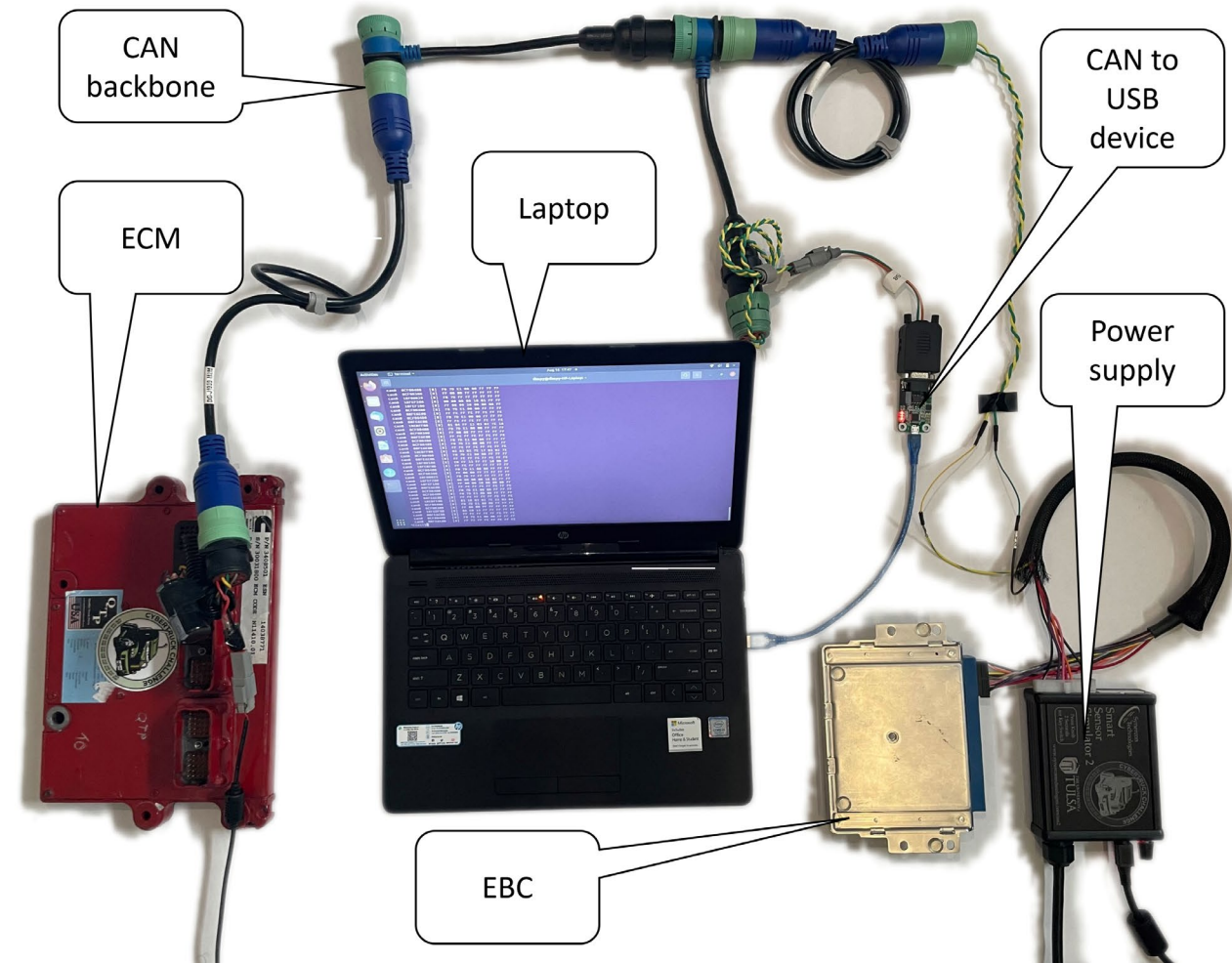
Rik Chatterjee



Colorado State University

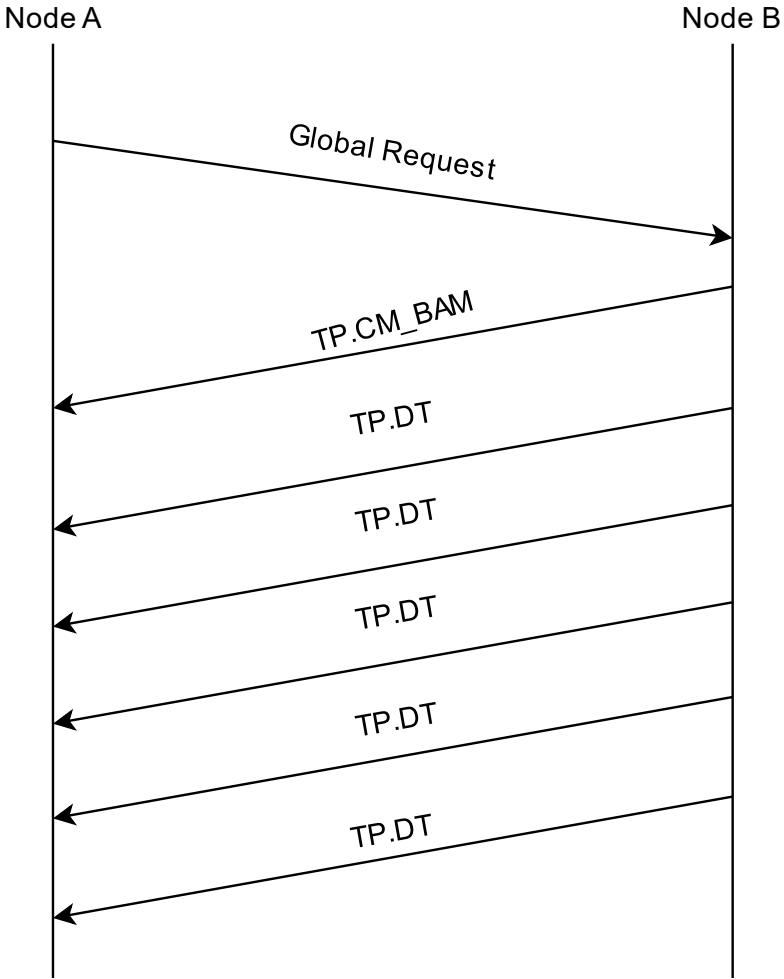
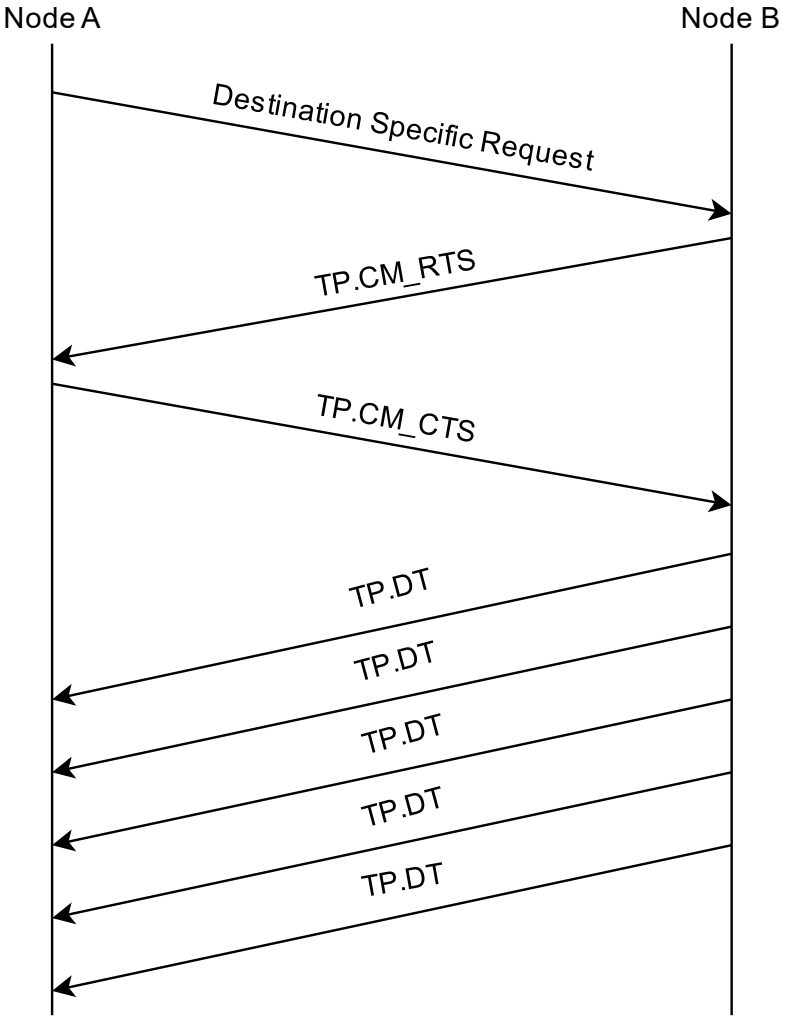
# Contents

