33rd Annual INCOSE international symposium

hybrid event

Honolulu, HI, USA
July 15 - 20, 2023

Jake Jepson, Subhojeet Mukherjee, Martin Span, Dr. Jeremy Daily – Colorado State University – INCOSE IS 2023

CANLay – A Network Virtualized Testbed for Vehicle Systems – Improving Systems Integration and Verification Efforts

Digital Engineering

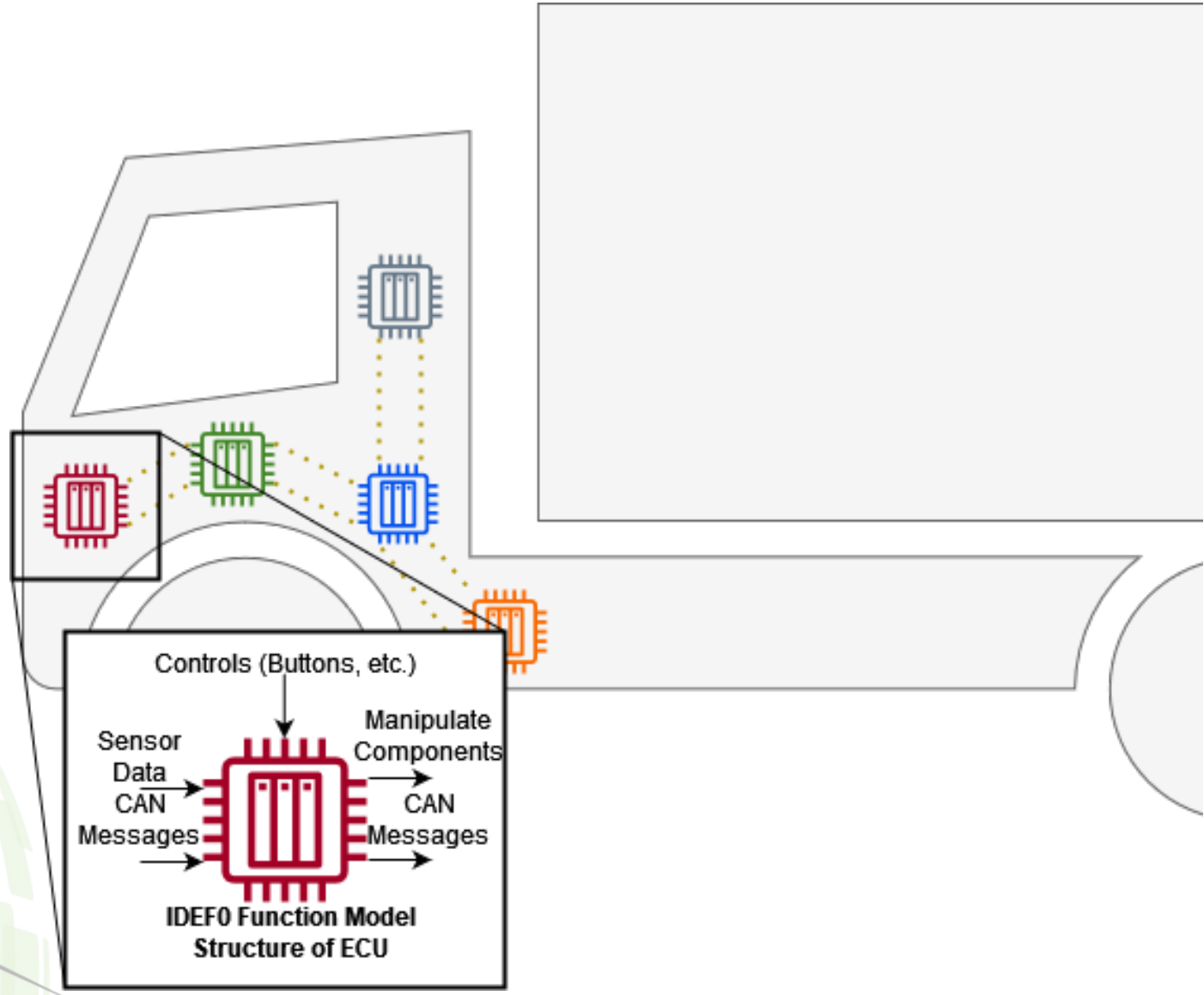
- Innovative, integrated digital approach to system design.
- Utilizes authoritative sources of system data and models for lifecycle activities.
- Digital Engineering is being adopted industry wide, especially in cyber-physical system design.
    - Department of Defense has a Digital Engineering Strategy directing its use in complex system design.

DE Challenges in Horizontally Integrated Industries

- Original Equipment Manufacturers (OEMs) may lack access to the complete technology stack.
  - Hinders comprehensive digital engineering.
  - As such, digital engineering approach must incorporate embedded hardware to represent the unavailable intellectual property.
- Hybrid method enables scalable, approach to testing at a systems level.

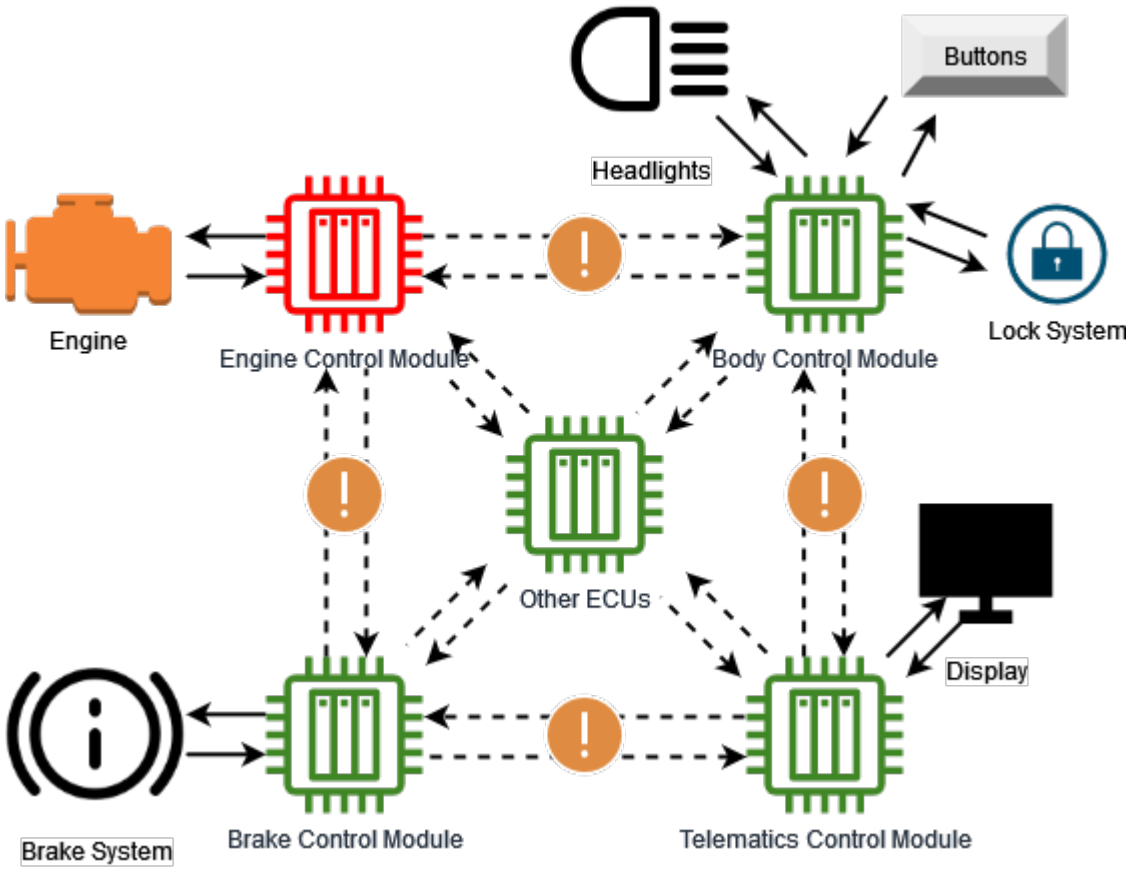
Brief Overview of: Electronic Control Units (ECUs)

- TLDR: They are the computers that control the vehicle.
- ECUs are embedded systems controlling electrical systems or subsystems in a vehicle.
- Essential for functions like engine management, transmission control, braking, and more.
- Increase vehicle efficiency, safety, and comfort.
- Contain proprietary information.



