OCTANE

(Open Car Testbed and Network Experiments): Bringing Cyber-Physical Security Research to Researchers and Students

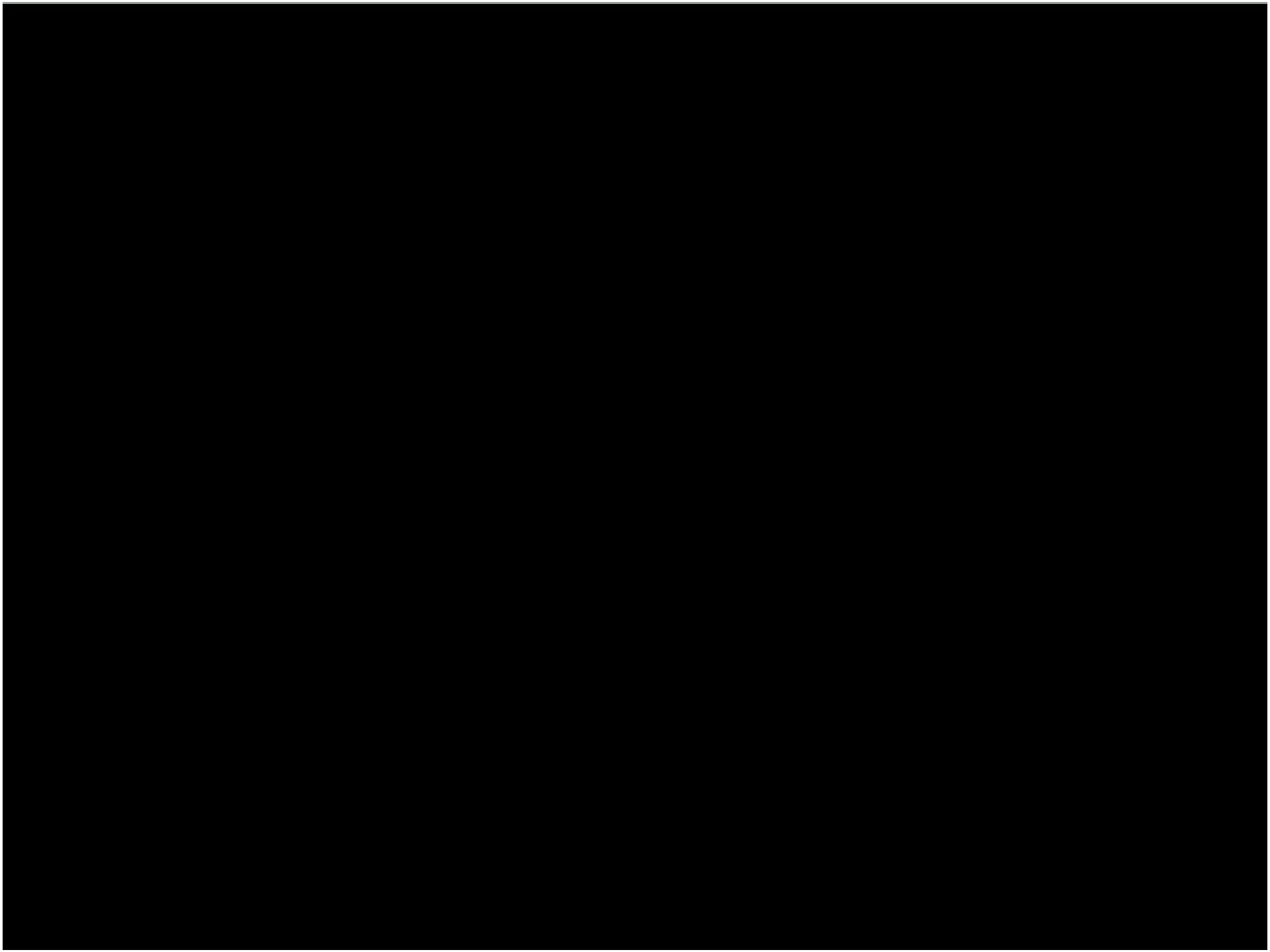
6th Workshop on Cyber Security Experimentation and Test (CSET `13)
August 12, 2013
Washington, D.C.

