Producing Cyber-Physical System Cybersecurity Talent: Lessons from the CyberTruck Challenge

Dr. Jeremy Daily
Maj. Martin “Trae” Span

SYSTEMS ENGINEERING
COLORADO STATE UNIVERSITY

Motivation and Purpose of the CyberTruck Challenge

A Tale of Two Markets

It was the worst of times……

Really, really worst of times…

CRITICAL Infrastructure

Our way of life is dependent upon transportation.

Ships share resources across continents

Cars give us local mobility

Airplanes give us national and global mobility

And **TRUCKs** fuel every aspect of our consumer-based society, enabling our culture's approach to logistics

Without Trucks

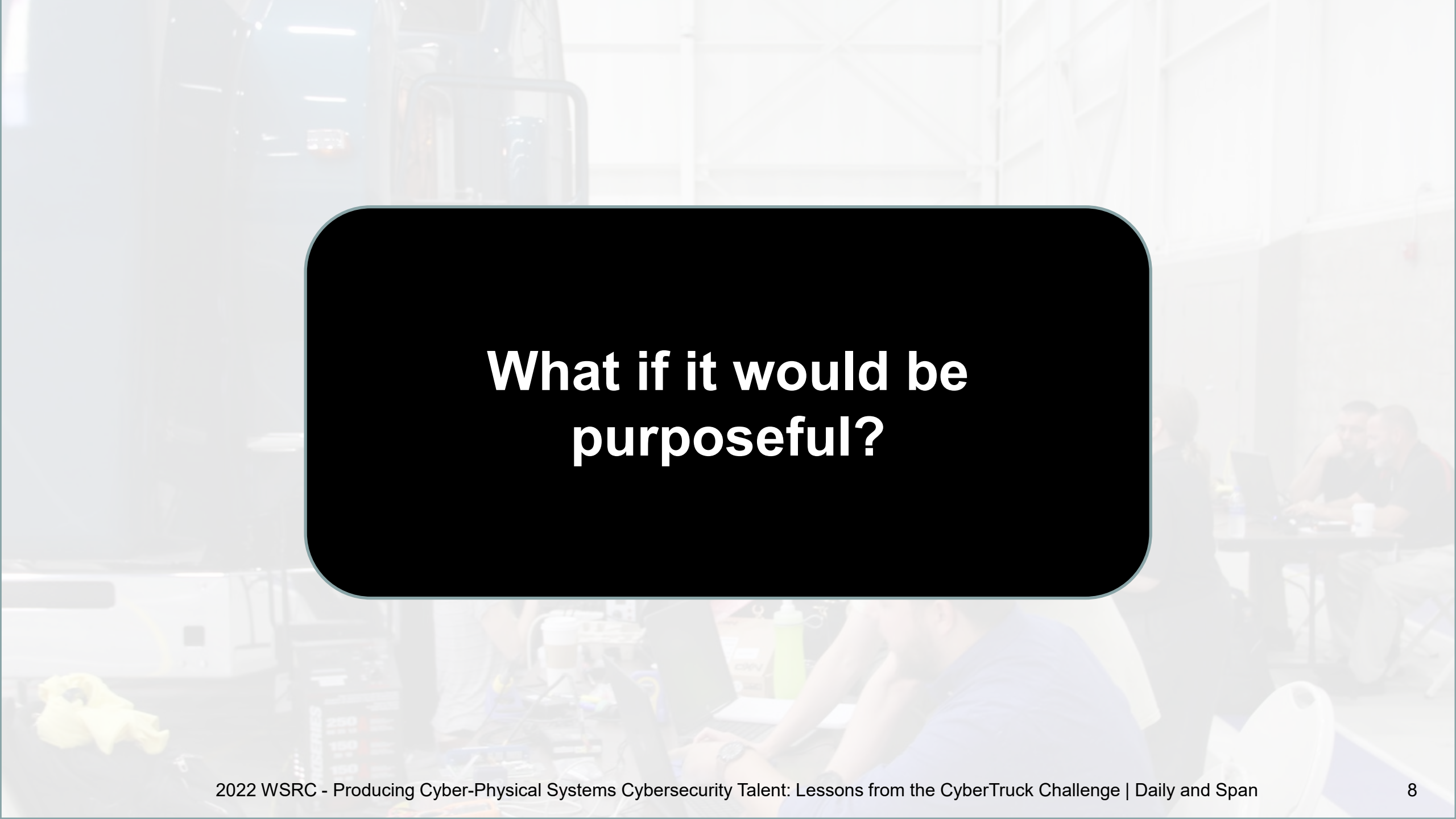
Day 1:
- Medical supply delivery stops
- Fuel stations not resupplied
- Mail stops
- Just-in-time model breaks

Day 2-3:
- Food shortages & hoarding
- Bottled water, milk - gone
- ATMs / Cash – gone
- Fuel stations – gone
- Garbage collection – stops
- Rail & Port operations

Day 7:
- Car travel stops (no fuel)
- Hospitals run out of oxygen

Day 14:
- Clean water almost gone

Day 30:
- Clean water gone

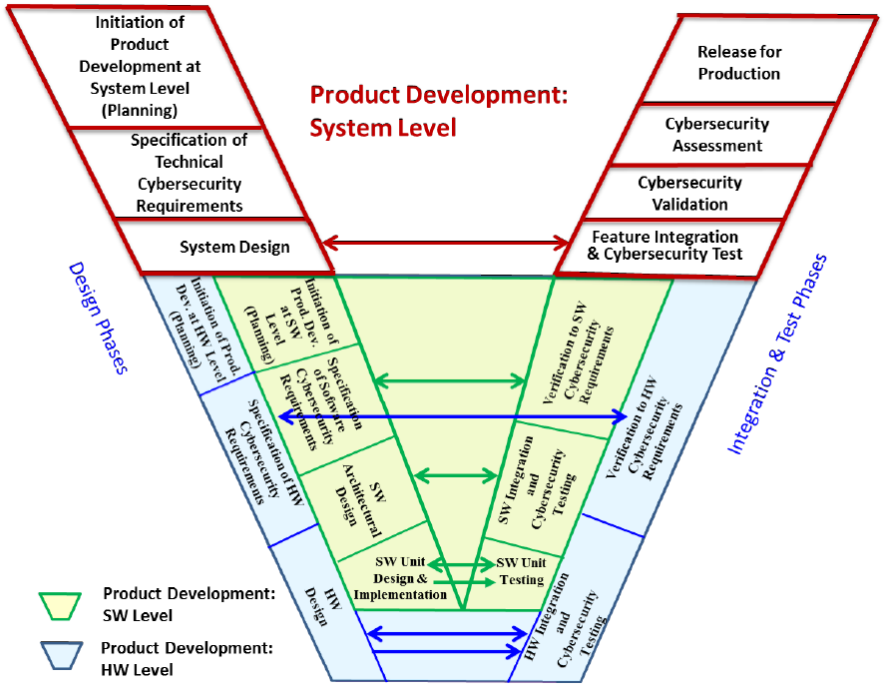

What if it would be purposeful?