- Experimental Testing Platforms
- Request Overload Vulnerability
- Connection Exhaustion Vulnerability
- ~~Broadcast Message Vulnerability~~
- ~~Memory Leak Vulnerability~~





# SAE J1939 Transport Protocol



# CSU Research Truck

## 2014 Kenworth T270



# Request Overload Hypothesis

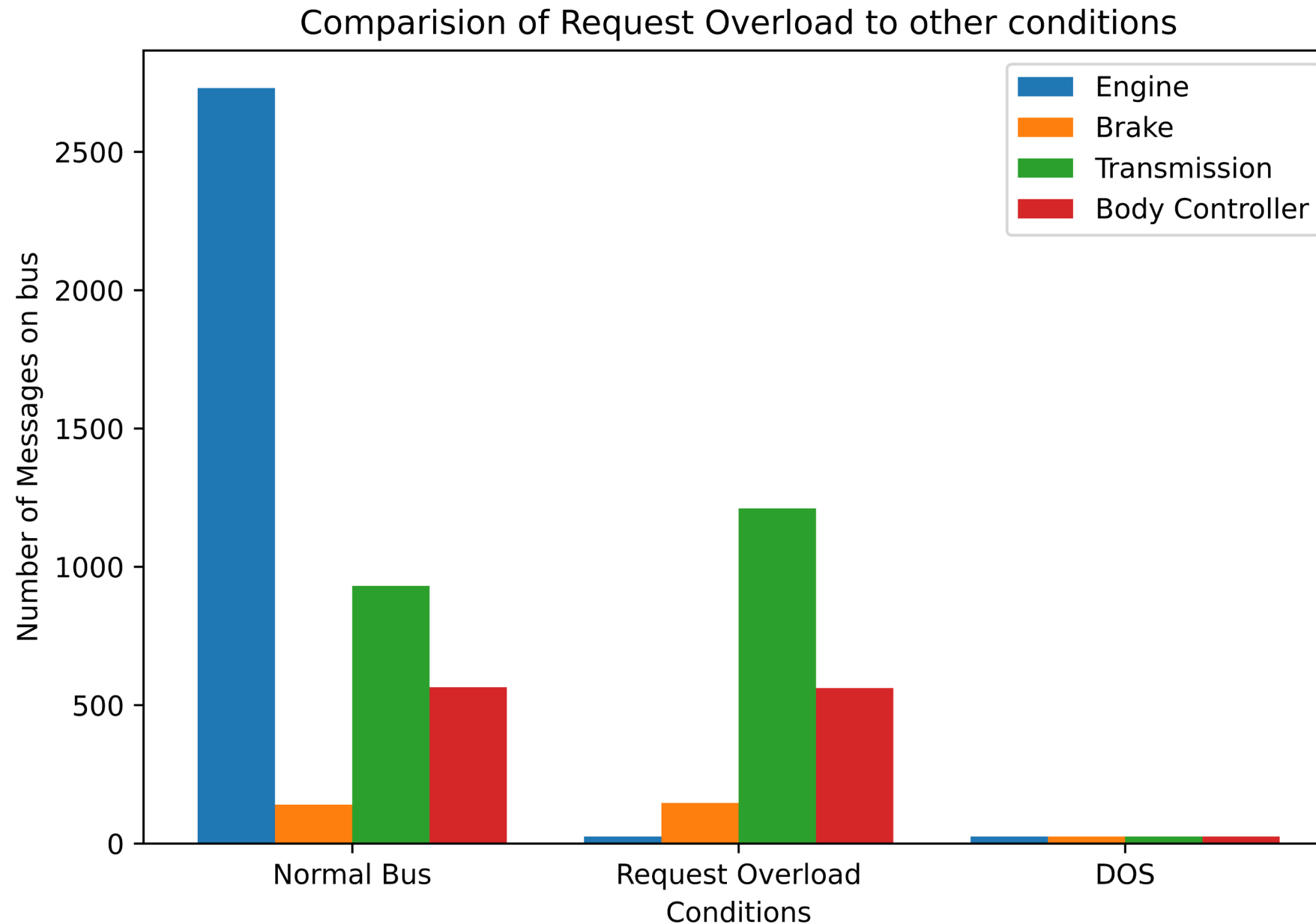
- The SAE J1939-21 standard suggests that an ECU must process all directed request messages
- An attacker can exploit this flaw in the standard by sending a large volume of request messages at a high rate to a recipient ECU.
- Sending large volume of request messages with lowest priority will increase the computational load of the recipient ECU, and its ability to send periodic messages.
- However, low priority normal messages should not have any effect on the recipient ECU.

## Testing Method

We wrote a Python script that repeatedly sends four different types of messages at rates varying from 0.1ms to 1ms and recorded the observations.

- The first message is a highest priority ( $00_{16}$ ) message with all zeros
- The second message is a lowest priority message ( $1C_{16}$ ) with all zeros
- The third message is a lowest priority request message for a supported PGN
- The final message is a lowest priority request message for an unsupported PGN.

