Undefined Behavior in Cyber Physical Systems

Jeremy Daily, Sergey Bratus

Trusted Computing Center of Excellence Summit

9 May 2024

SYSTEMS ENGINEERING
COLORADO STATE UNIVERSITY

Heavy Vehicles as Cyber-Physical Systems

- Networked electronic control units (ECU) communicating over an SAE J1939 network
  - Actuators
  - Sensors
  - Control
  - Communications
- SAE J1939 included a Transport Protocol to send large messages (9-1785) bytes.
- There exists some ambiguity in how to handle some communications.
- Examples give specificity to concepts.


How bad can undefined behavior really be?
Colorado State University
USDOT 0412285

Exploiting Transport Protocol Vulnerabilities in SAE J1939 Networks

Rik Chatterjee, Subhojeet Mukherjee, Jeremy Daily

Symposium on Vehicle Security and Privacy (VehicleSec) 2023
27 February 2023, San Diego, CA, USA
ISBN 1-891562-88-6
https://dx.doi.org/10.14722/vehiclesec.2023.23053
www.ndss-symposium.org

Exploiting Transport Protocol Vulnerabilities in SAE J1939 Networks

Rik Chatterjee
Colorado State University
rik.chatterjee@colostate.edu

Subhojeet Mukherjee
Colorado State University
subhojeet.mukherjee@colostate.edu

Jeremy Daily
Colorado State University
jeremy.daily@colostate.edu

***Abstract*—Modern vehicles are equipped with embedded computers that utilize standard protocols for internal communication. The SAE J1939 protocols running on top of the Controller Area Network (CAN) protocol is the primary choice of internal communication for embedded computers in medium and heavy-duty vehicles. This paper presents five different cases in which potential shortcomings of the SAE J1939 standards are exploited to launch attacks on in-vehicle computers that constitute SAE J1939 networks.**

In the first two of these scenarios, we validate the previously proposed attack hypothesis on more comprehensive testing setups. In the later three of these scenarios, we present newer attack vectors that can be executed on bench test setups and deployed SAE J1939 networks.

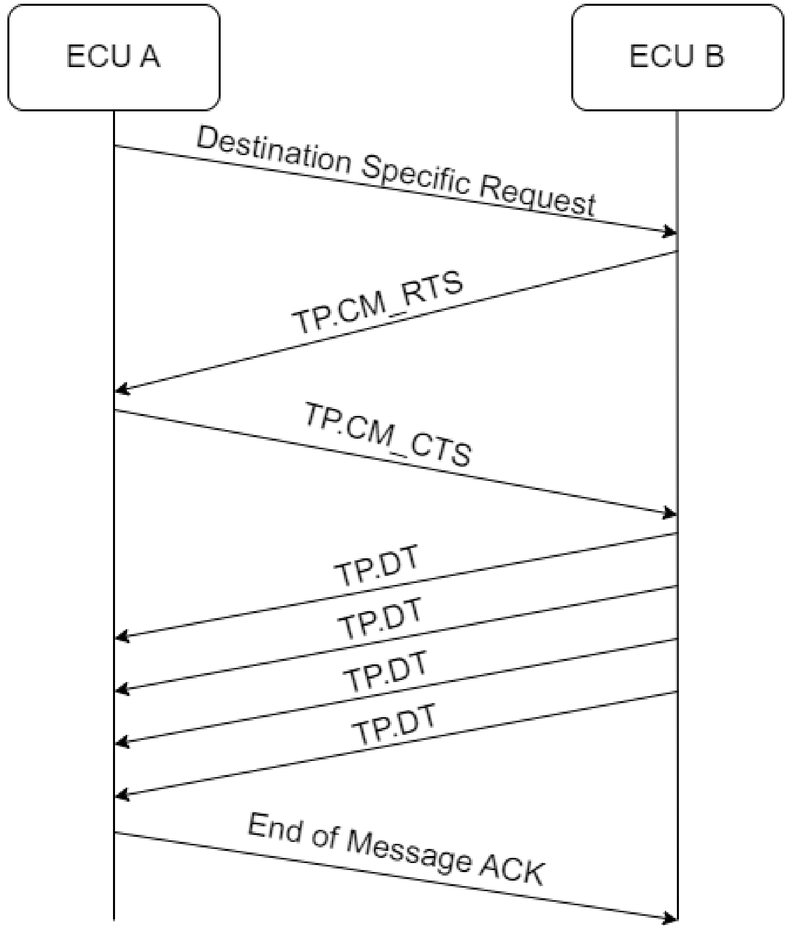
For the purpose of demonstration, we use bench-level test systems with real electronic control units connected to a CAN bus. Additional testing was conducted on a 2014 Kenworth T270 Class 6 truck under both stationary and driving conditions. Test results show how protocol attacks can target specific ECUs. These attacks should be considered by engineers and programmers implementing the J1939 protocol stack in their communications subsystem.