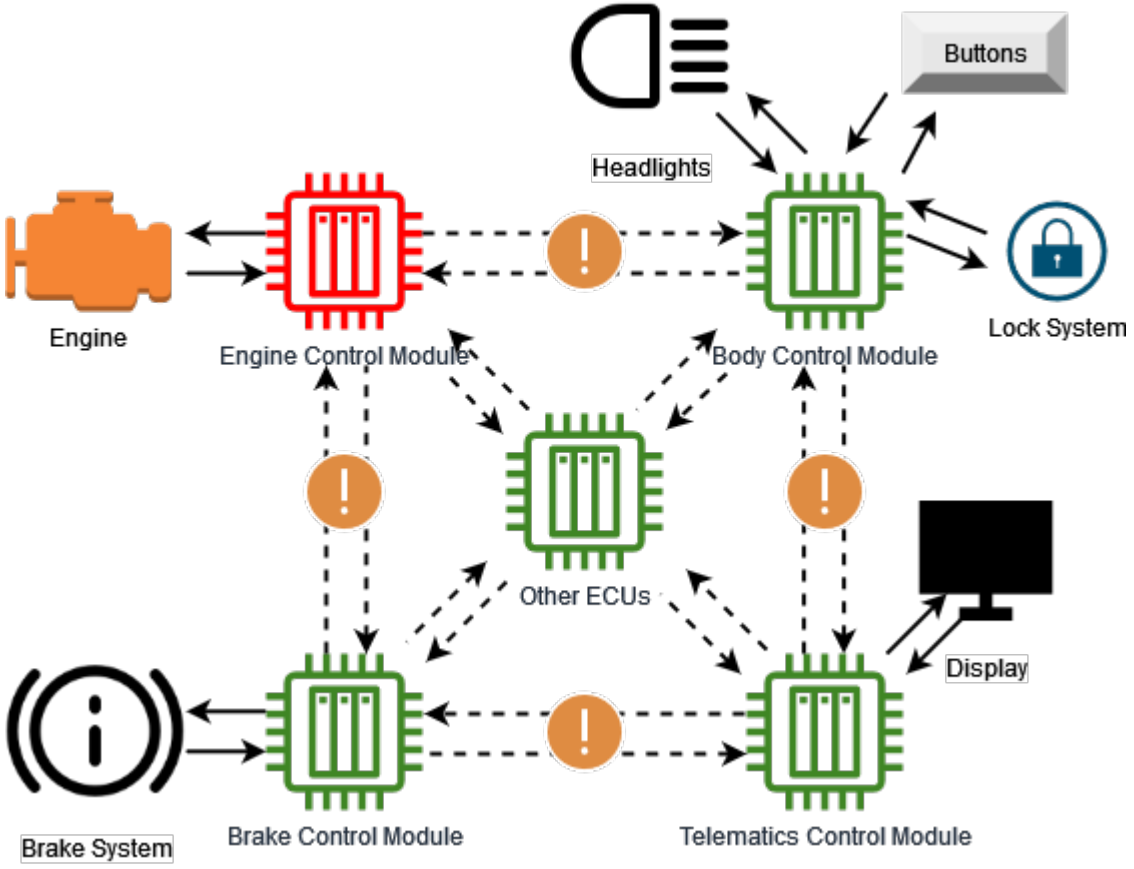
Brief Overview of: Controller Area Network

- Vehicle bus standard allowing inter-device communication
- Operates at OSI model's data link layer.
- Multi-master serial bus for networking Electronic Control Units (ECUs).
- Provides error detection, fault confinement, data consistency.
- Widely used in automotive and industrial applications.



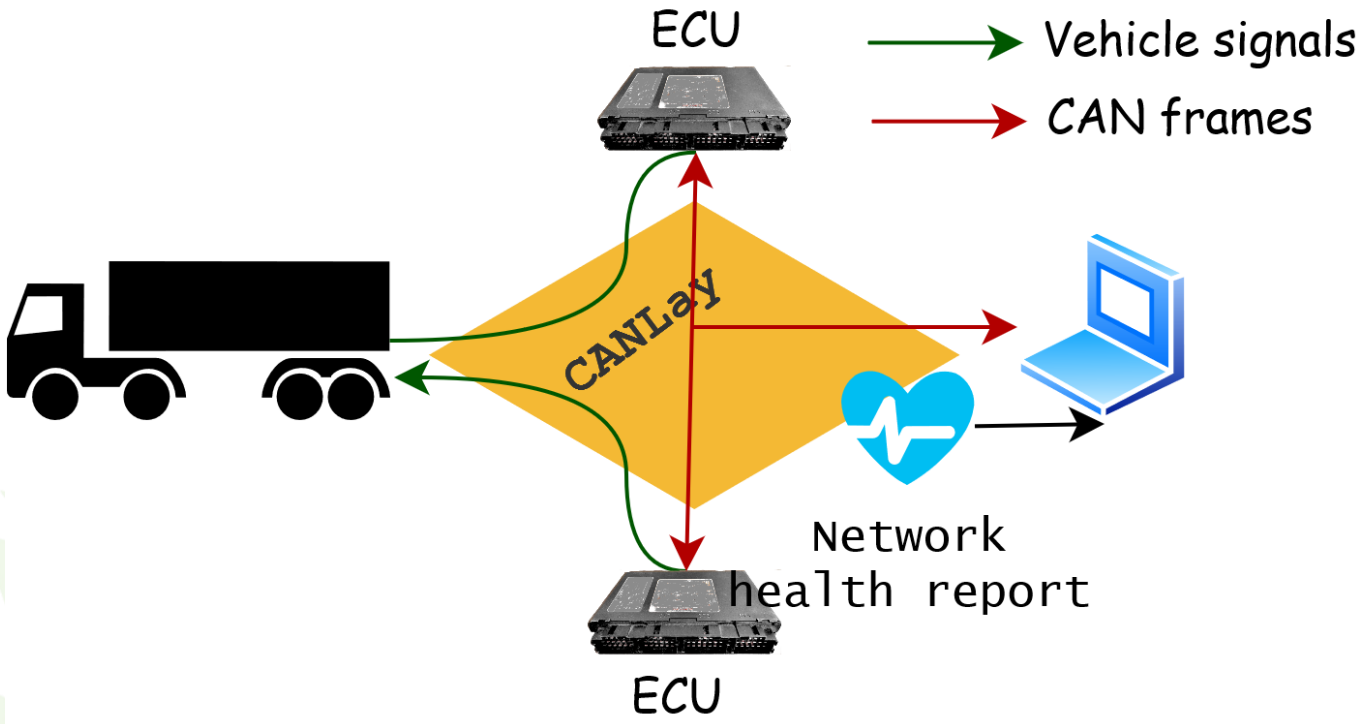
Brief Overview of: J1939

- High-level communications protocol for heavy-duty vehicles and industrial equipment.
- Operates on top of CAN, facilitates communication between ECUs.
- Defines messages for diagnostic, control, etc.
- Promotes standardization and interoperability in the industry.
- Defines standards that operate at the OSI layers 1, 4, 5, and 7.



