INSTITUTE FOR DEFENSE ANALYSES

DATAWorks 2021: Operational Cybersecurity Test and Evaluation of Non-IP and Wireless Networks

Peter M. Mancini, Project Leader

Vincent C. Bass
Mark R. Herrera

April 2021

Approved for Public Release.
Distribution Unlimited.

IDA Document NS D-21552

Log: H 2021-000036

INSTITUTE FOR DEFENSE ANALYSES
4850 Mark Center Drive
Alexandria, Virginia 22311-1882

About This Publication
This work was conducted by the Institute for Defense Analyses (IDA) under contract HQ0034-19-D-0001, Task C9096, “Cyber Experimentation and Training Lab,” for the Office of the Director, Operational Test and Evaluation. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Acknowledgments
The IDA Technical Review Committee was chaired by Mr. Robert R. Soule and consisted of Dr. Shawn C. Whetstone, Dr. Tye W. Botting, Dr. Shelby Highsmith, Dr. Steven M. Movit, and Dr. William J. Robbins from the Operational Evaluation Division.

For more information:
Peter M. Mancini, Project Leader
pmancini@ida.org • (703) 845-2496

Robert R. Soule, Director, Operational Evaluation Division
rsoule@ida.org • (703) 845-2482

INSTITUTE FOR DEFENSE ANALYSES

IDA Document NS D-21552

DATAWorks 2021: Operational Cybersecurity Test and Evaluation of Non-IP and Wireless Networks

Peter M. Mancini, Project Leader

Vincent C. Bass
Mark R. Herrera

Executive Summary

Nearly all land, air, and sea maneuver systems (e.g., vehicles, ships, aircraft, and missiles) are becoming more software-reliant and blending internal communication across both Internet Protocol (IP) and non-IP buses. IP communication is widely understood among the cybersecurity community, whereas expertise and available test tools for non-IP protocols such as Controller Area Network (CAN) and MIL-STD-1553 are not as commonplace. Although each protocol has unique qualities in how it communicates, the fundamental format and basic principles of each protocol remains the same regardless of implementation.

This presentation emphasizes the need to test non-IP communication in operational testing. It introduces a set of non-IP protocols that appear alongside IP in aircraft, ships, and land vehicles within private industry and the Department of Defense. We provide a brief discussion on the physical implementation of a CAN bus as it might appear in a land vehicle. We then execute a fictitious operational test on a land vehicle, during which an adversarial cyber team causes effects on the vehicle's CAN bus. Using results from the fictional operational test, we use measurable effectiveness metrics and observations to determine whether the cyber aggression negatively impacted the mission.

The basic principles and formatting of common communication protocols do not change. Therefore, we, as a test community, must challenge ourselves to build within our organizations a fundamental understanding of each of these protocols (including Transmission Control Protocol/IP, or TCP/IP). Doing so will allow us to plan and conduct better operational tests and communicate more accurately in our writing and presentations.

IDA

Operational Cybersecurity Test and Evaluation of Non-IP and Wireless Networks

DATAWorks 2021

Vincent Bass

Mark Herrera

Peter Mancini (Project Leader)

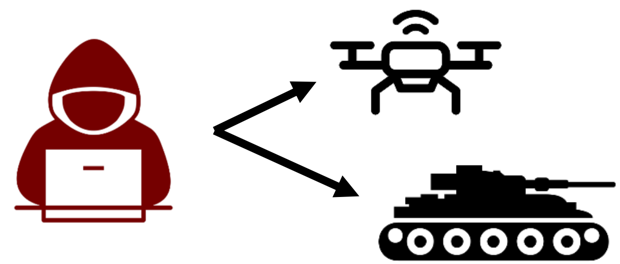
Institute for Defense Analyses

4850 Mark Center Drive ● Alexandria, Virginia 22311-1882

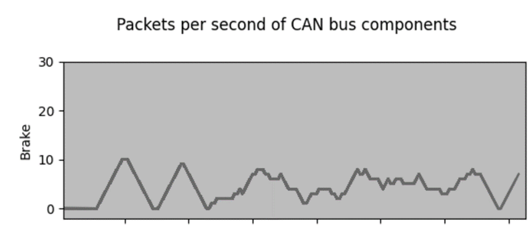
Roadmap for today's presentation

Introduction to non-standard communication protocols

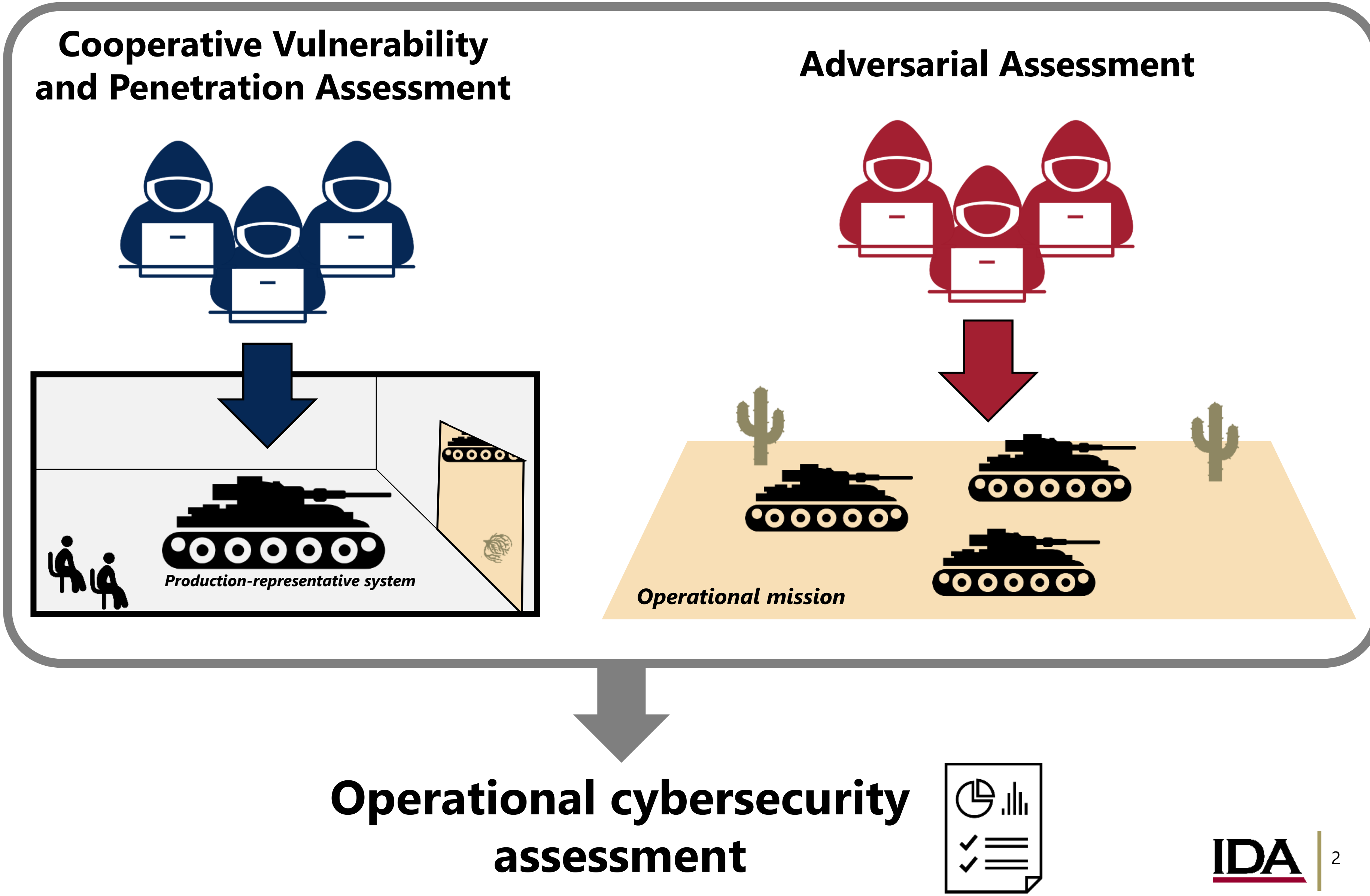
Cyber attack demonstrations



Capturing cyber effects and measuring mission effects



Operational cyber testing supports cybersecurity evaluation



Many DoD systems contain Internet Protocol (IP) and non-IP networks

Subsystems using non-IP communication methods include:

- Automotive controls
- Weapons system (e.g. firing, targeting)
- Radio communication
- Satellite communication
- Hull, Mechanical, and Electrical (HM&E)
- Supervisory Control and Data Acquisition (SCADA)
- Industrial Control Systems (ICS)

DOT&E guidance and memorandum have identified gaps in assessing cybersecurity of non-IP interfaces

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

2016

OPERATIONAL TEST AND EVALUATION

JUL 27 2016

SUBJECT: Cybersecurity Operational Test and Evaluation Priorities and Improvements

OTAs "should collaborate to develop methods to assess the cybersecurity of common **non Internet Protocol data transmission systems**."

OTAs "must develop the means to conduct cyber attacks on systems using wireless, **Bluetooth**, **radar**, and other **radio frequency** means as well as via sonar systems."

"At present, **the ability to test** against these threat vectors **is rudimentary**."

OFFICE OF THE SECRETARY OF DEFENSE
1700 DEFENSE PENTAGON
WASHINGTON, DC 20301-1700

2018

OPERATIONAL TEST AND EVALUATION

APR 03 2018

SUBJECT: Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs

OTAs "should identify components such as cross-domain solutions, **industrial controls**, **non-internet data transfers**, and data transfers via alternate media such as **radio frequency** and **data links**."

FY20 INTRODUCTION

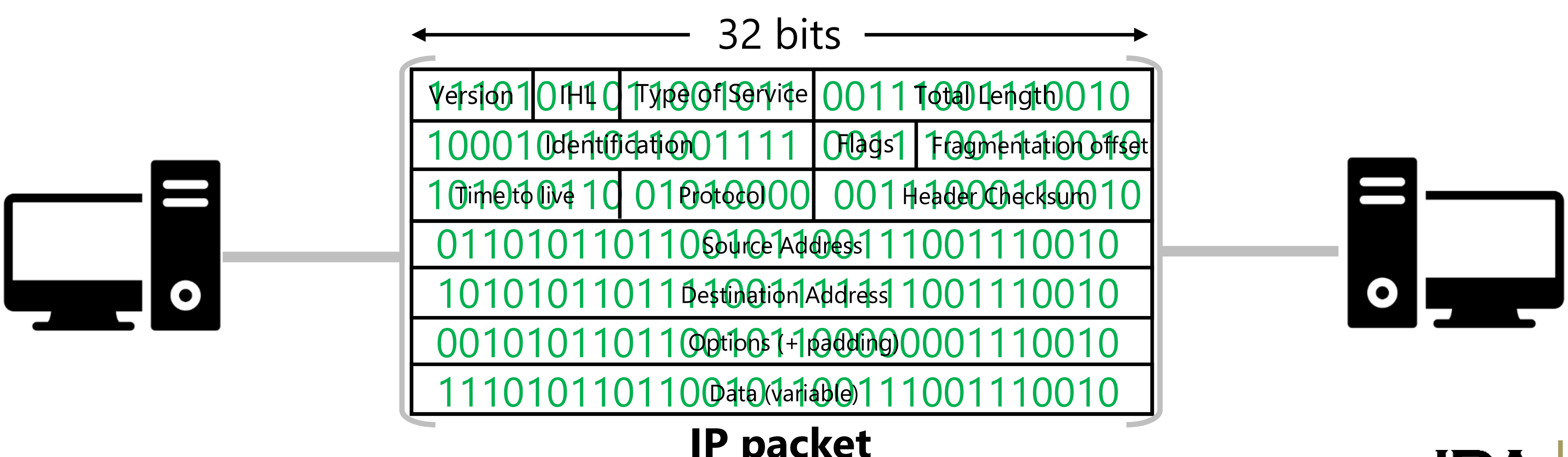
FY 2020
Annual Report

"**Tools and techniques** necessary to test specialized protocols, such as those in industrial control systems, tactical data links, and aircraft transponders, **are not adequate**."