points (vulnerable ECUs) to the CAN network, one can launch attacks on the vehicle to control or disrupt its operations. MHD vehicles also expose similar entry points [4] and, aside from CAN specific attacks, it has been shown that attacks can also be launched on the SAE J1939 protocols. Even so, the number of demonstrated attacks is still limited: Burakova et al. [5] have demonstrated a couple of attacks on the application layer specification of the SAE J1939 standards, Murvay et al. [6] have focused on weaknesses at the network management layer, and Mukherjee et al. [7] have targeted specific protocols at the data-link layer of the specifications.

While the application and network management layers are critical to the cyber-physical operations of the vehicle, important message transportation specifications are made in the data-link layer standards. As such, in this work we demonstrate newer attacks at the data-link layer of the SAE J1939 specifications that broaden the horizon of cyber threats already created by Mukherjee et al. [7]. Moreover, we validate two attacks that Mukherjee et al. demonstrated to work on laboratory

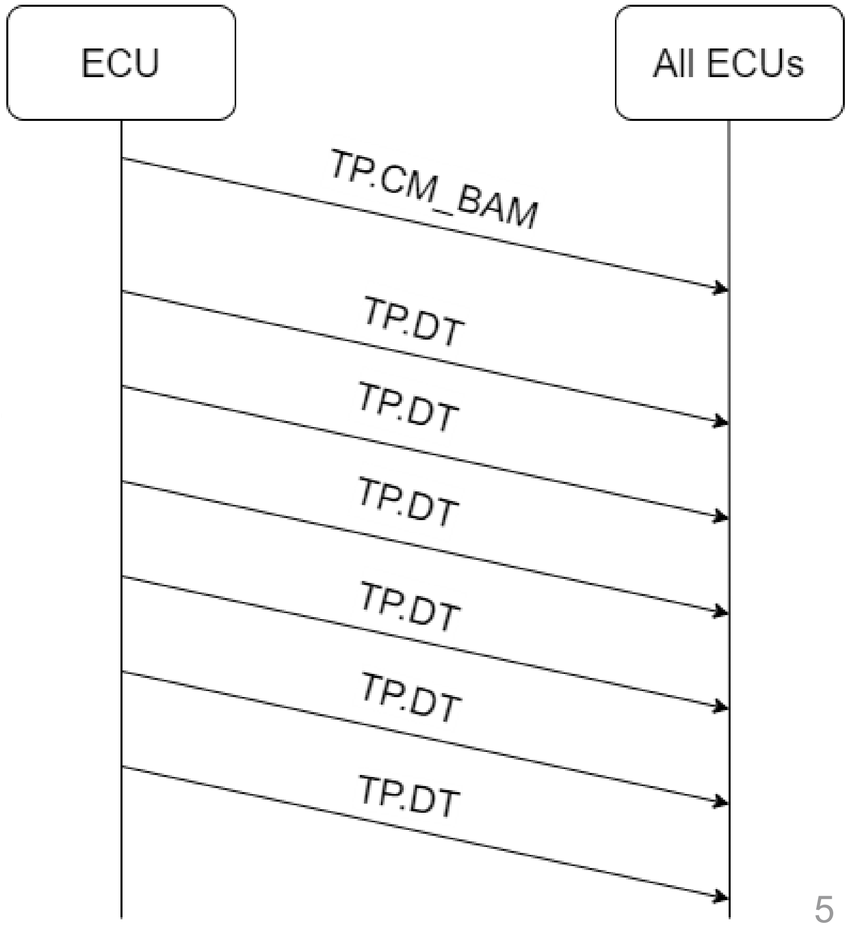
Two Types of J1939 Transport Protocol Messages

Point-to-Point



- TP.CM_RTS: Connection Management Message: Request-to-Send
- TP.CM_CTS: Connection Management Message: Clear-to-send
- TP.CM_BAM: Broadcast Announcement Message
- TP.DT: Data Packets

Broadcast



Request Overload

Electronic Control Unit (ECU)