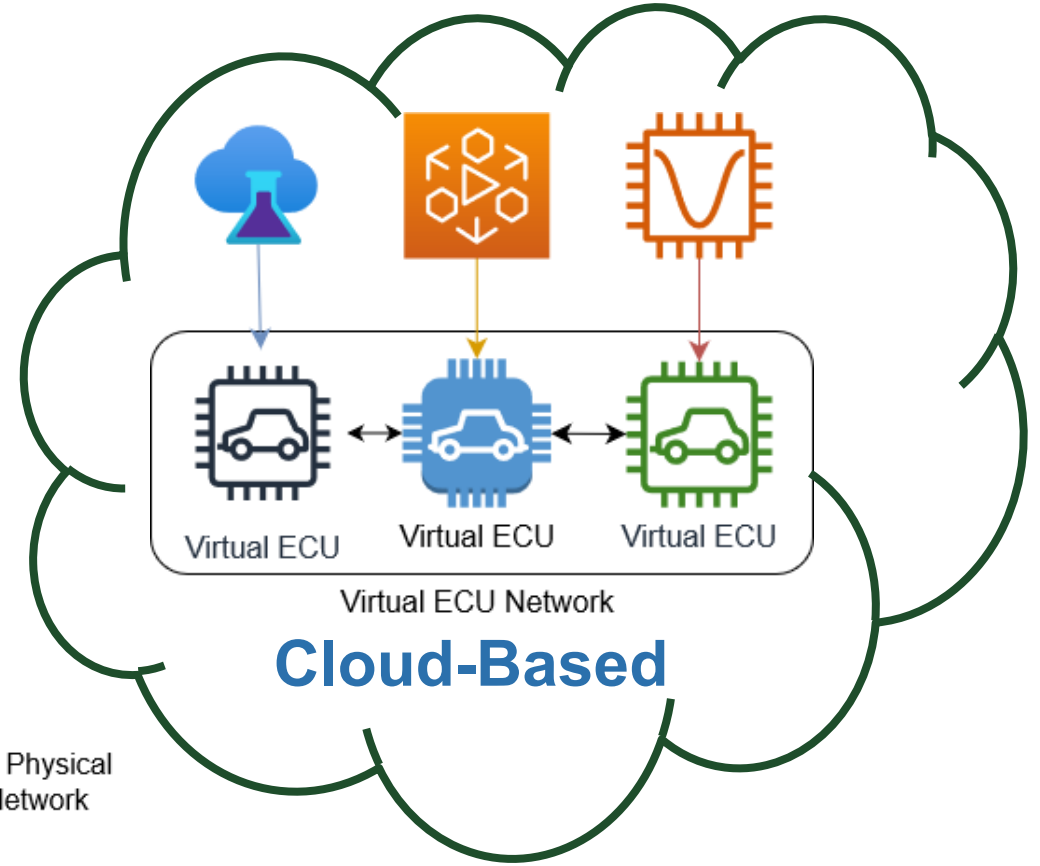
Introduction to CANLay

- CANLay: A network-based testbed enabling virtual configurations of real Electronic Control Units (ECUs)
- Allows early implementation testing and verification.
- Tests system configurations virtually, reducing the need for specific hardware test benches.
- Employs IP frames encapsulating traditional CAN frames.
- Test system can be established once and reconfigured for many systems architectures.

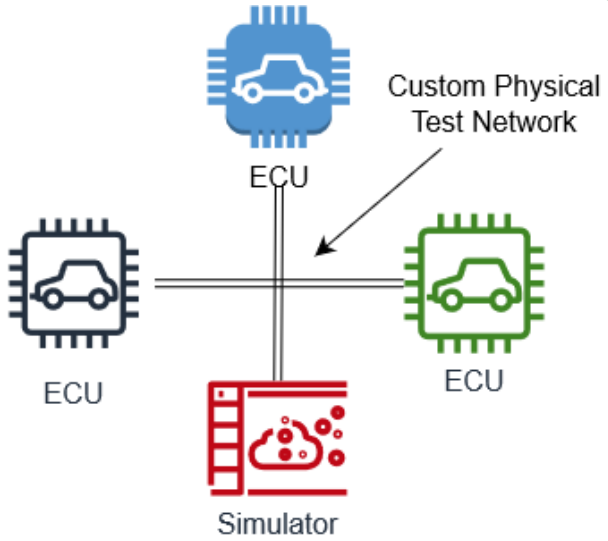


Current and Prior Efforts 1/2

- Commercial Solutions $$$
  - Cloud-based test beds
    - Fast
    - Flexible
    - Scalable
    - Requires access to source code
    - Isolated – may not represent complete system
- Hardware-in-the-loop test beds
  - Flexible
  - High fidelity
  - Limited range



