# CAN Data Security Diode

Presented by Jeremy Daily, Ph.D., P.E.

Associate Professor of Mechanical Engineering

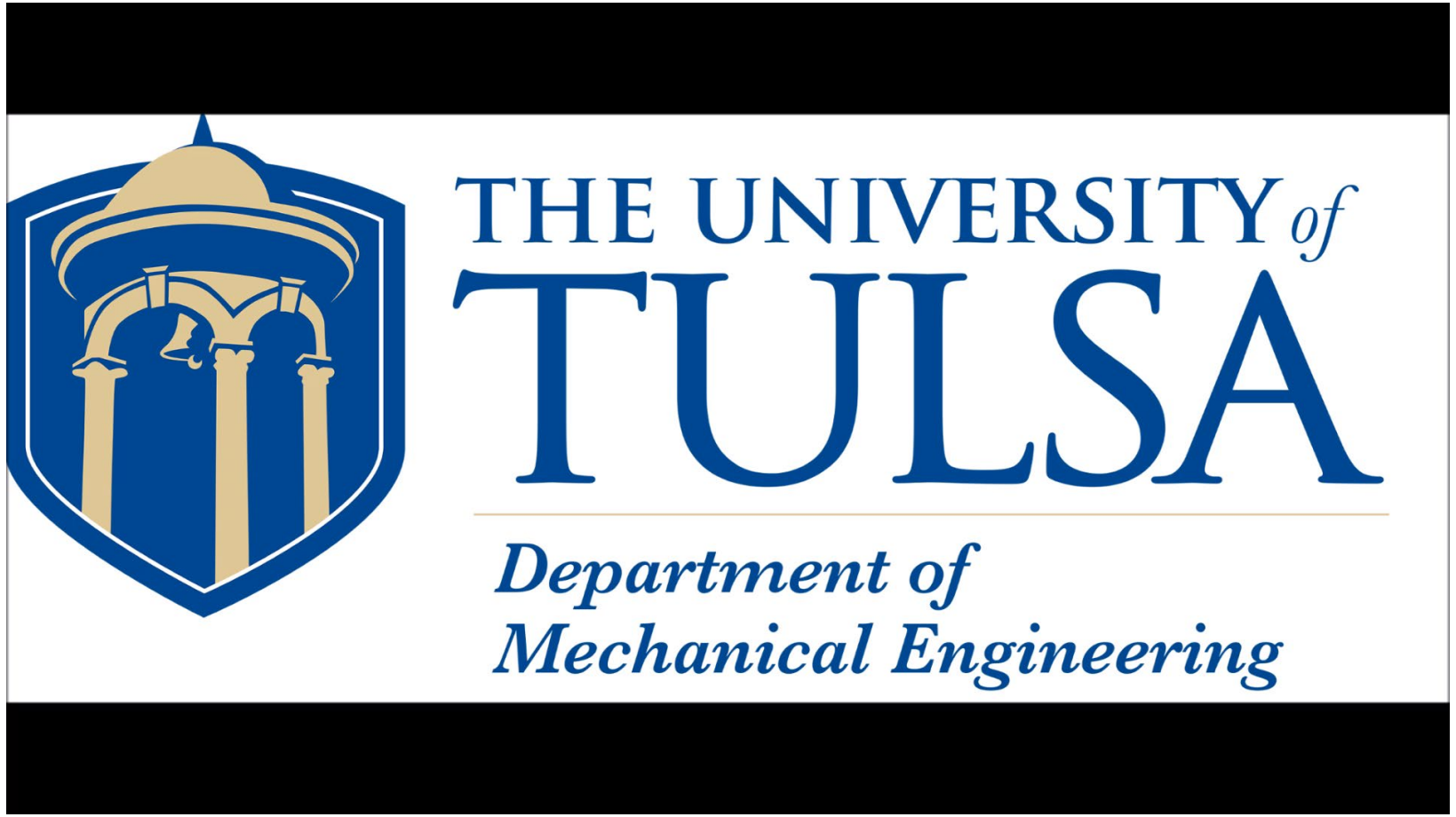
Co-Author: Hayden Allen

BSME 2018

THE UNIVERSITY of TULSA

Department of Mechanical Engineering

# Cars and Trucks Sometimes Crash



# Why did these trucks crash?

THE UNIVERSITY of TULSA
Department of Mechanical Engineering

- 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 15$^{th}$ hour of driving that day

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


THE UNIVERSITY of TULSA
Department of Mechanical Engineering

# FEDERAL REGISTER

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

Part II

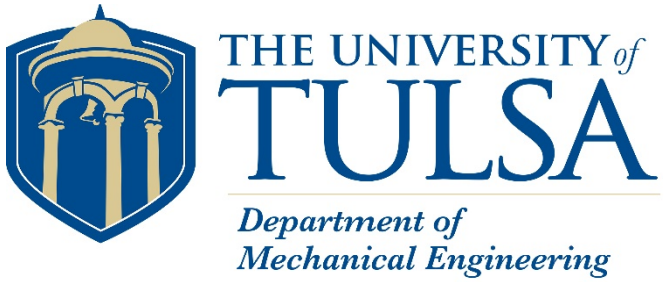
## Department of Transportation

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

THE UNIVERSITY of TULSA
Department of Mechanical Engineering

**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.

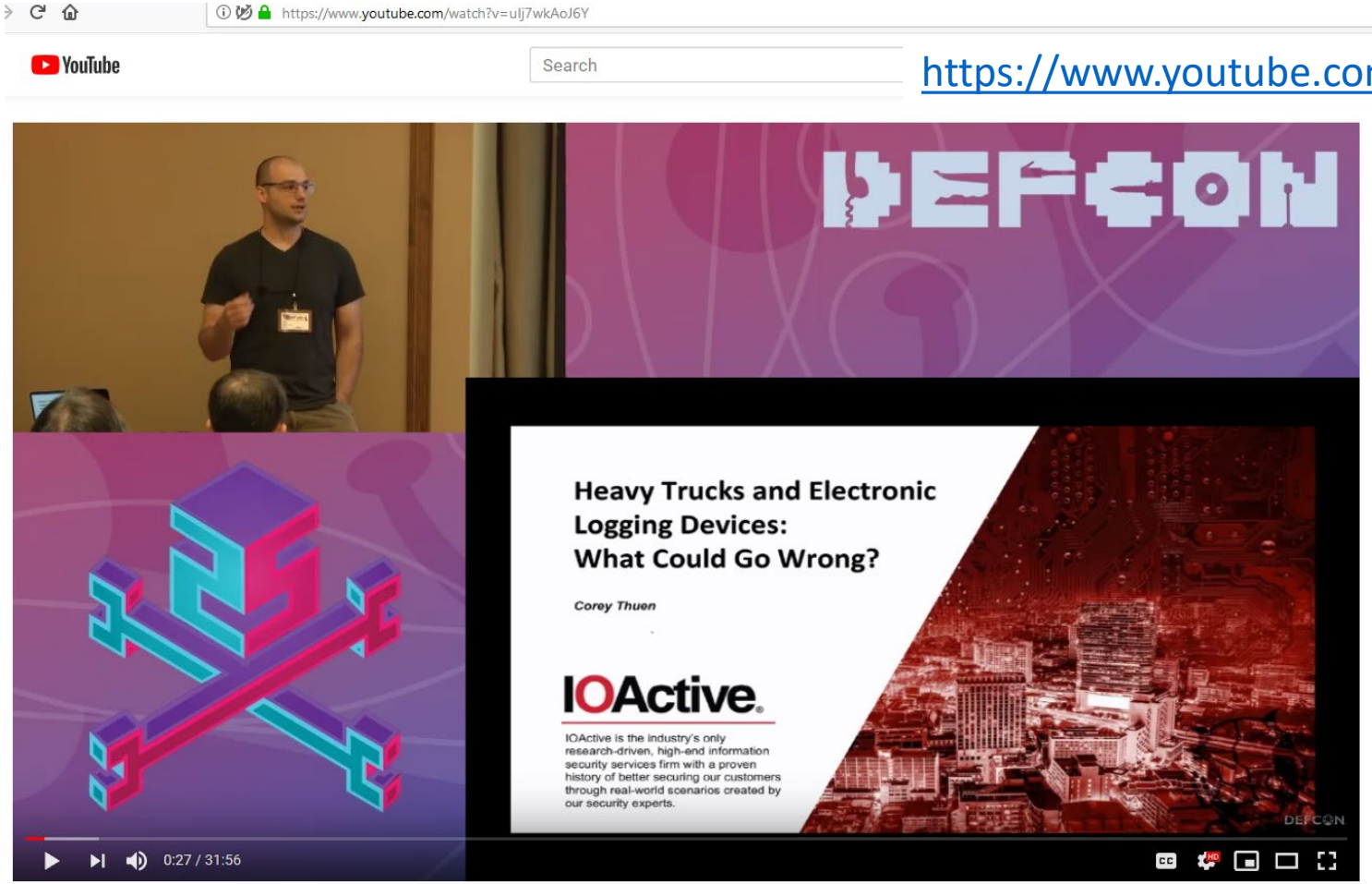
2. FMCSA Response

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

THE UNIVERSITY of TULSA
Department of Mechanical Engineering

https://www.youtube.com/watch?v=uIj7wkAoJ6Y



# What can we do?

THE UNIVERSITY of TULSA
Department of Mechanical Engineering

- 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?

THE UNIVERSITY of TULSA
Department of Mechanical Engineering

# Conspicuously Absent

THE UNIVERSITY of TULSA
Department of Mechanical Engineering

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

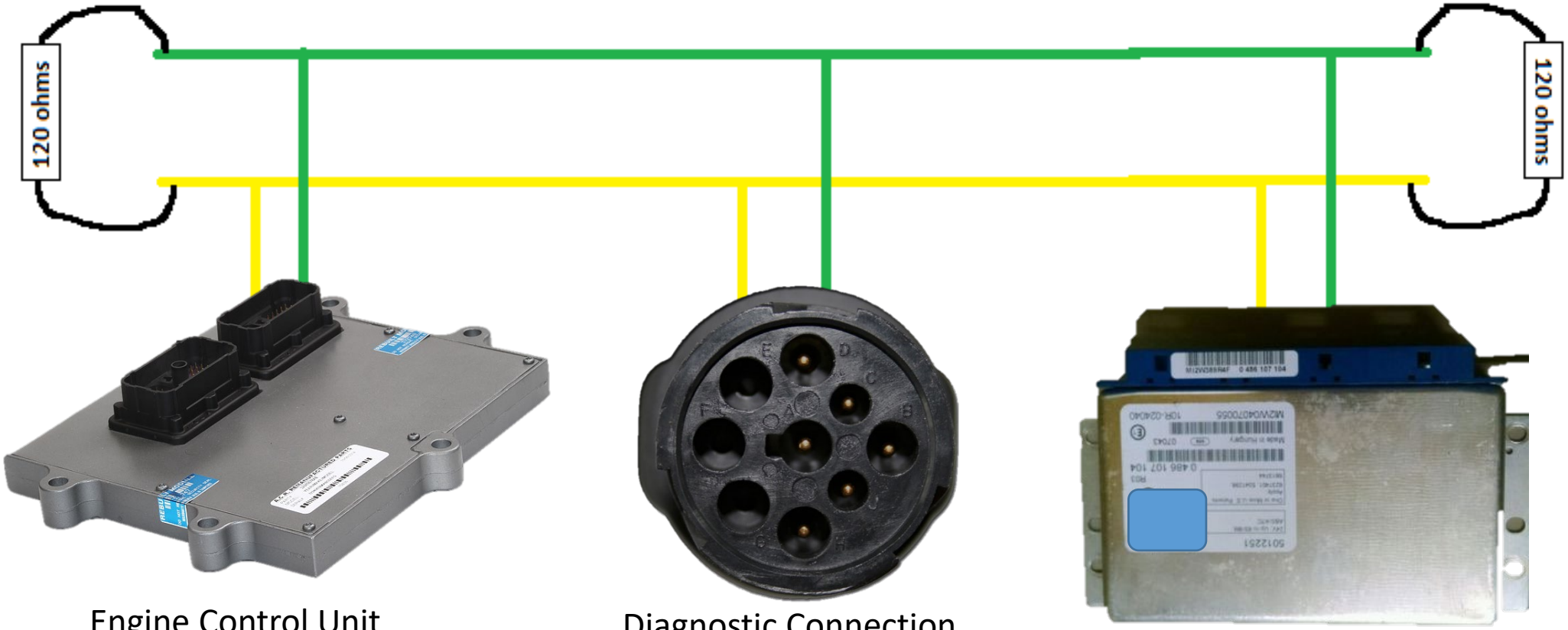
  Have the vendor demonstrate protections from affecting the CAN bus in an unintended manner.