TCP/IP is widely understood and can communicate over wired or wireless connections

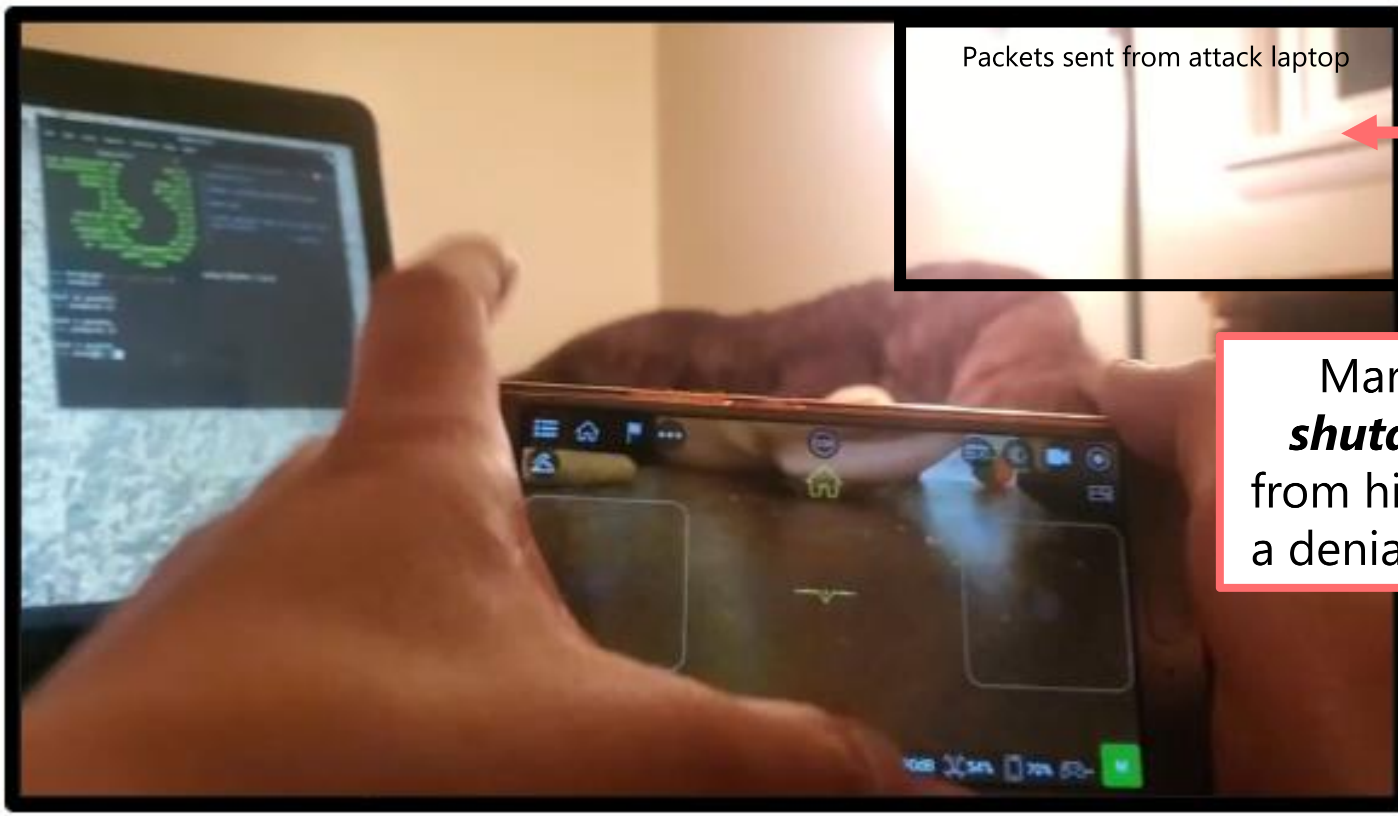
TCP/IP should be familiar to *everyone* learning any form of computer science

Wired and wireless TCP/IP traffic uses the same fixed format for packet structure



Cyber attacks can occur over wired or wireless TCP/IP connections

<u>Attack methodology:</u>
1. Crack weak password hash to access the wireless network
2. Spoof (impersonate) commands from attack laptop using the phone's network address and port



Mark replayed the ***shutdown*** command from his laptop to create a denial of service attack

Non-IP protocols also have standardized formats

ARINC 429

ARINC 429 data words are 32-bit words made up of five primary fields:

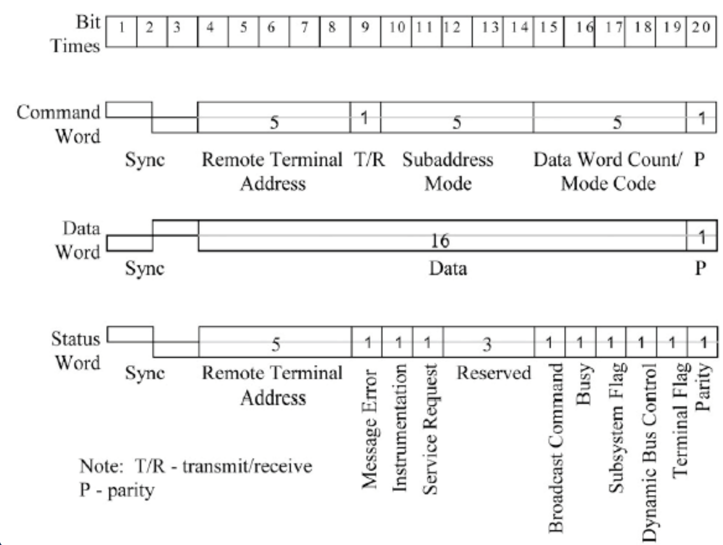
- Parity – 1-bit
- Sign/Status Matrix (SSM) – 2-bits
- Data – 19-bits
- Source/Destination Identifier (SDI) – 2-bits
- Label – 8-bits

MSB **LSB**

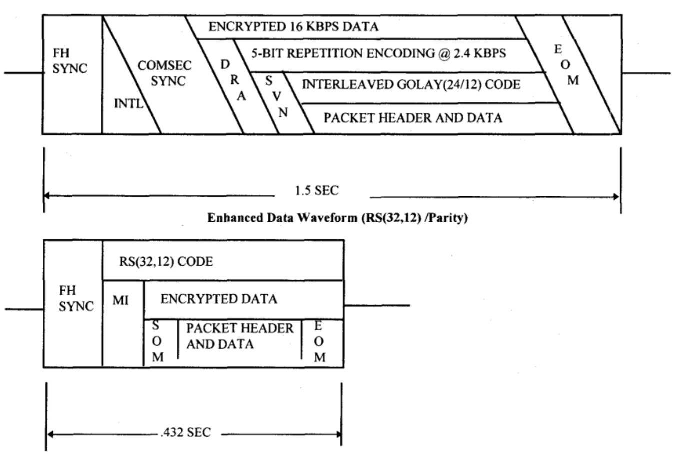
32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
P	**SSM**		**MSB**						**Data**												**LSB**	**SDI**		**Label**							

ARINC 429 32-bit Word Format

MIL-STD-1553



SINCGARS Data Waveform

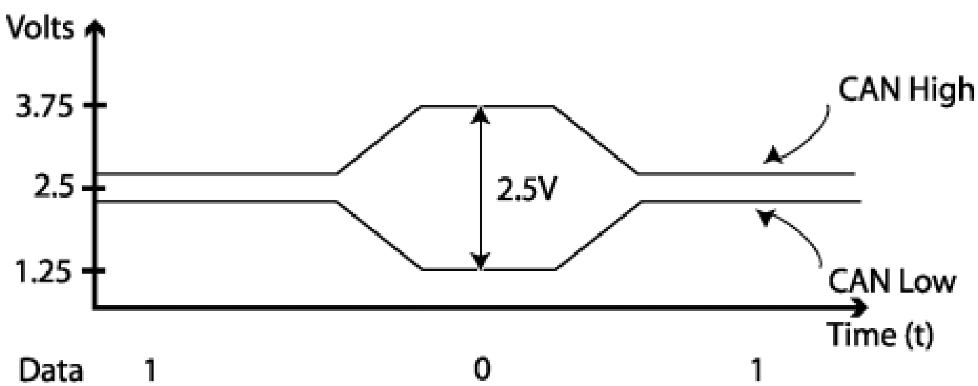


Controller Area Network (CAN)

Analyzing raw packets allows evaluator to visualize bus activity

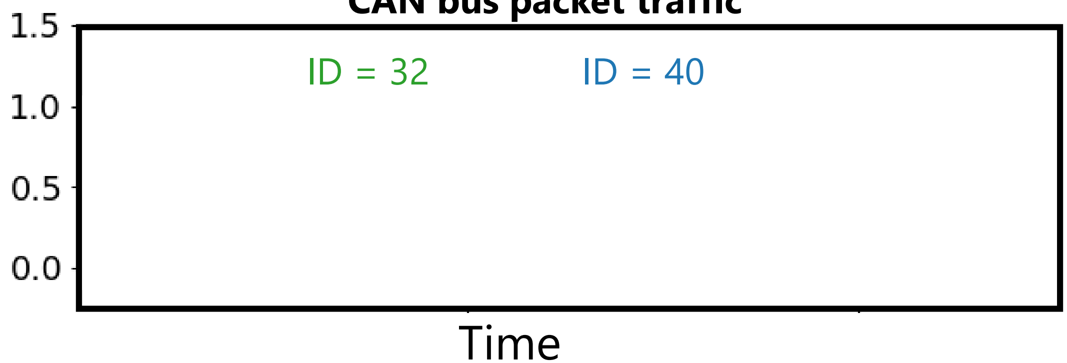
Controller Area Network (CAN)

How CAN bus modules communicates



- When the line is idle, both wires carry 2.5V.
- When data is being transmitted, lines reach voltage differential of 2.5V.

CAN bus packet traffic

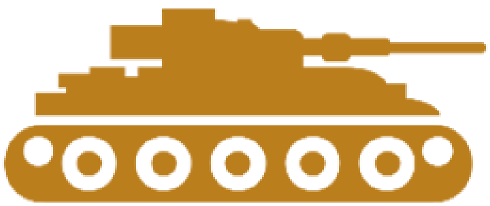


CAN bus attack demonstration

Demo: Armored vehicle will undergo operational cyber testing

Network design

- **IP network** for in-vehicle electronics
- **Controller Area Network** bus for automotive control
- **MIL-STD-1553** network for target acquisition and weapon firing



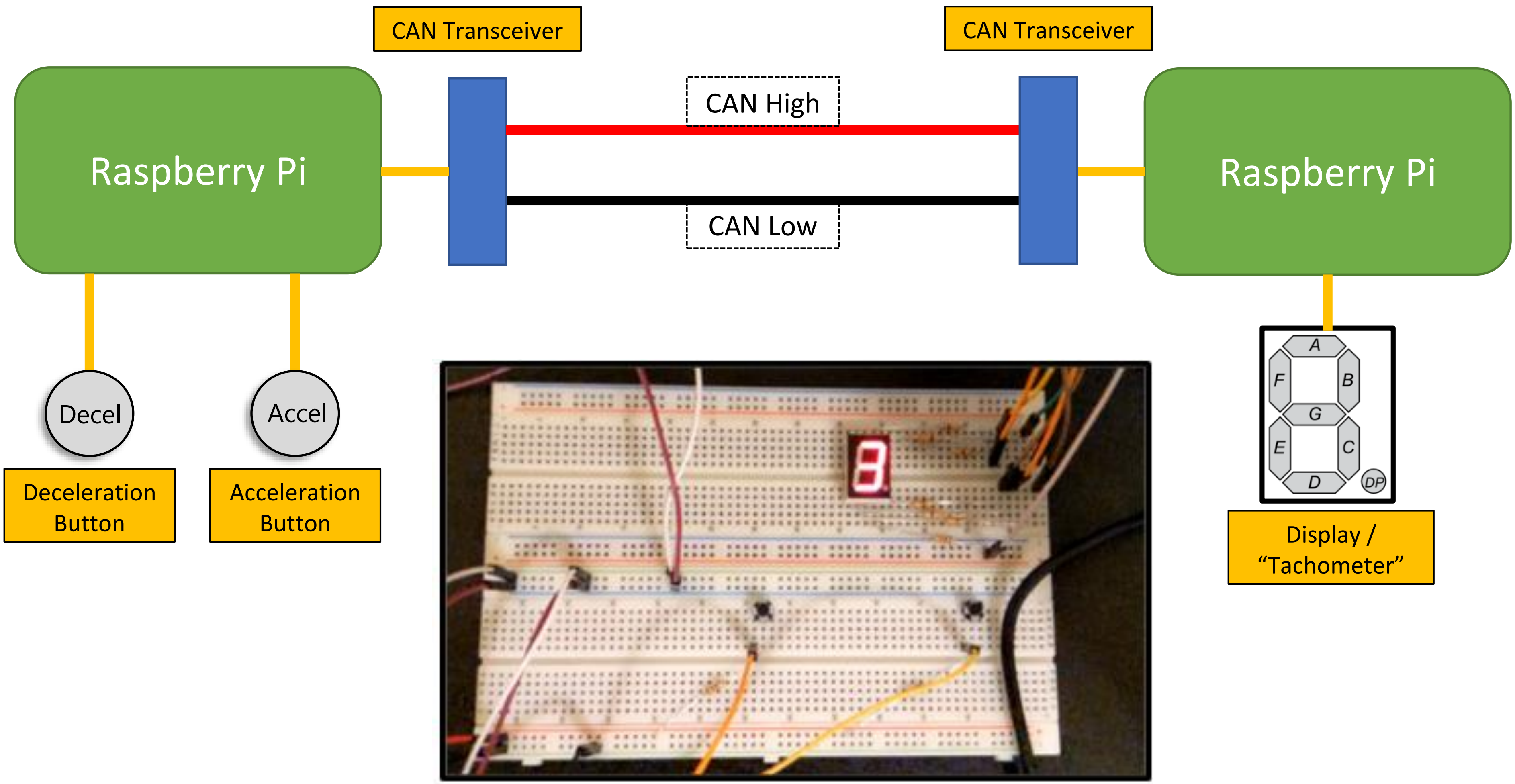
List of mission essential functions

Move	Shoot
Navigate	Communicate
Acquire targets	Protect

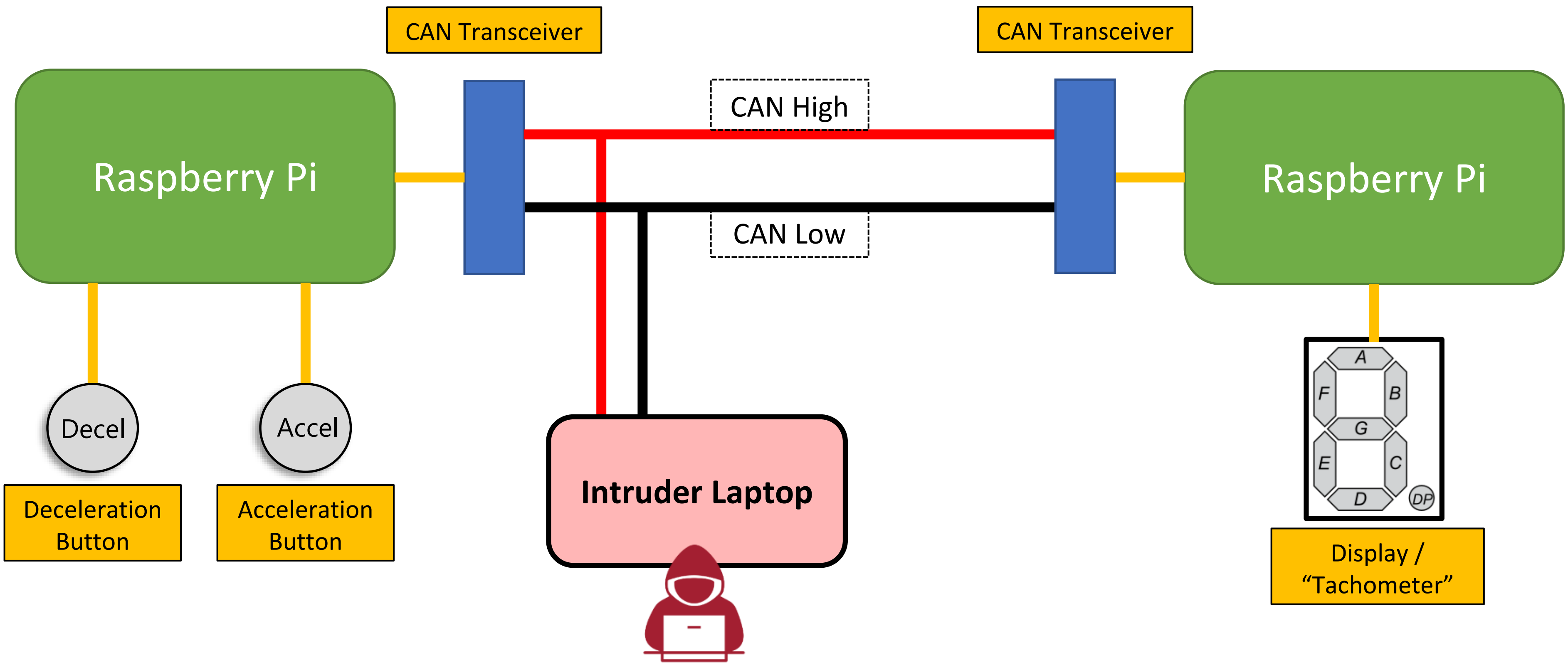
Measures of effectiveness (MOE)

