34th Annual INCOSE international symposium

hybrid event

Dublin, Ireland
July 2 - 6, 2024

Jeremy Daily, Associate Professor of Systems Engineering
Maj. Martin “Trae” Span, USAF, Ph.D. Candidate in Systems Engineering
Colorado State University

CyberX Challenge Events

A practical demonstration of

Understanding the Problem


We attempted and succeeded.

Commercial Vehicle Electronic Logging Device Security: Unmasking the Risk of Truck-to-Truck Cyber Worms

Jake Jepson
Colorado State University
jepson2k@rams.colostate.edu

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

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

***Abstract*—In compliance with U.S. regulations, modern commercial trucks are required by law to be equipped with Electronic Logging Devices (ELDs), which have become potential cybersecurity threat vectors. Our research uncovers three critical vulnerabilities in commonly used ELDs.**

First, we demonstrate that these devices can be wirelessly controlled to send arbitrary Controller Area Network (CAN) messages, enabling unauthorized control over vehicle systems. The second vulnerability demonstrates malicious firmware can be uploaded to these ELDs, allowing attackers to manipulate data and vehicle operations arbitrarily. The final vulnerability, and perhaps the most concerning, is the potential for a self-propagating truck-to-truck worm, which takes advantage of the inherent networked nature of these devices. Such an attack could lead to widespread disruptions in commercial fleets, with severe safety and operational implications. For the purpose of demonstration, bench level testing systems were utilized. Additional testing was conducted on a 2014 Kenworth T270 Class 6 research truck with a connected vulnerable ELD.

These findings highlight an urgent need to improve the security posture in ELD systems. Following some existing best practices and adhering to known requirements can greatly improve the security of these systems. The process of discovering the vulnerabilities and exploiting them is explained in detail. Product designers, programmers, engineers, and consumers should use this information to raise awareness of these vulnerabilities and encourage the development of safer devices that connect to vehicular networks.

I. Introduction

According to the US Bureau of Transportation Statistics, the United States alone has over 14 million medium and heavy-duty trucks registered, underscoring their prevalence and importance in national infrastructure [1]. Moreover, the American Trucking Association's report highlighted these trucks moved approximately 72.6% of the nation's freight by weight in recent years, showcasing their critical role in the country's freight transportation system [2]. This statistic further emphasizes the reliance of economies on these vehicles, not only for domestic transport but also for international trade and commerce. The seamless operation of these commercial vehicles is vital for the smooth functioning of supply chains, directly impacting everything from local businesses to international markets.

A. Background on Electronic Logging Devices (ELDs)

Many heavy vehicles are required to be equipped with Electronic Logging Devices (ELDs), since they are mandated by the Federal Motor Carrier Safety Administration (FMCSA) under the ELD Final Rule [3]. This so-called ELD Mandate is a component of the Moving Ahead for Progress in the 21st Century Act (MAP-21) and it went into effect December 18, 2017. These devices are essential for recording driving hours and ensuring compliance with Hours of Service (HOS) regulations, which are designed to prevent accidents due to

Results

- Coordinated Disclosure with Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security
- Vendor has developed a patch to address the security issues
- Best Paper Runner-Up at the VehicleSec ’24 Symposium
- Best Demo at the VehicleSec ’24 Symposium, Feb 26, 2024
- Viral News Coverage

Mandated technology without security requirements will likely lead to exploitable vulnerabilities.

Network and Distributed System Security (NDSS) Symposium 2024
26 February - 1 March 2024, San Diego, CA, USA
ISBN 1-891562-93-2
https://dx.doi.org/10.14722/vehiclesec.2024.23047
www.ndss-symposium.org

Responsible Disclosure

3.2.3 DOWNLOAD OF CODE WITHOUT INTEGRITY CHECK CWE-494

IO-1020 Micro ELD downloads source code or an executable from an adjacent location and executes the code wit sufficiently verifying the origin or integrity of the code.

CVE-2024-28878 has been assigned to this vulnerability. A CVSS v3.1 base score of 9.6 has been calculated; the CV vector string is (AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).

A CVSS v4 score has also been calculated for CVE-2024-28878. A base score of 9.4 has been calculated; the CVSS v string is (CVSS4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H).

SECURITY

73

Truck-to-truck worm could infect – and disrupt – entire US commercial fleet

The device that makes it possible is required in all American big rigs, and has poor security

Jessica Lyons

Fri 22 Mar 2024 // 00:03 UTC

Vulnerabilities in common Electronic Logging Devices (ELDs) required in US commercial trucks could be present in over 14 million medium- and heavy-duty rigs, according to boffins at Colorado State University.

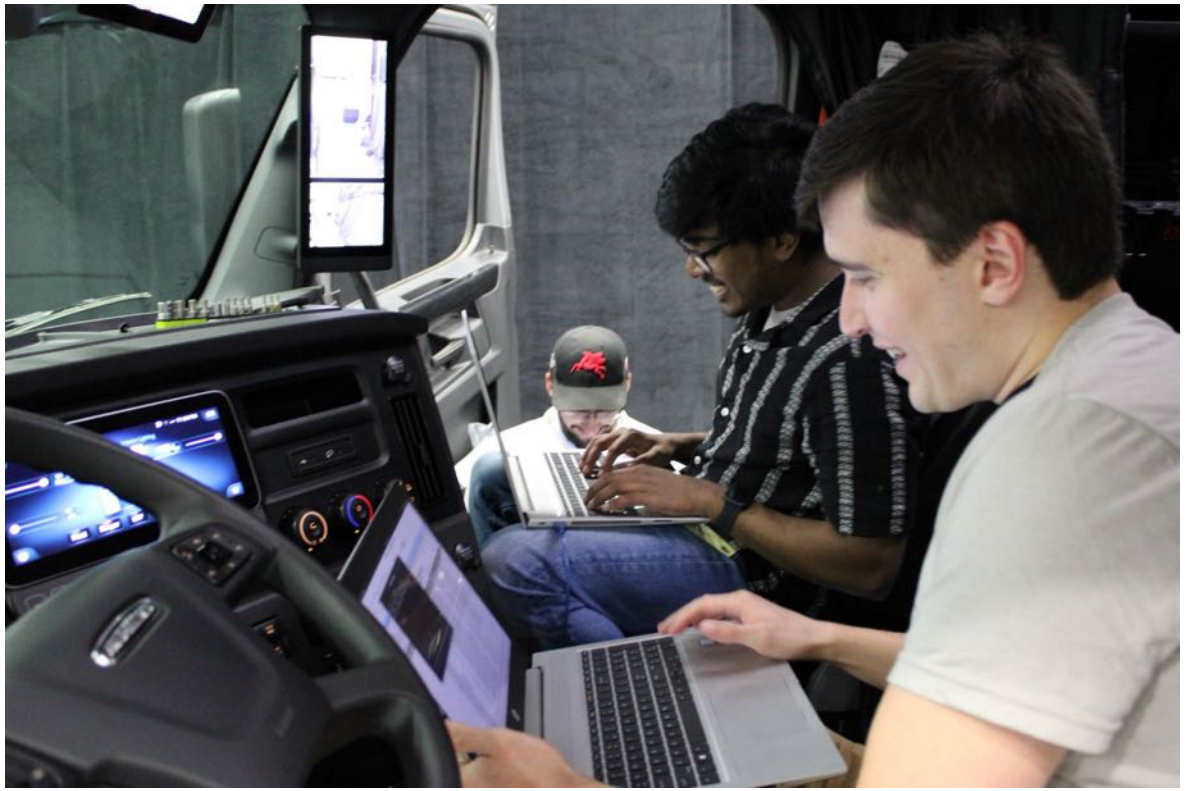
In a paper presented at the 2024 Network and Distributed System Security Symposium, associate professor Jeremy Daily and systems engineering graduate students Jake Jepson and Rik Chatterjee demonstrated how ELDs can be accessed over Bluetooth or Wi-Fi connections to take control of a truck, manipulate data, and spread malware between vehicles.

Part of the solution is to train people to address security of critical infrastructure.

Describing the CyberX Challenges

What is the X in CyberX Challenge?

- X = Industry with cyber-physical systems
  - CyberAuto Challenge
  - CyberTruck Challenge
  - CyberTractor Challenge
  - CyberBoat Challenge



The Cybersecurity & Infrastructure Security Agency (CISA) in the Department of Homeland Security (DHS) has identified 16 critical infrastructure sectors whose systems are of paramount importance to the modern way of life.

CyberX Challenge Events Relation to Systems Engineering

"By 2035, cyber-security will be as foundational a perspective in systems design as system performance and safety are today. The systems engineering discipline will grow to become even more interdisciplinary, embedding cyber expertise into the **team** to ensure cyber is considered through the full system life cycle."