- 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.

# What is connected via CAN?

THE UNIVERSITY of TULSA
Department of Mechanical Engineering



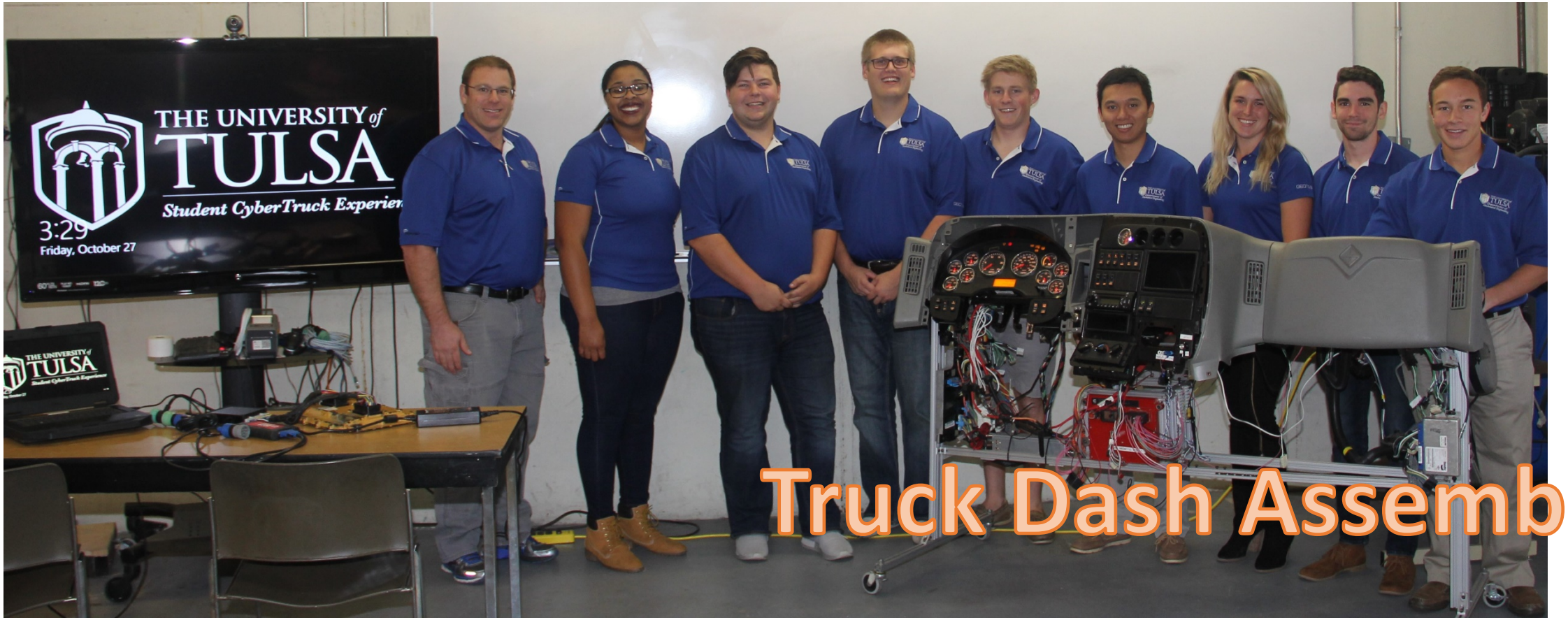

Engine Control Unit

Diagnostic Connection

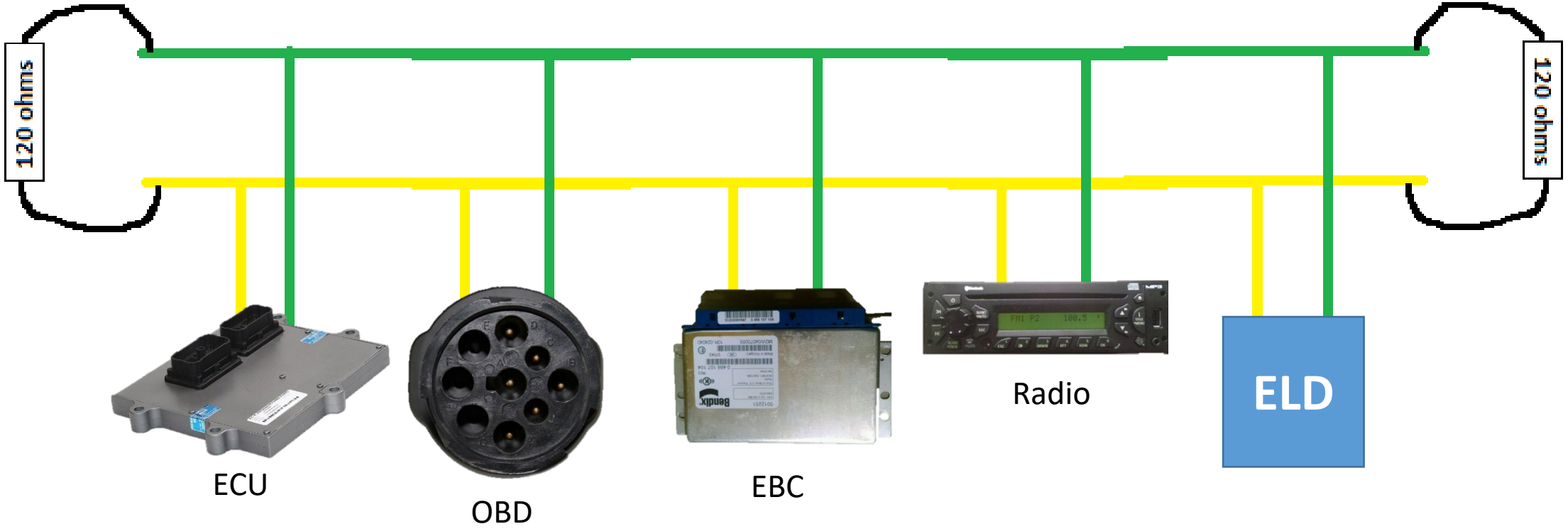
Electronic Brake Controller

# Just follow the wires…

THE UNIVERSITY of TULSA
Department of Mechanical Engineering



# What else?



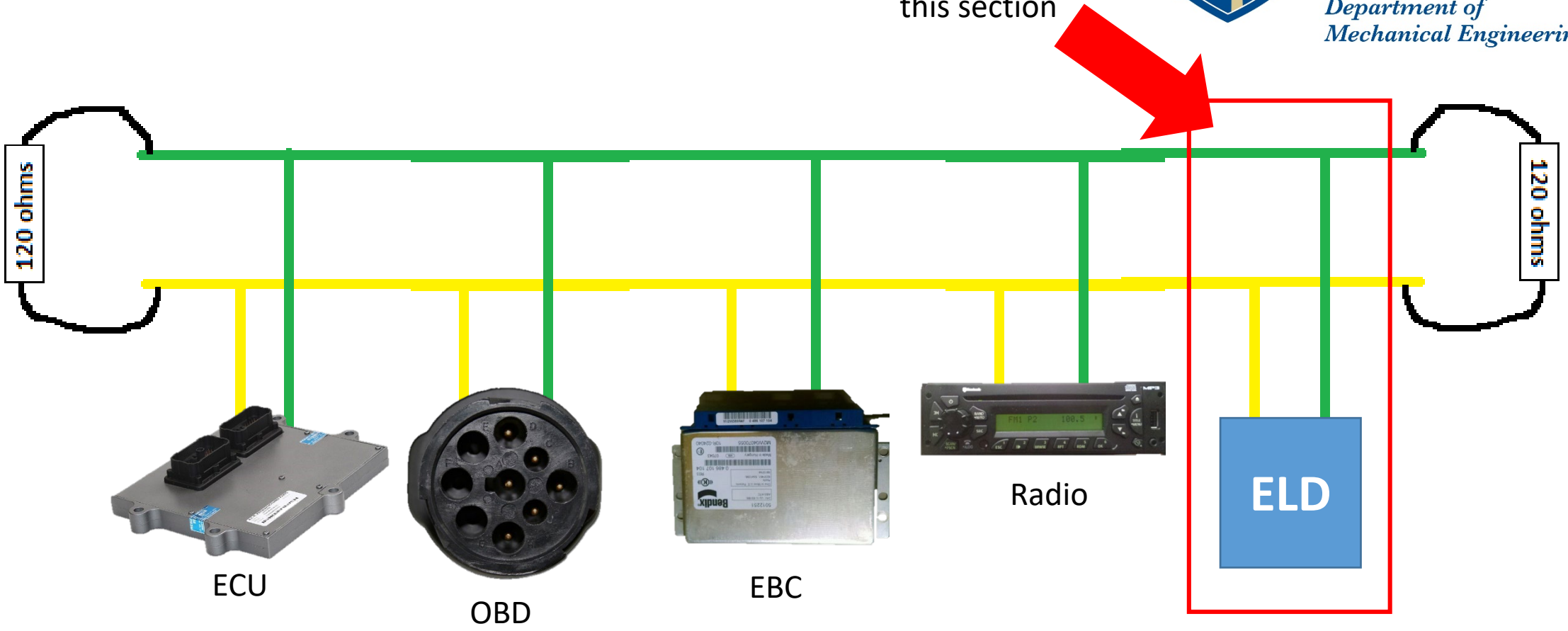
| |  |  |  |  | ELD |
|---|---|---|---|---|---|
| Actual Bus | RW | RW | RW | RW | RW |

| |  |  |  |  | ELD |
|---|---|---|---|---|---|
| Actual Bus | RW | RW | RW | RW | RW |
| Ideal Bus | ? | ? | ? | ? | ? |

| |  |  |  |  | ELD |
|---|---|---|---|---|---|
| Actual Bus | RW | RW | RW | RW | RW |
| Ideal Bus | RW | RW | RW | ? | ? |

| |  |  |  |  | ELD |
|---|---|---|---|---|---|
| Actual Bus | RW | RW | RW | RW | RW |
| Ideal Bus | RW | RW | RW | R | R |