- ❑ Time to reach destination
- ❑ Time to acquire target
- ❑ Ballistic accuracy
- ❑ Securely communicate with other vehicles

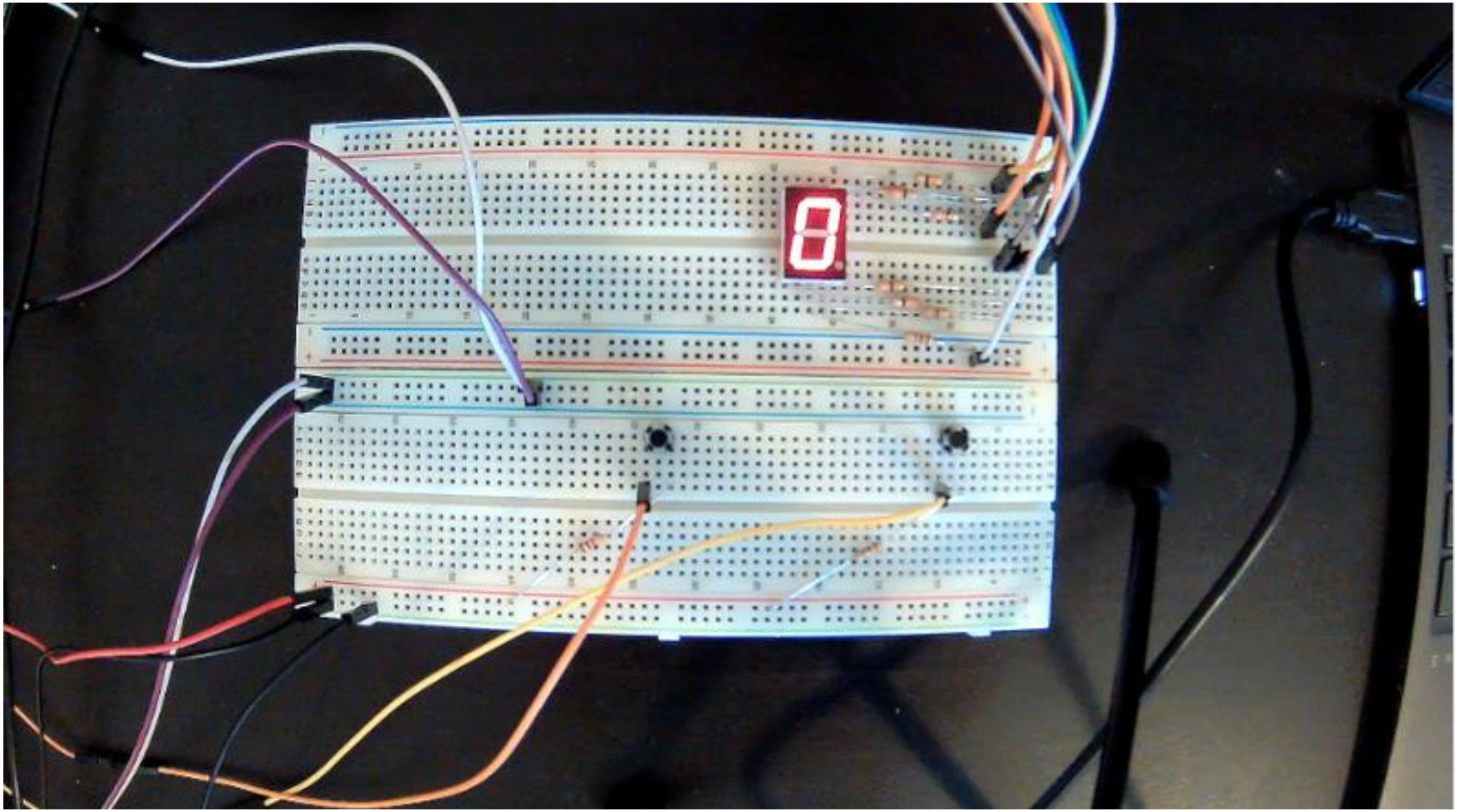
Vehicle acceleration and deceleration are directly controlled via CAN Bus



Vehicle acceleration and deceleration are directly controlled via CAN Bus

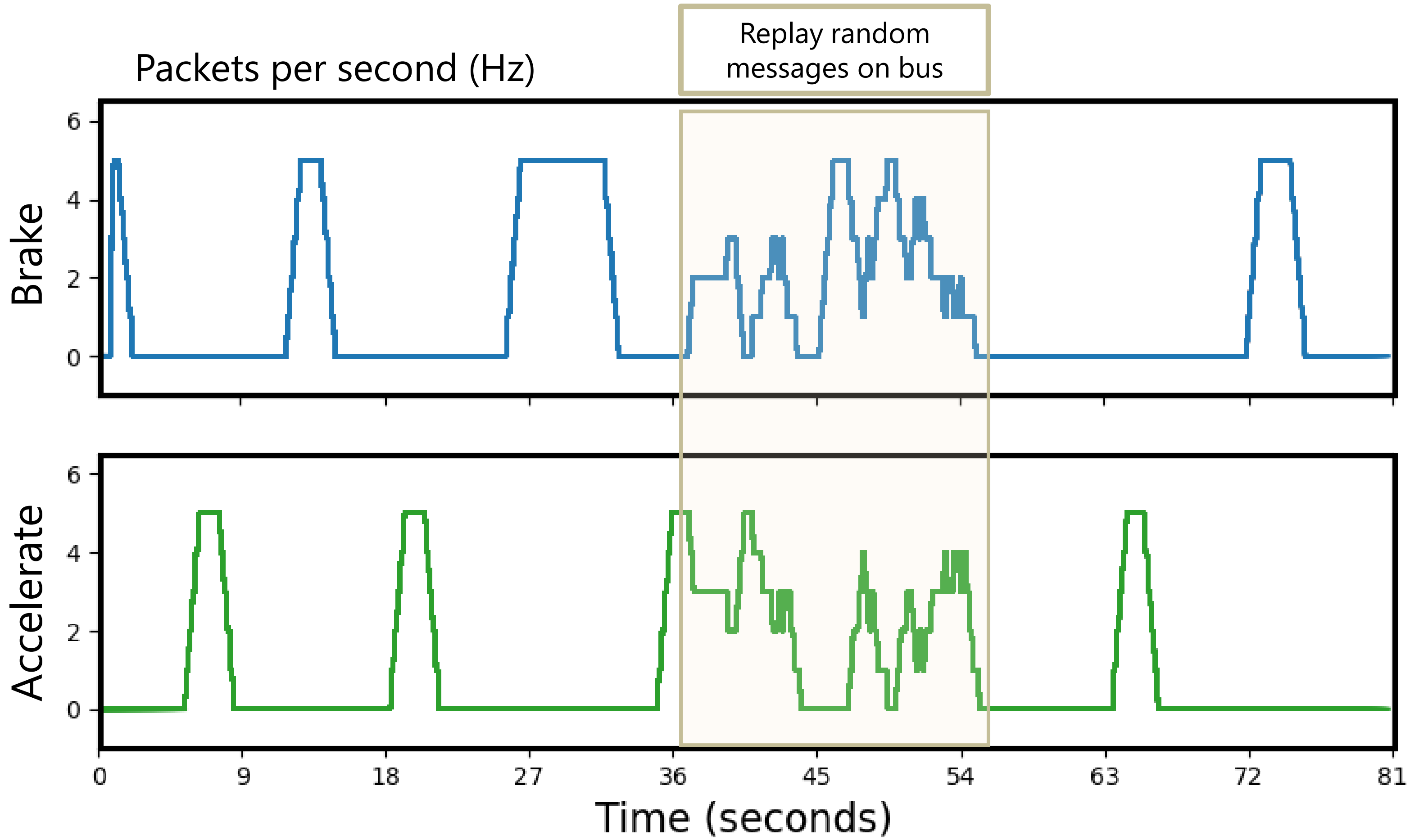


Vehicle acceleration and deceleration are directly controlled via CAN Bus



Capturing CAN traffic allows for data visualization of the cyber attack

Attack #1: Manipulate accelerator input



CAN Demo – Cyber effects leading to mission effects

Cyber Effect	Measure of Effectiveness		Mission Effect
	TTRD (<20 min)	TTAT (<5 min)	
Manipulate accelerator input (integrity attack)	27 minutes	4 minutes	Attack caused the crew to lose trust in the system. Unit reduced vehicle speed and refused to fire weapon due to distrust in system performance.
	15 minutes	3 minutes	Crew pressed onward through the attack, despite degraded movement capabilities, and completed the mission.
	12 minutes	3 minutes	Crew found the malicious device connected in-line to the CAN bus inside the vehicle. Soldiers disconnect the device and recovered full system capabilities.

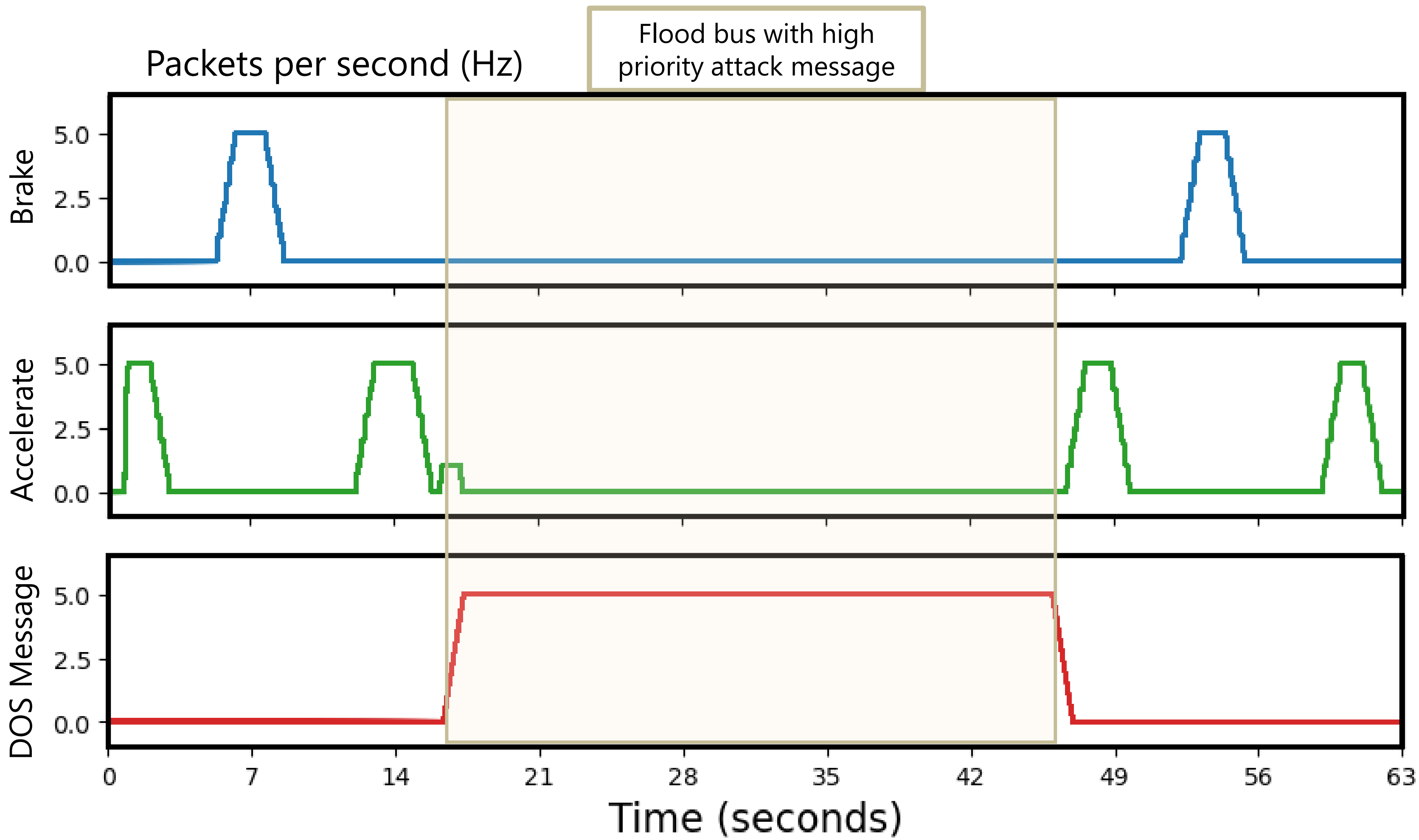
TTRD = Time to reach destination
TTAT = Time to acquire target

Mission failed Mission complete

All effectiveness data, thresholds, and mission effects are fictional.