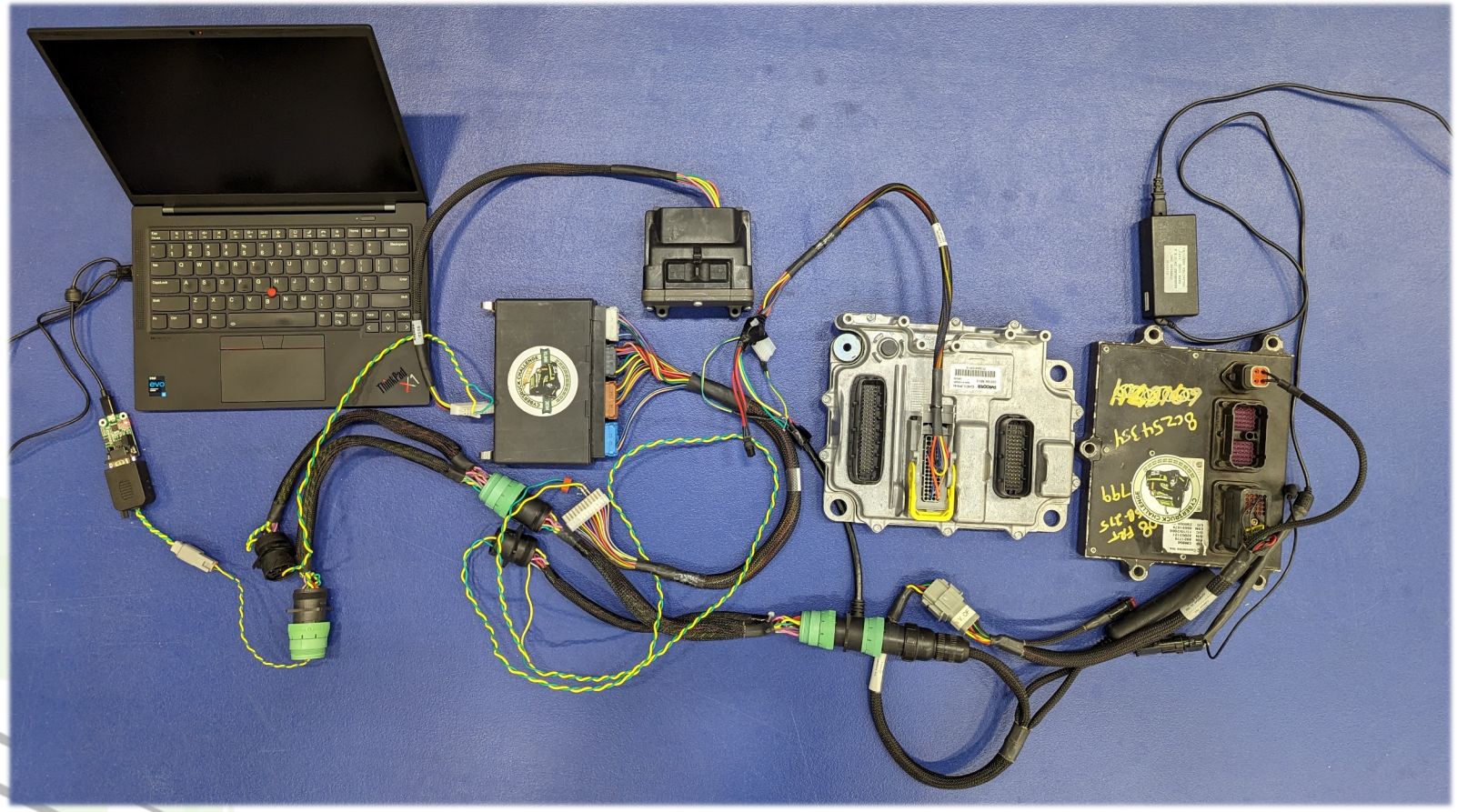
Cloud-Based



Hardware-in-the-Loop Test Beds

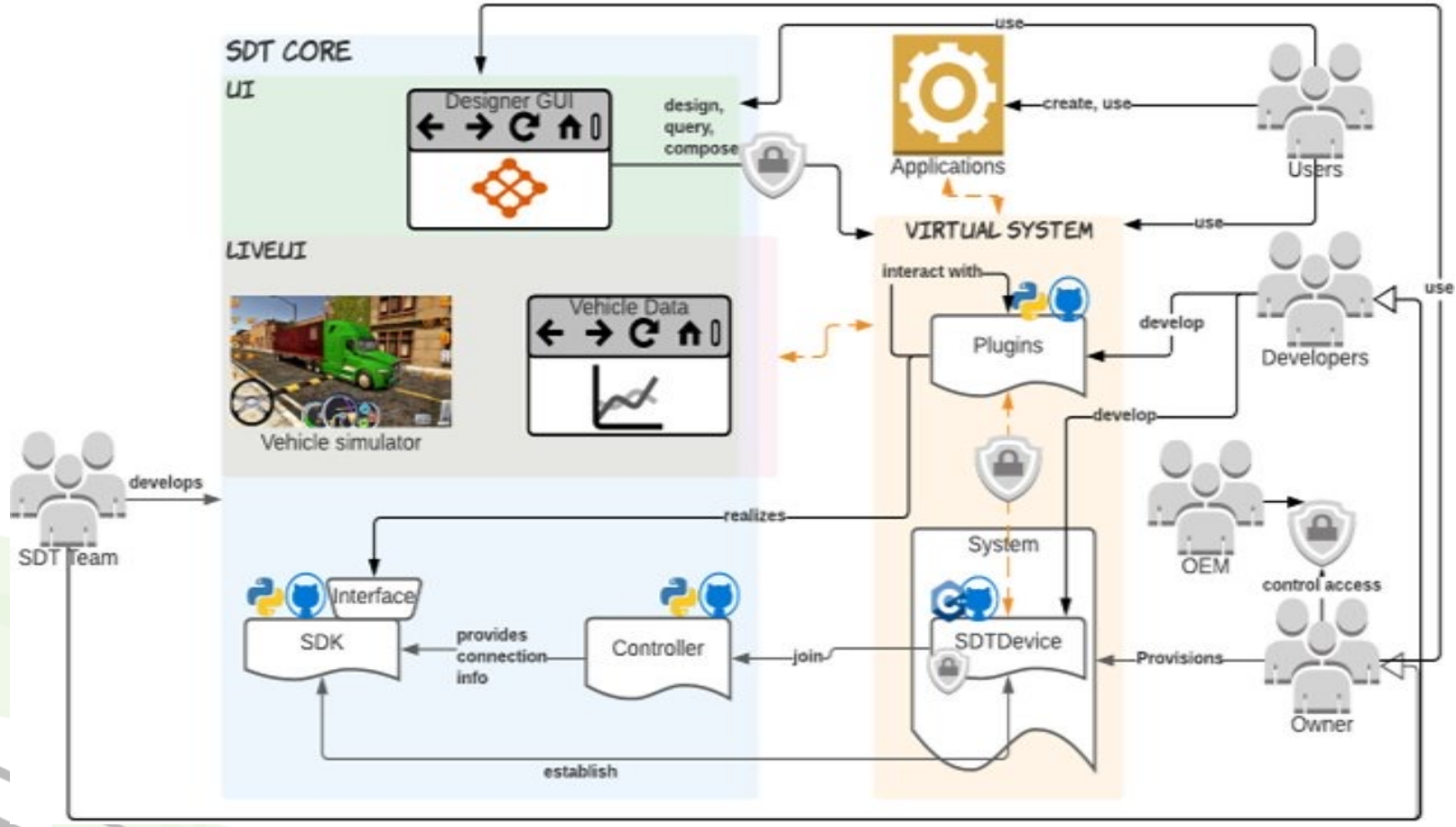
Current and Prior Efforts 2/2

- Manually building test beds
  - High fidelity
  - Low cost
  - Not flexible
  - Time consuming
- SocketCAN over Ethernet: Cannelloni, etc.
  - Lacks reconfigurable networks
  - Lacks support for auxiliary signals (event-driven testing)
- Software Defined Network for CAN
  - Built for in-vehicle networking



Software Defined Truck (SDT)

- Conceptual framework for CAN-based security testing in heavy vehicles.
- Globally accessible network of connected ECUs:
  - Encourages collaboration.
  - Provides expensive resources to limited-funding research projects.
- Remotely accessible, on demand reconfigurable CAN networks.

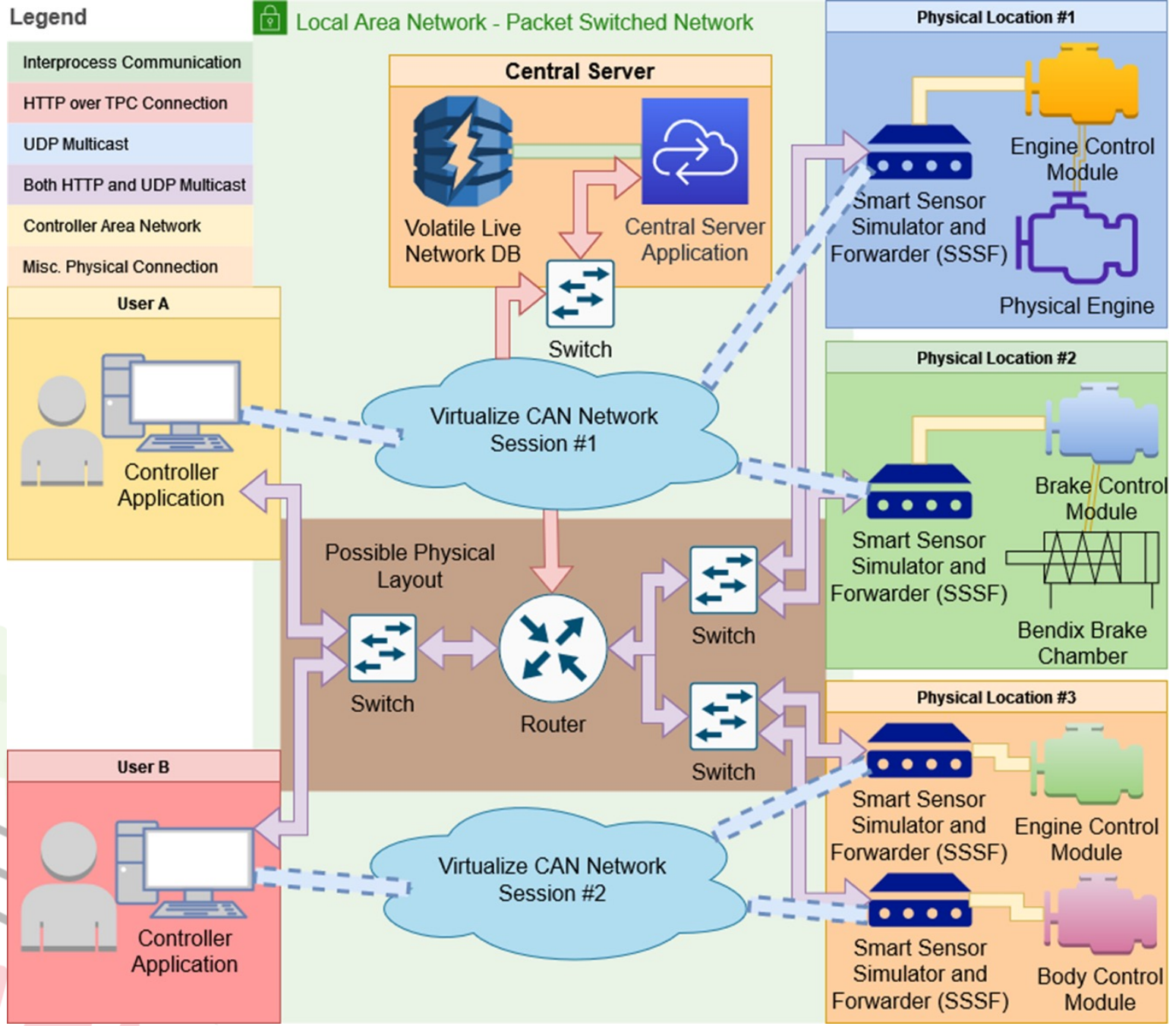


SSSF

- Smart Sensor Simulator and Forwarder
- Derivative of the Smart Sensor and Simulator devices.
  - Simulates sensor inputs to an ECU.
  - Interfaces with the CANLay network.
  - Compatible with Arduino Integrated Development Environment.
  - More information about the Smart Sensor Simulators and its evolution can be found here: https://github.com/SystemsCyber/SSS3

