

# Colorado State University

# SA STREAMS ENGINEERING

# USAFA Guest Lecture: Digital Forensics and Cybersecurity for Heavy Vehicle Systems

Jeremy Daily, Ph.D., P.E.

Associate Professor of Systems Engineering

Jeremy.Daily@colostate.edu

Trae Span, Major, USAF Systems Engineering PhD Student

Trae.span@colostate.edu

Gabe Salinger, Lt, USAF

Systems Engineering M.S. Student

Gabe.salinger@colostate.edu

#### Jeremy Daily Associate Professor of Systems Engineering

- Active duty Air Force as electronics technician, 1995-2002
- Wright State University, Ph.D. in Engineering, 2001-2006
- Aerospace Engineer, Wright-Patterson Air Force Base, Propulsion Directorate, Turbine Engines, Structures Branch, 2005-2006
- University of Tulsa, tenured faculty, 2006-2019

- Jackson Hole Scientific Investigations, Consultant, 2001-present
- Synercon Technologies, LLC, founder and CEO, 2013-2018
- CyberTruck Challenge, co-founder and director, 2017-present
- DG Technologies, Technical Advisor, 2018-present
- Associate Professor of Systems Engineering, Colorado State University, 2019-present
- Creator of ski boat trolling motor system with auto pilot; unofficial Yellowstone Lake invasive lake trout eradicator.

## Presentation Outline

- Vehicle Systems Approach to Cybersecurity with Definitions
- Passenger Vehicle Event Data Recorder Research
- Heavy Vehicles and SAE J1939
- Crash Testing with Videos
- Digital Forensics and HVEDRs
- Cybersecurity

- Epiphanies Along the Way
- Paths To Systems Engineering
  - Span and Salinger
- Observations and Discussion



## What is Cybersecurity?

Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use. (https://www.us-cert.gov/ncas/tips/ST04-001)

CIA for Data

4

- Confidentiality: Can the data be kept secret?
- Integrity: Is the data the same as when it was generated?
- Availability: Can the right people access the data at the right time?

- The three A's (AAA)
  - Authentication: Is the user or device who they say they are?
  - Authorization: Is the user or device allowed to do something?
    - Is the system in a state to accept commands for actions?
  - Auditing: Do we know who did what?

#### Cybersecurity is a verb:

A process of continuously understanding risks, vulnerabilities, and implementing mitigations.

Consequence: There is not an end-state for cybersecurity – it's an iterative process of determining requirements, risks, and mitigations.

#### Road Vehicles - Cybersecurity Engineering JSO/SAE21434



Systems Engineering drives requirements for concurrent development and testing of hardware and software for more secure solutions.

## What is Digital Forensics?

- Digital forensics is a branch of forensic science encompassing the recovery and investigation of material found in digital devices. <a href="https://en.wikipedia.org/wiki/Digital\_forensics">https://en.wikipedia.org/wiki/Digital\_forensics</a>)
- Forensic soundness gives reasonable assurance that digital evidence was not corrupted or destroyed during investigative processes whether on purpose or by accident.
  - I. Meaning: confidence in the interpretation of data.
  - 2. Error Detection: predicting and handling of issues during the forensic process.
  - 3. Transparency: following a documented and verifiable process
  - 4. Experience: properly trained investigators
  - 5. Integrity: be able to verify data has not been altered
- Some Electronic Control Modules/Units (ECMs or ECUs) record interesting digital information.



Johnson, J., Daily, J., and Kongs, A., "On the Digital Forensics of Heavy Truck Electronic Control Modules," SAE Int. J. Commer. Veh. 7(1):72-88, 2014, https://doi.org/10.4271/2014-01-0495.

Daily, J., DiSogra, M., and Van, D., "Chip and Board Level Digital Forensics of Cummins Heavy Vehicle Event Data Recorders," SAE Technical Paper 2020-01-1326, 2020, <u>https://doi.org/10.4271/2020-01-1326</u>.

