REPORT CDOT-2022-04 May 2022

Autonomous Truck Mounted Attenuator Incident Response - CSU Data Report

APPLIED RESEARCH & INNOVATION BRANCH

Jeremy Daily, Trae Span, Mars Rayno, Weston Brown, Ashley Nylen, Tyler Weldon

COLORADO
Department of Transportation

The contents of this report reflect the views of the author(s), who is(are) responsible for the facts and accuracy of the data presented herein. The contents do not necessarily reflect the official views of the Colorado Department of Transportation or the Federal Highway Administration. This report does not constitute a standard, specification, or regulation.

Technical Report Documentation Page

1. Report No. CDOT-2022-04	2. Government Accession No.	3. Recipient's Catalog No.
4. Title and Subtitle Autonomous Truck Mounted Attenuator (ATMA)Incident Response - CSU Data Report		5. Report Date May 2022 6. Performing Organization Code
7. Author(s) Jeremy Daily, Martin Span, Mars Rayno, Weston Brown, Ashley Nylen, Tyler Weldon		8. Performing Organization Report No.
9. Performing Organization Name and Address Colorado State University, Fort Collins, Colorado 80523 USA		10. Work Unit No. (TRAIS) 11. Contract or Grant No. SPR-5380-20-05
12. Sponsoring Agency Name and Address Colorado Department of Transportation - Research 2829 W. Howard Pl. Denver CO, 80204		13. Type of Report and Period Covered Final (2021-2022) 14. Sponsoring Agency Code

15. Supplementary Notes

16. Abstract

As a specific Connected and Automated Vehicle (CAV) technology, the Autonomous Truck Mounted Attenuator (ATMA) is being developed by hardware and software vendors to help save the lives of Department of Transportation (DOT) workers in active highway work zones. The ATMA utilizes an innovative Leader/Follower technology that allows manned and unmanned vehicles to perform cooperatively in a multi-vehicle configuration. The objective of this report is to provide an addendum of considerations for data recovery practices in the event of an incident. When crashes happen, the sequence of determining crash causation starts with a traffic crash reconstruction. This process gathers physical and digital evidence associated with the crash and reconstructs the events that lead to the crash. This process is explored with the ATMA since the technology is little precedent on which to base procedure.

The connection between cybersecurity and crash reconstruction is two-fold: 1) much of the evidence needed to accurately reconstruct the traffic crash is digital in nature and needs to be preserved in a secure manner, and 2) a potential of a cybersecurity breach could lead to a crash. Therefore, it is critically important to undergo a study where a forensic investigation is conducted (i.e. an exercise in data gathering from a simulated crash event).

This work provides samples of data available on the ATMA vehicle and presents recommendations in conjunction with the All Clear report from the ATMA July 2021 Tabletop exercise.

17. Keywords Autonomous Truck Mounted Attenuator (ATMA) Crash Reconstruction, Cybersecurity	18. Distribution Statement This document is available on CDOT’s website https://www.codot.gov/programs/research

19. Security Classif. (of this report) Unclassified	20. Security Classif. (of this page) Unclassified	21. No. of Pages 22	22. Price

Table of Contents

1. Introduction 1

1.1 Incident Response and Crash Reconstruction 1

1.2 Cybersecurity and Digital Forensics 2

1.3 Connecting Crash Reconstruction and Cybersecurity 3

2. ATMA Data Overview 3

2.1 Onboard Powertrain Data Example 4

2.2 Kratos technology log files 6

2.2.1 Kratos Log Files 7

3. Law Enforcement Data Considerations for Accident Response 8

4. ATMA Data Collection and Correlation Testing 8

4.1 Test 1 – Sudden Deceleration – Leader Initiated Heavy Braking 10

4.2 Test 2 – Sudden Deceleration – ESTOP Leader 11

4.3 Test 3 – Sudden Deceleration – ESTOP Follower 11

4.4 Test 4 – Uncommanded Sudden Stop from Follower 11

4.5 Test 5 – Sudden Deceleration – Barrel Intrusion 12

5. Test Results 13

5.1 Test 1 – Sudden Deceleration ASTOP 13

5.2 Test 2 – Sudden Deceleration – ESTOP Leader 15

5.3 Test 3 – Sudden Deceleration – ESTOP Follower 16

5.4 Test 4 – Uncommanded Sudden Stop from Follower 19

5.5 Test 5 – Sudden Deceleration – Barrel Intrusion 19

6. Data and Security Recommendations 21

6.1 Recommendation 1: Improve Data Attribution 21

6.2 Recommendation 2: Produce Clear and Concise ATMA Data Retrieval Procedures 22

6.3 Recommendation 3: Deliver a user friendly ATMA log analysis tool 23

6.4 Recommendation 4: Clarify roles for support to interpret log files 24

6.5 Recommendation 5: Modify the ATMA logging system to continue to log after an ESTOP 24

7. Acknowledgement 25

8. References 25

List of Figures

Figure 1: Leader vehicle (left) and follower vehicle (right) comprising the ATMA system. 1

Figure 2: First page of the Cummins Powerspec Sudden Deceleration report depicting a hard braking test run from 13 Jan 2022. 5

Figure 3: Kratos Leader Vehicle Setup showing the ATMA control panel 6

Figure 4 Kratos Ethernet Setup in the leader vehicle allowing physical access to the server 6

Figure 5: A Google Earth depiction of GPS data points obtained from ATMA log files. 7

Figure 6: VBox Setup in the follower vehicle to collect TSPI. 9

Figure 7: VBox Setup in the leader vehicle showing the connection between antennas.............. 10

Figure 8: Nominal Test Setup for Test 1-3 – Sudden Deceleration Events.................................. 11

Figure 9: CDOT Limon Yard Entry Uncommanded Stop – Test Event 4.................................... 12

Figure 10: CDOT Limon Yard Setup for Test 5 Barrel Instrusion... 13

Figure 11: Run 1 14

Figure 12: Run 2 15

Figure 13: Run 3 16

Figure 14: Run 4 16

Figure 15: Run 5 17

Figure 16: Run 6 18

Figure 17: Run 7 19

Figure 18: Run 8 20

Figure 19: Run 9 21

Figure 20 Kratos ATMA Log File Login Screenshot showing ‘root’ username.......................... 23

1. Introduction

This report is a supplement and extension to the Autonomous Truck Mounted Attenuator (ATMA) Incident Tabletop Exercise conducted by the Colorado Department of Transportation (CDOT) and All Clear Emergency Management Group. The approach of this project was to use the tabletop exercise for guidance and motivation to further explore data retrieval, extraction, preservation, interpretation, and security necessary to conduct an investigation resulting from an incident with an ATMA.

The Tabletop Exercise was held on 8 July 2021. However, the one-day event was insufficient to study the ATMA systems in depth, which is needed to understand the types of data available and how to extract the data. This report will provide an overview of data and analysis currently available for the vehicle powertrain systems and the Kratos Autonomous Impact Protection Vehicle (AIPV) system available at the CDOT facility in Limon, Colorado in the year 2021 and 2022. This system includes a leader vehicle, which is the paint striping vehicle, and the follower, which is the AIPV, as shown in Figure 1.

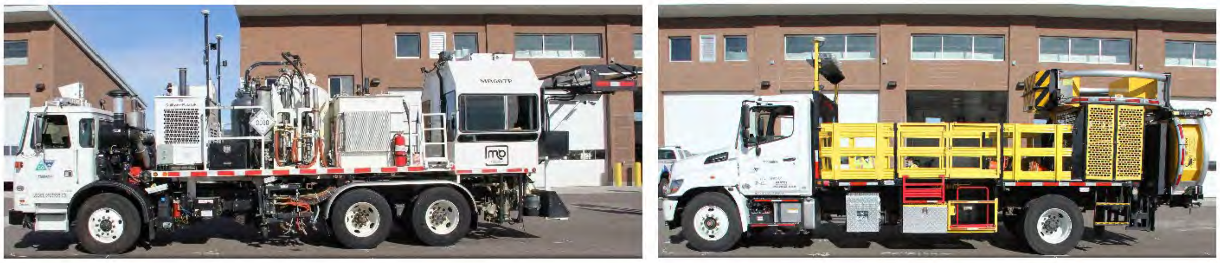


Figure 1: Leader vehicle (left) and follower vehicle (right) comprising the ATMA system.

1.1 Incident Response and Crash Reconstruction

When a crash happens on the highway, our society demands to understand why to improve public safety, vehicle and road design, and appropriately settle on insurance claims. In some cases, there are disputes that are settled in a court of law. These can be either civil or criminal proceedings. To conduct such hearings and trials, there must be evidence provided to substantiate the claims. This evidence may include the physical and digital evidence from the vehicles involved.

Physical evidence associated with traffic crashes has been the primary source of evidence for many years. These include things like tire marks, vehicle damage, scene measurements, and material transfers. In the mid-1990s, a new form of crash evidence became available in the form of event data recorders, which were primarily included as part of the air bag system. General Motors included crash pulse information in an Event Data Recorder, EDR, as an integral part of their airbag control module called the Sensing and Diagnostic Module, SDM. In subsequent decades additional sources of event records and digital evidence became available including precrash information. Each new type of data usually has some supporting research to demonstrate its efficacy in a court of law. The Daubert criteria is used to determine admissibility. This criterion requires the data be testable, published and peer reviewed, a known error rate, standards controlling the technique and the scientific community commonly accepts the method. All of these criteria have been met and a great deal of case law already exists surrounding the admissibility of digital data recorded prior to and during a crash. A contribution of this report and corresponding data is to provide independent verification of the accuracy of the data available from the ATMA system that may be useful in a crash investigation.

Often the vehicles involved in the incident are taken under law enforcement control during the initial investigation. Law enforcement must decide on whether to refer criminal charges to the district attorney. The basis for this decision may depend on the details revealed through interpreting the physical and digital evidence available to the investigators, which means investigators must be able to retrieve an interpret the data from the vehicles. With new or rare systems, like the ATMA, this process is not well known. Therefore, the goal of this report is to provide guidance to extract the data useful for incident investigation.

1.2 Cybersecurity and Digital Forensics

A hypothetical incident may result from a cyber-attack. However, the evidence of the attack is not well known, and may be easily conflated with other traditional crash causation mechanisms. The field of digital forensics as it applies to servers, personal computers, laptops, and cell-phones is well established and many investigative bodies have a digital forensics division. The forensics of the computing devices on the ATMA is out of scope for this report; however, if there was a suspected cybersecurity breach, then the digital forensics investigators should be requested to handle the additional computing devices from the AIPV system. This includes the visual display tablet computer and the system control unit.

During the process of collecting data and researching the system, the researchers noticed some cybersecurity concerns related to the ATMA. The top three concerns are as follows:

1. Recovery of data required root access to the system. This elevated privilege could allow for unintended actions, such as theft of intellectual property, loading of malicious operating code, and the destruction of evidence.
2. System requirements for cybersecurity are not specific nor based on the roles of the principals interfacing with the system. It is recommended that future acquisitions specify security and safety requirements in accordance with the processes highlighted in SAE/ISO 21434 Road Vehicles – Cybersecurity Engineering.
3. Passwords used to login to the system are fixed and well known. This decreases the challenges associated with social engineering or password cracking to gain access to the system.