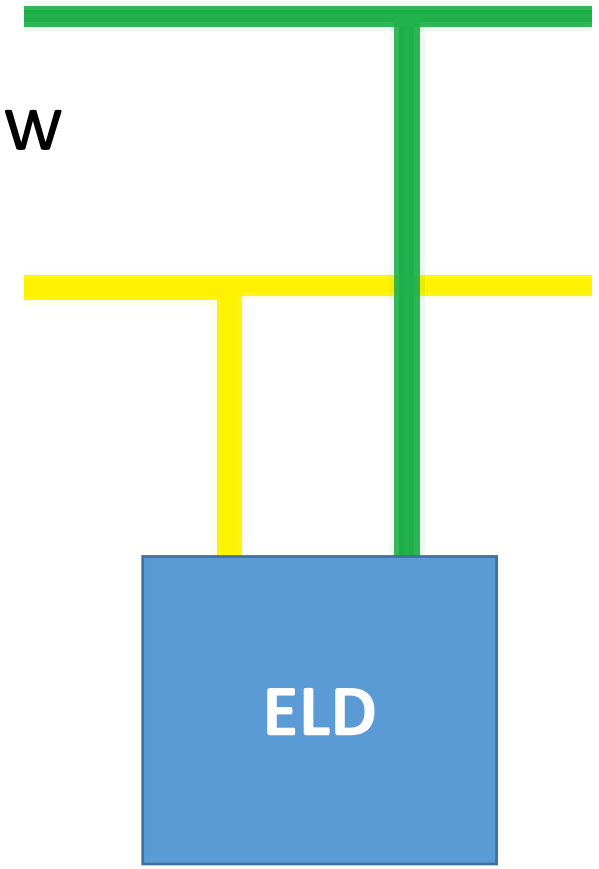
# CAN Bus


Let's look at this section
120 ohms
120 ohms
ECU
OBD
EBC
Radio
ELD

# How Do You Achieve Read Only?

THE UNIVERSITY of TULSA
Department of Mechanical Engineering

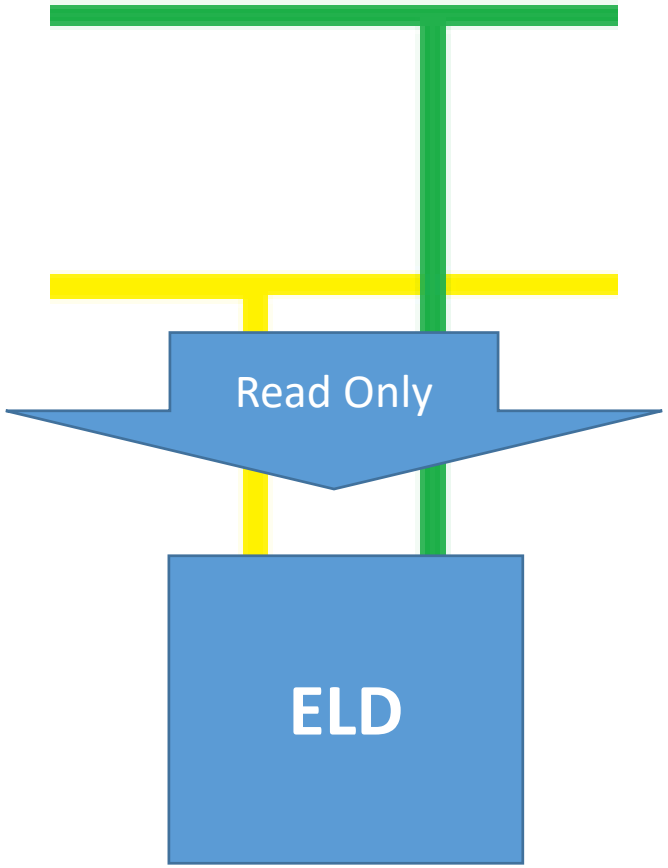
- To achieve read only access to CAN:
  - Must allow messages in (READ) but not allow messages out (WRITE).
  - Must maintain functionality of the downstream device (i.e. the ELD).



# Achieving Read Only

THE UNIVERSITY of TULSA
Department of Mechanical Engineering

- Install an additional hardware device in inline.
  - Software is vulnerable to attack and can be changed to allow for new functionality.
- Inspired by similar strategies in SCADA



THE UNIVERSITY of TULSA
Department of Mechanical Engineering

# CAN Data Diode

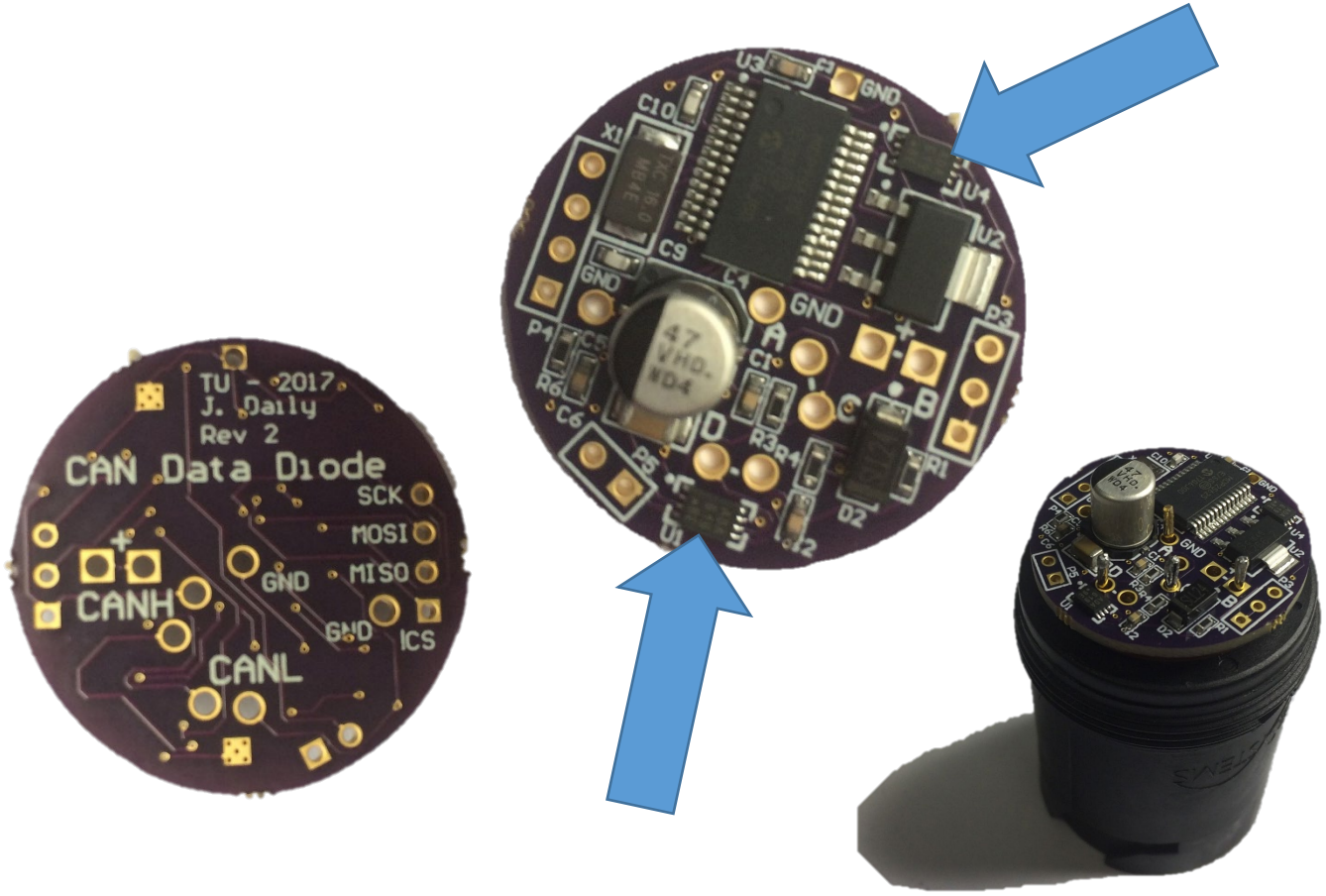
Establishing a more secure CAN bus

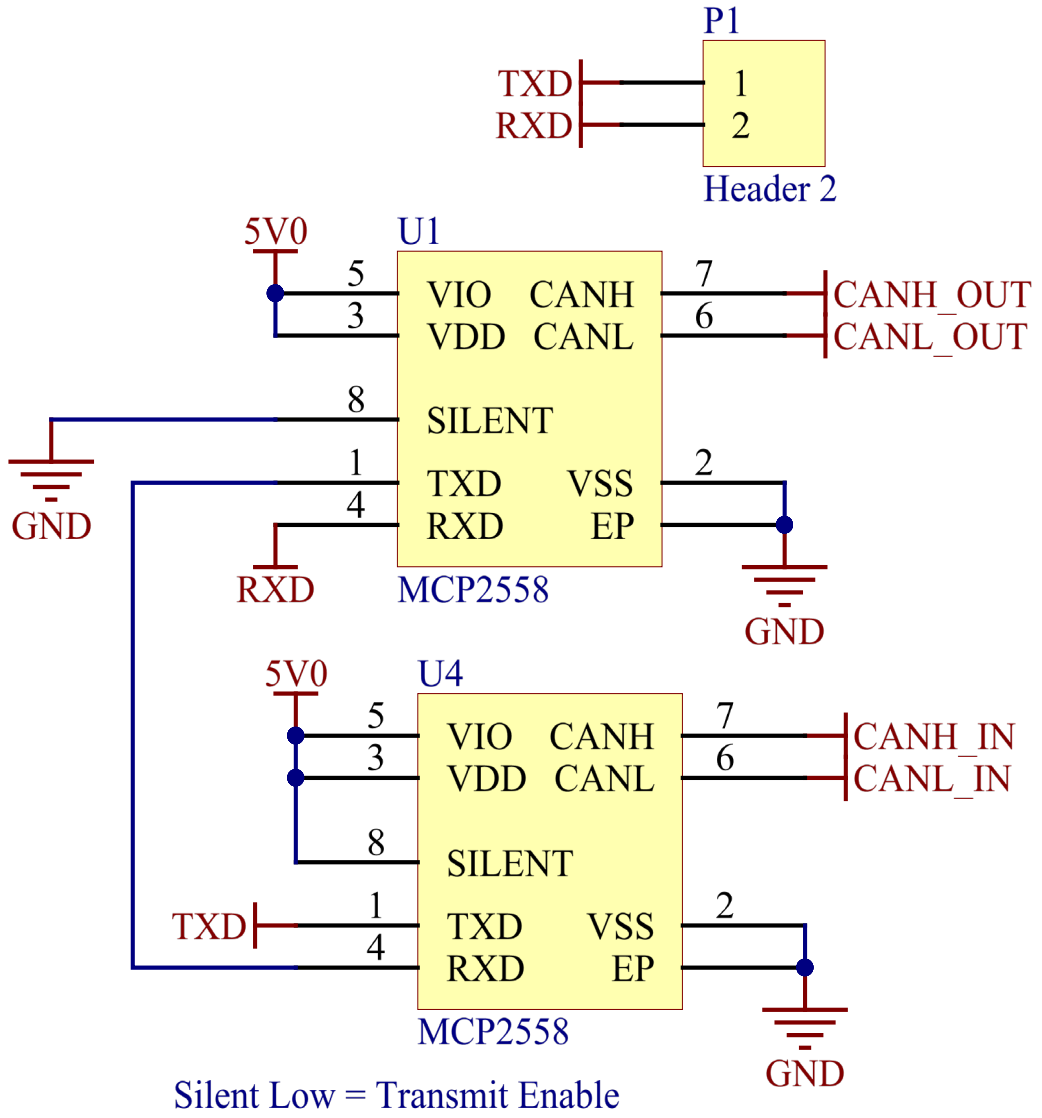
# What is a Data Diode?

THE UNIVERSITY of TULSA
Department of Mechanical Engineering

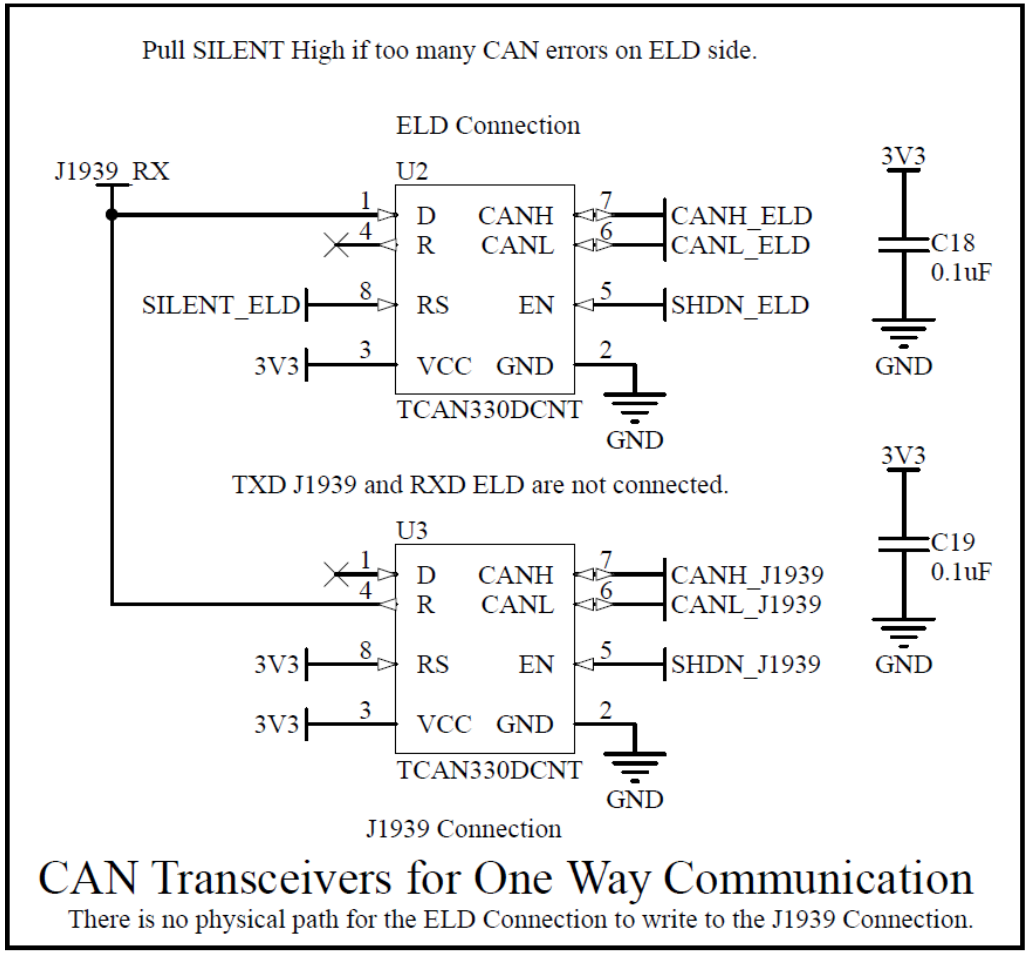
- Removes full bus write access
  - Accomplished by wiring TX and RX pins together on two separate CAN transceivers
  - This removes full write ability
- Maintains functionality of isolated devices
  - The data diode contains an extra controller and transceiver to acknowledge the downstream unit
  - This maintains full functionality of the downstream device (ELD)

