Colorado State University

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?

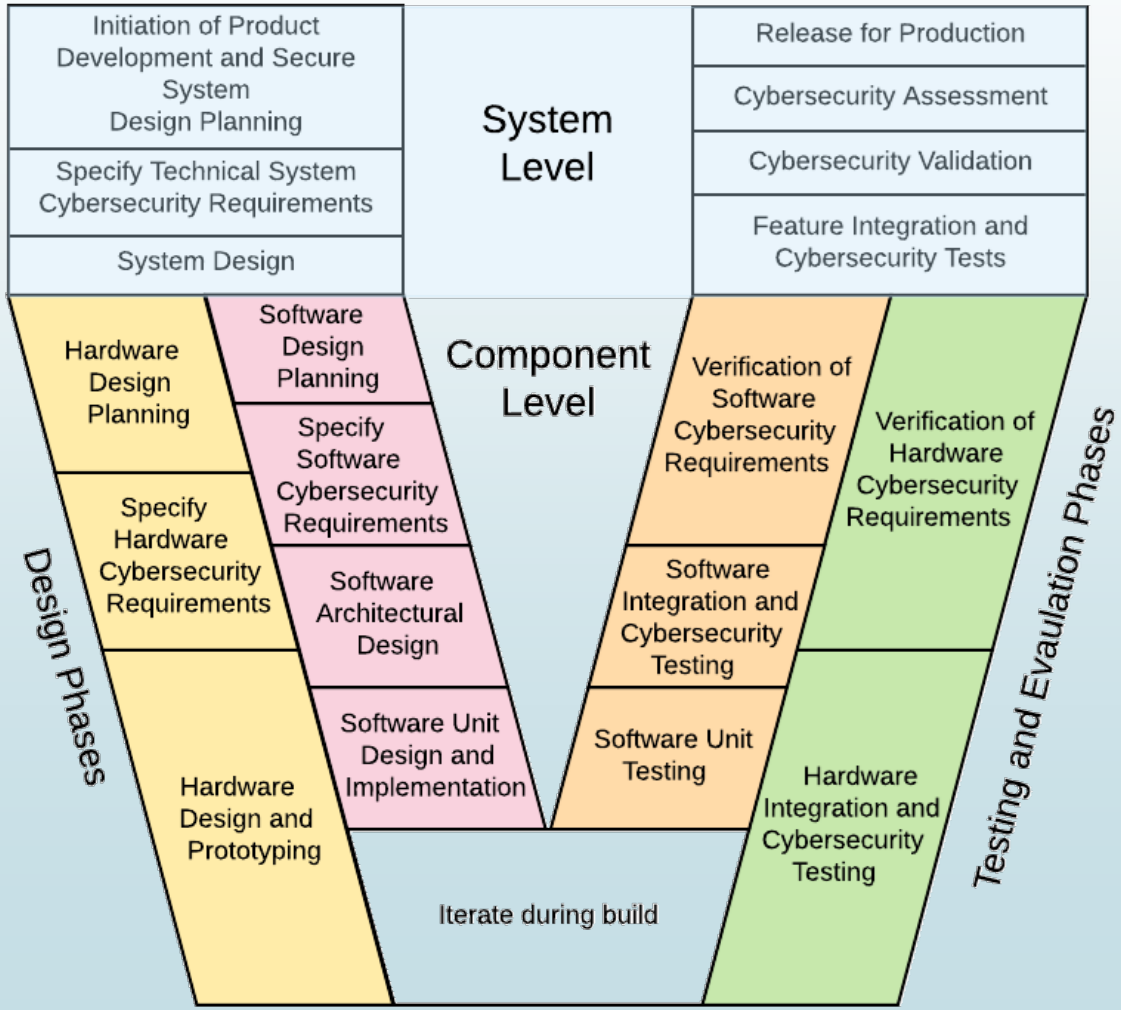
Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use. (https://www.us-cert.gov/ncas/tips/ST04-001)

- CIA for Data
  - 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 ISO/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. (https://en.wikipedia.org/wiki/Digital_forensics)
- **Forensic soundness** gives reasonable assurance that digital evidence was not corrupted or destroyed during investigative processes whether on purpose or by accident.
  1. 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.

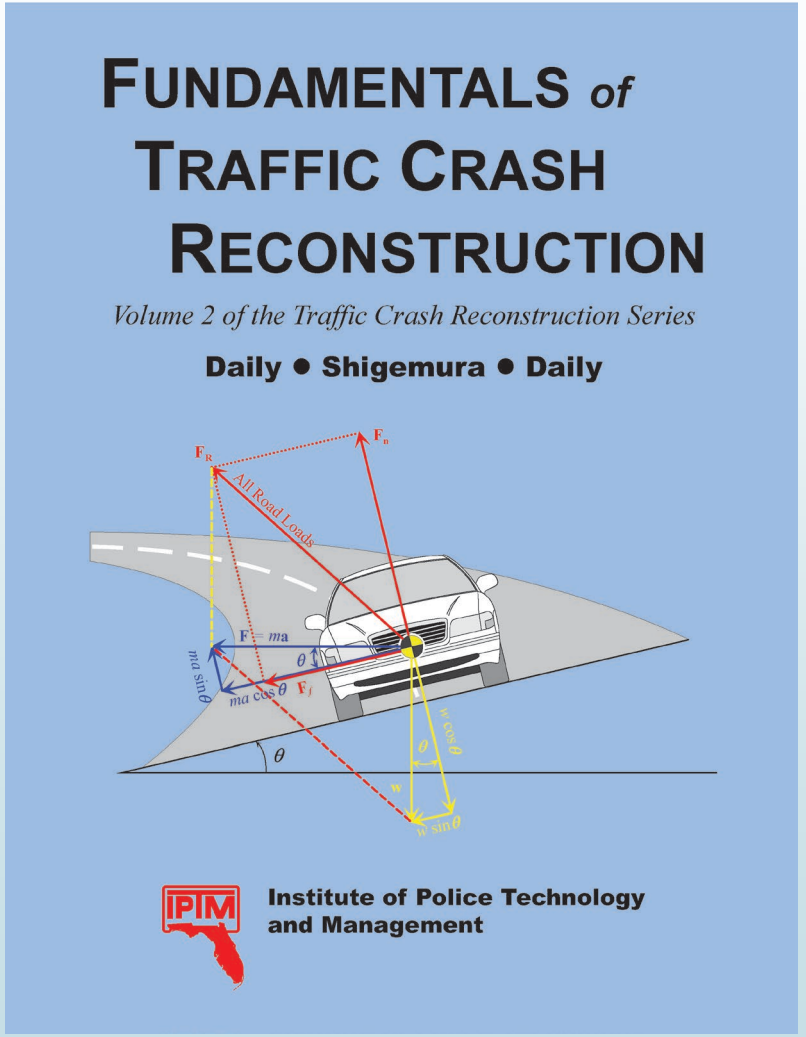
Johnson, J., Daily, J., and Kongs, A., "On the Digital Forensics of Heavy Truck Electronic Control Modules," *SAE Int. J. Commer. Veh.* 7(1):72-88, 2014, https://doi.org/10.4271/2014-01-0495.

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, https://doi.org/10.4271/2020-01-1326.

Origins and Progress

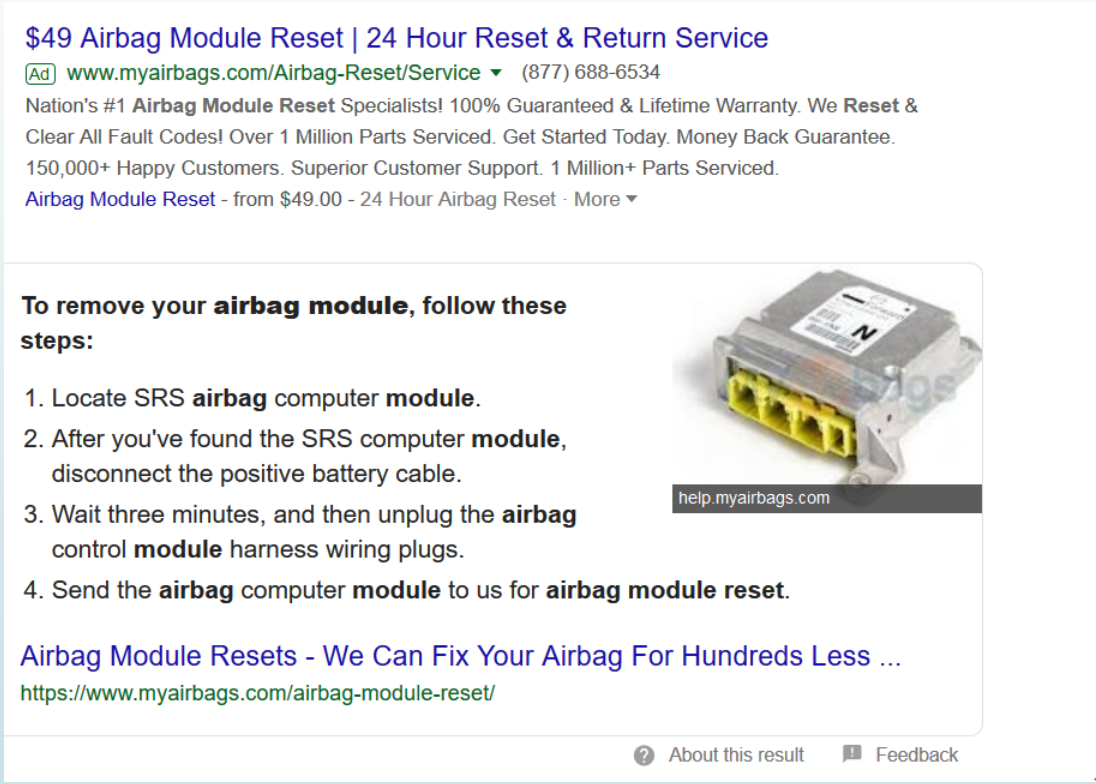
How a mechanical engineer becomes interested in cybersecurity…

- Interest in Traffic Crash Reconstruction
  - Wrote the book
  - 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…



Passenger Vehicle Air Bag Module Data

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




The University of Tulsa
Crash Reconstruction
Research Consortium


0
MPH

Crash Testing

THE UNIVERSITY of TULSA
Crash Reconstruction Research Consortium

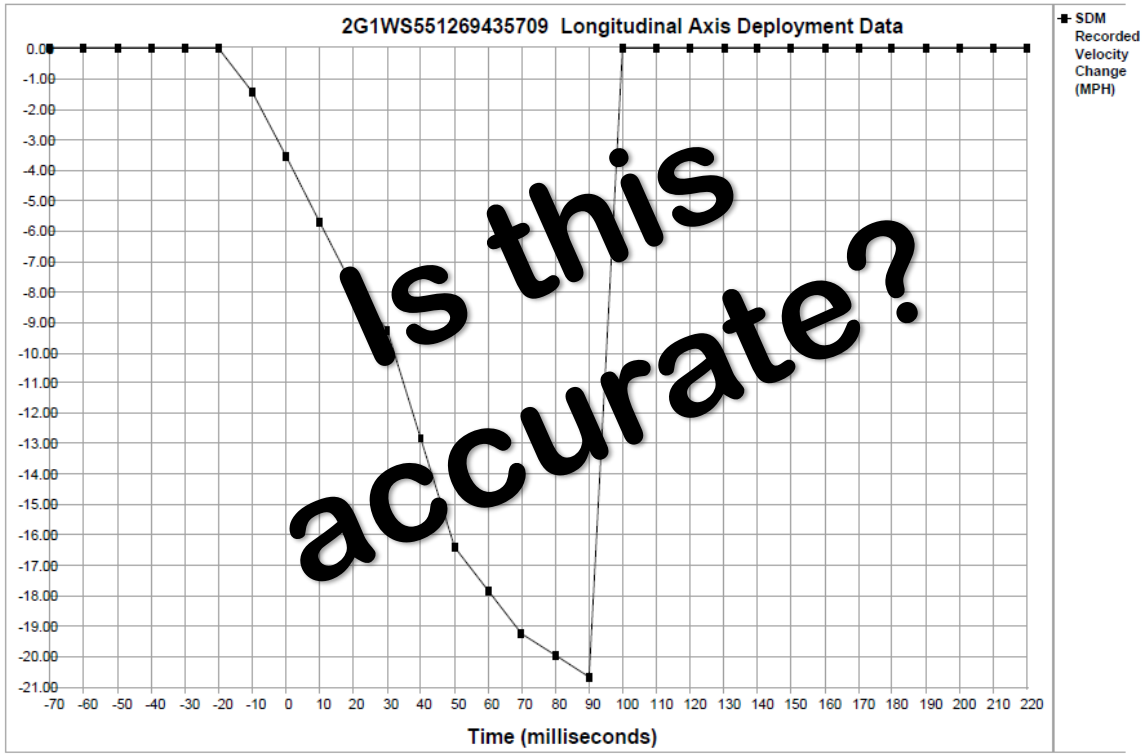
- Understand dynamics of crashes
- Compare instrumented test data to event data recorder information
  - 5 seconds of pre-crash data
  - Crash Delta-V (from accelerometer)

Strategy:

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

BOSCH

CDR CRASH DATA RETRIEVAL

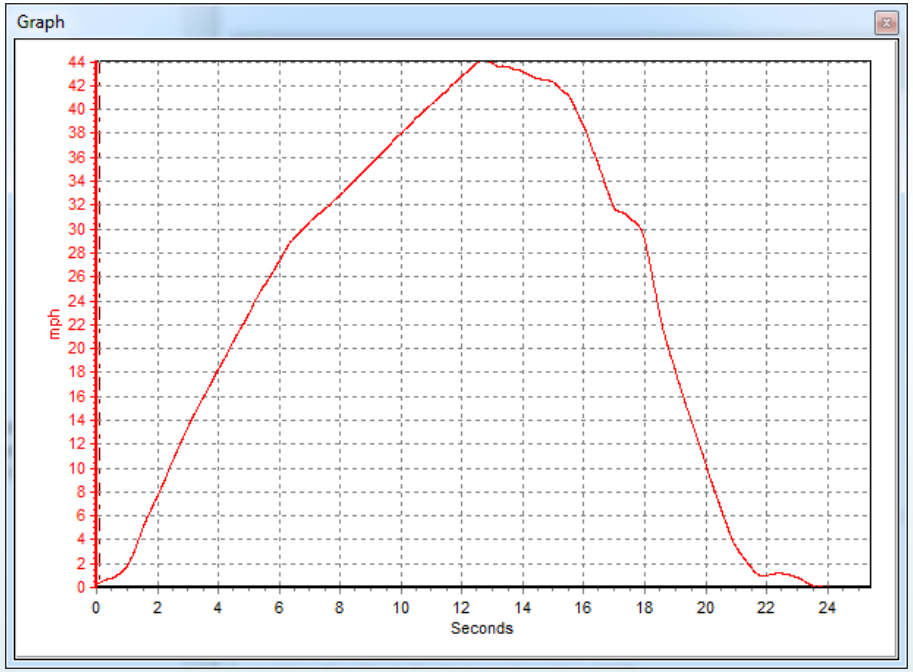


Typical crash data from an airbag module.