# Origins and Progress

How a mechanical engineer becomes interested in cybersecurity...

- Interest in Traffic Crash Reconstruction
  - Wrote the book

7

- Performed crash tests
- Evolved to Digital Forensics
  - Bosch Crash Data Retrieval for Air Bag Modules
  - Accuracy of Stored Network Data
- Theory: Compare Network Traffic to External Reference to determine EDR accuracy
  - SAE 2012-01-1000
  - SAE 2012-01-0999
- Need to "hack" the CAN bus to correlate measurements...

#### FUNDAMENTALS of TRAFFIC CRASH RECONSTRUCTION

Volume 2 of the Traffic Crash Reconstruction Series



### Passenger Vehicle Air Bag Module Data

 Recorded crash pulse (Delta-V) and pre-impact vehicle operation

8

- Data can compliment physics-based traffic crash reconstructions
- Started with GM vehicles as early as 1994
- Toyota and Ford released tools (through the Bosch CDR kit) around 2001
- NHTSA Rule 563 mandates minimum data elements and tool availability in 2012.
  - Nearly all newer cars have event recordings

#### \$49 Airbag Module Reset | 24 Hour Reset & Return Service (Ad) www.myairbags.com/Airbag-Reset/Service ▼ (877) 688-6534

Nation's #1 Airbag Module Reset Specialists! 100% Guaranteed & Lifetime Warranty. We Reset & Clear All Fault Codes! Over 1 Million Parts Serviced. Get Started Today. Money Back Guarantee. 150,000+ Happy Customers. Superior Customer Support. 1 Million+ Parts Serviced. Airbag Module Reset - from \$49.00 - 24 Hour Airbag Reset - More ▼

#### To remove your **airbag module**, follow these steps:

1. Locate SRS airbag computer module.



- 2. After you've found the SRS computer **module**, disconnect the positive battery cable.
- 3. Wait three minutes, and then unplug the **airbag** control **module** harness wiring plugs.
- 4. Send the airbag computer module to us for airbag module reset.

Airbag Module Resets - We Can Fix Your Airbag For Hundreds Less ... https://www.myairbags.com/airbag-module-reset/

About this result
Feedback



## Crash Testing

crashes



BOSCH



 Compare instrumented test data to event data recorder information

Understand dynamics of

- 5 seconds of pre-crash data
- Crash Delta-V (from accelerometer)

#### Strategy:

- CAN data comparison for pre-crash data
- Accelerometers for crash pulses measurements



Typical crash data from an airbag module.

#### CAN Bus Reconnaissance

1. Record CAN data along with external measurements during a dynamic maneuver

2. Group messages by ID

3. Generate all probable combinations of data bytes

4. Plot the generated data interpretations

5. Determine the best fit to derive meaning



#### External Reference





Network Traffic

### Manual pattern recognition

Sample recording of a figure-8 maneuver in a parking lot.



Maybe a machine can do this for us now...

Epiphany #1: Humans are pretty good at recognizing patterns

#### Mechanical Hacking 15

2. airbag module. 3. Accelerometer traffic.

#### Air Bag Module

Ruth, R., Bartlett, W., and Daily, J., "Accuracy of Event Data in the 2010 and 2011 Toyota Camry During Steady State and Braking Conditions," SAE Int. J. Passeng. Cars - Electron. Electr. Syst. 5(1):358-372, 2012, https://doi.org/10.4271/2012-01-0999.

- Record CAN data while 1. braking hard.
- Tap the mallet to set nondeployment events in the
- Recover airbag module data and compare to the newly discovered decoding for CAN

Dowel Rod

#### Safe and Repeatable Event Setting





Forensic data and lab data are synchronized so we can assess accuracy in time and value.

Epiphany #2: Understanding the vehicle network is critical to forensics.

## Unlock **your** door with a computer



Epiphany #3: Messing around with vehicle networks is fun!