# Back to Back Transceivers

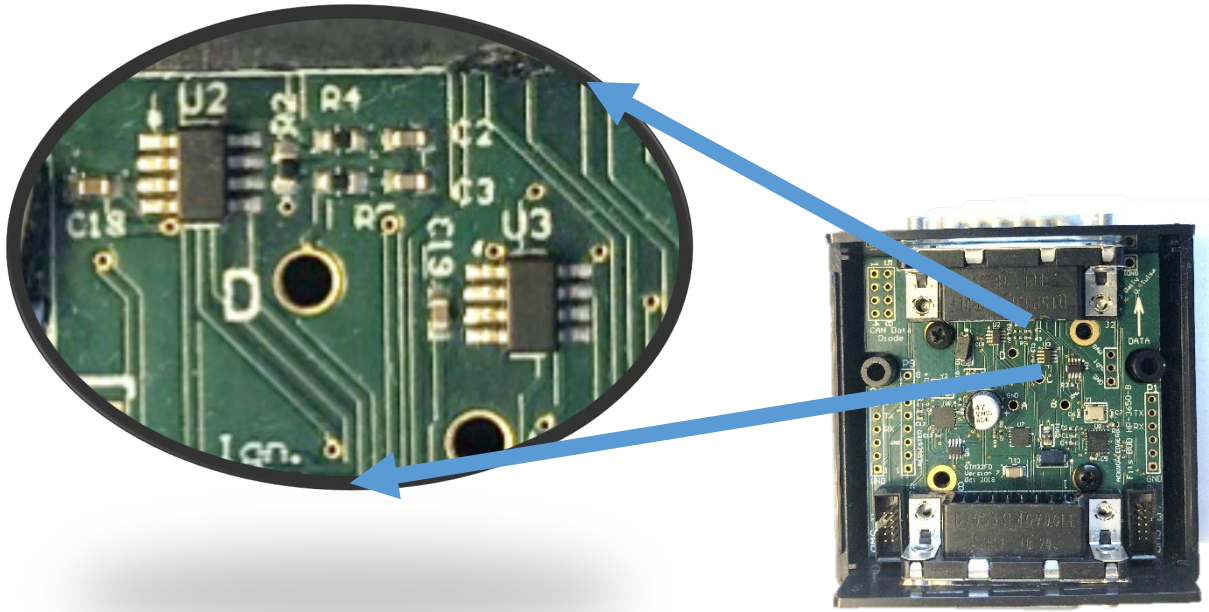


# Back to Back CAN Transceivers




- Small TI TCAN330 transceivers
  - Silent Pin
  - Shutdown Pin

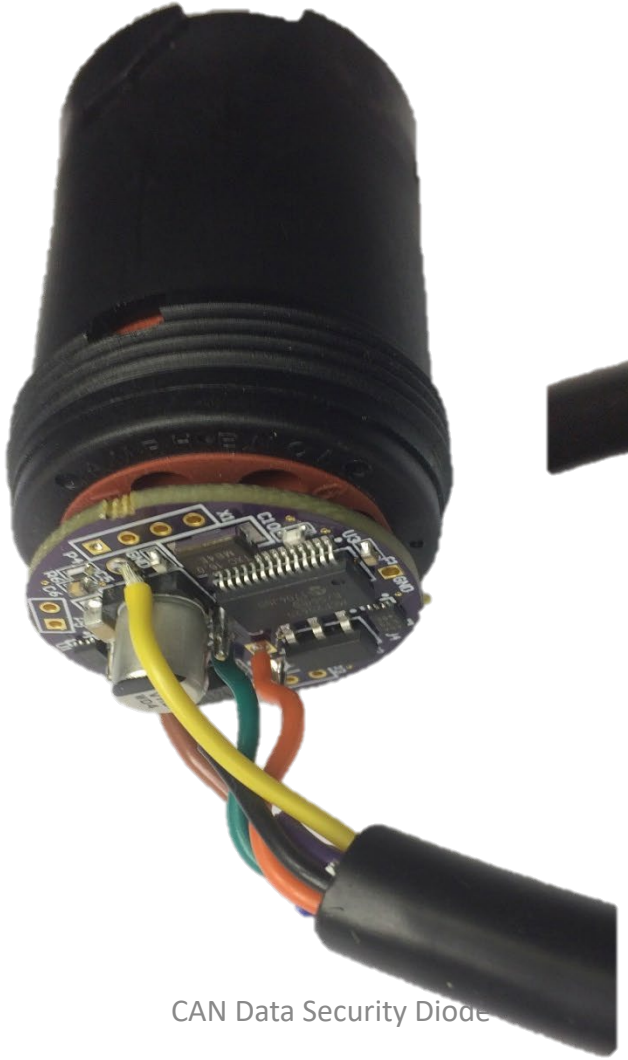


THE UNIVERSITY of TULSA
Department of Mechanical Engineering


# of Concept

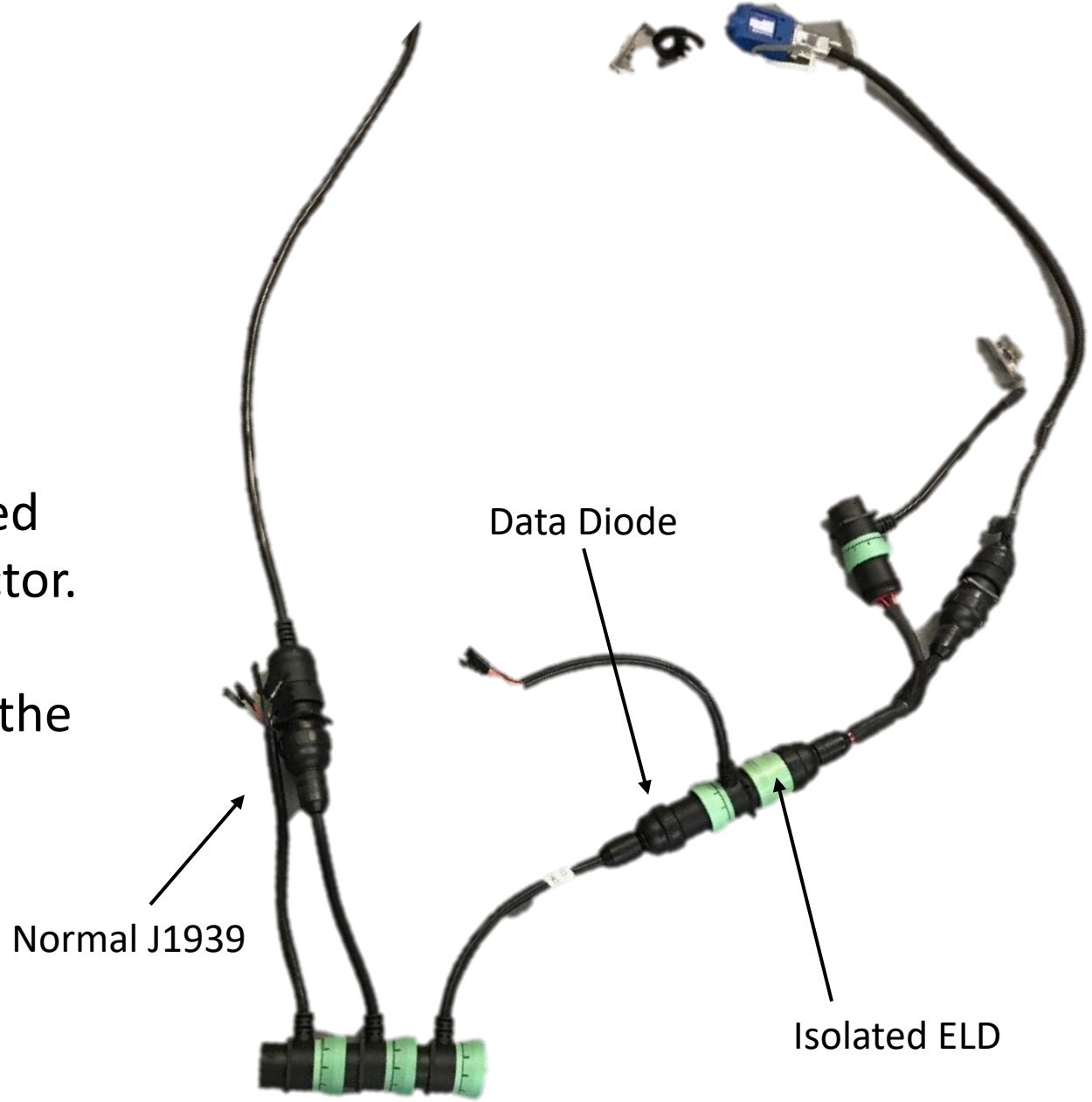
# Prototype: Build the CAN Data Diode into the Connector

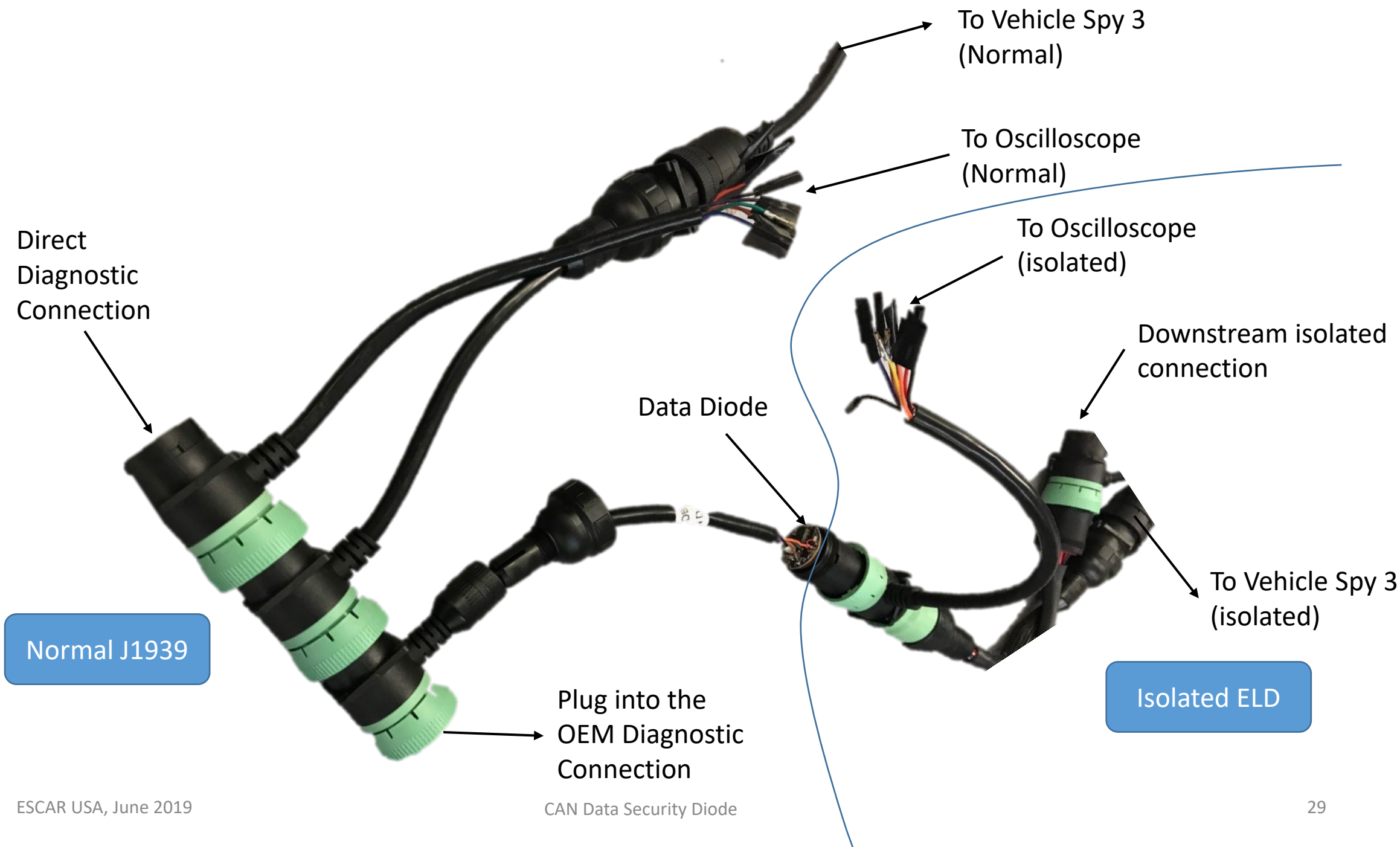
THE UNIVERSITY of TULSA
Department of Mechanical Engineering