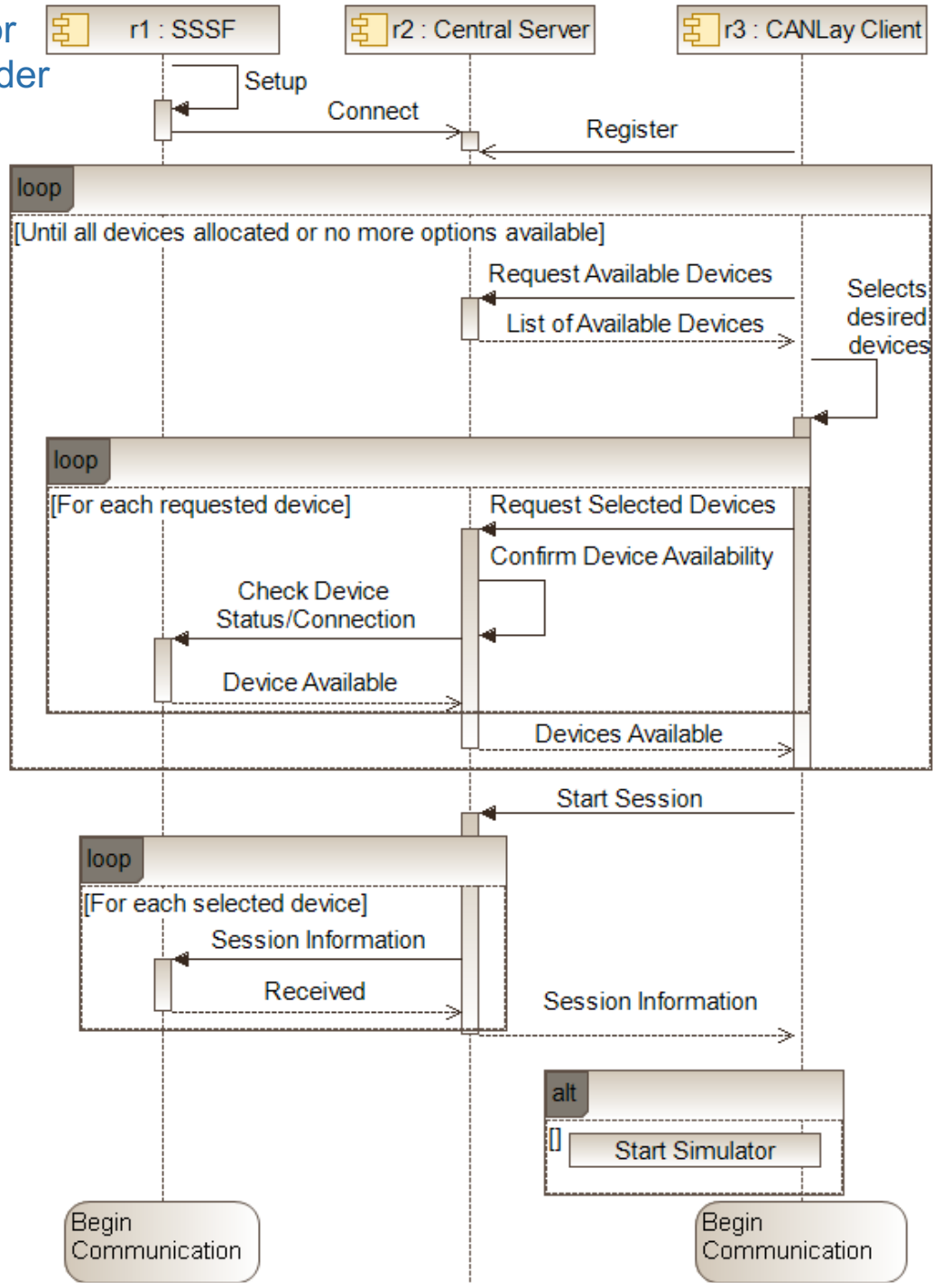
Design of CANLay

- Client: User Interface
- CANLay API: network management.
- Smart Sensor Simulator and Forwarder: Gateway for ECUs, forwards sensor signals and CAN data.
- Server: Brokering, device management, and API handling.
- Vehicle Simulator: Provides realistic signals for event driven testing.
- Physical Devices: ECUs for data exchange and testing.



Implementation of CANLay 1/3

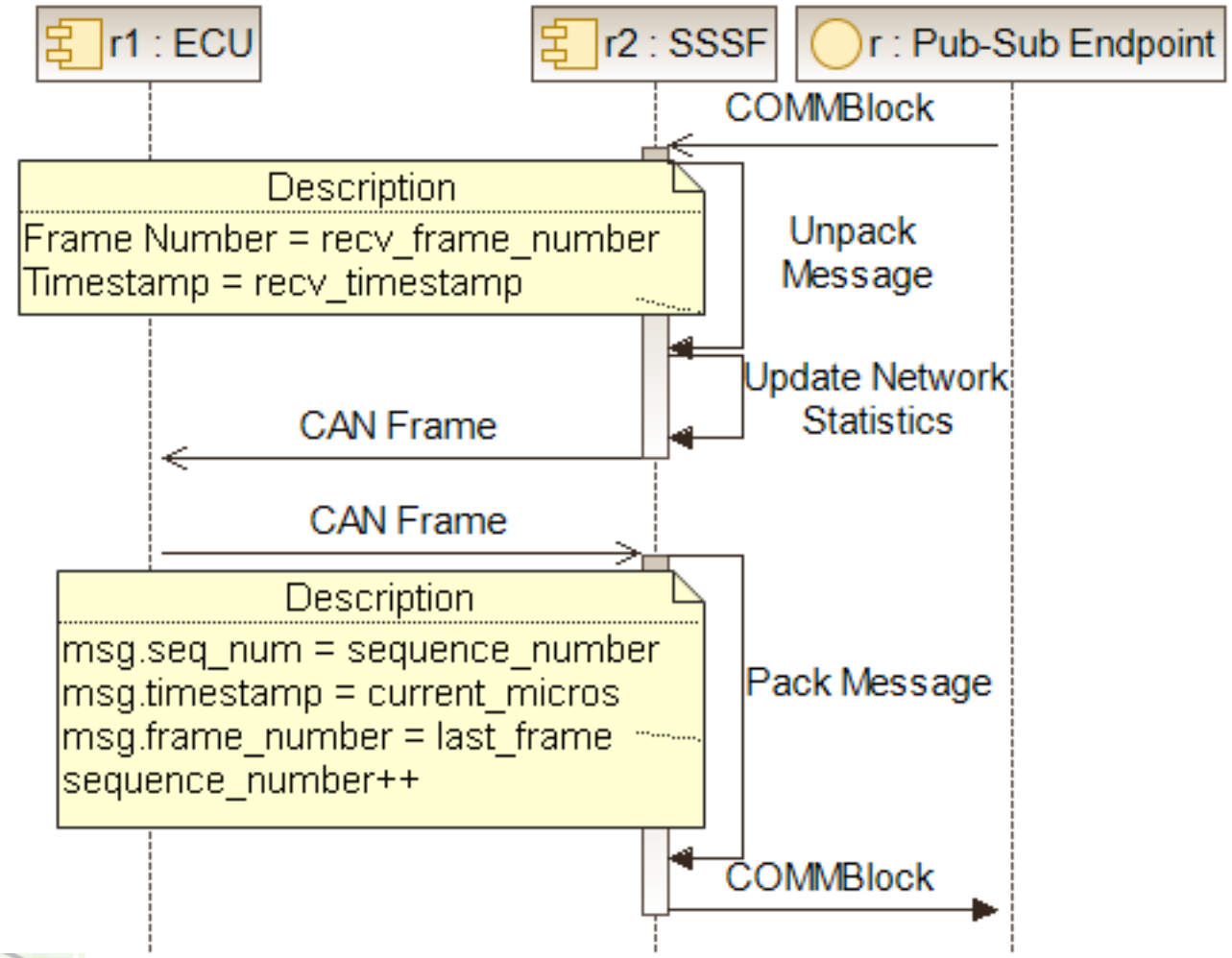
- CANLay Setup Process:
  - SSSFs connect and send ECU info to Server.
  - Controller registers and requests available ECUs.
  - Server checks registration and availability, assigns endpoint.
  - Connection data is sent to Controller and SSSFs.
  - Endpoints synchronize time, allocate data structures, and start forwarding messages.
- Launch simulator if applicable.