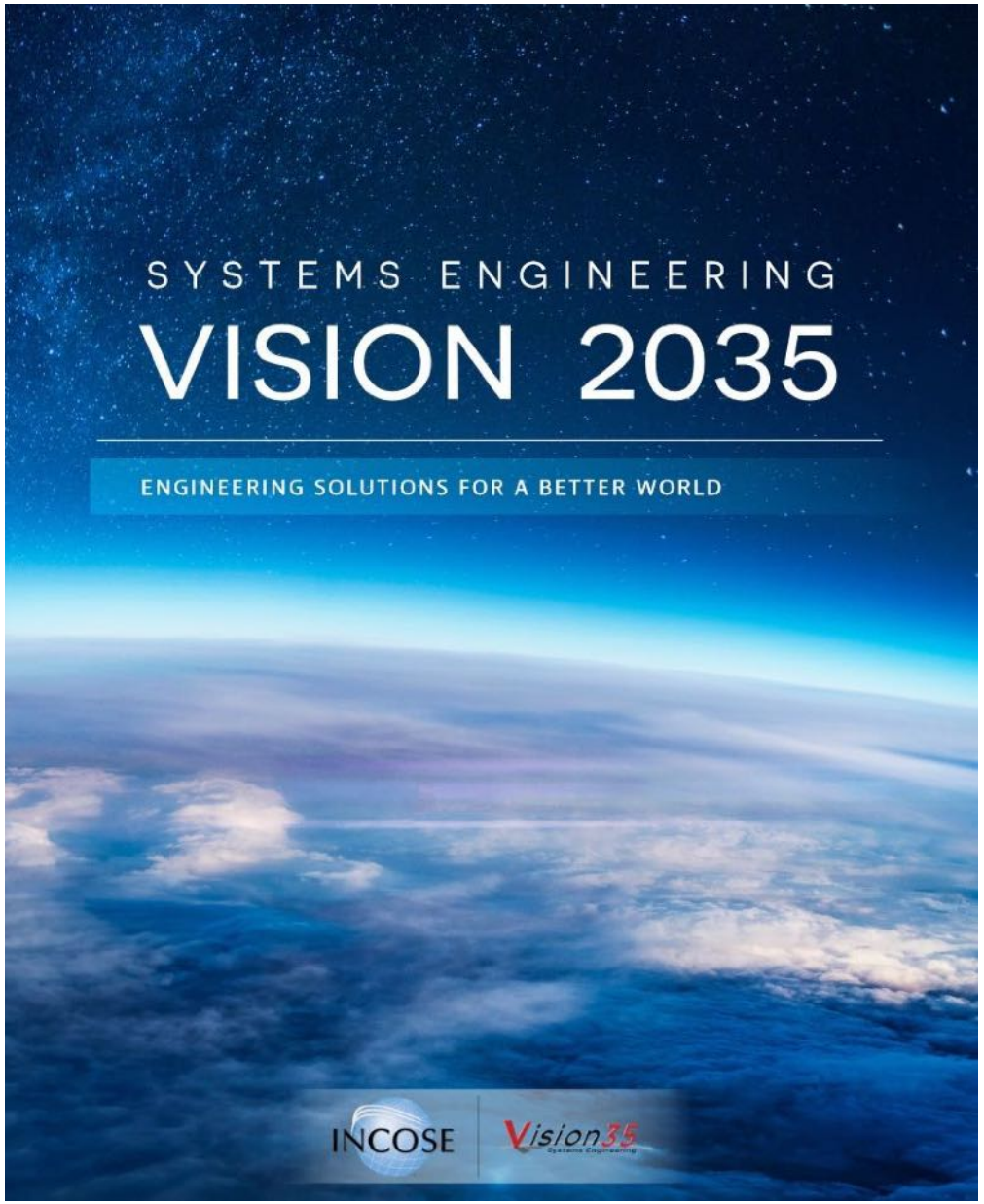
-Page 37, INCOSE VISION 2035

"A wide range of education and **training programs** provide systems engineers the requisite systems engineering fundamentals, and help them continue to stay abreast of advances in practice and technologies."

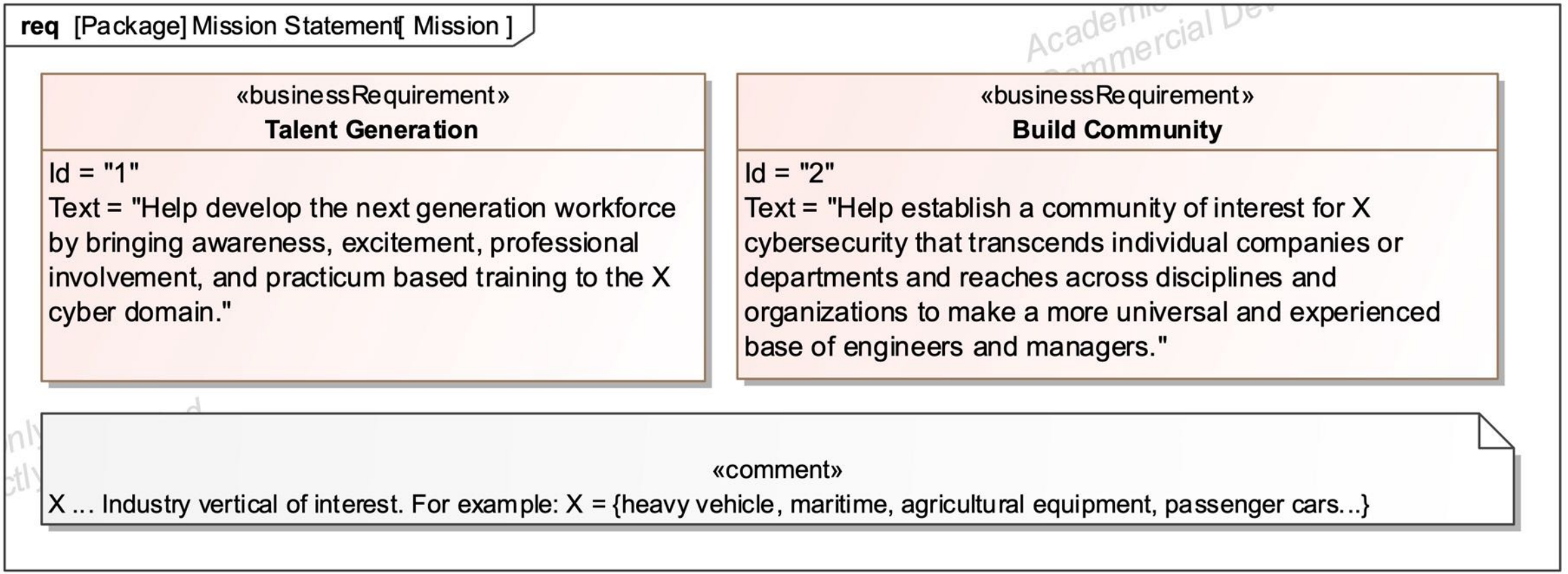
-Page 44, INCOSE VISION 2035

"Challenge-based, **hands-on education**, and training of integrated methods and approaches evolves."

- Page 60, INCOSE Vision 2035



Mission Statement



Concepts from INCOSE Vision 2035 map to the Mission Statements

Stakeholders

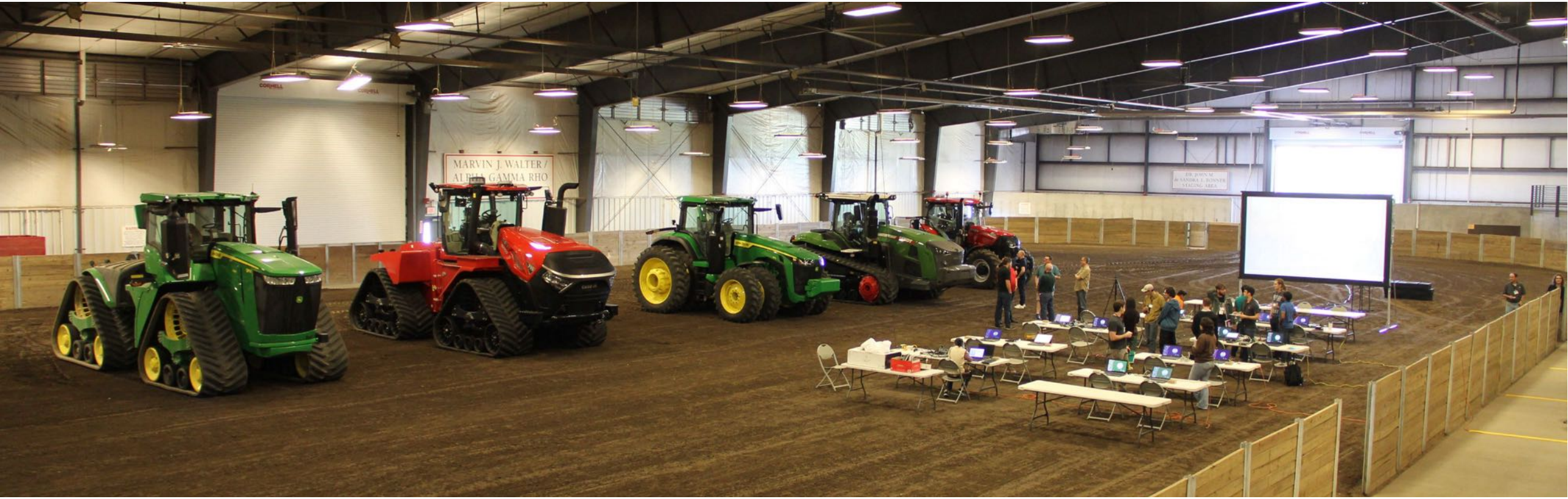
Industry partners network with their peers at the 2024 CyberTruck Challenge.