# Testing Setup

- To test the data diode, two branches were created:
  1. Normal (J1939) – Directly connected to a truck or test bed through the diagnostic connector.
  2. Isolated (ELD) – Connected to diagnostic but is protected by the CAN Data Diode




To Vehicle Spy 3
(Normal)
To Oscilloscope
(Normal)
Direct
Diagnostic
Connection
To Oscilloscope
(isolated)
Downstream isolated
connection
Data Diode
To Vehicle Spy 3
(isolated)
Normal J1939
Plug into the
OEM Diagnostic
Connection
Isolated ELD

# Truck Test Bed

# Arduino based Tone Ring Frequency Generator

THE UNIVERSITY of TULSA
Department of Mechanical Engineering

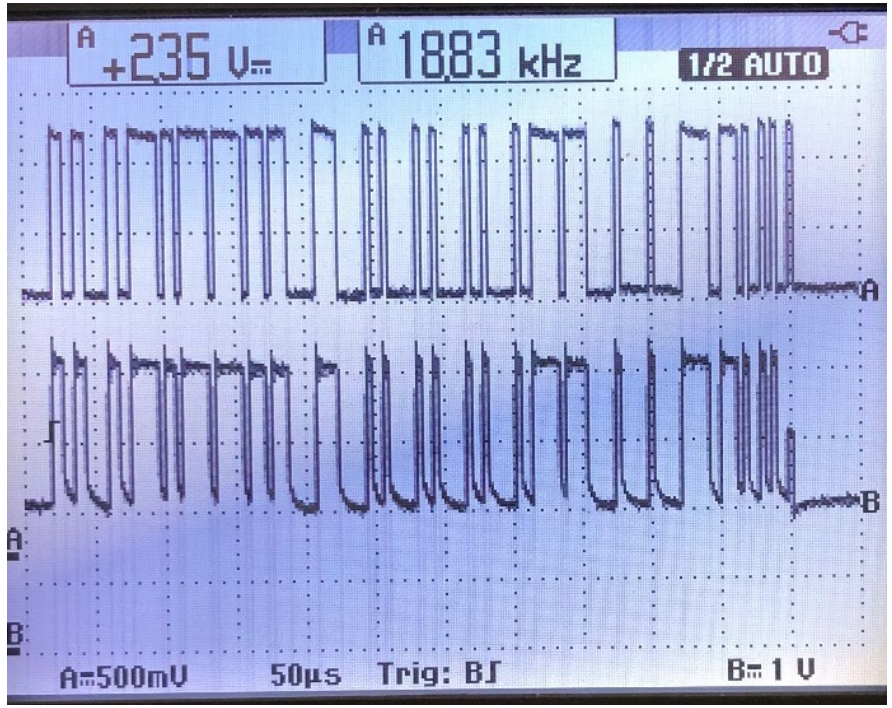
- Created to be able to display vehicle speed on a live bus
  - Offers a physical display of bus functionality
- A Teensy 3.2 Arduino compatible device emits an adjustable frequency into the vehicle speed sensor input on the test ECM
- A potentiometer is used to change the output frequency


RIGOL
T'D
H
5.000ms
100.0MSa/s
7.00M pts
D
278.800000us
T
310mV
HORIZONTAL
AUTO
J1939 Bus
ELD Bus
Undo
1
100mV
2
100mV
11:17

# Propagation Delay

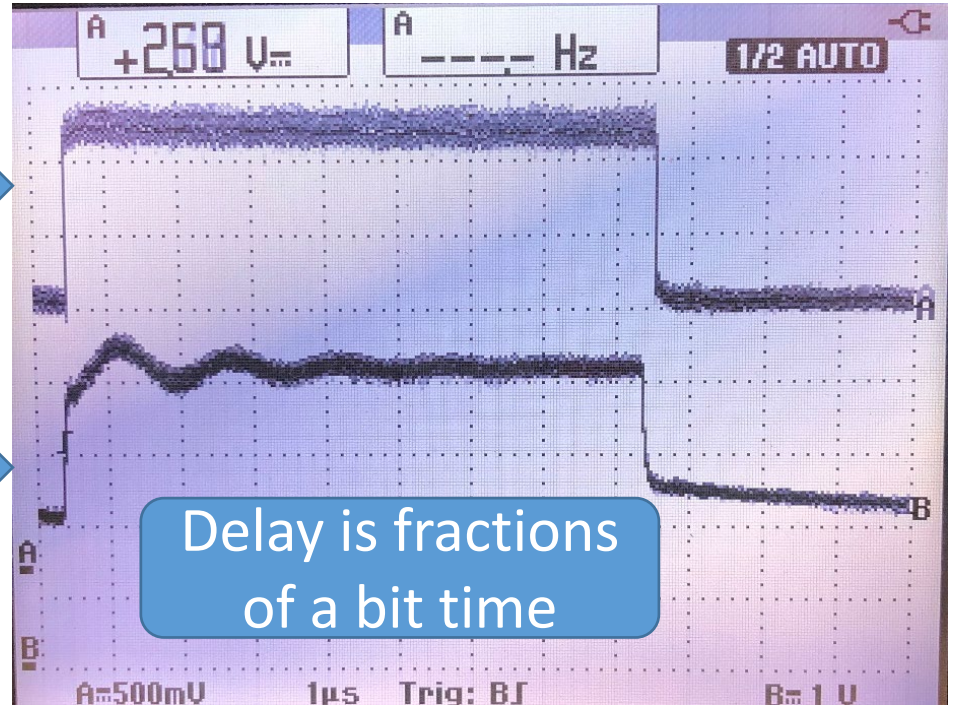
THE UNIVERSITY of TULSA
Department of Mechanical Engineering

- How long does it take for a CAN frame to move from one side of the CAN Data Diode to the other?

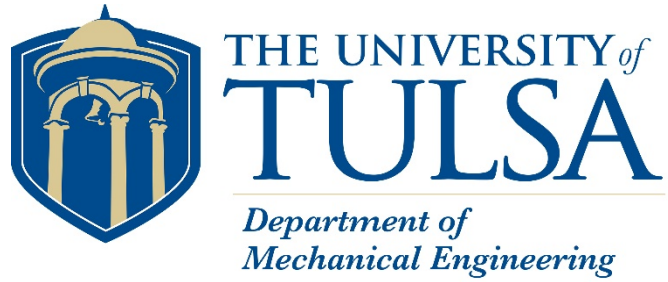



CAN High – Isolated ELD

CAN High – Normal J1939



# Denial-of-Service




- DOS attack
  - Works by sending the inherent highest priority message
    - ID = 0x00;
  - Simple attack to execute
  - When implemented, all bus communication ceases
    - Visually evident by gauge cluster no longer displaying the speed from the tone ring frequency generator

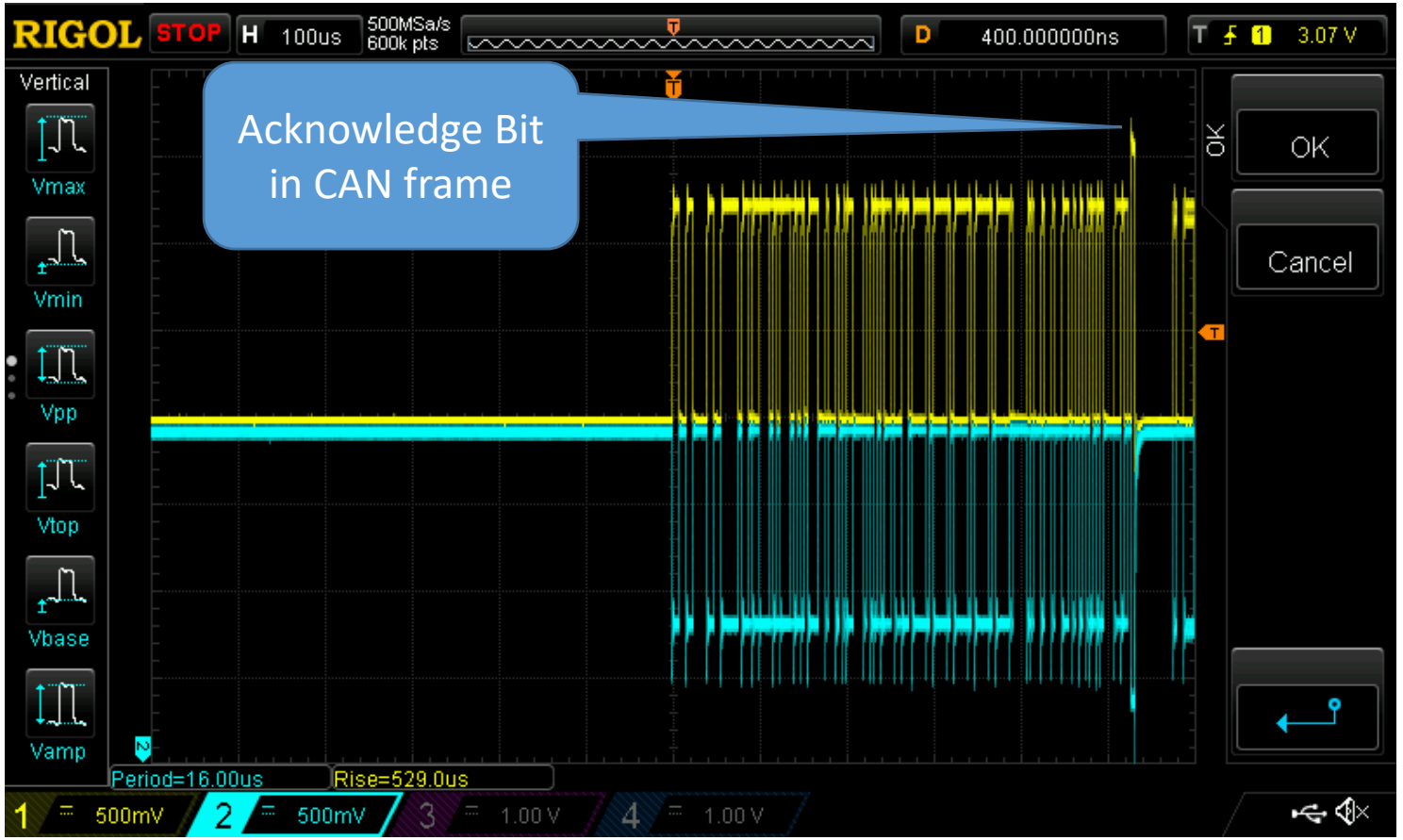
```
#include <FlexCAN.h>
#include <kinetis_flexcan.h>

FlexCAN J1939bus(250000);
static CAN_message_t txmsg,rxmsg;

void setup() {
   J1939bus.begin();
   txmsg.id = 0x00000000;
   txmsg.len = 8;
   txmsg.ext = 1;
   txmsg.buf[0 ]= 0x00;
   txmsg.buf[1] = 0x00;
   txmsg.buf[2] = 0x00;
   txmsg.buf[3] = 0x00;
   txmsg.buf[4] = 0x00;
   txmsg.buf[5] = 0x00;
   txmsg.buf[6] = 0x00;
   txmsg.buf[7] = 0x00;
}
void loop() {
J1939bus.write(txmsg);
}
```


