33rd Annual INCOSE international symposium
hybrid event
Honolulu HI USA

Balancing Digital Forensic Investigation with Cybersecurity for Heavy Vehicle Traffic Crashes

Mars Rayno Jeremy Daily

Outline

- Introduction and Background
  - Traffic Crash Investigations
  - Systems Engineering Aspects
  - Event Data Recorders
- Digital Forensics
  - Systems Engineering: Forensic Analysis
  - Systems Engineering: IP Considerations
- Cybersecurity
  - CIA Triad
  - Data Retrieval
- Balancing Forensic Availability with Cybersecurity
  - Systems Engineering: Needs Analysis
  - Systems Engineering: Forensic Requirements
  - Potential Solution
- Conclusion

Introduction and Background

Introduction: Traffic Crash Investigations

- In 2020, there were 439,206 accidents involving large trucks in the United States.
- First responders and traffic crash investigators collect evidence at crash scenes to determine the cause of the accidents.
- The evidence collected includes photographs, recorded video, phone records, pavement markings, vehicle crush profiles, eyewitness statements, telematics records, and data from event data recorders (EDRs).
- Collision reconstruction is done using the gathered data to determine liability and damage for the accident.
- EDR data can be used in criminal and civil procedures, potentially leading to a person's conviction. Thus, it is imperative that chain of custody is maintained to ensure integrity of the data.

Large truck accident

(img source https://www.vecteezy.com/photo/11110424-padang-indonesia-2022-truck-in-the-river)

Introduction: Systems Engineering Aspects

- Well-engineered systems are necessary for the creation and preservation of EDR data.
- The Retirement phase in systems engineering involves deactivating and removing the system elements from operations.
- Unplanned end-of-life events, like major crash events, require improved design processes.
- Vehicle event data and vehicle cybersecurity are important system needs.
- System requirements are constructed to provide robust forensic information and improve vehicle cybersecurity.

Background: Event Data Recorders

- Passenger Vehicle Event Data:
  - EDR data includes vehicle speed, throttle positioning, and other data for accident reconstruction.
  - National Highway Traffic Safety Administration (NHTSA) developed the EDR standard with requirements for pre-crash and crash event data in 49 CFR Part 563.
  - Autonomous vehicles gather extensive data, and SAE provides data output formats for analysis, covered by SAE Recommended Practice J3197.
- Heavy Vehicle Event Data Recorders:
  - Heavy vehicles have event data recording capabilities in the engine control module (ECM).
  - SAE J2728 defines a standard for Heavy Vehicle Event Data Recorders (HVEDR), but adoption is not universal.
  - HVEDR may lack relevant information for collision reconstruction, and sub 1-second data is often unavailable.
  - Each ECM manufacturer has its own HVEDR recovery software, complicating data extraction.

Event Data Recorder with some ECU's. Img src: https://crashdatagroup.com/pages/edr-explained

Background: Autonomous Vehicles

- Concerns with Autonomous Vehicles:
  - Autonomous vehicles are increasing in number, and safety drivers may become unnecessary soon.
  - Verbal accounts from drivers/passengers are lost in autonomous vehicle crash events.
  - Current recording devices may not capture certain system failures or cyber-attacks.
    - Traffic crash investigators lack necessary data for cyber-attack detection and liability determination.

Img src: https://www.vecteezy.com/free-photos/autonomous-truck

Background: Systems Engineering

- System Engineering Considerations:
  - Systems engineers consult with stakeholders to determine their needs
    - Traffic Crash Investigators need access to the data that the vehicle recorded prior to the crash event.
    - Original Equipment Manufacturers (OEM) have conflicting needs to protect proprietary software and equipment binaries.
  - Balancing availability of forensic data and protection of intellectual property is essential.

Systems Engineering Considerations

Systems Engineer

- The overall hero of the story.

Stakeholders

- Traffic Crash Investigators
- Original Equipment Manufacturers
- Insurance
- Fleets

Needs

- Data Availability.
- Data Integrity.
- Protection of IP.

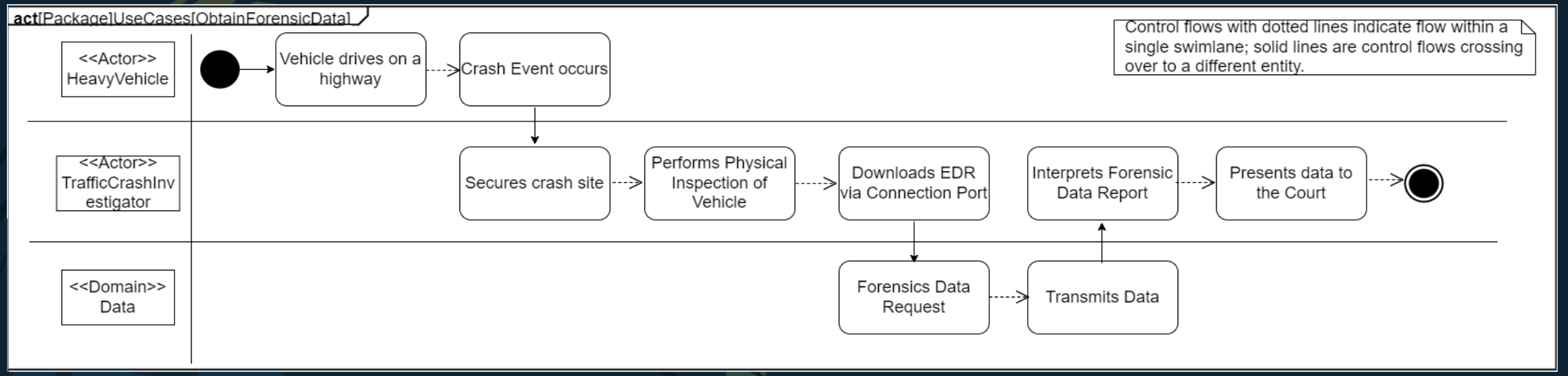
Requirements

Clearly defined methods by which the Needs are met.