- Industry
  - Build community
  - Establish relationships
  - Learn about their products
- Academia
  - Students see opportunities
  - Professors learn state of the art
- Security Researchers
  - Demonstrate capabilities
  - Business development
- Government
  - Understand operating environment
  - Build connections
  - Keep public safe

Details regarding the

CyberTractor Challenge

Hansen Center, Iowa State University



Tractors provided by John Deere, Case New Holland and Agco

Hands-on Learning with Tractor Equipment

- J1939, CAN, and ISOBus
- Wireless Systems
- Embedded Linux Hacking
- Open Source Intelligence (OSINT) Gathering

www.cybertractorchallenge.org

Practical Classroom Environment

Details regarding the

CyberBoat Challenge

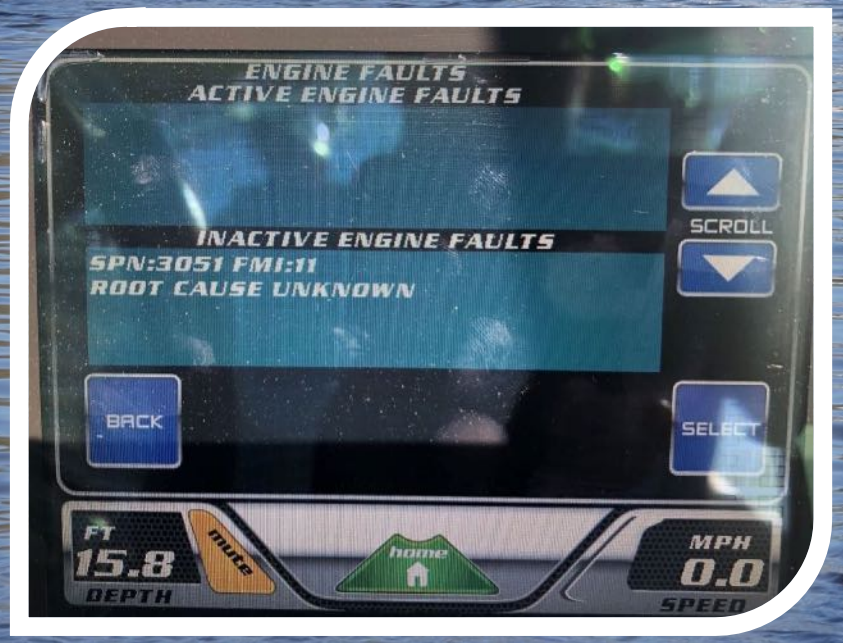
Students connected to the NMEA2000 network on a Mastercraft X30

CyberBoat Challenge

- Inaugural Event at Michigan Tech Univ.
  - May of 2022
  - Houghton, MI (Upper Peninsula)

Co-located Classroom and Learning Platform (Boat)

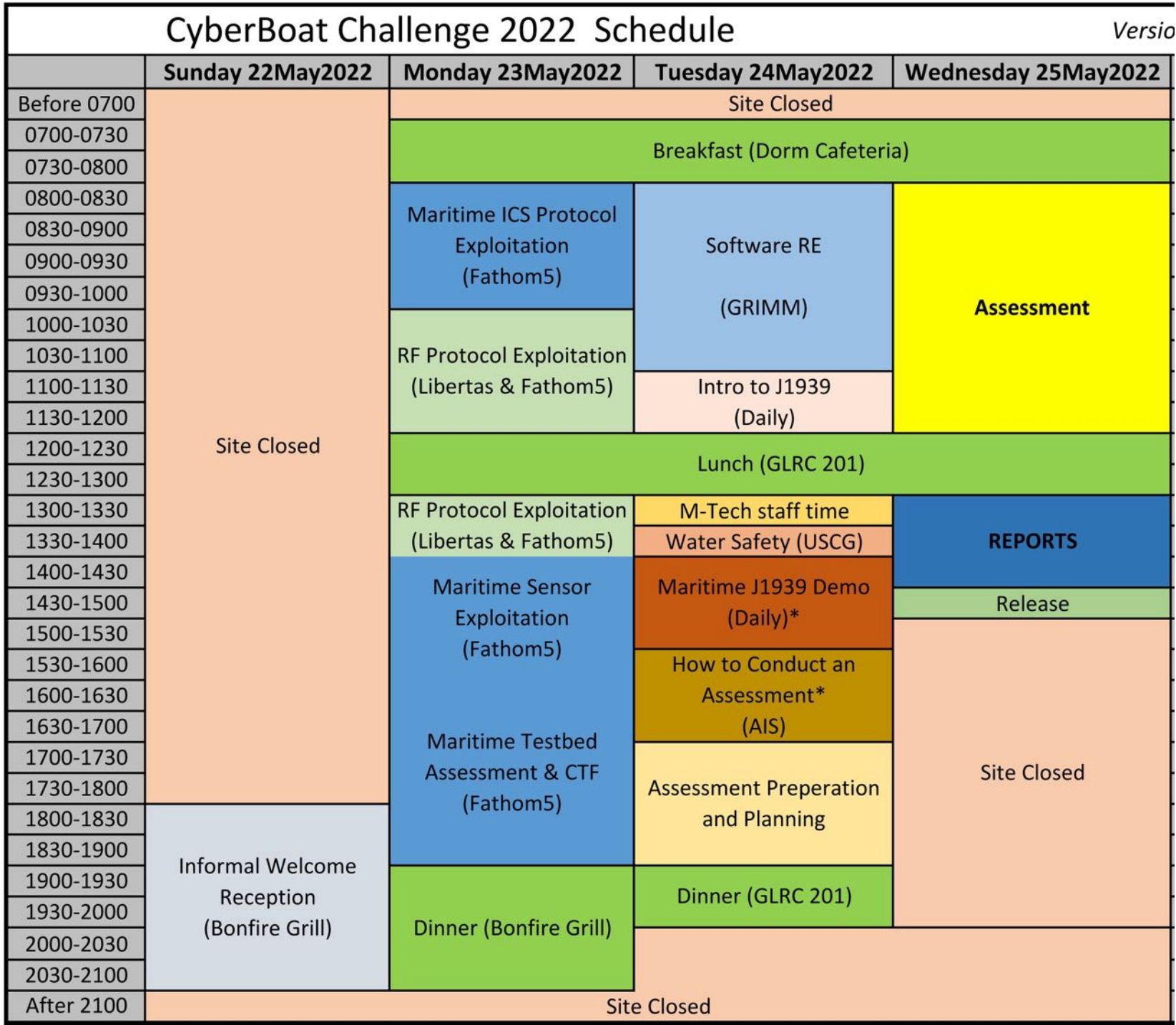
Students get unique opportunities to apply theory on the water



Schedule Highlights

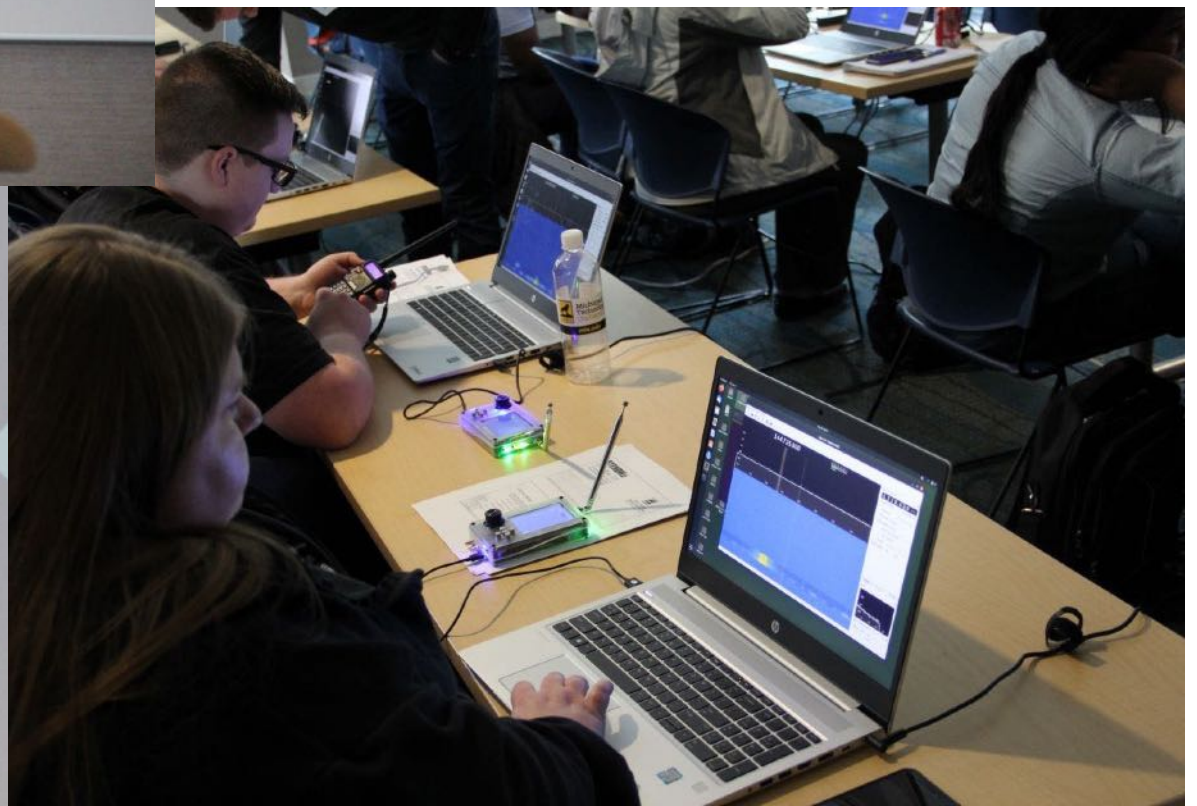
Industry experts teach specialty classes