#### Crash Testing... for Science

- 2011 Illinois Association of Technical Accident Investigators (IATAI)
- GMC Envoy vs Mini Cooper

- Cable pull system on a non-used section of an airport
- Recorded CAN on Mini-Cooper
- Validated accelerometer readings from the Envoy Airbag Module





#### Making use of a Crash Test



22

The Mini Cooper Alarm Clock Cluster



#### How to Hack Your Mini Cooper: Reverse Engineering CAN Messages on Passenger Automobiles

Jason Staggs University of Tulsa Institute for Information Security Crash Reconstruction Research Consortium jason-staggs@utulsa.edu

#### ABSTRACT

With the advent of modern vehicular technology, the computerized components of passenger vehicles have become increasingly interconnected to facilitate automotive efficiency, driving current increasing and control of the second secon (NRZ) format over the wire, and facilitates the use of automatic collision detection with arbitration. Essentially, any message sent out by any node on a CAN network will be seen by all other nodes [4]. European manufactured automobiles were early adopters of CAN networks. However, since 2008, all cars sold in

https://www.defcon.org/images/defcon-21/dc-21-presentations/Staggs/DEFCON-21-Staggs-How-to-Hack-Your-Mini-Cooper-WP.pdf

## Class Projects turn into Defcon Presentations

Vehicle and Industrial Communication Systems





DEF CON 21 - Jason Staggs - How to Hack Your Mini Cooper 5,507 views

#### CAN Clock: Hours on speedometer, minutes on tachometer

Epiphany #4: Students like hands-on vehicle networking projects

#### **Example Forensic Recovery**

## **IPTM Special Problems 2015**

## **Transit Bus Vs School Bus**



## Recovery of Data

Cat Electronic Technician 20154 VI.0 - Snapshot Viewer						
File View Diagnostics Information Service Utilities Help						
🖴 🖫 🖴   🚧   🎇 🏁 🎘 🏈   攀 🎽   📅 🥞   🔂 🧐   🏦 🤸   🍙 ? 🖳						
Snapshot: 9608:00:55 External Trigger- External Switch 10/23/2009 6:08:17 AM						
-9.380, 0.00						
ecm Snapshots						
13151:53:53 Diagnostic 164- 3 Injection Actuation Pressure voltage high (15) 5/21/2015 12:	41:04 PM					
13152:02:38 Diagnostic 164- 3 Injection Actuation Pressure voltage high (15) 5/21/2015 12:47						
<sup>07</sup> 13145:30:01 External Trigger- Data Link Message 5/18/2015 12:48:41 PM						
5000.00.55 External Thyger- External Switch 10/25/2005 0.00.17 AM						
13151:49:37 Sudden Stop 84-14 Quick Stop Occurrence 5/20/2015 12:33:42 PM						
0.3						
Clear Clear	All					
Snapshot Information						
ECM Ingger Time: 12:41:04 PM						
View Data View Graph Ca	ncel					