Digital forensic elements for heavy vehicles were introduced by Daily, et al. in SAE 2014-01-0495 [1]. There are 3 levels of examination for a heavy vehicle system. The most invasive is at a chip level where individual data bearing chips are removed from the circuit board and the contents are read and decoded. This is a destructive method of forensic examination and was not used for this project. The second level of investigation is at the board level where the data bearing chips and microprocessor are examined using in-circuit debugging and programming ports, like the JTAG port. This requires access to the circuit board and is invasive to the system.

The enclosure would need repaired for the electronic control unit to be put back in service. This is also out of scope for this project. The last approach to acquire digital forensic data from heavy vehicles is to download it over the in-vehicle network. This is usually done with a diagnostics service tool and was used for this project. Specifically, the data from the Cummins-powered leader vehicle was gathered using the Cummins PowerSpec software.

1.3 Connecting Crash Reconstruction and Cybersecurity

Autonomous systems require computational resources to actively make decisions on vehicle operations without human input. These systems rely on sensing technologies, physics, and decision engines. While operating heavy vehicles autonomously is a feat and shows immense promise, the current implementation and deployment of these autonomous systems have enjoyed a non-adversarial environment. However, to grow and scale the ATMA program, the system will need to be robust in an adversarial environment. The cybersecurity of the system needs to be assessed and the threats and potential attack vectors need to be explored and any discovered vulnerabilities will need to be addressed.

A potential effect of a cybersecurity attack on the ATMA barrier would lead to a traffic crash. Interestingly, the AMTA barrier is designed to dissipate the energy of a vehicle that potentially strikes it. In fact, this scenario may be an inevitability, in which the barrier technology should slow down the dissipation of energy. However, when crashes happen, the sequence of determining crash causation starts with a traffic crash reconstruction. This process gathers physical and digital evidence associated with the crash and reconstructs the events that lead to the crash. This process is not well understood with AMTA since the technology is emerging.

The connection between cybersecurity and crash reconstruction is two-fold: 1) much of the evidence needed to accurately reconstruct the traffic crash is digital in nature and needs to be preserved in a secure manner, and 2) a potential of a cybersecurity breach could lead to a crash. Therefore, it is critically important to undergo a study where a forensic investigation is conducted (i.e. an exercise in data gathering from a simulated crash event).

It is important to understand how to investigate a crash when it happens. What do crash investigators do when they first arrive on scene and gather data? The data they need are both physical, (i.e. photographs and measurements), and electronic from event data recorders, video feeds, and operating logs. How does law enforcement request the appropriate data and how accurate is it? This report highlights answers to these questions.

2. ATMA Data Overview

The forensic data from the ATMA system (leader and follower) include the following:

- Kratos AIPV log file stored on the follower
- Heavy Vehicle Event Data Recorder (HVEDR) data from the leader
- Heavy Vehicle Event Data Recorder (HVEDR) data from the follower (if available)

These data are stored in non-volatile memory and can be retrieved from the vehicle after an incident. There are other data that may be available if the vehicle is still powered when investigative personnel arrive at the scene. These are the temporary log files from the system computers for the AIPV system.

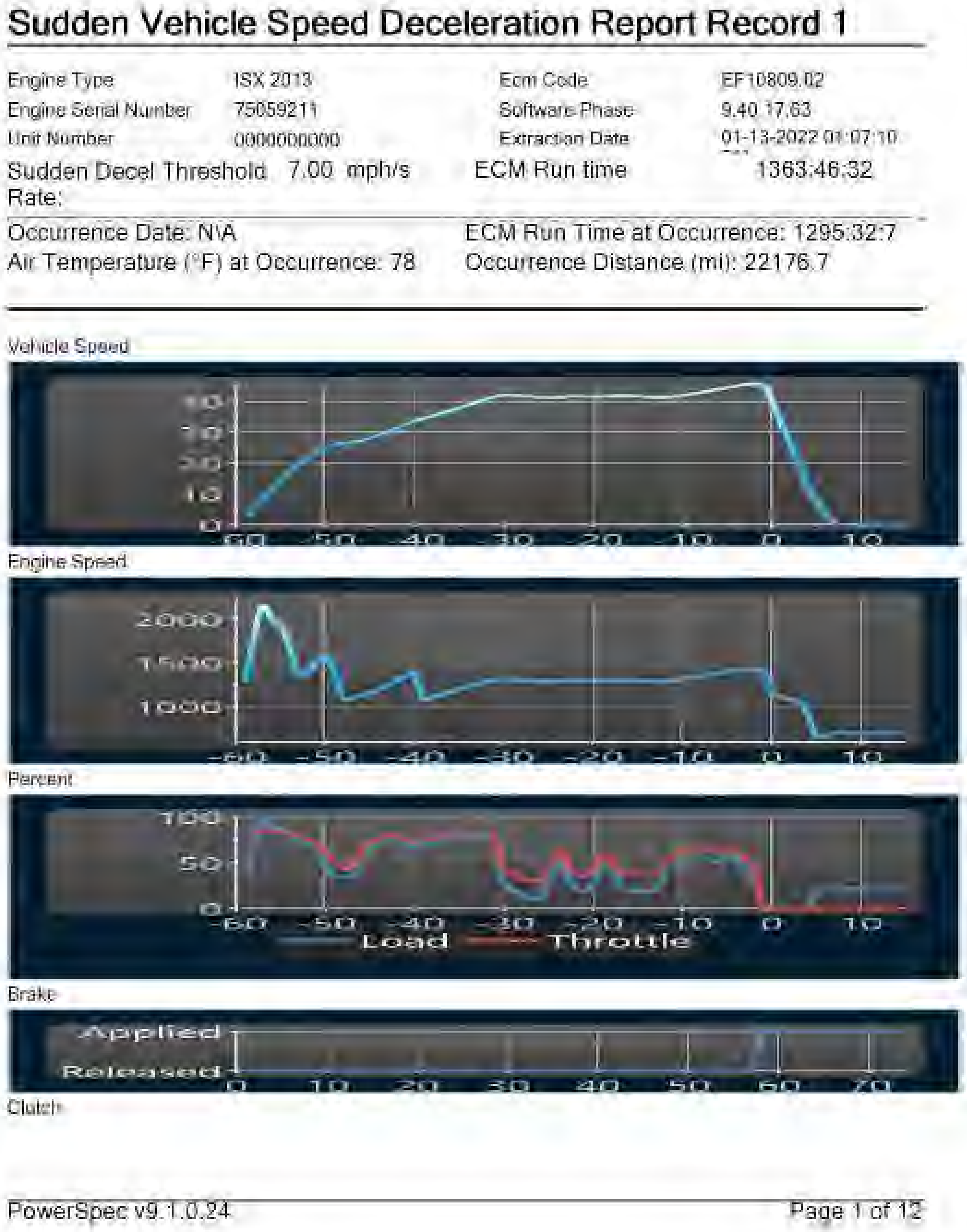
Live data may be used for study and verification. The live data is not stored on the system, but it reflects the current system operation. This live operational data is available on the in-vehicle network utilizing the SAE J1939 standard for communications. There is also live data available on the AIPV Ethernet network; however, the meaning of that data is not known outside Kratos.

2.1 Onboard Powertrain Data Example

The heavy vehicles the ATMA system is installed on still retain all OEM J1939 data available on the CAN bus. This data is not modified as a part of the ATMA system. Data available on the CAN bus includes engine, transmission, and brake controller network log files. As a part of this effort, CAN data logs were extracted from the ATMA leader and follower vehicles during our testing on 13 Jan 2022. These log files can show system developers what data is available from the network.

For the ATMA vehicles in Limon, CO, the leader vehicle is equipped with a Cummins engine which provides additional data via the Cummins PowerSpec application. The follower vehicle is equipped with a Hino engine which does not have the additional data logging. The Cummins PowerSpec software extracts data that provides an event recorder for hard braking events, which is defined by changing speed faster than 9 mph per second. These hard braking were collected after each test on 13 Jan 2022, which is described in an upcoming section. An example of the first page of the PowerSpec data, detailing a sudden deceleration / hard brake event, is shown in Figure 2. Full versions of this report are included in the data repository for this project as maintained by CDOT.

These vehicle data files would be extracted during a traditional heavy vehicle accident investigation. For the ATMA system it is expected these files would be collected in the process of an accident investigation as well. They are not modified as a part of the ATMA system and do not require any additional steps to access or retrieve than a traditional truck.



Sudden Vehicle Speed Deceleration Report Record 1

Engine Type	ISX 2013	Ecm Code	EF10809.02
Engine Serial Number	75059211	Software Phase	9.40 17.63
Unit Number	0000000000	Extraction Date	01-13-2022 01:07:10
Sudden Decel Threshold Rate:	7.00 mph/s	ECM Run time	1363:46:32

Occurrence Date: N\A
ECM Run Time at Occurrence: 1295:32:7
Air Temperature (°F) at Occurrence: 78
Occurrence Distance (mi): 22176.7

PowerSpec v9.1.0.24 Page 1 of 12

Figure 2: First page of the Cummins Powerspec Sudden Deceleration report depicting a hard braking test run from 13 Jan 2022.

2.2 Kratos technology log files

In addition to the vehicle data available via the J1939 interface, separate log files are recorded in the Kratos Technology ATMA system. The leader vehicle control station is pictured in Figure 2 and the Ethernet connection provides access to the data is pictured in Figure 3. It is important to note that the Kratos data logging system is separate from the vehicle CAN Bus network. It requires a direct Ethernet connection access the log files. Download of the Kratos ATMA log files requires a browser input of a specific IP address along with a username and password. Of note, a recommendation for security is to implement a non 'root' username and a lower permission level for the data extraction, see Figure 20. Kratos log files were captured during our series of tests of the ATMA system on 13 Jan 2022.