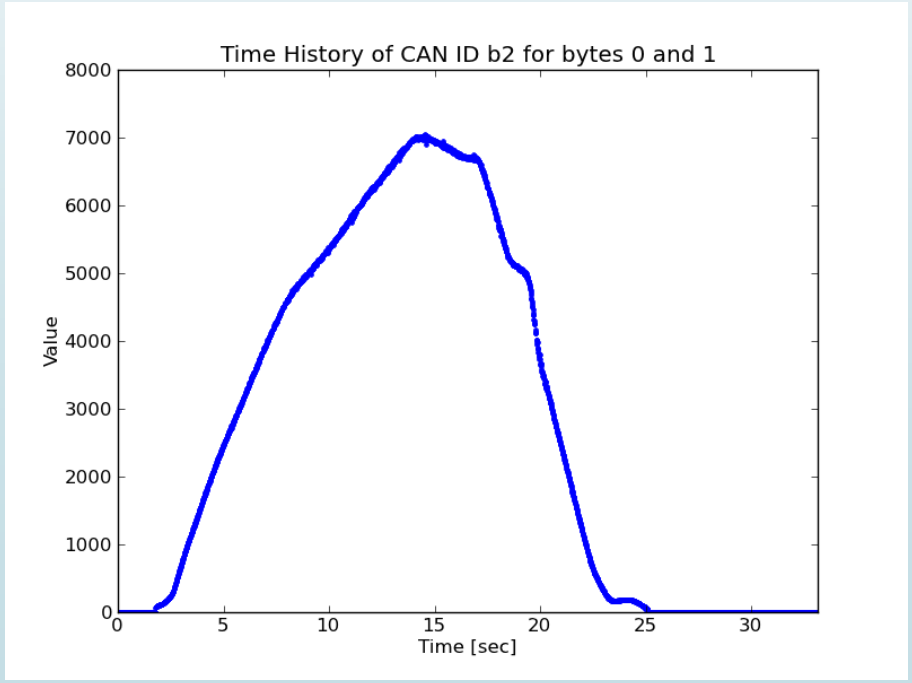
CAN Bus Reconnaissance

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

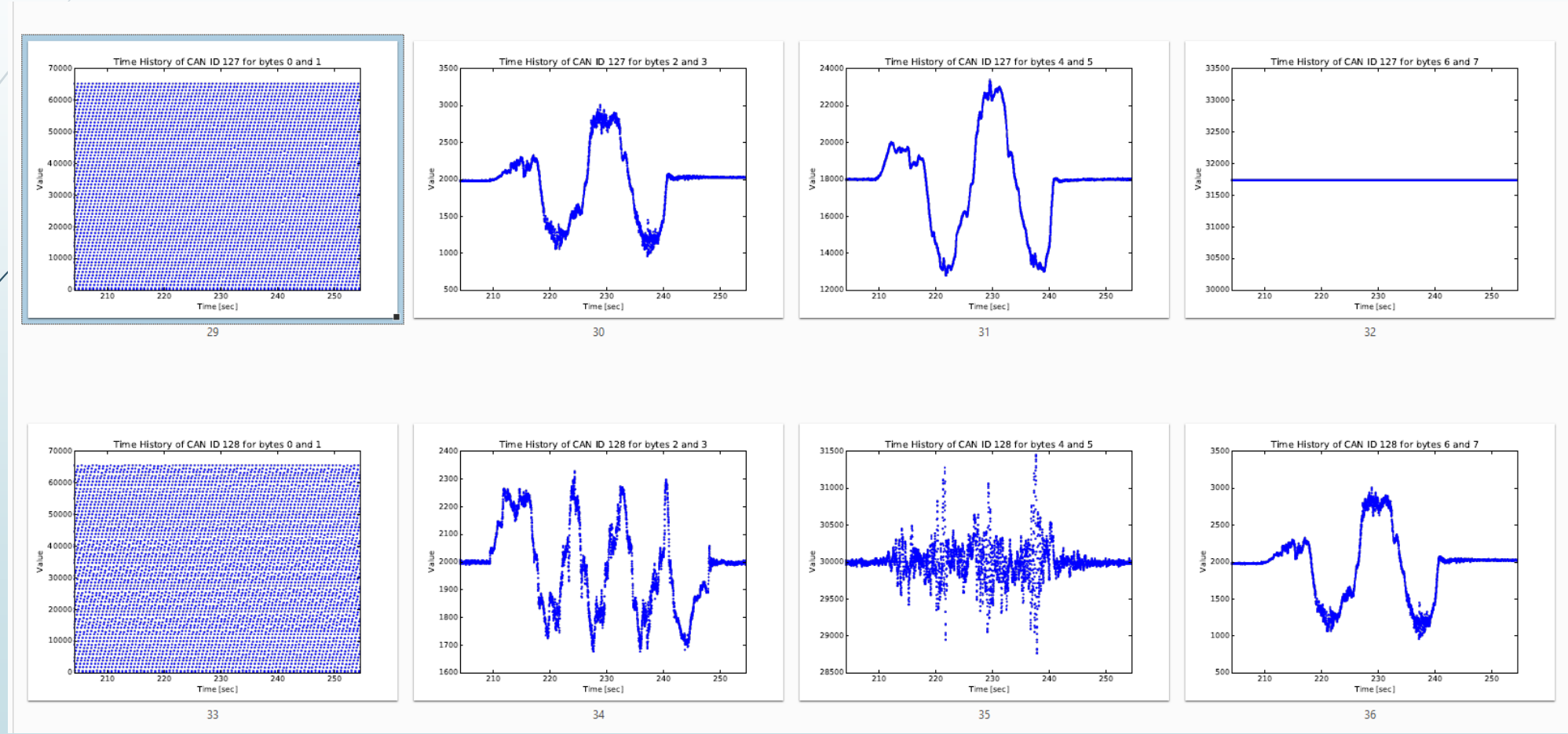


Network Traffic



Manual pattern recognition

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

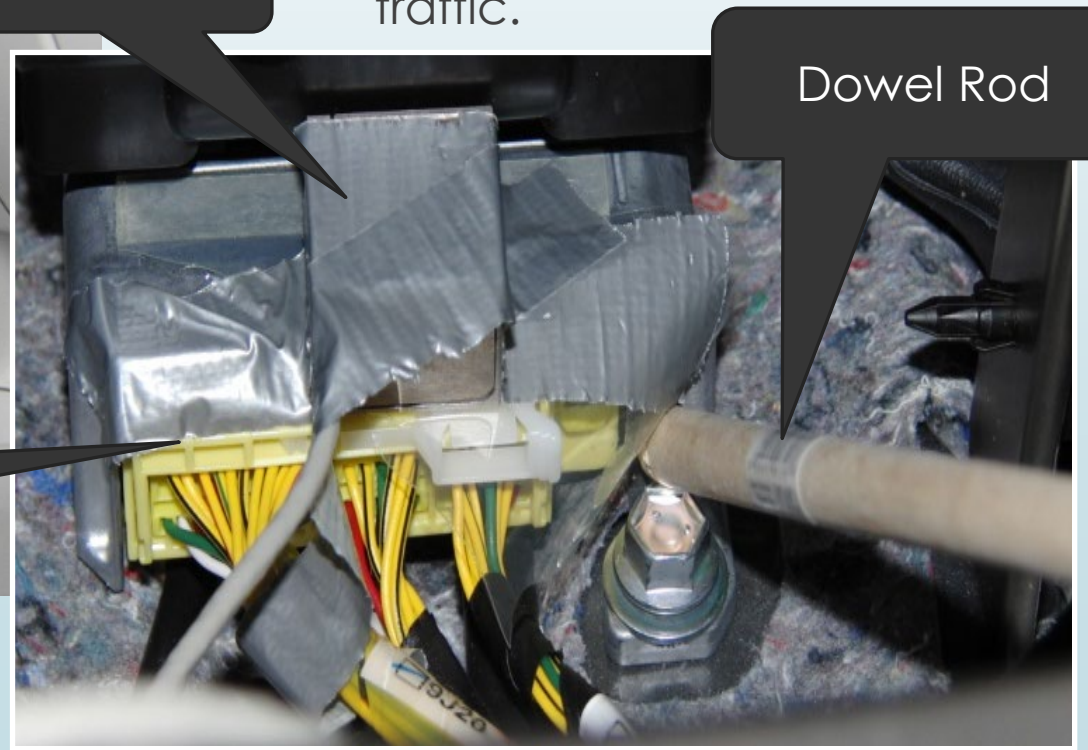


Maybe a machine can do this for us now…

Epiphany #1:
Humans are pretty good at recognizing patterns

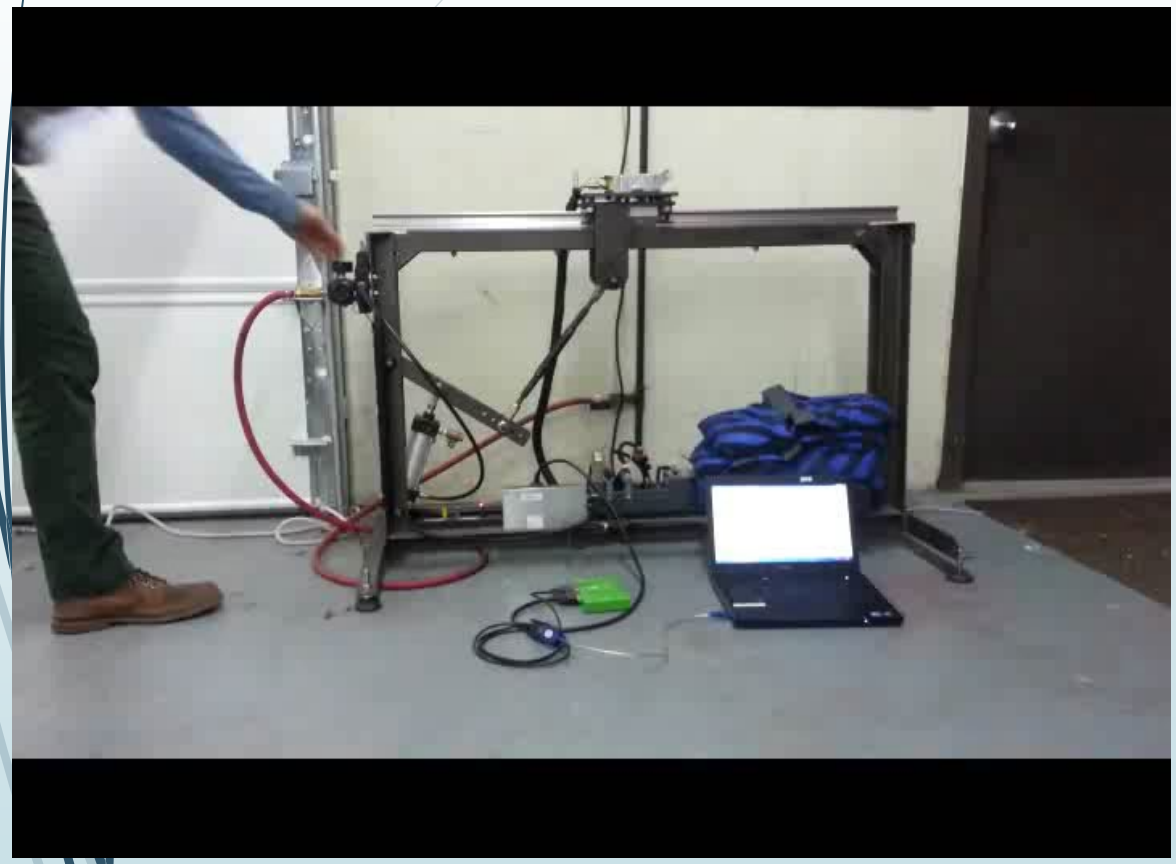
Mechanical Hacking

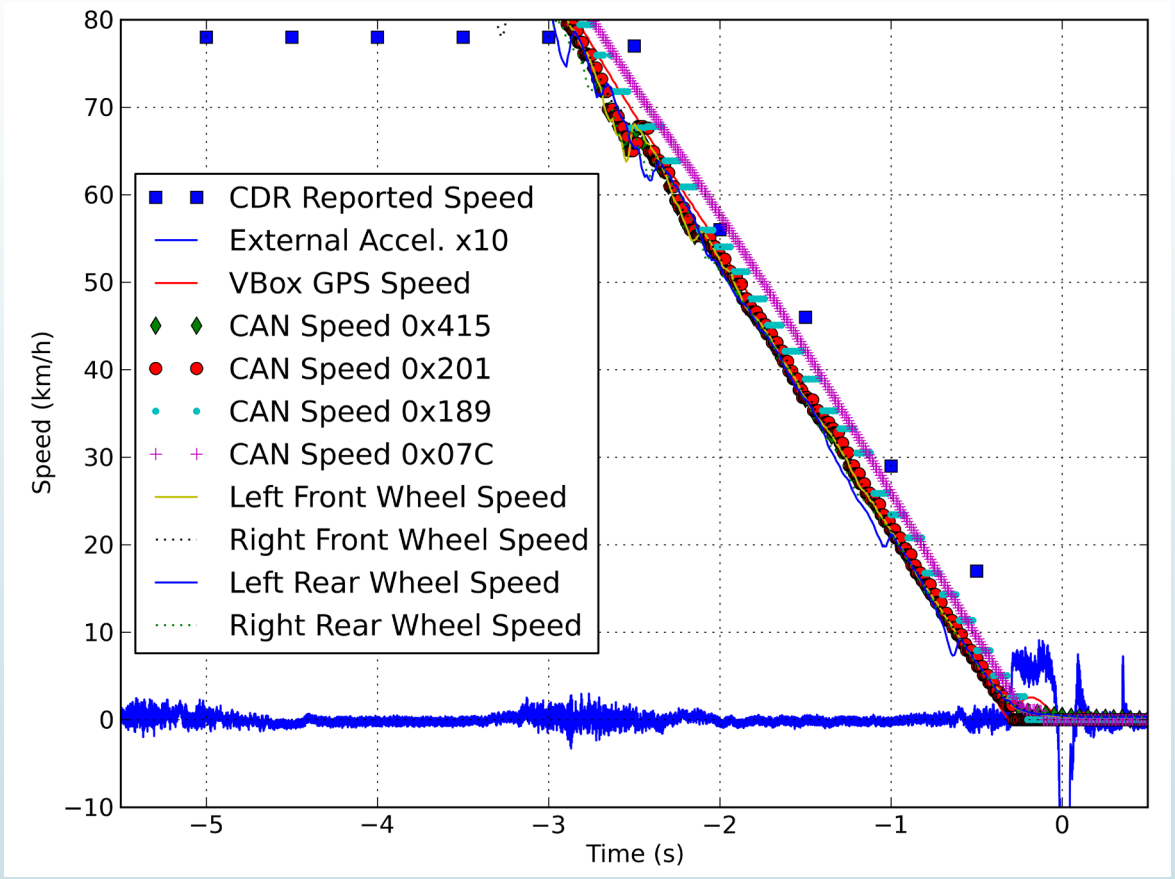
1. Record CAN data while braking hard.
2. Tap the mallet to set non-deployment events in the airbag module.
3. Recover airbag module data and compare to the newly discovered decoding for CAN traffic.



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.

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

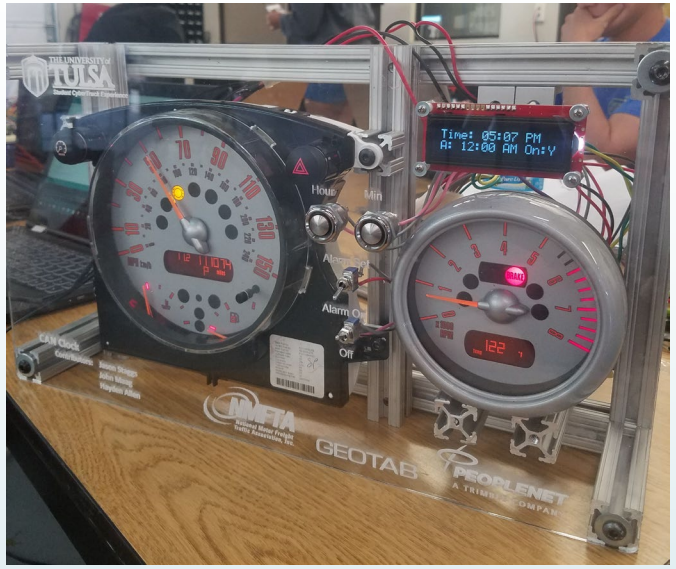
Epiphany #3:
Messing around with vehicle networks is fun!

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

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

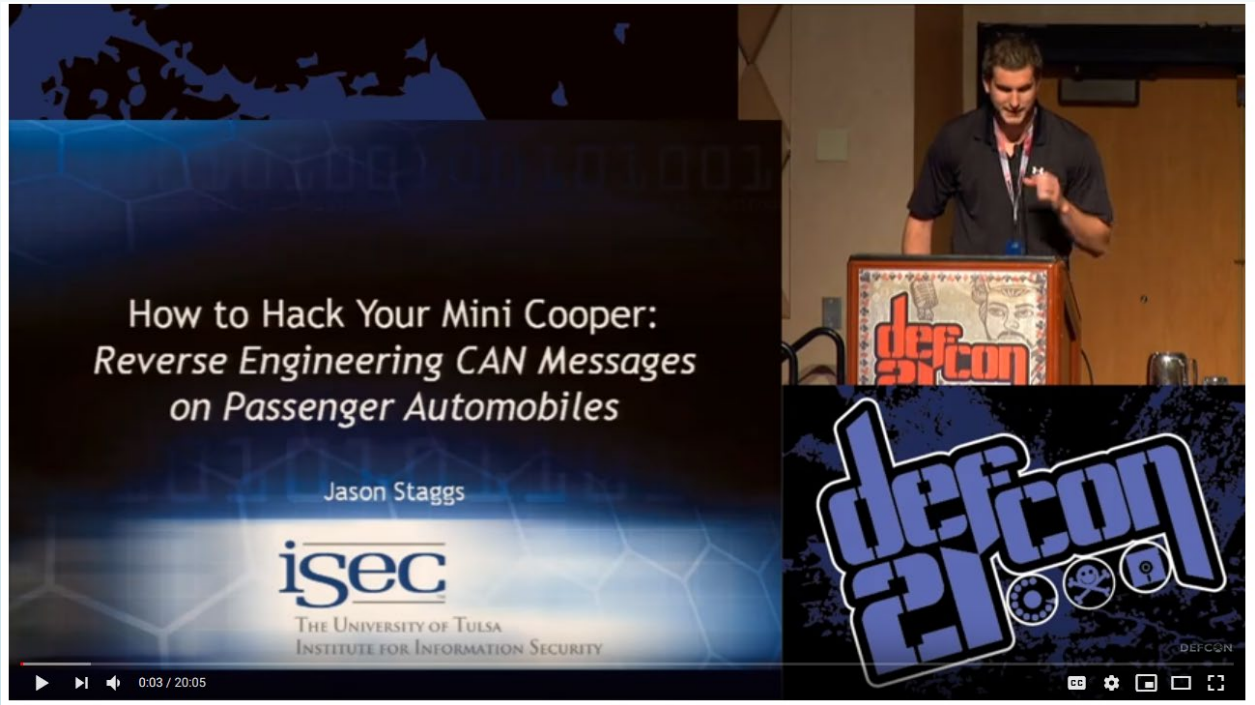
With the advent of modern vehicular technology, the computerized components of passenger vehicles have become increasingly interconnected to facilitate automotive efficiency,