FARO

Who Wants to Hack a Truck?

Cybersecurity as a Systems Engineering problem

SURFACE VEHICLE RECOMMENDED PRACTICE	J3061™	JAN2016
	Issued	2016-01
Cybersecurity Guidebook for Cyber-Physical Vehicle Systems		



- Cybersecurity affects all phases of the lifecycle
  - Acquisition Phase
  - Utilization Phase
  - Production
  - Maintenance and Support

SURFACE VEHICLE STANDARD	ISO/SAE 21434
	Issued 2021-09
Road Vehicles - Cybersecurity Engineering	

Mission Statement

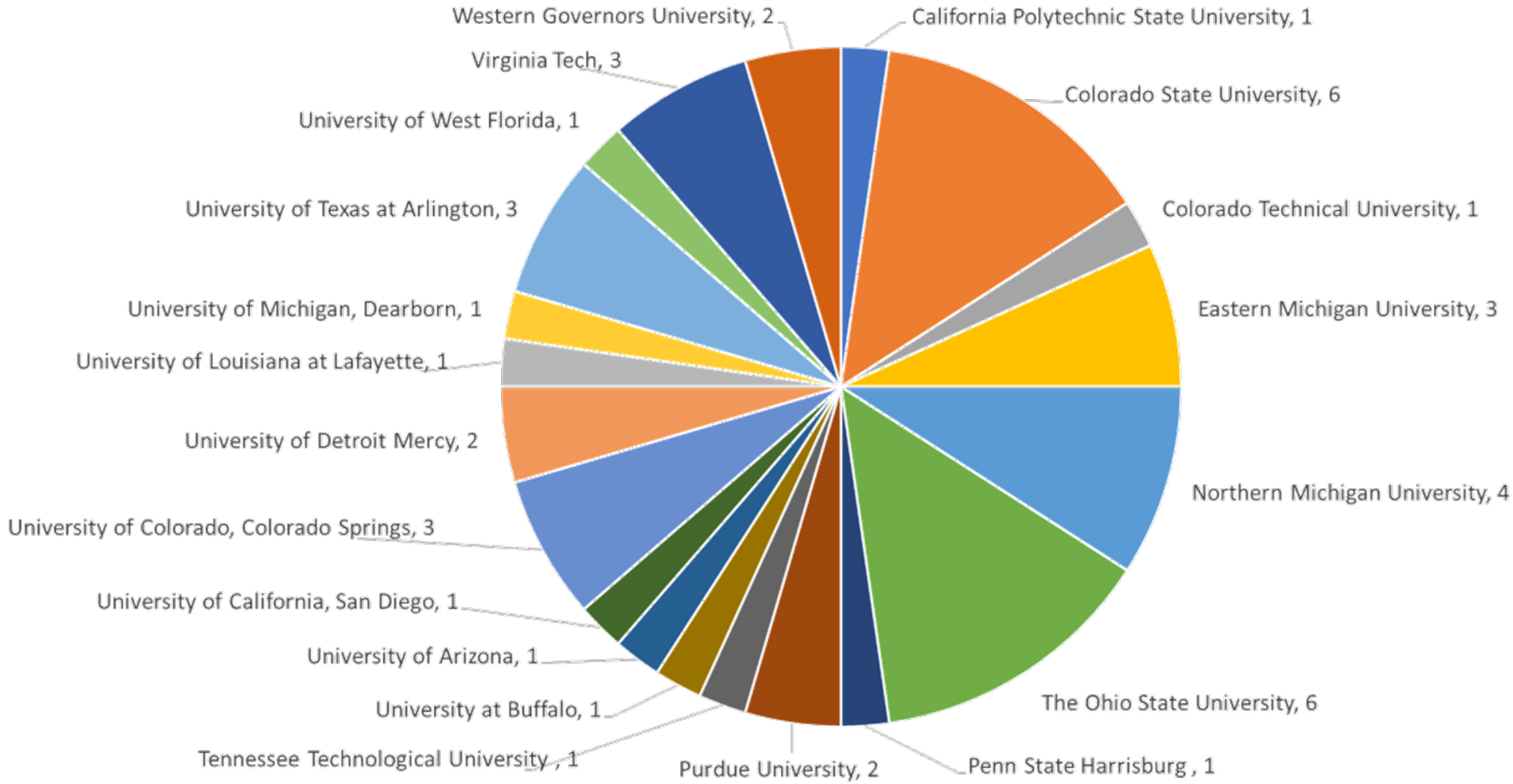
Develop talent *for the next generation workforce by bringing awareness, excitement, professional involvement, and practicum-based training to the heavy vehicle cybersecurity domain.*

Establish community *of interest for heavy vehicle cybersecurity that transcends individual companies or departments and reaches across disciplines and organizations to make a more universal and experienced base of engineers and managers.*