Digital Forensics

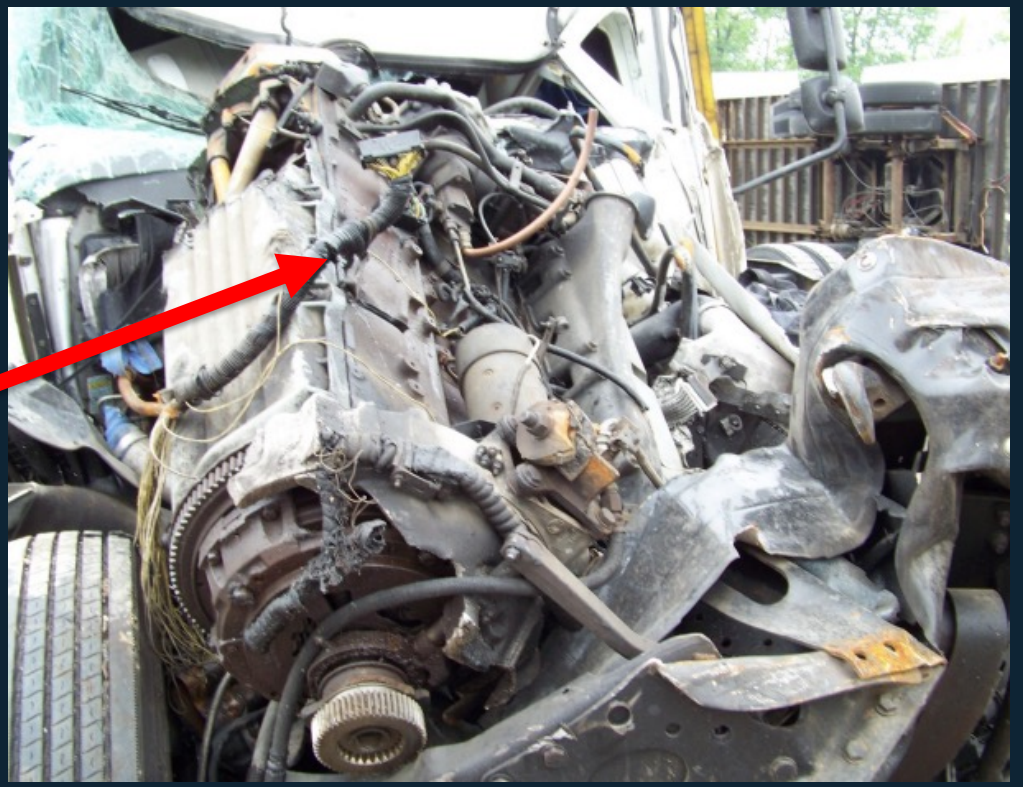
Digital Forensics

- Data Acquisition for Crash Reconstruction:
  - Traffic crash investigators obtain data from the vehicle(s) involved in the accident, shown here in SysML.



Systems Engineering: Forensic Analysis

- Systems Engineering and Forensic Analysis:
  - Traffic crash investigators become stakeholders in the vehicle design process.
- System Design Considerations:
  - Systems engineers typically design for end of life and retirement stages, including disposal processes.
  - For vehicles, the end of life may occur due to a crash event that completely totals the vehicle.
  - Obtaining data for crash reconstruction is crucial for determining liability and informing OEMs about design flaws.
  - Clearly defined requirements ensure the availability of data for forensic analysis throughout the design process.