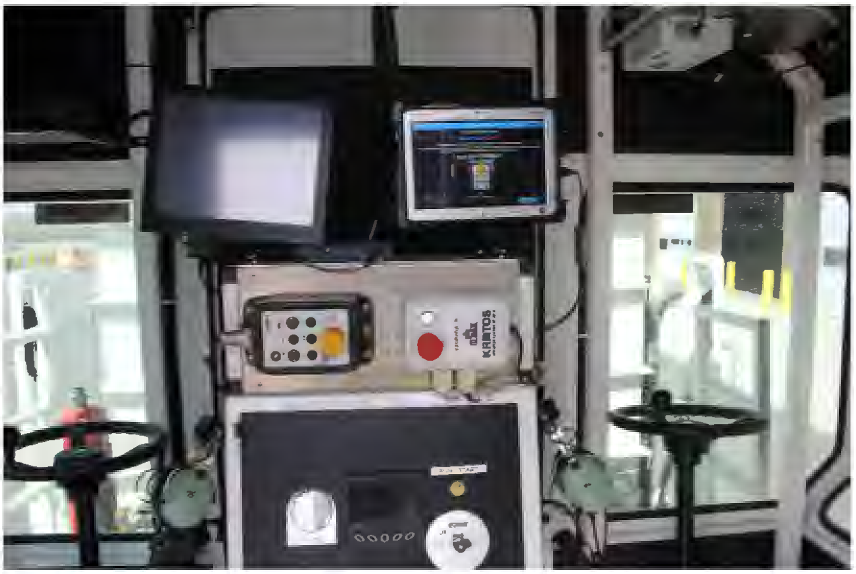


Figure 3: Kratos Leader Vehicle Setup showing the ATMA control panel

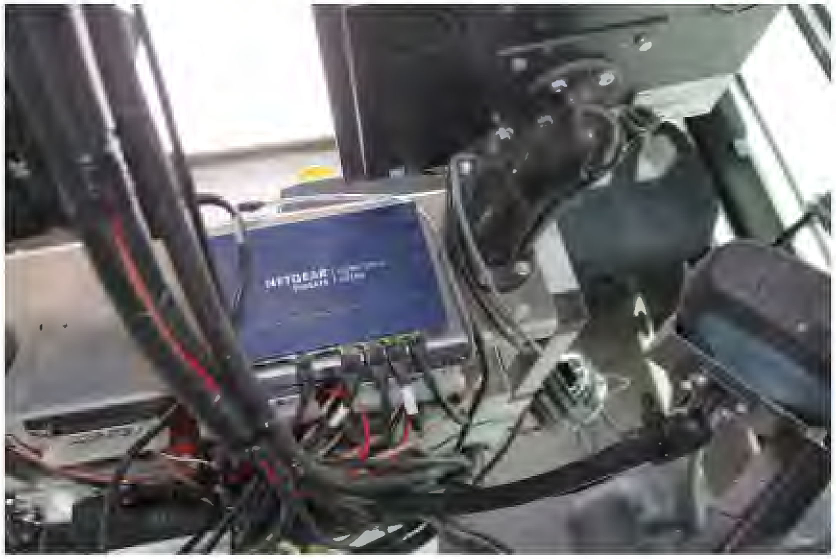


Figure 4 Kratos Ethernet Setup in the leader vehicle allowing physical access to the server

2.2.1 Kratos Log Files

The log files available on the Kratos system include a combination of .csv and .txt log files.

The log files available on the ATMA console include the following:

1) Date_time_nav.csv
2) aipv_msg_broker.log
3) gps.log
4) leader.log
5) nav.log
6) overhead.log
7) timeset.log

The primary log file is labeled Year-Month-Day_Time_log. This log file provides the data described in Table 1. Full log files have been delivered along with this report and should be available on the CDOT file share.

Table 1. Data Headers from ATMA CSV Log File

Vehicle	Crumb	Stamp	Lat	Lon	Alt	Heading	Heading (Desired)	Velocity
Velocity (Desired)	Gap	Gap (Desired)	#of Satellites	Valid	CTE	Accel	Steer	State

GPS latitudinal and longitudinal data can be imported from the nav log file to Google Earth, as shown in Figure 5. Of note, the data fields do not include any data fields extracted from the CAN bus. As such correlation of the data directly to the on-board data extracted from the truck systems is more challenging. Further discussion on this and recommendations is included in Section 6.

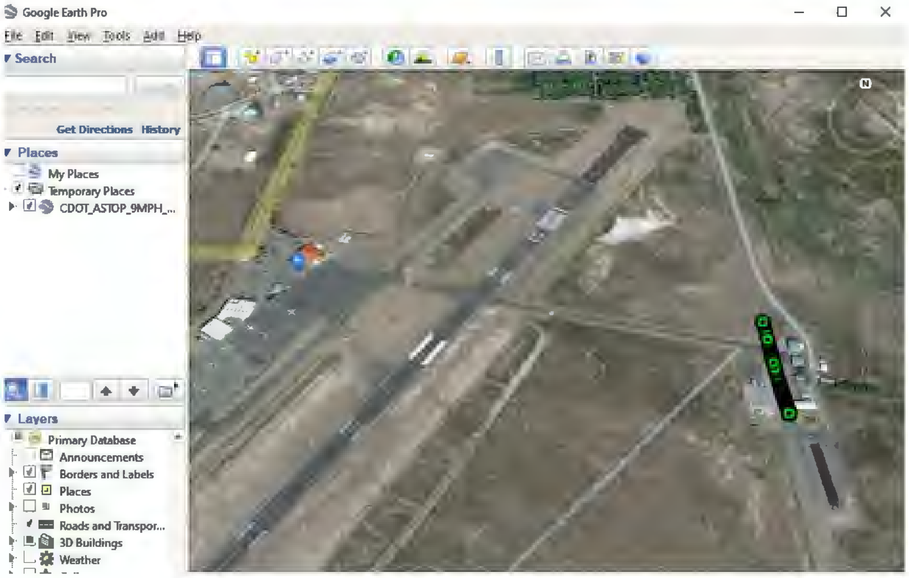


Figure 5: A Google Earth depiction of GPS data points obtained from ATMA log files.

3. Law Enforcement Data Considerations for Accident Response

This section describes additional law enforcement considerations for incident response specific to the ATMA.

Any serious injury or fatal collision is challenging with regard to response, both immediate and long term. Life saving measures take a clear priority in an initial response. Once life saving measures have been addressed the next priority becomes security. In a traditional collision scenario the primary concern is scene security. A response to an ATMA collision is no different for protecting physical evidence at the scene, however a new challenge is introduced regarding securing the autonomous vehicle and securing any data. The data within the autonomous vehicle becomes a priority within the scene. Many heavy commercial vehicles can have data spoliated if the ignition is turned on, or left on. It is crucial that the crews operating the autonomous vehicle know how to respond to secure data. The spoliation of data can create a liability.

It is important to consider that in the event of a fatality or even serious injury, a collision scene becomes a crime scene. Access to the scene will be limited by law enforcement officials. A serious consideration should be made to include state police (or other police agencies where the ATMA will be operated) in training or familiarization. This will reduce the learning curve and also reduce any misunderstanding of what information can, should and will be collected and manners and mechanisms that will reduce chances of data spoliation. This will also assist the CDOT in understanding the legality of data recorded on vehicles and what will be needed by the police agency investigating just such a crash. The Federal Driver Privacy Act of 2015 [2] requires legal authority, either in the form of written, electronic audio or recorded permission or court order, to access data from an event data recorder (EDR). NHTSA defines an EDR as, “a device or function in a vehicle that records the vehicle's dynamic time-series data during the time just prior to a crash event (e.g., vehicle speed vs. time) or during a crash event (e.g., delta-V vs. time), intended for retrieval after the crash event. For the purposes of this definition, the event data does not include audio and video data [3]. As such, the recording capacity of the data logs falls under the EDR data requirement, however, assuming the vehicle is over 8500 pounds GVW, the recording of data is not required to meet the requirements for Part 563. Legal consultation is recommended for this one section based on the addition of much of the recorded data as it is associated with the autonomous features of this highly specialized vehicle.

As an investigation moves from the scene to the courtroom a consideration must be made for the retention of evidence. The vehicle itself will need to be preserved in its post -crash condition for inspection for both criminal and civil litigation. The ATMA may be placed in impound by the police agency investigating the collision. A consideration should be made for the extended storage of the vehicle in the event of a serious collision.

4. ATMA Data Collection and Correlation Testing

On 13 January 2022, the CSU research team and the CDOT ATMA team in Limon performed a series of tests focused on exhaustive data source collection and correlation to an external truth source. The test generated simulated potential crash data events associated with hard braking emergency stops and object intrusion between the leader and follower vehicles. Of note, this test series was not designed to test ATMA performance but rather to simulate potential accident-related scenarios to create data products of interest to investigators and understand what data is available from which source.

The tests centered around determining the utility of the data products available onboard the vehicles and the data logging devices specific to the autonomous functionality. In the testing, the team utilized Racelogic's VBox in both the leader and follower vehicles to provide a truth source for comparison of the collected vehicle data. Racelogic manufactures the VBox product as a high-fidelity Time Space and Position Information (TSPI) source compatible with mobile vehicle applications. It is an industry accepted source of truth for location and speed data during vehicle testing. Figure 6 and Figure 7 show some of the installation of the VBox onto the trucks. The VBox system has its own data recorder and its output was reconciled against that of the vehicle and autonomy solutions as shown in Section 5.

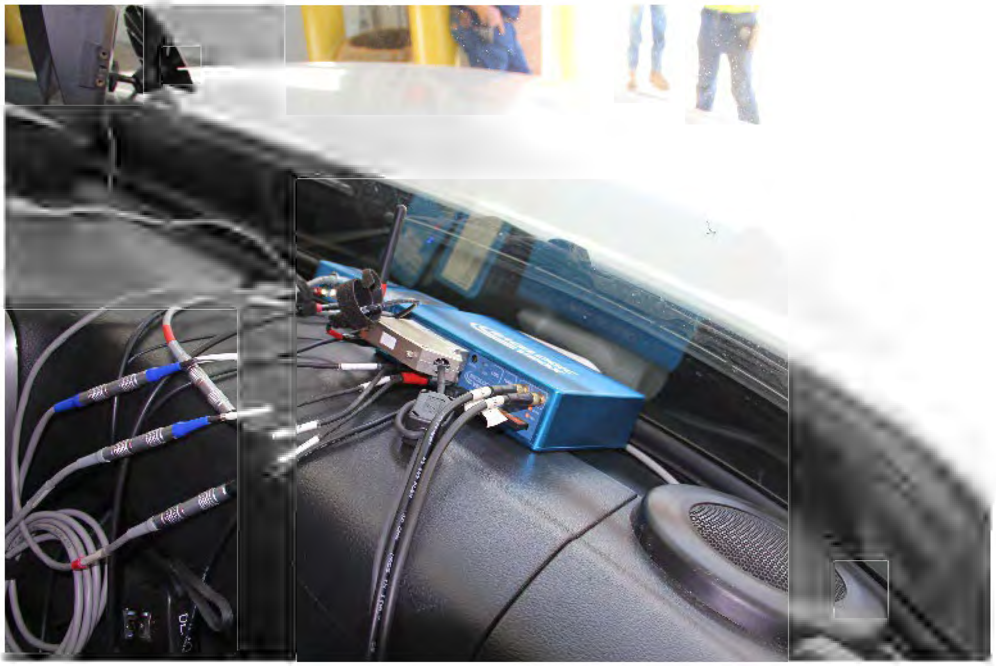


Figure 6: VBox Setup in the follower vehicle to collect TSPI.