Class of 2022

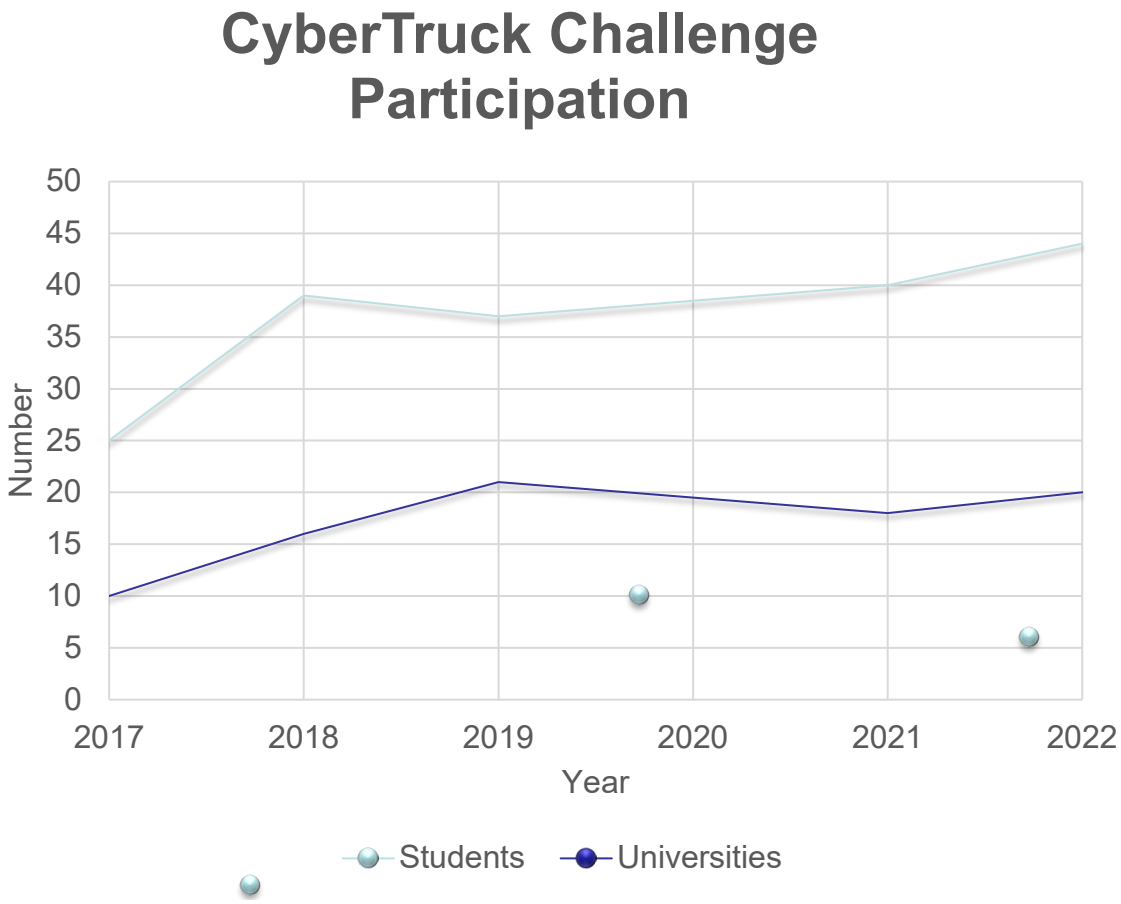
Photo taken on June 22, 2022 in the Sports and Expo Center of Macomb Community College, Warren, Michigan

2022 Student and University Participation
44 Students from 20 Universities



Student Participation Growth over 5 Years

Year	Students	Universities
2017	25	10
2018	39	16
2019	37	21
2021	40	18
2022	44	20



Student Expectations

All student expenses are covered, including:

- Travel
- On-site Meals
- Lodging

Student participants are expected to:

- Apply to the program in the spring
- Address the importance of the mission
- Answer a technical question on J1939
- Attend the entire program
- Actively participate in the assessments
- Present results at the end of the week
- Become ambassadors for the CyberTruck Challenge and vehicle cybersecurity

Thank you to the CyberTruck Challenge sponsors

U.S. Department of Transportation

Federal Motor Carrier Safety Administration

SYSTEMS ENGINEERING

COLORADO STATE UNIVERSITY


Munich RE


NAVISTAR


BATTELLE
It can be done


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


Bendix


DG TECHNOLOGIES
Vehicle Network Solutions


AUTO-ISAC
Automotive Information Sharing and Analysis Center


UNIVERSITY OF
DETROIT MERCY
COLLEGE OF ENGINEERING & SCIENCE


ais


CALSTART

Description of Activities

Real Vehicles

Sponsors bring new vehicles as assessment targets. Company engineers work with students and mentors.

Real Hackers

Experienced mentors from professional security firms help coach students through exercises and security related assessments.

Real Fun!

Students have a unique opportunity to solve challenging problems, learn from experts and experience engineering in the heavy-duty industry.

CyberTruck Challenge 2022 Schedule

Version:20220619

	Sunday, 19 June	Monday, 20 June		Tuesday, 21 June		Wednesday, 22 June	Thursday, 23 June	Friday, 24 June	Time
		Group A	Group B	Group A	Group B				
Before 0700	Site Closed	Site Closed							Before 0700
0700-0730		Breakfast						Breakfast	0700-0730
0730-0800								Student Team Briefs (30 minutes each group)	0730-0800
0800-0830		Welcome // NDA		Vehicle Network Security	***Ghidra***	Legal Briefing	Assessment		0800-0830
0830-0900		Safey and Orientation				Assessment			0830-0900
0900-0930		***Software RE***	Truck Systems and J1939						0900-0930
0930-1000									0930-1000
1000-1030				***Cryptography***	Vehicle Network Security				1000-1030
1030-1100									1030-1100
1100-1130									1100-1130
1130-1200								Awards	1130-1200
1200-1230	Site Closed	Lunch						Lunch	1200-1230
1230-1300									1230-1300
1300-1330		Truck Systems and J1939	***Software RE***	***Android***	Embedded Firmware Patching	Assessment	Assessment	Site Closed	1300-1330
1330-1400									1330-1400
1400-1430									1400-1430
1430-1500									1430-1500
1500-1530									1500-1530
1530-1600									1530-1600
1600-1630		***Trucking Industry***	Cryptography	Embedded Firmware Patching	***Android***				1600-1630
1630-1700									1630-1700
1700-1730		***Ghidra***							1700-1730
1730-1800									1730-1800
1800-1830	Informal Welcome Reception (offsite)		Trucking Industry						1800-1830
1830-1900									1830-1900
1900-1930		Dinner							1900-1930
1930-2000									1930-2000
2000-2030		Introduction to Learning Platforms		**Assessment Preparation**		Assessment	Free		2000-2030
2030-2100									2030-2100
2100-2130	Site Closed	Free		Free					2100-2130
2130-2200									2130-2200
After 2200		Site Closed							After 2200

Snacks will be served each afternoon. *Survey *Survey

Legend	
Lecture / Demo	All participants
Volvo Side	Interactive lecture and activities
Cummins Side	Interactive lecture and activities
Meals	Meals will be catered on-site
"Hacking"	On vehicle assessments
Free	Can hack, study, rest, leave, etc.
Site Closed	No access the facility
Off Site	Limelight Grill on VanDyke Ave

Topic	Instructor, Affiliation	Verified
Welcome and Review	Karl Heimer [MEDC] & Sponsor Representatives	Yes
Embedded Firmware Patching	Ang Cui, Edward Larson [Red Balloon Security]	Yes
Decompilation with Ghidra	Justin "Ozzie" Osborn [JHU-APL]	Yes
Software Reverse Engineering	Erin Cornelius [GRIMM]	Yes
Truck Systems and J1939	Jeremy Daily [Colorado State University]	Yes
Android	Eduardo Novella [Now Secure]	Yes
Cryptography	Ben Gardiner [NMFTA]	Yes
Vehicle Network Security	Hannah Silva [Leviathan Security]	Yes
Trucking Industry	Urban Jonson [Serjon]	Yes