Transport Layer Networking Specifications SAE J1939/21

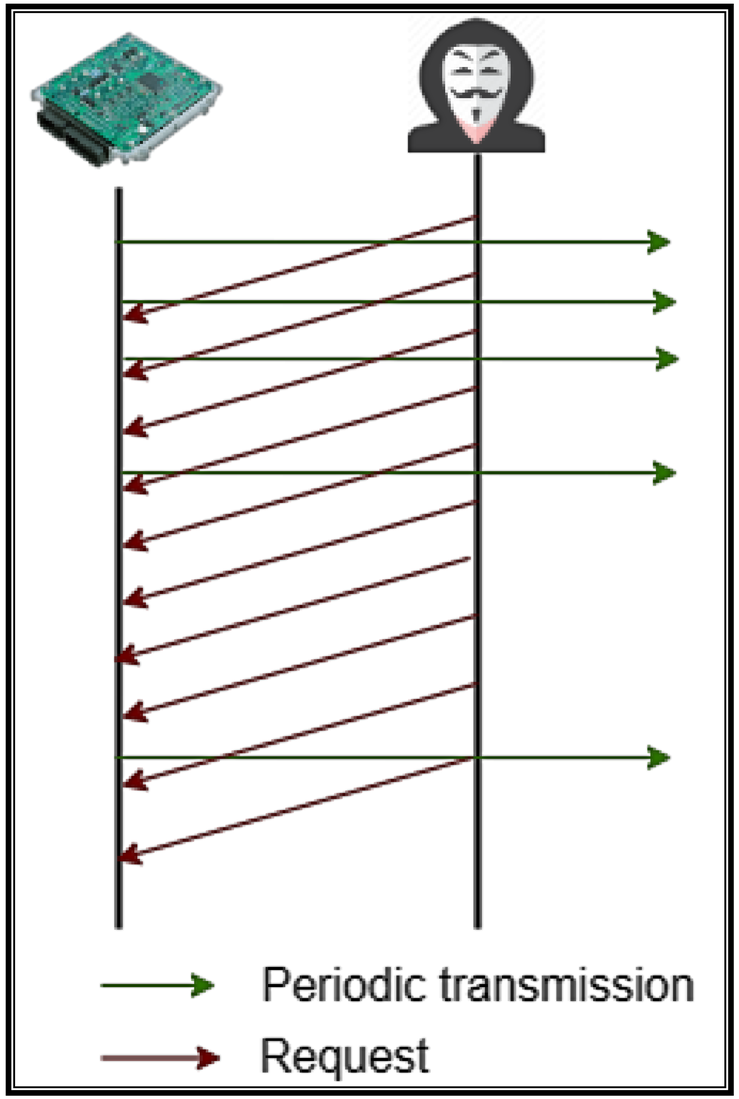
Controller Area Network (CAN)

- **Request Overload** → Depletion of traffic from target ECU
- **Connection Exhaustion** → Denial of connections to target ECU
- **BAM Block** → Blocking Multi-packet Broadcast Messages
- **Malicious CTS** → Stopping all Multi-packet communication
- **Memory Leak** → Reading inaccessible memory on target ECU

Colorado State University

Hypothesis

- **Specification**
  - All directed requests to an ECU must be processed.
- **Attack**
  - Send a high volume of SAE J1939 requests to the target ECU
- **Expected result**
  - In an attempt to serve the sent requests, the ECU fails to perform regular, more critical tasks like transmission of periodic messages



Model Based Systems Engineering (MBSE)

- Language – System Modeling Language (SysML)
- Tool – CATIA Magic Systems of Systems Architect
- Method – Magic Grid v2
- Pillars of MBSE
  - Structure
  - Behavior
  - Requirements
  - Parametrics
- SysML (v1) is an extension of UML