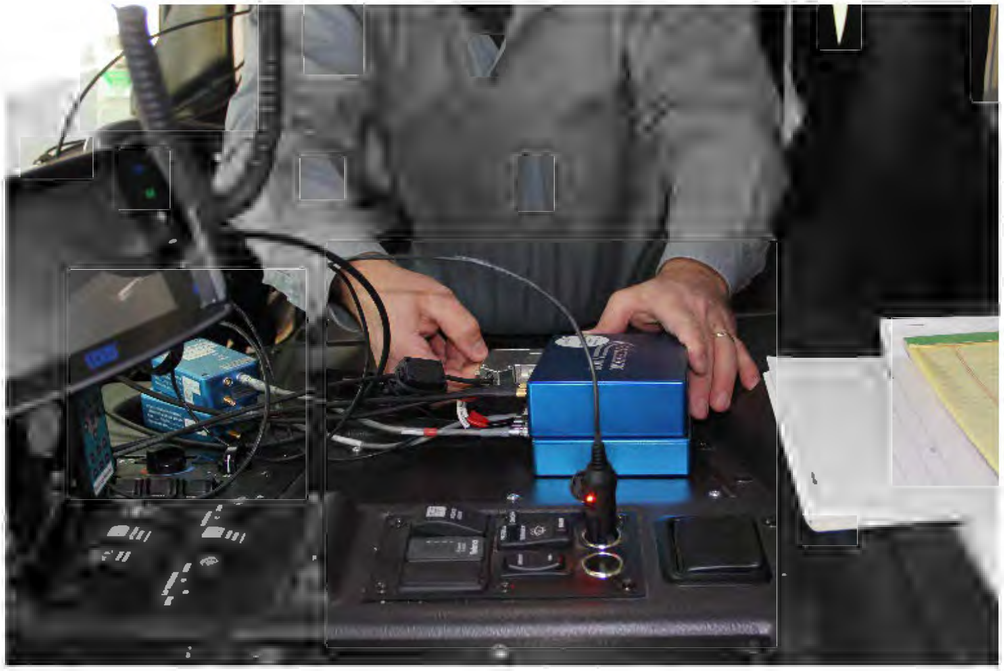


Figure 7: VBox Setup in the leader vehicle showing the connection between antennas.

The execution of the test events occurred on 13 January 2022 in Limon Colorado on a dry 55-degree Fahrenheit day. The nominal setup for tests 1-3, consisting of runs 1-6, is pictured in Figure 8. The leader vehicle was at least 100 ft in front of the follower vehicle, and the two were generally aligned laterally for the tests. Tests 1-3 exercised the various sudden deceleration modes of operation expected to be encountered in normal operating conditions. The specific mode of deceleration is described for each test scenario. Test 4 was an unplanned stoppage of the follower due to object detection. After completion of the deceleration testing, the team then transitioned to a service area where object intrusion, using a barrel, was exercised in Test 5.

4.1 Test 1 – Sudden Deceleration – Leader Initiated Heavy Braking

Runs 1 and 2 consisted of a sudden deceleration caused by the leader applying heavy braking. This caused the follower system to detect the braking with its onboard sensors and initiate its own hard brake, known as an ASTOP. The ASTOP event is not a manually triggered command; it is initiated by the follower when it senses the gap between it and the leader is rapidly decreasing or if the follower detects an intrusion between itself and the leader.

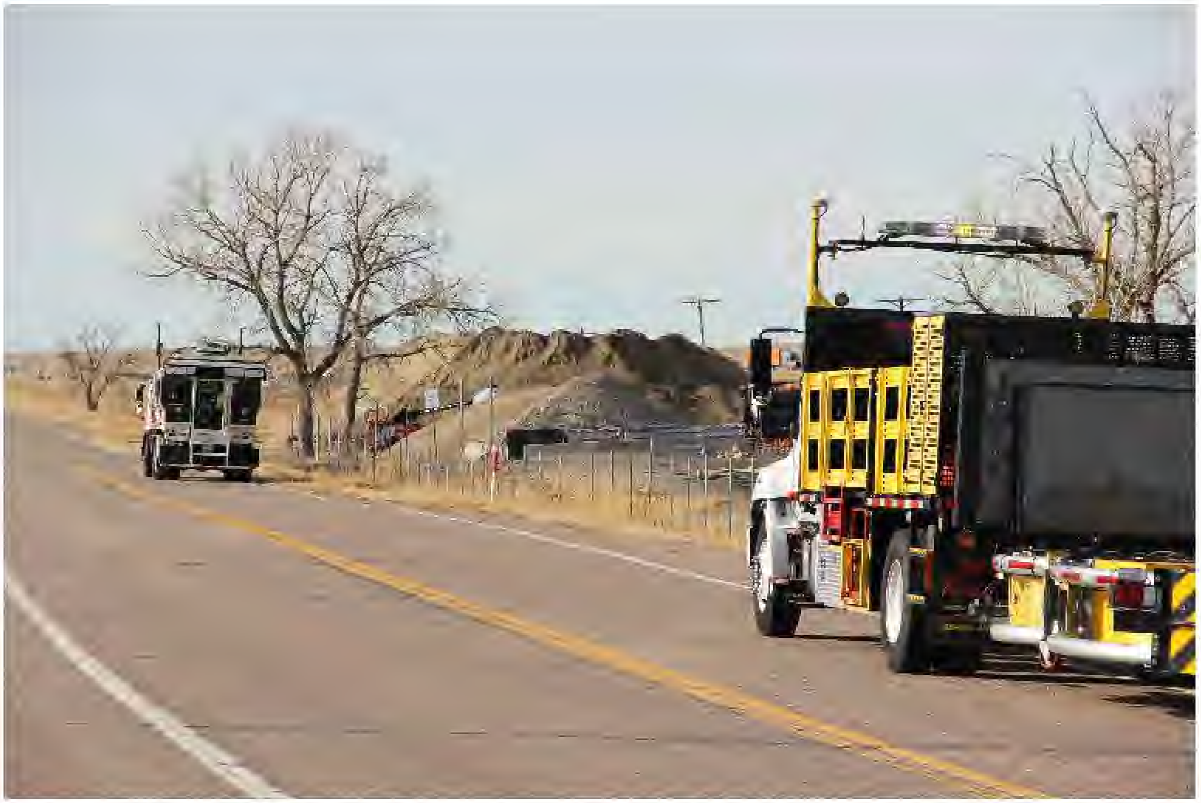


Figure 8: Nominal Test Setup for Test 1-3 – Sudden Deceleration Events

4.2 Test 2 – Sudden Deceleration – ESTOP Leader

Runs three and four consisted of a sudden deceleration caused by the leader depressing the ESTOP button onboard. This button triggers an Emergency stop in the follower vehicle. The ESTOP button does not trigger immediate braking in the leader, only the follower.

Of note, in these runs, it was discovered that the ESTOP command not only applies full braking power to the follower, it also kills the ignition power on the engine. This became problematic with the setup of the onboard data logs. Once ignition power was removed, the onboard ATMA logs ceased data recording. For these two runs, no data is recorded on the actual ESTOP event as the data logs terminate just before hard braking is applied upon termination of ignition power. The nominal test setup is shown in Figure 8.

4.3 Test 3 – Sudden Deceleration – ESTOP Follower

Runs 5 and 6 consist of a sudden deceleration event, but this time executed by the follower vehicle depressing the ESTOP button onboard. This button triggers an Emergency stop in the follower vehicle. The ESTOP button does not trigger immediate braking in the leader, only the follower. As noted previously, the ESTOP button does remove ignition power so the ATMA vehicle logs terminate prior to hard braking being applied.

4.4 Test 4 – Uncommanded Sudden Stop from Follower

While transiting between locations from Test 3 to begin Test 5, the team was able to record an unplanned test event. While in autonomous follow mode, the trucks required a 90-degree left turn to enter the test setup area for Test 5, followed by another 90-degree turn to the right, shown in Figure 9. Upon completion of the first 90-degree turn the follower triggered an ASTOP. This was not expected as hard braking did not occur and no known intrusions to the path occurred. The team suspects an object in the yard to the edge of the drive path may have triggered an object sensor and triggered the ASTOP.

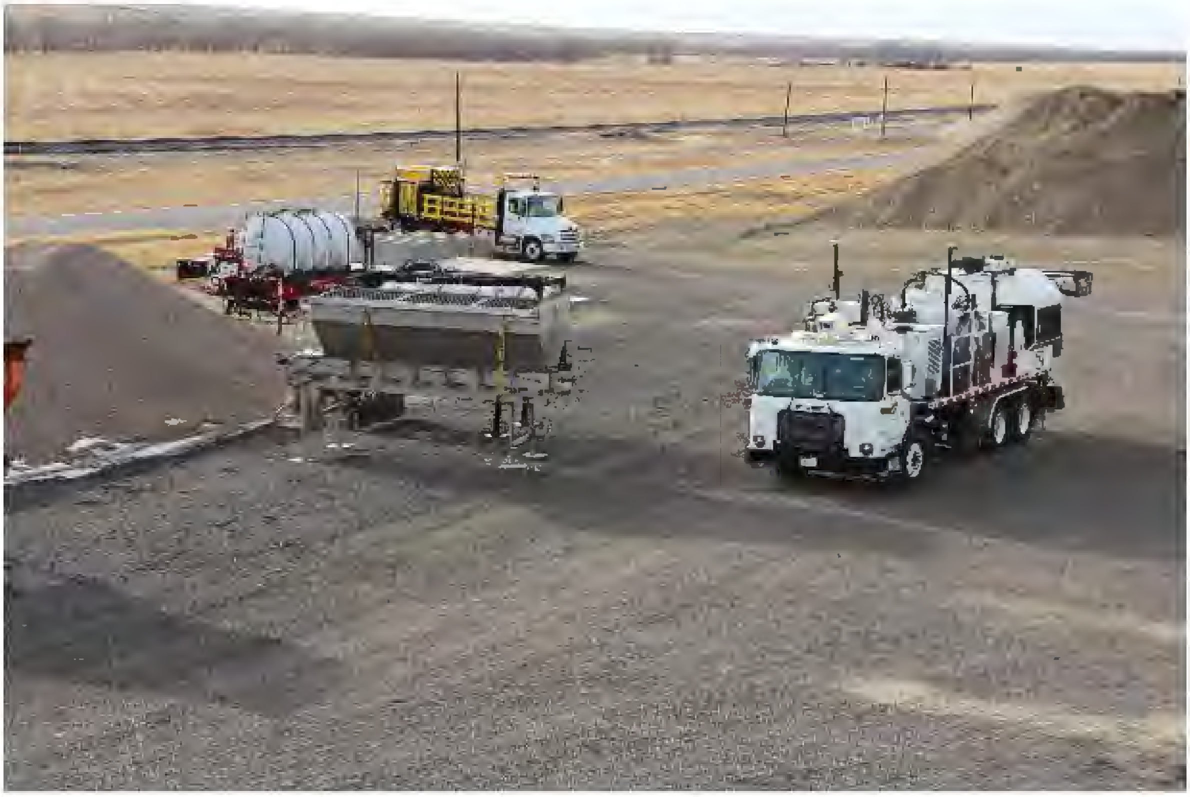


Figure 9: CDOT Limon Yard Entry Uncommanded Stop – Test Event 4

4.5 Test 5 – Sudden Deceleration – Barrel Intrusion

Runs 8 and 9 consisted of a sudden deceleration event, but this time triggered by a team member rolling a barrel in between the leader and follower vehicles, as seen in Figure 10. This obstacle intrusion triggers an ASTOP in the follower vehicle.