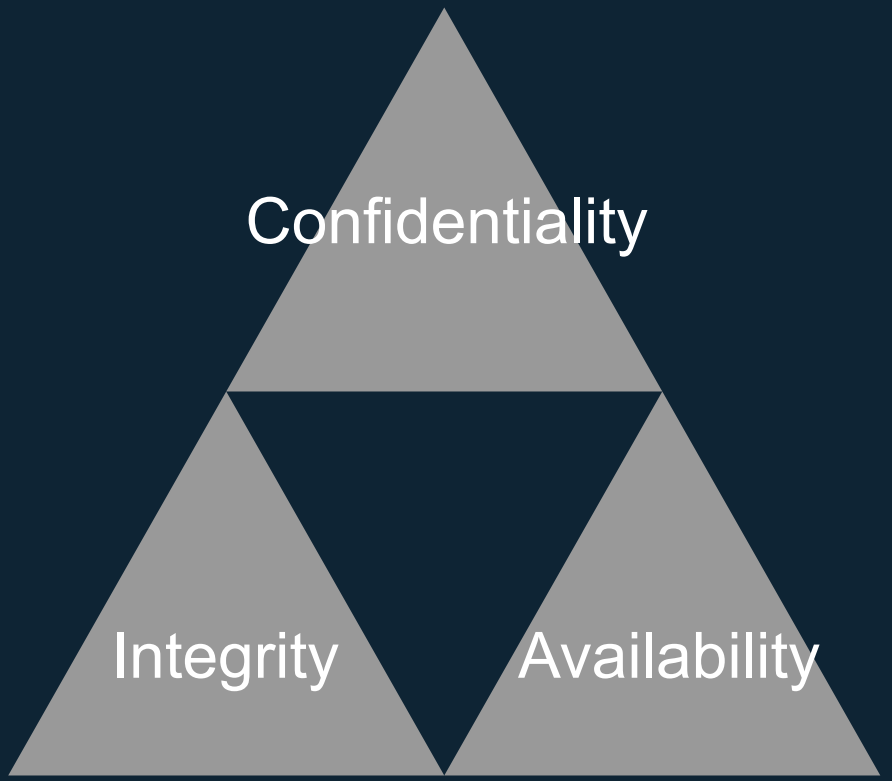
Systems Engineering: IP Considerations

- Issue of OEM's Proprietary Binaries and Software:
  - The proprietary nature of OEM's binaries and software poses a challenge.
  - Balancing the need for data accessibility for forensic analysis with the protection of OEMs' intellectual property is crucial.

Cybersecurity

Cybersecurity

- CIA Triad in Information Security:
  - Confidentiality protects data and restricts access to authorized users.
  - Integrity ensures that data remains unaltered as intended.
  - Availability ensures data accessibility to authorized users.
- *Integrity* and *Availability* are crucial for traffic crash reconstruction.



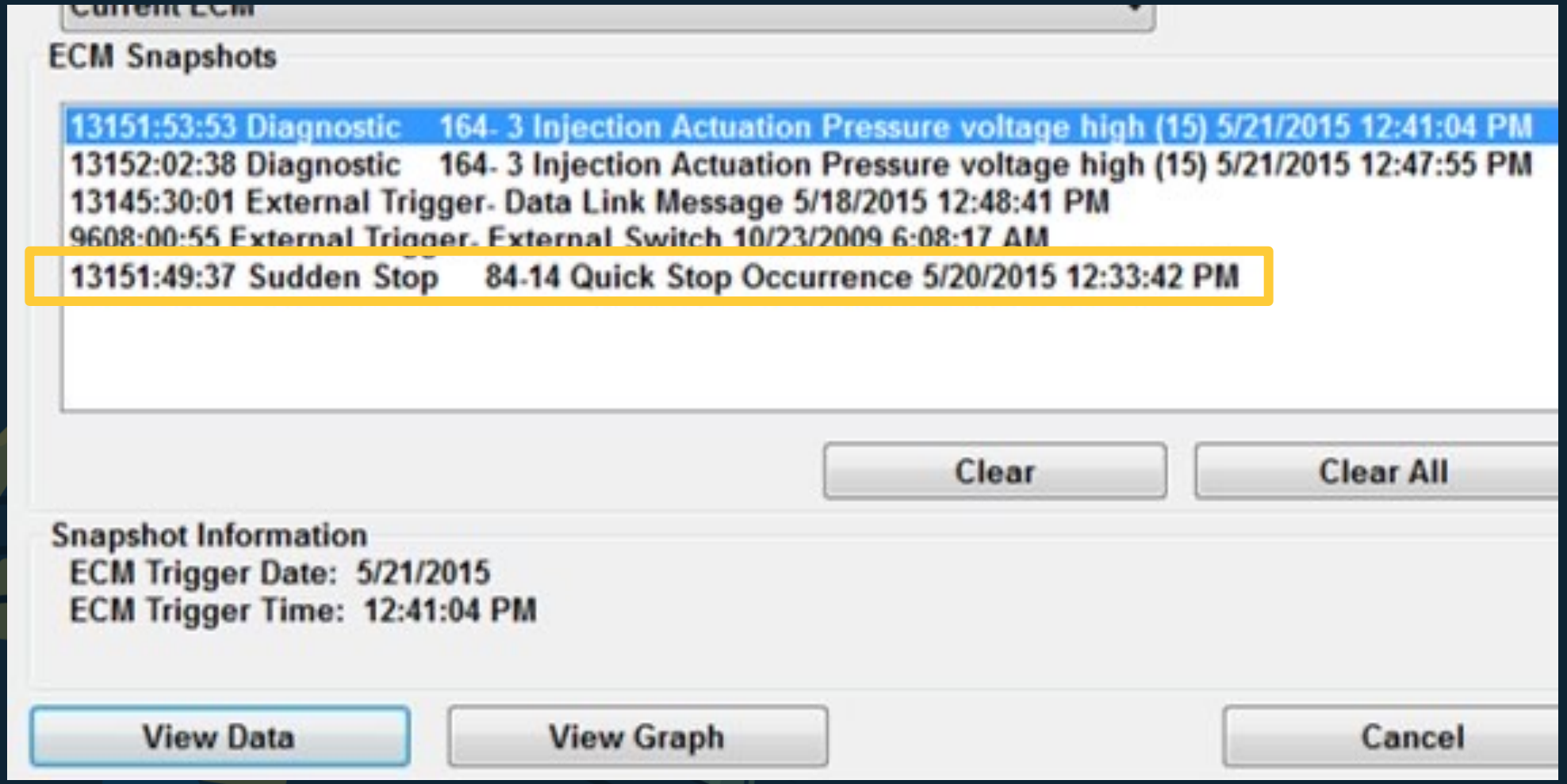
Cybersecurity

- Cybersecurity Controls and Forensic Data Availability:
  - Vehicle cybersecurity is of great interest to OEMs due to the connected nature of heavy vehicles.
  - The connected nature has increased with additional gateways in in-vehicle networks.
  - Proposed or implemented cybersecurity controls may impact the availability of forensic data.