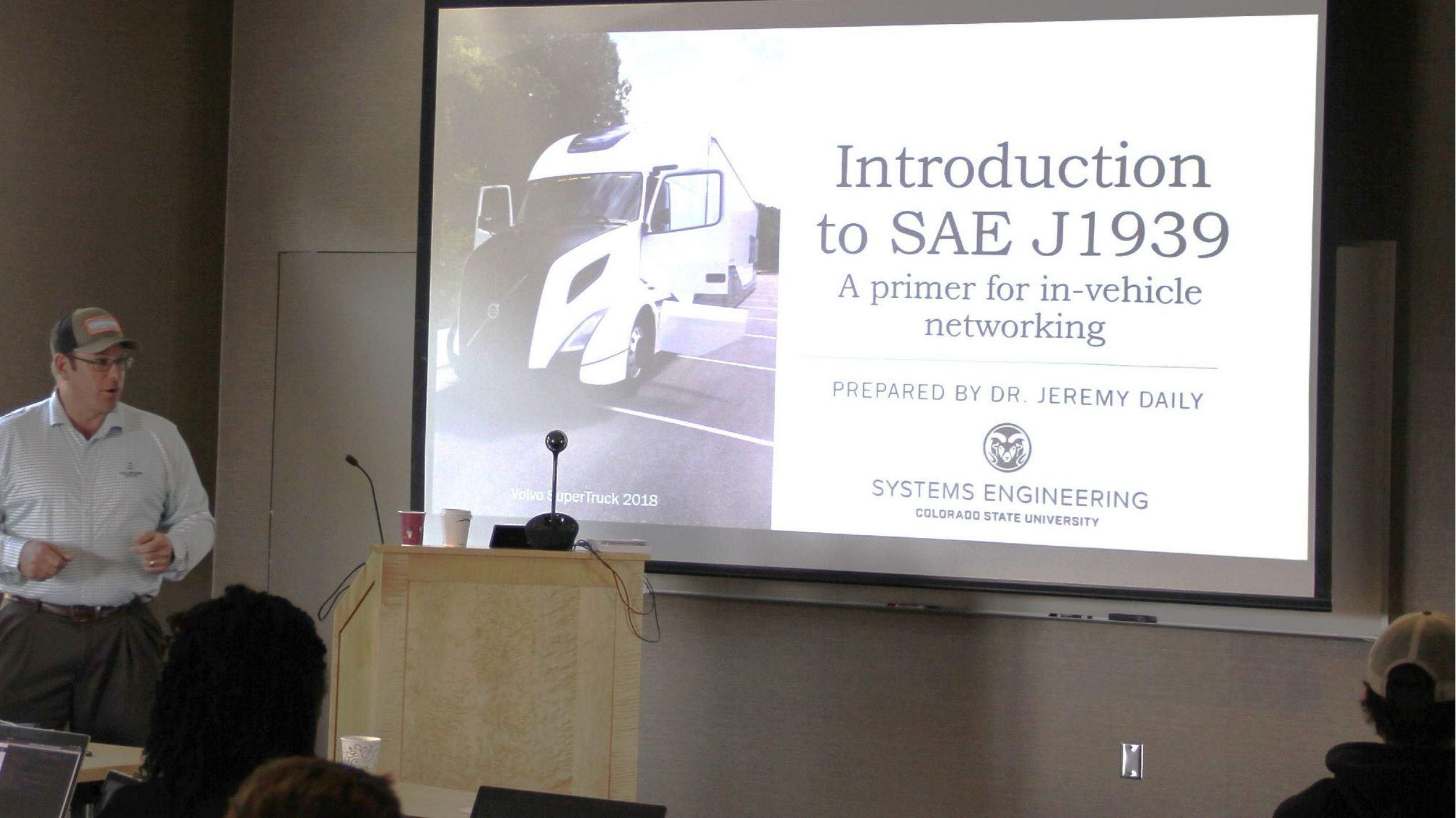
Last day is reserved for free-form assessments and student reports



Maritime Automatic Identification System (AIS) (in)security

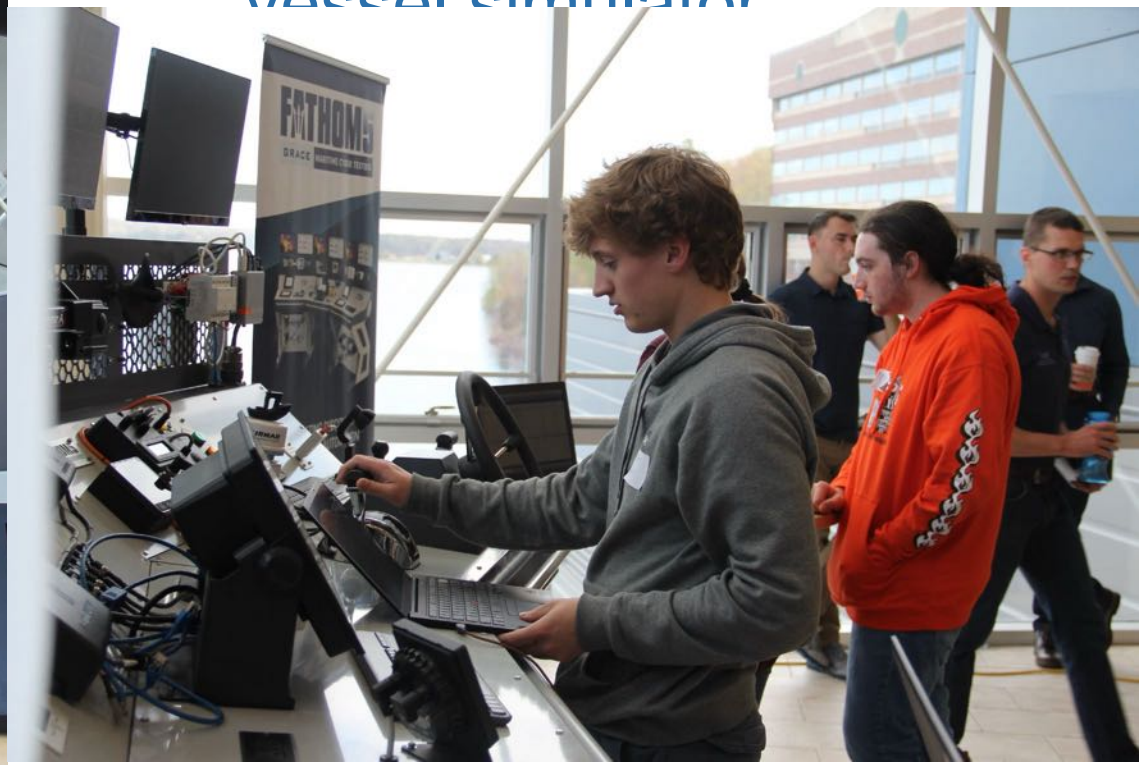
Wireless Systems and Software Defined Radio (SDR)




Volvo SuperTruck 2018
Introduction to SAE J1939
A primer for in-vehicle networking
PREPARED BY DR. JEREMY DAILY
SYSTEMS ENGINEERING
COLORADO STATE UNIVERSITY

Grace Maritime Cyber Testbed

- Hands on with a large vessel simulator



NMEA 2000 Decoding Example

- can0 0DF50B81 42 B5 08 00 00 00 00 FF

0D – Priority (0b0000 1101 = 3)
DF50B – Water Depth PGN (0x1F50B)
81 – Dynamically Claimed Source Address

42 – Sequence ID (0x42 = 66)
B5 08 00 00 – Depth (0x8B5 = 2,229*0.01m = 22.29m = 73.13ft)
00 00 – Offset (zero)
FF – Maximum Depth Range (Not Available)

Water Depth **PGN: 128267 hex: 1F50B**

Water depth relative to the transducer and offset of the measuring transducer. Positive offset numbers provide the distance from the transducer to the waterline. Negative offset numbers provide the distance from the transducer to the part of the keel of interest.

Single Frame: Yes | Priority Default: 3 | Default Update Rate: 1000 milliseconds | Frequency: 1. cycles per second
Destination: Global | Query Support: Optional | Command Support: Optional | ACK Rqmnts: None

Original Reference ID # 60

Field #	Field Name				
1	**Sequence ID**	Byte Field Size: 1		Request Parameter	Optional
		Bit Field Size:		Command Parameter:	Optional
	DD056 Sequence ID		An upward counting number used to tie related information together between different PGNs . For example, the SID would be used to tie together the COG, SOG and RAIM values to a given position. 255=no valid position fix to tie it to. Range 0 to 252 for valid position fixes.		
	DF53 Integer, 8 bit unsigned	**uint8**	Range: 0 to 252	Resolution: 1 bit	Unit-less number
2	**Water Depth, Transducer**	Byte Field Size: 4		Request Parameter	Optional
		Bit Field Size:		Command Parameter:	Optional
	DD162 Water Depth At Transducer		Depth relative to the transducer location. Range of value specified in "Maximum Depth Range" (field 4).		
	DF09 Distance	**uint32**	Range: 0 to ~4.295x10E+7 m	Resolution: 1x10E-2 m	
3	**Offset**	Byte Field Size: 2		Request Parameter	Optional
		Bit Field Size:		Command Parameter:	Optional
	DD161 Transducer Offset		Positive values represent distance from transducer to water line and negative values represent distance from the transducer to the keel.		
	DF46 Distance, signed, medium	**int16**	Range: +/- 32.764 m	Resolution: 1x10E-3 m	
4	**Maximum Depth Range**	Byte Field Size: 1		Request Parameter	Optional
		Bit Field Size:		Command Parameter:	Optional
	DD350 Maximum Depth Range		Device classification of the Maximum Range over which water depth can be measured. 253 = Deeper than 2,520 meters 254 = Error 255 = Data Not Available		
	DF109 Distance, Rough Approxi	**uint8**	Range: 0 - 2,520 meters	Resolution: 10 meters	