Capturing CAN traffic allows for data visualization of the cyber attack

Attack #2: Disable all bus components



CAN Demo – Cyber effects leading to mission effects

Cyber Effect	Measure of Effectiveness		Mission Effect
	TTRD (<20 min)	TTAT (<5 min)	
Manipulate accelerator input (integrity attack)	27 minutes	4 minutes	Attack caused the crew to lose trust in the system. Unit reduced vehicle speed and refused to fire weapon due to distrust in system performance.
	15 minutes	3 minutes	Crew pressed onward through the attack, despite degraded movement capabilities, and completed the mission.
	12 minutes	3 minutes	Crew found the malicious device connected in-line to the CAN bus inside the vehicle. Soldiers disconnect the device and recovered full system capabilities.
Disable brakes (availability attack)	Did not complete	Did not complete	Attack prevented the unit from reaching target destination and acquiring target, thus, the unit could not complete their mission.

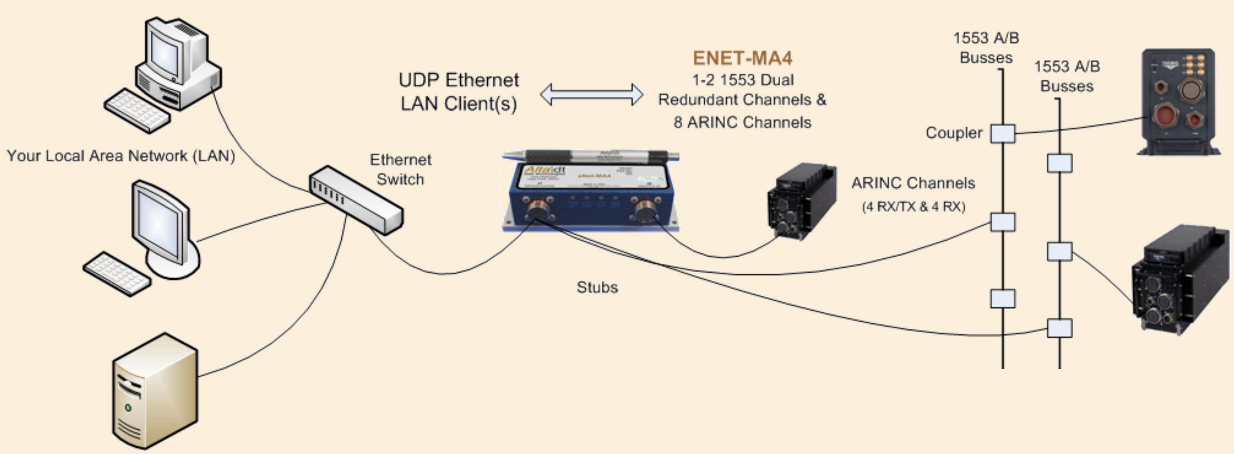
Mission failed   Mission complete

TTRD = Time to reach destination
TTAT = Time to acquire target

All effectiveness data, thresholds, and mission effects are fictional.

Commercial tools exist to provide non-IP traffic monitoring and injection capabilities

Alta dt: Real-time Ethernet connectivity to 1553 and ARINC 429 busses



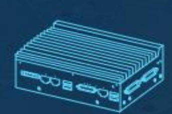
AIM

ARINC 429

MIL-STD-1553A/B databus

ARINC825/CAN bus systems

Shift 5



Shift5 Intake

Shift5 Intake provides full-take embedded data bus capture through continuous collection.

Shift5 Engine

Shift5 Engine is an advanced algorithm and rules engine that uses behavior heuristics to detect, log, and alert on anomalies.

Shift5 Gauge Cluster

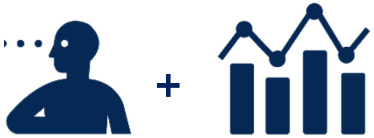
Shift5 Gauge Cluster tracks incident response using advanced analytics to detect intrusions and prevent cyberattacks on OT.

Conclusions

Many systems on DoD oversight use non-IP buses to support mission-critical capabilities

- DOT&E guidance and memoranda emphasize the need to test non-IP buses and have identified gaps in test tools

Well-documented data collection of bus activity allows for quantitative confirmation of observed cyber effects

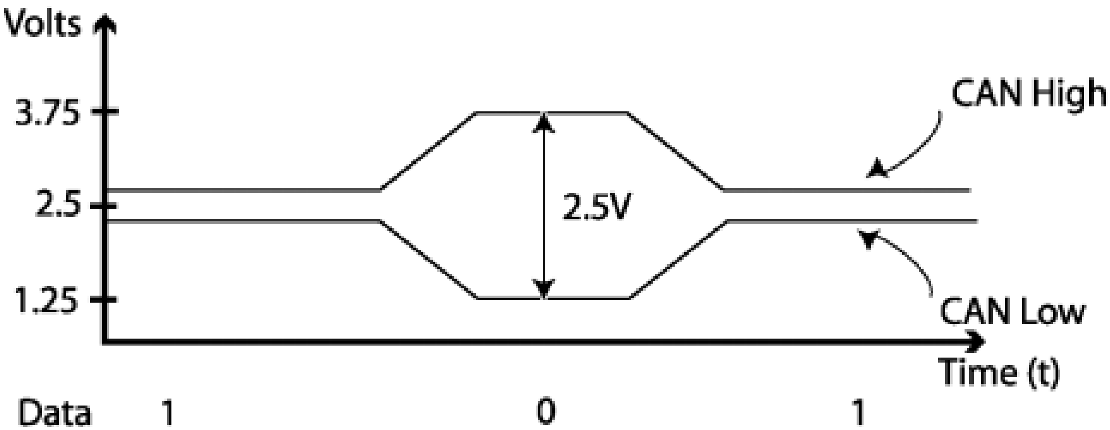


Improving our fundamental understanding of non-standard communication protocols will lead to better operational test planning, data collection, and reporting.

Backup

How do CAN bus modules communicate?

CAN bus uses two dedicated wires for communication. The wires are called CAN high and CAN low. When the CAN bus is in idle mode, both lines carry 2.5V. When data bits are being transmitted, the CAN high line goes to 3.75V and the CAN low drops to 1.25V, thereby generating a **2.5V differential** between the lines. Since communication relies on a voltage differential between the two bus lines, the CAN bus is NOT sensitive to inductive spikes, electrical fields or other noise. This makes CAN bus a reliable choice for networked communications on mobile equipment.



CAN power can be supplied through CAN bus. Or a power supply for the CAN bus modules can be arranged separately. The power supply wiring can be either totally separate from the CAN bus lines (using suitable gauge wiring for each module) resulting in two 2-wire cables being utilized for the network, or it can be integrated into the same cable as the CAN bus lines resulting in a single 4-wire cable. CAN bus cabling is available from multiple vendors.

https://www.axiomatic.com/whatiscan.pdf

Appendix A
Slides with Notes

Slide 1

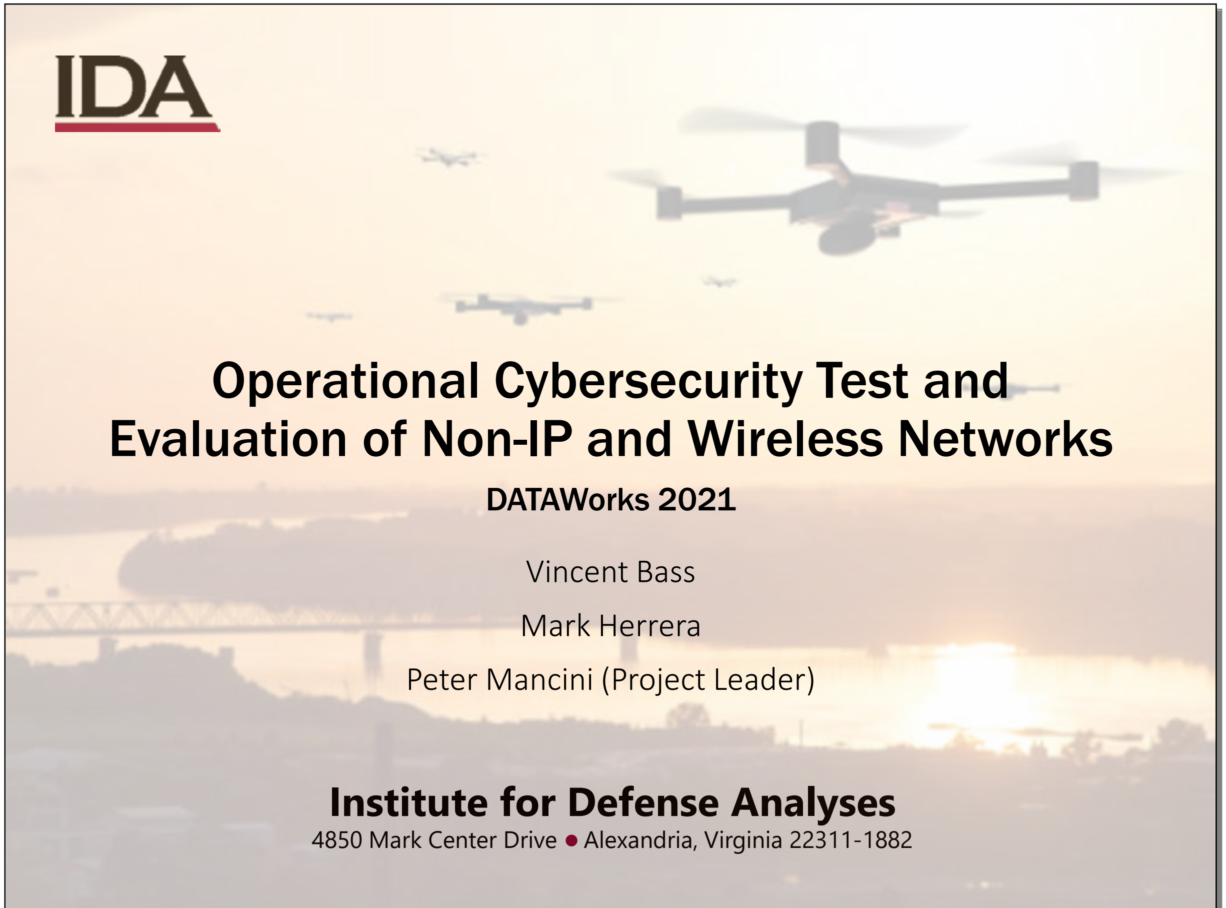
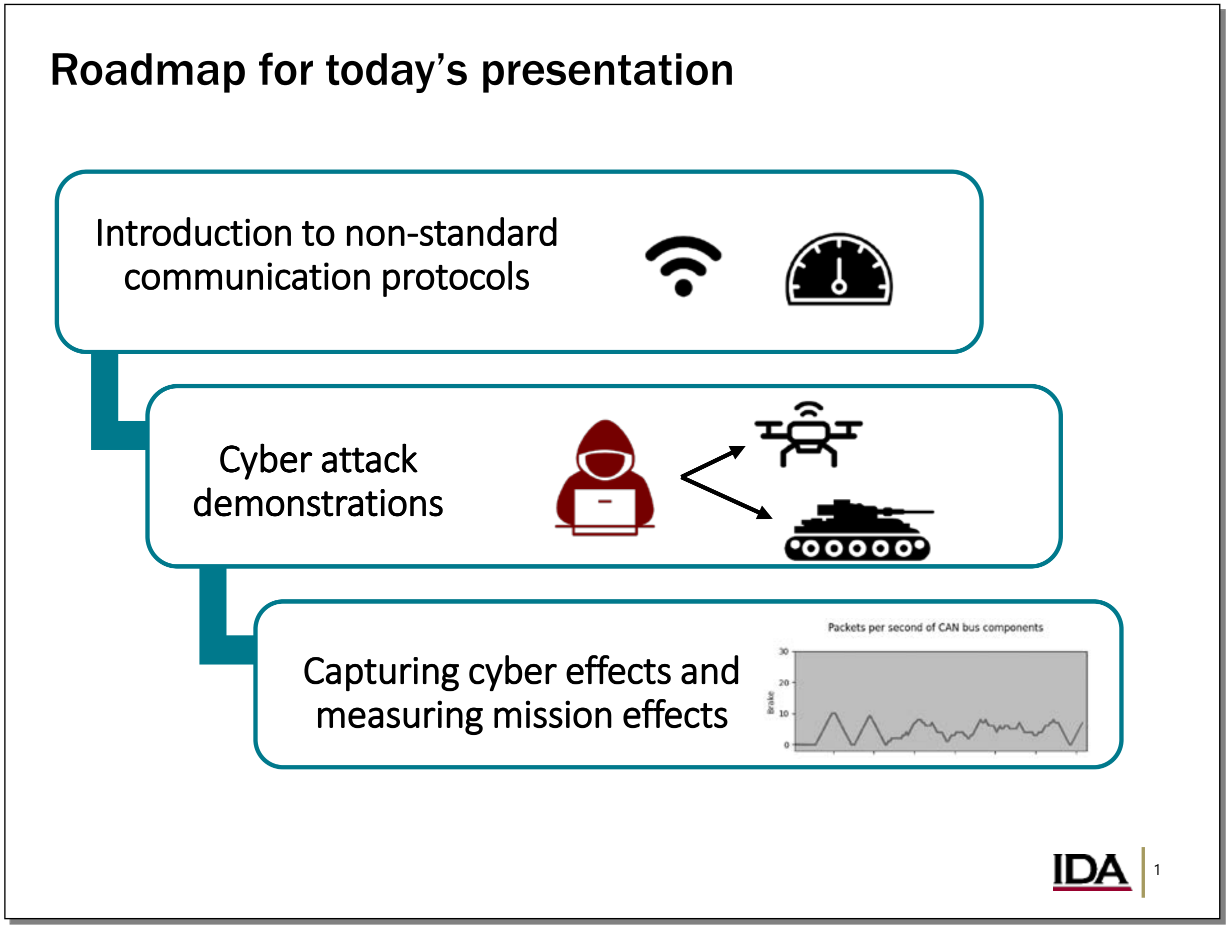