Data Retrieval

- Data Retrieval from ECM:
  - An OEM service tool can download data from the ECM over the in-vehicle network.
  - Example: the data is reported in one-second intervals but actually recorded at 0.2-second intervals.
  - Cross-referencing with other data sources is necessary, and the method may not detect anomalies or cyberattacks.
  - The ECM's survival after a crash event is required for this data retrieval method.

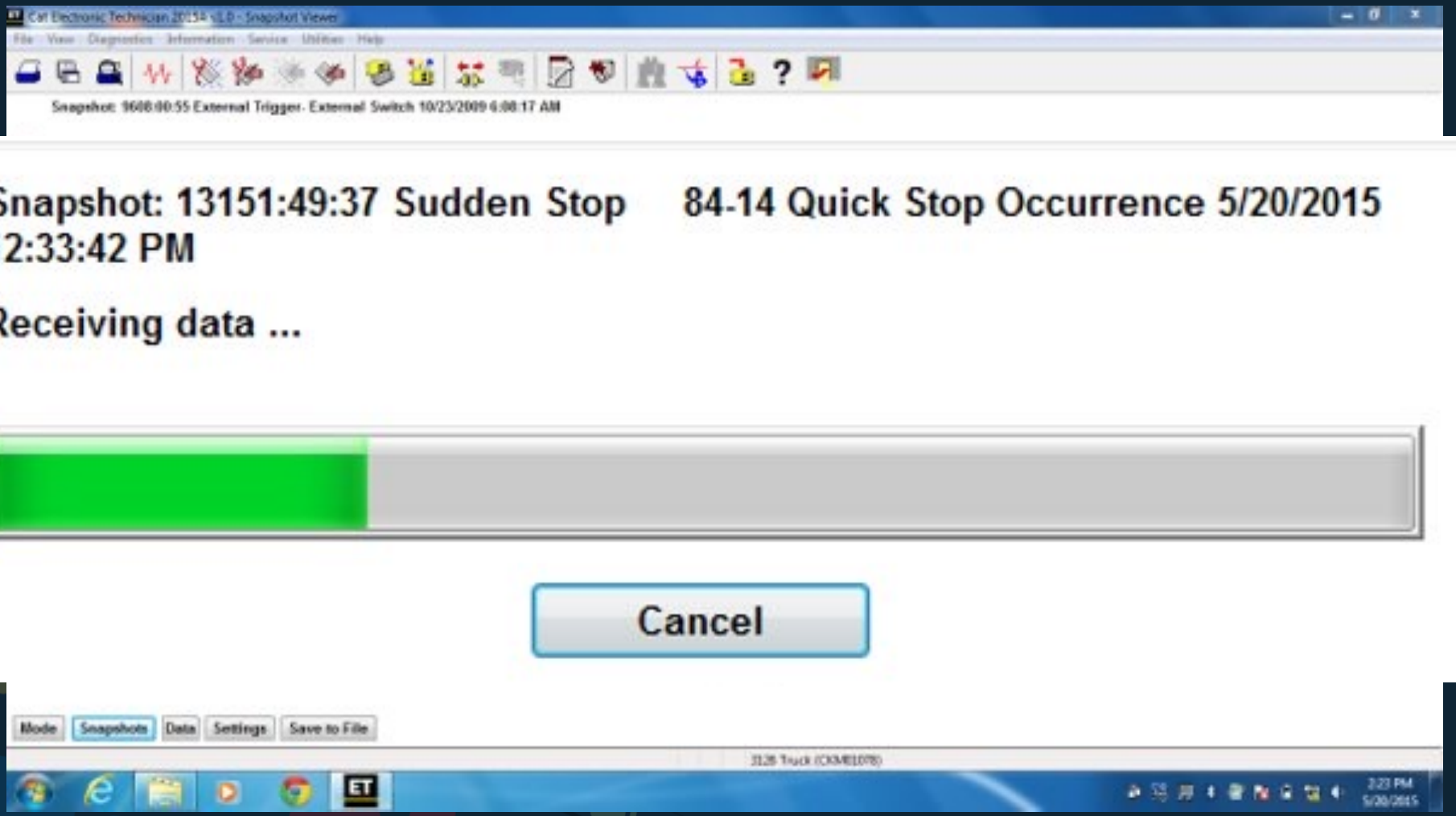
Data Retrieval



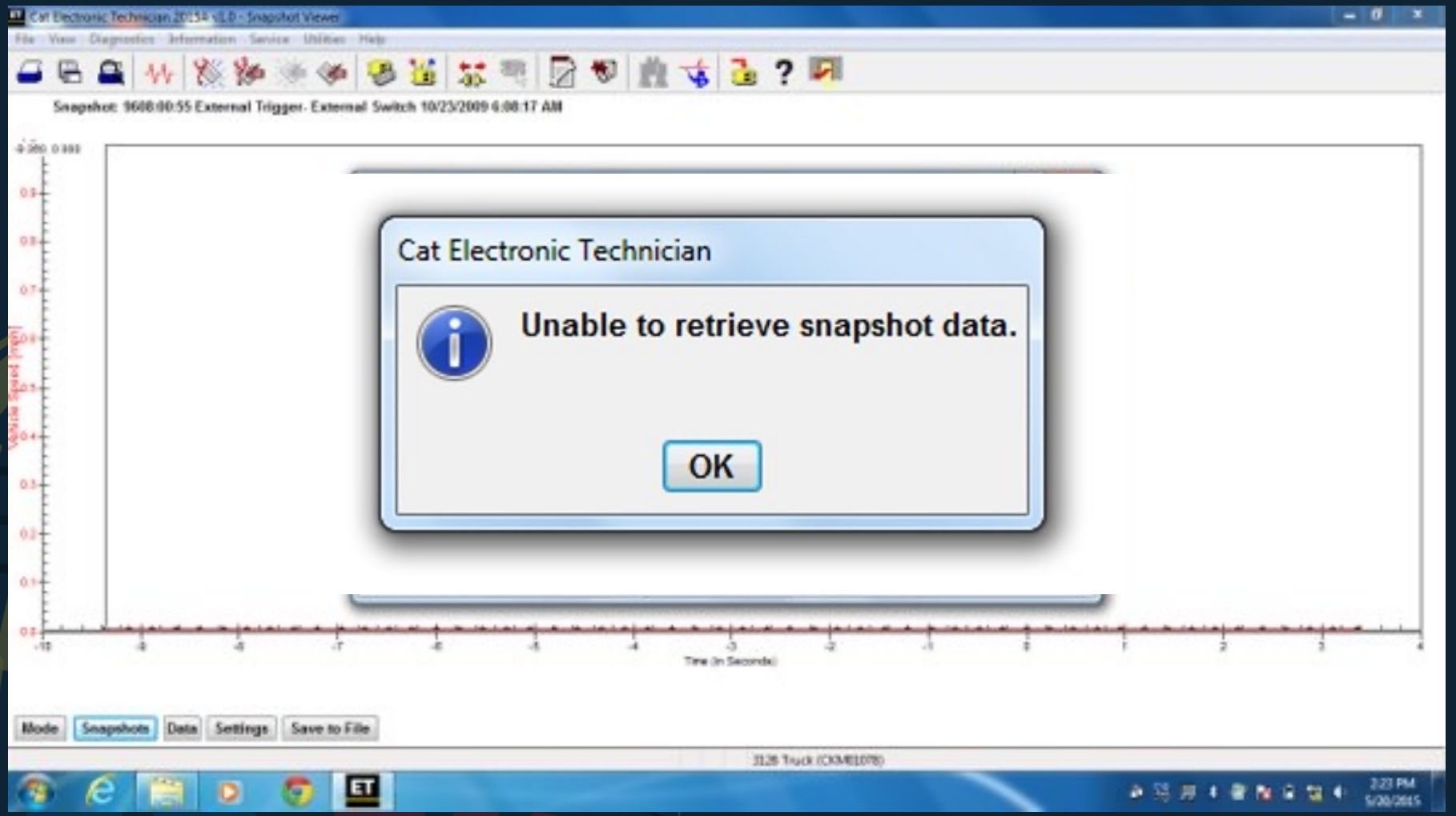
IPTM Special Problems 2015

Transit Bus Vs School Bus

Data Retrieval



Data Retrieval: Failed Download

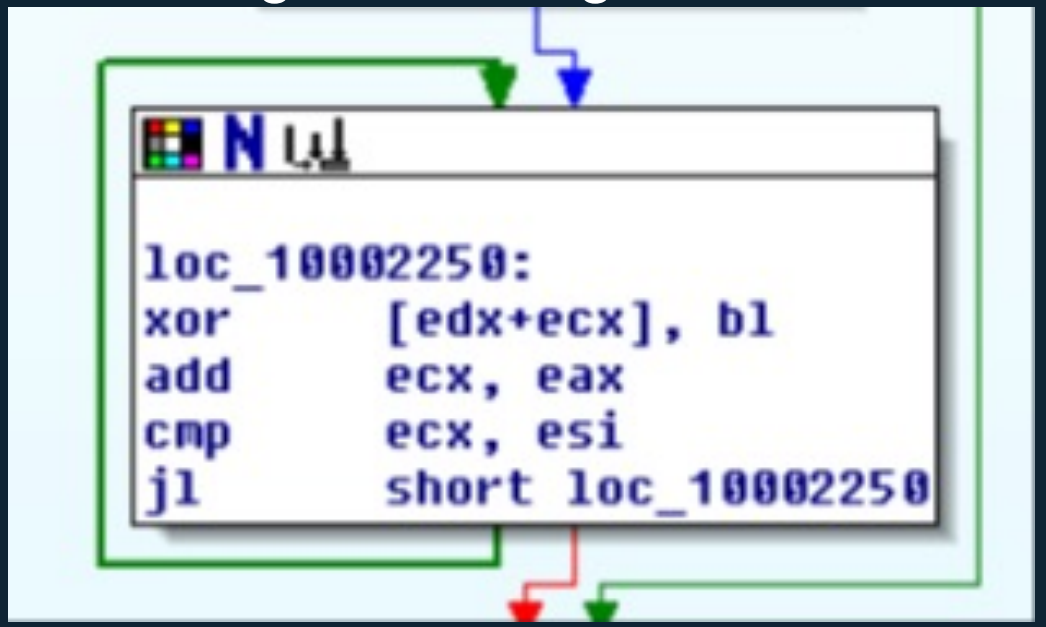