Christopher E. Everett Damon McCoy
George Mason University

How OCTANE can help with security research!

- Advantages:
  - Sharing of portable XML files
  - Easy to use GUI for software package
  - Quick addition of network hardware
  - Straight-forward guidelines to setup/select hardware framework for testing
  - Software package to be released open source

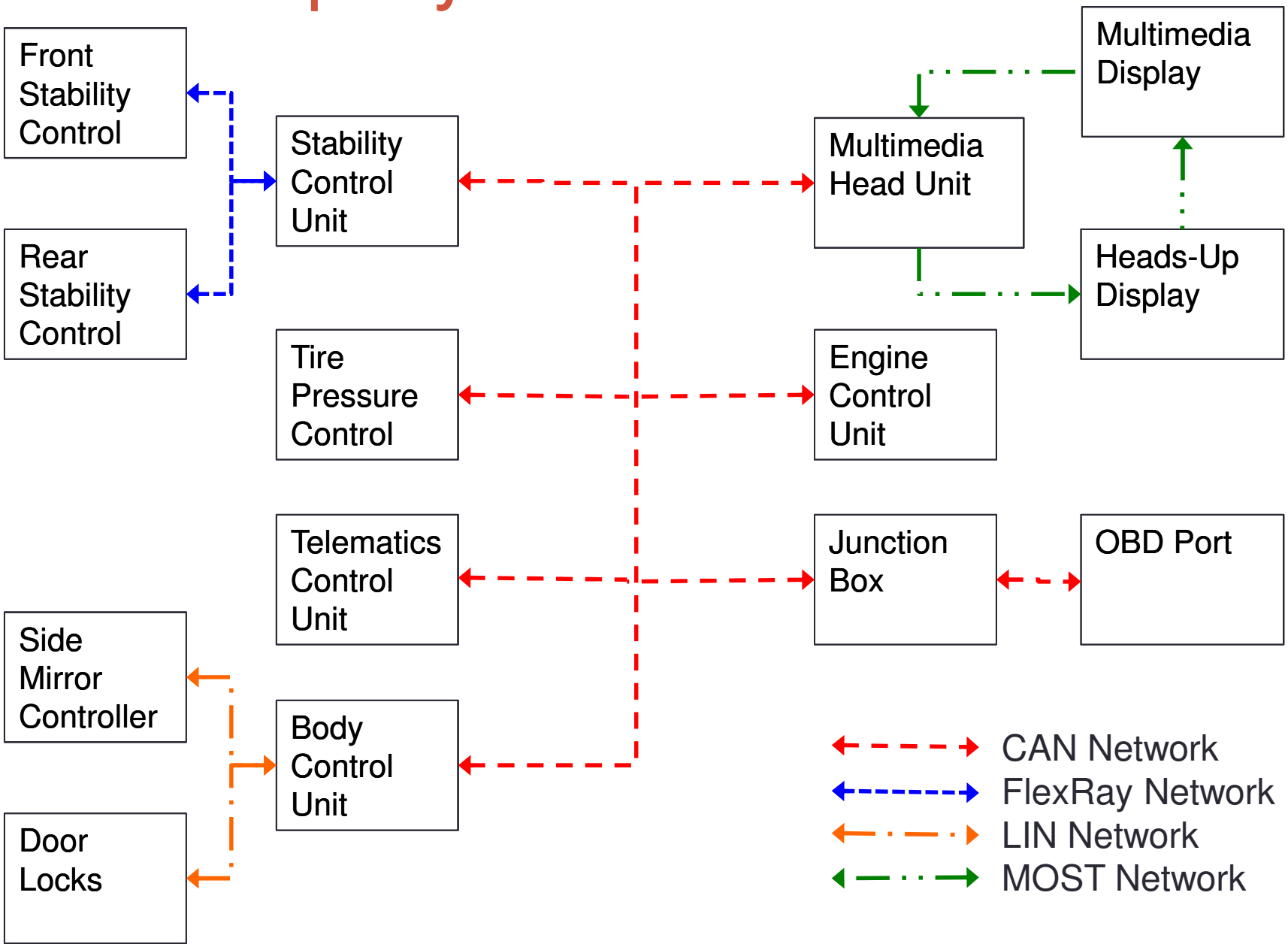
- These advantages mean:
  - Your lab can be up and running faster and at a lower cost!
  - Your team does not have to worry about the network setup and configuration but can focus on your expertise – Security!
  - Your team can extend the software package to fit your needs instead of being limited by a commercial software package designed for network development.