Image from: https://www.istockphoto.com/photo/aerial-photographing-with-drone-gm1026580116-275288768

Slide 2



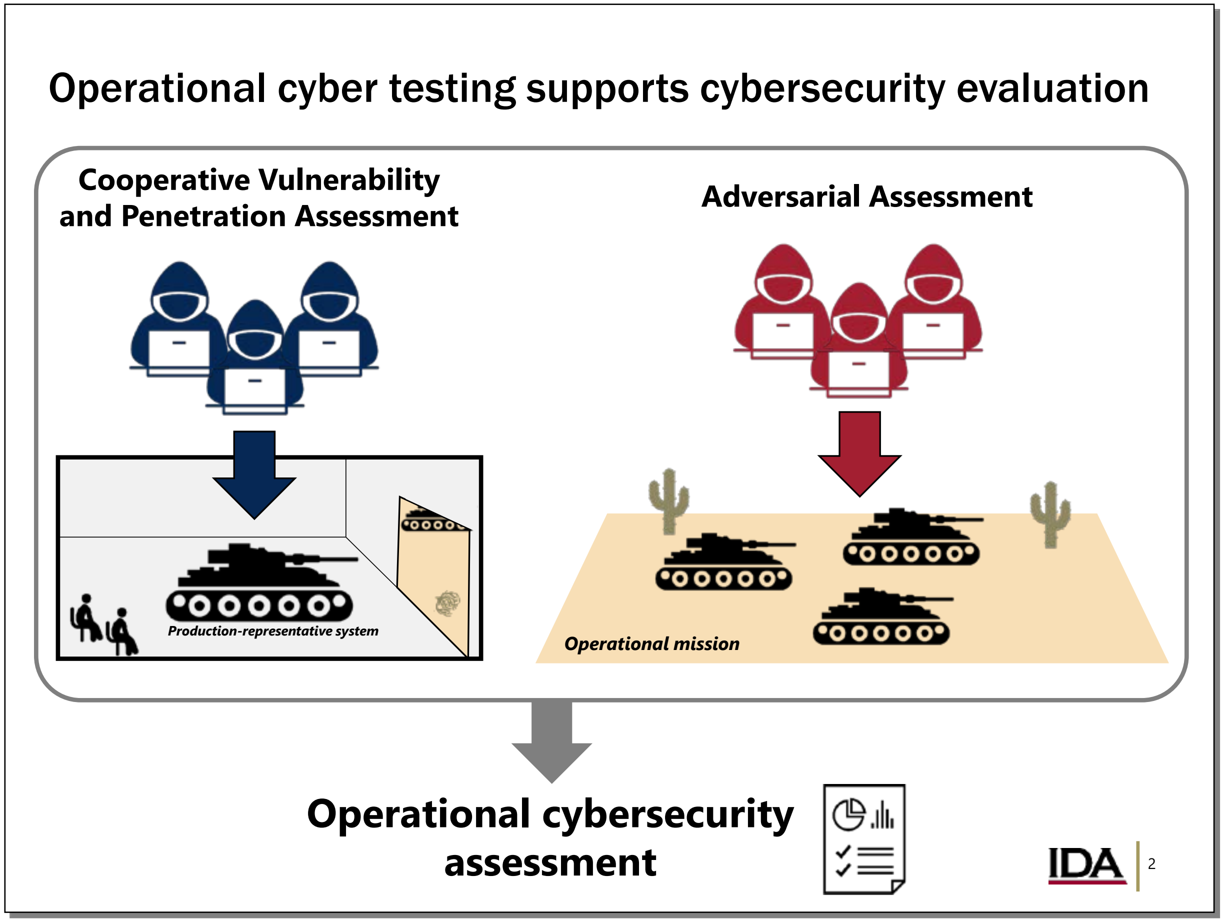
Purpose of operational cybersecurity assessments

Non-standard communication methods: Wi-Fi and non-IP protocols

System capabilities and mission functions typically related to those buses

Cyber effects and Mission effects

Slide 3



The general concept of cyber operational testing (OT) will be described here, but for a more detailed dive into Cyber OT, I recommend you check out our 90-minute presentation from last year's DATAWorks.

DATAWorks 2021 Introduction to Cyber Operational T&E

https://www.youtube.com/watch?v=dmlQCDRMcsk

Taking Down a Turret (dramatization)
https://www.youtube.com/watch?v=kYeMKtbQamw

Additional information regarding the roles of DOT&E and IDA:

DOT&E Responsibilities (https://www.dote.osd.mil/About/Responsibilities/)

Prescribe DoD OT&E and LFT&E policy.
Provide guidance on all OT&E and LFT&E matters.
Monitor & review all OT&E and LFT&E in DoD.
Report annually to Congress on OT&E and LFT&E.
Member of Defense Acquisition Board and Info Tech Acquisition Board.
Approve test plans for OT & LF oversight programs.
Report on programs, before full-rate production decision:

- Adequacy of OT&E & LFT&E.
- Operational effectiveness & operational suitability.
- Survivability and lethality.
- To Secretary, OSD, Services, & four congressional committees.

IDA Responsibilities (https://www.ida.org/ida-ffrdcs/systems-and-analyses-center/oed)

OED researchers apply deep technical, analytical, and subject-matter expertise to support Department of Defense (DoD) operational testing and evaluation

Slide 4

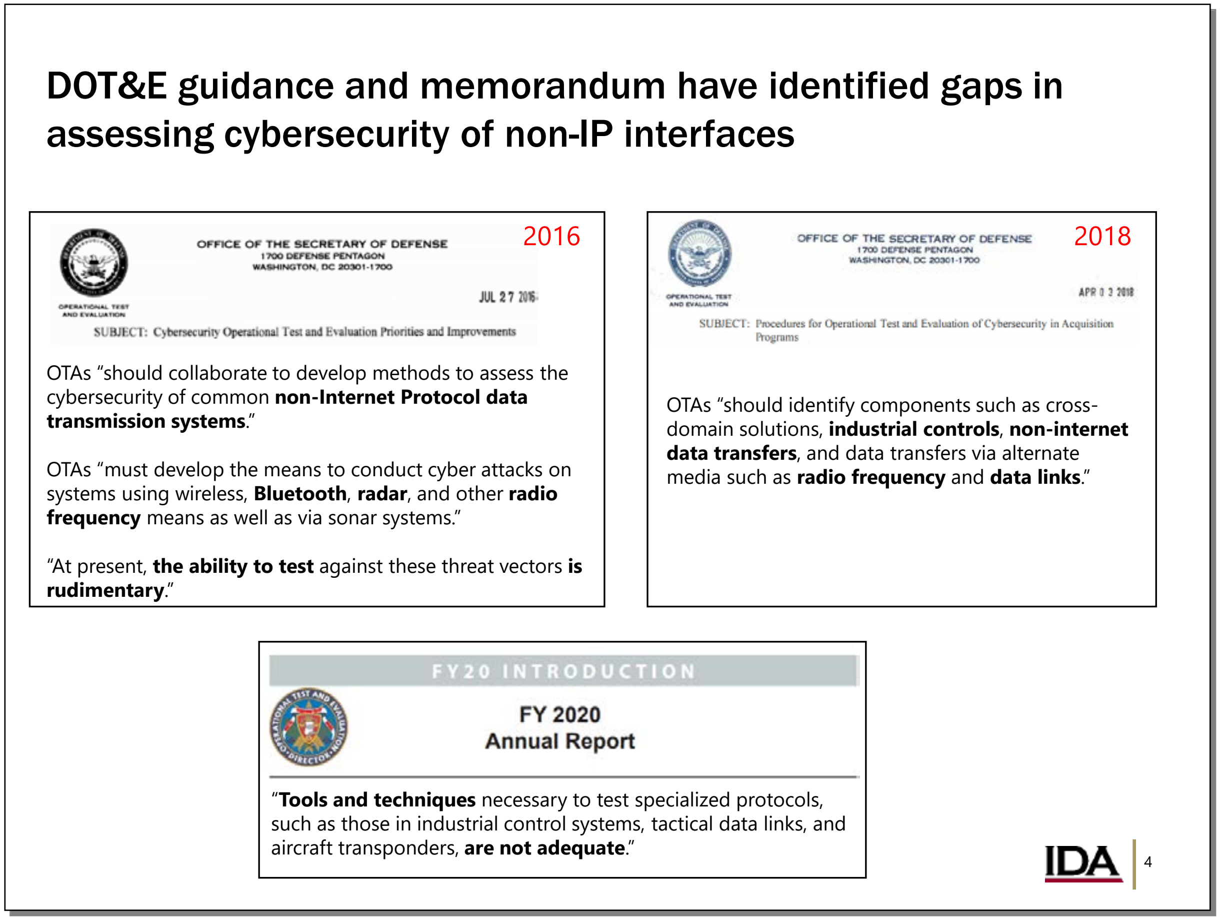
Many DoD systems contain Internet Protocol (IP) and non-IP networks

Subsystems using non-IP communication methods include:

- Automotive controls
- Weapons system (e.g., firing, targeting)
- Radio communication
- Satellite communication
- Hull, Mechanical, and Electrical (HM&E)
- Supervisory Control and Data Acquisition (SCADA)
- Industrial Control Systems (ICS)

IDA | 3

Slide



0: A classified DOT&E memo provides guidance for testing industrial control systems and non-IP protocols. Message me your SIPR address if you would like me to send you a copy.

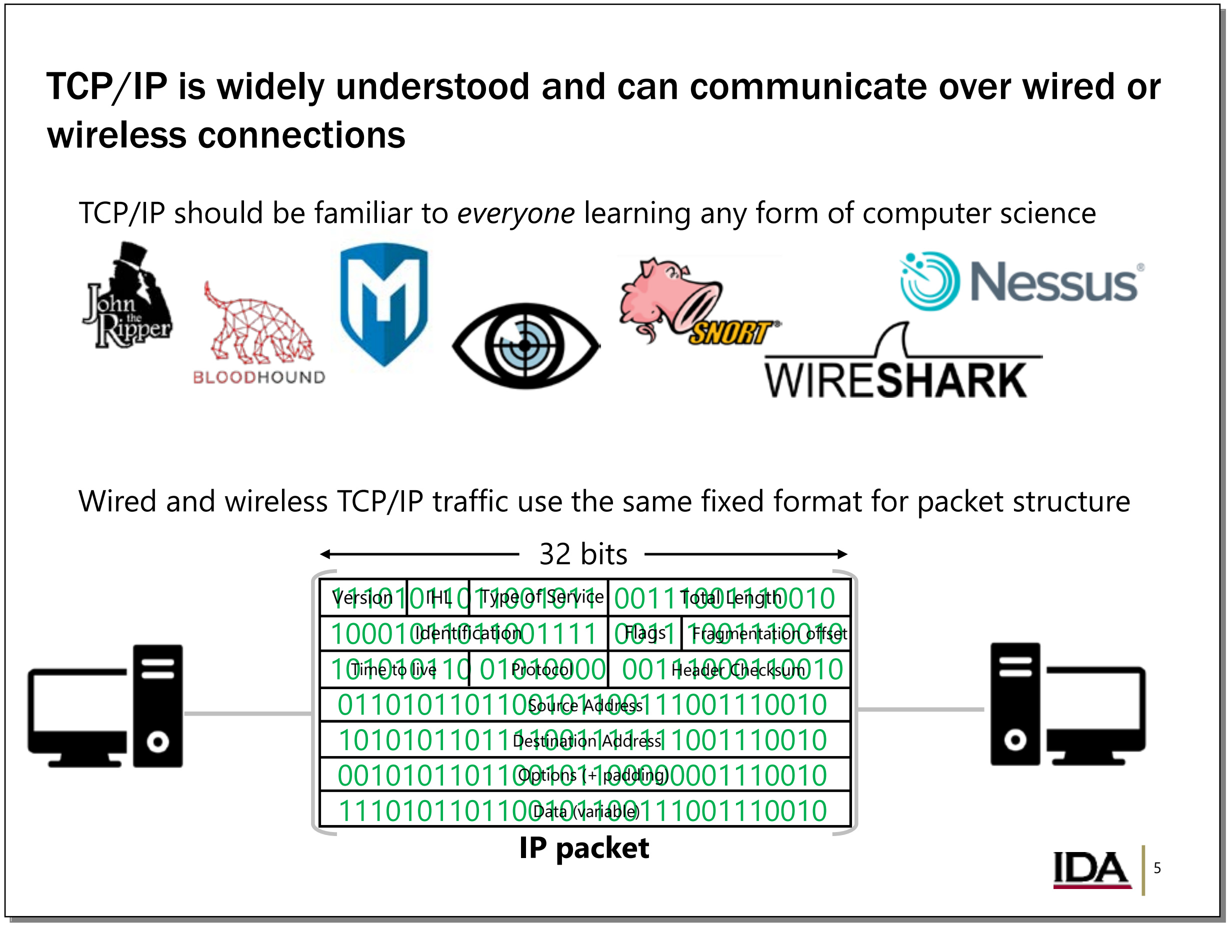
Most testing does *consider* testing all interfaces, but not all tests actually do test them. Variety of reasons we won't get into here, because we're not really interested in why they're not tested.
We want to emphasize that it's important you *do* test them, tools exist, and here's what you miss if you don't test them.