Reverse Engineered Protocol

Communications Keys

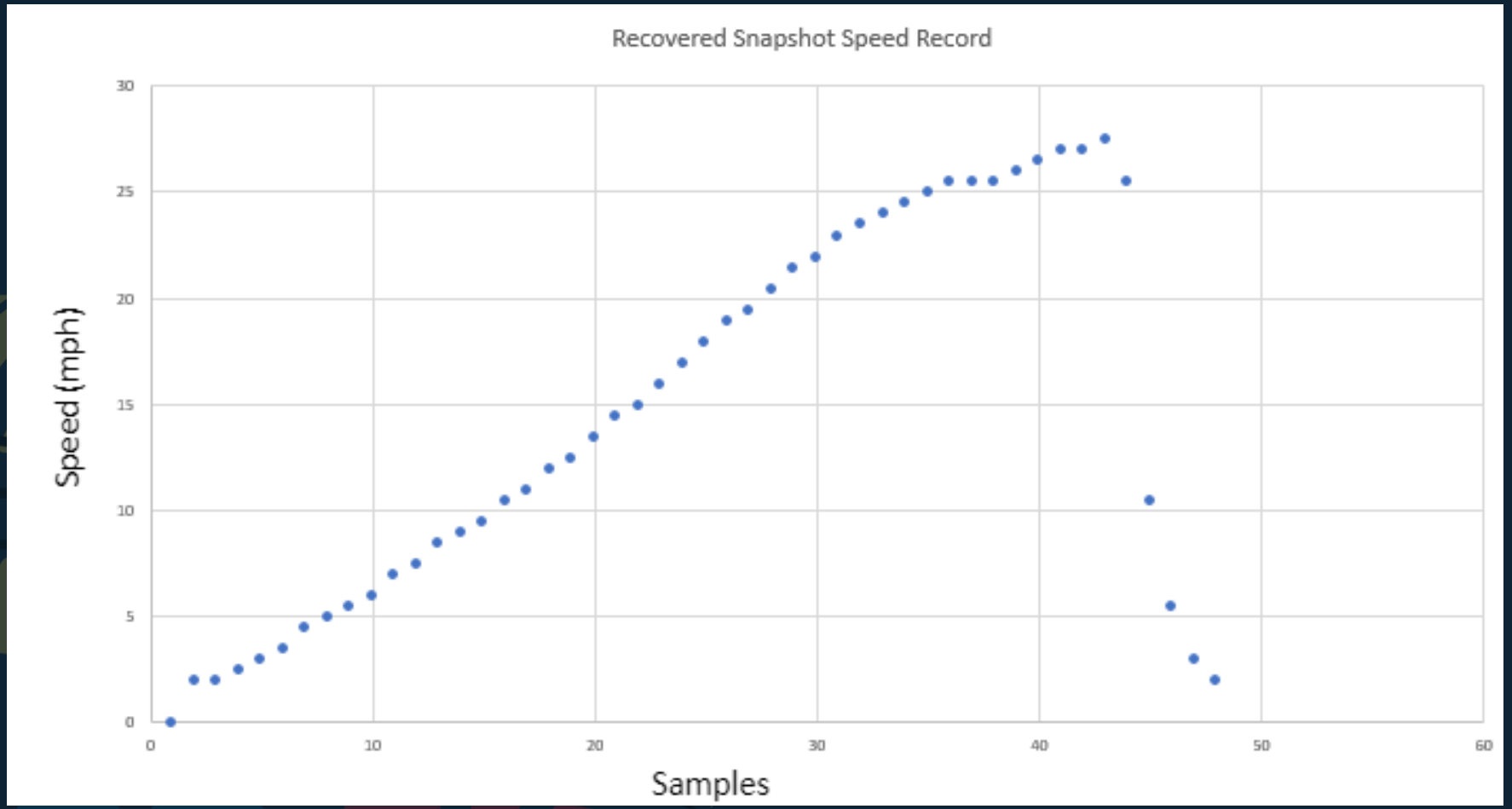
```
mov     cl, 84h
mov     [ebp+var_1A], cl
mov     [ebp+var_6], cl
mov     ecx, [ebp+key]
xor     eax, eax
push    ebx
mov     [ebp+var_2C], 7D5CAB19h
mov     [ebp+var_28], 1B9691EDh
mov     [ebp+var_24], 78A2B78Bh
mov     [ebp+var_20], 0B5E897Ah
mov     bl, 4Dh
```