Why is Automotive Security Testing Challenging?

Positives	Issues
Automotive networks (e.g., CAN) are standardized	Limited documentation about propriety automotive network implementations of networks
Automotive network hardware is readily available off the shelf	Hardware is designed for testing and building the systems
Automotive network software is readily available off the shelf	Software is designed for testing and building the systems & is expensive
Automotive networks are readily available (most folks have a car)	Researchers do not want to use their own vehicles for invasive testing & purchasing new cars is expensive
Automotive parts are readily available (numerous stores selling parts)	Automotive parts infrastructure designed for replacement/repair

Exemplary Automobile Network



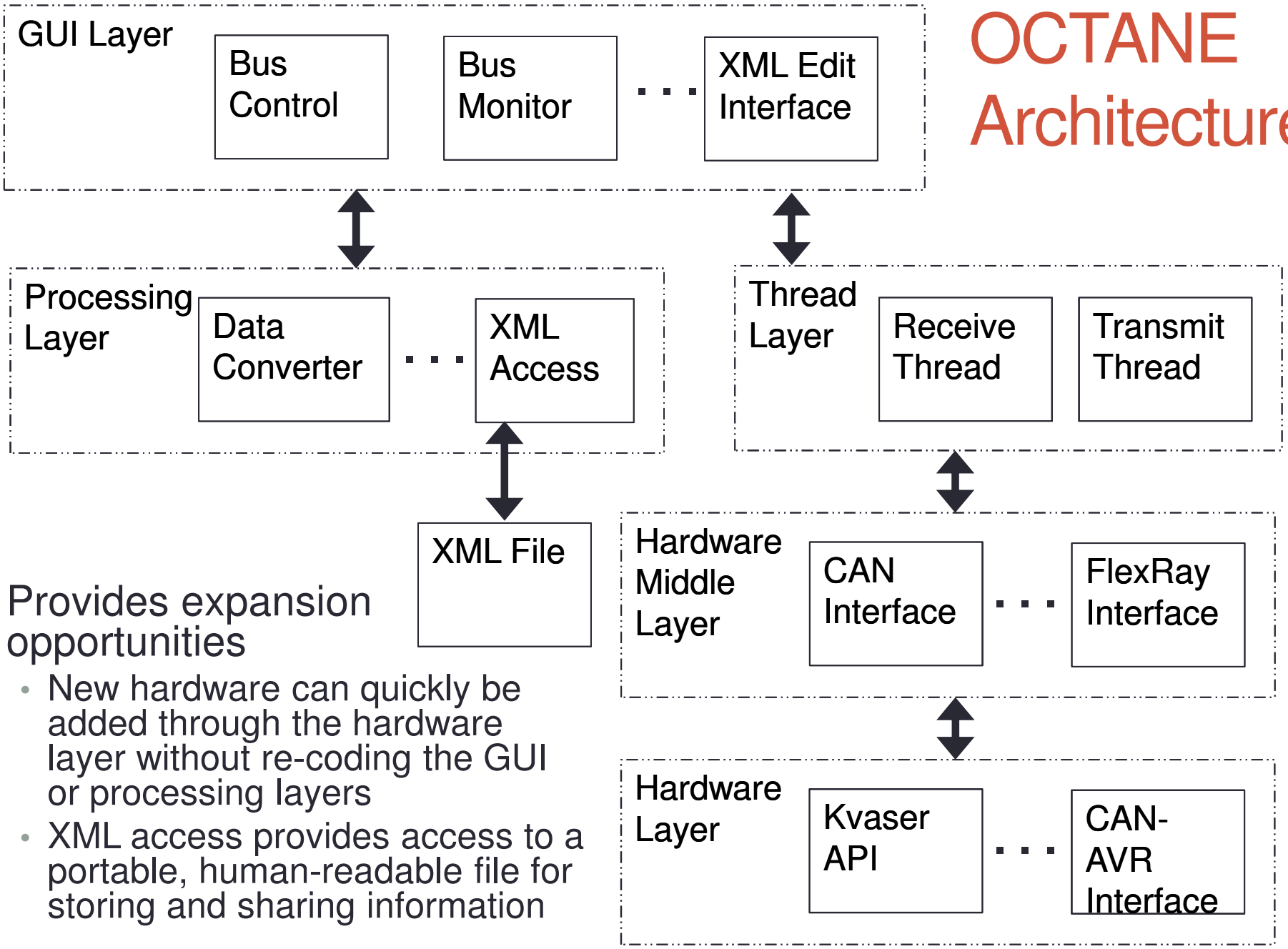
Solution: OCTANE

Issues	Solution
Limited documentation about propriety automotive network implementations of networks	Enables reverse engineering & storing of the discovered information in XML files
Hardware is designed for testing and building the systems	Hardware framework is selected based on research/teaching needs
Software is designed for testing and building the systems & is expensive	Software package is specifically designed for security testing & will be released open source
Researchers do not want to use their own vehicles for invasive testing & purchasing new cars is expensive	Hardware framework enables selection of low cost network setup
Automotive parts infrastructure designed for replacement/repair	Hardware framework provides a guide to selection of parts

OCTANE

- Software package and hardware framework for reverse engineering and testing of automotive networks
- Software Package
  - Goal: Facilitate reverse engineering and security testing
  - Architecture
  - XML automation
  - Packet monitor
  - Custom transmit
- Hardware Framework
  - Goal: Enable researchers/students to quickly setup an automobile network
  - Lab network setup
  - Real-world test setup

OCTANE Architecture



- Provides expansion opportunities
  - New hardware can quickly be added through the hardware layer without re-coding the GUI or processing layers
  - XML access provides access to a portable, human-readable file for storing and sharing information

XML Automation

- Enables storage and sharing of packets, messages, and ECU IDs for future use
- Provides a user the ability to quickly and accurately reproduce and identify network traffic