(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



CAN Clock:
Hours on speedometer, minutes on tachometer

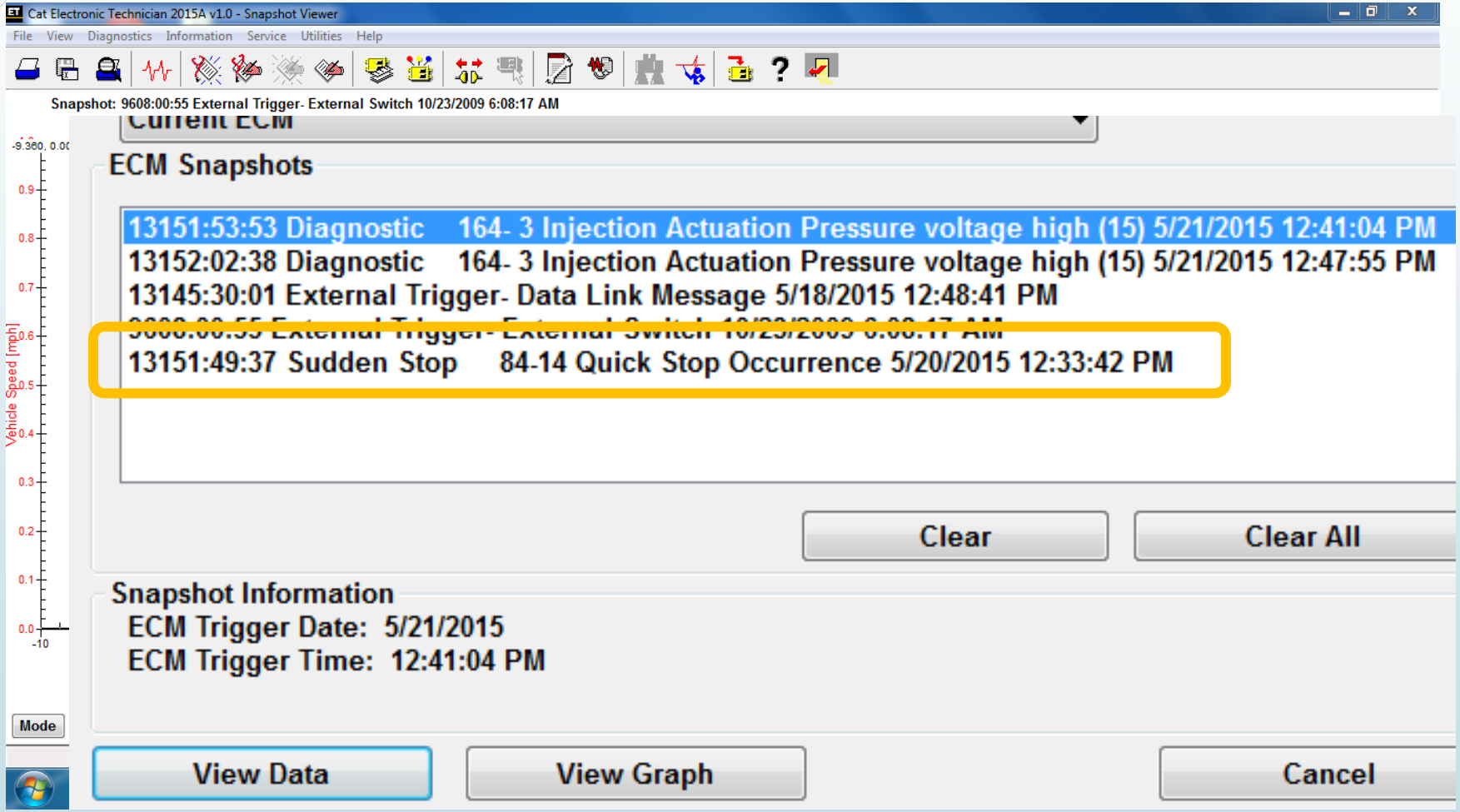
Epiphany #4:
Students like hands-on vehicle networking projects

Example Forensic Recovery

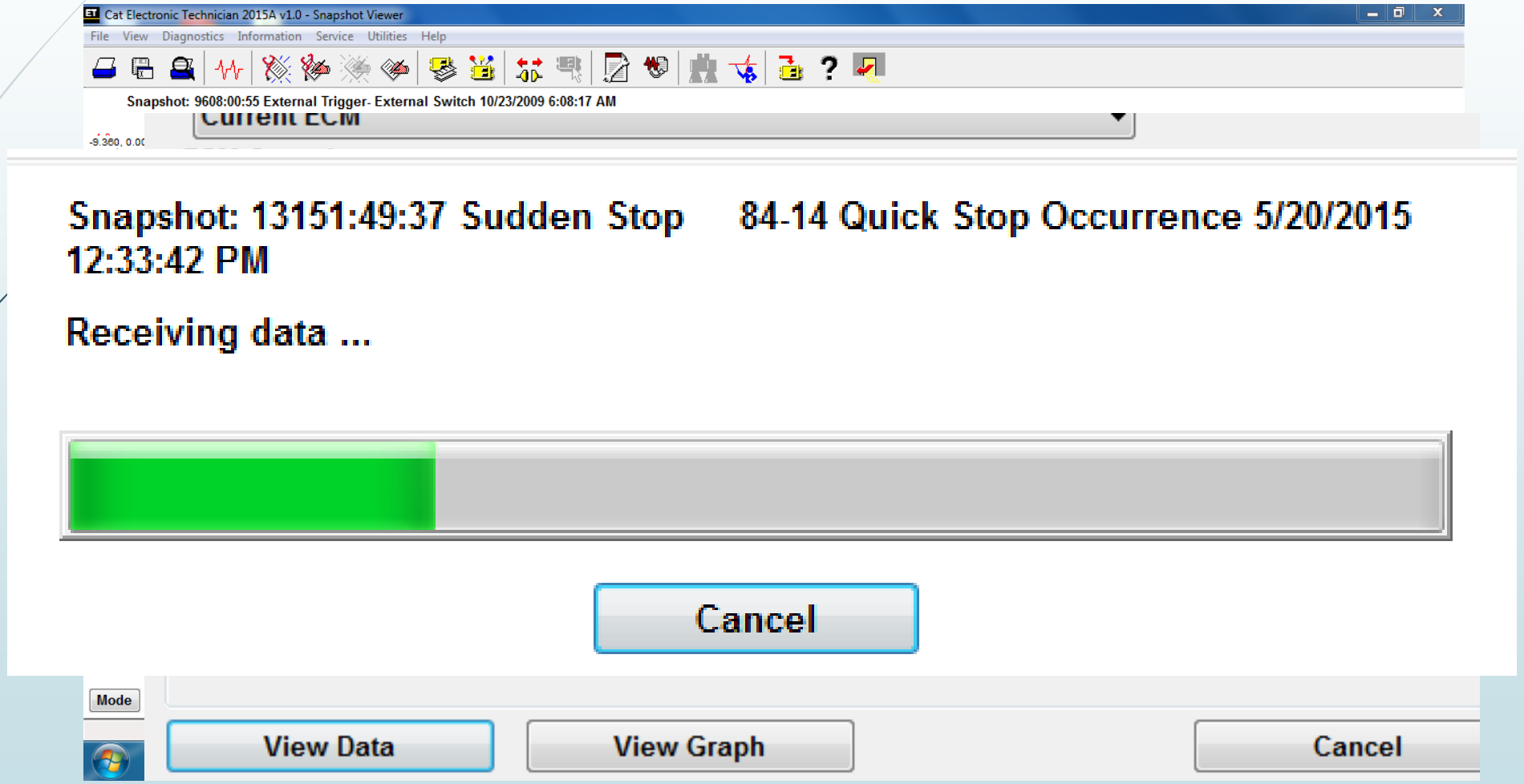
IPTM Special Problems 2015

Transit Bus Vs School Bus

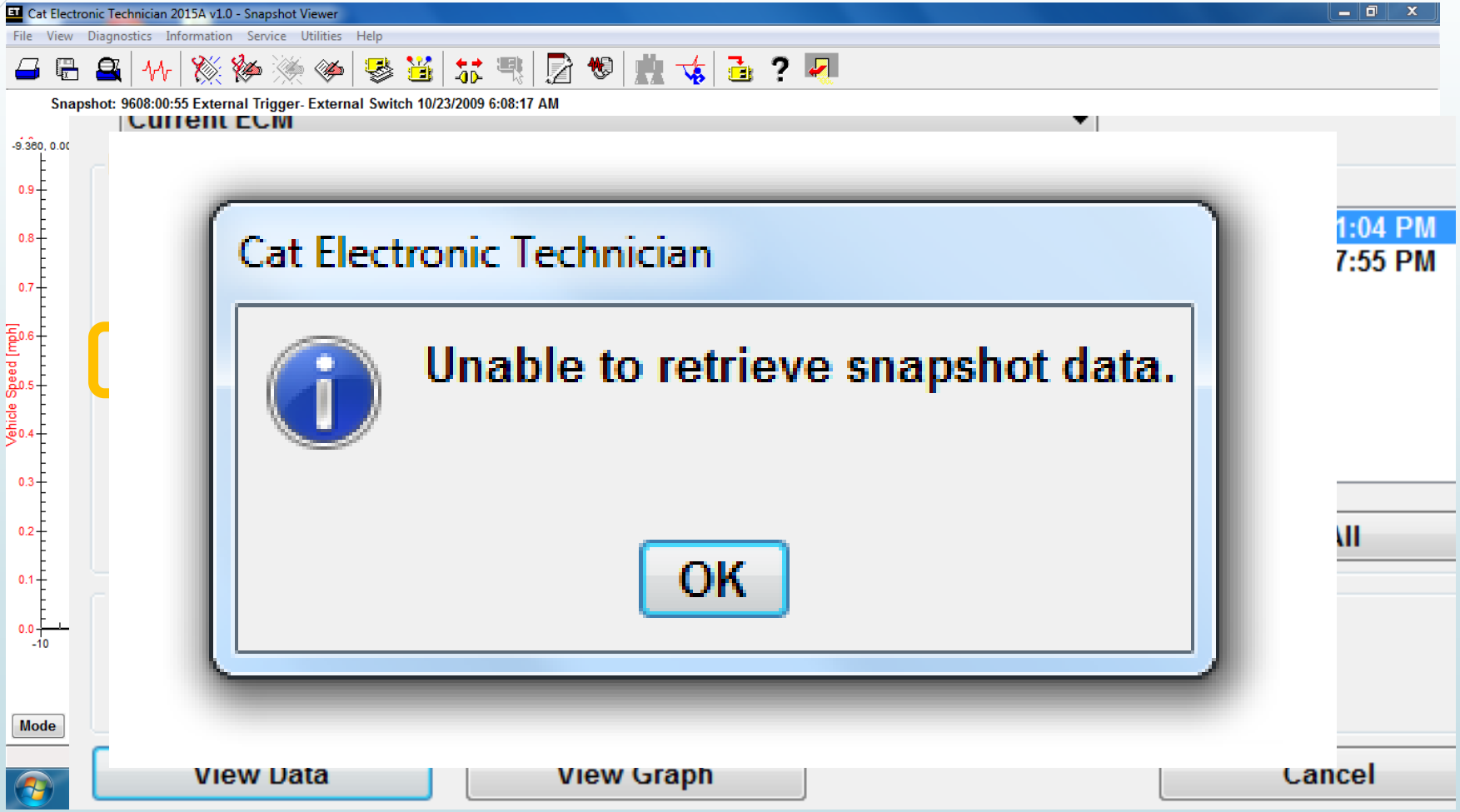
Recovery of Data



Recovery of Data



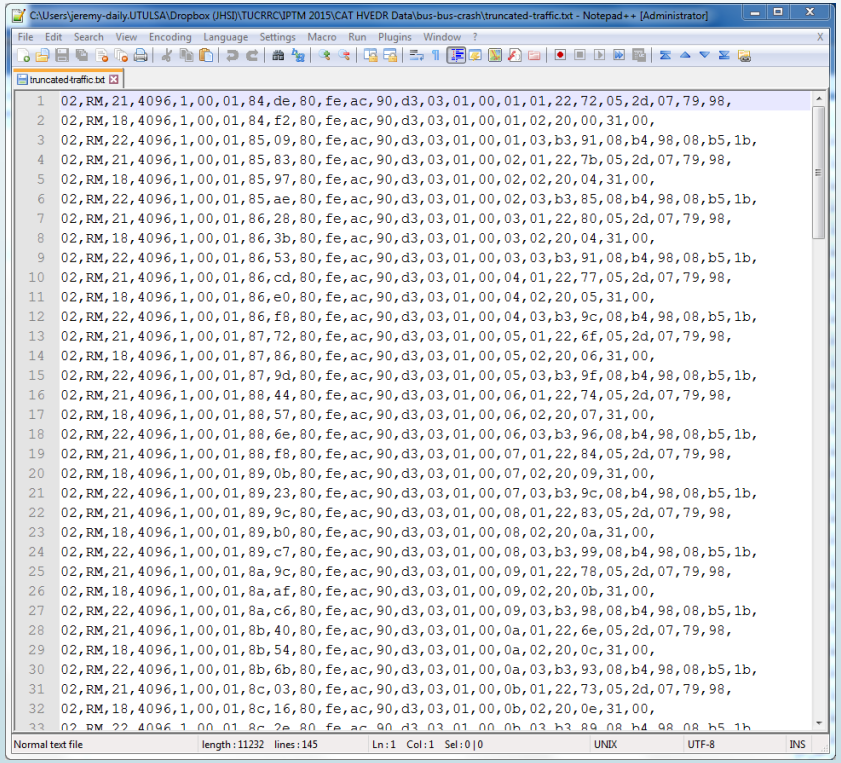
Recovery of Data



But we know data exists!