# Results and Observations – Kenworth T270

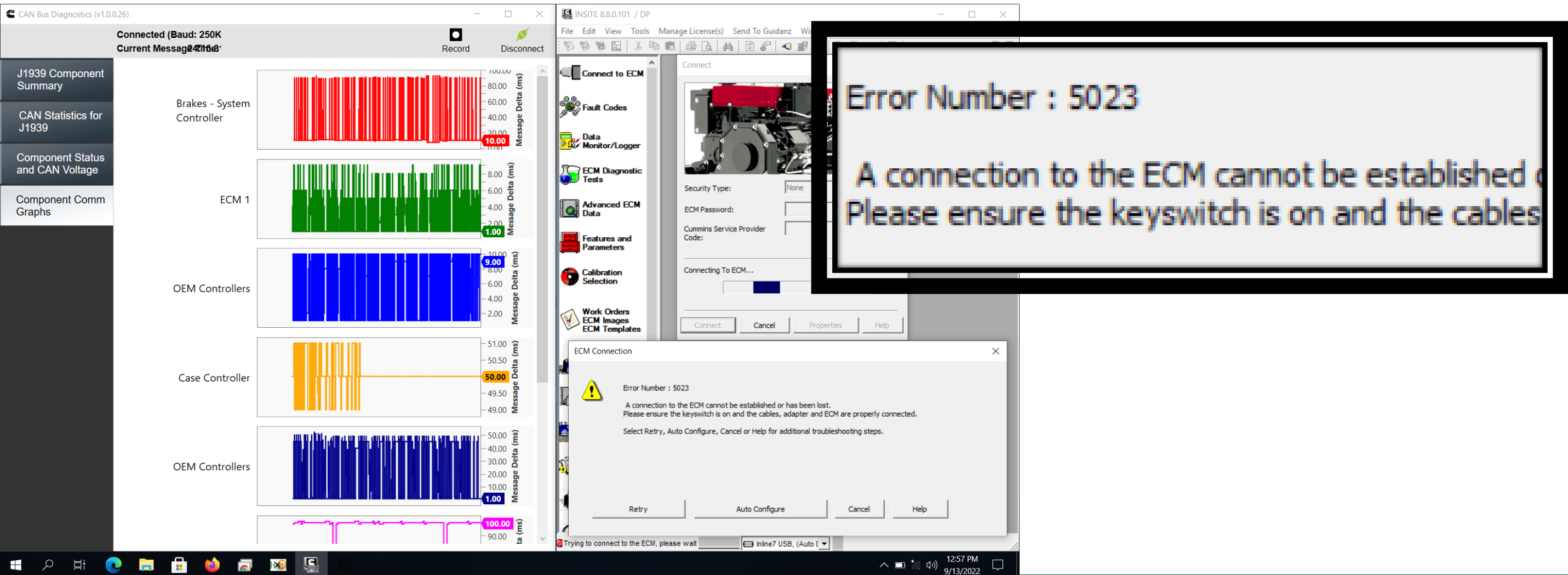




# Connection Exhaustion Hypothesis

- According to the J1939-21 standards, there can only be one established connection for multipacket transfer between a source Electronic Control Unit (ECU) and a destination ECU at a time.
- It also states that after data has been transmitted a connection can be kept open for a maximum of 1250 milliseconds by not sending the end of message acknowledgment.
- In addition, a Clear-to-send (CTS) message can be sent to request one or more packets that may have been sent already, but not received by the destination ECU.
- Using these three specifications, an attack can be crafted to deny legitimate connection attempts to an ECU by creating multiple spoofed connections and keeping them open by periodically (typically of less than a second) sending a CTS message but not the end of message acknowledgment

# Connection Exhaustion Results and Observations – Kenworth T270



# CANLay – Distributed Hardware Testbed for CAN-Based Devices

---

Jake Jepson | NMFTA Fall 2022



Colorado State University

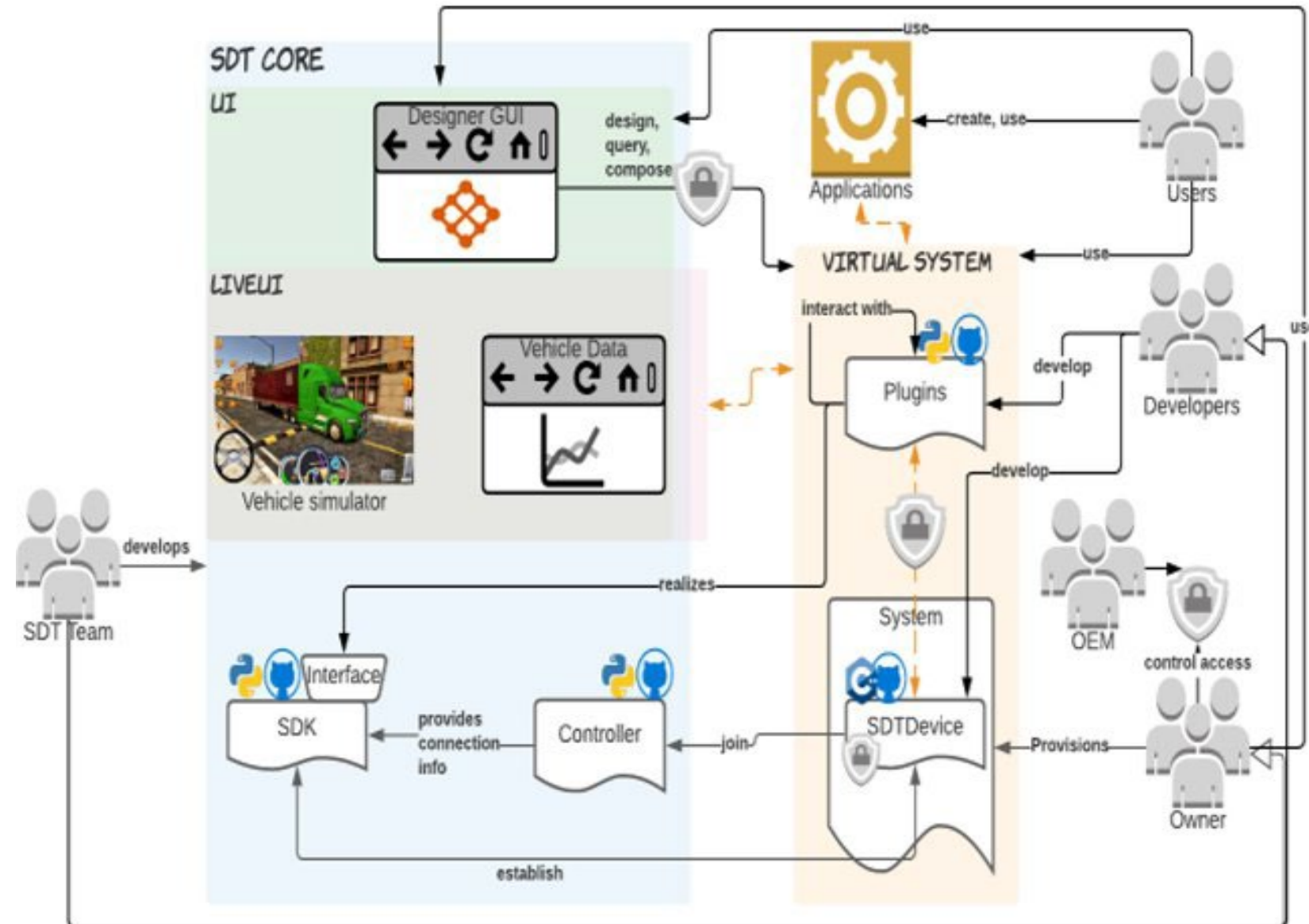
# Needs for a Software Defined Truck

1. Dynamic creation of ECU testbeds.
  1. Enables ECU reuse.
  2. Supports cybersecurity testing of multiple configurations efficiently.
2. Support physically distant ECUs.
  1. Allows easier testing for ECU hardware pairs.
  2. Enables integrated testing of ECUs from separate manufacturers.
3. Remote access to virtual CAN network for the testbed.
  1. Crucial to any vehicle network testing.
4. Support proprietary ECUs (no access to code) without physical modification.
  1. Supports black-box cybersecurity testing of all ECUs used in a configuration.