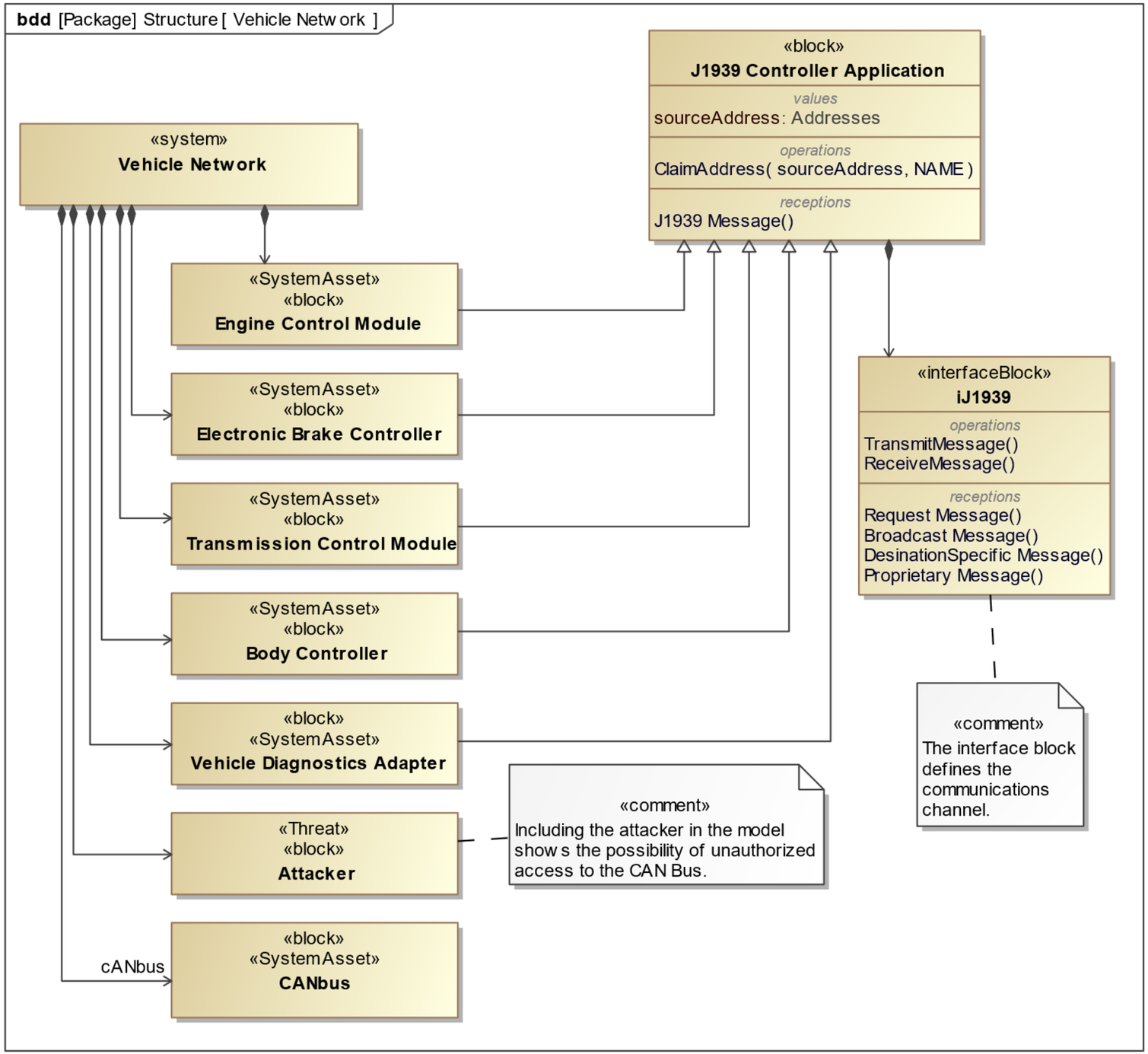
System Composition

- Block Definition Diagrams (bdd) show structure
- SysML closed diamonds show directed composition

"The Vehicle Network is composed of an Engine Control Module."