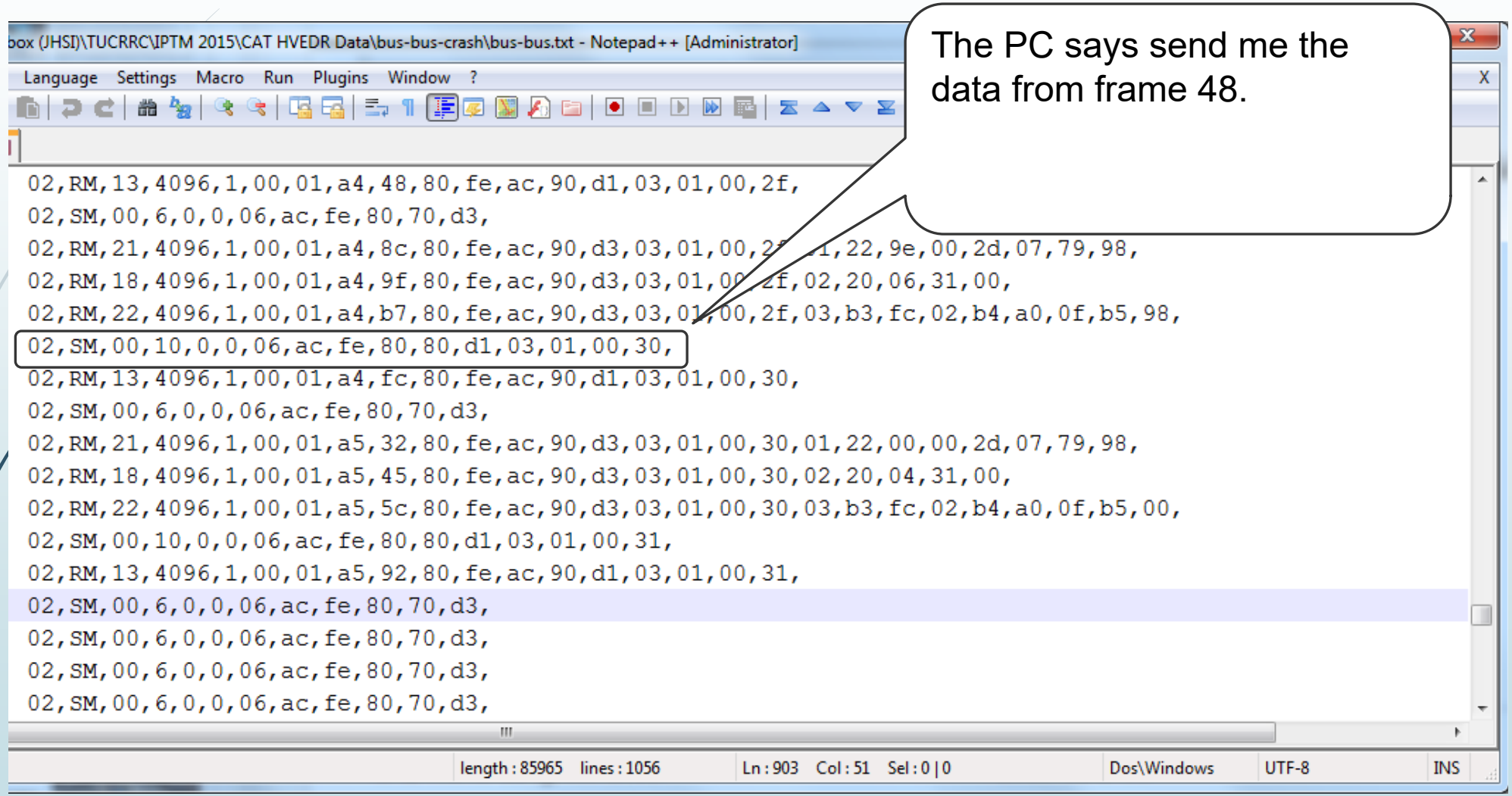
Data Bus was Recorded During the Crash

Network Logs from ET Showed Data for Quickstop



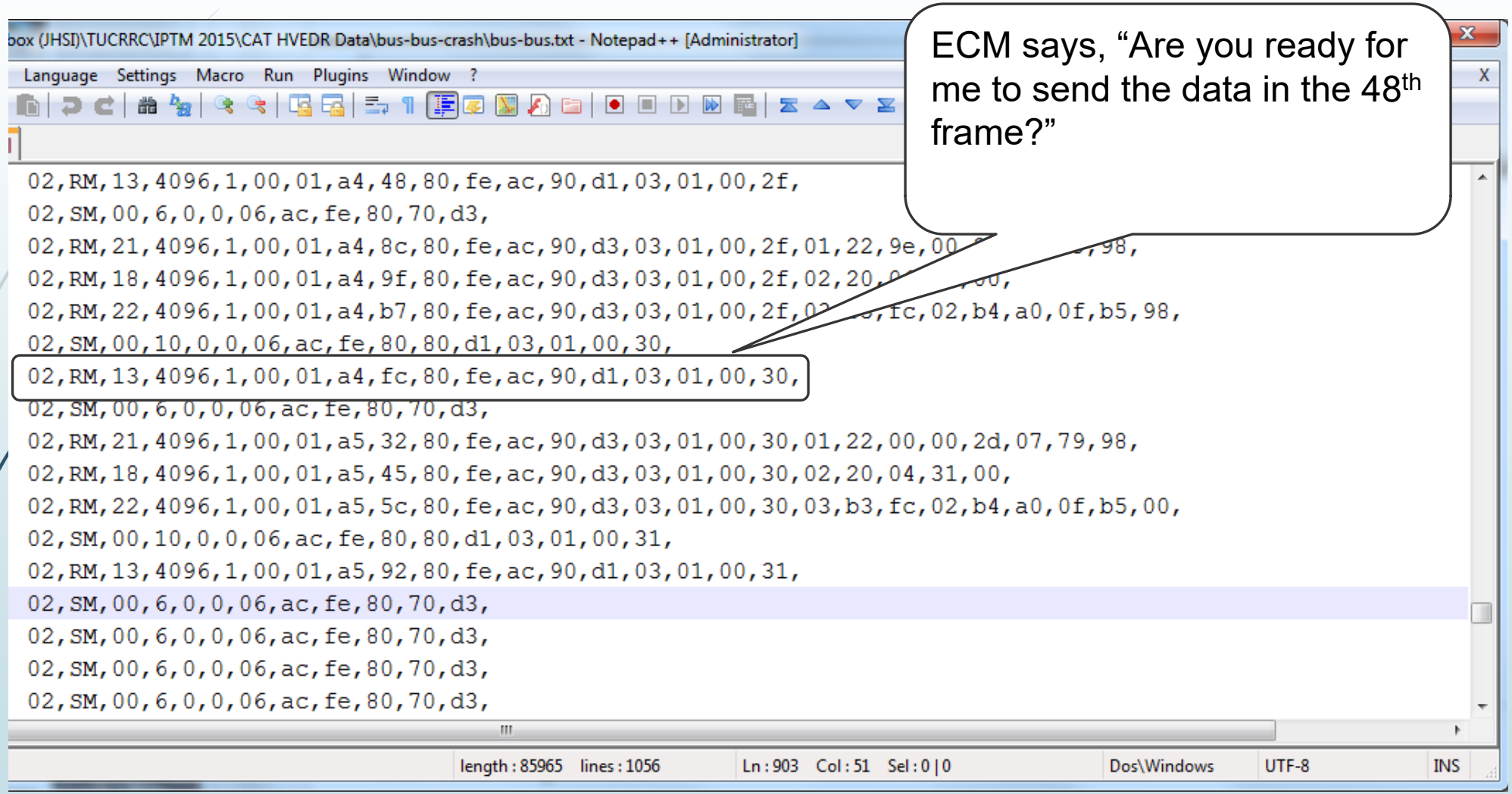
Data Extraction Algorithm

J1708 Network Analysis

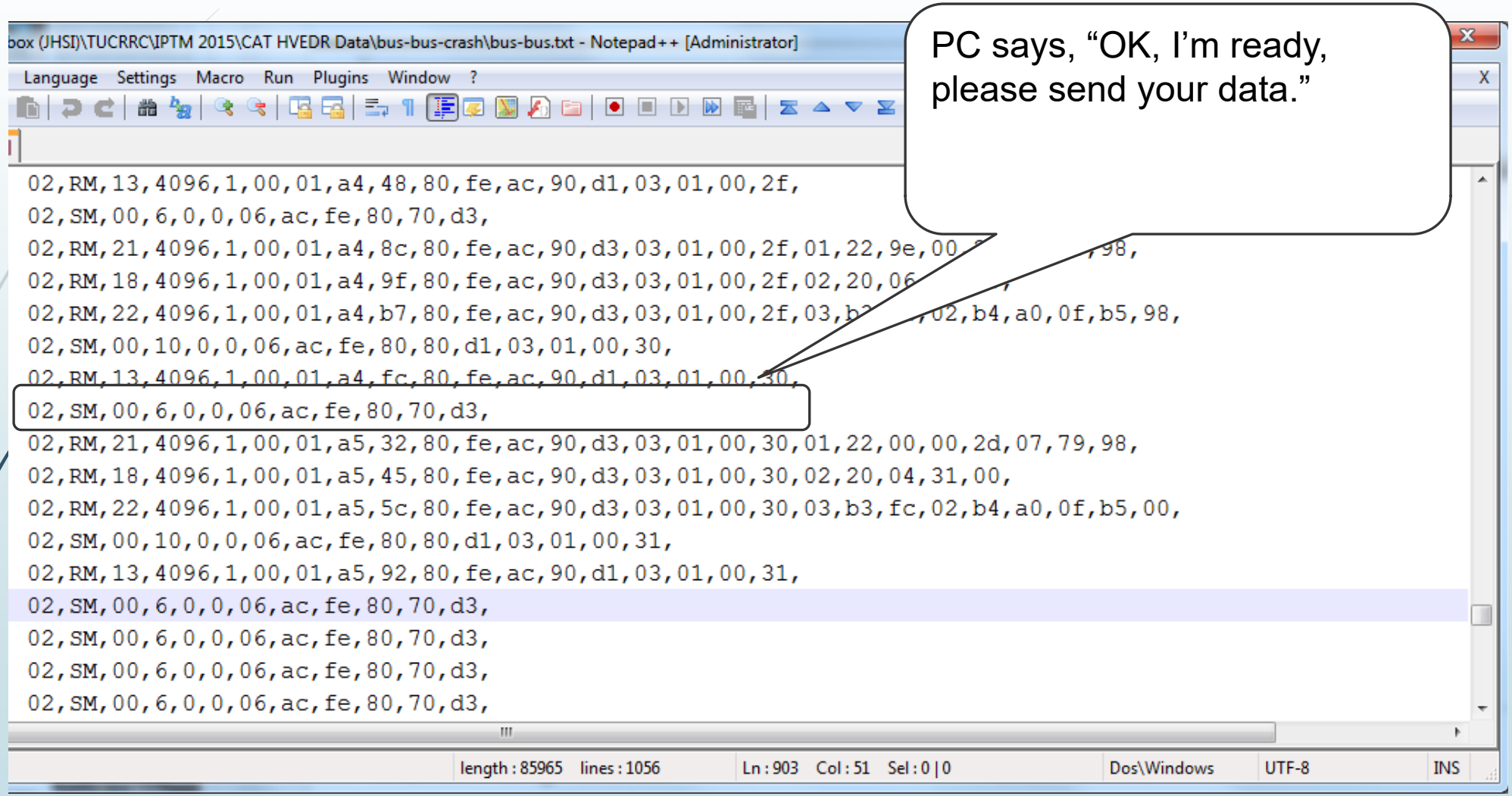


The PC says send me the data from frame 48.