## Recovery of Data



#### But we know data exists!

#### Data Bus was Recorded During the Crash



#### Network Logs from ET Showed Data for Quickstop

📔 C:\Us	sers\jeremy-daily.UTULSA\Dropbox (JHSI)\TUCRRC\JPTM 2015\CAT HVEDR Data\bus-bus-crash\truncated-traffic.txt - Notep	ad++ [Administrator]		
File E	dit Search View Encoding Language Settings Macro Run Plugins Window ?			Х
🔓 🖨	- E & S & A + M () > C + M + A + C = G = 1 [E Z   D + M + A + A + A + A + A + A + A + A + A	🖻 🔤 🛛 🏧 🖉	Ζ 🛃	
📄 trunca	ated traffic bt 🗵			
1	02,RM,21,4096,1,00,01,84,de,80,fe,ac,90,d3,03,01,00,01,01,22,72,0	)5,2d,07,79,98	,	<u>^</u>
2	02,RM,18,4096,1,00,01,84,f2,80,fe,ac,90,d3,03,01,00,01,02,20,00,3	31,00,		
3	02,RM,22,4096,1,00,01,85,09,80,fe,ac,90,d3,03,01,00,01,03,b3,91,0	08,b4,98,08,b5	,1b,	
4	02,RM,21,4096,1,00,01,85,83,80,fe,ac,90,d3,03,01,00,02,01,22,7b,0	5,2d,07,79,98	,	
5	02,RM,18,4096,1,00,01,85,97,80,fe,ac,90,d3,03,01,00,02,02,20,04,3	31,00,		-
6	02,RM,22,4096,1,00,01,85,ae,80,fe,ac,90,d3,03,01,00,02,03,b3,85,0	08,b4,98,08,b5	,1b,	
7	02,RM,21,4096,1,00,01,86,28,80,fe,ac,90,d3,03,01,00,03,01,22,80,0	)5,2d,07,79,98	,	
8	02,RM,18,4096,1,00,01,86,3b,80,fe,ac,90,d3,03,01,00,03,02,20,04,3	31,00,		
9	02,RM,22,4096,1,00,01,86,53,80,fe,ac,90,d3,03,01,00,03,03,b3,91,0	08,b4,98,08,b5	,1b,	
10	02,RM,21,4096,1,00,01,86,cd,80,fe,ac,90,d3,03,01,00,04,01,22,77,0	)5,2d,07,79,98	,	
11	02,RM,18,4096,1,00,01,86,e0,80,fe,ac,90,d3,03,01,00,04,02,20,05,3	31,00,		
12	02,RM,22,4096,1,00,01,86,f8,80,fe,ac,90,d3,03,01,00,04,03,b3,9c,0	)8,b4,98,08,b5	,1b,	
13	02,RM,21,4096,1,00,01,87,72,80,fe,ac,90,d3,03,01,00,05,01,22,6f,0	)5,2d,07,79,98	<i>'</i>	
14	02,RM,18,4096,1,00,01,87,86,80,fe,ac,90,d3,03,01,00,05,02,20,06,3	31,00,		
15	02,RM,22,4096,1,00,01,87,9d,80,fe,ac,90,d3,03,01,00,05,03,b3,9f,0	)8,b4,98,08,b5	,1b,	
16	02,RM,21,4096,1,00,01,88,44,80,fe,ac,90,d3,03,01,00,06,01,22,74,0	)5,2d,07,79,98	,	
17	02,RM,18,4096,1,00,01,88,57,80,fe,ac,90,d3,03,01,00,06,02,20,07,3	31,00,		
18	02,RM,22,4096,1,00,01,88,6e,80,fe,ac,90,d3,03,01,00,06,03,b3,96,0	18,64,98,08,65	, 1D,	
19	02,RM,21,4096,1,00,01,88,f8,80,fe,ac,90,d3,03,01,00,07,01,22,84,0	)5,2d,07,79,98	,	
20	U2, RM, 18, 4096, 1, 00, 01, 89, 00, 80, 10, ac, 90, d3, 03, 01, 00, 07, 02, 20, 09, 3	31,00, No. 14,00,00, 15	11.	
21	02,RM,22,4096,1,00,01,89,23,80,fe,ac,90,d3,03,01,00,07,03,b3,9c,0	18, 64, 98, 08, 65	, 1D,	
22	02, RM, 21, 4096, 1, 00, 01, 89, 90, 80, 10, ac, 90, d3, 03, 01, 00, 08, 01, 22, 83, 0	15,20,07,79,98	'	
23	02, RM, 18, 4096, 1, 00, 01, 89, 50, 80, 18, ac, 90, d3, 03, 01, 00, 08, 02, 20, 04, 3	91,00, 00 b4 00 00 b5	116	
24	02, RM, 22, 4096, 1, 00, 01, 89, 67, 80, 10, 20, 90, d3, 03, 01, 00, 00, 03, 05, 99, 0	10, D4, 90, 00, D3	,10,	
20	02, RM, 21, 4096, 1, 00, 01, 02, 56, 00, 16, 26, 90, 03, 03, 01, 00, 09, 01, 22, 76, 0	0,20,07,79,90	'	
20	02, RM, 10, 4090, 1, 00, 01, 02, c6, 00, fe ac, 90, d3, 03, 01, 00, 09, 02, 20, 00, 30, 02, 00, 00, 00, 00, 00, 00, 00, 00, 0	)	1h	
28	02 RM 21 4096 1 00 01 8b 40 80 fe ac 90 d3 03 01 00 0a 01 22 6e 0	15 24 07 79 98	, 10,	
29	02.RM.18.4096.1.00.01.8b.54.80.fe.ac.90.d3.03.01.00.0a.02.20.0c.3	31.00.	,	
30	02.RM, 22, 4096, 1, 00, 01, 8b, 6b, 80, fe, ac, 90, d3, 03, 01, 00, 0a, 03, b3, 93, 0	08, b4, 98, 08, b5	.1b.	
31	02.RM, 21, 4096, 1, 00, 01, 8c, 03, 80, fe, ac, 90, d3, 03, 01, 00, 0b, 01, 22, 73, 0	)5,2d,07,79.98	~,	
32	02, RM, 18, 4096, 1, 00, 01, 8c, 16, 80, fe, ac, 90, d3, 03, 01, 00, 0b, 02, 20, 0e, 3	31,00,		
22	02 RM 22 4096 1 00 01 Rc 20 80 fe ac 90 d3 03 01 00 0b 03 b3 89 0	18 h4 98 08 h5	1h	-
Normal t	text file length : 11232 lines : 145 Ln : 1 Col : 1 Sel : 0   0 UNI	X UTF-8		INS