Assembly Language for Message Encoding

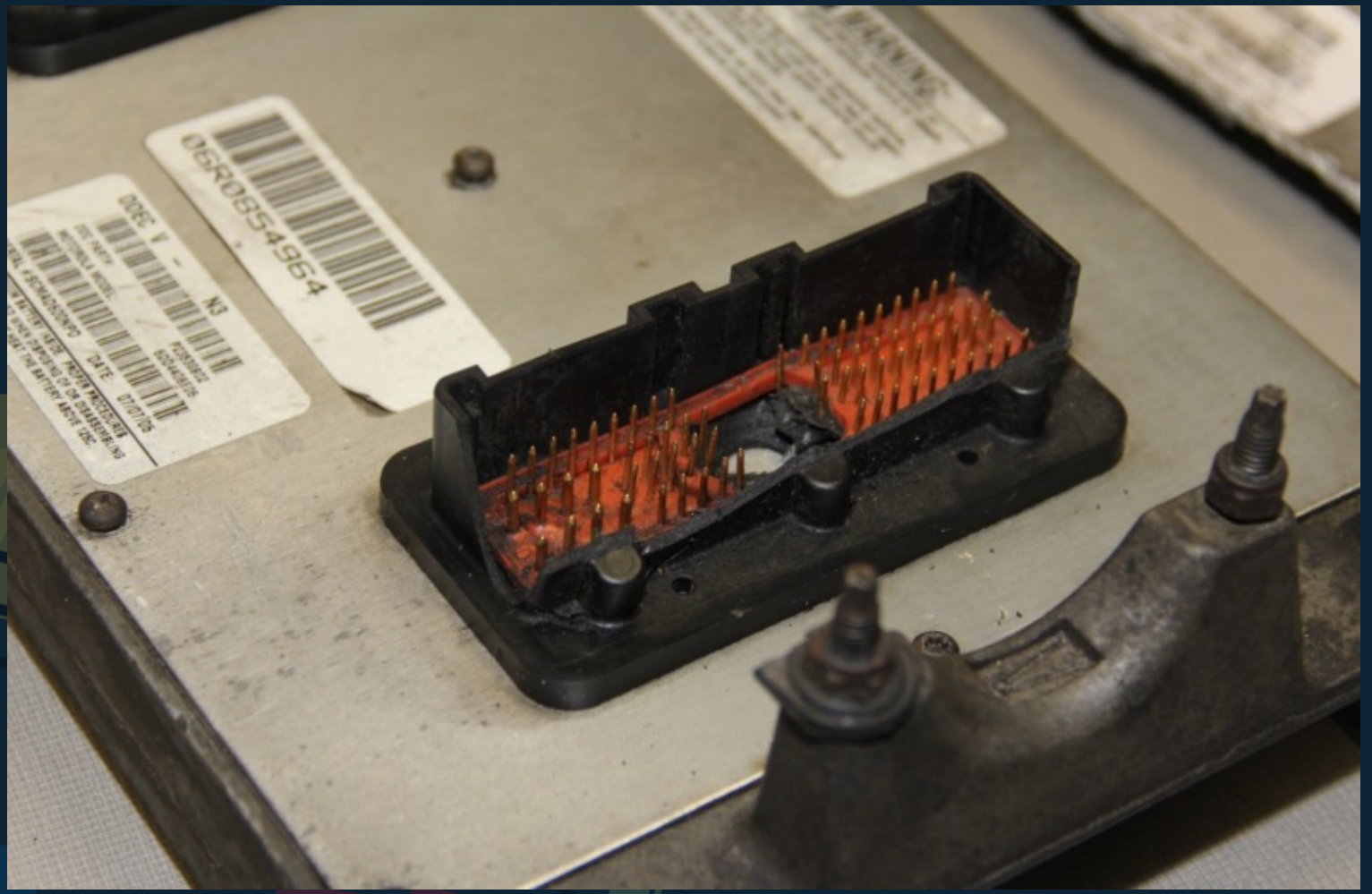


Source: Johnson, J. “A FORENSICALLY SOUND METHOD FOR EVIDENCE EXTRACTION FROM HEAVY TRUCK ECMS”, The University of Tulsa, 2014

Successful Data Recovery



Data Retrieval: ECM Damaged



What if the ECM is damaged?

- Board-Level Analysis and Chip-Level Security:
  - Board-level analysis using JTAG instrumentation can retrieve data from a damaged ECM.
  - Data collection directly from the chip using an IC chip programming device.

Systems Engineering: Issues with IP

- Getting the binary through physical methods means getting the whole binary … including the IP of the OEM.
  - Some OEMs lock the JTAG port to protect their intellectual property (IP).
  - Attempting data collection directly from the chip using an IC chip programming device may fail due to binary obfuscation by OEMs.

What if the ECM is *really* damaged?

Balancing Forensic Availability with Cybersecurity

Balancing Availability with Cybersecurity

- Conflict Between Confidentiality and Availability:
  - OEMs prioritize protecting intellectual property (IP) over forensic data availability.
  - The increasing involvement of autonomous vehicles in crash events demands accessible forensic data.
  - Security requirements may conflict with data requirements.
- Meeting Security and IP Requirements:
  - Regardless of the Requirement written to ensure data availability, preserving OEM IP security is another requirement.
  - Ensuring that system requirements derived for forensic data availability do not conflict with other needs is a challenge.