2016 Memo:
https://www.dote.osd.mil/Portals/97/pub/policies/2016/20160727_Cybersec_OTE_Priorities_and_Improvements(11093).pdf?ver=2019-08-19-144201-123

2018 Guidance:
https://www.dote.osd.mil/Portals/97/pub/policies/2018/20180403ProcsForOTEofCybersecurityInAcqProgs(17092).pdf?ver=2019-08-19-144104-027

2020 Annual Report:
https://www.dote.osd.mil/Portals/97/pub/reports/FY2020/other/2020DOTEAnnualReport.pdf?ver=rvLsaCQ_njLmPDrNIFJBWQ%3d%3d

Slide 6



In our experience observing operational tests, we have noticed that teams are generally more comfortable dealing with IP networks and web applications, and better equipped with tools for IP networks than non-IP.

However, in order to perform comprehensive cyber tests on DoD systems, cyber teams must be familiar with several other protocol formats and their respective test and analysis tools.

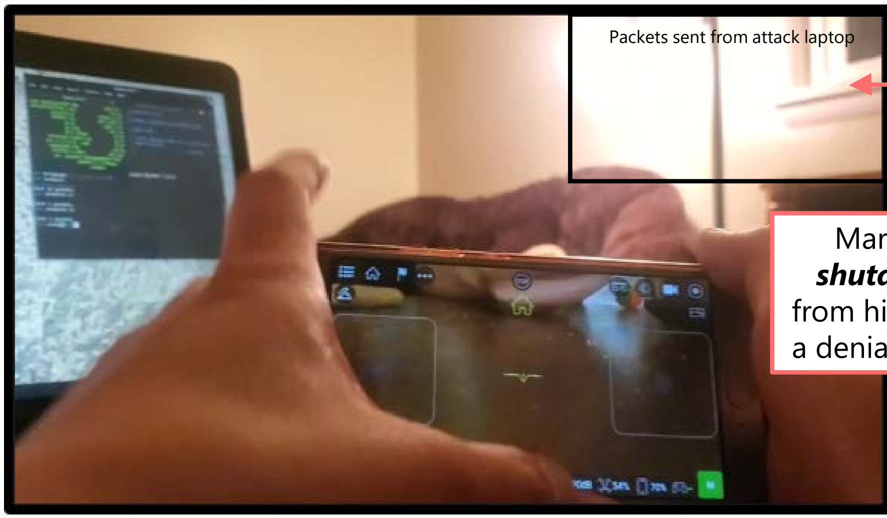
TCP/IP should be familiar to *everyone* learning computer science and many open source and commercial tools exist to perform testing on IP networks.

Slide 7

Cyber attacks can occur over wired or wireless TCP/IP connections

<u>Attack methodology:</u>

1. Crack weak password hash to access the wireless network
2. Spoof (impersonate) commands from attack laptop using the phone's network address and port

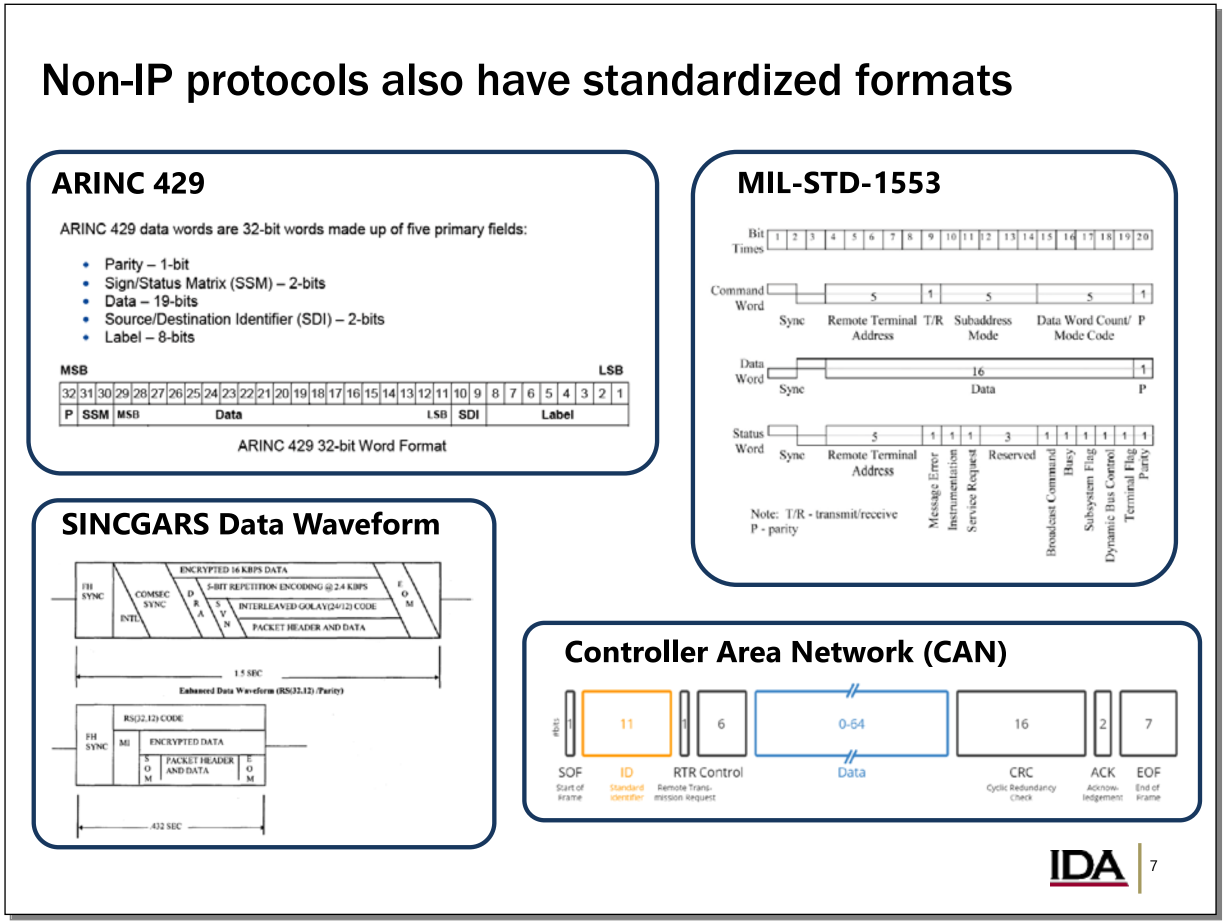


Mark replayed the ***shutdown*** command from his laptop to create a denial of service attack

IDA 6

Video removed.

Slide 8

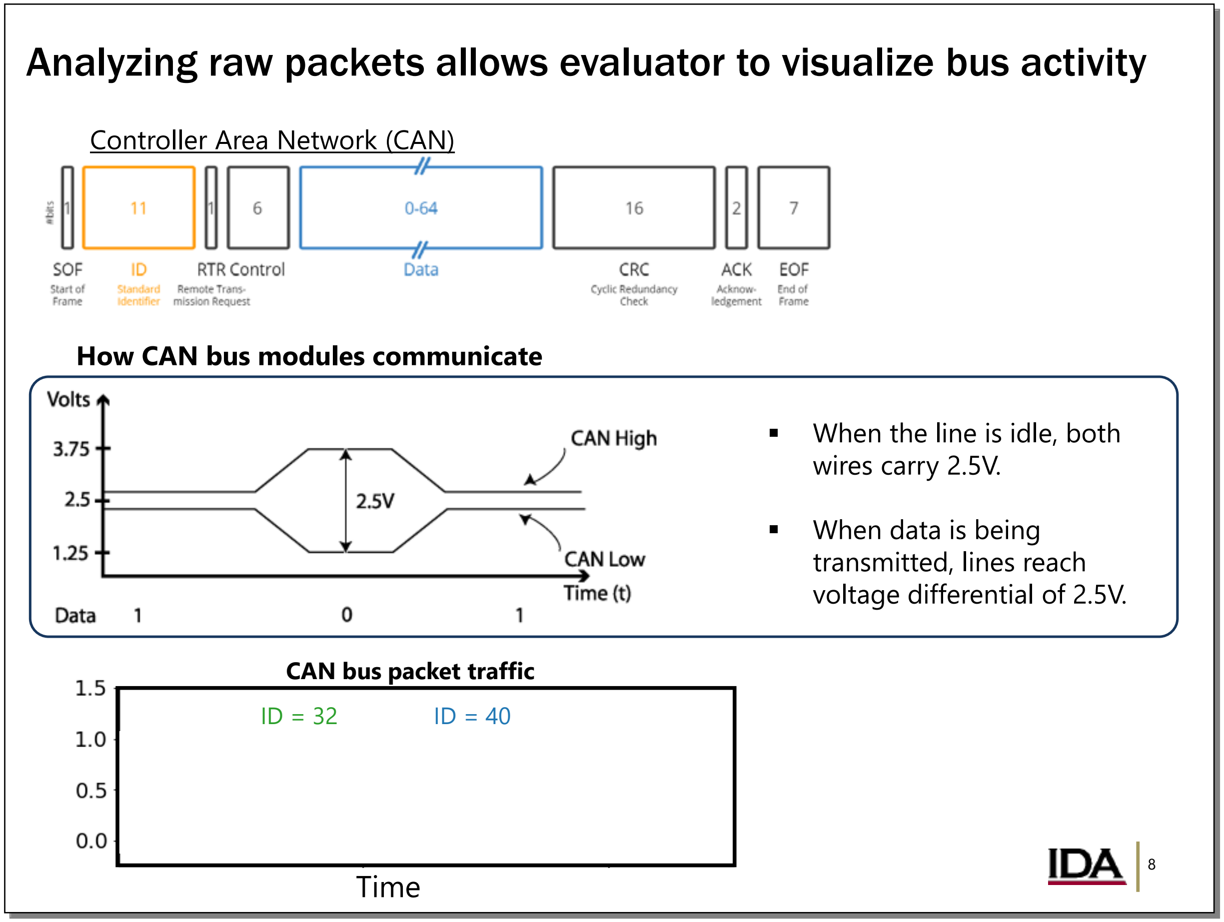


Just like TCP/IP has a fixed format for its packets, so do non-IP protocols. Although they each have unique qualities in how they communicate, the fundamental format and basic principles of each protocol remains the same regardless of implementation.

Because the basic principles do not change, we, as a test community, need to challenge ourselves to build within our organizations a fundamental understanding of each of these protocols (including TCP/IP). That way we can plan and conduct better tests, write more precise reports, and more effectively communicate findings.

SINCGARS: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=561109
1553: https://www.milstd1553.com/wp-content/uploads/2012/12/MIL-STD-1553B.pdf
ARINC 429
https://www.aim-online.com/wp-content/uploads/2019/07/aim-tutorial-oview429-190712-u.pdf

Slide 9



CAN is a very simple protocol. It is a broadcast type of message, meaning every component on the network receives every message sent. Vince will talk about the physical CAN setup he built for the demo in later slides, but I will introduce the core concepts here. From an electrical perspective, CAN bus uses two wires, CAN high and CAN low. When the line is idle, both wires carry 2.5V. When data is being transmitted, the high and low lines reach a voltage differential of 2.5V. This results in an on/off type of signal.

Our attack today will manipulate the “ID” and “Data” fields of the CAN message. The ID indicates priority of the message on the bus, with “0” indicating highest priority. Lower the ID number, higher the priority. The Data field contains zero to eight bytes and contains the actual message content.

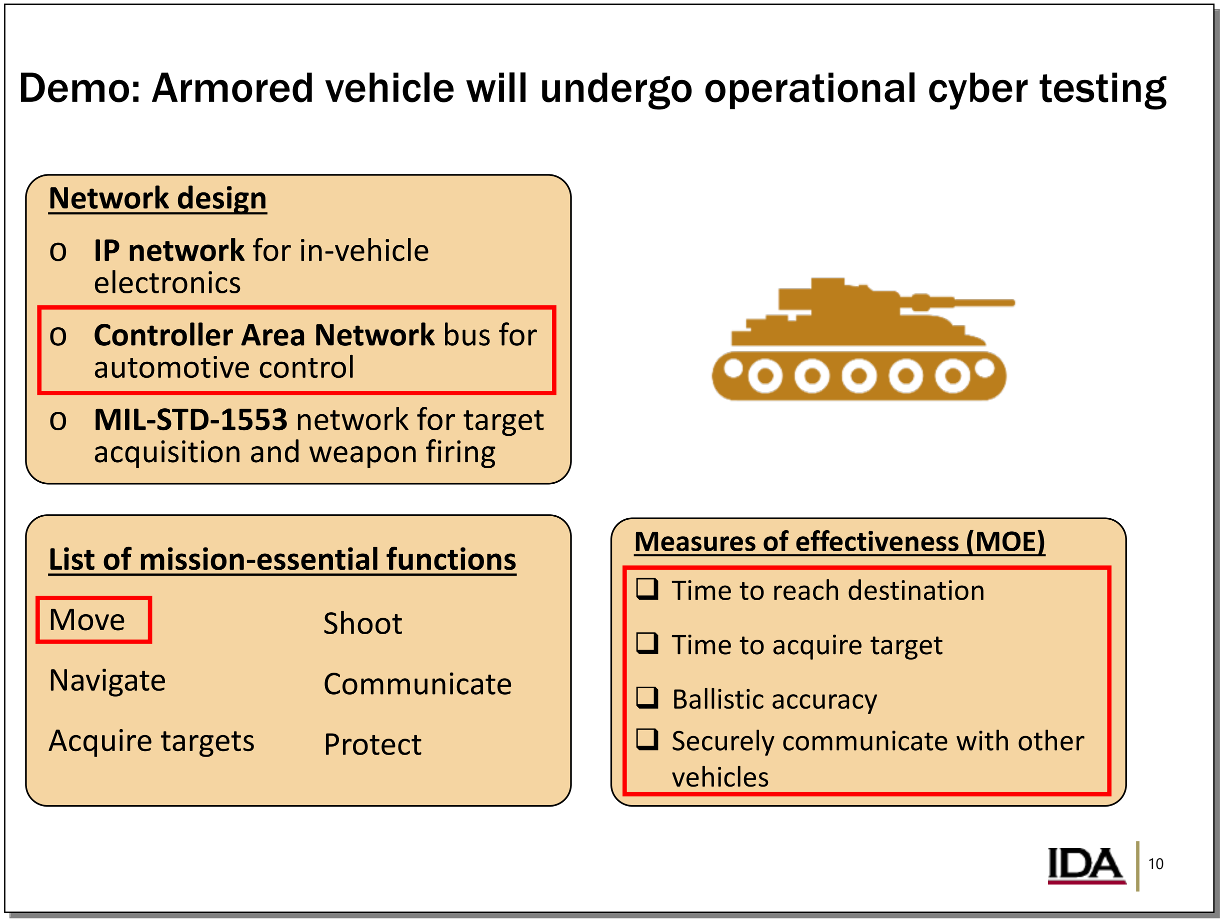
“How CAN bus modules communicate” image from *https://www.axiomatic.com/whatiscan.pdf*