CyberAuto Challenge Example Schedule

	Welcome & Inprocessing	Training Days			Assessment Day	Report & Release
24-hour	**Sunday 21July2019**	**Monday 22July2019**	**Tuesday 23July2019**	**Wednesday 24July2019**	**Thursday 25July2019**	**Friday 26July2019**
0700-0730		Site Opens				Sleep / Recover / Clear Hotel
0730-0800						
0800-0830		Welcome	CANBUS 1	Software RE	Ethics	
0830-0900		Legal			**ROE and Planning**	
0900-0930		Lab Orientation			ASSESSMENT	
0930-1000		Team Intros / Integration	Networking / Break	Networking / Break		**Outbrief**
1000-1030		CANBUS 1	CANBUS 1	Hardware RE		
1030-1100						
1100-1130						
1130-1200			Boss Talks			Review of NDA
1200-1230		Lunch				RELEASE
1230-1300						
1300-1330		CANBUS 1	Forensics	Electrical Vehicles	ASSESSMENT	
1330-1400						
1400-1430		Networking / Break	Networking / Break			
1430-1500		Boss Talks	Forensics	Networking / Break		
1500-1530		Ghidra		Electrical Vehicles		
1530-1600						
1630-1630	Inprocessing - Window 1	Networking / Break	Networking / Break			
1630-1700		Ghidra	Forensics Exercise	Boss Talks		
1700-1730				Electrical Vehicles Exercise		
1730-1800						
1800-1830		Dinner				
1830-1900						
1900-1930	Inprocessing - Window 2	Transportation			ASSESSMENT	
1930-2000						
2000-2030						
2030-2100						
2100-2130						
2130-2200						
2200-2230						
2230-2400						
0000-0630 next day						

Truck Systems and SAE J1939

By Jeremy Daily

Associate Professor of Systems Engineering at Colorado State

SYSTEMS ENGINEERING
COLORADO STATE UNIVERSITY

Software Reverse Engineering

By Erin Cornelius

Senior Security Researcher

Trucking Industry

By Urban Jonson

SVP Information Technology and Cybersecurity

Cryptography

By Ben Gardiner

Researcher, National Motor Freight Traffic Association, Inc.

Heavy Vehicle Network Security

By Hannah Silva

Security Researcher

leviathan security group

Using Ghidra

By Justin “Ozzie” Osborne

Security Researcher

Android Security

By Eduardo Novella

Mobile Security Researcher

NowSecure™

Patching Embedded Systems

By Wyatt Ford and Andrés Hernández

Software Engineers at Red Balloon Security

Red Balloon Security

Assessment Period: Forming Teams

A typical team would include

- 4-6 Students
- 1-2 Mentors
- 1-3 Industry
- 1-2 Government
- 1 named Vehicle Boss

Vehicle Bosses can stop an assessment at any time.

Results and presentations only go to the vehicle boss.

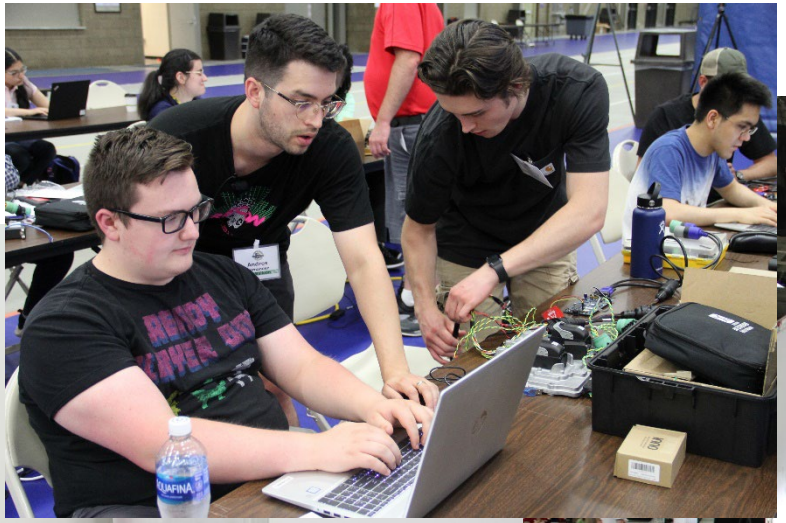
Students from the same school are encouraged to join separate teams.

In 2022, 8 teams were formed

Each team has 30 minutes to present their results at the end.

Assessment Period: Applying the hands-on lecture content

Assessment Period: Students Explore with Mentors



Student Presentations

Results from the assessment are presented to the other participants.

This is a CLOSED event; only participants who have agreed to the non-disclosure agreement can attend.

Student reports are not archived or available to be released.

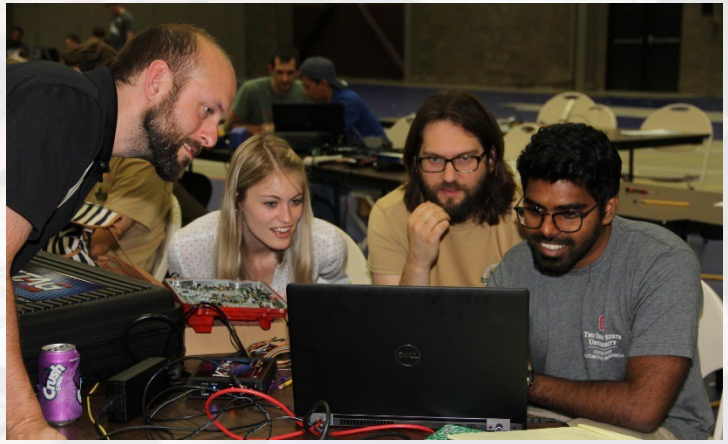
Results from the assessment are communicated to the equipment engineers