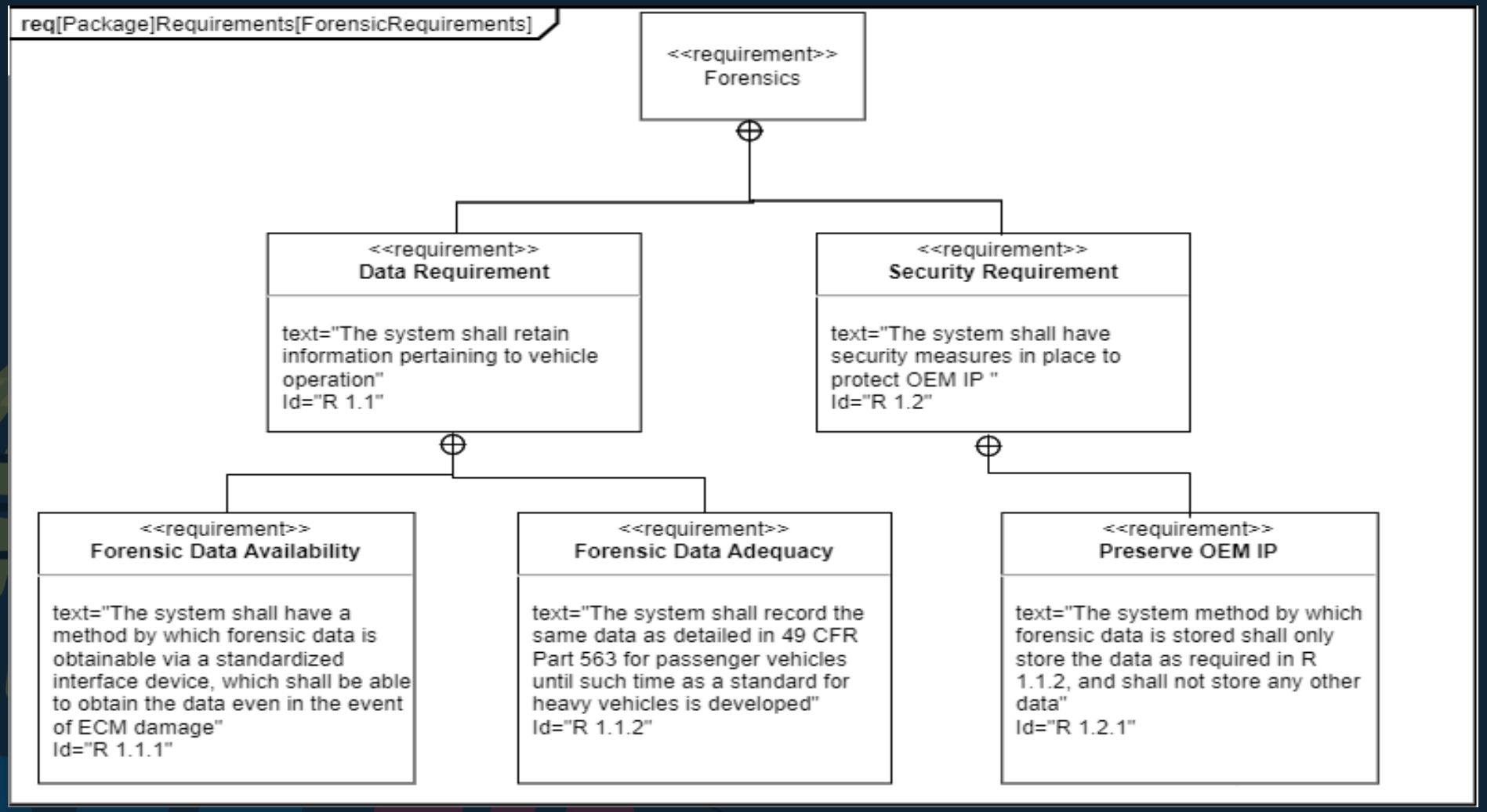
Systems Engineering: Needs Analysis

- Derived System Needs:

Need Number	Stakeholder	Need
1	Traffic Crash Investigator	Safeguard Forensic Data Availability
2	Traffic Crash Investigator	Confirm Forensic Data Adequacy
3	Manufacturer	Protect OEM IP

- The challenge is ensuring that Requirements for Needs 1 and 2 do not conflict with a Requirement for Need 3!
- Derive Forensic Requirements from these Needs.

Systems Engineering: Forensic Requirements



Potential Solution

- Requirement for a Dedicated Recorder Chip:
  - A dedicated recorder chip without IP but containing operational data from the ECM could satisfy both OEM's IP protection and forensic data availability.
  - Size-intensive data storage may require compression methods.
- Lifecycle and Power Loss Challenges:
  - EEPROM chips typically have a limited write cycle lifespan, which may not meet the 15-20 year lifecycle of heavy vehicles.
  - Sudden power loss during crash events can corrupt data if a buffer/data dump method is used.
  - Real-time continuous writing of data can mitigate data loss caused by power loss.

Conclusion

Conclusion

- Crash Events, Data Availability, and Cyberattacks:
  - Increasing usage of autonomous vehicles and potential cyberattacks necessitate ample data availability for traffic crash investigators.
  - Balancing data availability with OEMs' IP protection is crucial.
  - Current trend favors security over data availability.
- Identifying Needs and Generating Requirements:
  - Needs can be identified through crash event end-of-life studies.
  - Specific requirements can be derived that meet the needs of both traffic crash investigators and OEM stakeholders.
  - Requirements should aim to avoid conflicts and satisfy the needs of both stakeholders.

Mars Rayno
mars.rayno@colostate.edu

Jeremy Daily
Jeremy.daily@colostate.edu

33rd Annual INCOSE international symposium

hybrid event

Honolulu HI USA

www.incose.org/symp2023

#INCOSEIS

Systems Engineering: Forensic Requirements

- Example System Requirements:
  i. Safeguard Forensic Data Availability:
    i. Forensic data shall be obtainable via a standardized interface device, which shall remain obtainable even in the event of ECM damage.
  ii. Confirm Forensic Data Adequacy:
    i. Forensic data shall record the same required data as specified in 49 CFR Part 563 for passenger vehicles until such a time as a standard for heavy vehicles is developed.
  iii. Preserve OEM IP:
    i. The method of storing forensic data shall only store data as required in Requirement (ii), and shall not store any other information, proprietary or otherwise.