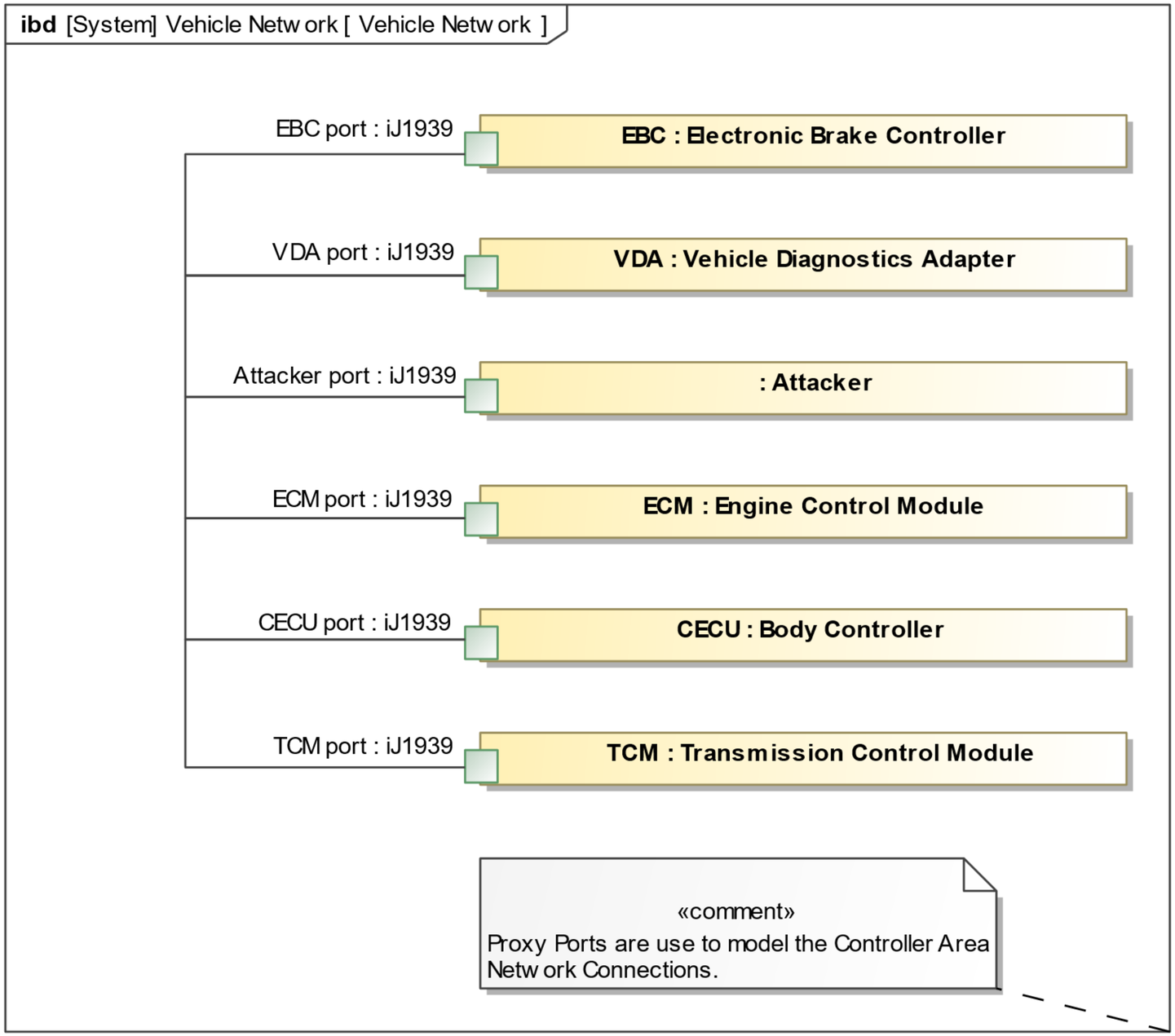
- SysML Open Triangles show generalization

"The Body Controller is a type of J1939 Controller Application."