Implementation of CANLay 2/3

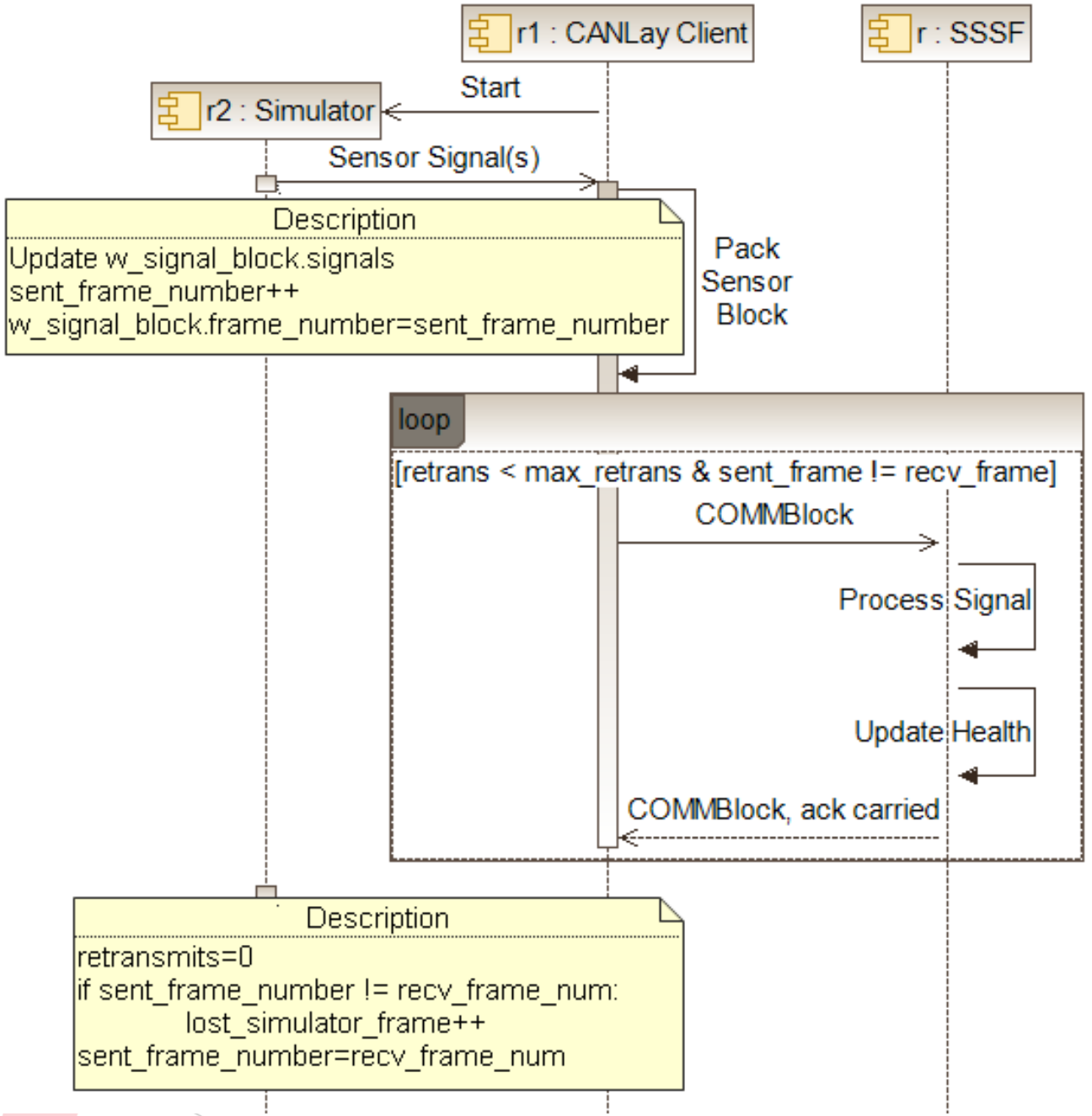
- CANLay CAN Exchange Process:
- Smart Sensor Simulator and Forwarders:
  - Exchange CAN messages between the Pub/Sub network its attached ECU(s)
  - Update statistics upon receiving and sending CANLay messages.
- Controller (not shown):
  - Exchanges CAN messages between the user and the Pub/Sub network.
  - Update statistics upon receiving and sending CANLay messages.

SSSF: Smart Sensor Simulator and Forwarder



Implementation of CANLay 3/3

- CANLay Signal Exchange Process:
  - Controller forwards sensor signals to pub/sub endpoint.
  - SSSFs receive and forward sensor frames. (if applicable)
  - Controller resends sensor messages until acknowledged or max retransmissions.
- Network health monitoring tracks latency, jitter, packet loss, and goodput (application throughput).