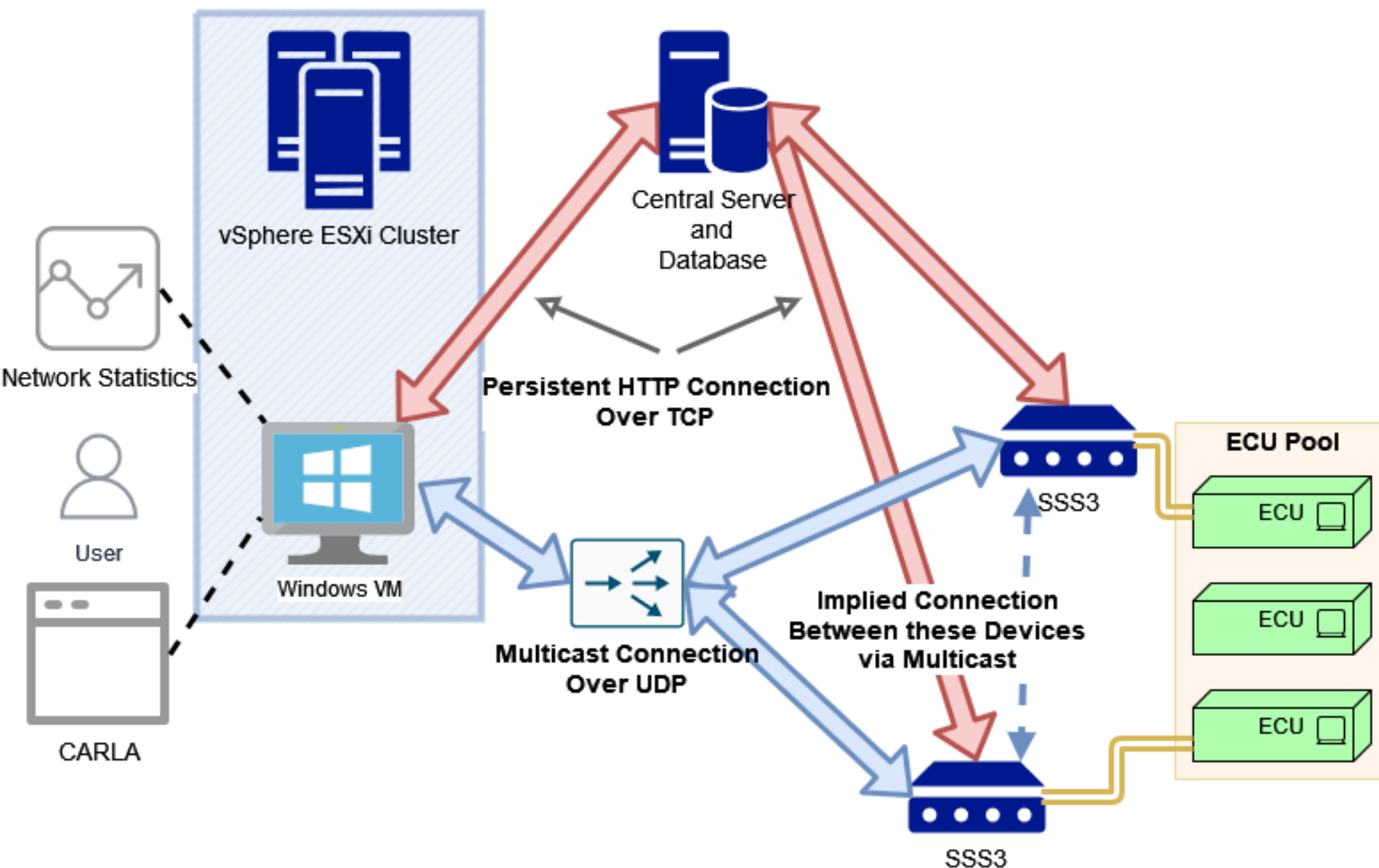


# Previous Work

- CANLay is a continuation of *Towards a Software Defined Truck*, INCOSE 2021
- Remote-accessible hardware-in-the loop distributed testbed for trucks
  - Focused on J1939 and heavy vehicles
  - Reconfigurable emulated CAN network using traditional packet switch networks
  - No required modification of target ECUs



Mukherjee, S. M., & Daily, J. D. (2021). Towards a Software Define Truck. *INCOSE International Symposium*.



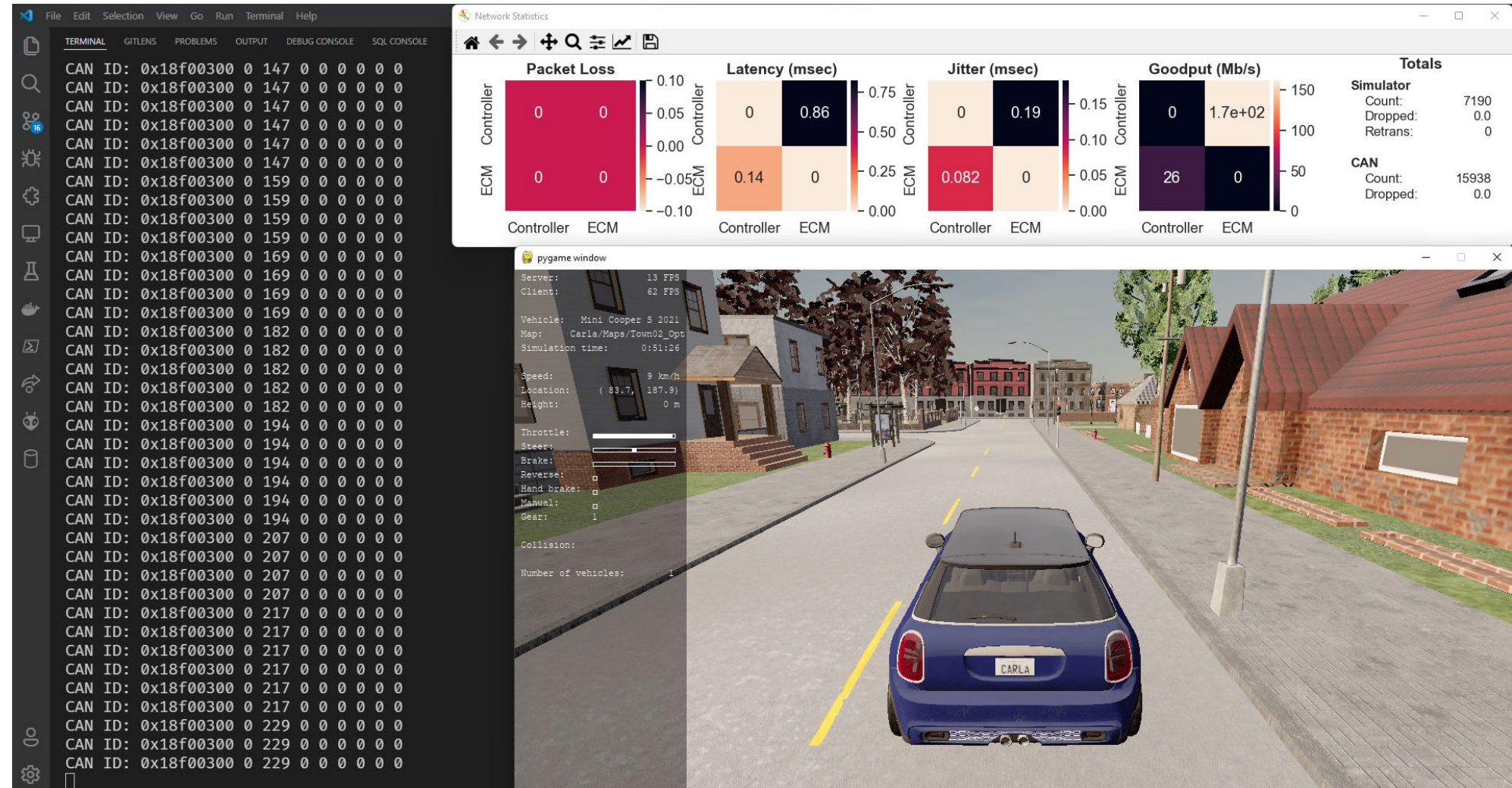
## CANLay 1.0 Overview

- Extended SDT from truck-only approach to supporting ECUs using CAN.
- Implement initial prototype for CANLay.
- Novel contribution for implementing CAN over local packet switched network.



# CANLay 1.0 Prototype

- Dynamic creation of testbeds from pool of ECU candidates.
- Support for physically distant ECUs.
- Access to emulated low-latency broadcast-style CAN networks.
- Supports proprietary ECUs.





# PIVOT: Platform for Innovative Use of Vehicle Open Telematics

A new National Science Foundation collaborative effort with

- University of Memphis
- Colorado State University
- University of Southern California
- Geotab



# Need for High Quality Automotive Datasets

- High quality, real-life vehicle network datasets are needed by researchers who are advancing the state of the art in automotive and related systems
- When it comes to passenger cars and heavy vehicles, such datasets are ad hoc, hard to obtain, and have limited utility, which prevents (or slows) the research community from growing the discipline