RIGOL
TD
H 5.000ms
100.0MSa/s
7.00M pts
D 278.800000us
T
310mV
HORIZONTAL
AUTO
Unprotected J1939 Bus
ELD Bus
Undo
1 = 100mV
2 = 100mV
11:18


RIGOL
T'D
H
5.000ms
100.0MSa/s
7.00M pts
D
278.800000us
T
310mV
HORIZONTAL
AUTO
Protected J1939 Bus
ELD Bus
Undo
MENU
1
100mV
2
100mV
11:18

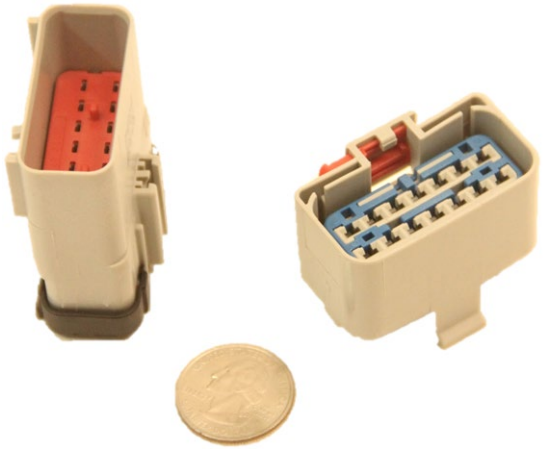
# Acknowledger

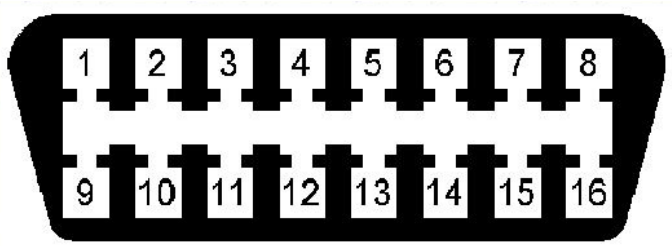
- Mechanism for reliable delivery in CAN is a CRC and Acknowledge bit.
- Other nodes send ACK bit
  - Results in higher signaling voltages on scope.
- If an isolated node does not receive an ACK bit, then it may be an error.

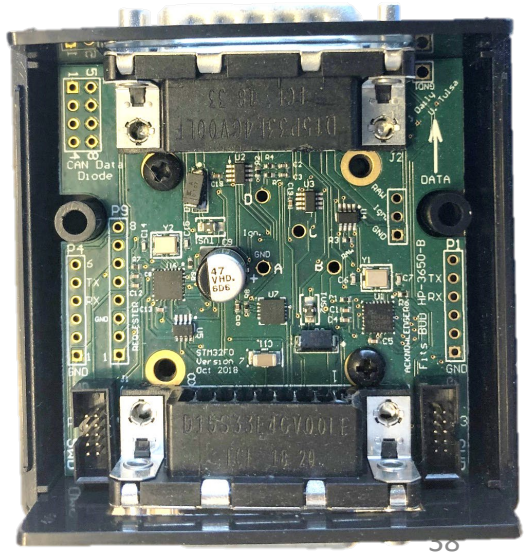


# Potential Implementations

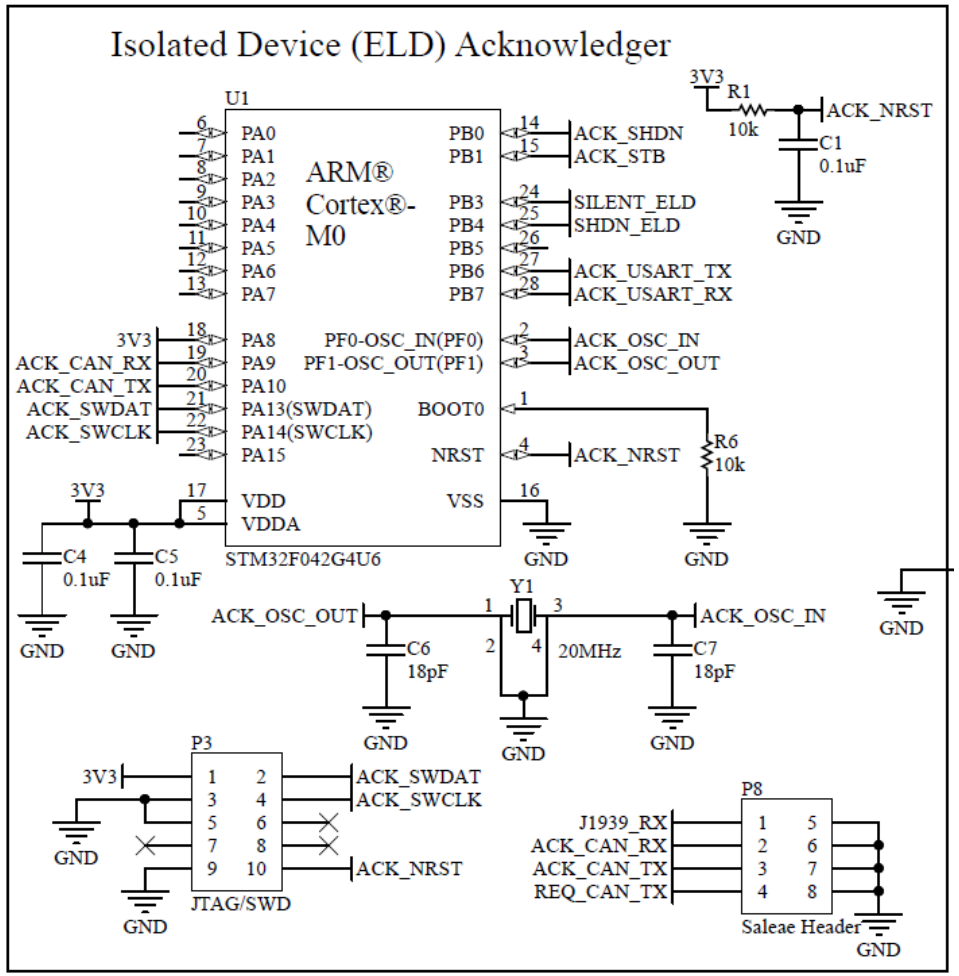
- Direct In-Line Connection
  - As displayed in testing
- DSub 15 Connection
- Delphi 14 pin Connection
- J1962 OBD-II Connection





# CAN Data Diode Acknowledger

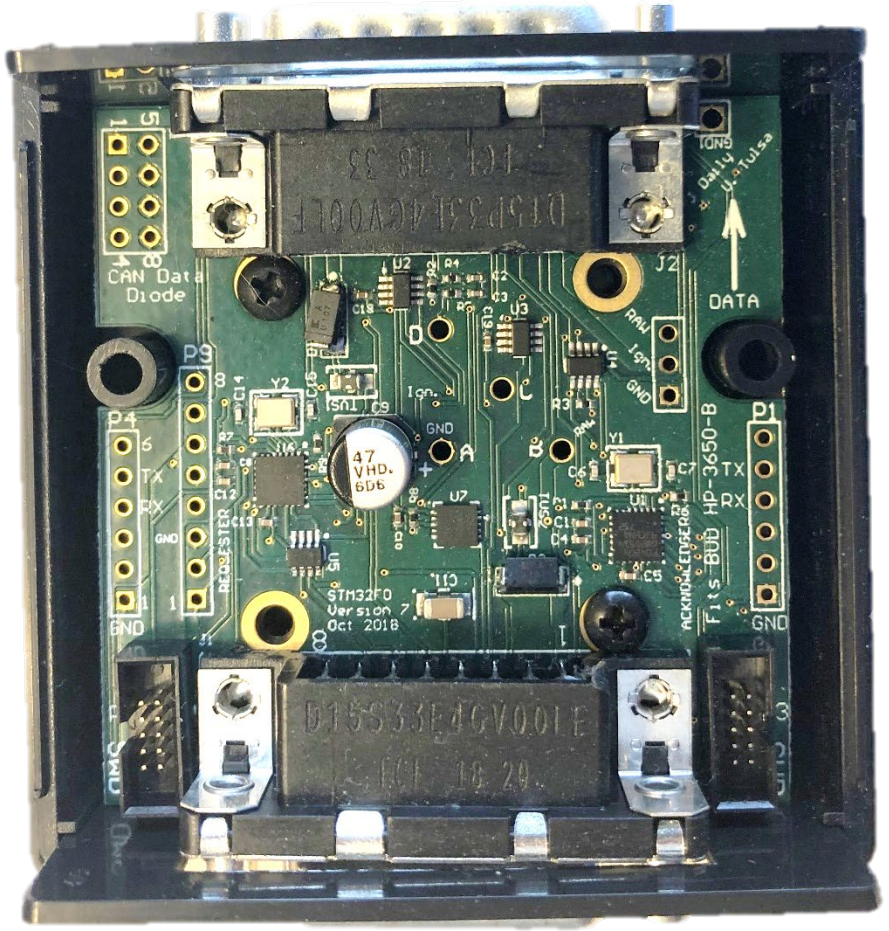



- Small, low cost CAN controller to receive valid CAN frames and send the ACK bit.
- Include a termination resistor for the Isolated node.
- Keeps isolated node from going into an error state based on lack of ACK bits.

# STM32F04 Based Design

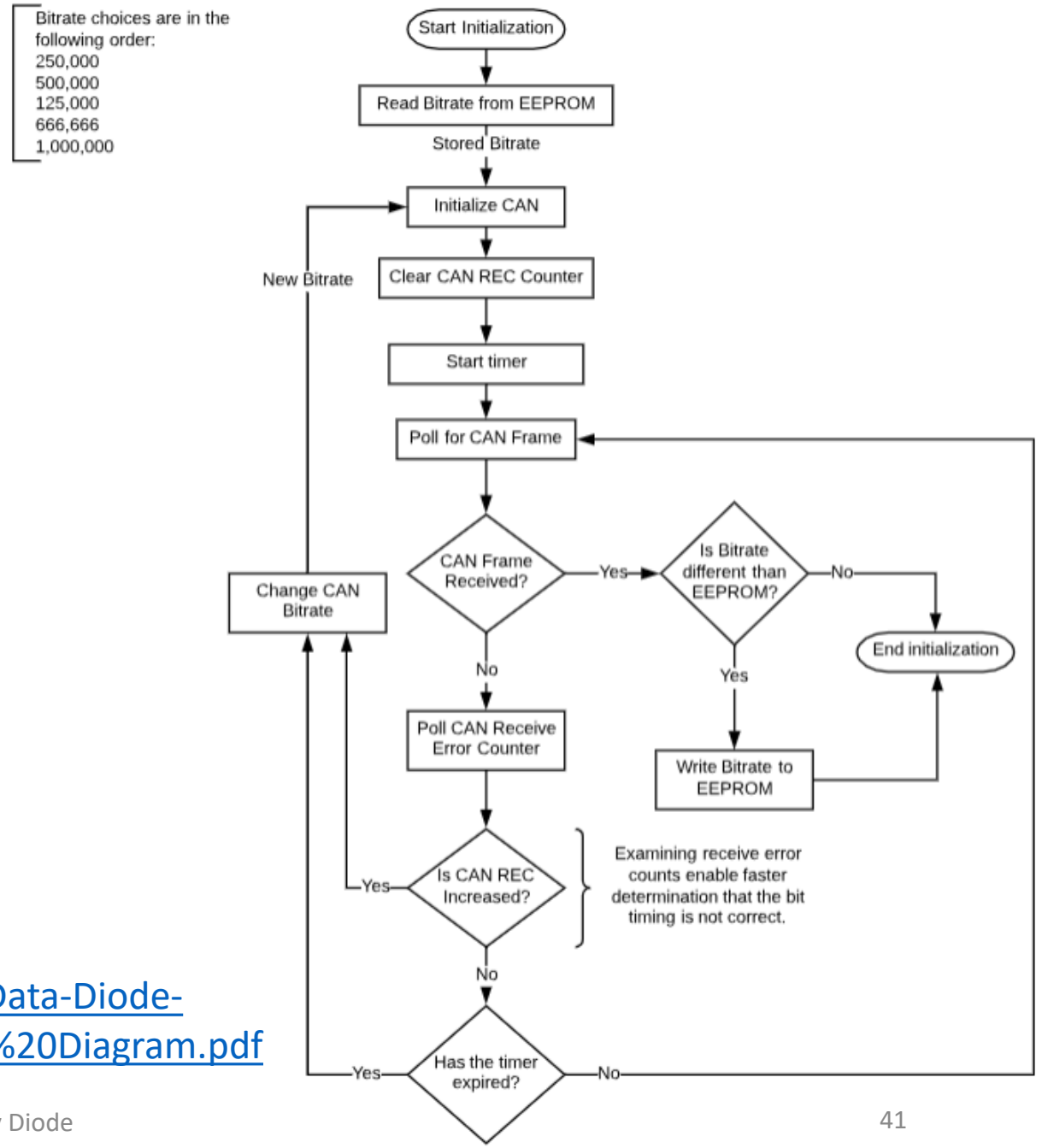
THE UNIVERSITY of TULSA
Department of Mechanical Engineering