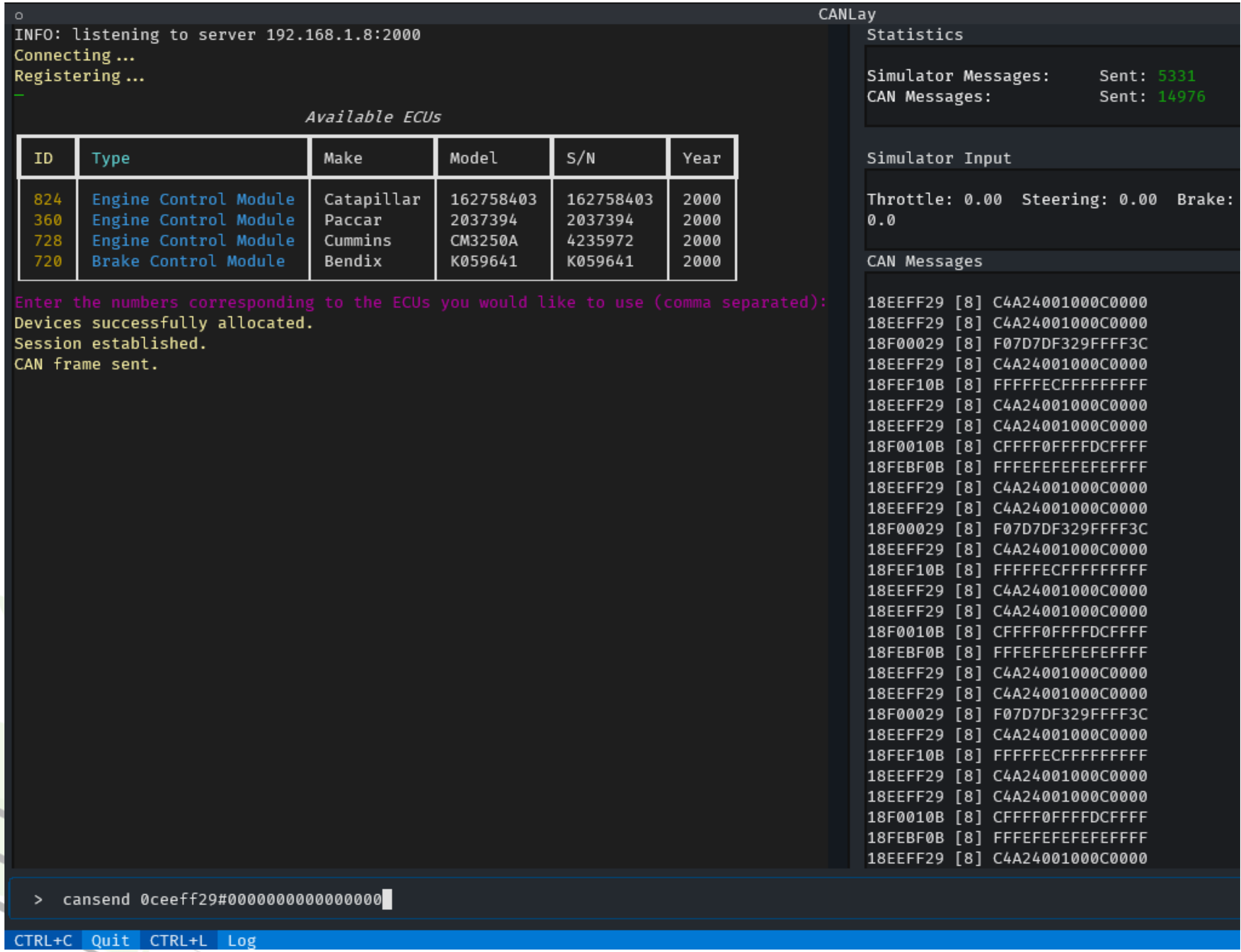
CANLay's API

- Controller application interfaces with CANLay using a set of APIs.
- Key API features include:
  - Device registration and setup.
  - Retrieving and selecting devices.
  - Sending sensor signals to pub/sub endpoint.
  - Monitoring network health.
  - Controlling message (re)transmission.
  - Managing network connections and synchronization.
  - Accessing transport and network health data structures.

AI generated to fill page based on prompt: API

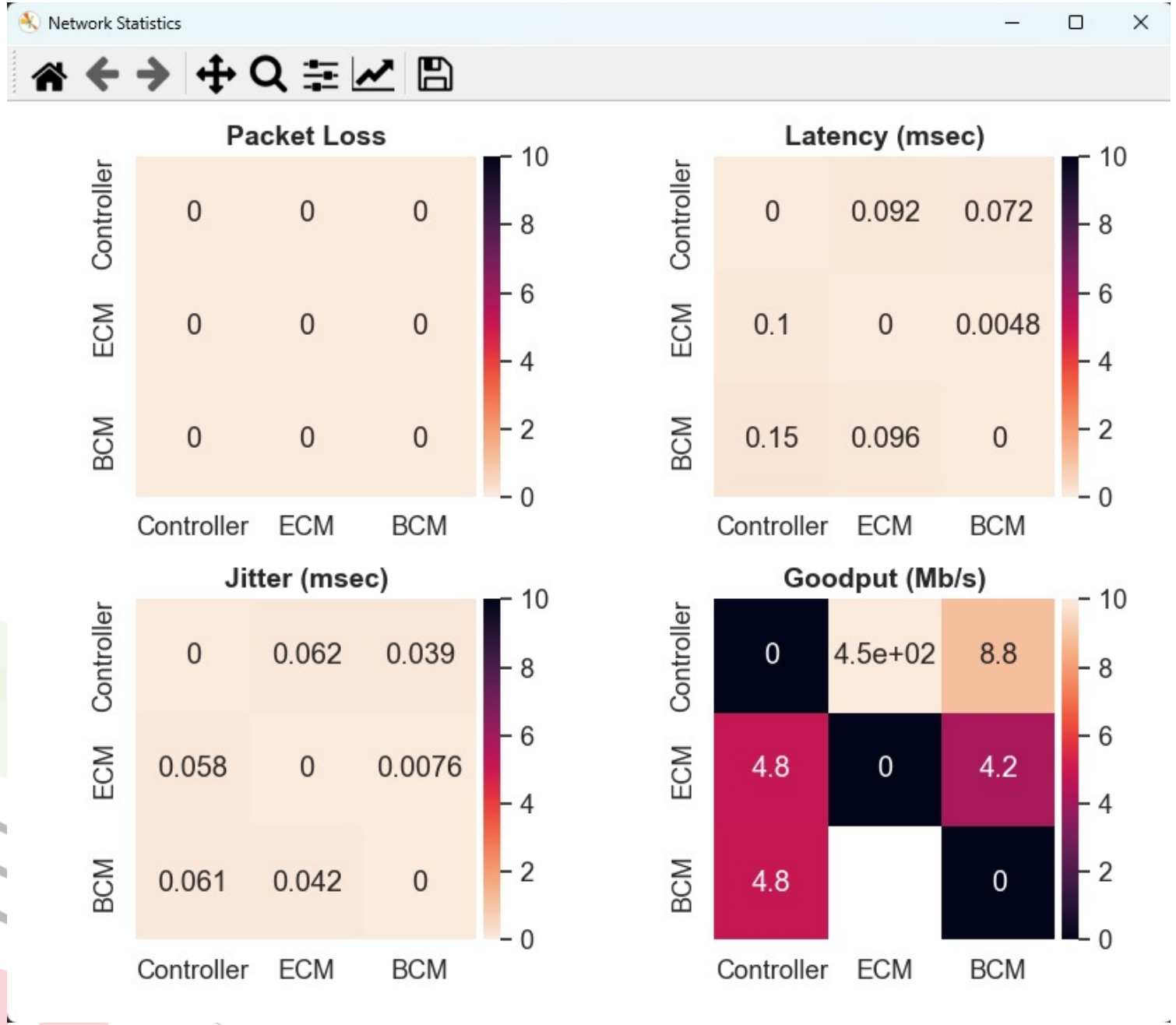
CANLay's TUI

- CANLay's TUI (Text User Interface) provides a bare-bones interface for interacting with the CANLay API.
- Key features of the TUI include:
  - Device discovery and selection.
  - Session setup and configuration.
  - Sending sensor signals and CAN messages.
  - Viewing network statistics and reports.
  - Managing experiment sessions and connections.