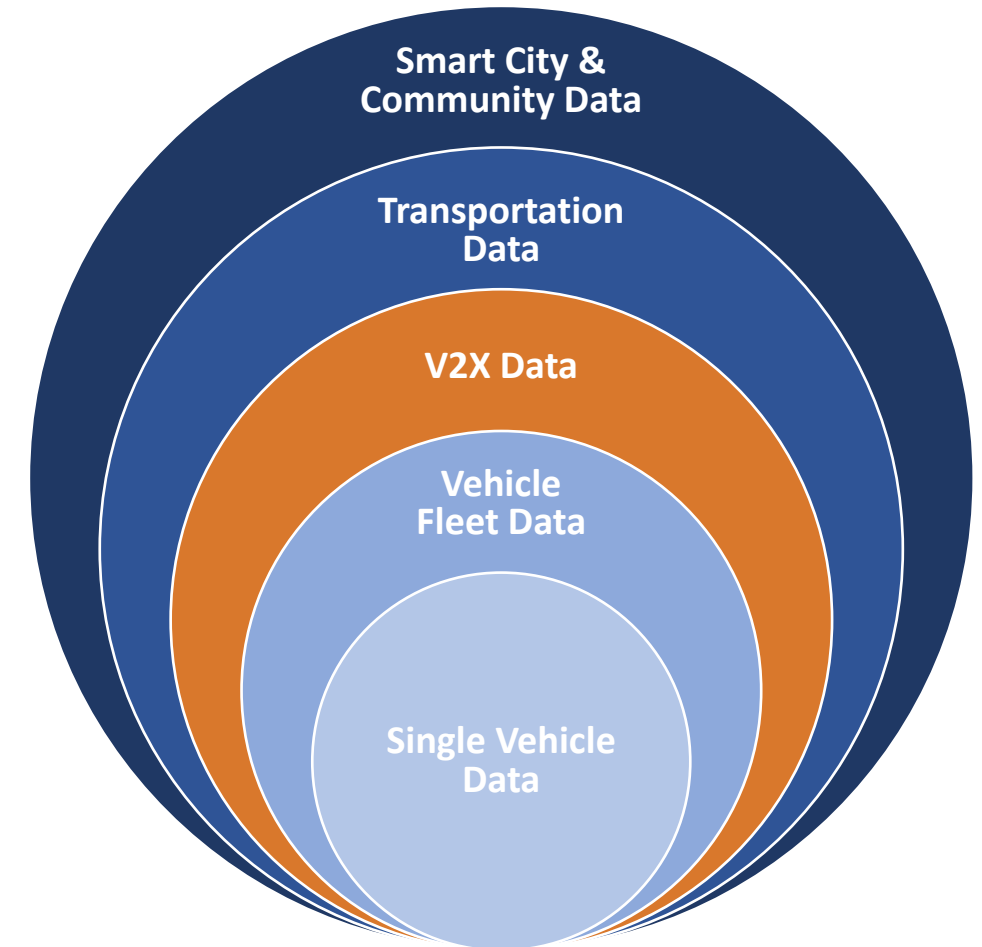
## Need for PIVOT Infrastructure

- The PIVOT infrastructure is needed to transform the ad-hoc, small-group endeavors for vehicle data curation into a scientific body of work done by a larger synergistic community



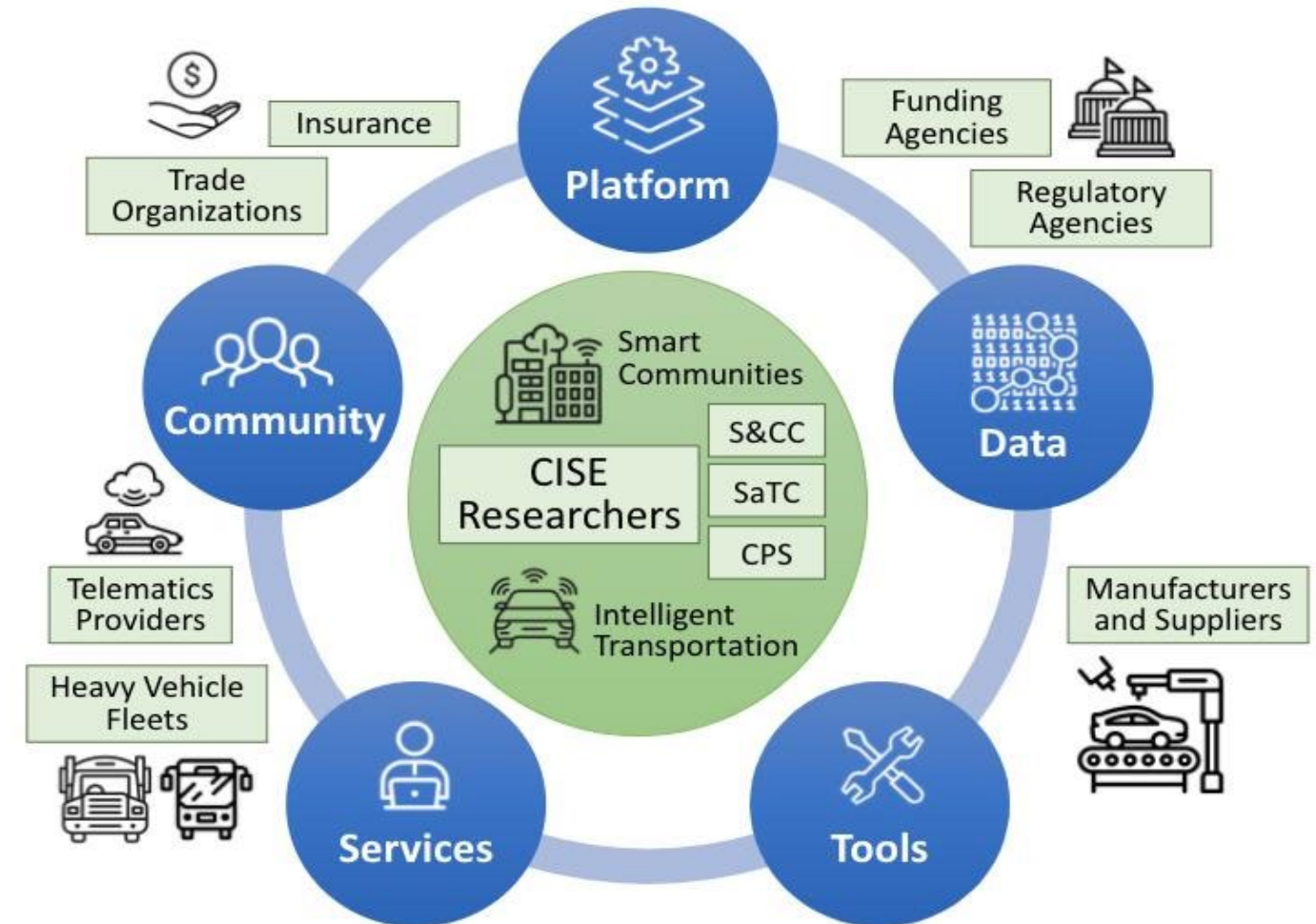
# Examples of Automotive Research Datasets

- Oak Ridge ROAD and potential future datasets
- U. South Korea HCRL Datasets
- Bosch SynCAN (for CANet)
- TU Eindhoven Lab Automotive CAN Bus Intrusion
- CrySiS Lab CAN-Log Infector and Ambient CAN Traces
- Cephas Baretto Dataset
- Heavy Truck Datasets from Jeremy Daily @ CSU
- Geotab Ignition-Altitude
- U. Michigan Mcity
- US Department of Transportation Public Data Portal
- SmartColumbus Datasets Curated for Visualization
- Wyoming DOT CV Pilot



# PIVOT Five Pillars

- (1) Robust and reliable hardware/software platform upon which the system runs
- (2) Curation and sharing of the data and contextual information
- (3) Researcher centric services for sharing, securing, and evaluating datasets
- (4) Common software-based tools to collect, transform, combine, filter, and visualize the data
- (5) Extensive community outreach and engagement to improve the data utility using design feedback mechanisms



# Annual Community Workshops

- Bring together the community around development and sharing of robust automotive and heavy-duty datasets to support open research in areas with strong societal impact
- November 2021 workshop brought together close to 70 researchers producing and/or using datasets; commercial vehicle telematics providers willing to share data; and other interested parties

## YOU'RE INVITED!

The next workshop will be held VIRTUALLY on November 17-18, 2022.

RSVP to [info@pivot-auto.org](mailto:info@pivot-auto.org) if you are interested in participating!