Smart Buoy Hacking

Mentors work with students to explore

Connecting to the CAN Bus on the Boat

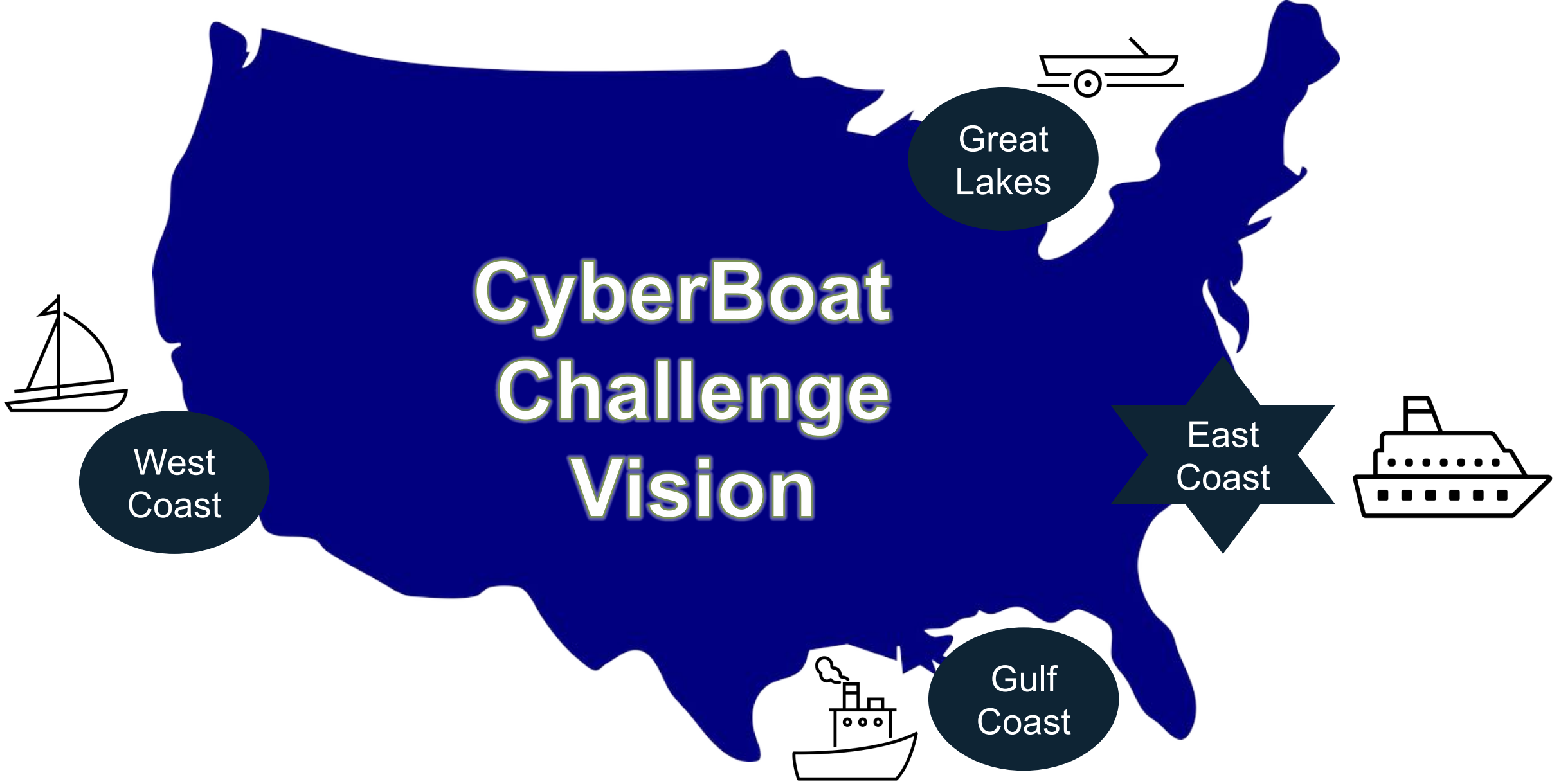
Students had their own connection to the NMEA2000 network.

Student Presentations

CyberBoat Challenge Sponsorship

- Michigan Tech Univ. provided housing
- Systems Engineering at Colorado State Univ. provided meals and travel
- Students provide their own travel
- We towed the boat from CO to MI
  - Yes, that's snow on the ski boat

SYSTEMS ENGINEERING
COLORADO STATE UNIVERSITY

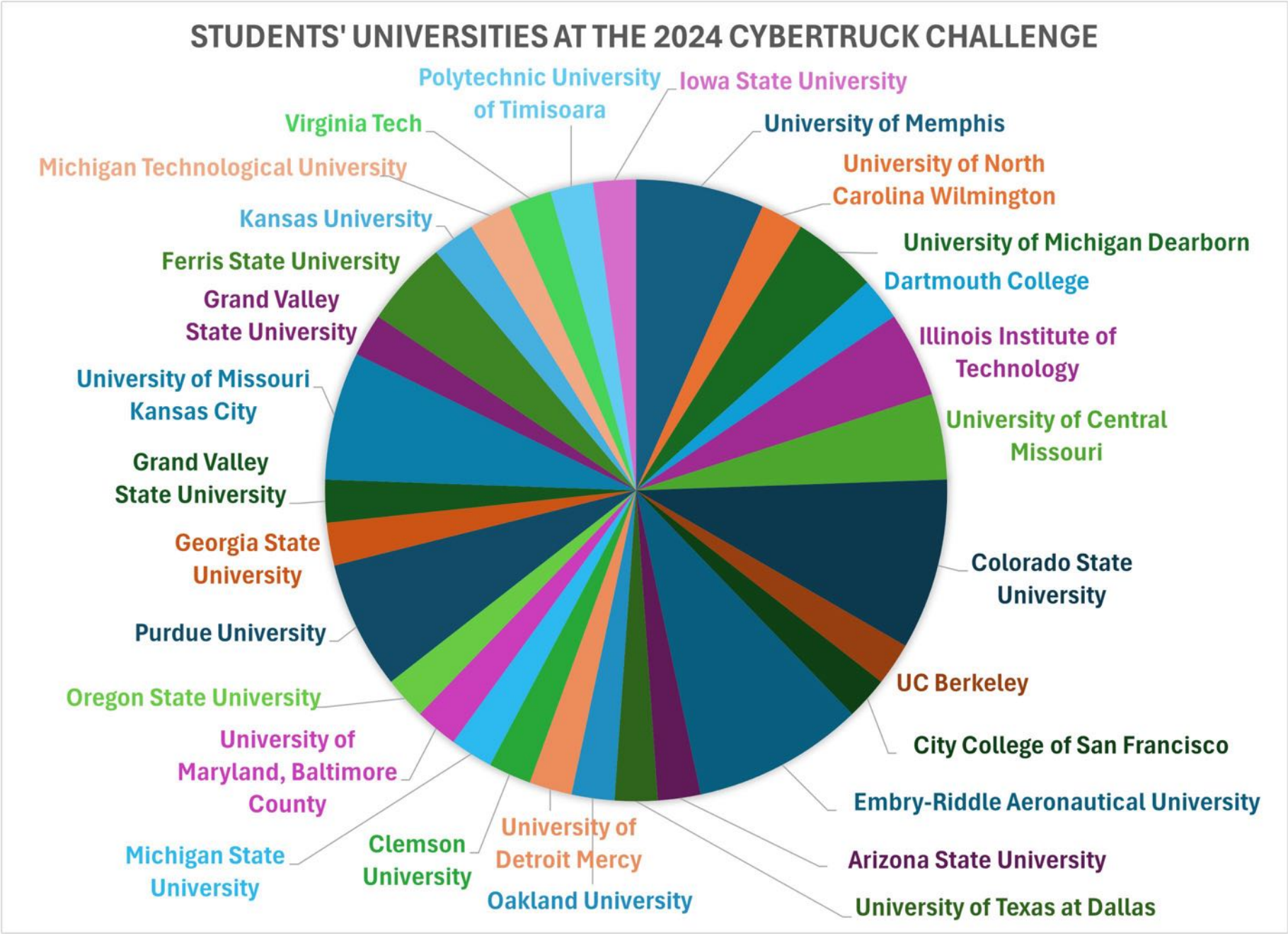


Goal: Rotating regional events culminating with the CyberShip Challenge on a large vessel.

Class of 2024 at the Macomb Community College in Warren, MI

Details regarding the

CyberTruck Challenge



For 2024, there were 46 students from 29 universities.

Thank you to the CyberTruck Challenge® sponsors

All Cyber Challenge events are organized as independent non-profit entities.

Premier Sponsor

NMFTA™ National Motor Freight Traffic Association, Inc.

CYBERTRUCK CHALLENGE®

Platinum Sponsors

PACCAR

GEOTAB management by measurement

samsara Connected Operations Cloud

Cummins

DEVCOM Ground Vehicle Systems Center

Gold Sponsors

BOSCH

NAVISTAR®

Silver Sponsors

Allison Transmission

DAIMLER TRUCK North America

VOLVO

GAMBER JOHNSON

PMT · Yanfeng · Adient · InfoCase · LIND

ORBITAL Installation Technologies

U.S. Department of Transportation
Federal Motor Carrier Safety Administration

Bronze Sponsors

SYSTEMS ENGINEERING COLORADO STATE UNIVERSITY

NetSPI™

Stoneridge

AUTO-ISAC Automotive Information Sharing and Analysis Center

Macomb Community College
Education • Enrichment • Economic Development
Discover. Connect. Advance.

Bendix

Contributors

Old Dominion Freight Line

PITT OHIO SUPPLY CHAIN • LTL • TL

ais

University of Detroit Mercy Build A Boundless Future

Warren Michigan, 24-28 June 2024.

Sponsorship covers the costs for student travel, venue, catering, staff, instructors, etc.