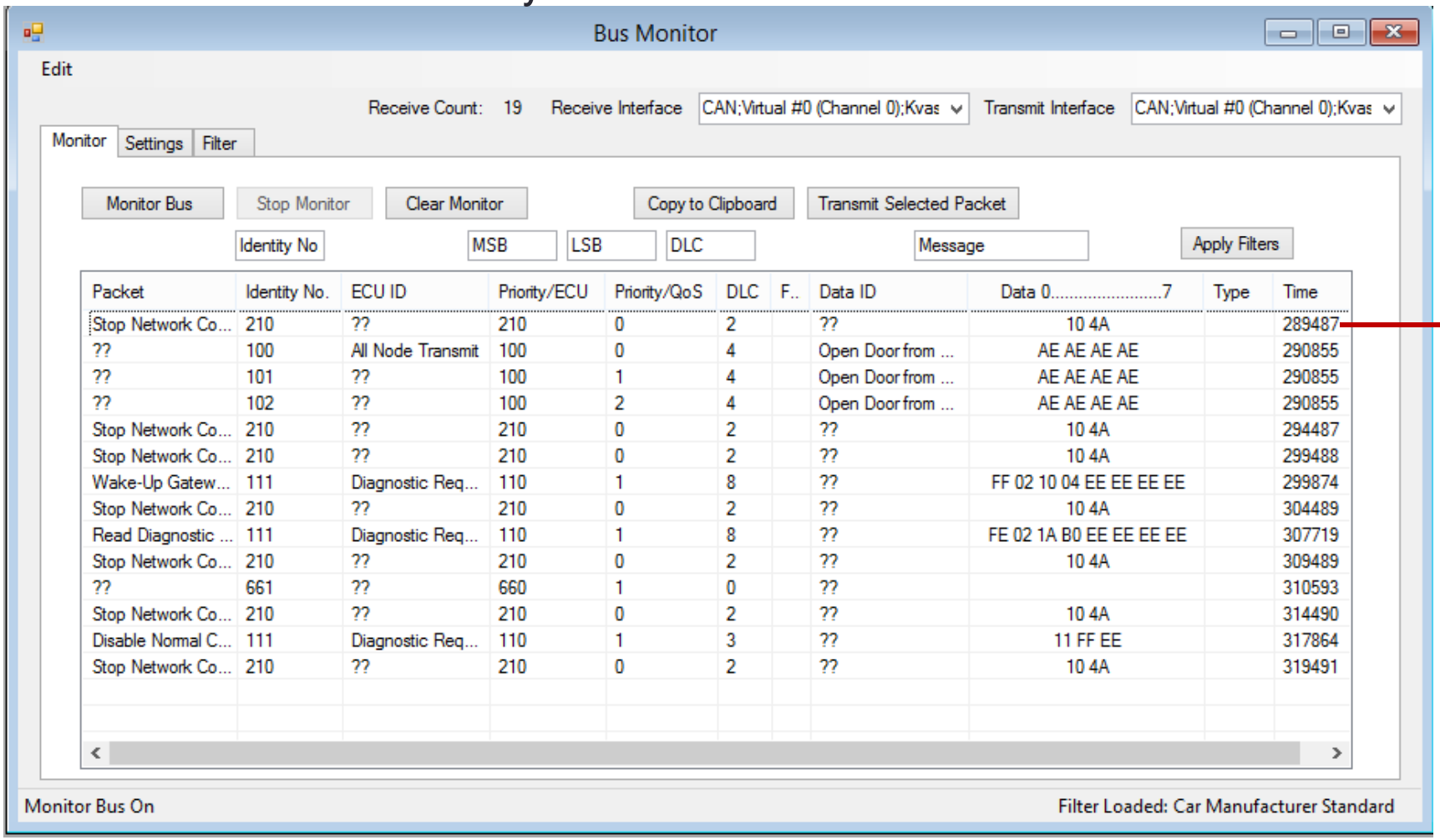
<Packet>		
<Name>	Stop Network Communications	<\Name>
<ID>	210	<\ID>
<DLC>	2	<\DLC>
<Message>	104A	<\Message>
<\Packet>		

- Future Improvements
  - Wildcards
  - Packet Sequences
  - Packet Responses
  - Packet Subroutines
  - Calculated Packet Responses

Bus Monitor

- Enables viewing of received network packets and transmission of selected packets back to the network
- Provides a user the ability to test interactions with the network and test security features of the network