**Christos  
Papadopoulos**  
(U. Memphis)



**Jeremy  
Daily**  
(Colo State)



**David  
Balenson**  
(USC-ISI)



**Wes  
Hardaker**  
(USC-ISI)



**Glenn  
Atkinson**  
(Geotab)



**Ted  
Guild**  
(Geotab)



**Stacy  
Prowell**  
(ORNL)



**Sam  
Hollifield**  
(ORNL)

# Benefits of PIVOT

- Help coordinate existing isolated efforts
- Facilitate exchange of knowledge and resources
- Encourage, nurture, and sustain ongoing conversations
- Stimulate research collaborations among users and producers of datasets
- Engage industry, including OEMs, suppliers, and other important partners
- Engage relevant standards bodies and applicable government organizations

## Community Impact

- Create robust ecosystem that works to develop, share, and exploit community resources, including automotive research datasets and tools
- Enable research community to address important problems, define high quality research initiatives, and develop new, innovative applications to benefit society
- Active outreach and community building, like the **CyberTruck Challenge**





# Mission Statement

***Develop talent** for the next generation workforce by bringing awareness, excitement, professional involvement, and practicum-based training to the heavy vehicle cybersecurity domain.*

***Establish community** of interest for heavy vehicle cybersecurity that transcends individual companies or departments and reaches across disciplines and organizations to make a more universal and experienced base of engineers and managers.*

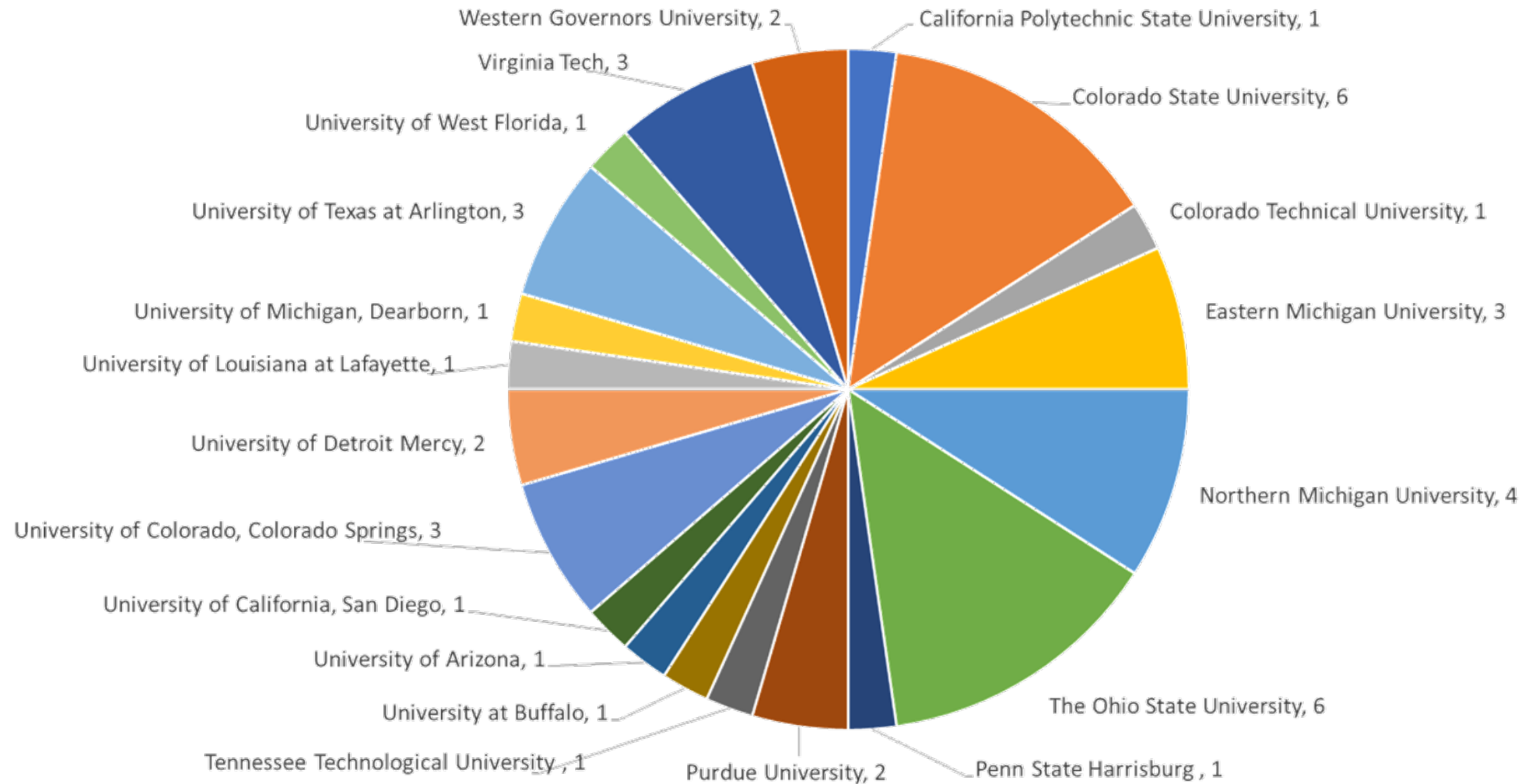




Photo taken on June 22, 2022 in the Sports and Expo Center of Macomb Community College, Warren, Michigan

# 2022 Student and University Participation

## 44 Students from 20 Universities



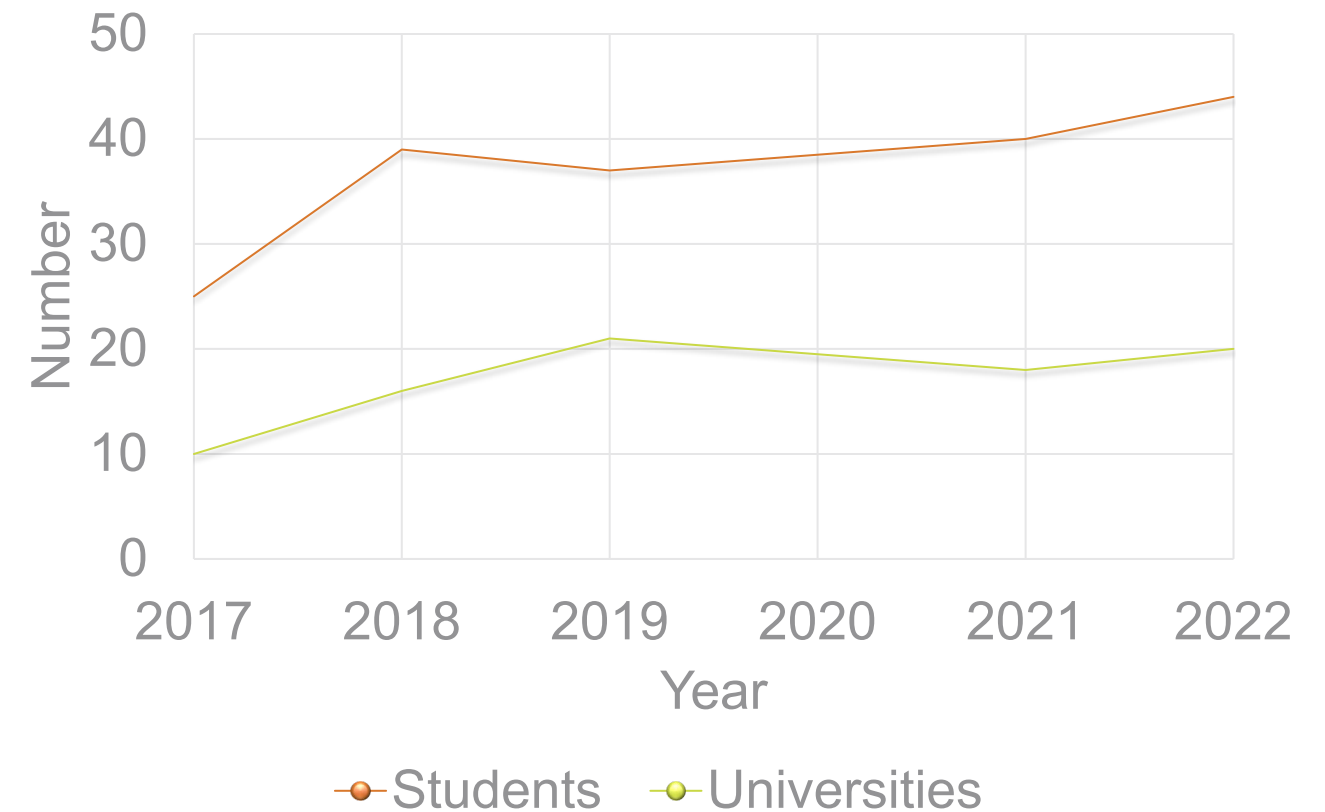


# Student Participation Growth over 5 Years

Year	Students	Universities
2017	25	10
2018	39	16
2019	37	21
2021	40	18
2022	44	20