CyberTruck Challenge 2024 Schedule

Version:20240621

	Sunday, 23 June	Monday, 24 June		Tuesday, 25 June		Wednesday, 26 June	Thursday, 27 June	Friday, 28 June	Time
		Group A	Group B	Group A	Group B				
Before 0700	Site Closed	Site Closed							Before 0700
0700-0730		Breakfast		Breakfast		Breakfast	Breakfast	Breakfast	0700-0730
0730-0800								Awards	0730-0800
0800-0830		Welcome // NDA		***Playing in Traffic***	Wireless Systems	Safety & Legal Briefing	Assessment	Student Team Briefs (30 minutes each group)	0800-0830
0830-0900		Vehicle Orientation				Assessment			0830-0900
0900-0930									0900-0930
0930-1000		Truck Systems and Ethernet	***Hardware Reverse Engineering***						0930-1000
1000-1030									1000-1030
1030-1100				Break	Break				1030-1100
1100-1130		Truck Networks and Communication		Wireless Systems	***Playing in Traffic***				1100-1130
1130-1200			***Firmware Hacking 1***						1130-1200
1200-1230									1200-1230
1230-1300		Lunch (Education)				Lunch	Lunch	Lunch	1230-1300
1300-1330									1300-1330
1330-1400		***Hardware Reverse Engineering***	Playing with Traffic	Lunch		Assessment	Assessment	Site Closed	1330-1400
1400-1430									1400-1430
1430-1500				Vehicle Hacking 2	***Firmware Hacking 2***				1430-1500
1500-1530									1500-1530
1530-1600		Break							1530-1600
1600-1630		***Firmware Hacking 1***	Truck Systems and Ethernet						1600-1630
1630-1700				Break	Break				1630-1700
1700-1730		***Playing with Traffic***		***Firmware Hacking 2***	Vehicle Hacking 2				1700-1730
1730-1800			Truck Networks and Communication						1730-1800
1800-1830	Informal Welcome Reception (offsite)								1800-1830
1830-1900									1830-1900
1900-1930		Dinner		Dinner		Dinner	Dinner		1900-1930
1930-2000									1930-2000
2000-2030		Trucking Industry Impact		Working in Industry		Assessment	Free		2000-2030
2030-2100		Free		**Assessment Preparation**					2030-2100
2100-2130	Site Closed								2100-2130
2130-2200				Free					2130-2200
After 2200		Site Closed							After 2200

Truck Networks

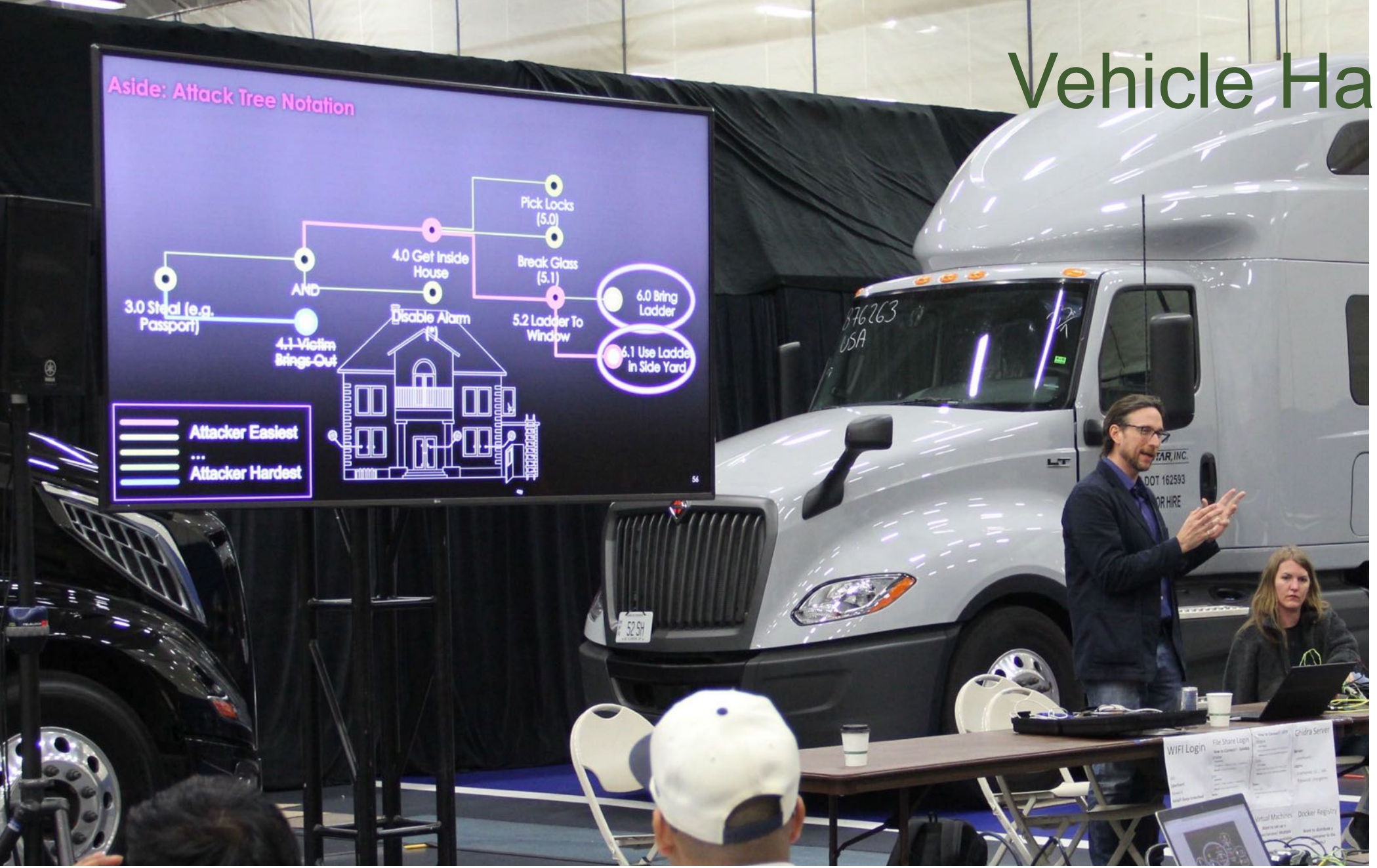
- Instructor: Amy Koefod,
- Navistar

Objectives:

- Learn to interpret SAE J1939 Messages
- Python scripting to probe networks

Wireless Systems

Vehicle Hacking 2



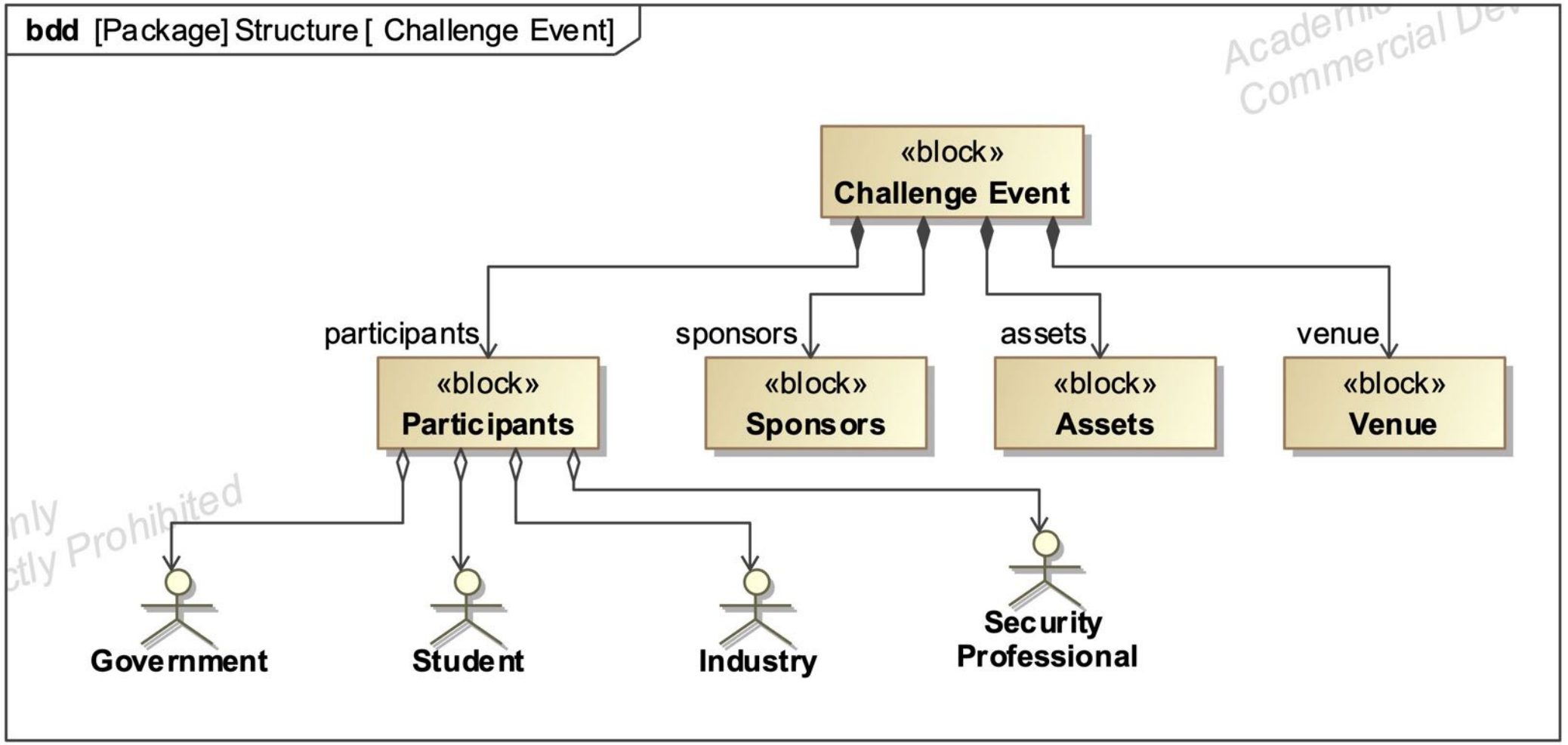
Bringing it together through

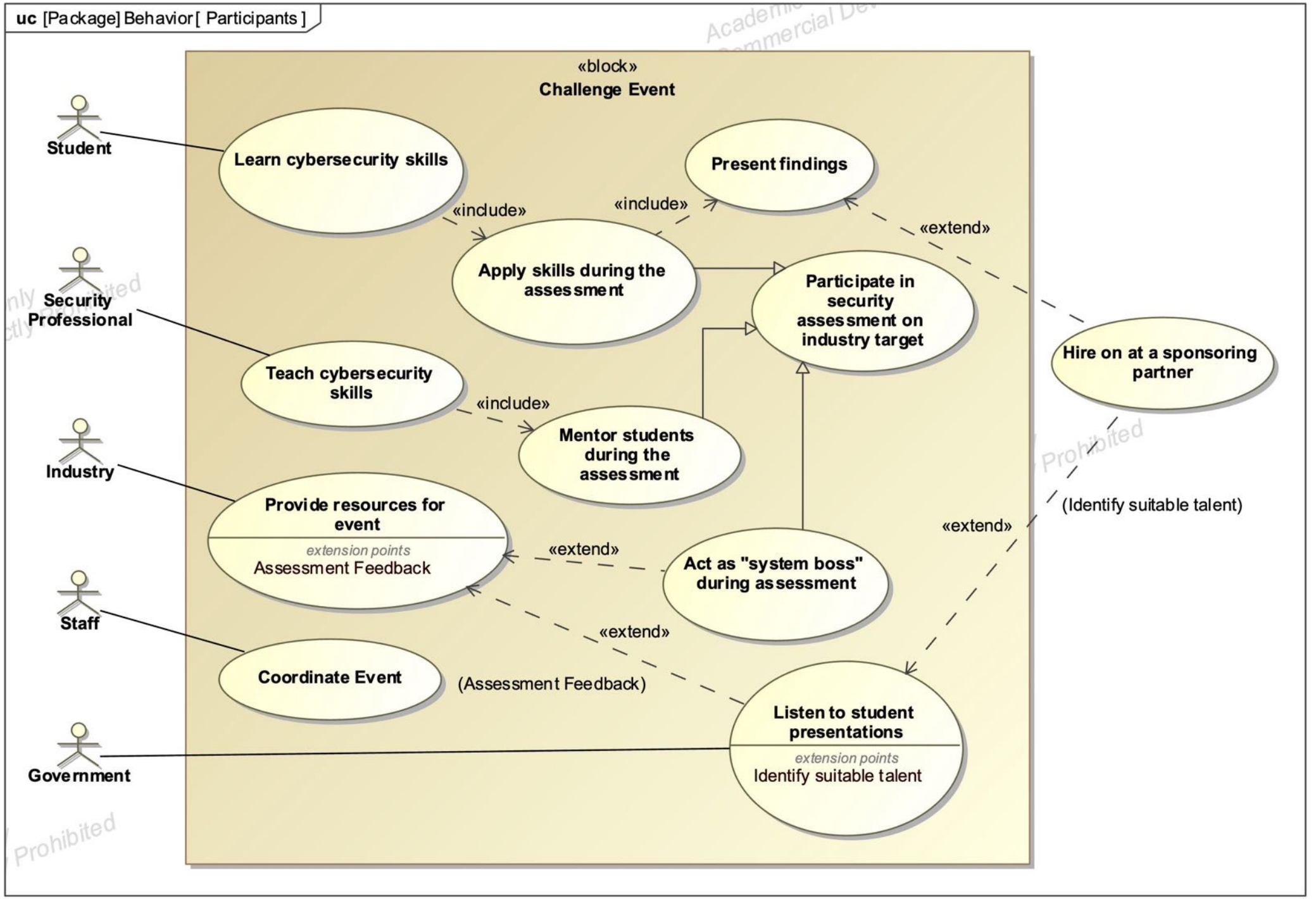
Systems Modelling for the Cyber Challenges

Model-Based Systems Engineering

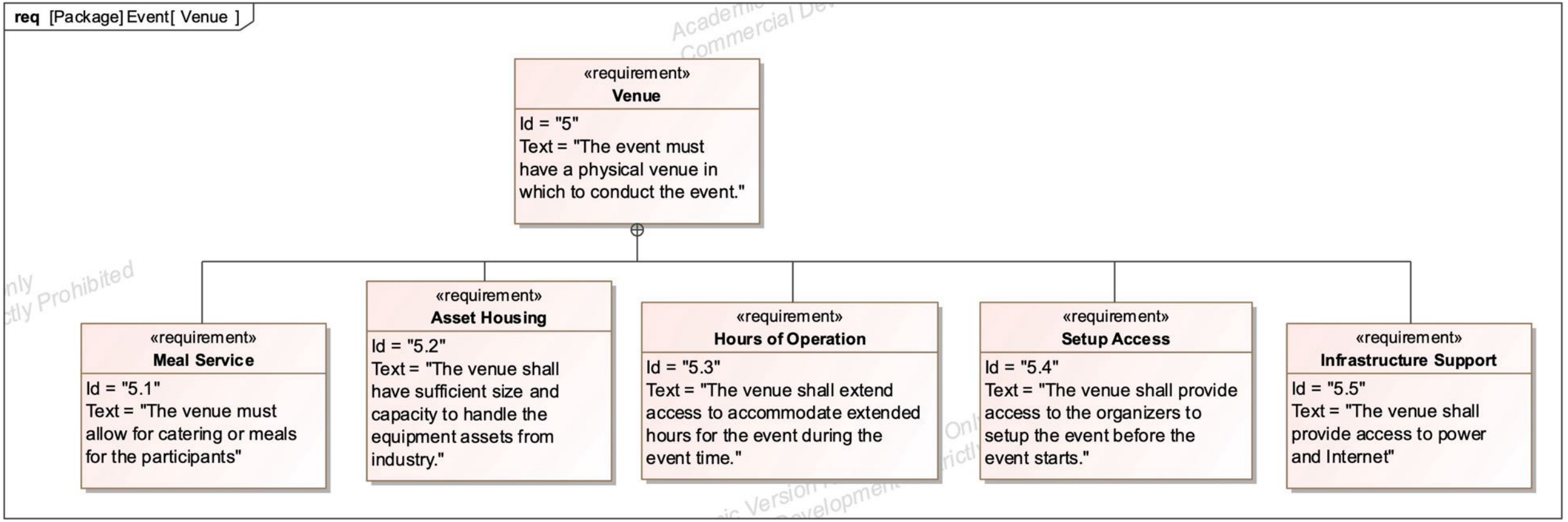
- SysML as the Language
- Catia Magic Systems of Systems Architect for the tool
- Magic Grid Method (partial)
- Added the Mission Statement as part of the stakeholder needs.