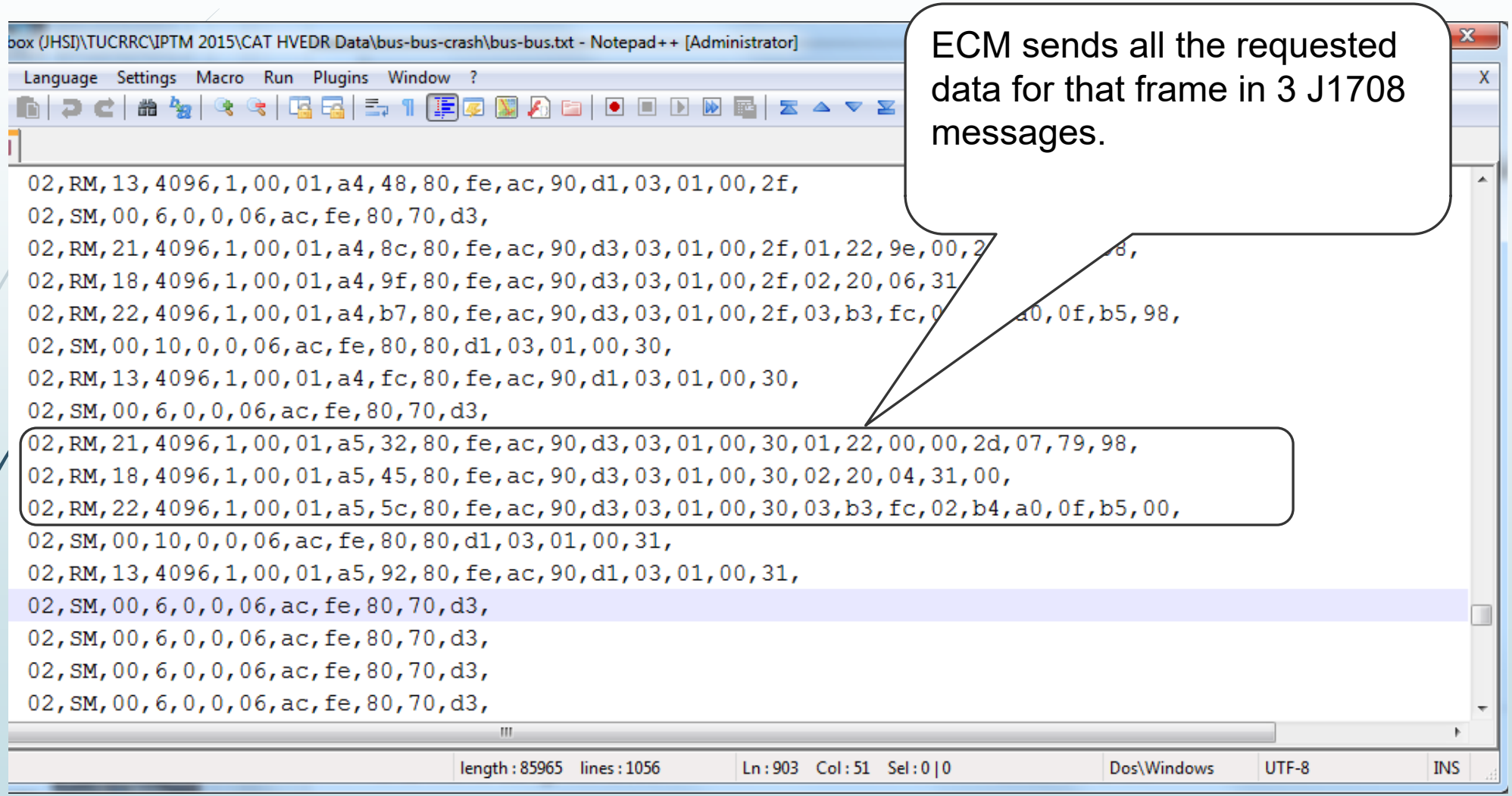
J1708 Network Analysis



J1708 Network Analysis

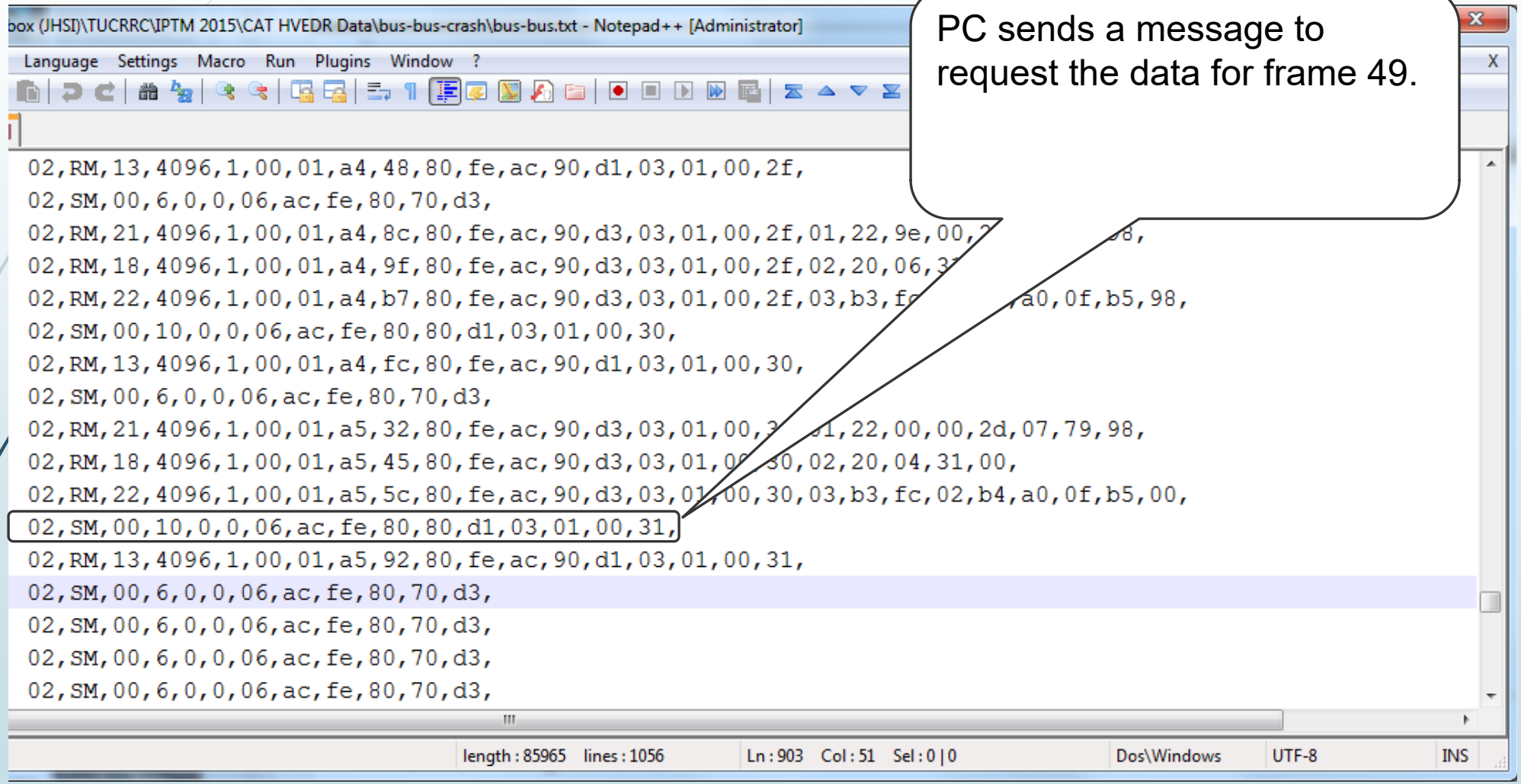


J1708 Network Analysis

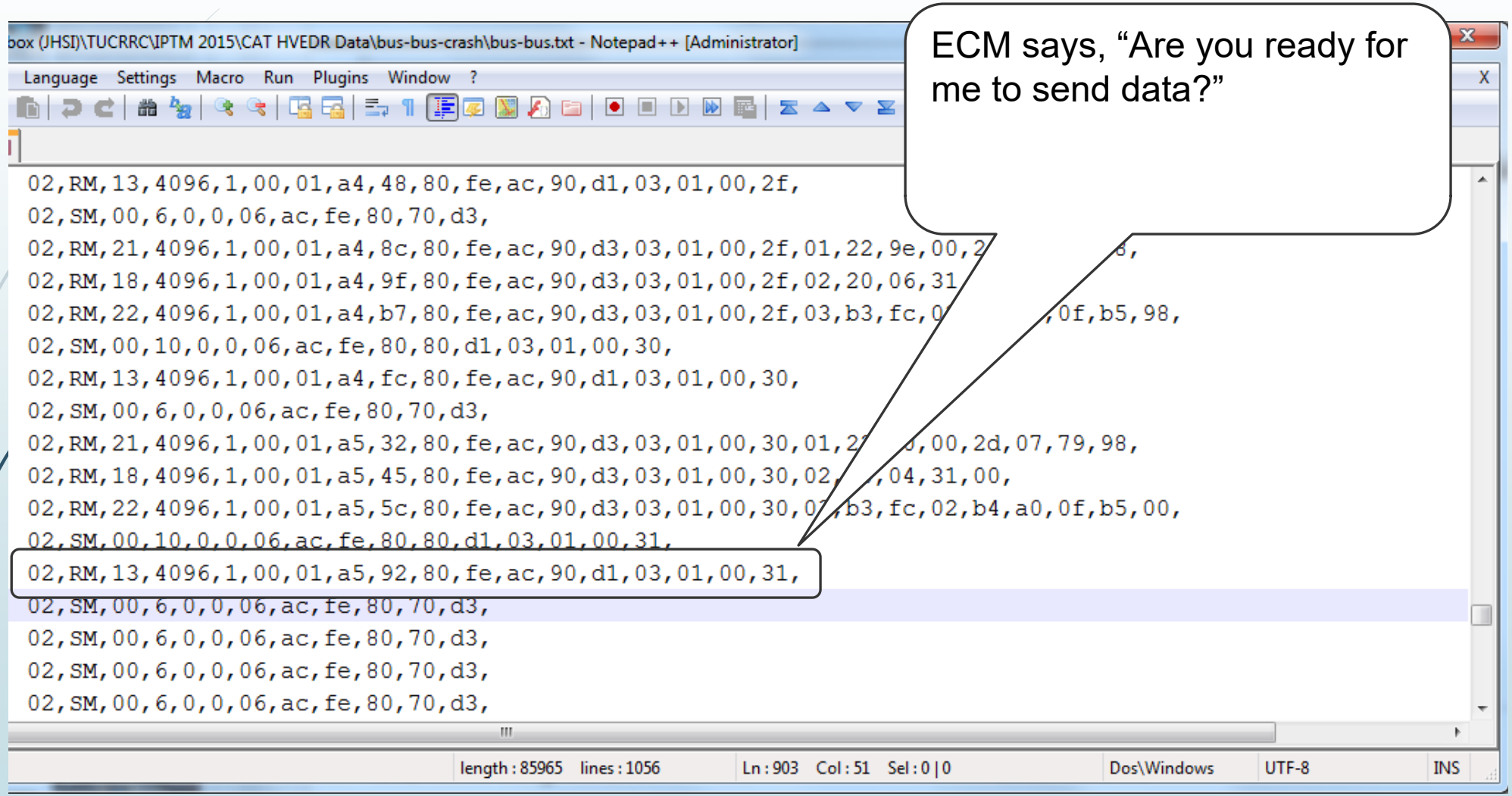


ECM sends all the requested data for that frame in 3 J1708 messages.

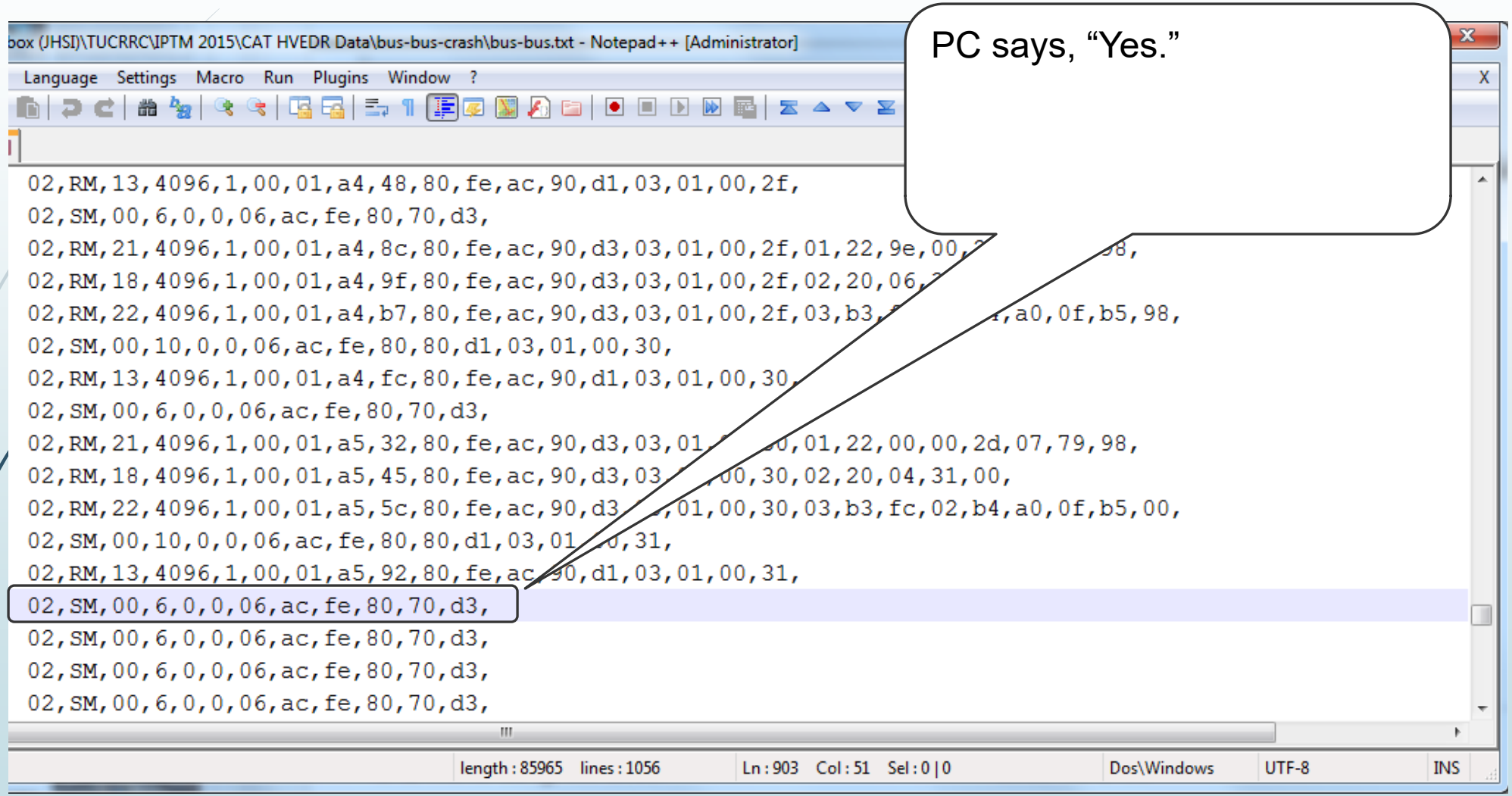
J1708 Network Analysis



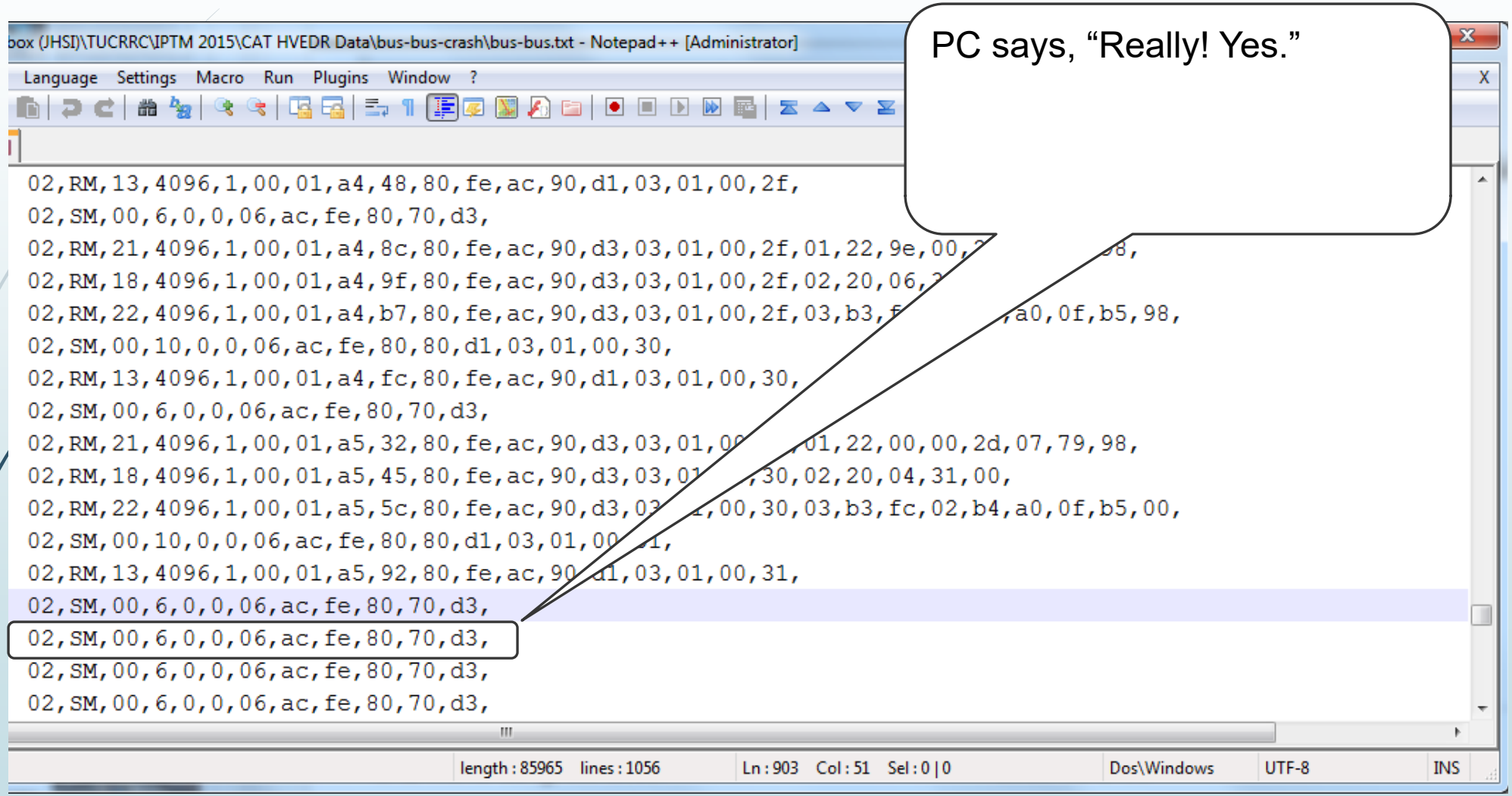
J1708 Network Analysis



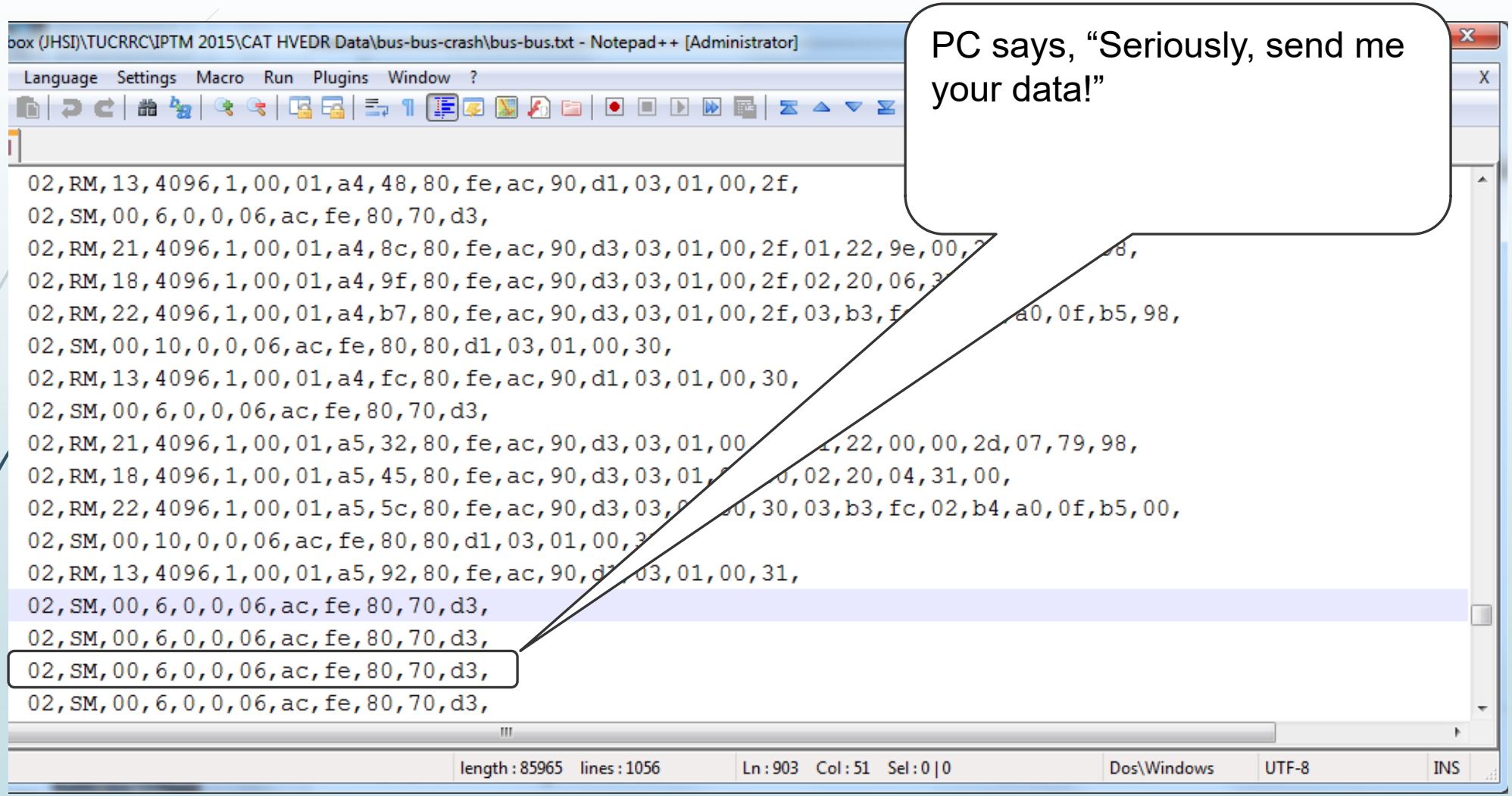
J1708 Network Analysis



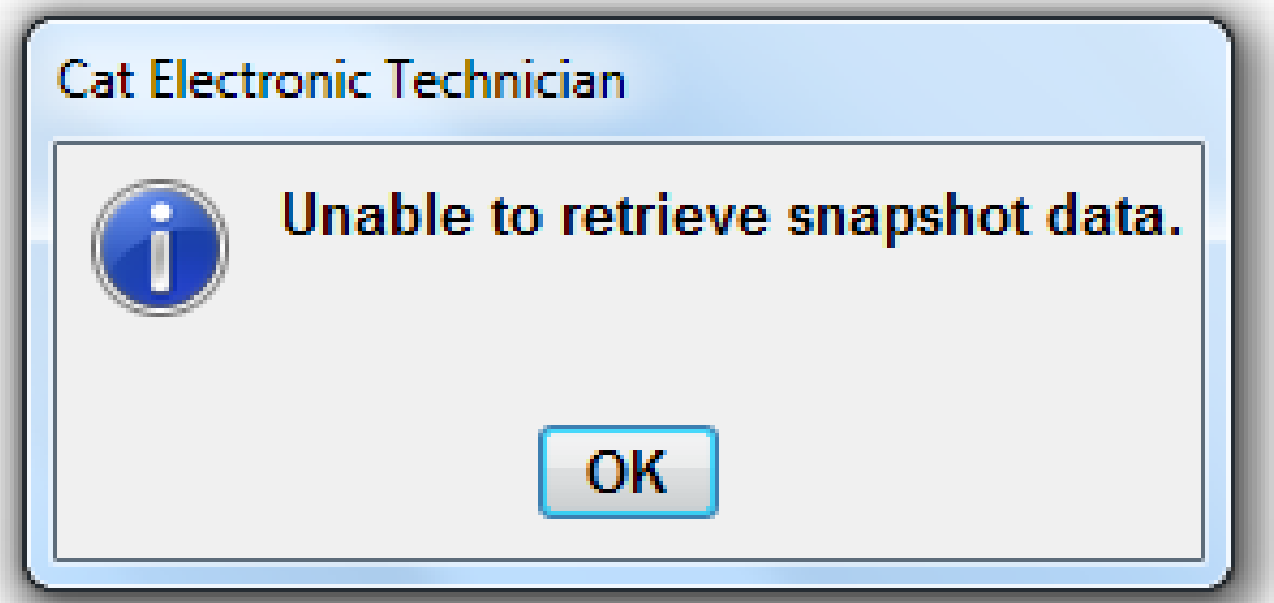
J1708 Network Analysis



J1708 Network Analysis



PC says, “Seriously, send me your data!”