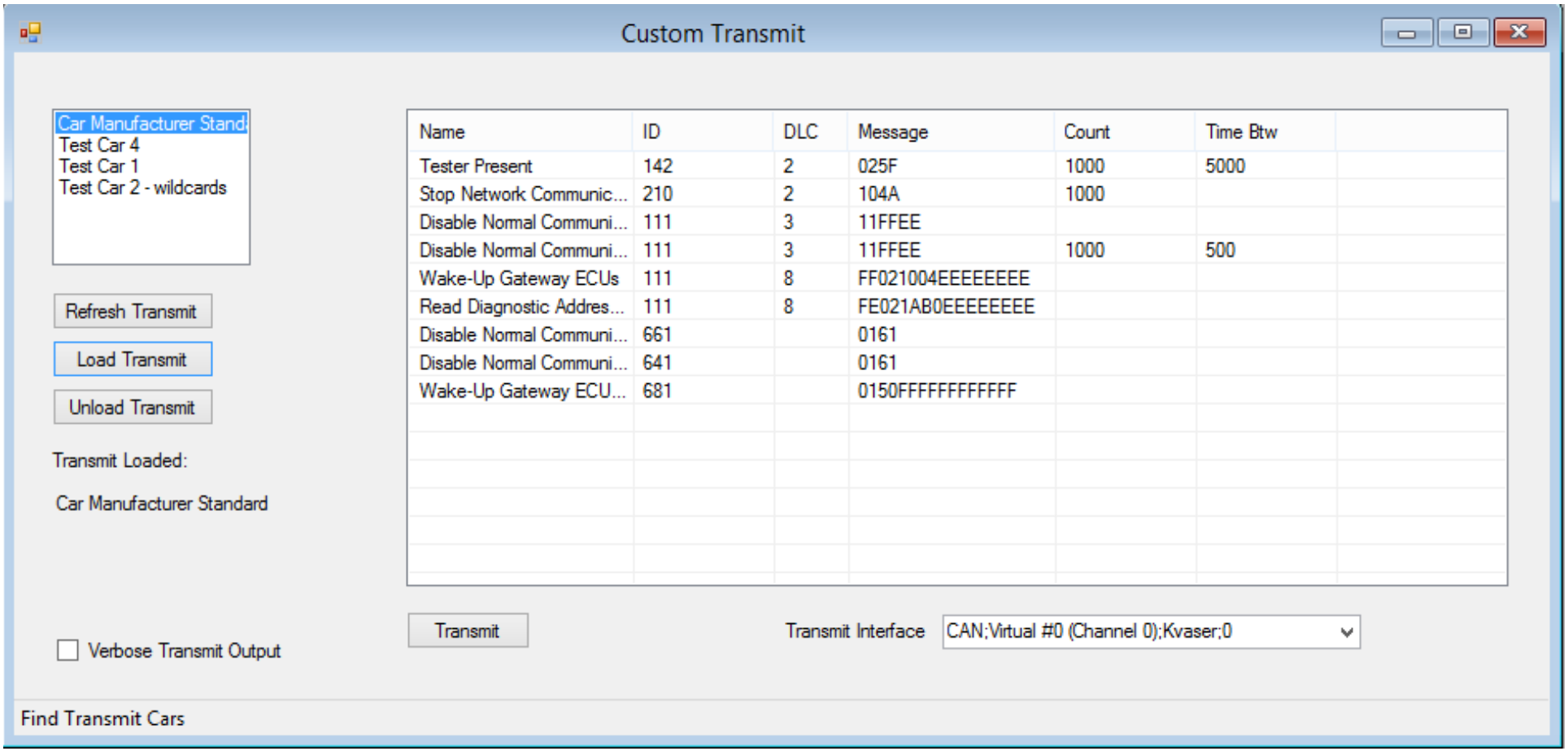
CAN Packet
Identity No.: 210
DLC: 2
Data: 10 4A



Packet	Identity No.	ECU ID	Priority/ECU	Priority/QoS	DLC	F..	Data ID	Data 0.....7	Type	Time
Stop Network Co...	210	??	210	0	2		??	10 4A		289487
??	100	All Node Transmit	100	0	4		Open Door from ...	AE AE AE AE		290855
??	101	??	100	1	4		Open Door from ...	AE AE AE AE		290855
??	102	??	100	2	4		Open Door from ...	AE AE AE AE		290855
Stop Network Co...	210	??	210	0	2		??	10 4A		294487
Stop Network Co...	210	??	210	0	2		??	10 4A		299488
Wake-Up Gatew...	111	Diagnostic Req...	110	1	8		??	FF 02 10 04 EE EE EE EE		299874
Stop Network Co...	210	??	210	0	2		??	10 4A		304489
Read Diagnostic ...	111	Diagnostic Req...	110	1	8		??	FE 02 1A B0 EE EE EE EE		307719
Stop Network Co...	210	??	210	0	2		??	10 4A		309489
??	661	??	660	1	0		??			310593
Stop Network Co...	210	??	210	0	2		??	10 4A		314490
Disable Normal C...	111	Diagnostic Req...	110	1	3		??	11 FF EE		317864
Stop Network Co...	210	??	210	0	2		??	10 4A		319491