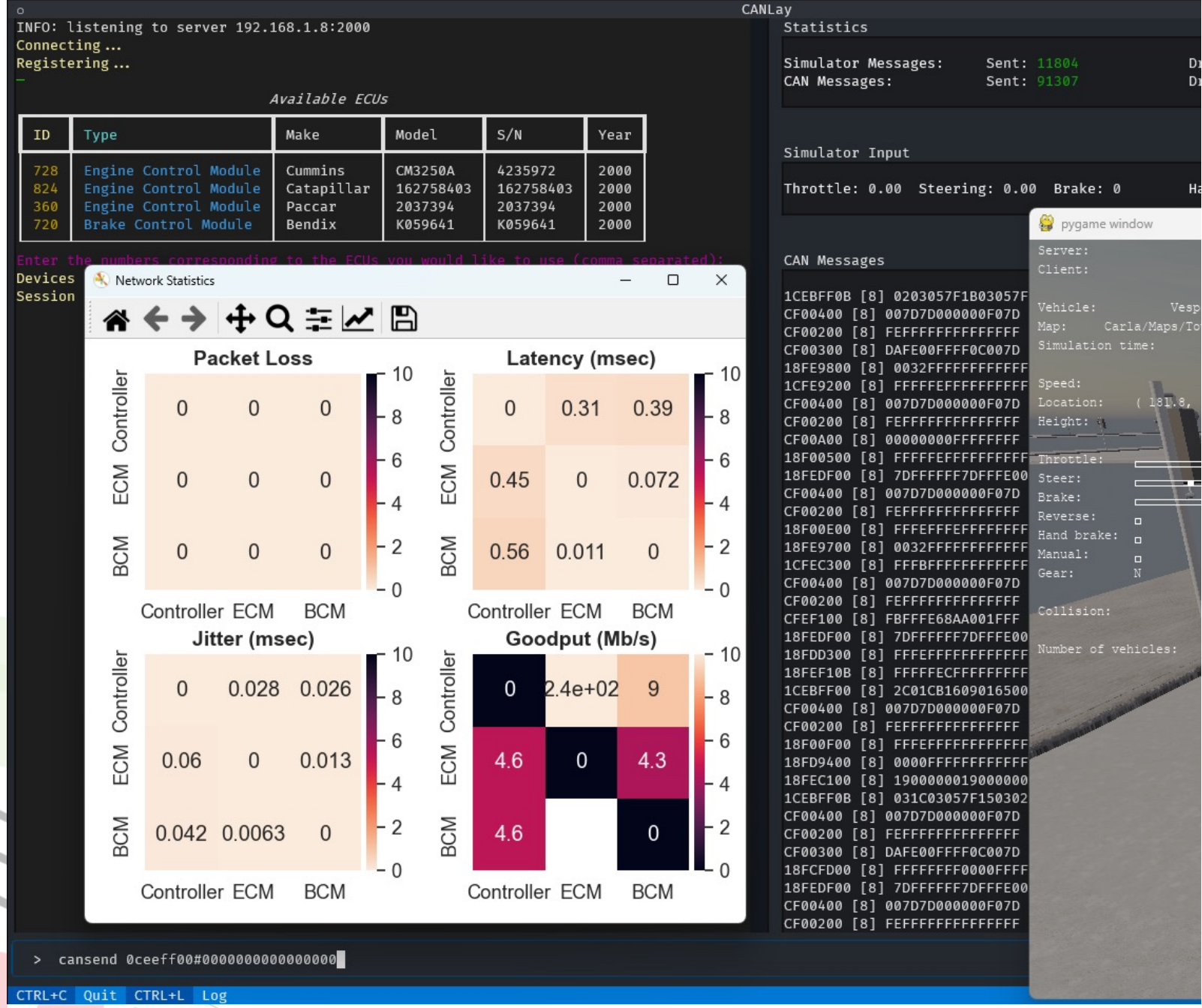
CANLay's Health Montoring

- Real-time health monitoring for the CANLay network.
  - Tracks packet loss, latency, jitter, and goodput.
  - Calculates network health metrics automatically.
  - Displays network health reports and statistics.
- Using shared networks presents issues when network conditions are poor.
- Displaying network health keeps user informed of network conditions.



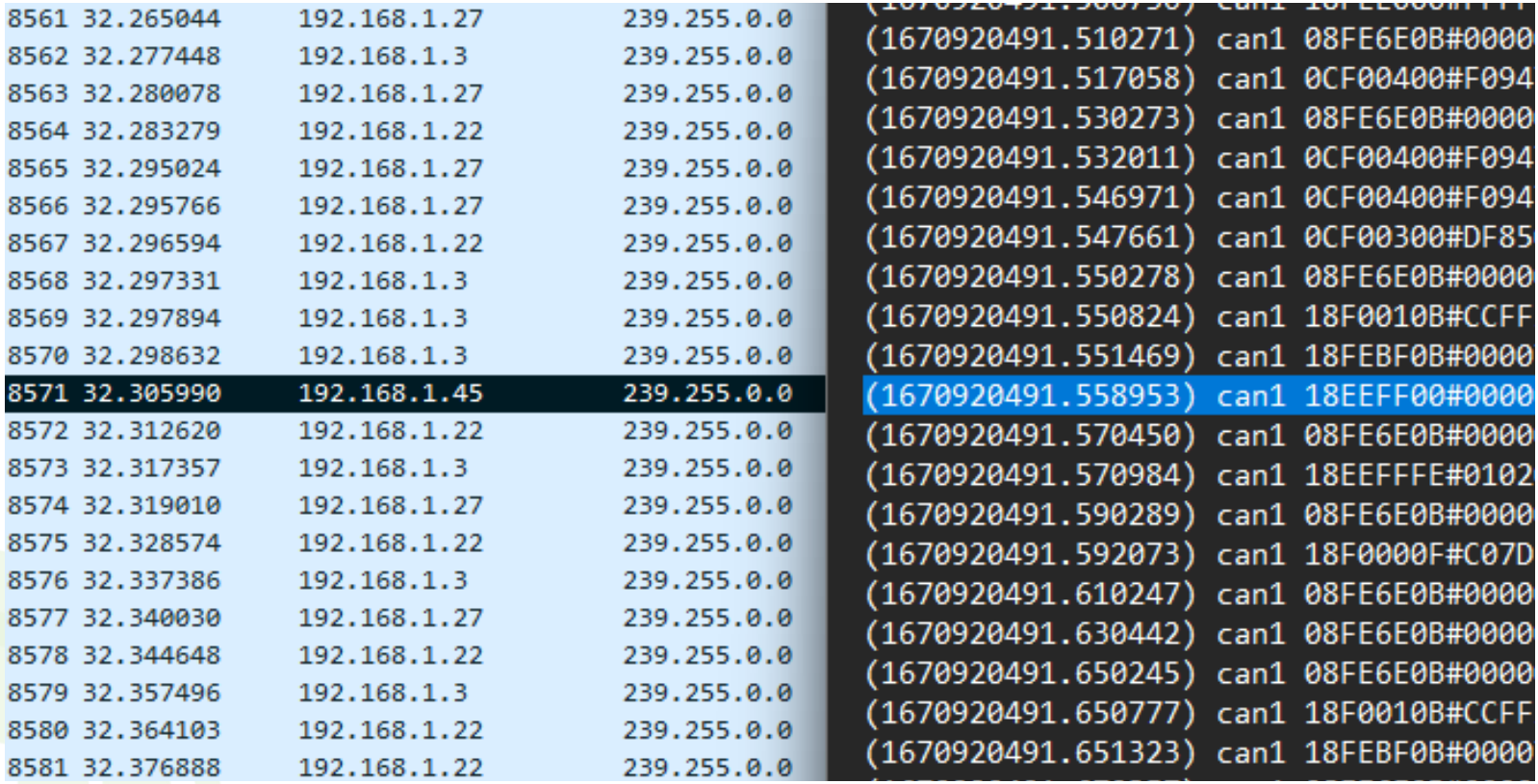
Example Usage

- Vulnerability: Address claim attack on J1939 protocol. (Murvay and Groza, 2018)
- Targets: J1939 Electronic Control Module
- Setup: Shared gigabit local area network.
- Procedure: Select devices, start session, send malicious message.
- Result: Caterpillar ECM stopped broadcasting on to the network.
- Time: Testing completed in just a **few minutes.**



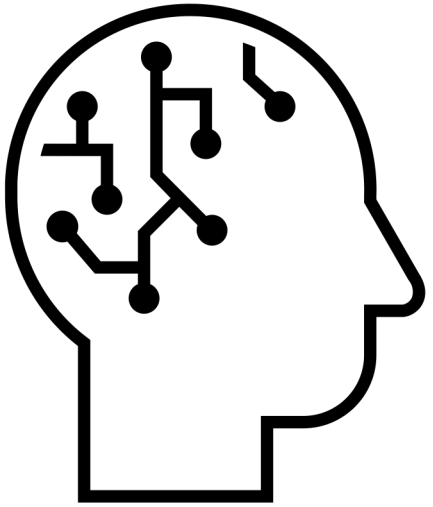
Summary and Conclusions

- Rapid Testing: CANLay significantly reduces testing time.
- Seamless Integration: CANLay integrates with CARLA and ECUs.
- Real-time Monitoring: Network health metrics enable proactive decisions.
- Vulnerability Detection: Identified vulnerable ECMs in the experiment.
- Scalability: CANLay can be used with multiple devices and networks.
- Picture shown displays logs from experiment.



Future Work

- SocketCAN compatibility. Acts as abstract network layer for existing security engineering tools such as SavvyCAN and Metasploit.
- Precision Time Protocol (PTP): Switching to PTP for sub-millisecond accurate synchronization. (Done!)
- API Integration: Enabling faster, automated testing and compatibility with vulnerability scanners. (Done!)
- Explore efficient and secure wide area networking capabilities.



33rd Annual INCOSE international symposium

hybrid event

Honolulu, HI, USA
July 15 - 20, 2023

www.incose.org/symp2023
#INCOSEIS

Jake Jepson
Colorado State University, 6029 Campus Delivery
Fort Collins, CO 80523-6029
478-335-8520
jepson2k@rams.colostate.edu