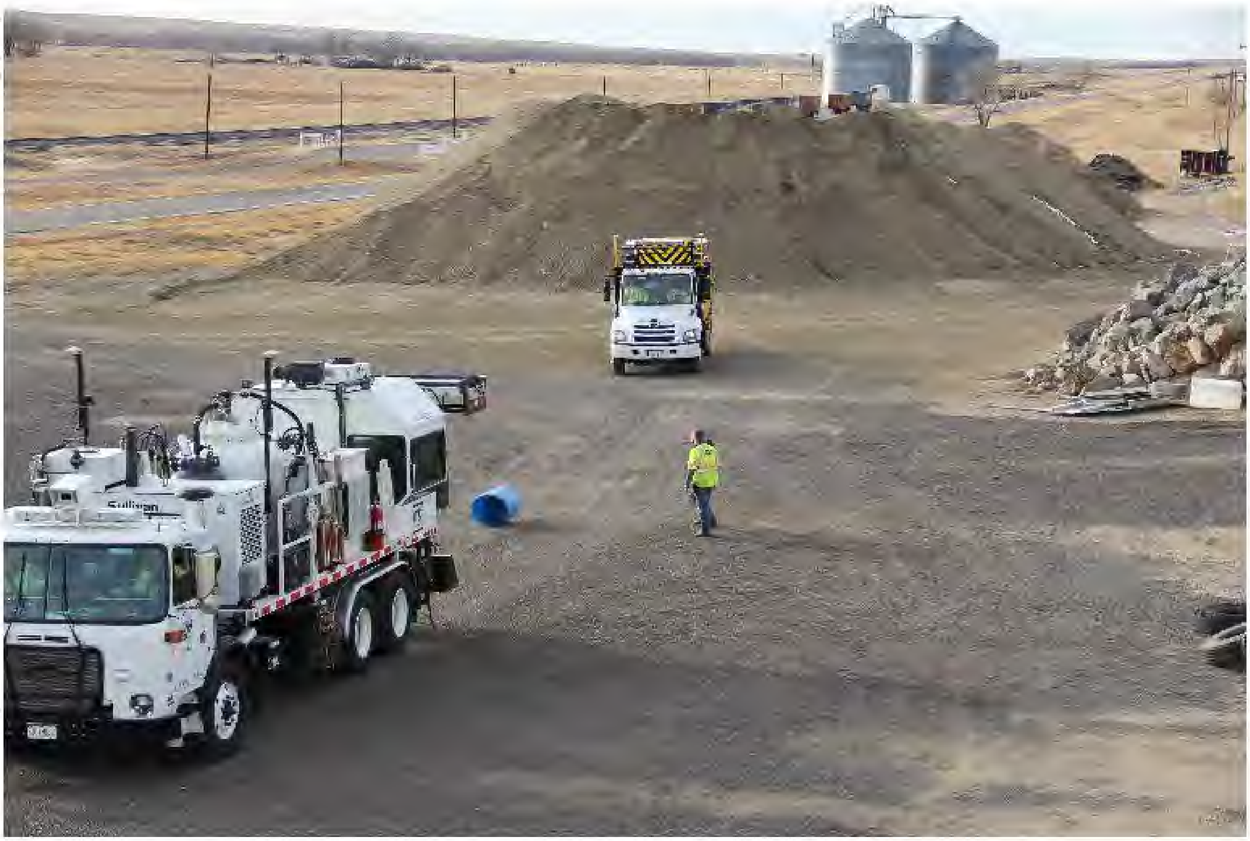


Figure 10: CDOT Limon Yard Setup for Test 5 Barrel Instrusion

5. Test Results

This section will document the data collected ruing the test runs and discuss any anomalies encountered during the events. Figures 10-18 plot the data collected during the test events on 13 January 2022. The plots include 6 distinct data sources plotting speed and time values for each test event. The data sources include both leader and follower: VBox TSPI sources, J1939 CAN Bus wheel speed data, and Kratos AIPV log velocity data.

5.1 Test 1 – Sudden Deceleration ASTOP

The first two test events had the leader vehicle apply hard brakes and come to a quick stop. The results of the sudden deceleration events from runs 1 and 2 are shown in Figure 11 and Figure 12. The follower vehicle appeared to detect the rapid deceleration and initiate an ASTOP event coming to a similarly abrupt stop while maintaining close to the preset follow distance. Of note, this effort and report is focused on data collection methods and not performance testing, however some behavior was documented that may want to be reviewed further by ATMA performance and requirements experts. Run 1 went as expected and the data demonstrates close alignment between the sources of data. During Run 2 the follower vehicle entered a rapid deceleration as expected but then did not come to a complete stop with the same speed profile as the leader; instead, the follower vehicle slowed but then released brake pressure to roll forward before initiating full brake application, see Figure 12.

The end of the graphs (right side) shows a steep decent of speed with respect to time. These steep slopes are the highest accelerations. The graph in Figure 11 shows a consistent decrease in speed. However, in Figure 12, the speed change of the follower stops and the graph shows a slight increase in speed of the follower from about 5 to 6 km/h after the leader had stopped. There are three independent data sources for each vehicle shown in the graphs. Furthermore, the test team noticed the change in acceleration in the follower during run 2. This speed behavior would be consistent with the notion of trying to reduce the distance gap between the vehicles to the set amount, however, it is not the intent of this project or report to analyze the control algorithms and mode switching criteria for the AIPV system.

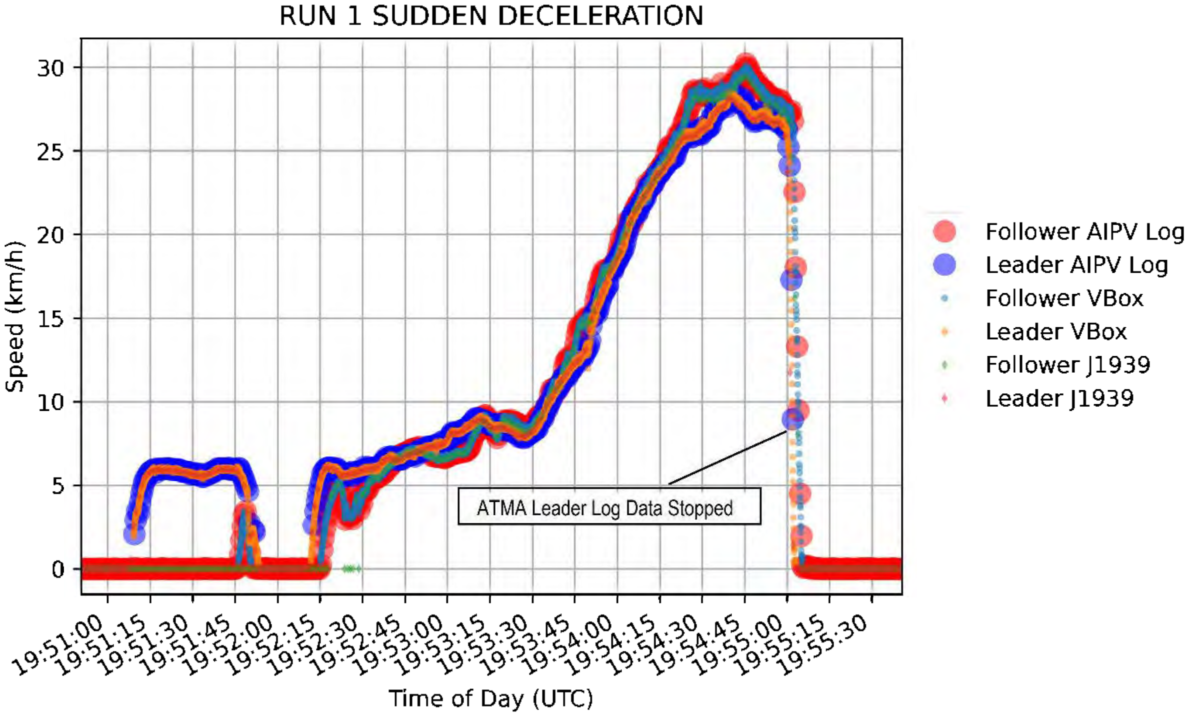


Figure 11: Run 1, sudden deceleration of the leader vehicle

The AIPV log files for these events were uploaded to the pooled fund Google Drive share. The log files for Run1 and Run 2 show the follower vehicle was operating in different states between runs. On run 1, as soon as the leader began his sudden deceleration, the logs show the detection of the leader's braking and the follower vehicle enters an ASTOP mode triggering its own rapid deceleration and full brake application. During Run 2, while the rapid deceleration occurred, the follower mode remained in RUN rather than changing to ASTOP as it did in Run 1. The leader's driving and operation were consistent between the runs.

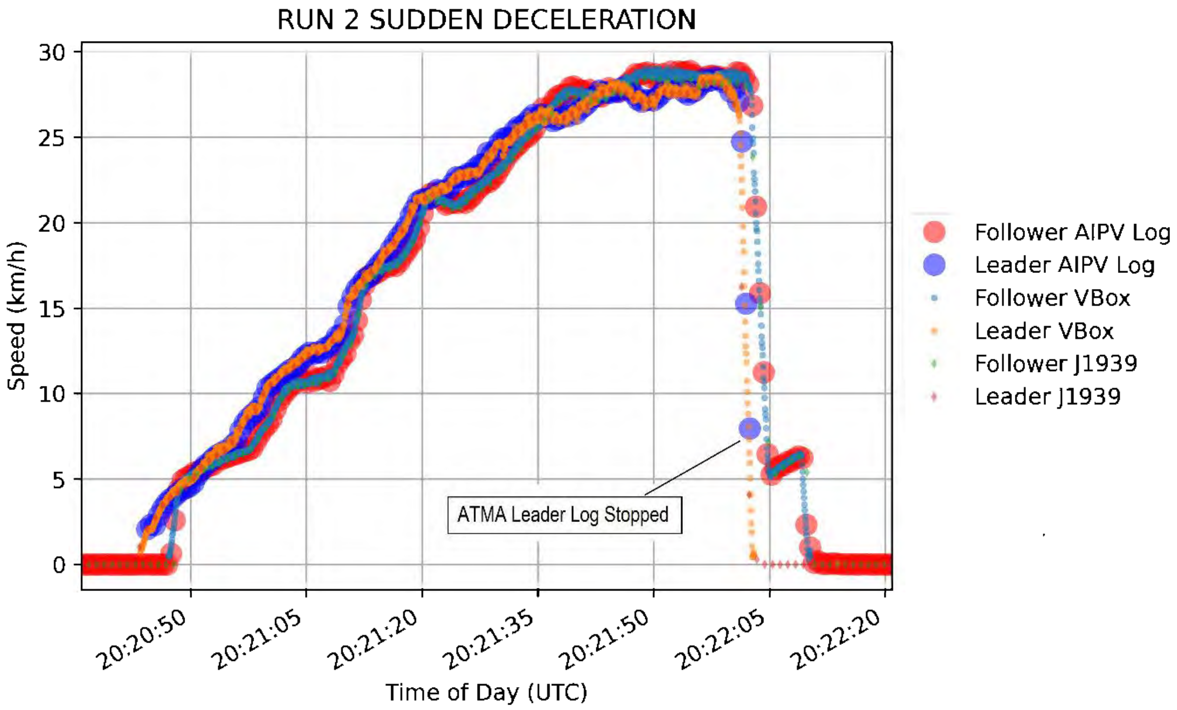


Figure 12: Run 2, sudden deceleration of the leader vehicle

5.2 Test 2 – Sudden Deceleration – ESTOP Leader

Runs 3 and 4 test the ESTOP functionality as triggered from the leader vehicle. The test engineer sat with the crew in the "dog house" of the paint striping vehicle. The ESTOP button was pushed by the test engineer. Shortly after initiating the ESTOP, the driver of the