# Data Extraction Algorithm





	box (JHSJ)\TUCRRC\IPTM 2015\CAT HVEDR Data\bus-bus-crash\bus-bus.txt - Notepad++ [Administrator] Language Settings Macro Run Plugins Window ?	ECM says, "Are you me to send the data frame?"	ready for in the 48 <sup>th</sup>	X
	02,RM,13,4096,1,00,01,a4,48,80,fe,ac,90,d1,03,01,00,2f,			•
	02,SM,00,6,0,0,06,ac,fe,80,70,d3,			' I
	02,RM,21,4096,1,00,01,a4,8c,80,fe,ac,90,d3,03,01,00,2f,01,22,9e	, 00		
/	02,RM,18,4096,1,00,01,a4,9f,80,fe,ac,90,d3,03,01,00,2f,02,20	00,		
	02, RM, 22, 4096, 1, 00, 01, a4, b7, 80, fe, ac, 90, d3, 03, 01, 00, 2f, 0, fo	c,02,b4,a0,0f,b5,98,		
	02,SM,00,10,0,06,ac,fe,80,80,d1,03,01,00,30,			
	02,RM,13,4096,1,00,01,a4,fc,80,fe,ac,90,d1,03,01,00,30,			
`	02,SM,00,6,0,0,06,ac,fe,80,70,d3,			
	02,RM,21,4096,1,00,01,a5,32,80,fe,ac,90,d3,03,01,00,30,01,22,00	),00,2d,07,79,98,		
	02,RM,18,4096,1,00,01,a5,45,80,fe,ac,90,d3,03,01,00,30,02,20,04	4,31,00,		
	02,RM,22,4096,1,00,01,a5,5c,80,fe,ac,90,d3,03,01,00,30,03,b3,fc	c,02,b4,a0,0f,b5,00,		
	02,SM,00,10,0,0,06,ac,fe,80,80,d1,03,01,00,31,			
	02,RM,13,4096,1,00,01,a5,92,80,fe,ac,90,d1,03,01,00,31,			
	02,SM,00,6,0,0,06,ac,fe,80,70,d3,			
	02,SM,00,6,0,0,06,ac,fe,80,70,d3,			
	02,SM,00,6,0,0,06,ac,fe,80,70,d3,			
	02,SM,00,6,0,06,ac,fe,80,70,d3,			-
				Þ.
	length : 85965 lines : 1056 Ln : 903 Col : 51 Sel	:0 0 Dos\Windows	UTF-8 IN	IS <sub>ad</sub>