## CyberTruck Challenge Participation



# Thank you to the CyberTruck Challenge sponsors



DAIMLER

PACCAR



BOSCH



Allison  
Transmission®



U.S. Department of Transportation  
**Federal Motor Carrier Safety Administration**



SYSTEMS ENGINEERING  
COLORADO STATE UNIVERSITY







# Description of Activities

## Real Vehicles

*Sponsors bring new vehicles as assessment targets. Company engineers work with students and mentors.*



## Real Hackers

*Experienced mentors from professional security firms help coach students through exercises and security related assessments.*



## Real Fun!

*Students have a unique opportunity to solve challenging problems, learn from experts and experience engineering in the heavy-duty industry.*



CyberTruck Challenge 2022 Schedule								Version:20220619						
	Sunday, 19 June	Monday, 20 June		Tuesday, 21 June		Wednesday, 22 June	Thursday, 23 June	Friday, 24 June	Time					
		Group A	Group B	Group A	Group B									
Before 0700	Site Closed	Site Closed							Before 0700					
0700-0730		Breakfast						Breakfast	0700-0730					
0730-0800								Student Team Briefs (30 minutes each group)	0730-0800					
0800-0830		Welcome // NDA		Vehicle Network Security	Ghidra	Legal Briefing	Assessment		Assessment	0800-0830				
0830-0900		Safety and Orientation									0830-0900			
0900-0930		Software RE	Truck Systems and J1939	Vehicle Network Security	Assessment	Assessment				Student Team Briefs (30 minutes each group)	0900-0930			
0930-1000											Cryptography	Vehicle Network Security	0930-1000	
1000-1030														1000-1030
1030-1100														1030-1100
1100-1130														
1130-1200							Awards	1130-1200						
1200-1230			Lunch						Lunch	1200-1230				
1230-1300										1230-1300				
1300-1330		Truck Systems and J1939	Software RE	Android	Embedded Firmware Patching	Assessment	Assessment	Site Closed	1300-1330					
1330-1400											1330-1400			
1400-1430											1400-1430			
1430-1500											1430-1500			
1500-1530											1500-1530			
1530-1600											1530-1600			
1600-1630		Trucking Industry	Cryptography	Embedded Firmware Patching	Android						1600-1630			
1630-1700											1630-1700			
1700-1730		Ghidra	Trucking Industry								1700-1730			
1730-1800											1730-1800			
1800-1830							1800-1830							
1830-1900	Informal Welcome Reception (offsite)	Dinner						1830-1900						
1900-1930								1900-1930						
1930-2000		Introduction to Learning Platforms		Assessment Preparation		Assessment	Free	1930-2000						
2000-2030								2000-2030						
2030-2100	Site Closed	Free		Free				2030-2100						
2100-2130								2100-2130						
2130-2200								2130-2200						
After 2200		Site Closed							After 2200					
Snacks will be served each afternoon.		*Survey		*Survey										
<div>Legend</div> <div><div>Lecture / Demo</div><div>Volvo Side</div><div>Cummins Side</div><div>Meals</div><div>"Hacking"</div><div>Free</div><div>Site Closed</div><div>Off Site</div></div> <div>All participants</div> <div>Interactive lecture and activities</div> <div>Interactive lecture and activities</div> <div>Meals will be catered on-site</div> <div>On vehicle assessments</div> <div>Can hack, study, rest, leave, etc.</div> <div>No access the facility</div> <div>Limelight Grill on VanDyke Ave</div>				Topic		Instructor, Affiliation		Verified						
				Welcome and Review		Karl Heimer [MEDC] & Sponsor Representatives		Yes						
				Embedded Firmware Patching		Ang Cui, Edward Larson [Red Balloon Security]		Yes						
				Decompilation with Ghidra		Justin "Ozzie" Osborn [JHU-APL]		Yes						
				Software Reverse Engineering		Erin Cornelius [GRIMM]		Yes						
				Truck Systems and J1939		Jeremy Daily [Colorado State University]		Yes						
				Android		Eduardo Novella [Now Secure]		Yes						
				Cryptography		Ben Gardiner [NMFTA]		Yes						
				Vehicle Network Security		Hannah Silva [Leviathan Security]		Yes						
				Trucking Industry		Urban Jonson [Serjon]		Yes						





# Assessment Period

A typical team would include

- 4-6 Students
- 1-2 Mentors
- 1-3 Industry
- 1-2 Government
- 1 named Vehicle Boss

Vehicle Bosses can stop an assessment at any time.

Results and presentations only go to the vehicle boss.

Students from the same school are encouraged to join separate teams.

8 teams were formed in 2022.

Each team has 30 minutes to present their results on Friday.



# Assessment Period: Applying the hands-on lecture content





# Assessment Period: Students Explore with Mentors





# Student Presentations

- Results from the assessment are presented to the other participants.
- This is a CLOSED event; only participants who have agreed to the non-disclosure agreement can attend.
- Student reports are not archived or available to be released.
- Results from the assessment are communicated to the equipment engineers



# Why Participate?



Workforce Development



Demonstrate high-tech nature of commercial vehicles



Attract top students to the industry



Improve Current Workforce



Continuous Product Improvement



## What to bring?

Truck, trailer  
Electronic systems  
Bench setups  
Diagnostic tools  
Telematics