Slide 10

CAN bus attack demonstration

IDA 9

Slide 11

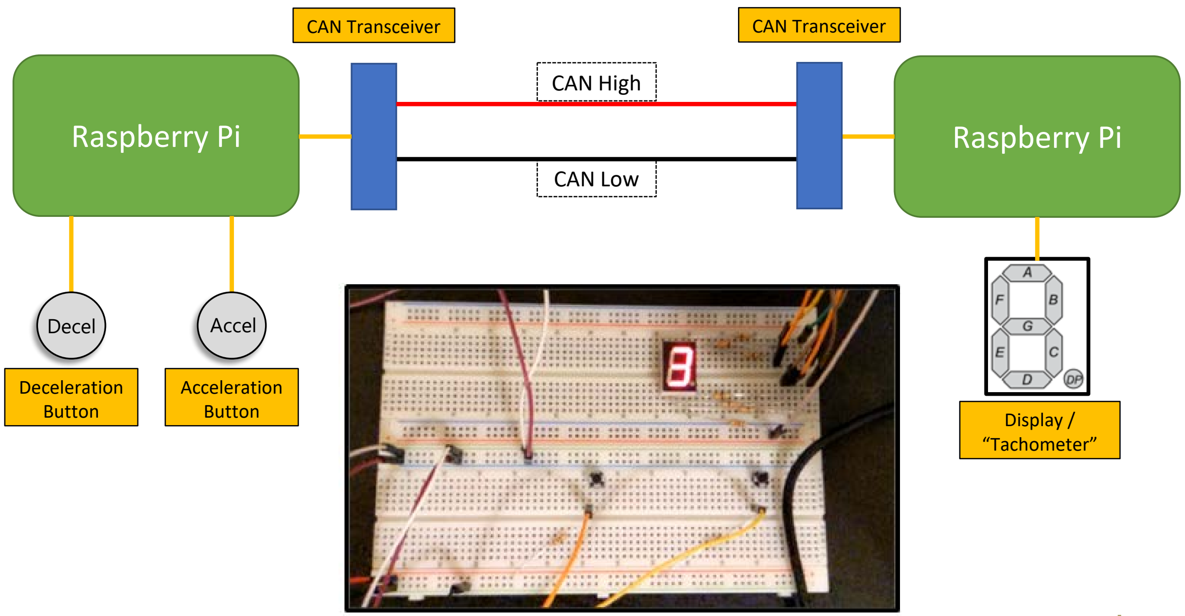


Automotive subsystems that may reside on CAN:

Engine control
Transmission control
Brakes
Suspension
Hydraulics

Slide 12

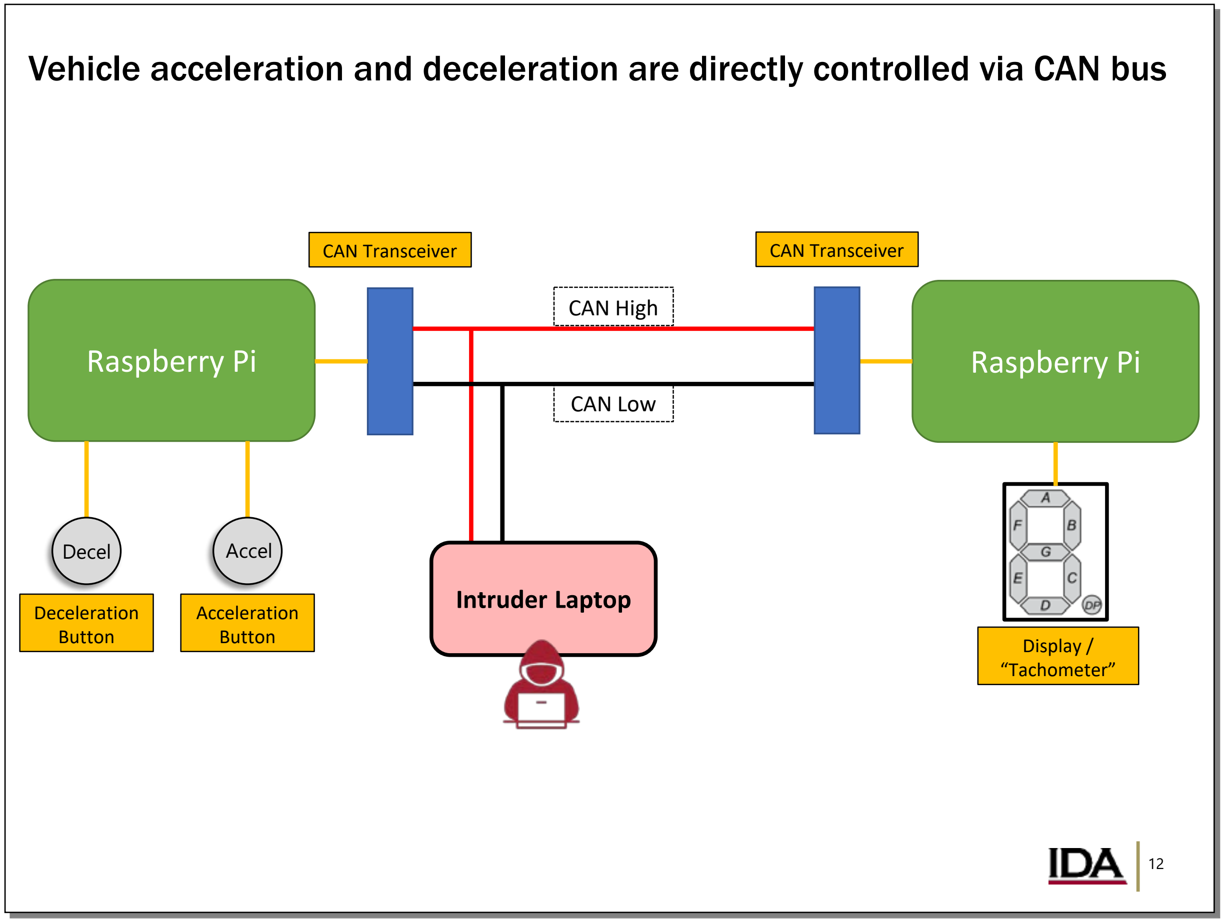
Vehicle acceleration and deceleration are directly controlled via CAN Bus



IDA 11

Video removed.

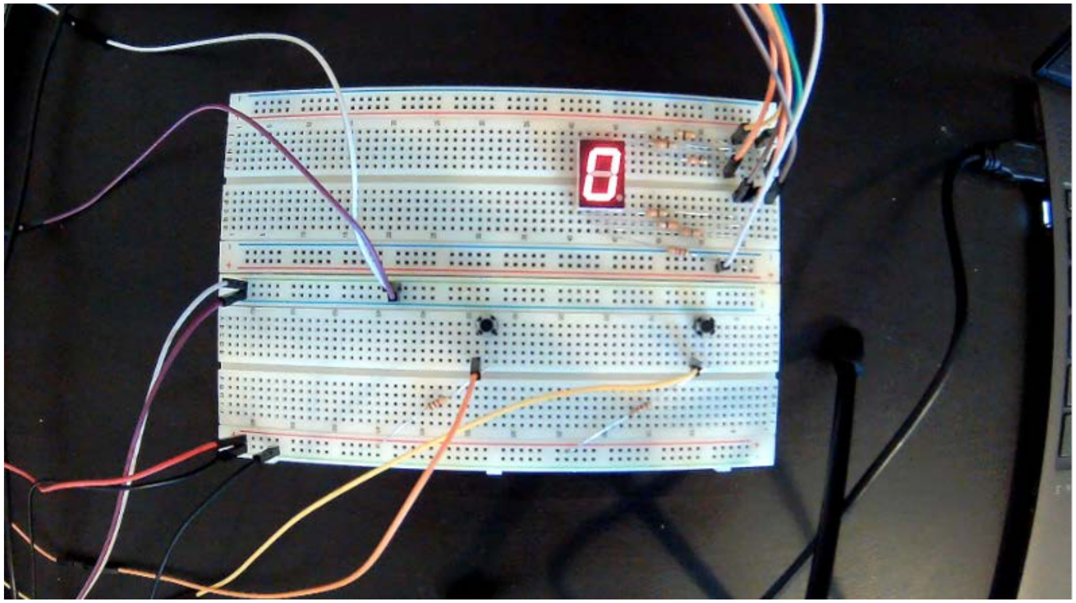
Slide 13



Although our demonstration includes a physical connection to the CAN high/low, identical attacks can be injected via the supply chain through malicious software updates or compromised line replaceable units.

Slide 14

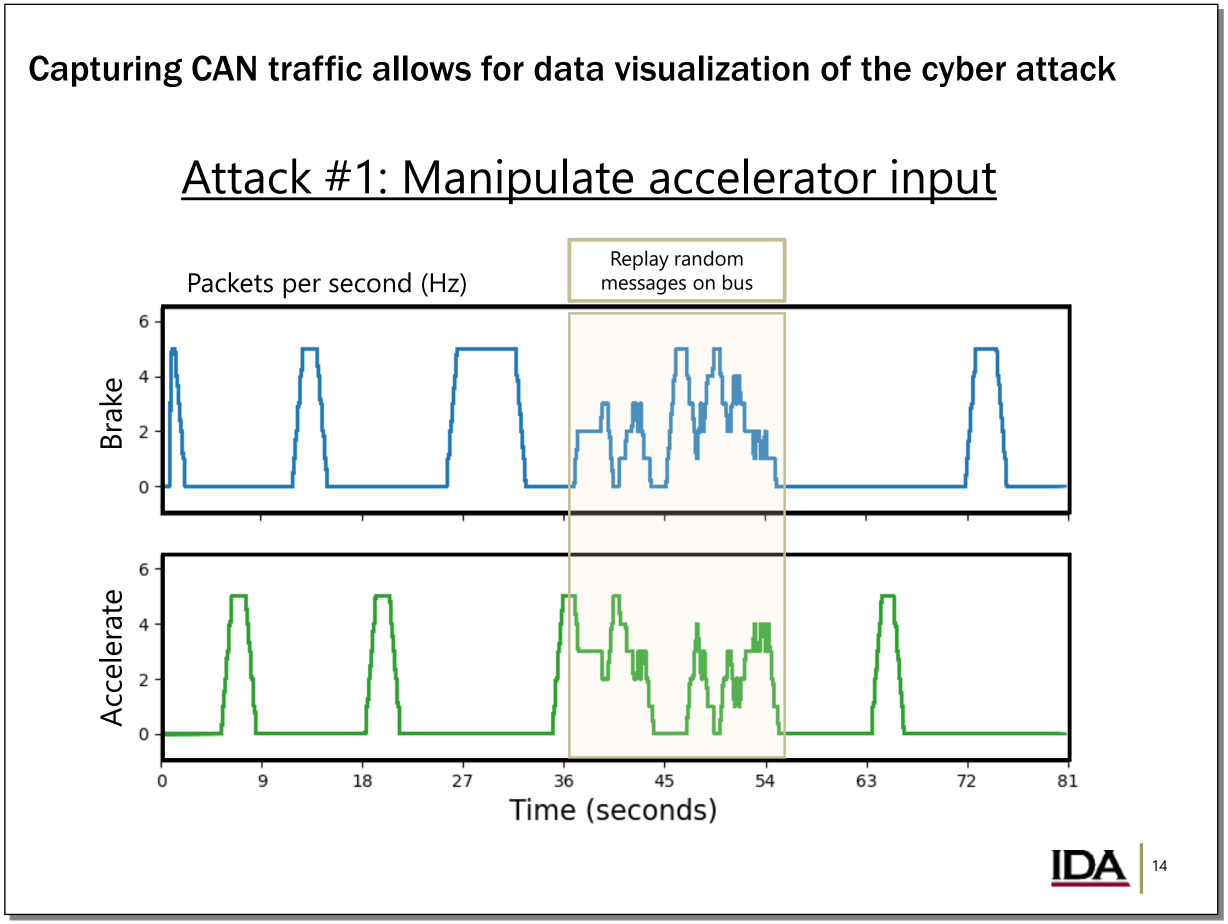
Vehicle acceleration and deceleration are directly controlled via CAN bus



IDA | 13

Video removed.

Slide 15



These plots present a sliding sum (window size of 5) of the CAN traffic. In this example, messages are sent at 5 Hz, thus a window of size of 5 data points provides the number of packets from each CAN ID per second.