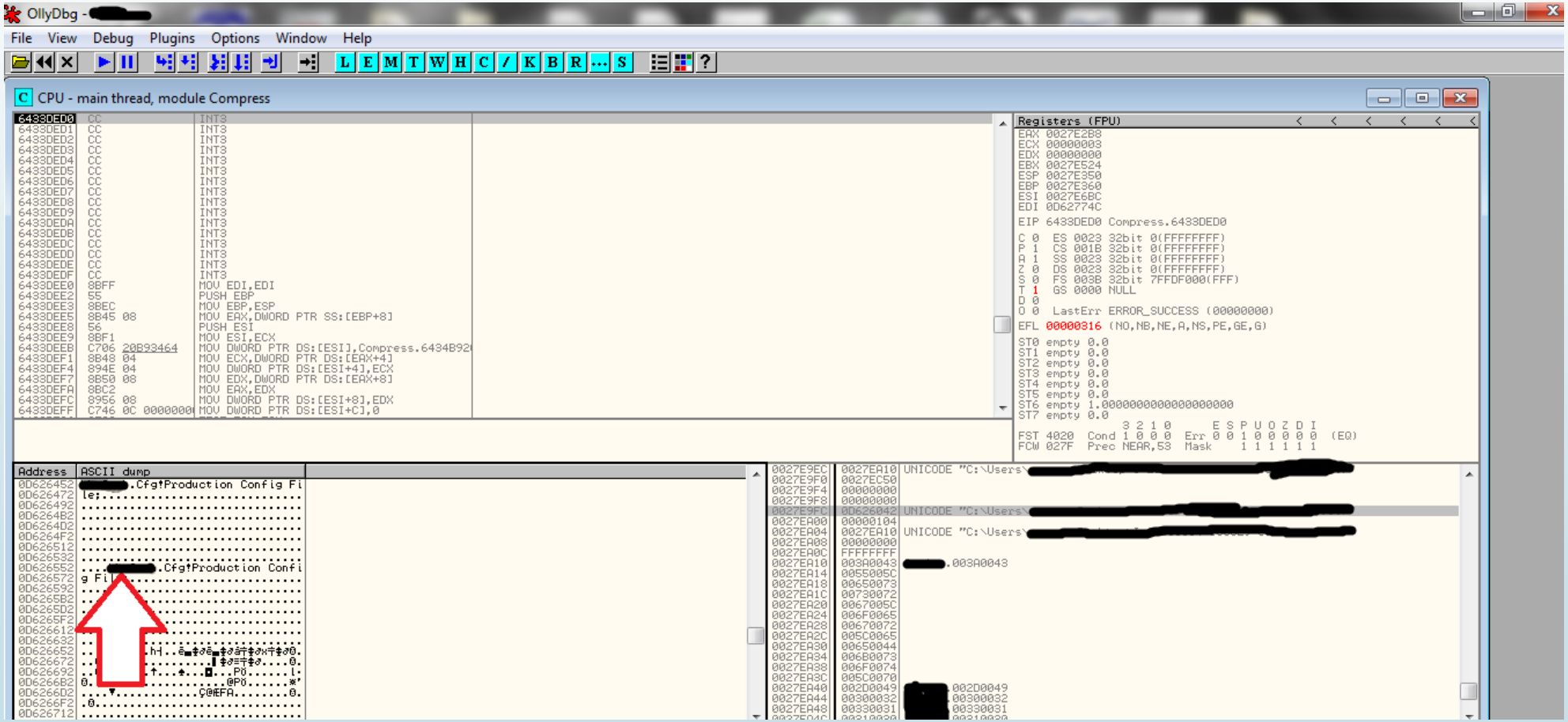

Cat Electronic Technician
Unable to retrieve snapshot data.
OK

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

OllyDbg

Passwords from diagnostic software sniffed from memory



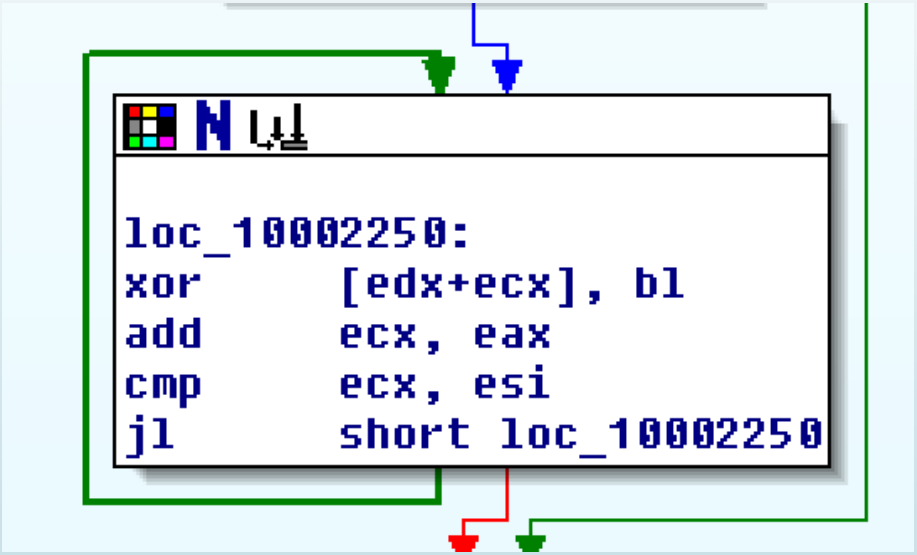
Epiphany #5:
Digital forensics and cybersecurity go hand-in-hand

Disassembling the Communication Protocol

Communications Keys

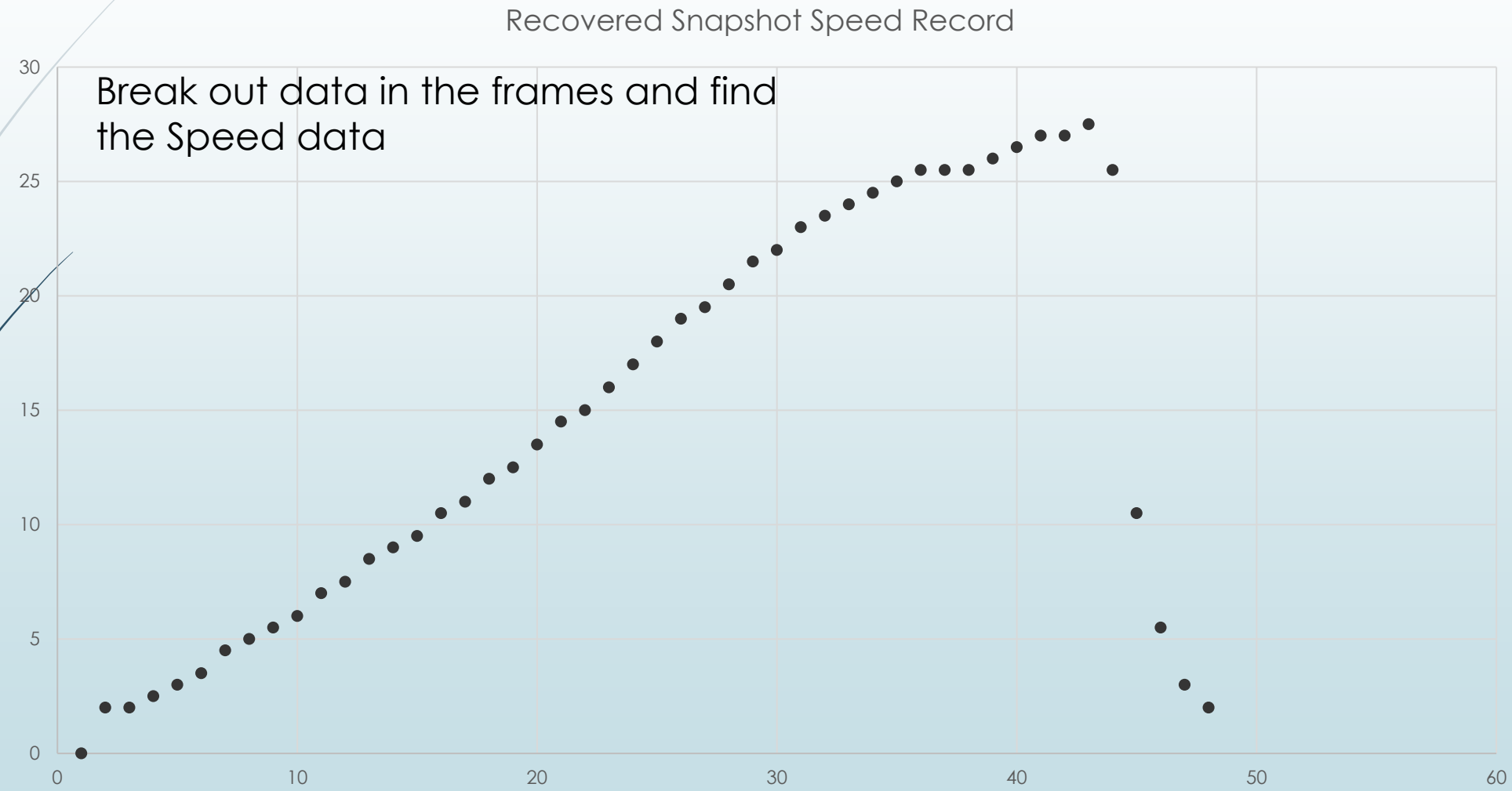
```
mov     cl, 84h
mov     [ebp+var_1A], cl
mov     [ebp+var_6], cl
mov     ecx, [ebp+key]
xor     eax, eax
push    ebx
mov     [ebp+var_2C], 7D5CAB19h
mov     [ebp+var_28], 1B9691EDh
mov     [ebp+var_24], 78A2B78Bh
mov     [ebp+var_20], 0B5E897Ah
mov     bl, 4Dh
```

Assembly Language for Message Encoding

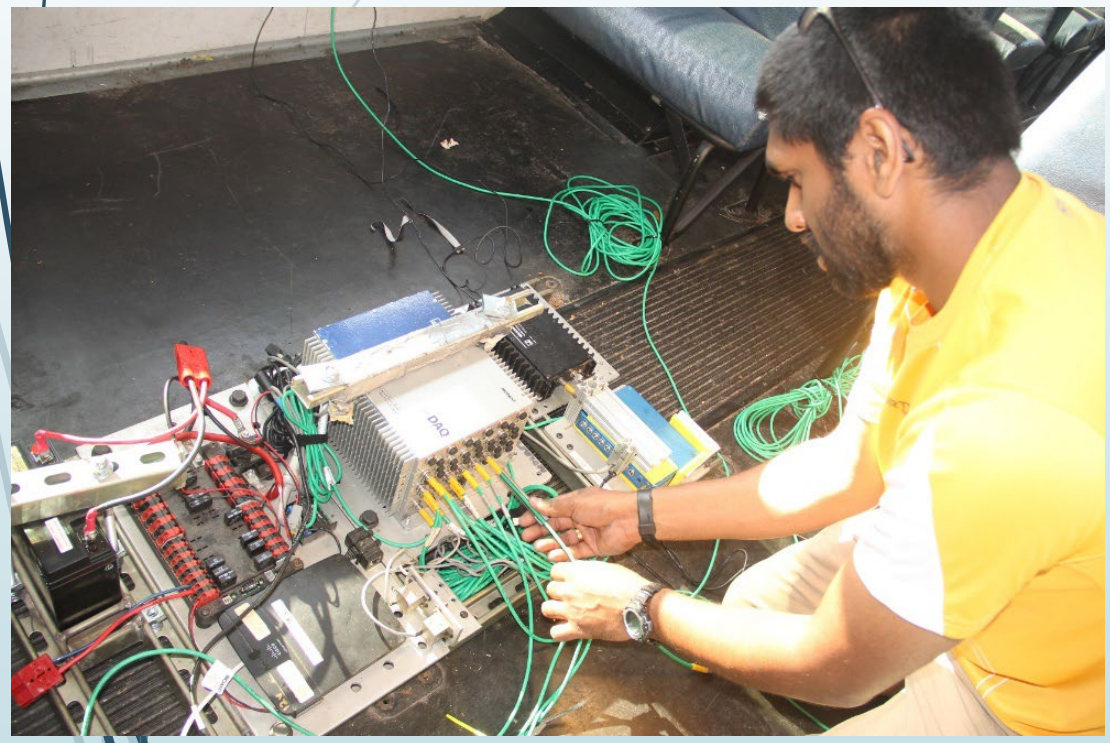


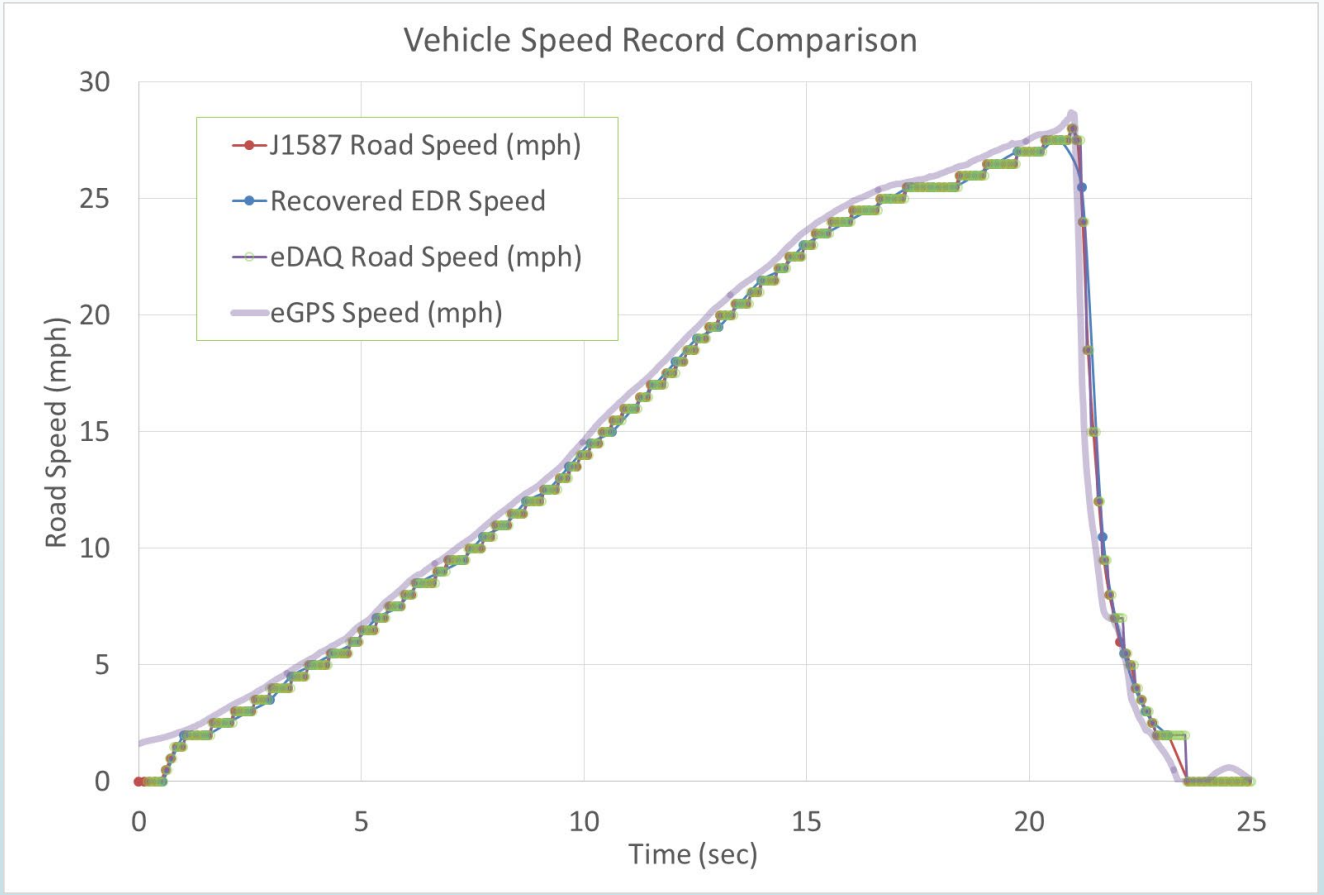
Source: Johnson, J. "A FORENSICALLY SOUND METHOD FOR EVIDENCE EXTRACTION FROM HEAVY TRUCK ECMS", The University of Tulsa, 2014

Recovered Speed Data



Instrumentation for Comparison





Heavy Vehicle Event Data Recorder Data Forensics

Customers are crash investigators, both private and law enforcement

Synercon Technologies

(12) **United States Patent**
Daily et al.