Cyber Challenge Event Composition

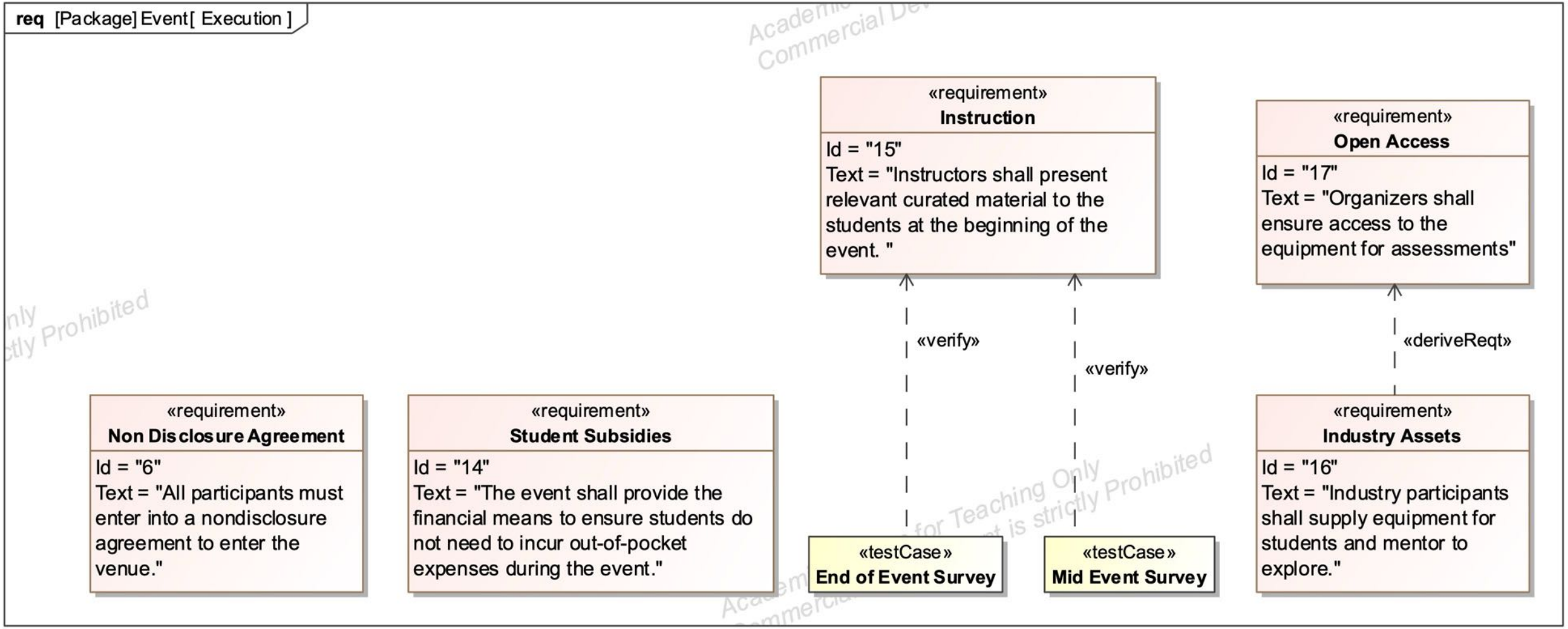



uc [Package] Behavior [Participants]
«block»
Challenge Event
Student
Security Professional
Industry
Staff
Government
Learn cybersecurity skills
Present findings
«include»
«include»
«extend»
Apply skills during the assessment
Participate in security assessment on industry target
Hire on at a sponsoring partner
Teach cybersecurity skills
«include»
Mentor students during the assessment
Provide resources for event
extension points
Assessment Feedback
«extend»
Act as "system boss" during assessment
«extend»
(Identify suitable talent)
«extend»
Coordinate Event
(Assessment Feedback)
Listen to student presentations
extension points
Identify suitable talent

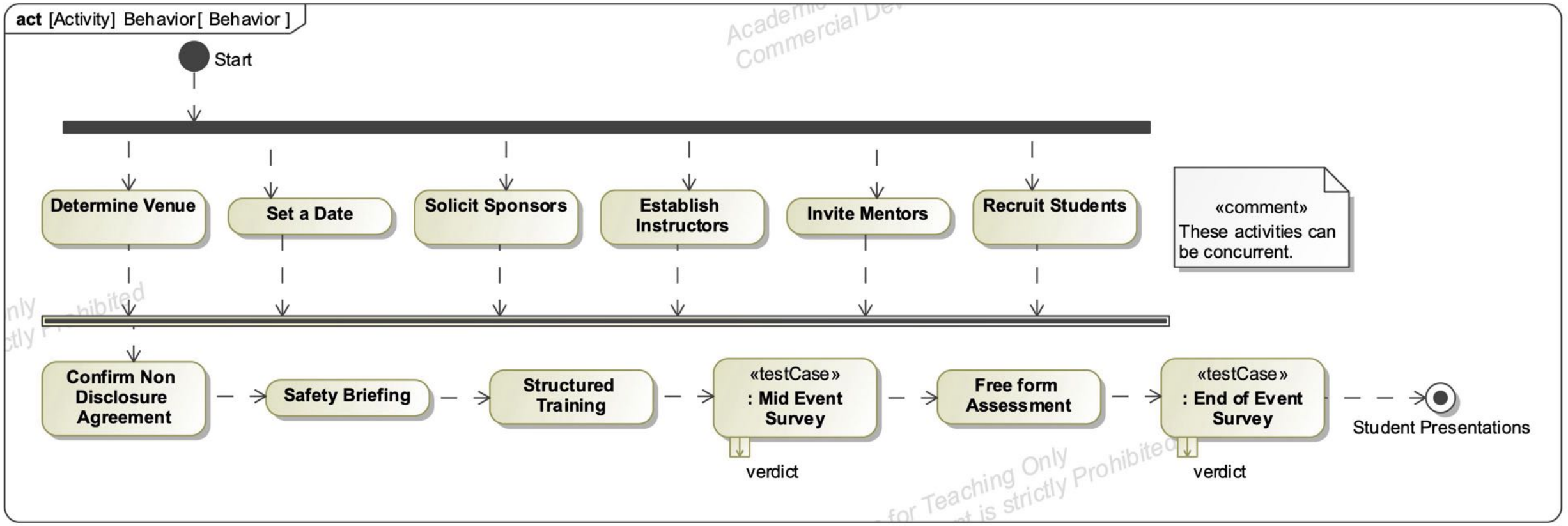
Example Requirements for the Venue



Requirements on Conducting the Event



Modeled Activities for the Cyber Events



Modeling Comments

- Modeling enhances thinking, organizing, and communicating about the different events.
- Identifies shared and common resources.

Tractor Connector

Boat Connector

Truck Connector

Industry realizes

Residual Benefits

Expansion of the Definition of the System

- Many approaches limit the scope to the vehicle itself.
- Attackers may utilize diagnostics and maintenance systems.

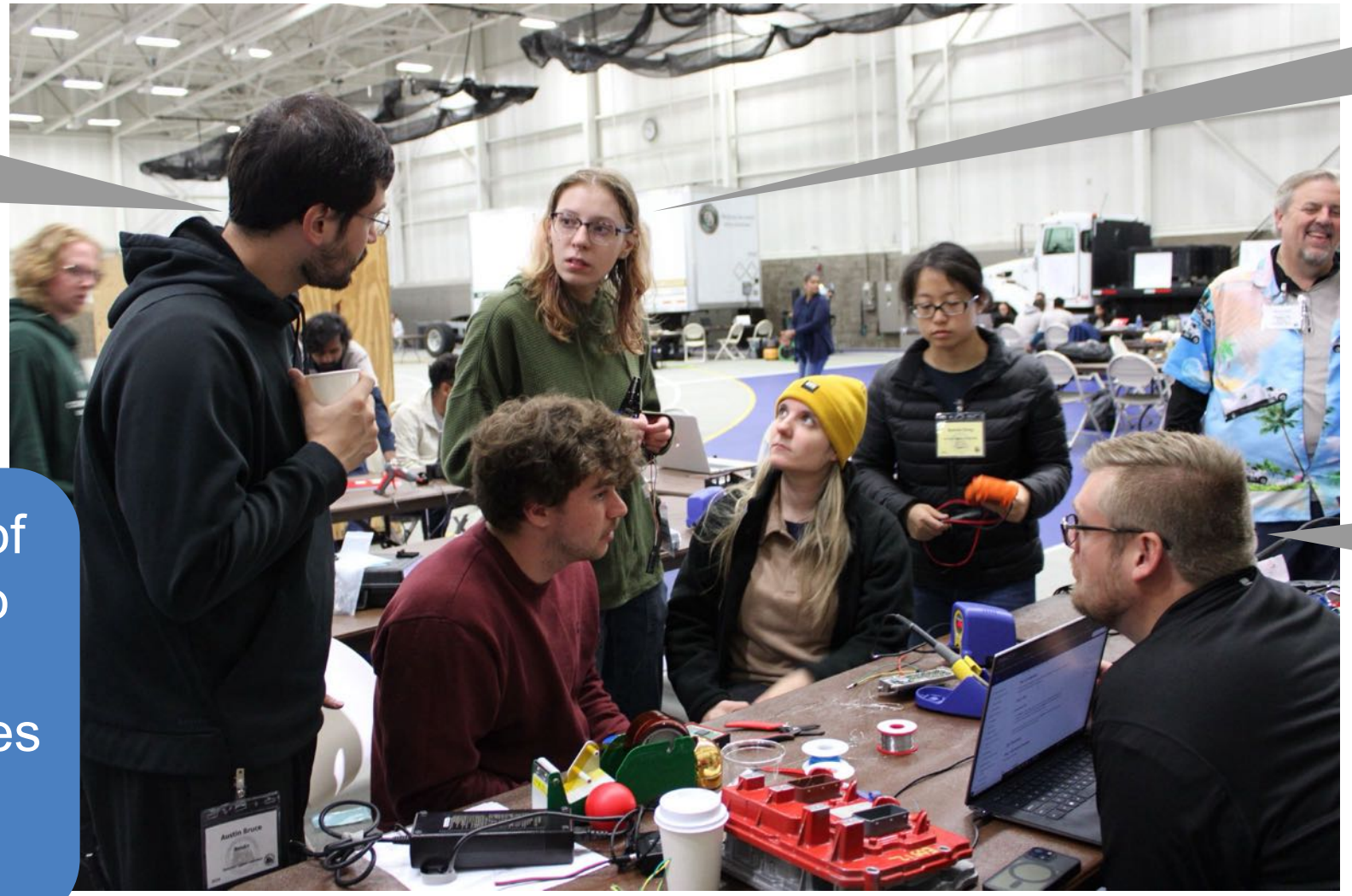
CyberX Challenges Focus on Systems as Built

- Embedded Systems binaries may include undocumented features.
- Firmware may be extracted through JTAG.
- Systems models may not include the as-built features in the executable.

Cyber Challenge Alums in Industry

Alumnus as a Mentor

Alumnus as a Mentor



Alumnus as a Mentor

Transition of students to industry demonstrates mission success.

System Complexity Outpaces Security Posture

2024 Volvo VNL with Automotive Ethernet

- New trucks have new technology, like Automotive Ethernet.
- Fleet system trackers may leak data on open MQTT brokers.
- Adversaries have complete physical access to the system.


Security breaches may become scapegoats for crashes

Concluding Remarks

- Hands-on security assessments inspire students.
- Security Researchers often know aspects of systems better than the system owner.
- The Cyber Challenge events facilitates growth of an industry's security posture.
- A systems model was developed to describing the Cyber Challenge events.
- We need more talent to address security concerns keep pace with innovation.
- Cyber attacks on critical infrastructure can have devastating results.
- Exposure to adversarial thinking is beneficial to Systems Engineers.