### J1708 Network Analysis



### J1708 Network Analysis



### J1708 Network Analysis





## The data didn't make sense. Let's figure it out using hacker tools...

- Fuzzing or Black Box Approach
  - Buffer Overflows
  - Low Cost and Minimal Effort
- Static Analysis
  - Decompiled Code
  - Detailed Discovery
  - Time Consuming
- Dynamic Analysis
  - Debuggers
  - System Controls
  - Development Tools





# Passwords from diagnostic software sniffed from memory

SECTION CC LIN	ТЗ	Registers (EPI)
Sabelli CC      In        Sabelli SBEC      Sabelli N        Sabelli SBES      PU        Sabelli SB45      84        Sabelli SB45      84        Sabelli SB52      95        Sabelli SB52      96        Sabeli SB52      96	13 13 13 13 13 13 13 13 13 13	EAX 0027E288 000200003 EDX 00000003 EDX 00000000 EDX 00000000 EDX 00000000 ESF 0027E360 EST 0027E360 EST 0027E360 EST 0027E260 ED 0022332bit 0(FFFFFFF) P 1 CS 0018 32bit 0(FFFFFFFF) P 1 CS 0018 32bit 0(FFFFFFFFF) P 1 CS 0018 32bit 0(FFFFFFFFFF) P 1 CS 0018 32bit 0(FFFFFFFFFF) P 1 CS 0018 32bit 0(FFFFFFFFF) P 1 CS 0018 32bit 0(FFFFFFFFFF) P 1 CS 0018 32bit 0(FFFFFFFFFF) P 1 CS 0018 32bit 0(FFFFFFFFFF) P 1 CS 0018 32bit 0(FFFFFFFFFFFF) P 1 CS 0018 32bit 0(FFFFFFFFFF) P 1 CS 0018 32bit 0(FFFFFFFFFFFFF) P 1 CS 0018 32bit 0(FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
		FON 022F Prec NEAR,53 Mask 1 1 1 1 1
dress (BSCII dump i626452 i626472 i626472 i626482 i626482 i626482 i626482 i626512 i626512 i626529 i626582 i626582 i626582 i626582 i626582 i626582 i626582 i626682 i626888 i6268888 i6268888 i6268888 i626888 i6268888 i6268888 i6268888 i6268888 i6268888 i6268888 i6	ion Config Fi duction Confi duction Confi duction Confi dection Confi d	0827154EL    08272EL20      0827154FL    02000000      0827154FL    02000000      0827154FL    0000000      0827154FL    00000000      0827154FL    000000000      0827154FL    000000000      0827154FL    000000000000      0827154FL    000000000000000000      0827154FL    0000000000000000

## Epiphany #5: Digital forensics and cybersecurity go hand-in-hand

43

## Disassembling the Communication Protocol

Communications Keys

Assembly Language for Message Encoding

mov	c1, 84h
mov	[ebp+var_1A], cl
mov	[ebp+var_6], cl
mov	ecx, [ebp+key]
xor	eax, eax
push	ebx
mov	[ebp+var_2C], 7D5CAB19h
mov	[ebp+var_28], 1B9691EDh
mov	[ebp+var_24], 78A2B78Bh
mov	[ebp+var_20], 0B5E897Ah
mov	bl, 4Dh



Source: Johnson, J. "A FORENSICALLY SOUND METHOD FOR EVIDENCE EXTRACTION FROM HEAVY TRUCK ECMS", The University of Tulsa, 2014

#### **Recovered Speed Data** Recovered Snapshot Speed Record Break out data in the frames and find the Speed data

### Instrumentation for Comparison





46

## Heavy Vehicle Event Data Recorder Data Forensics

Customers are crash investigators, both private and law enforcement



(12) United States Patent Daily et al.