(10) **Patent No.: US 9,865,102 B2**
(45) **Date of Patent: Jan. 9, 2018**

(54) **WHEELED VEHICLE EVENT DATA RECORDER FORENSIC RECOVERY AND PRESERVATION SYSTEM**

(71) Applicant: **The University of Tulsa**, Tulsa, OK (US)

(72) 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)

(52) **U.S. Cl.**
CPC ***G07C 5/0841*** (2013.01)

(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)

FOREIGN PATENT DOCUMENTS

The Forensic Link Adapter

Synercon Technologies

FARO

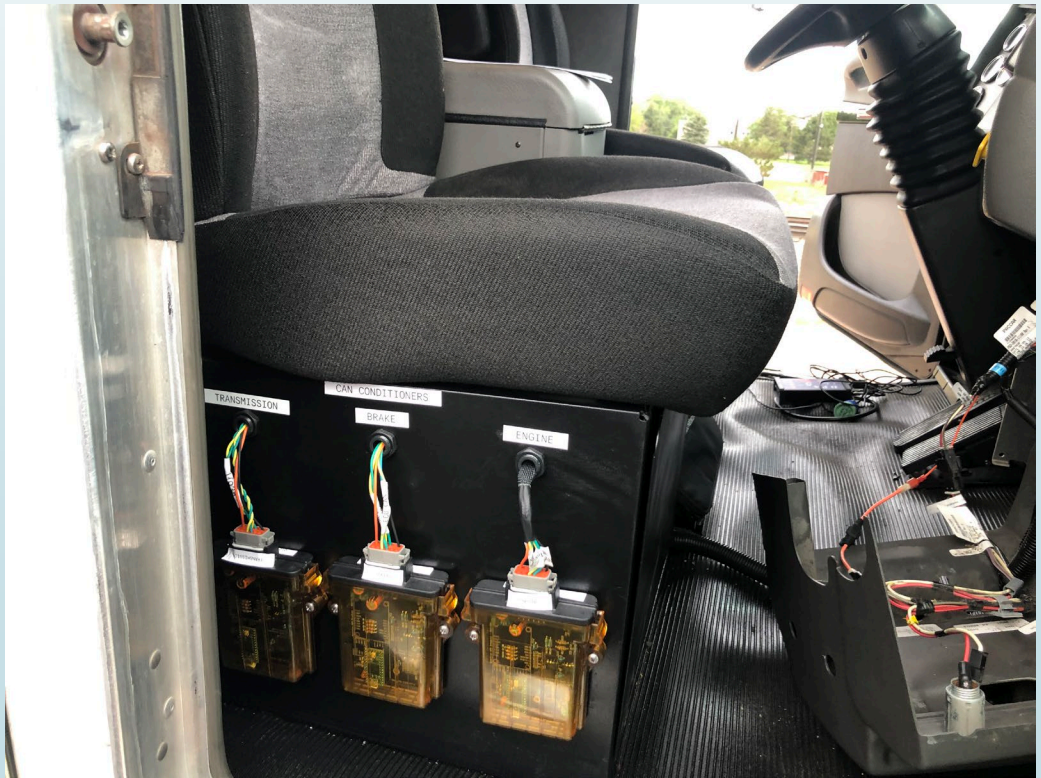
Epiphany #6:
There is a market for vehicle digital forensics.

There's a huge black market for cybersecurity exploits.

Some Crashes Leave No Data To Recover

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


CYBERTRUCK CHALLENGE
SYSTEMS ENGINEERING
COLORADO STATE UNIVERSITY
USDOT 0412285

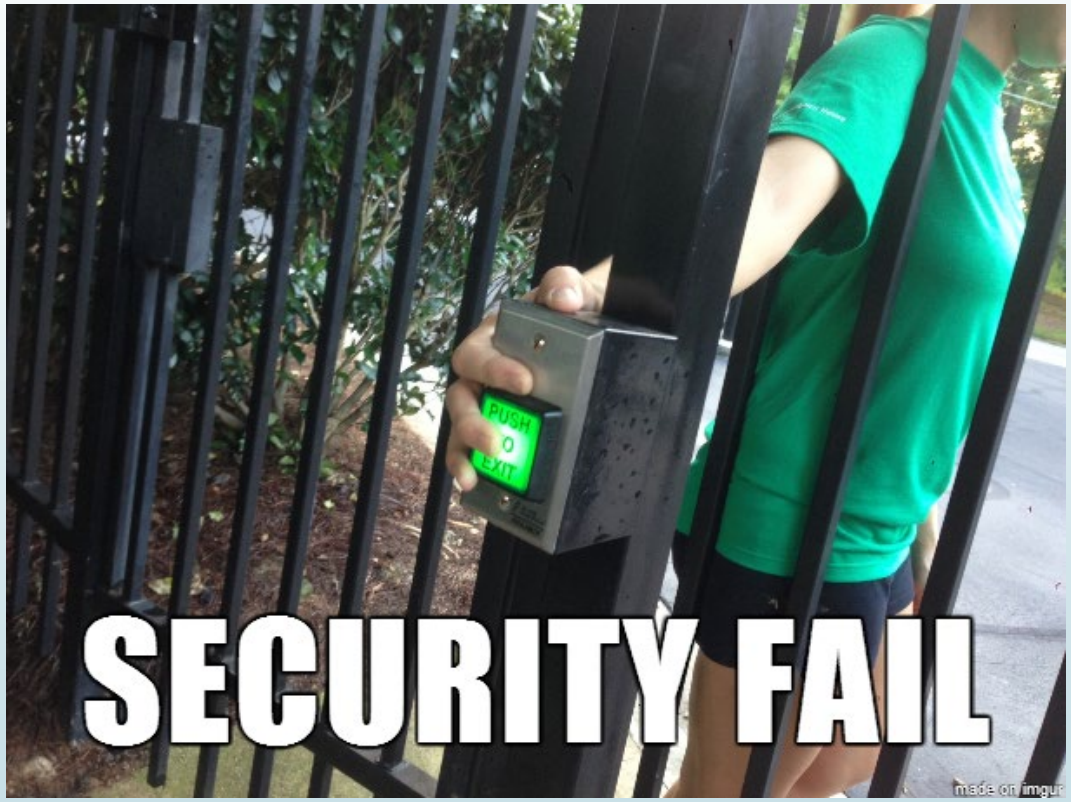

TRANSMISSION
BRAKE
AIR CONDITIONERS
ENGINE

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

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.

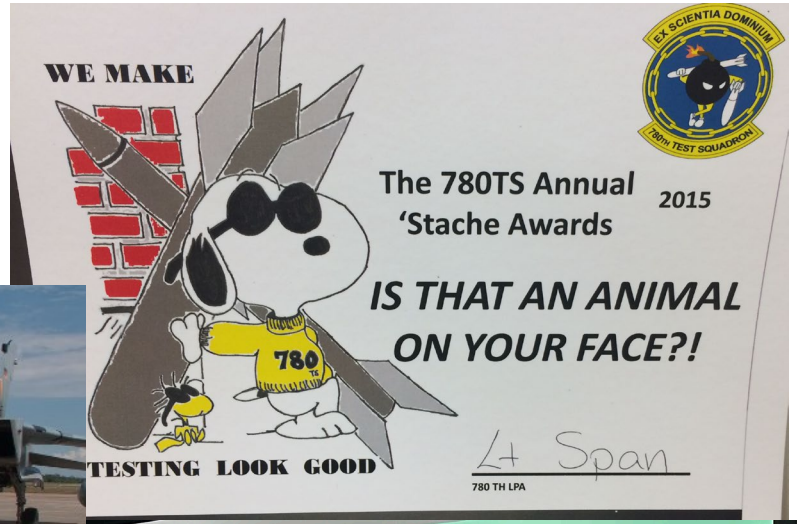
Don’t Design Systems Like This…



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

Thank you
Questions?

SPAN- Path to SE



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

Martin “Trae” Span

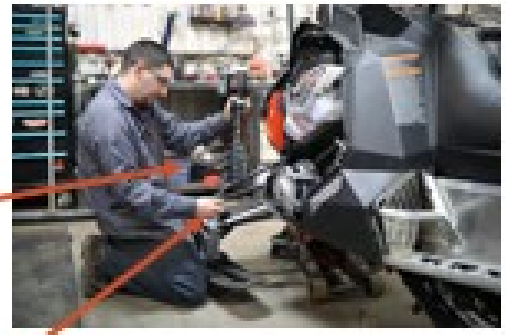
Dr. Jeremy Daily

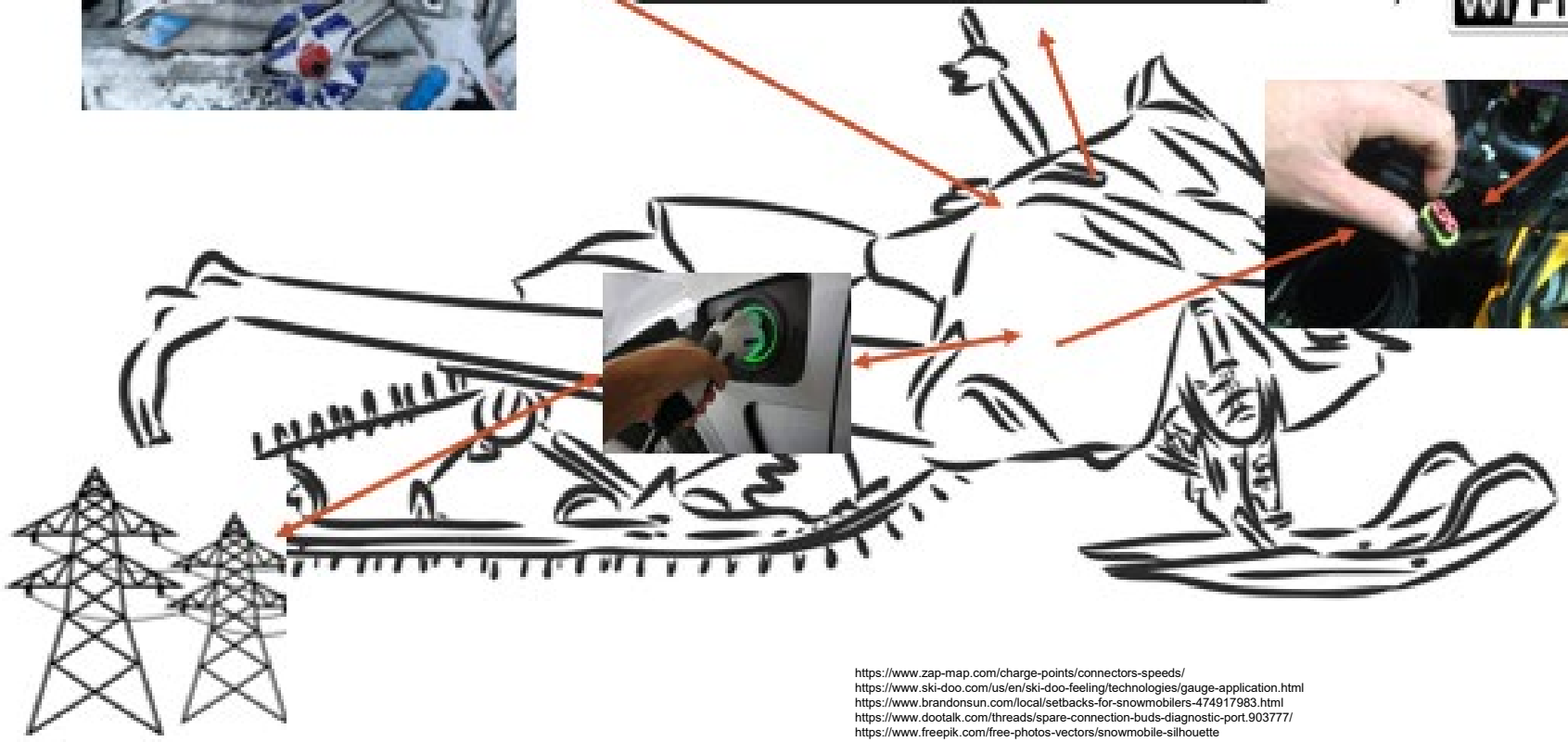
Colorado State University

October 2, 2022

2022 INCOSE Western States Regional Conference – Golden, CO

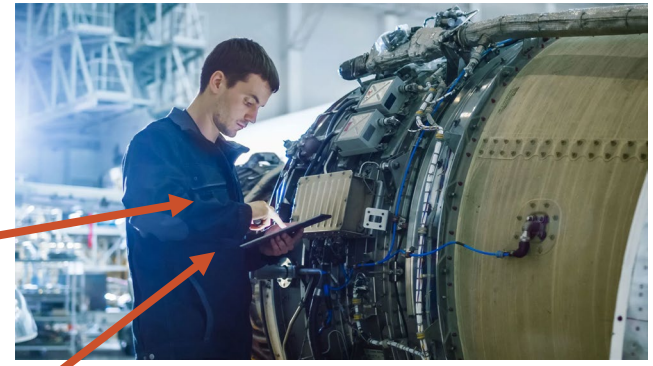
Simplified System Architecture Overview

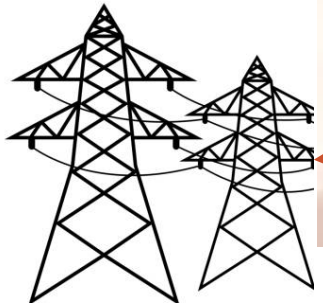




https://www.zap-map.com/charge-points/connectors-speeds/
https://www.ski-doo.com/us/en/ski-doo-feeling/technologies/gauge-application.html
https://www.brandonsun.com/local/setbacks-for-snowmobilers-474917983.html
https://www.dootalk.com/threads/spare-connection-buds-diagnostic-port.903777/
https://www.freepik.com/free-photos-vectors/snowmobile-silhouette

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

https://www.google.com/url?sa=i&url=https%3A%2F%2Ftwitter.com%2Fjosephsteinberg%2Fstatus%2F1091363160446169092%3Flang%3Dhu&psig=AOvVaw0Mg37O-AIUgSDK7edFPACJ&ust=1666637222730000&source=images&cd=vfe&ved=0CA4QjhxqFwoTCIjIyM6B9_oCFQAAAAAdAAAAABAi

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&source=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]
  - https://youtu.be/RZVYTJarPFs
- 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
  - Hazard Analysis technique to facilitate requirements for safe and secure

GAO 2021 Report on Weapon System Cybersecurity

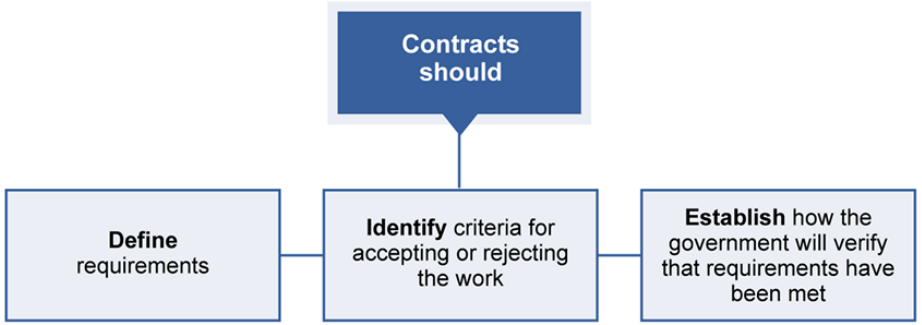
- Contracting for cybersecurity **requirements** is key.
- DOD guidance states that these **requirements** should be treated like other types of system **requirements**
- Specifically, cybersecurity **requirements** should be defined in acquisition program contracts, and criteria should be established 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 better communicate cybersecurity **requirements** and

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.

Incorporating Cybersecurity in Contracts



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:

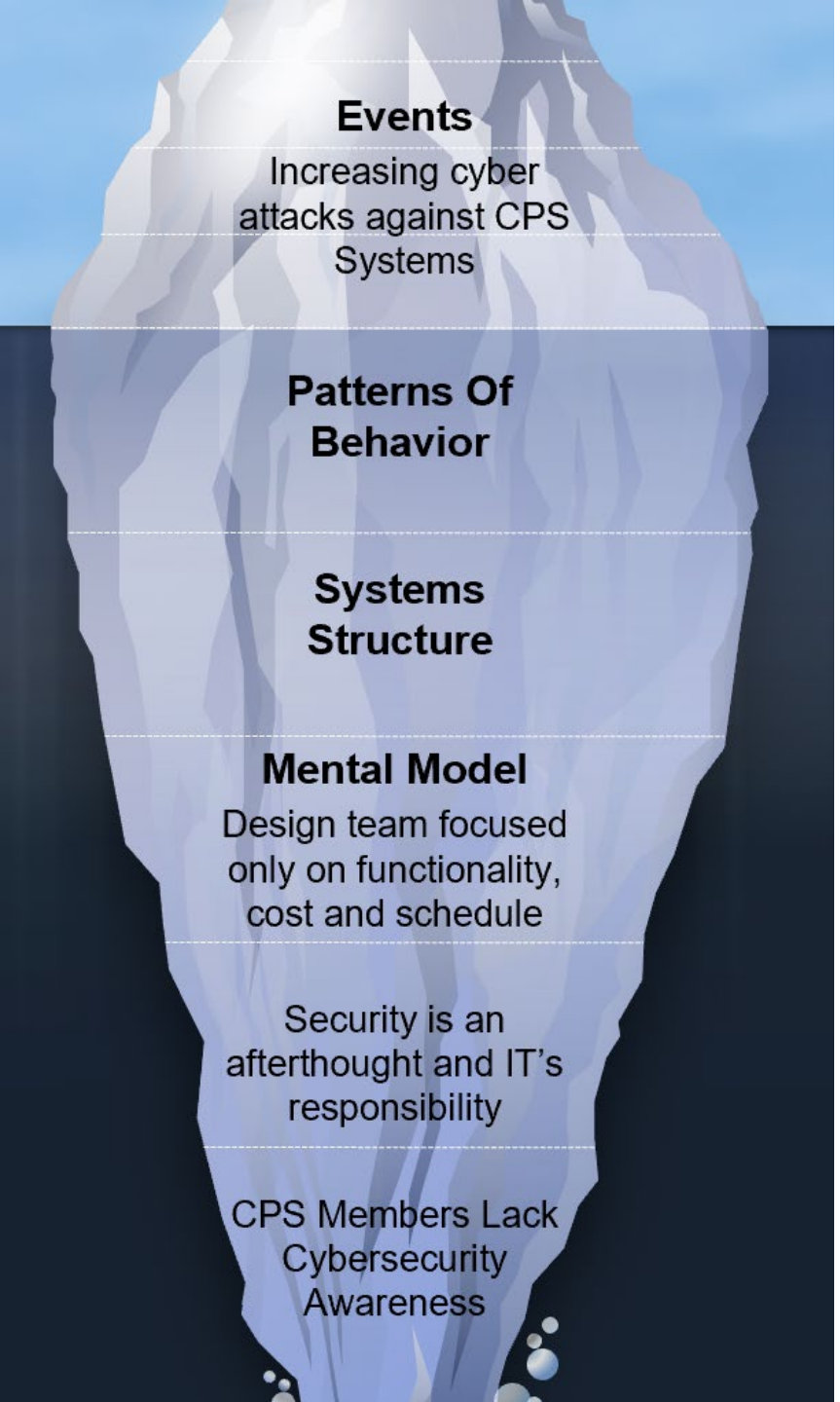
- Taking three classes
  - Fundamentals of Systems engineering
  - Program and Project Management
  - Aerospace Actuation Systems
- Assisting with research under Dr. Daily

Questions?