System Connectivity

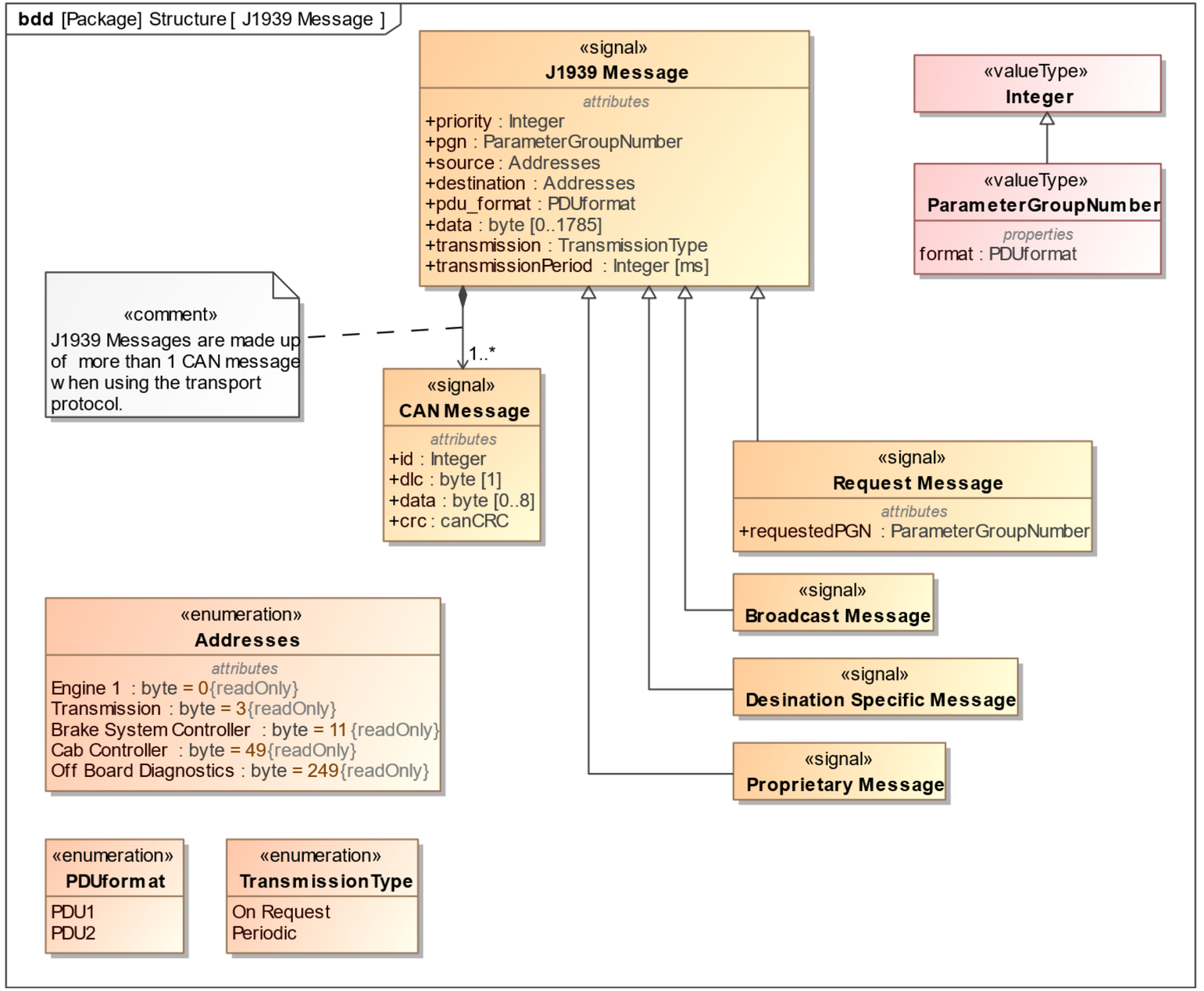
- SysML Internal Block Diagrams (ibd) show system connectivity through ports.
- The iJ1939 interface block is used to declare the type of the port.