## Who to bring?

People who can mentor  
People who need to learn

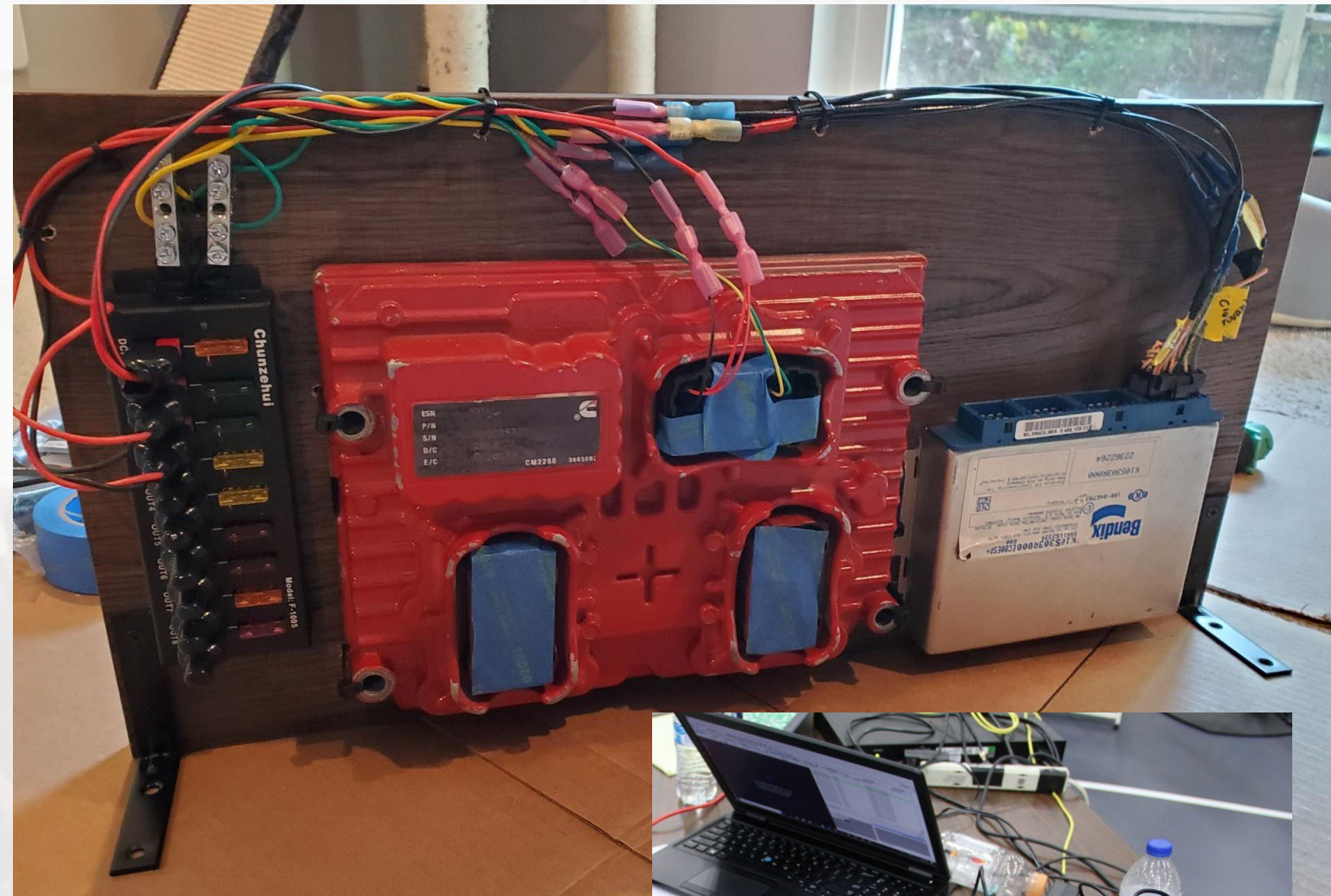
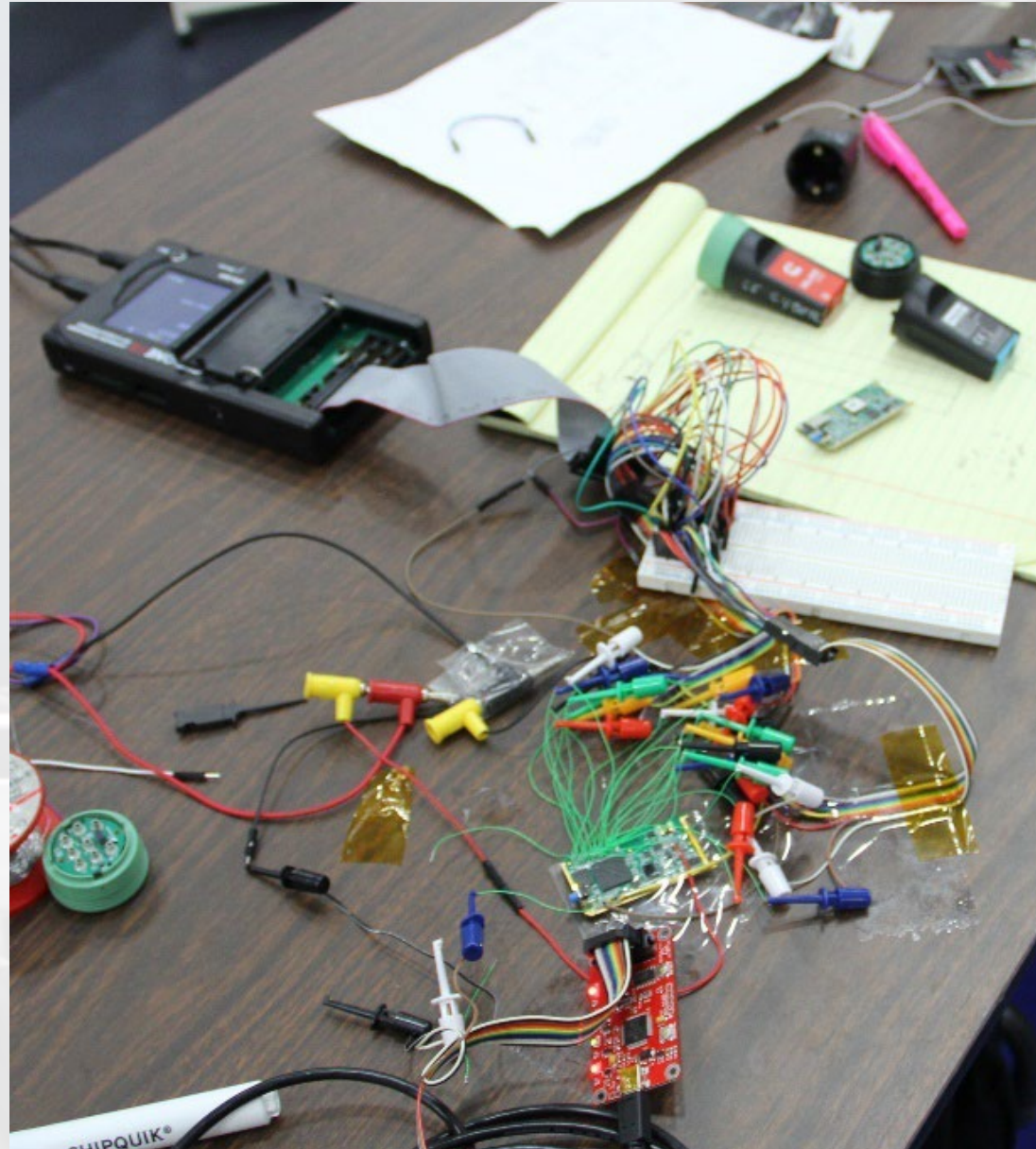


## Network

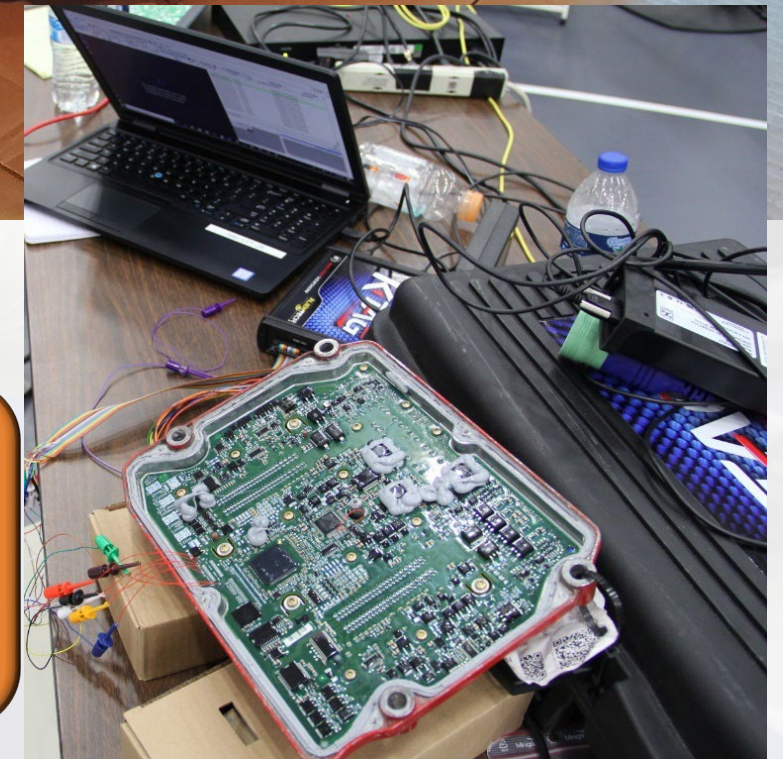
Industry peers  
Academics  
Security researchers  
Students  
Fleets



Industry products will be there ...



... even if OEMs are not.





# Save the Date

CyberTruck Challenge 2023  
June 12 – 16, 2023  
Macomb Community College  
Warren, Michigan

[www.cybertruckchallenge.org](http://www.cybertruckchallenge.org)

[Jeremy.Daily@colostate.edu](mailto:Jeremy.Daily@colostate.edu)  
[karl.heimer@outlook.com](mailto:karl.heimer@outlook.com)

Workshop, 17-18 Nov  
[info@pivot-auto.org](mailto:info@pivot-auto.org)