Industry Perspective of the CyberTruck Challenge

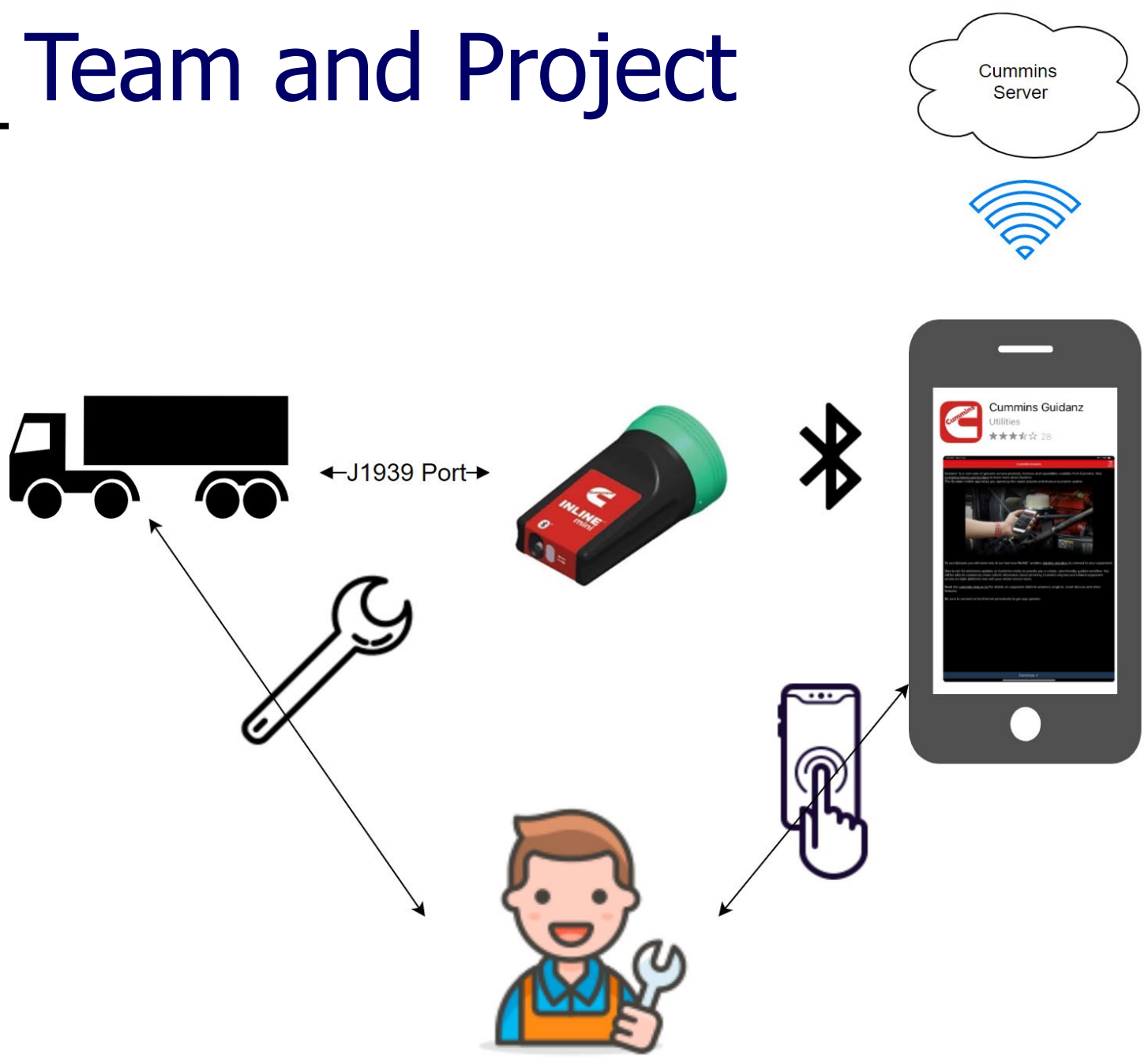
CyberTruck Challenge Experience

Students learned

Students had fun

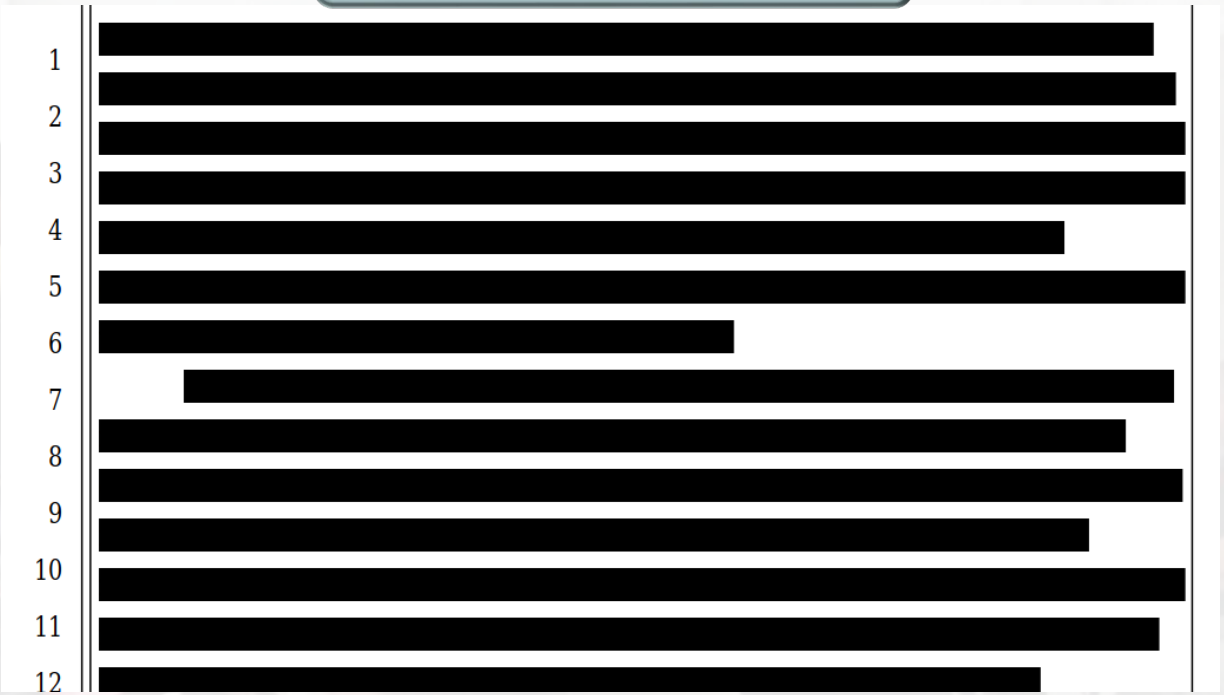


Typical Student Team and Project



CyberTruck Challenge, How was it?

Action items, redacted



Students learned…
Students had fun …
Industry left with action items

Why Participate?

- Workforce Development
- Demonstrate high-tech nature of commercial vehicles
- Attract top students to the industry
- Improve Current Workforce
- Continuous Product Improvement

Industry Perspective

What to bring?

Truck, trailer

Electronic systems

Bench setups

Diagnostic tools

Telematics

Who to bring?