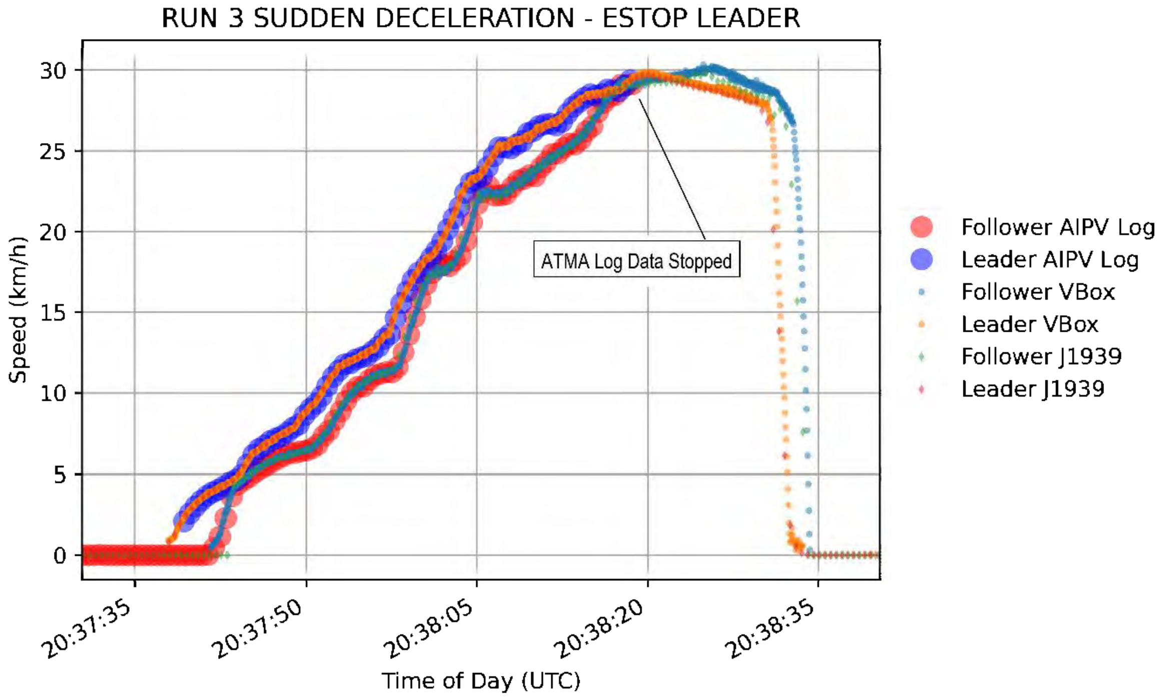


Figure 13: Run 3, Estop initiated in the leader vehicle during braking

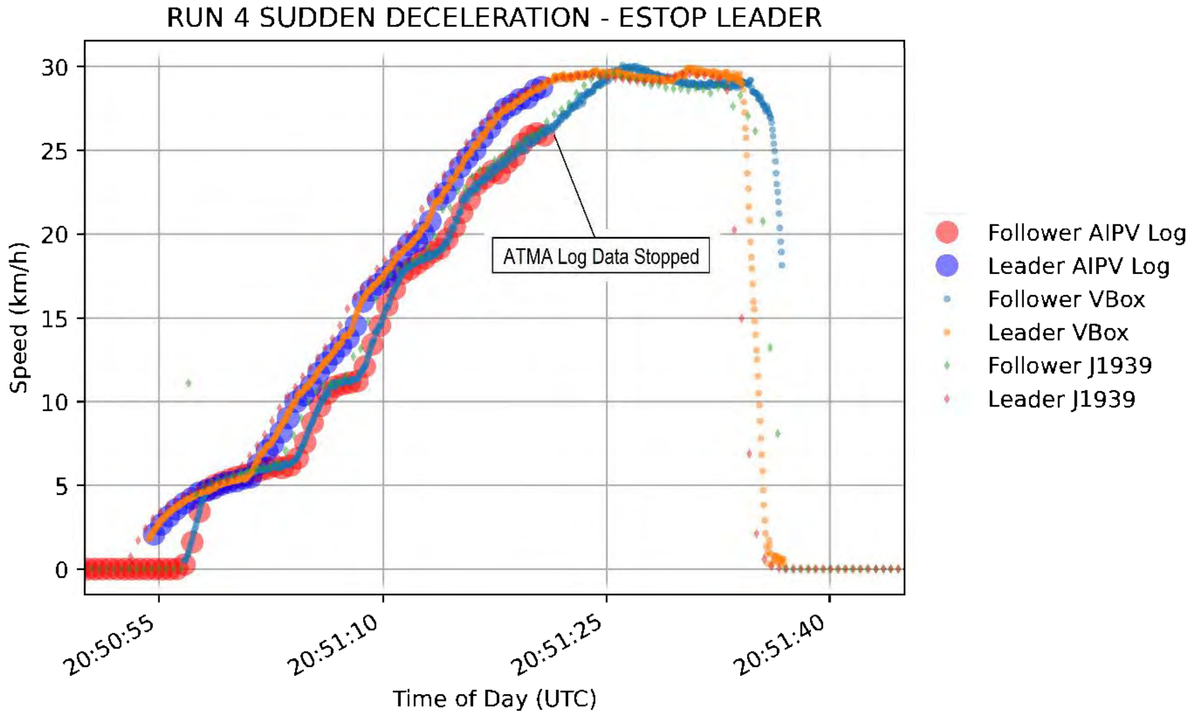


Figure 14: Run 4, Estop initiated in the leader vehicle during braking

5.3 Test 3 – Sudden Deceleration – ESTOP Follower

Runs 5 and 6 were again a sudden deceleration event, but this time executed by depressing the ESTOP button onboard the follower vehicle. This could happen if a safety observer is in the cab of the vehicle or crew presses one of the emergency stops on the outside of the vehicle. The goal of these tests was to examine and compare the AIPV log files with the external reference for different event triggering scenarios. Having the ESTOP on the follower depressed is a possible scenario.

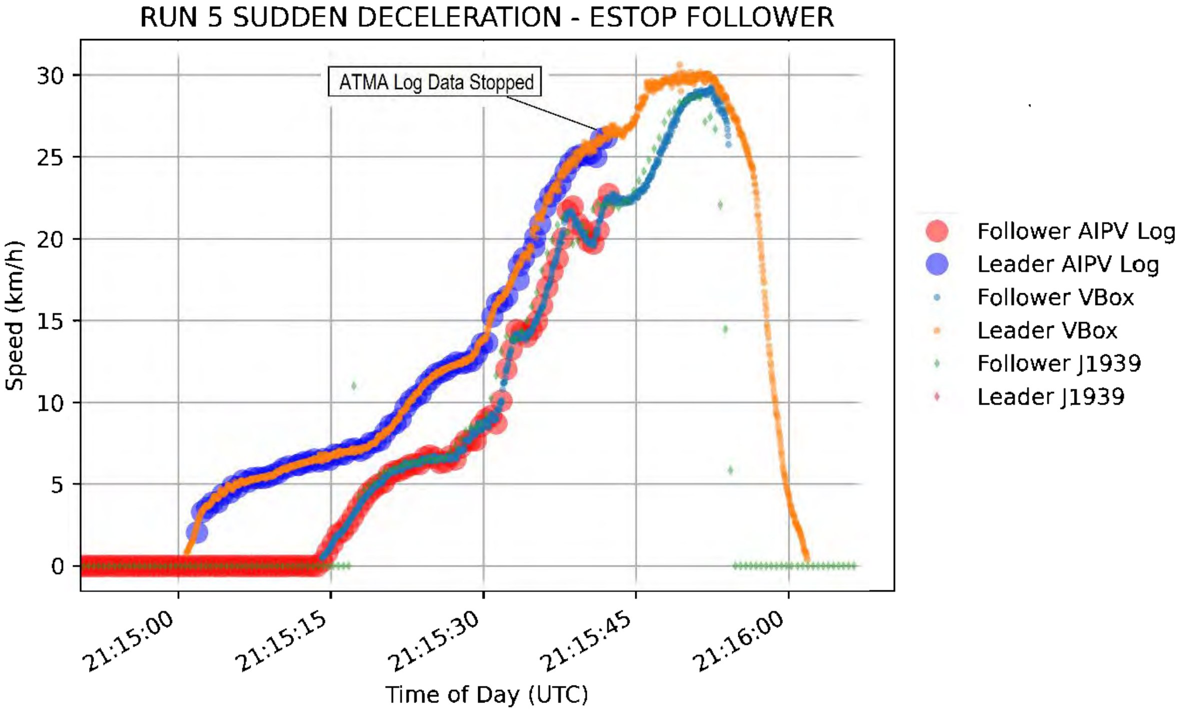


Figure 15: Run 5, follower initiated Estop followed by braking.