- Back to back transceivers to implement diode functionality
- Low Cost ARM-Cortex M0 with integrated CAN controller to give acknowledgements
- Protected power and ignition.
- Use de-facto standard DSub-15 pinouts



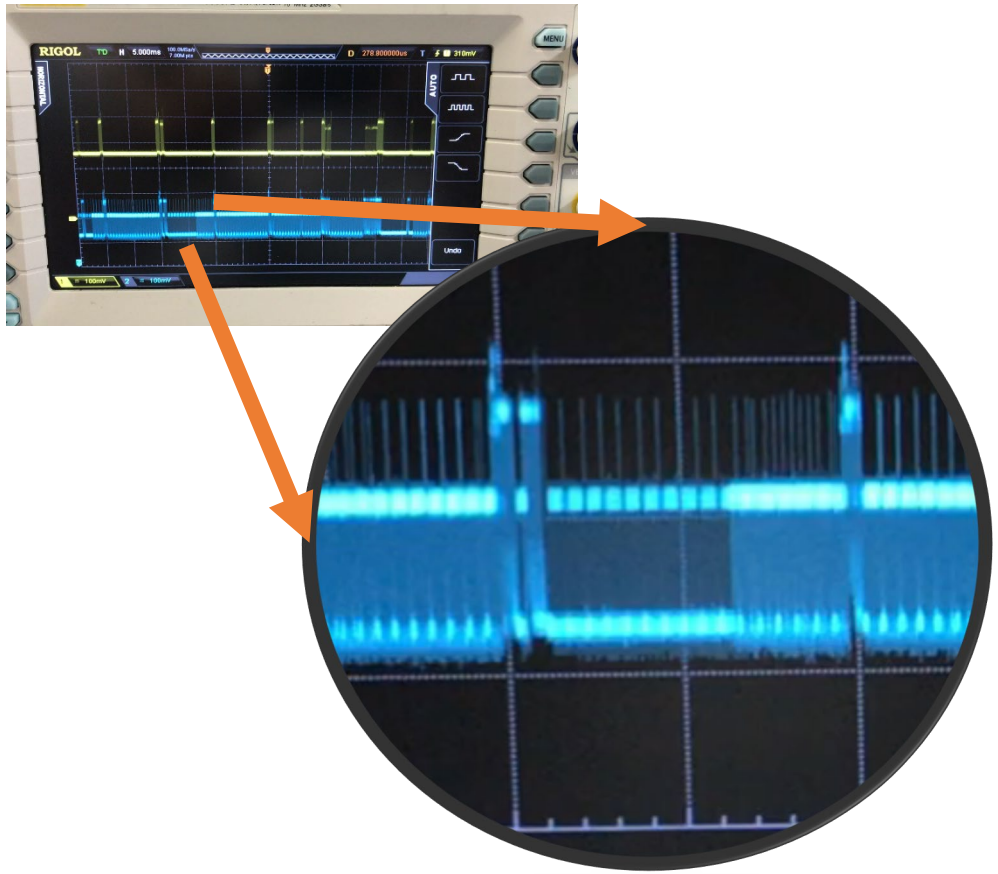
# AutoBaud Routine

- Defaults to 250k baud initially
- Once routine is executed, the final value is stored in EEPROM
- Upon repowering device, autobaud begins with the previously stored baudrate
  - Optimize time operation and power on
- Autobaud does not require messages to be sent, thus not introducing errors




https://github.com/Heavy-Vehicle-Networking-At-U-Tulsa/CAN-Data-Diode-STM32-ARM/blob/master/docs/Autobaud%20Routine%20Block%20Diagram.pdf

# Error Handling Strategy

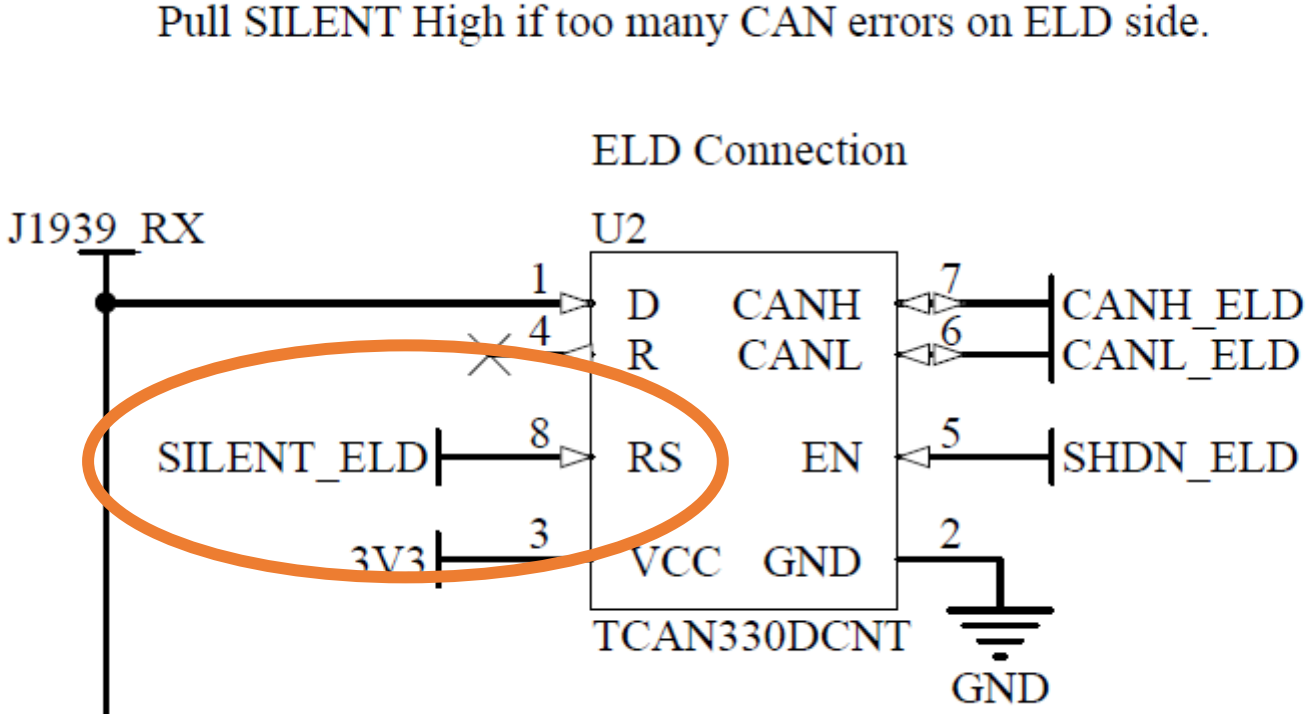



- The normal J1939 network cannot detect transmission from anything on the isolated (ELD) side.
  - ELD appears as a quiet bus
  - J1939 side will transmit regardless of the isolated side
- Scenario:
  - ELD Side is “chatty”
  - Produces errors on the isolated bus
- May not be a real problem… the isolated bus is supposed to only listen

# Error Handling Strategy

THE UNIVERSITY of TULSA
Department of Mechanical Engineering

- Acknowledger microprocessor monitors the CAN Receive Error Count (REC)
- If REC increases, pull the SILENT_ELD pin HIGH to stop transmitting data coming from the normal J1939 traffic



THE UNIVERSITY of TULSA
Department of Mechanical Engineering

# Data Diodes w/ Requests

Optional on some J1939 systems.

# ELD Mandate: Engine Hours

THE UNIVERSITY of TULSA
Department of Mechanical Engineering

## 4.3.1.4. Engine Hours

(a) An ELD must monitor engine hours of the CMV over the course of an ignition power on cycle (elapsed engine hours) and over the course of the total engine hours of the CMV's operation.

SAE J1939-71 Revised FEB2010 - 1176 -

***PGN 65253 Engine Hours, Revolutions HOURS***

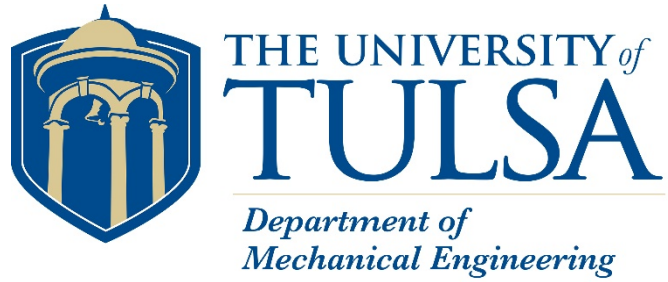
| | | |
|---|---|---|
| Transmission Repetition Rate: | On request | |
| Data Length: | 8 | |
| Extended Data Page: | 0 | |
| Data Page: | 0 | |
| PDU Format: | 254 | |
| PDU Specific: | 229 | PGN Supporting Information: |
| Default Priority: | 6 | |
| Parameter Group Number: | 65253 (0x00FEE5) | |

# Some Requests Handled by Other Nodes

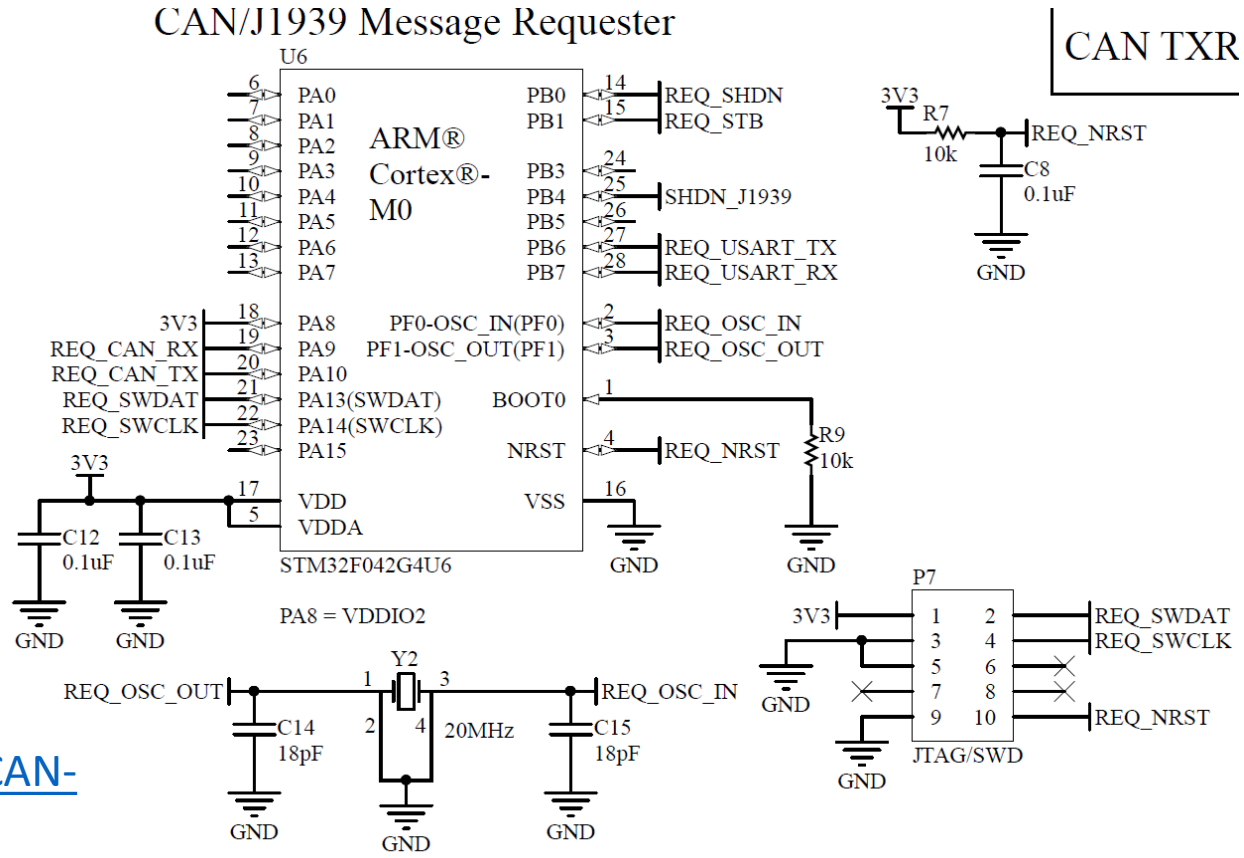
THE UNIVERSITY of TULSA
Department of Mechanical Engineering

- A ELD will be unable to request any additional information if behind a data diode.
  - VIN Number
  - Engine Hours
- The ELD is not the only node that may need to know this information
  - An instrument cluster may request Engine Hours from the ECM

# Requesting Enabled Data Diodes




- Requestor transmits out timely request messages
- Operates parallel to the ELD
- Sends requests only if not otherwise available.