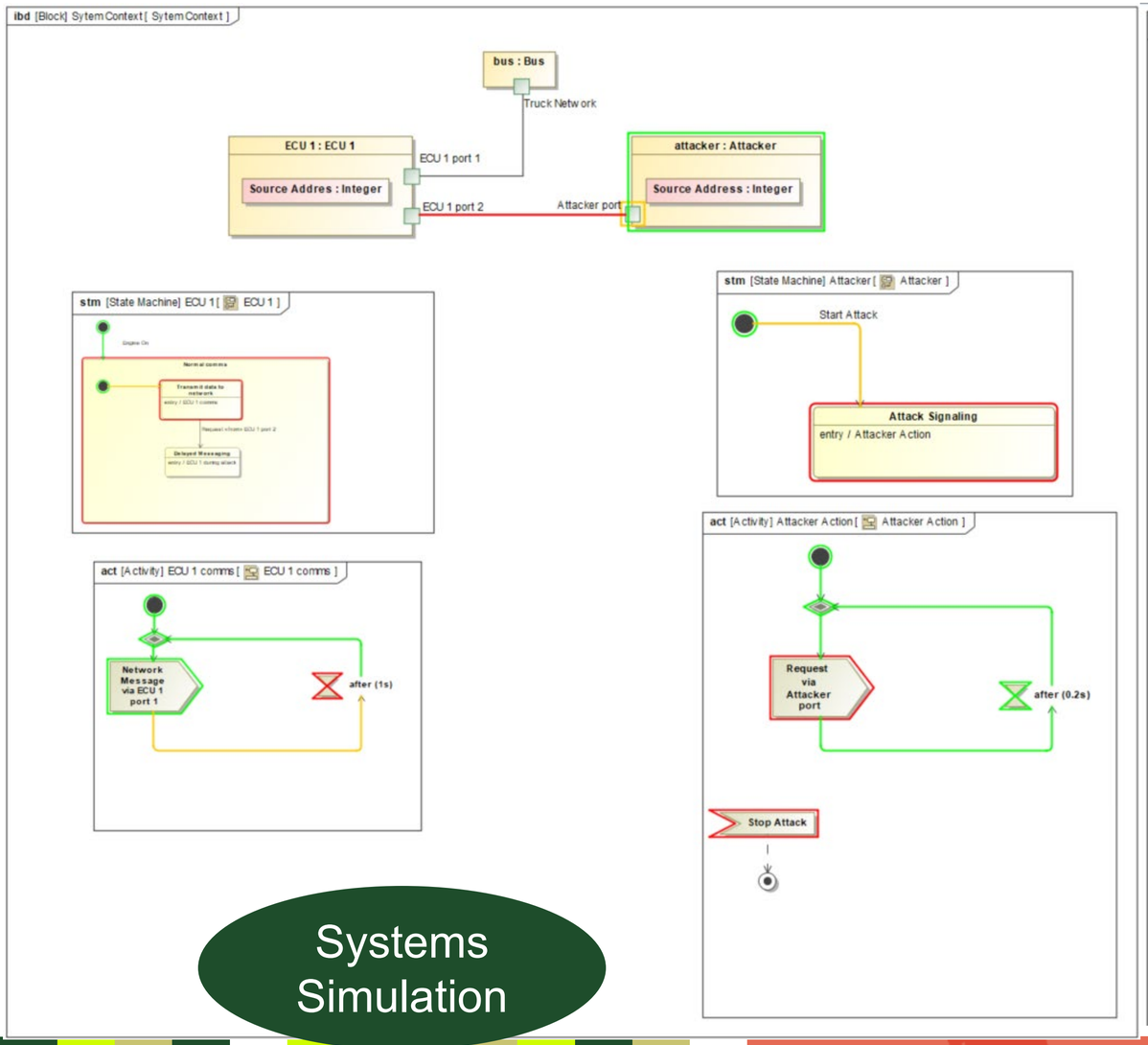
J1939 Message Definition

Based on the SAE Standard

J1939 messages can use the Transport Protocol for sending large messages.