People who can mentor

People who need to learn

Throughout Organization

Network

Industry peers

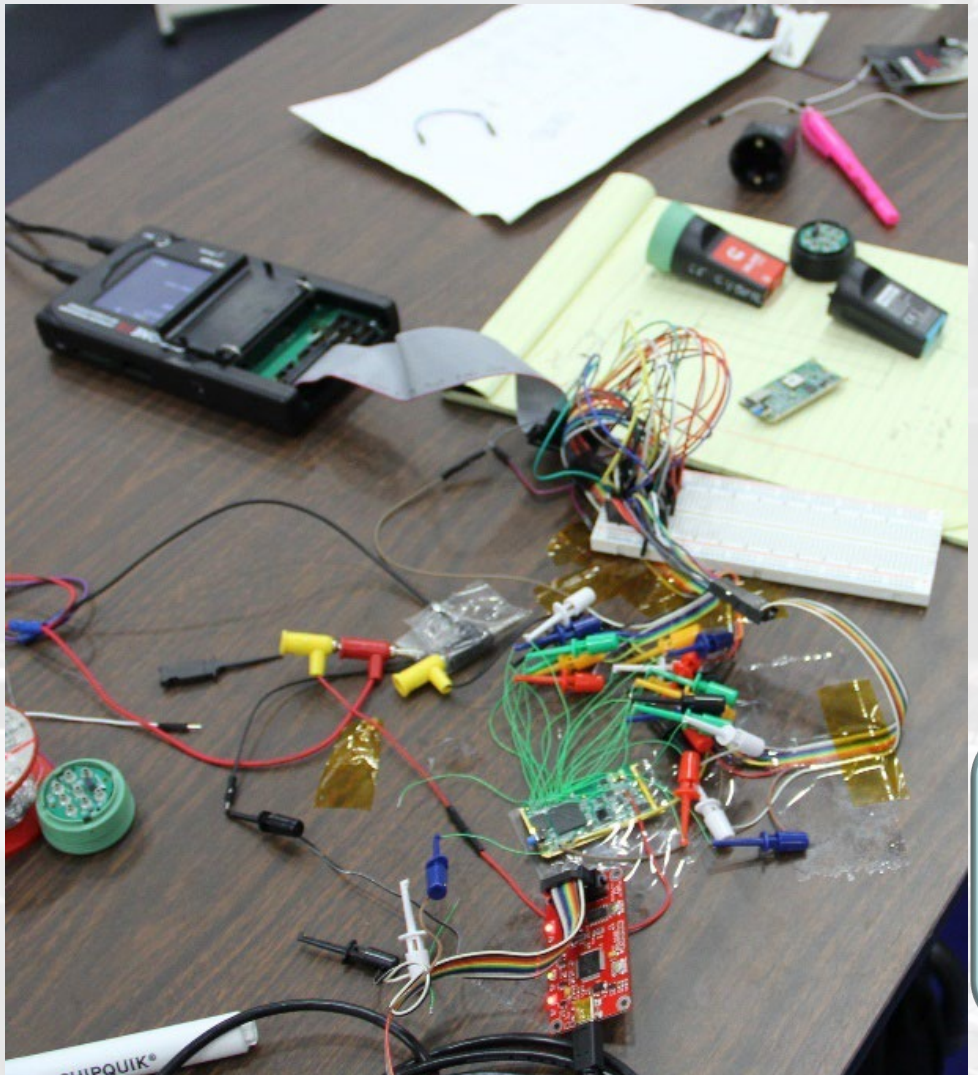
Academics

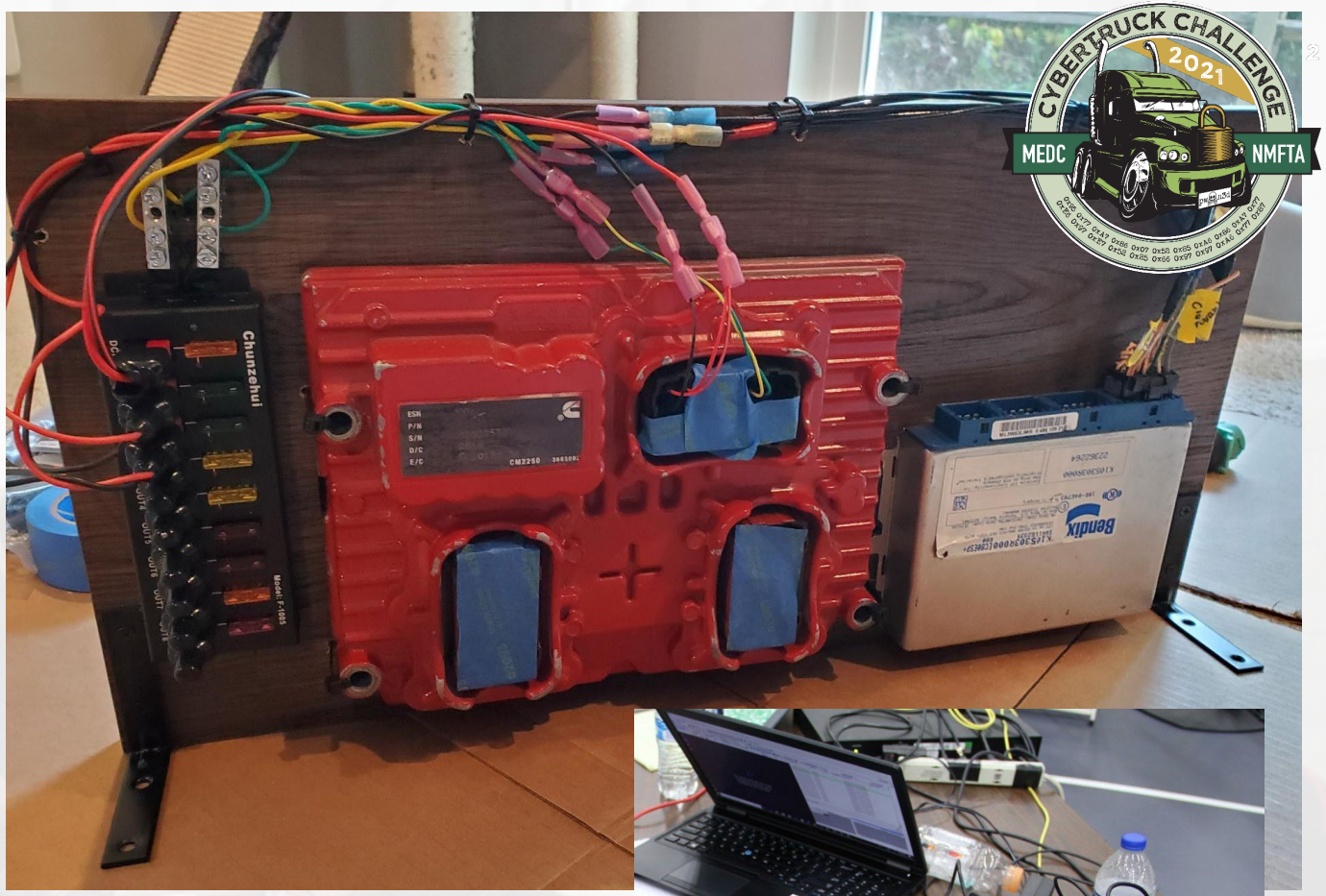
Security researchers

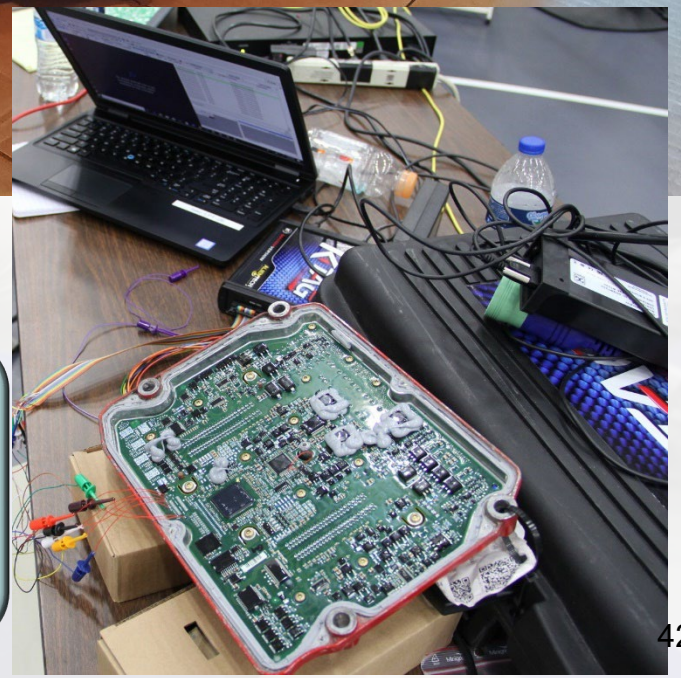
Students

Fleets

Industry products will be there …







… even if they are not.

Save the Date

CyberTruck Challenge 2023
June 12 – 16, 2023
Macomb Community College
Warren, Michigan

www.cybertruckchallenge.org

Additional CyberX Events