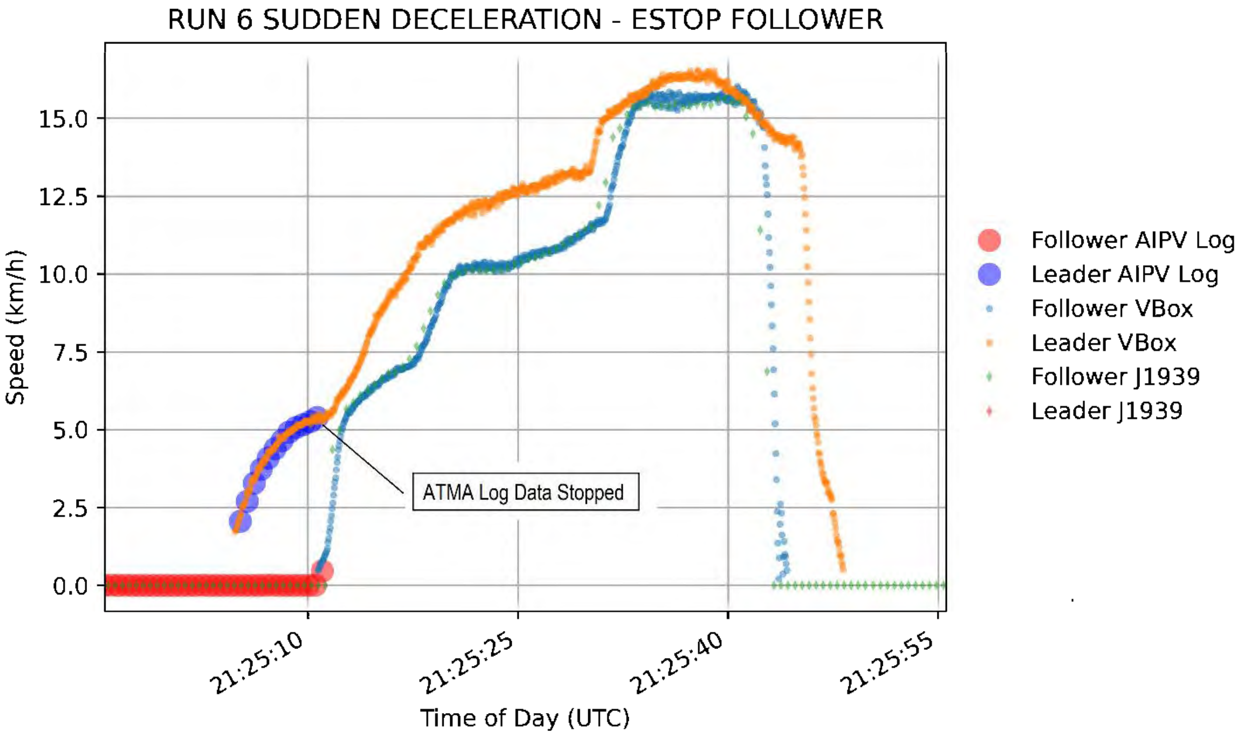


Figure 16: Run 6

Runs 5 and 5 shows the log files generated before an ESTOP fail to capture the speeds and operation of the system at or slightly before the ESTOP was pressed. The ESTOP was pressed at the time slightly before the speed record begins to rapidly decrease. Notice the speed record of the follower vehicle comes to a stop before the leader. This is because the human driver of the leader vehicle was reacting to the initiation of the ESTOP from visual and audio (hand-held radio) stimuli. The braking on the leader was a reaction and the human driver chose to apply hard brakes, which mimicked the follower. However, the leader speed could have easily slowed more gradually if the brakes were not applied as hard. The order of the braking events, (follower first, leader second) is different than Runs 3 and 4. Due to the similarity of the shapes of the graphs between tests 2 and 3, it can be confusing on which vehicle initiated the ESTOP and which vehicle came to a stop first. The causal chain of events is important for an incident investigator to determine. It is not clear to the authors as to why it appears as the data is missing.

Of concern with the ESTOP initiated events (Tests 2 and 3, Runs 3-6) is the recorded log files do not capture the true speeds and times of the vehicles at or around the time the ESTOP was pressed. This means the data available from the logs may not reveal the operations of interest to an incident investigator. If there is a desire for these log files to contain more data before and after an ESTOP is pressed, then the requirements for the system may need to be updated to reflect that data logging function. For the system under evaluation, the data from an ESTOP could older than 30 seconds and not reveal the true state of the vehicle during an incident. A careful examination of times and PowerSpec data will be needed to figure out what period of operation time the system logs reveal.

5.4 Test 4 – Uncommanded Sudden Stop from Follower

Test 4 (Run 7) was an unplanned test as the goal was to move towards Test 5 after the ESTOP tests. However, during the maneuver of turning left into the yard shown in Figure 9, the follower went into the ASTOP mode, so the team collected the data from the longer run ending in the left turn. The ATMA log files capture the operations of turn, which tool place at between 6 and 7 km/h, which is shown on the right side of the Run 7 graph.

The term "sudden stop" in the title of Run 7 is because the follower suddenly came to an unplanned stop. This is a slightly different meaning of a sudden stop as determined by a high deceleration rate. The research team did not determine the actual cause for the ASTOP in run 7 and this run was not repeated.

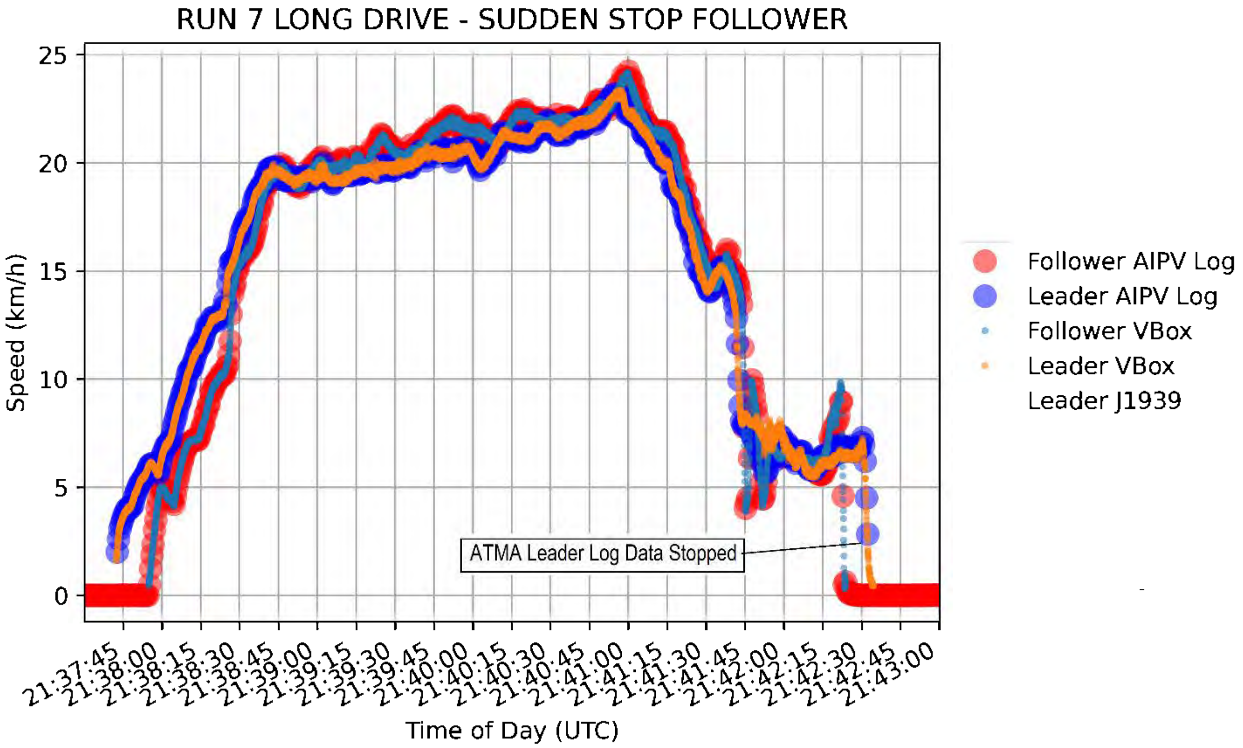


Figure 17: Run 7

5.5 Test 5 – Sudden Deceleration – Barrel Intrusion

Runs eight and nine where a sudden deceleration event, but this time triggered by a team member rolling a barrel in between the leader and follower vehicles. The barrel would simulate path intrusions and it is the author's understanding that such an intrusion would trigger a stop. It is possible for a path intrusion to preceded an incident, so examining the data associated with this event is important. The graphs in Figure 18 (Run 8) and Figure 19 (Run 9) shows the presence and accuracy of the AIPV log files. These will be helpful for incident investigations.

In Runs 8 and 9, the Follower vehicle stops first and the driver of the leader stopped in reaction to that event. The data on the leader's engine control module that is obtained with Cummins PowerSpec may not exist if the sudden deceleration trigger threshold was not exceeded. This means the data obtained during the PowerSpec data collection could be from a previous event. The investigator will need to properly attribute any of these records to the incident in question by examining mileage, engine hours, and real-time data available from the different records.

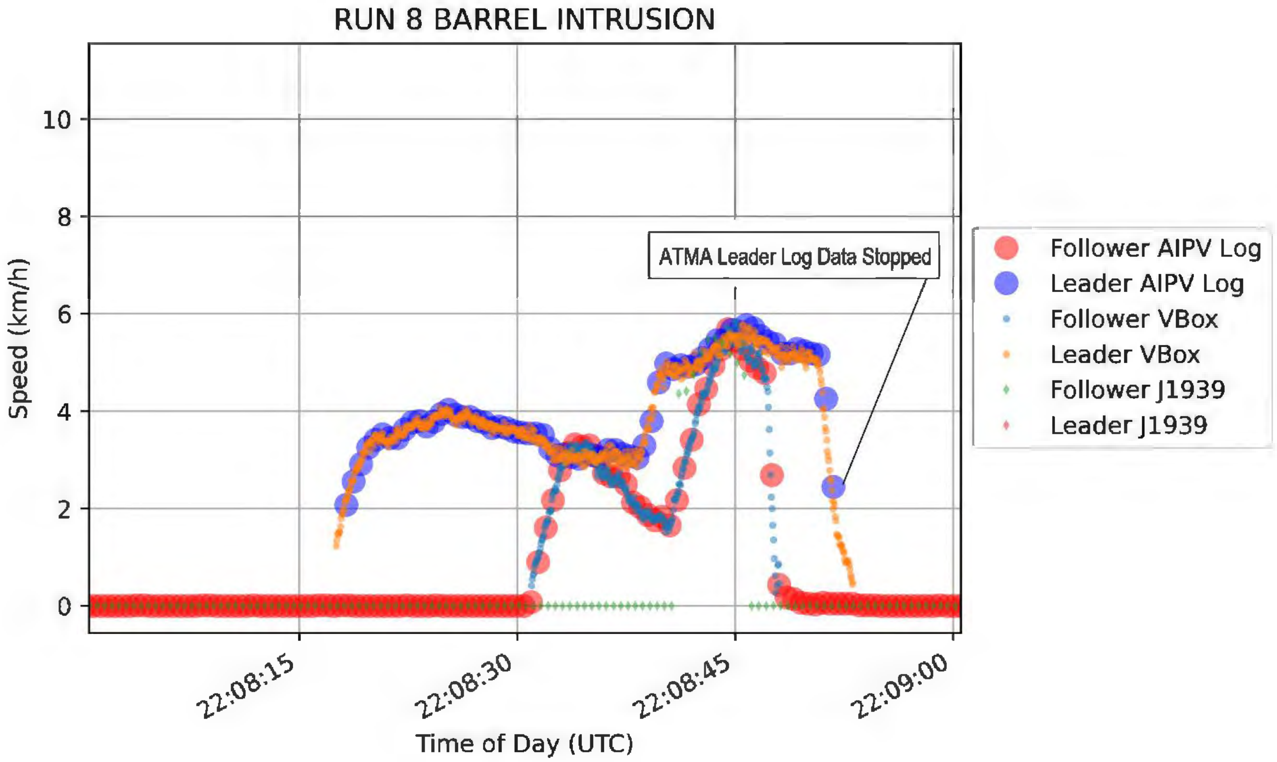


Figure 18: Run 8

5.6 Supplemental Data

For most runs, the following data was collected and is available in its raw form on the shared Google Drive for this project.