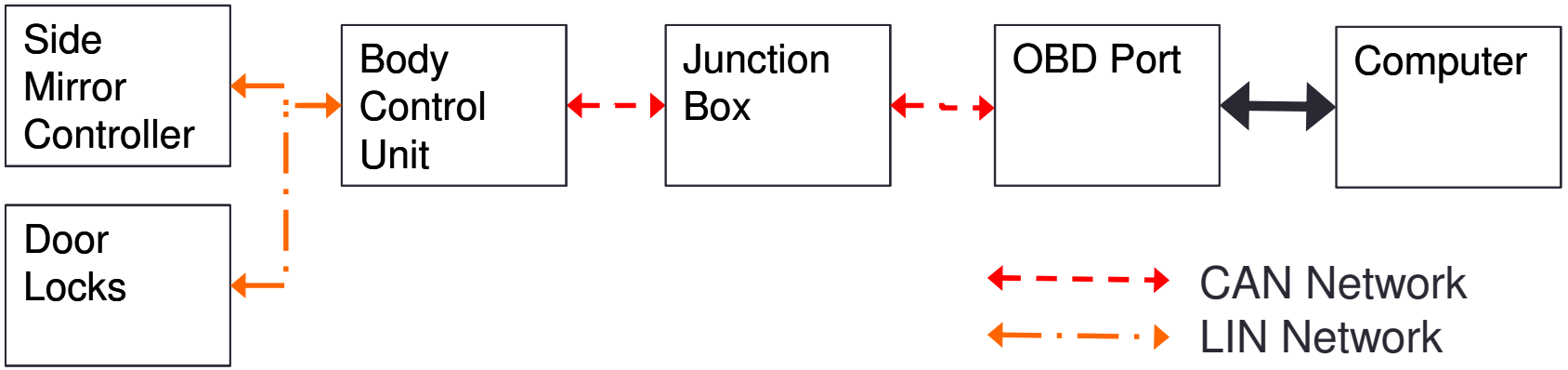
Custom Transmit

- Enables transmission of pre-configured packets to the network
- Provides a user the ability to test interactions with the network and test security features of the network



Hardware

- Lab Network Setup
  - Process to select parts to meet research types, automotive network types, automobile types, adapters, and budget



- Real-World Test Setup
  - Process to select automobiles that meet automotive network types, automobile types, adapters, and access