- Cyberboat Challenge 2022
  - 1st Time Offering
  - 14 Students from 5 Universities
- CyberAuto 2022
  - 32 of students from US, UK, and Germany
  - Sponsored by Ford, GM, and Toyota
- CyberTractor 2022
  - 1st Time Offering
  - Sponsored by John Deere

https://www.deere.com/en/stories/featured/seeking-the-next-generation-of-cyber-security-talent/

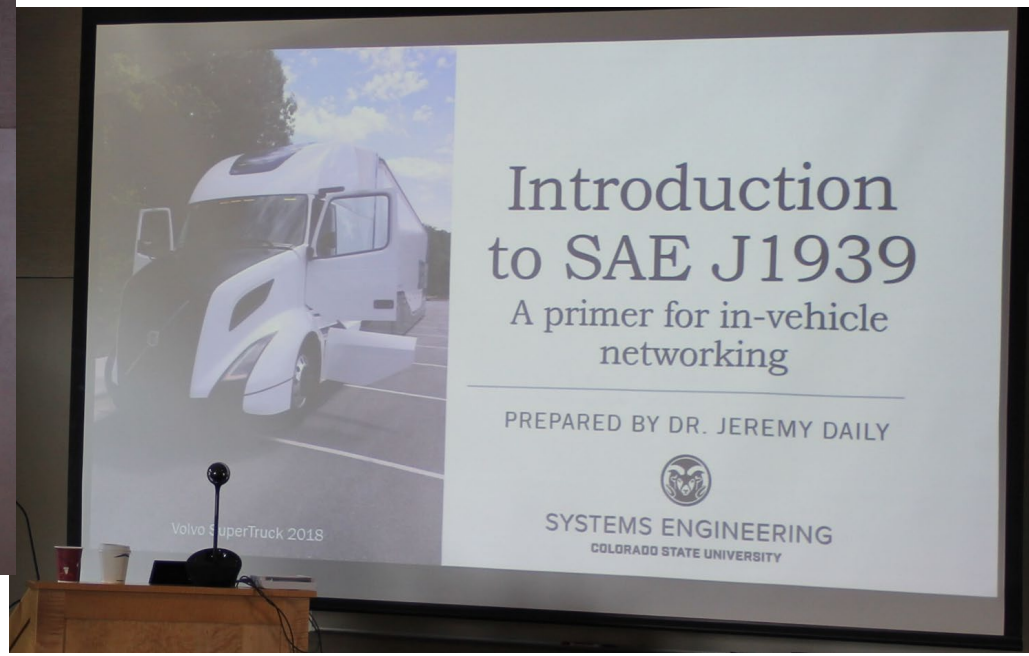
CyberBoat Challenge Recap from 2022

Snow in Colorado, May 21, 2022, starting trip to Michigan.