- (54) WHEELED VEHICLE EVENT DATA RECORDER FORENSIC RECOVERY AND PRESERVATION SYSTEM
- (71) Applicant: The University of Tulsa, Tulsa, OK (US)
- Inventors: Jeremy Daily, Broken Arrow, OK (US); James Johnson, Tulsa, OK (US);
   Andrew Kongs, Tulsa, OK (US); Jose Corcega, Broken Arrow, OK (US)
- (73) Assignee: The University of Tulsa, Tulsa, OK (US)

(10) Patent No.:	US 9,865,102 B2
(45) <b>Date of Patent:</b>	Jan. 9, 2018

- (58) **Field of Classification Search** CPC ...... G07C 5/08; G06F 17/00; G06F 19/00 See application file for complete search history.
- (56) **References Cited**

#### U.S. PATENT DOCUMENTS

2002/0145666 A1 10/2002 Scaman et al. 2010/0250053 A1 9/2010 Grill et al. (Continued)

EODEICN DATENT DOCUMENTS





## Epiphany #6: There is a market for vehicle digital forensics.

There's a huge black market for cybersecurity exploits.

50

### Some Crashes Leave No Data To Recover



51

### Epiphany #7: There are 10 types of engineers in this world: Those that understand binary and those that don't.



## We never want cyberattacks to result in a crash. We need more talent.



54

## Summary of Epiphanies:

- 1. Humans are pretty good at recognizing patterns.
- 2. Understanding the vehicle network is critical to forensics.
- 3. Messing around with vehicle networks is fun.
- 4. Students like hand-on vehicle networking projects.
- 5. Digital forensics and cybersecurity go hand-in-hand.
- 6. There is a market for vehicle digital forensics.
- 7. Some people don't understand binary.

## Don't Design Systems Like This...



https://images.app.goo.gl/V3tQ3c8TYkpECKBEA

## Thank you Questions?



Username : admin Password : admin

## **SPAN-** Path to SE





ystems Thinking and Model Based Systems Engineering's Utility to Solve Complex anizational Problems - Cyber-Physical Systen Design Teams



CAPT MARTIN SPAN III



## A Systems Thinking Approach to Eliciting Cybersecurity Requirements for an Electric Snowmobile

Martin "Trae" Span

Dr. Jeremy Daily

**Colorado State University** 

October 2, 2022

2022 INCOSE Western States Regional Conference – Golden, CO Copyright © 2022 by Martin Span. Permission granted to INCOSE to publish and use

### Simplified System Architecture Overview



### IEEE SYSCON – Autonomous Flight System Architecture





Systems Thinking and Model Based Systems Engineering's Utility to Solve Complex Organizational Problems - Cyber-Physical System Design Teams

Martin "Trae" Span, Shwetha Gowdanakatte, Jeremy Daily, Indrakshi Ray, Kamran Eftekhari Shahroudi Colorado State University Fort Collins, CO, USA

## Motivation



Username : admin Password : admin

https://www.google.com/url?sa=i&url=https%3A%2F%2Ftwitter.com%2Fjosephsteinberg%2Fstatus%2F1091363160446 169092%3Flang%3Dhu&psig=AOvVaw0Mg37O-

AIUgSDK7edFPACJ&ust=1666637222730000&source=images&cd=vfe&ved=0CA4QjhxqFwoTCljlyM6B9\_oCFQAAAA AdAAAABAi

The cybersecurity program you want to run



The cybersecurity program you're forced to run on your current budget



https://www.balbix.com/blog/top-10-cybersecurity-memes/



https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.lanworks.com%2Fcyber-attack-ransomware-emergency-

response%2F&psig=AOvVaw3cyi5WY0kV6KRS9nE2FFBe&ust=1666637129764000&so urce=images&cd=vfe&ved=0CA4QjhxqFwoTCLjZpKKB9\_oCFQAAAAAdAAAAABAE