2013 Chevrolet Cruze

From: Wikimedia Commons

2011 Chevrolet HHR

From: Wikimedia Commons

2010 Toyota Matrix

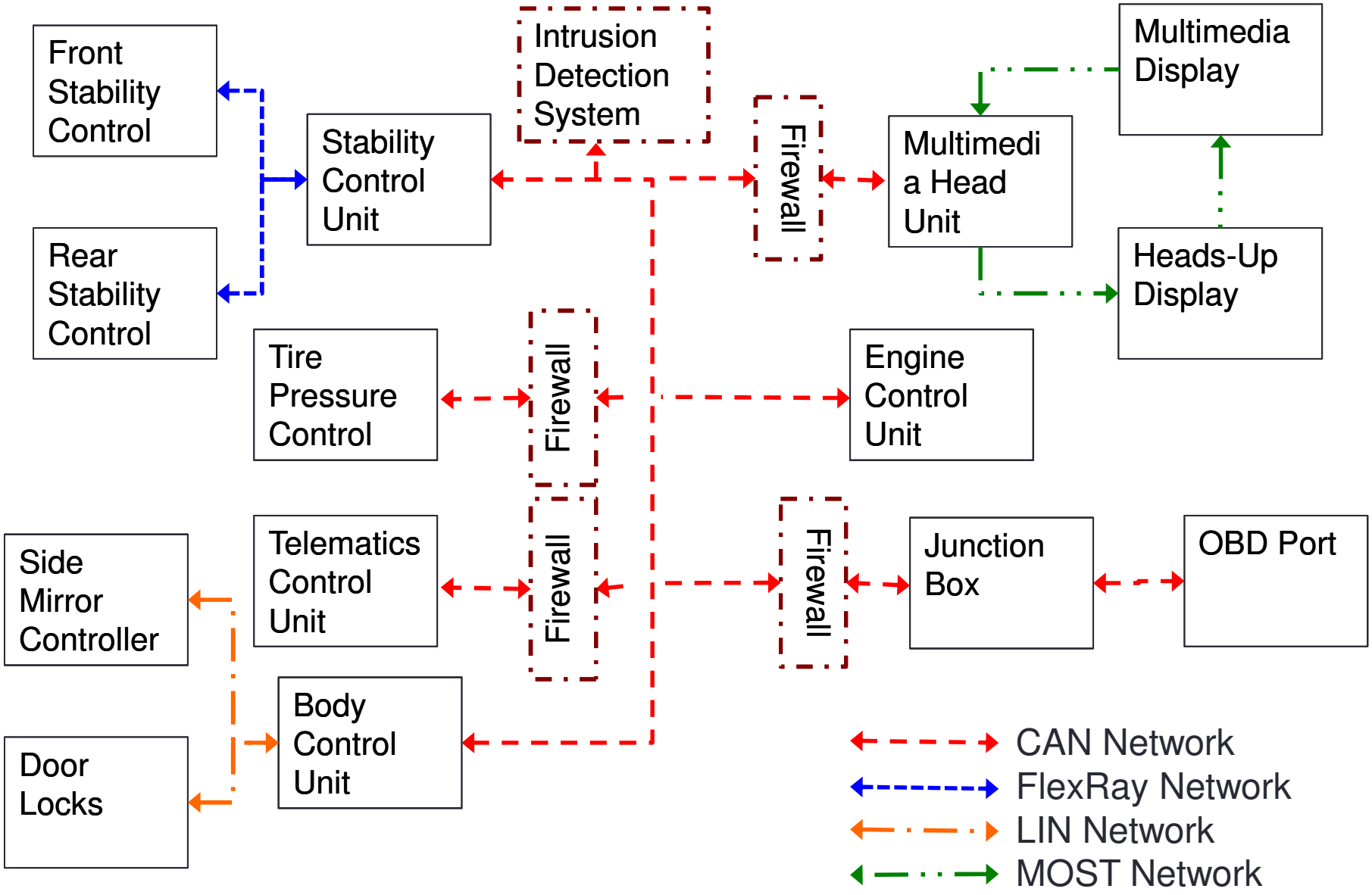
From: Wikimedia Commons

Research and Teaching Opportunities

- Research Opportunities
  - Firewall
  - Intrusion Detection System
  - Packet Encryption
  - ECU Authentication
  - ECU Security

- Teaching Opportunities
  - Undergraduate Lab Security Exercise
  - Undergraduate Lab Embedded Programming Exercise
  - Graduate Security Testing Exercise

Security Devices in Network



OCTANE Advantages

- Portable XML files
- GUI for fast and accurate packet receipt and transmission
- GUI for creation of XML files
- Wide variety of network hardware
- Hardware framework provides many options for researchers
- Open source software package enables sharing and extensions

- Results in:
  - Faster setup and configuration!
  - Cheaper setup and configuration!
  - More time spent on security setup and testing!

Wrap-Up & Discussion

- Future Work / Thoughts
  - XML Automation Extensions
    - Sharing of XML files useful?
    - How would security testing be changed?
  - Remote Access
    - Open the door for researchers to test solutions on other automotive networks?
    - Would researchers/students use remote access?
  - Firewalls
    - Too complicated for CAN networks?
    - Who would manage rules?
  - ECU Security
    - Is ECU built-in security too complicated for automotive manufacturing environment?
    - Who would manage keys/security authorization?