CyberBoat Challenge Venue

Great Lakes Research Center, Michigan Technological University, Houghton, MI

CyberBoat Challenge, Lessons



CyberBoat Challenge 2022 Schedule

Version:20220513

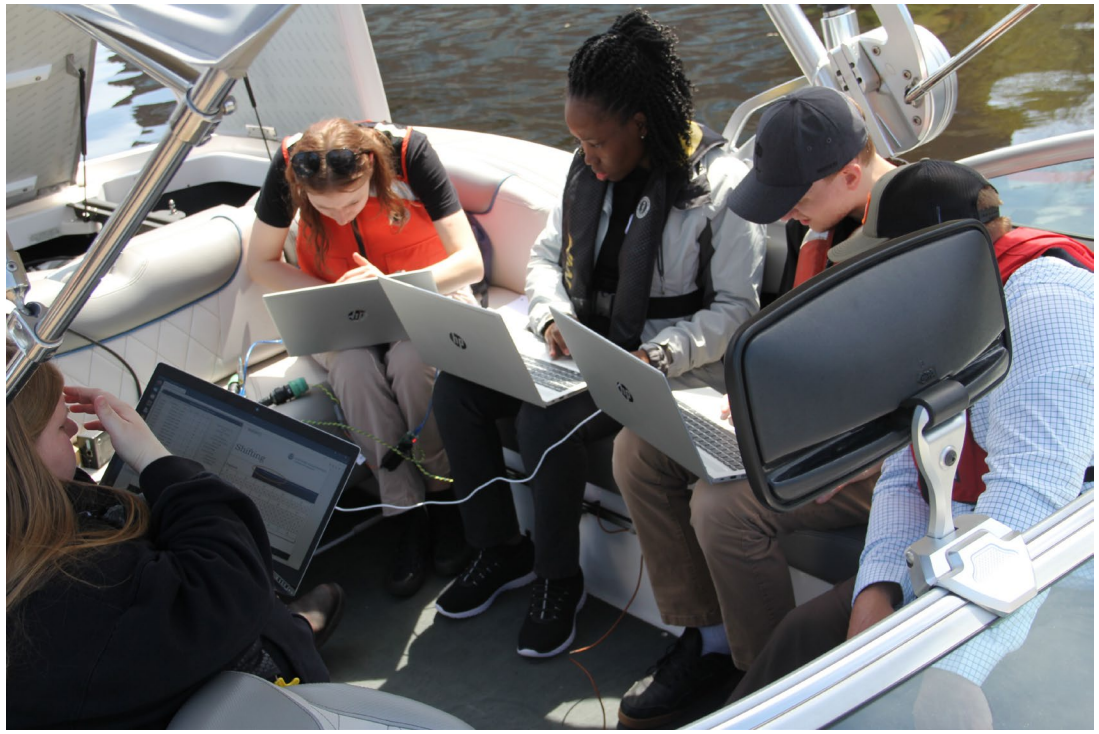
	Sunday 22May2022	Monday 23May2022	Tuesday 24May2022	Wednesday 25May2022	Time
Before 0700	Site Closed	Site Closed			Before 0700
0700-0730		Breakfast (Dorm Cafeteria)			0700-0730
0730-0800					0730-0800
0800-0830		Maritime ICS Protocol Exploitation (Fathom5)	Software RE (GRIMM)	**Assessment**	0800-0830
0830-0900					0830-0900
0900-0930					0900-0930
0930-1000					0930-1000
1000-1030		RF Protocol Exploitation (Libertas & Fathom5)			1000-1030
1030-1100					1030-1100
1100-1130			Intro to J1939 (Daily)		1100-1130
1130-1200					1130-1200
1200-1230		Lunch (GLRC 201)			1200-1230
1230-1300					1230-1300
1300-1330		RF Protocol Exploitation (Libertas & Fathom5)	M-Tech staff time	**REPORTS**	1300-1330
1330-1400			Water Safety (USCG)		1330-1400
1400-1430		Maritime Sensor Exploitation (Fathom5)	Maritime J1939 Demo (Daily)*		1400-1430
1430-1500				Release	1430-1500
1500-1530				Site Closed	1500-1530
1530-1600			How to Conduct an Assessment* (AIS)		1530-1600
1600-1630					1600-1630
1630-1700		Maritime Testbed Assessment & CTF (Fathom5)			1630-1700
1700-1730			Assessment Preperation and Planning		1700-1730
1730-1800					1730-1800
1800-1830	Informal Welcome Reception (Bonfire Grill)	Dinner (Bonfire Grill)	Dinner (GLRC 201)		1800-1830
1830-1900					1830-1900
1900-1930					1900-1930
1930-2000					1930-2000
2000-2030					2000-2030
2030-2100					2030-2100
After 2100	Site Closed				After 2100

CyberBoat Challenge, Indoor

Smart Beacon

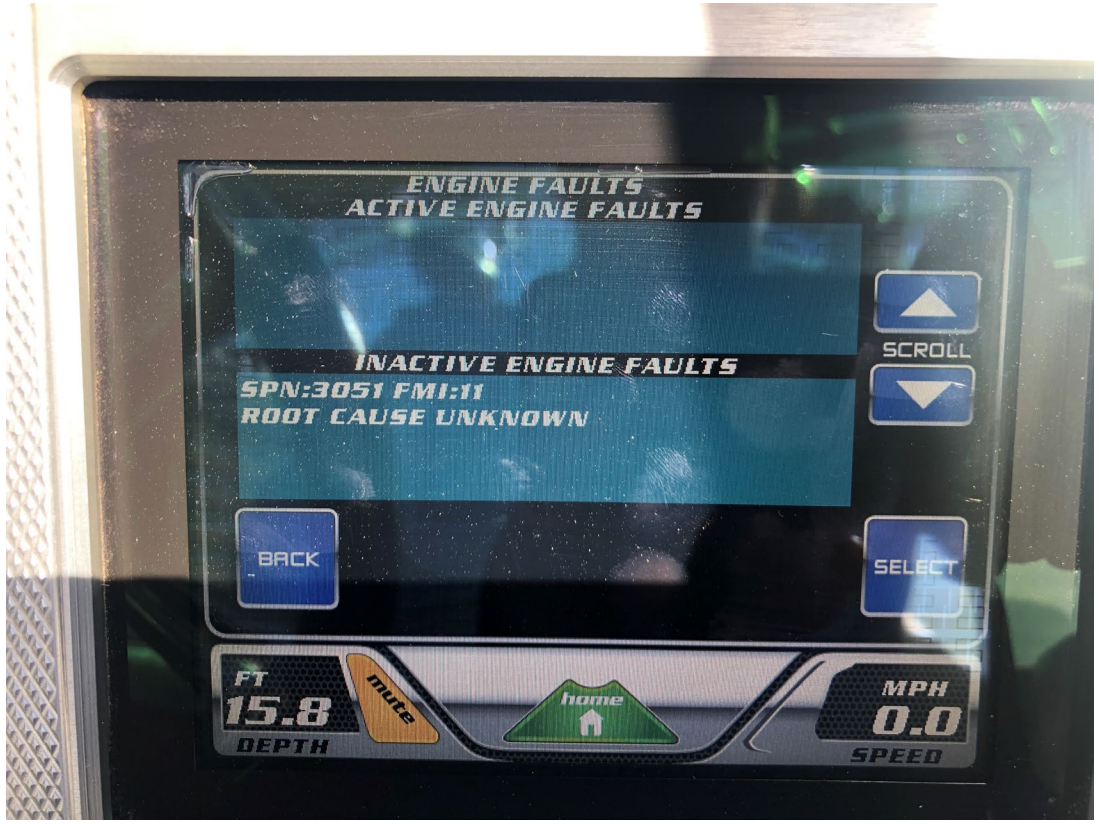
“Grace” training aid

CyberBoat Challenge, Outdoor



Students connecting to the ski boat J1939 network.

CyberBoat Challenge, Testing



On water testing produced fault codes…

CyberBoat Challenge, Presentations

Students show off their learning from the week.

Takeaways and Systems Engineering Considerations

- Traditional IT security doesn't keep up with the demand for cyber-physical system security talent
- Strong need for cybersecurity engineering talent
  - Formal degree programs insufficient
- Need a model to train and excite a cyber-physical systems workforce
  - Requires community sponsorship and mentorship
  - Each cyber event needs a champion
- What future cyber challenges are of interest?
  - CyberDrone, CyberRail, CyberGrid, CyberSat, CyberGrid?

THANK YOU!

Contacts:
Jeremy Daily, jeremy.daily@colostate.edu,
+1 937.238.4907
Karl Heimer, karl.heimer@outlook.com,
+1 248.270.0117

Typical Slide Title (2 Column)

- Level 1 bullet text 1
  - Level 2 bullet 1
    - Level 3 bullet 1
    - Level 3 bullet 2
  - Level bullet 2
- Bullet text 2
- Bullet text 3

- Level 1 bullet text 1
  - Level 2 bullet 1
    - Level 3 bullet 1
    - Level 3 bullet 2
  - Level bullet 2
- Bullet text 2
- Bullet text 3