## **Problem Introduction**

- Shift from Mechanical to Software based functionality [1]
- Cyber Physical Systems Vehicles, Airplanes, Weapons Systems
  Vulnerable to Cyber Attacks: [2], [3], [4], [5]
  - <u>https://youtu.be/RZVYTJarPFs</u>
- Acknowledged need to improve Cybersecurity by *Design* 
  - ISACs for Vehicles [6], NDAA requirements for weapons systems [7]
- Need to Improve Requirements Elicitation Process for Security
  - Failure of checklist approach[8]— limits functionality and design trade space
- System Theoretic Process Analysis (STPA) [9], [10], [11]
  - Top-Down Systems Approach







## GAO 2021 Report on Weapon System Cybersecurity

- Contracting for cybersecurity **requirements** is key.
- DOD guidance states that these requirements should be treated like other types of system requirements
- Specifically, cybersecurity requirements should be defined in acquisition program contracts, and criteria should be established for accepting or rejecting the work and for how the government will verify that requirements have been met.
- GAO found examples of program contracts omitting cybersecurity requirements, acceptance criteria, or verification processes. For example, GAO found that contracts for three of the five programs did not include any cybersecurity requirements when they were awarded.
- A senior DOD official said standardizing cybersecurity **requirements** is difficult and the department needs to

#### key. Since GAO's 201 make its network

What GAO Found

Since GAO's 2018 report, the Department of Defense (DOD) has taken action to make its network of high-tech weapon systems less vulnerable to cyberattacks. DOD and military service officials highlighted areas of progress, including increased access to expertise, enhanced cyber testing, and additional guidance. For example, GAO found that selected acquisition programs have conducted, or planned to conduct, more cybersecurity testing during development than past acquisition programs. It is important that DOD sustain its efforts as it works to improve weapon systems cybersecurity.

Contracting for cybersecurity requirements is key. DOD guidance states that these requirements should be treated like other types of system requirements and, more simply, "if it is not in the contract, do not expect to get it." Specifically, cybersecurity requirements should be defined in acquisition program contracts, and criteria should be established for accepting or rejecting the work and for how the government will verify that requirements have been met. However, GAO found examples of program contracts omitting cybersecurity requirements, acceptance criteria, or verification processes. For example, GAO found that contracts for three of the five programs did not include any cybersecurity requirements when they were awarded. A senior DOD official said standardizing cybersecurity requirements is difficult and the department needs to better communicate cybersecurity requirements and systems engineering to the users that will decide whether or not a cybersecurity risk is acceptable.



Source: GAO analysis of DOD information. | GAO-21-179

## Gabe Salinger

Why SE?

- Good middle ground between Mechanical Engineering and Management
- Saw the application of SE in many fields
- Can use it in my AF job

#### At USAFA

- Degree in SE with a focus in Mech
- AFSC is Pilot
- Received a fall-out GSP slot in April
- Was approved by AFIT to attend a civilian institution
- Selected CSU



## Cont.

Grad School (CSU):

- Dr. Daily is my research advisor (and source of funding)
- Receiving a Master's of Science in Systems Engineering
  - Total of 30 credits (24 credits of classes, 6 credits of research)
  - One completed and defended thesis (75-100 pages)

This Semester:

- Taking three classes
  - Fundamentals of Systems engineering
  - Program and Project Management
  - Aerospace Actuation Systems
- Assisting with research under Dr. Daily



## Questions?



## Thank you



Grad School/Open Discussion



## Characterization of the Problem Space

Current problems with CPS Design Teams: Lack of systems thinking mindset Minimal adoption of systems thinking principles: Holism: Lack of holistic view of a CPS Evolution: Attackers evolve, but CPS does not Emergence: Security is an emergent property, reductionist approach inadequate Feedback: Vulnerabilities emerge from feedback loops

and delays

## Characterization of the Problem Space using Systems Thinking Models: CPS Design Team



#### CPS Design Team Current State Systems Dynamics Model



Figure 3: Systemic Identification: Causal Loop Diagram showing complexity of CPS Design Team and CPS Security

#### Proposed BDD for more effective CPS Design Team


## Application of Systems Thinking Models for CPS Design Team