Brake - CAN ID: 40
Accelerate - CAN ID: 32

Slide 16

CAN Demo – Cyber effects leading to mission effects

Cyber Effect	Measure of Effectiveness		Mission Effect
	TTRD (<20 min)	TTAT (<5 min)	
Manipulate accelerator input (integrity attack)	27 minutes	4 minutes	Attack caused the crew to lose trust in the system. Unit reduced vehicle speed and refused to fire weapon due to distrust in system performance.
	15 minutes	3 minutes	Crew pressed onward through the attack, despite degraded movement capabilities, and completed the mission.
	12 minutes	3 minutes	Crew found the malicious device connected in-line to the CAN bus inside the vehicle. Soldiers disconnected the device and recovered full system capabilities.

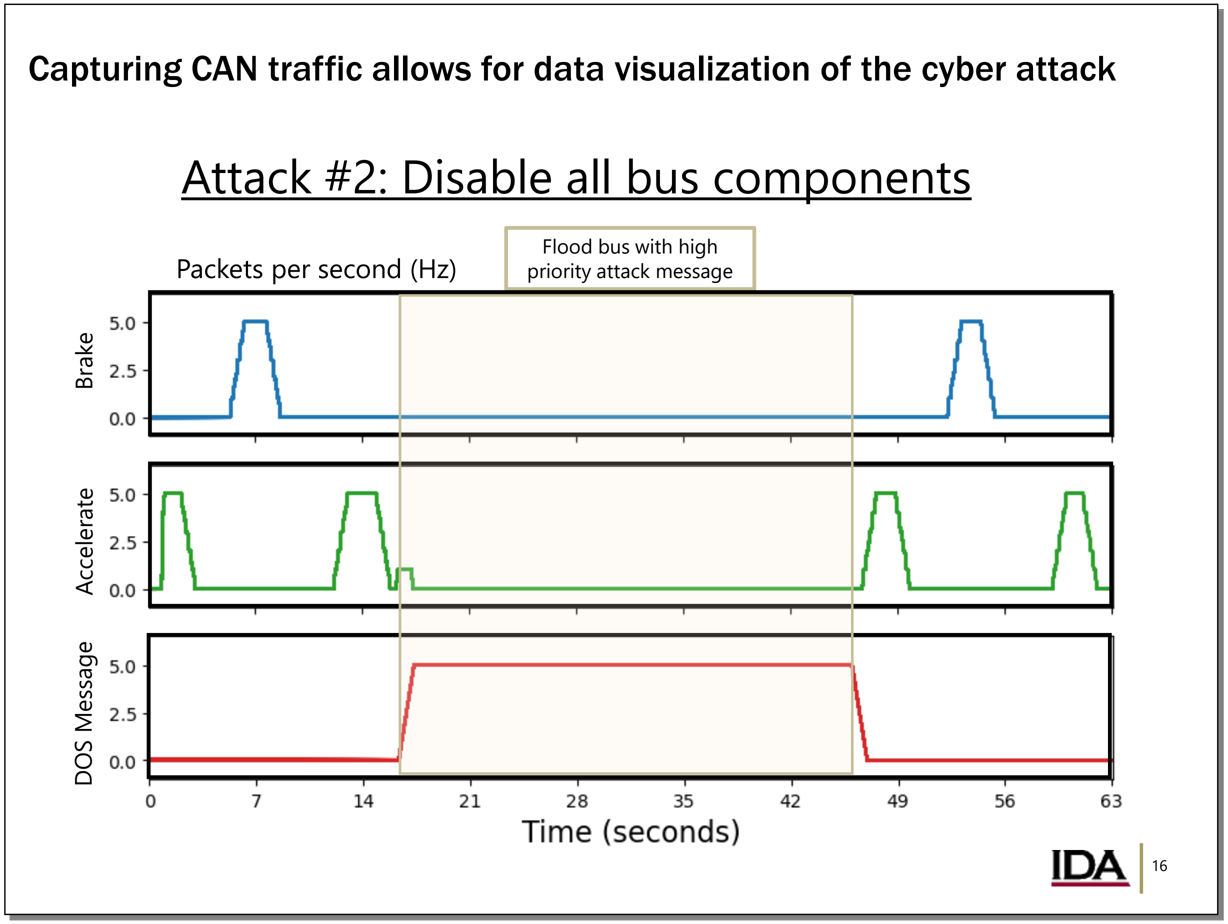
Mission failed (pink) | Mission complete (green)

TTRD = Time to reach destination
TTAT = Time to acquire target

All effectiveness data, thresholds, and mission effects are fictional.

IDA 15

Slide 17



These plots present a sliding sum (window size of 5) of the CAN traffic. In this example, messages are sent at 5 Hz, thus a window of size of 5 data points provides the number of packets from each CAN ID per second.

Brake - CAN ID: 40
Accelerate - CAN ID: 32
DOS Message – CAN ID: 00

Slide 18

CAN Demo – Cyber effects leading to mission effects

Cyber Effect	Measure of Effectiveness		Mission Effect
	TTRD (<20 min)	TTAT (<5 min)	
Manipulate accelerator input (integrity attack)	27 minutes	4 minutes	Attack caused the crew to lose trust in the system. Unit reduced vehicle speed and refused to fire weapon due to distrust in system performance.
	15 minutes	3 minutes	Crew pressed onward through the attack, despite degraded movement capabilities, and completed the mission.
	12 minutes	3 minutes	Crew found the malicious device connected in-line to the CAN bus inside the vehicle. Soldiers disconnected the device and recovered full system capabilities.
Disable brakes (availability attack)	Did not complete	Did not complete	Attack prevented the unit from reaching target destination and acquiring target. Thus, the unit could not complete their mission.

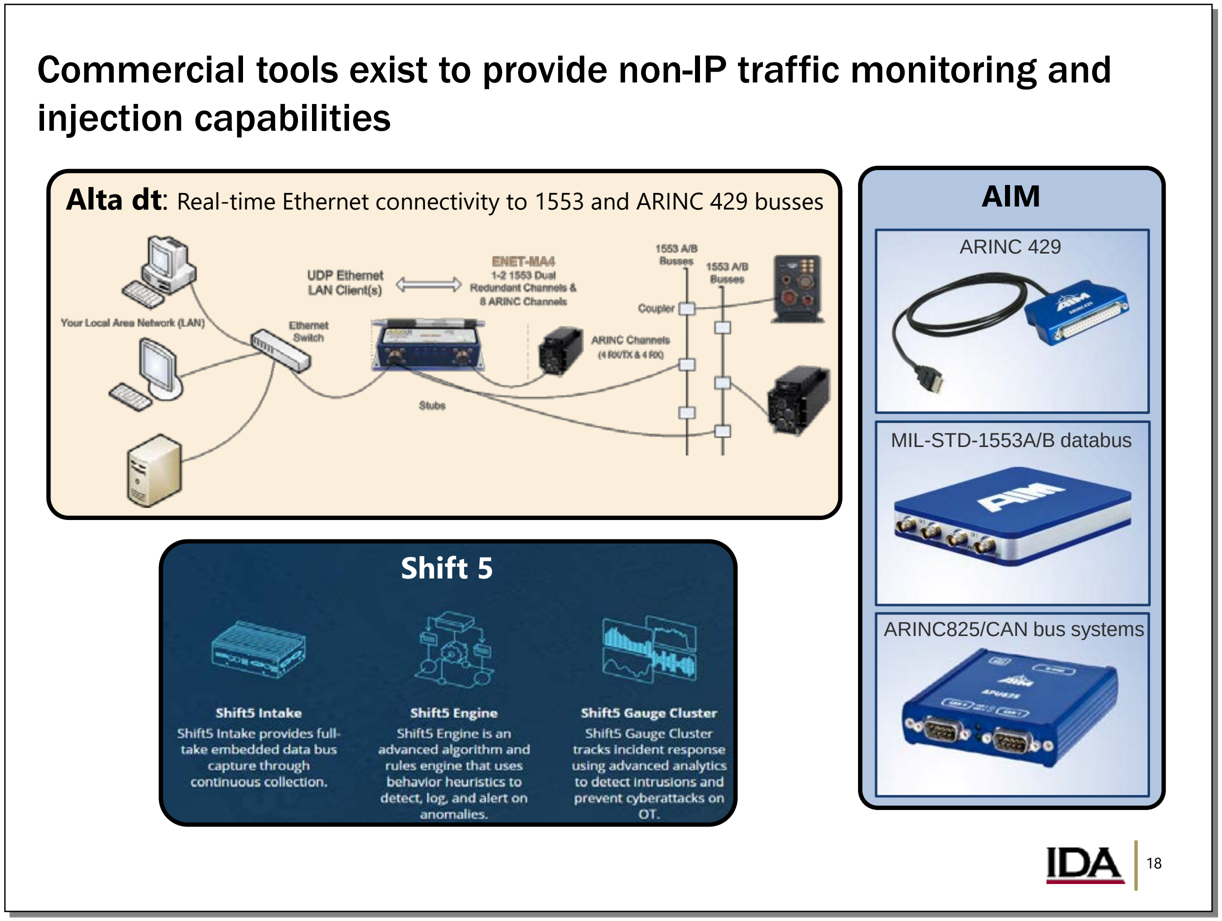
TTRD = Time to reach destination
TTAT = Time to acquire target

Mission failed (red) / Mission complete (green)

All effectiveness data, thresholds, and mission effects are fictional.

IDA 17

Slide 19



These products cost O($10k)

But the many tests they support are each on the order of O($1M)

-

Alta DT: https://www.altadt.com/product/enet-ma4-1553-arinc-ethernet-converter/

AIM:
- CAN: https://www.aim-online.com/products/apu825/
- 1553: https://www.aim-online.com/products/anet1553-x/
- ARINC429: https://www.aim-online.com/products/asc429-x/

Shift 5: https://www.shift5.io/

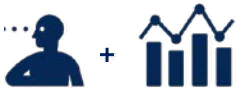
Slide 20

Conclusions

Many systems on DoD oversight use non-IP buses to support mission-critical capabilities

- DOT&E guidance and memoranda emphasize the need to test non-IP buses and have identified gaps in test tools

Well-documented data collection of bus activity allows for quantitative confirmation of observed cyber effects



Improving our fundamental understanding of non-standard communication protocols will lead to better operational test planning, data collection, and reporting.

IDA 19

Slide 21

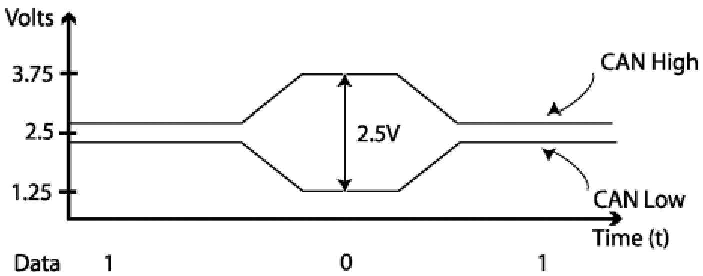
Backup

IDA 20

Slide 22

How do CAN bus modules communicate?

CAN bus uses two dedicated wires for communication. The wires are called CAN high and CAN low. When the CAN bus is in idle mode, both lines carry 2.5V. When data bits are being transmitted, the CAN high line goes to 3.75V and the CAN low drops to 1.25V, thereby generating a **2.5V differential** between the lines. Since communication relies on a voltage differential between the two bus lines, the CAN bus is NOT sensitive to inductive spikes, electrical fields or other noise. This makes CAN bus a reliable choice for networked communications on mobile equipment.



CAN power can be supplied through CAN bus. Or a power supply for the CAN bus modules can be arranged separately. The power supply wiring can be either totally separate from the CAN bus lines (using suitable gauge wiring for each module) resulting in two 2-wire cables being utilized for the network, or it can be integrated into the same cable as the CAN bus lines resulting in a single 4-wire cable. CAN bus cabling is available from multiple vendors.

https://www.axiomatic.com/whatiscan.pdf

IDA 21

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
4-2021	Final	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
DATAWorks 2021: Operational Cybersecurity Test and Evaluation of Non-IP and Wireless Networks	HQ0034-19-D-0001
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Peter M. Mancini (OED); Vincent C. Bass (OED); Mark R. Herrera (OED)	C9096
	5e. TASK NUMBER
	C9096
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Institute for Defense Analyses 4850 Mark Center Drive Alexandria, Virginia 22311-1882	D-21552 NS H 2021-000036
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	**10. SPONSOR/MONITOR'S ACRONYM(S)**
Institute for Defense Analyses 4850 Mark Center Drive Alexandria, Virginia 22311-1882	IDA
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for Public Release. Distribution Unlimited.

13. SUPPLEMENTARY NOTES

Project Leader: Mancini, Peter M

14. ABSTRACT

Nearly all land, air, and sea maneuver systems (e.g., vehicles, ships, aircraft, and missiles) are becoming more software-reliant and blending internal communication across both Internet Protocol (IP) and non-IP buses. IP communication is widely understood among the cybersecurity community, whereas expertise and available test tools for non-IP protocols such as Controller Area Network (CAN) and MIL-STD-1553 are not as commonplace. However, a core tenet of operational cybersecurity testing is to asses all potential pathways of information exchange present on the system, to include IP and non-IP. In this presentation, we will introduce a few non-IP protocols (e.g., CAN, MIL-STD-1553) and provide a live demonstration of how to attack a CAN network using malicious message injection. We will also discuss how potential cyber effects on non-IP buses can lead to catastrophic mission effects to the target system.

15. SUBJECT TERMS

Cybersecurity; IP; hacking; operational testing; CAN bus; 1553

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Peter M. Mancini
Unclassified	Unclassified	Unclassified	Unlimited	52	**19b. TELEPHONE NUMBER** *(Include area code)* (703) 845-2496