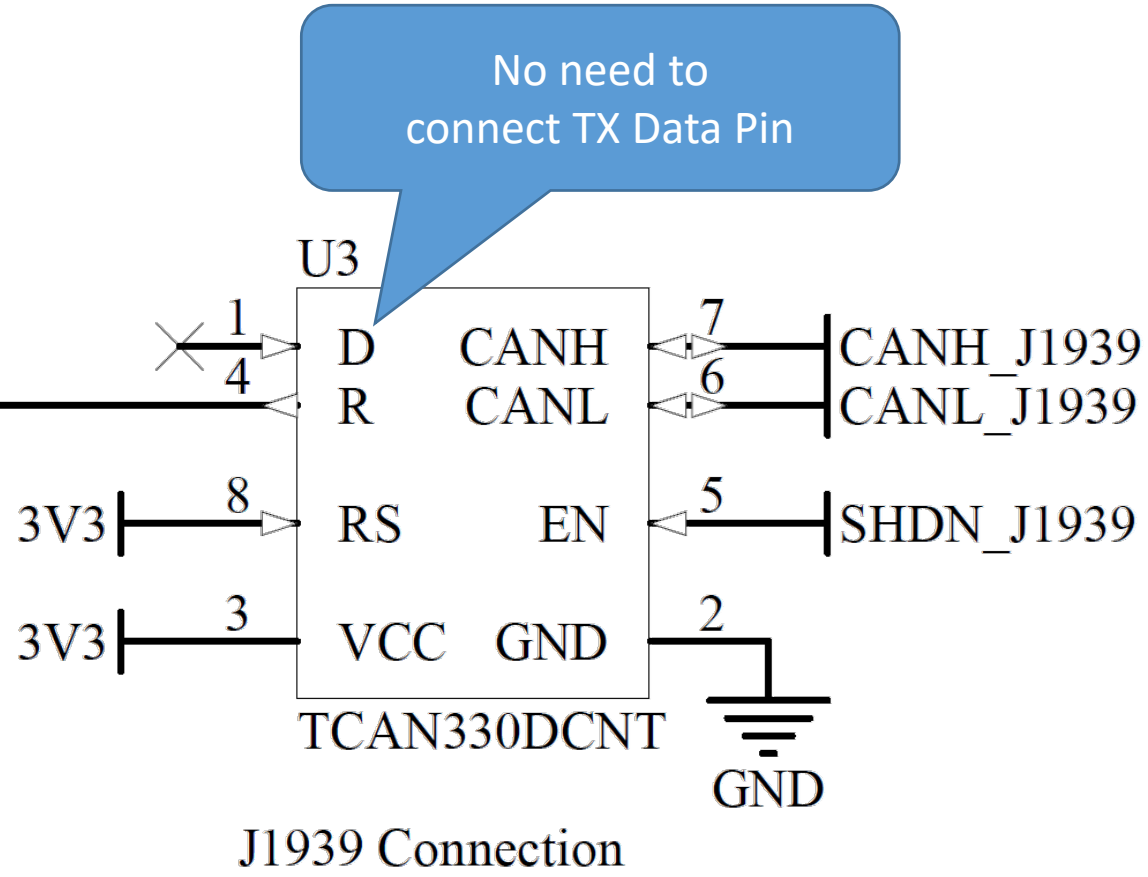

ARM Cortex 32-bit Microprocessor with CAN. Programmed with Serial Wire Debug. End User Interface through UART.

https://github.com/Heavy-Vehicle-Networking-At-U-Tulsa/CAN-Data-Diode-STM32-ARM/tree/master/docs

# New Designs

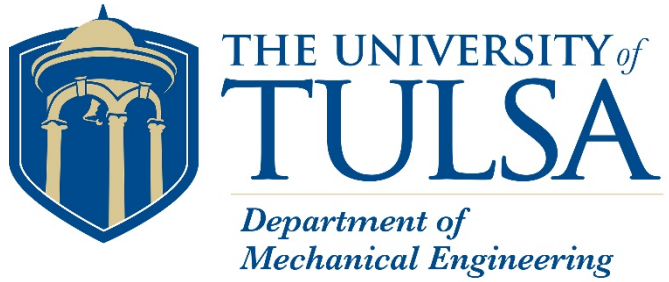
- Can you install a new radio in an old truck?
- Are radios potential attack vectors?
- Do radios need to write to CAN?

- Is it cheaper to sustain a cybersecurity program for a product's lifetime or remove a wire  from the design?




J1939 Connection

# Summary and Conclusions




- Mandated ELD connectivity created new attack vectors.
- Some modules (i.e. radio) do not need to write to the CAN bus.
- The CAN Security Data Diode is a transceiver based hardware solution to prevent isolated modules writing to the CAN bus.
- An independent CAN controller is present on the isolated side to acknowledge CAN traffic from an ELD.
- A strategy for auto-detecting CAN bitrate was explained.
- Using the transceiver silent pin helps manage bit and checksum errors when the protected network overwrites the isolated network.

# Free Samples

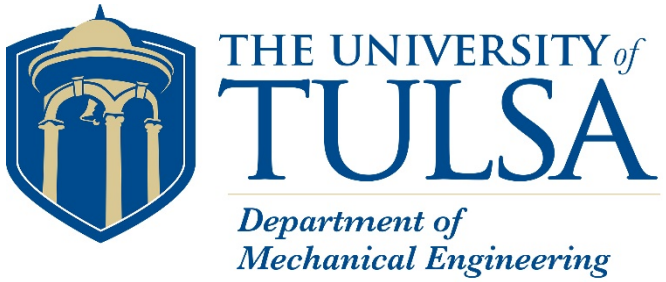
THE UNIVERSITY of TULSA
Department of Mechanical Engineering

- Limited production run available for evaluation and development
- Diode Function Work
- Github
  - Schematics
  - Altium Files
  - Gerbers
  - Friendly licensing terms
- Work In Progress
  - Validate Autobaud routine with STM32F0
  - Test Requester with ELD
  - Complete the frame error handling

https://github.com/Heavy-Vehicle-Networking-At-U-Tulsa/CAN-Data-Diode-STM32-ARM

https://github.com/Heavy-Vehicle-Networking-At-U-Tulsa/CAN-Data-Diode

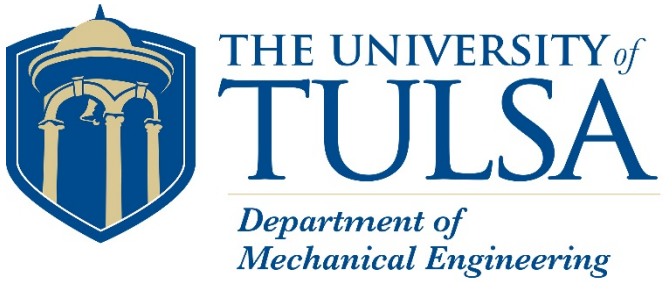
# Thank you




The support of the different industry experts that helped us when working through the different challenges associated with converting an idea into a prototype was invaluable.

Thank you for providing insight and guidance on this project.

# Acknowledgements





This material is based upon work supported by National Motor Freight Traffic Association, Inc (NMFTA). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect those of NMFTA.

# CyberTruck Challenge

- Help **develop the next generation workforce** by bringing awareness, excitement, professional involvement, and practicum based training to the heavy vehicle cyber domain.

- Help **establish a 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.

https://cybertruckchallenge.org

MICHIGAN DEFENSE CENTER

MICHIGAN ECONOMIC DEVELOPMENT CORPORATION

NMFTA

National Motor Freight Traffic Association, Inc.


https://cybertruckchallenge.org

VOLVO

VOLVO GROUP

DAIMLER

PACCAR

THE OHIO STATE UNIVERSITY

CENTER FOR AUTOMOTIVE RESEARCH

Bendix®

GEOTAB

management by measurement

Cummins®

OLD DOMINION FREIGHT LINE®

omnitracs

THE UNIVERSITY of TULSA

# Questions?

Name: Jeremy Daily

Email: jeremy-daily@utulsa.edu

Phone: (937) 238-4907

Name: Hayden Allen

Email: hayden-allen@utulsa.edu

Phone: (918) 645-4938

THE UNIVERSITY of TULSA

Department of Mechanical Engineering

# Supplemental Slides

THE UNIVERSITY of TULSA
Department of Mechanical Engineering

# How Much Does It Cost?

# Adding an ELD

- The FMSCA projects that adding a web supported ELD will cost $419 annually, with an initial purchase price of $500/unit.
- USB 2.0 or Bluetooth ELDs will cost $166 annually.
- How much would adding a diode cost?

In today's rule FMCSA estimates the annualized cost for an ELD that must support one of two options for electronic transfer. The first option is a telematics type ELD. We estimate a total annualized cost of $419 for an ELD with telematics. The RIA prepared for the SNPRM assumed an annualized device cost of $495, which FMCSA acknowledged was on the high end of the range of costs of existing units. The $495 figure cited by OOIDA is therefore no longer relied upon by the Agency. The reduction in the estimated annualized cost for an ELD with telematics, from $495 to $419, is largely attributable to the reduction in purchase price of the device from $799 to $500. The second option is a local transfer method type ELD (ELD with USB 2.0 and Bluetooth). The estimated annualized cost of an ELD with USB 2.0 and Bluetooth is $166. The lower price

# Data Diode Prototyping Costs

- Amphenol/Deutsch 9-pin Connector: $9.22
- 4 Deutsch PCB pins: $8.00
- M/F J1939 Type II Pigtail Cable: $11.84
- CAN Data Diode Assembled Printed Circuit Board: $72.49
- Backshell and Compression Nut: $7.05
- 0.25 Hours Assembly: $5.00
- Total: $113.60

Aug. 8, 2014

Advanced Assembly
SMT Assembly for Engineers

**Quote 68022**

| Reference Quote Number |
|---|
| 68022 |

| Customer Name: | Buyer/Contact | Contact Information: | Part# - Rev | PCB Rev: |
|---|---|---|---|---|
| University of Tulsa | Jeremy Daily | jeremy-daily@utulsa.edu | CanDiodeWTXRX | |

**Base Quote (Quantities & Days)**

**Select One Base Quote**

| | |
|---|---|
| 25 Assemblies, 5 Day; Parts; PCBs 5 Day | $1,489.53 |

**Quote Specifications (Counts Per Board)**

| | |
|---|---|
| SMT / THT Count: | 18 / 0 |
| Line / Fine Pitch Count: | 11 / 0 |
| X-Ray Count: | 0 |
| Assembly Sides: | Top |
| Assembly Types: | SMT&THT |
| RoHS Required: | YES |
| ITAR Required: | NO |

**Options**

| Quoted By: | Date: | Email: | Phone: |
|---|---|---|---|
| Ashlie Johns | 4/19/2017 | ajohns@aapcb.com | 720-484-3013 |

Add Shipping Acct: Example: "UPS 12F3Y4"

AA Overnight

Discount: $-250.00
Order Total: $ 1,762.30
Per Board: $ 70.49
11 Business Days

Place Order

Total Includes Shipping and NRE