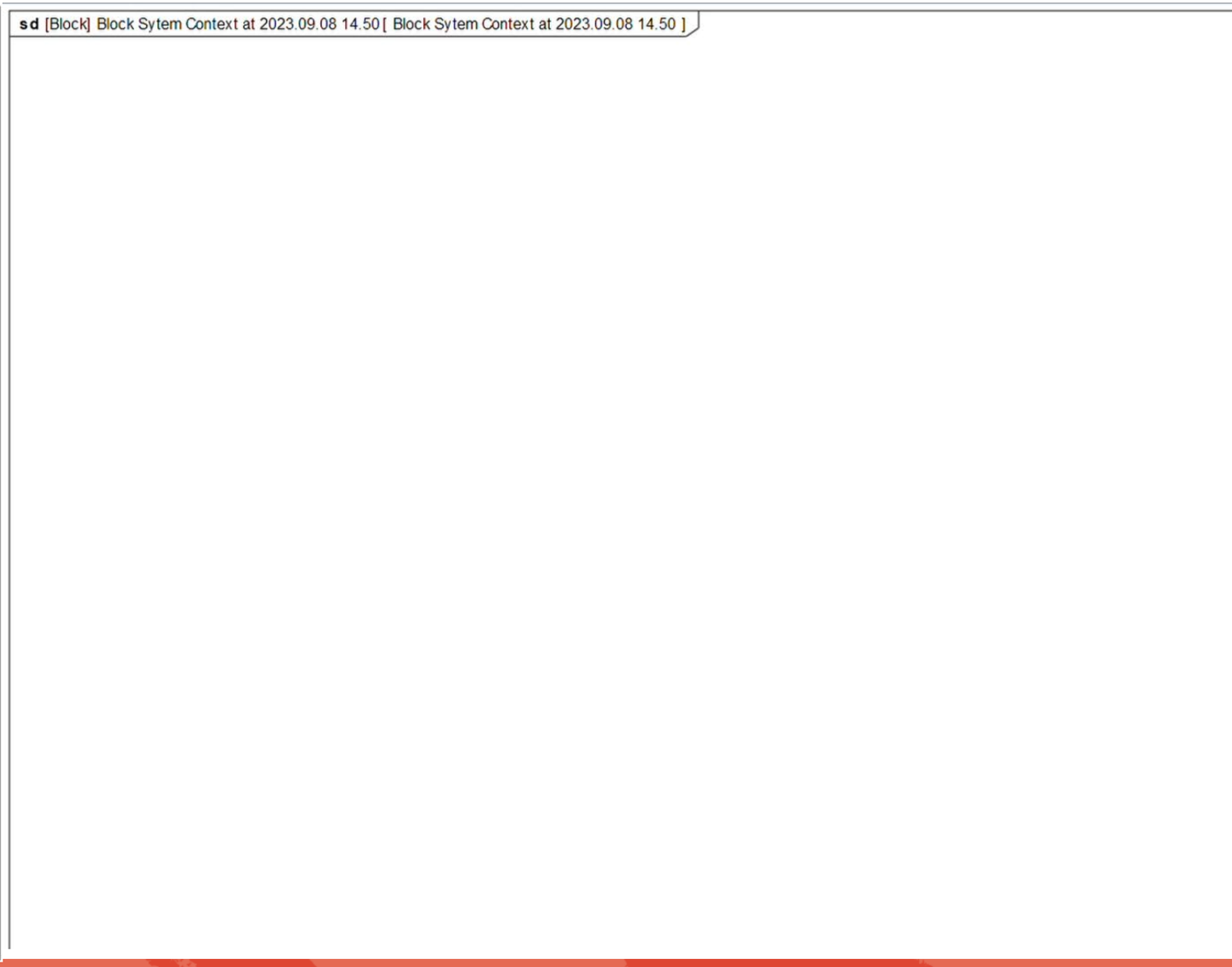


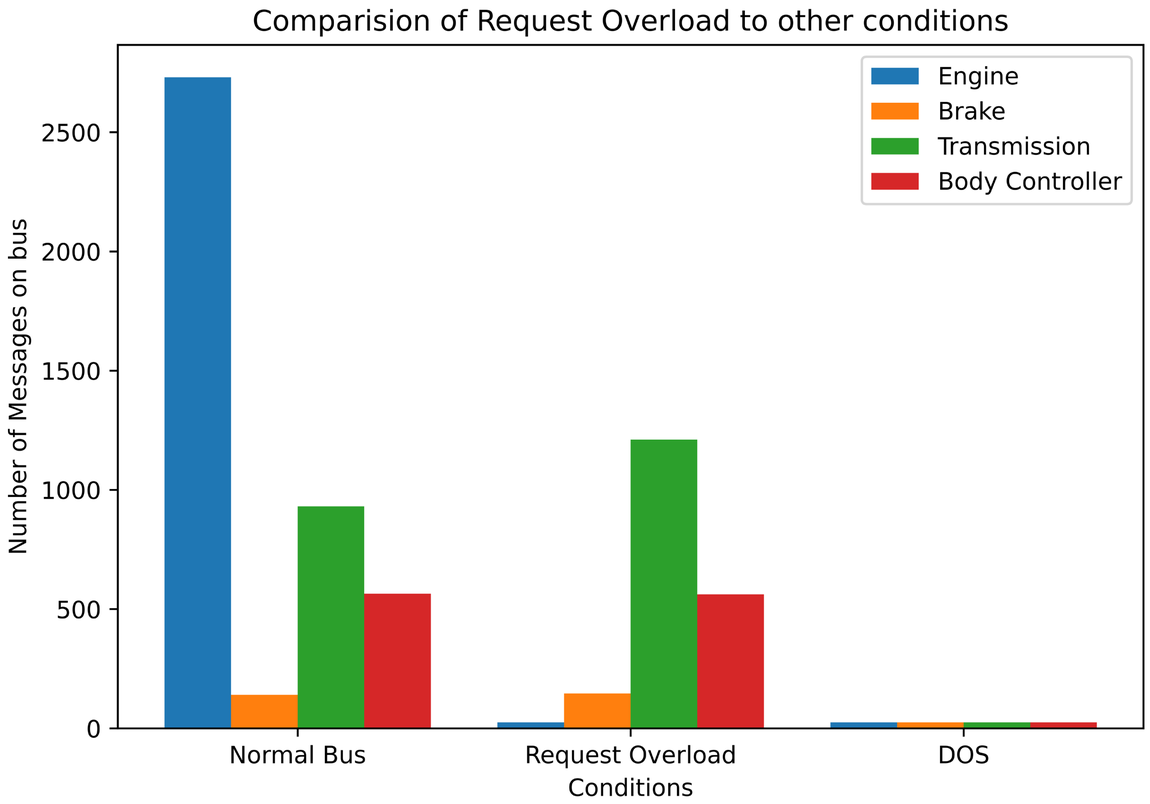
Internal Block Diagram – Network component information flow/behavior



Systems Simulation

Simulated Sequence Diagram Network Messaging





Observation on the Kenworth T270 Truck

Request overloads represent a targeted Denial of Service (DOS) attack

Colorado State University

Live Demonstration on Kenworth T270 Truck

The need for Data Definition Languages

- SysML v1 is based on UML
- SysML v2 is new (KernelML)
- Systems engineers are responsible for testable consistency across subsystems
- SEs must understand and design for emergent behaviors
- Clarity on the design space and its complement