Thank you

Grad School/Open Discussion

Colorado State University



Characterization of the Problem Space

Current problems with CPS Design Teams:

Lack of systems thinking mindset

Minimal adoption of systems thinking principles:

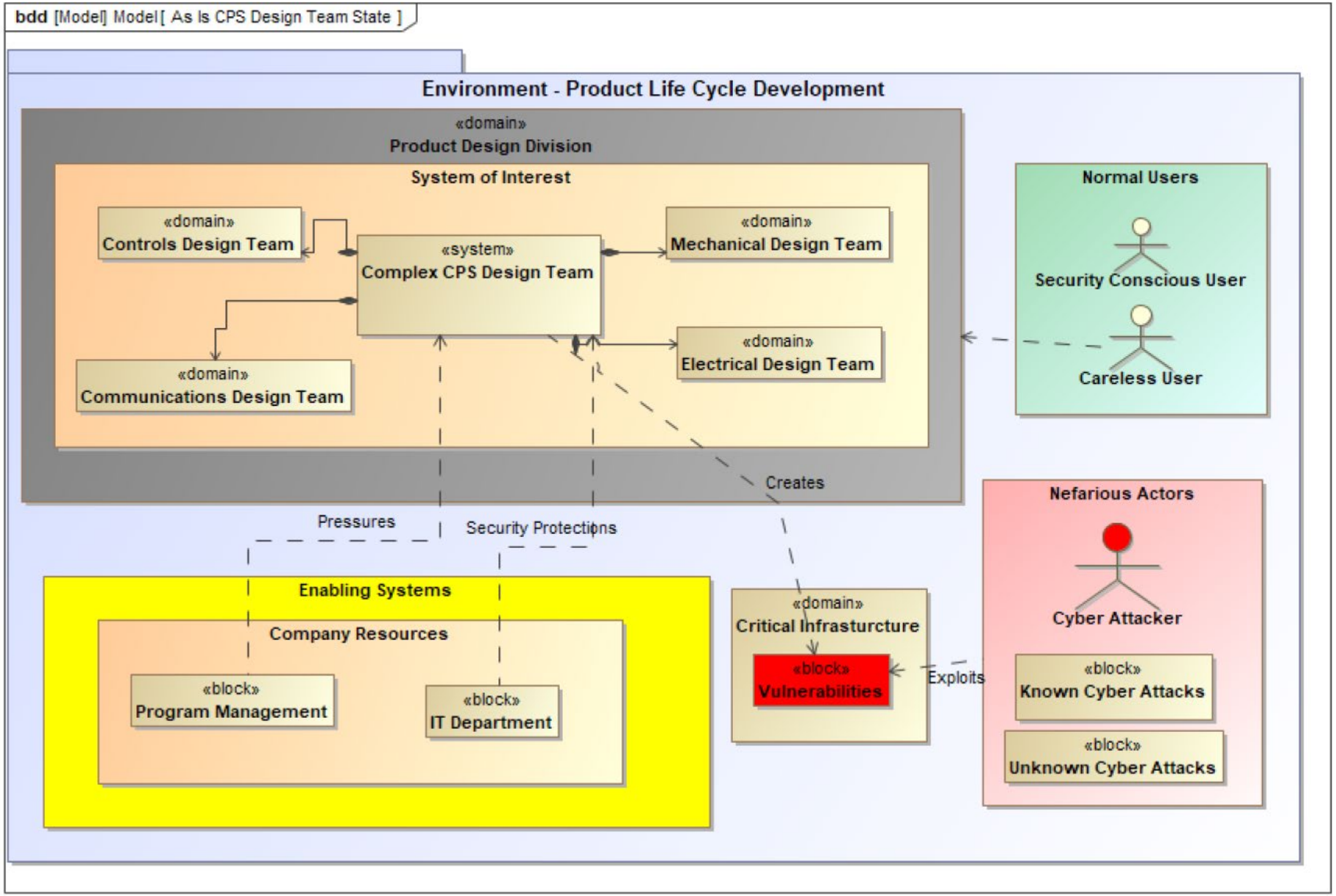
Holism: Lack of holistic view of a CPS

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

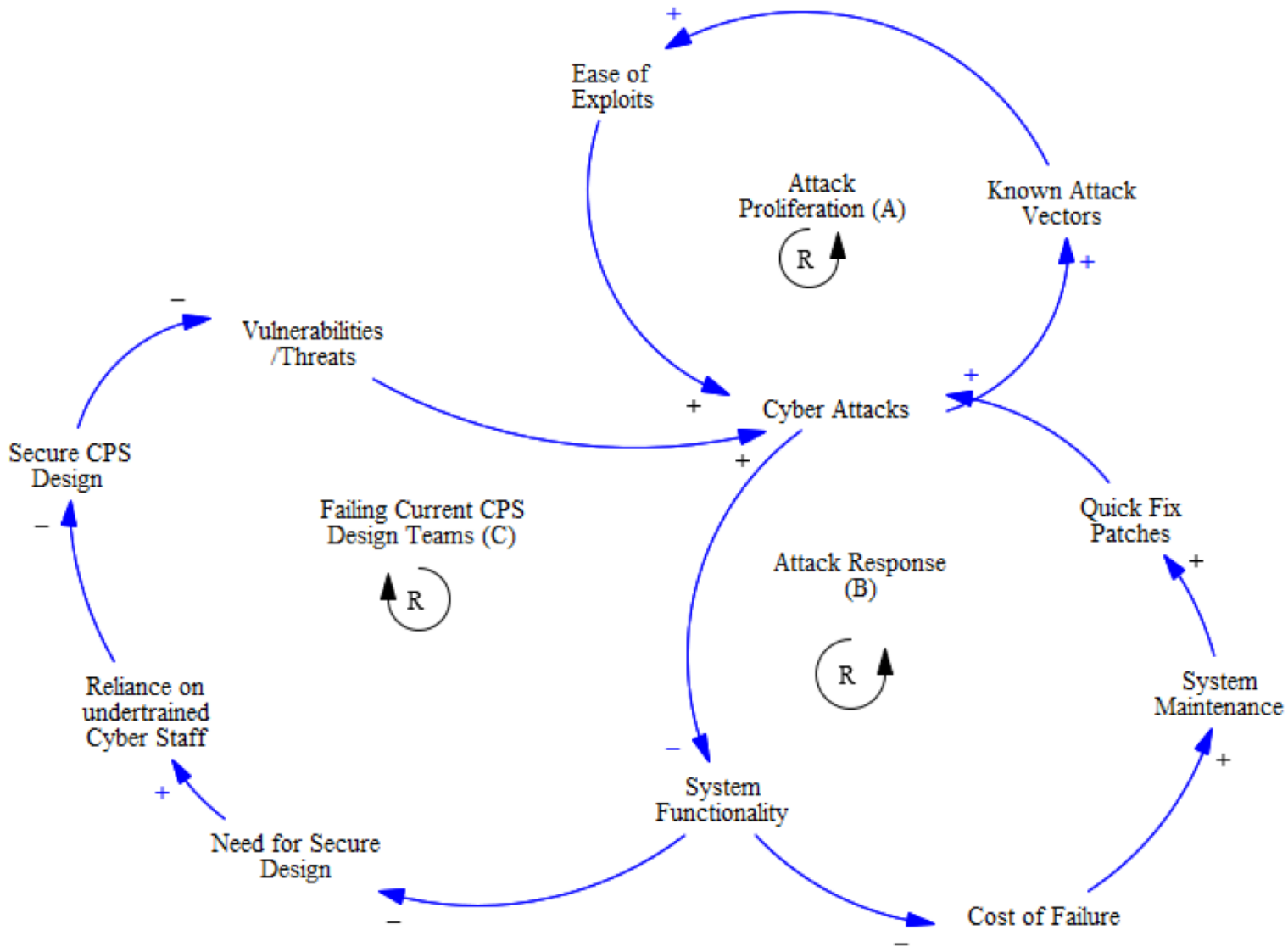


Diagram generated with VENSIM software

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

Proposed BDD for more effective CPS Design Team

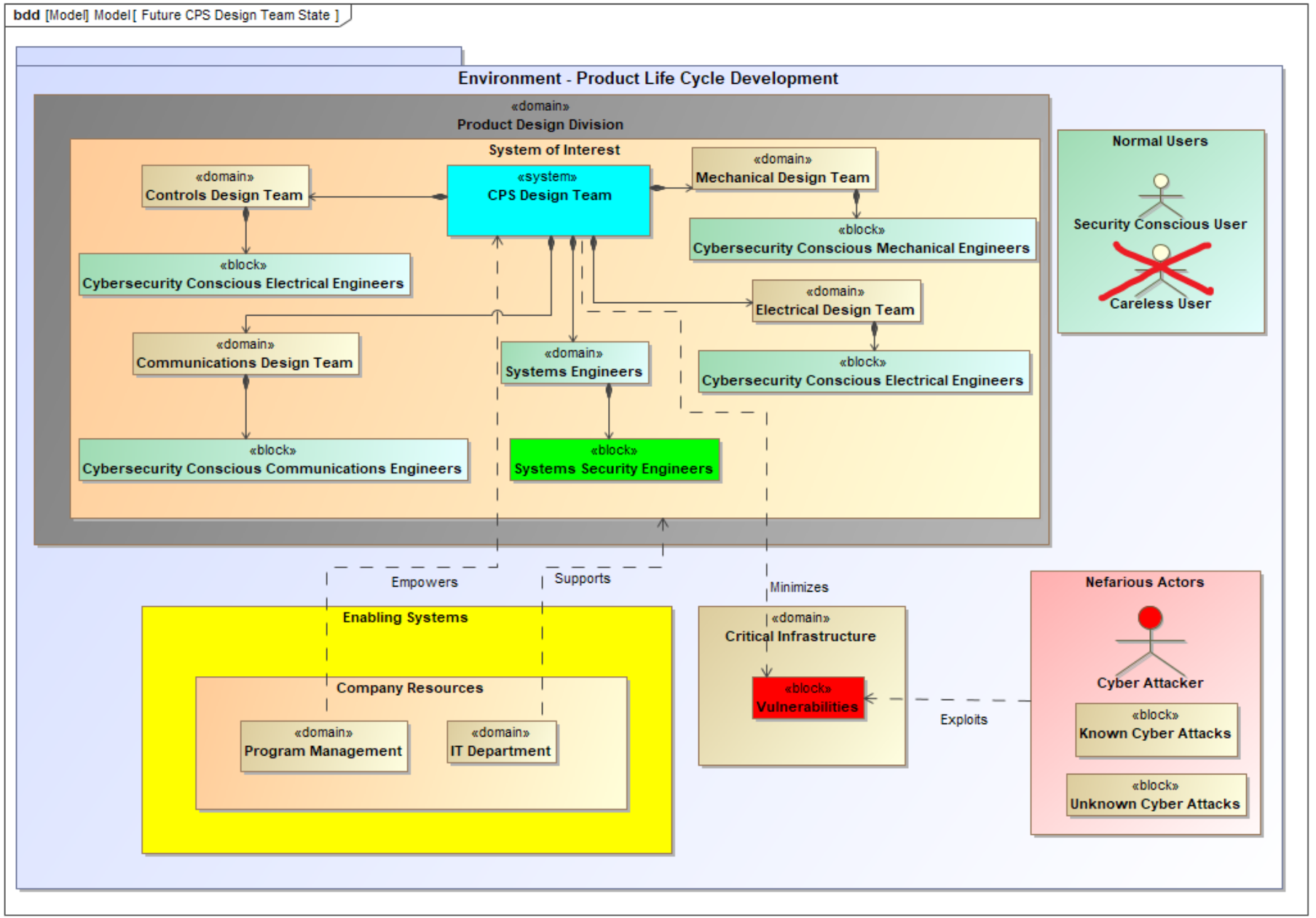


Figure 4: SysML BDD Of Proposed Design Team Solution

Application of Systems Thinking Models for CPS Design Team

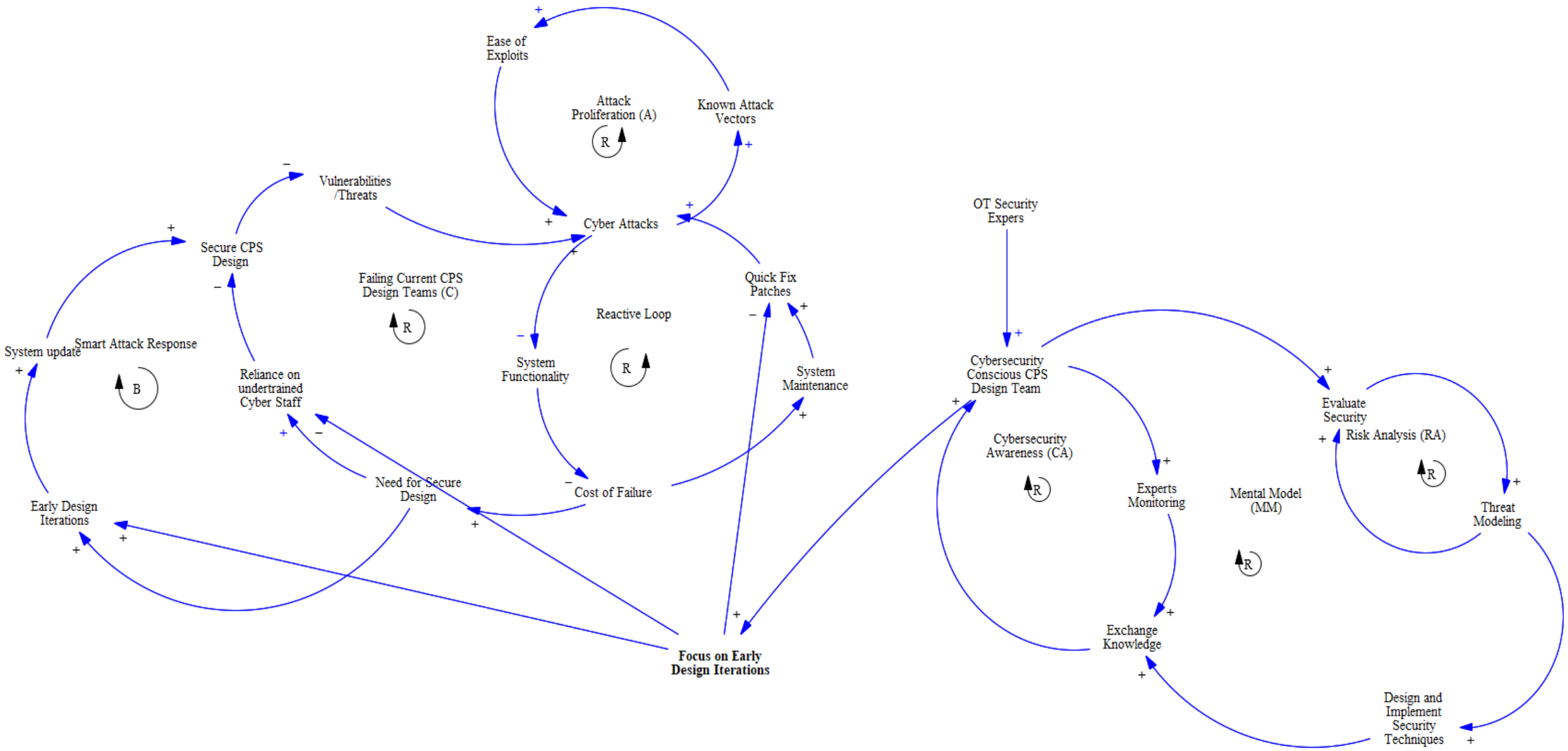


Figure 6: Integration of solution with the problem CLD