- Reference vehicle kinematic data (position, speed, heading) based on the Racelogic VBox 3i RTK for both the leader and follower. These are considered to be our accurate reference data.
- Vehicle J1939 log files in their original binary and translated ASCII form. These ASCII formatted files follow the format from the can-utils candump format used by SocketCAN in Linux. A J1939 database may be needed to decode the signals in the CAN logs.
- The AIPV logs and volatile log files from the follower system. These are in CSV format and can be examined with a text editor. Some utilities are available to convert coordinates into KML. Additional details and descriptions from the manufacturer of the headers and units would be helpful.
- Ethernet network packet captures (PCAPS) were recorded with Wireshark in the leader and follower vehicles during the tests.

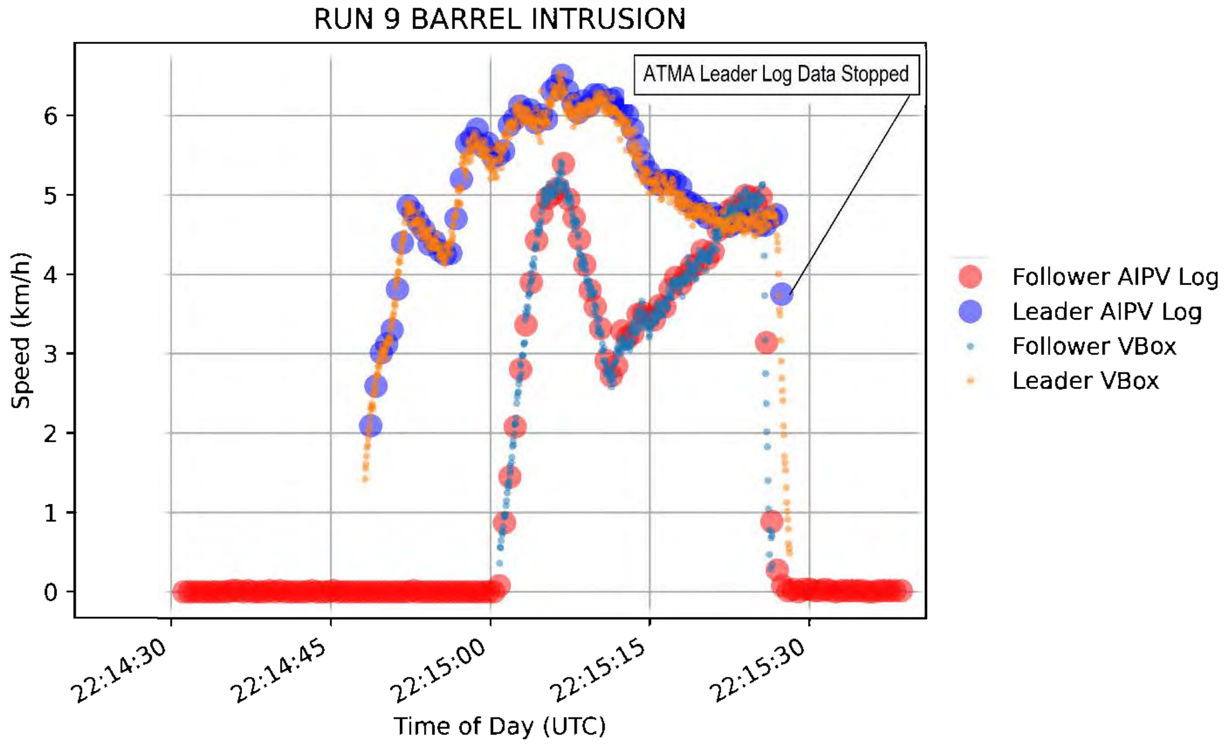


Figure 19: Run 9

- The Cummins PowerSpec data and the logs of extracting the data through an RP1210 adapter (DPA5) are also included. These were obtained as an investigator would – after the incident or event was over.

All of these data are organized in folders based on the runs. Additional helper files and plotting utilities are also on the shared drive.

6. Data and Security Recommendations

This section will detail recommendations generated by the CSU team from both the tabletop exercise and hands-on testing of the ATMA system.

6.1 Recommendation 1: Improve Data Attribution

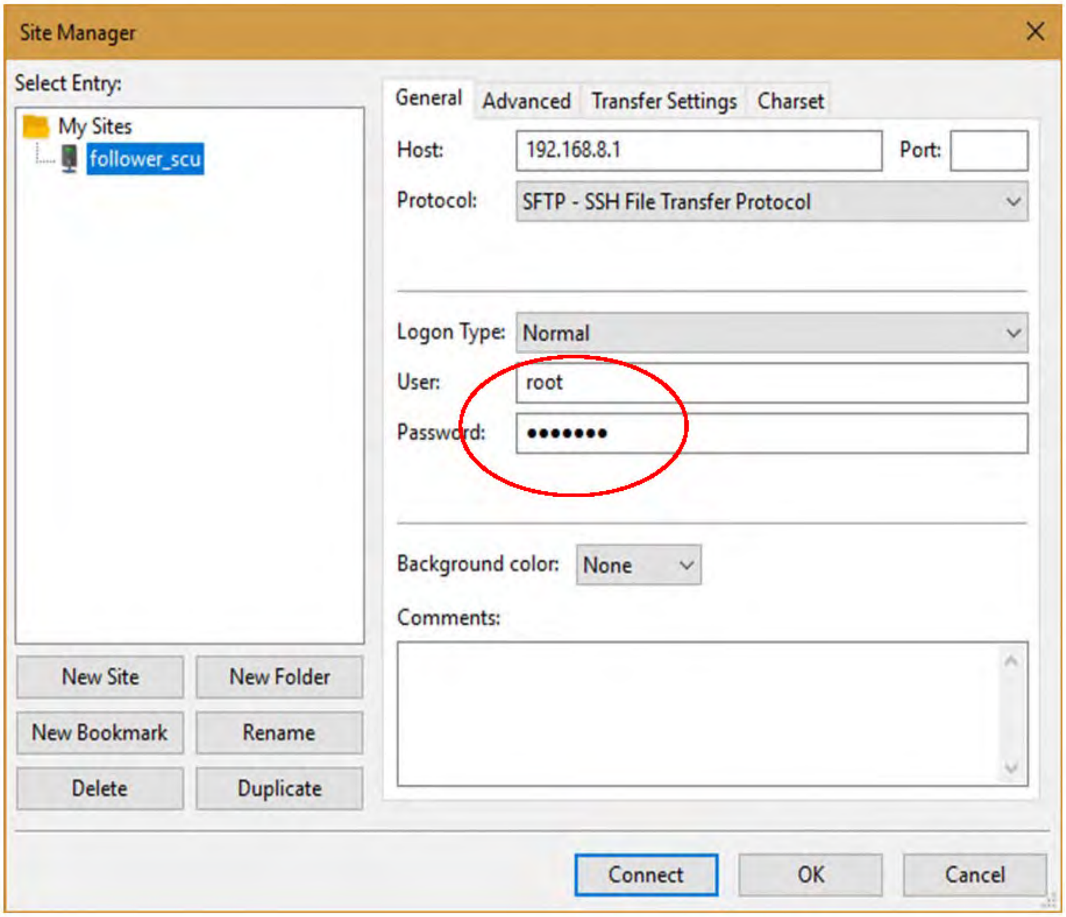
Currently the ATMA specific logs provide a GPS timestamp for data correlation, but available powertrain onboard data does not provide a GPS timestamp of data. The primary method of data attribution used in traditional accident investigation from the powertrain data is ECM run time, or engine hours. Additional further data fields that correlate include wheel speed, engine rpm and engine odometer. The ATMA system does not log any of those specific fields. The ATMA is designed for a variety of vehicle manufacturers with a variety of subsystem vendors. It is not feasible to expect each vendor of powertrain systems for the variety of trucks in the CDOT fleet to add a GPS based timestamp to the current powertrain logs. However, it is more feasible to modify the Kratos ATMA logging system to incorporate powertrain data via a connection to the J1939 Network in a read-only method.

The introduction of a requirement to the Kratos ATMA system logs for powertrain attributable data fields is highly recommended. This requirement would be in line with SAE J3197, Surface Vehicle Recommended Practice for Automated Driving System Data Logger [4]. A potential solution would include the use of a data diode from the J1939 CAN Network to allow a read only inclusion of powertrain specific data fields into existing ATMA Kratos logs. A data diode solution would preserve the integrity of CAN Bus by providing a physical limitation via the diode allowing data to flow only one direction from the network to the Kratos ATMA system. This solution should not introduce data integrity or confidentiality concerns to either system by restricting the flow as read only between the powertrain to the Kratos architecture. This data would considerably simplify the data attribution efforts of law enforcement and crash investigators in mapping the autonomous functionality to that of currently understood powertrain data already used in the investigation of crashes and other system anomalies.

6.2 Recommendation 2: Produce Clear and Concise ATMA Data Retrieval Procedures

Current ATMA log file download procedures are complex and not readily available in the vehicles. The CSU team struggled first to obtain the data download procedure and then also struggled to execute it given the current instructions. The procedure is written for engineers with familiarity in both ATMA and Linux systems. Additionally, it was concerning to the team how few users outside Kratos are trained on how to accomplish ATMA log file download.

A security concern was uncovered during the data download procedures currently in place. The download instructions currently use the “root” permission, Figure 20, which is a security vulnerability [5].



My Sites
follower_scu

Host: 192.168.8.1
Port:
Protocol: SFTP - SSH File Transfer Protocol
Logon Type: Normal
User: root
Password: •••••••
Background color: None
Comments:

Figure 20 ATMA Log File Login Screenshot showing 'root' username

This recommendation aligns with the write up found in the Tabletop after-action report area for Improvement 3.2

> "Participating agencies acknowledged the lack of protocols stating what to do with the data that is extracted from the vehicle and how to manage it for further investigation or storage."

Procedures should be explicit and clear for download and handling of the data to ensure the integrity of the data if an incident occurs. While this process will likely mimic existing vehicle data downloads, it needs to be explicitly defined for ATMA, and procedures need to be readily available and understandable.

6.3 Recommendation 3: Deliver a user friendly ATMA log analysis tool

After the download process is completed for the ATMA log files, the user is provided with a significant amount of data in a .csv file and various .txt log files. The data quantity exceeds the threshold of using excel for a quick user driven analysis. Kratos provided the team with a set of Python scripts to automate some of the log file analysis. However, many potential investigators may not be familiar with Python or its execution. The current Python scripts require download of multiple Python add in packages and do not use a GUI or have a readme file to explain their use. A GUI based tool could be developed providing a user-friendly interface to ingest the data logs and produce tables and graphics of interest for an incident. In addition, it is recommended the log files be digitally signed to prevent undetected manipulation.

6.4 Recommendation 4: Clarify roles for support to interpret log files

In addition to the previously mentioned Recommendation 2 for clarifying data retrieval procedures, this recommendation addresses the need for formal documentation of roles and responsibilities for log files download, analysis, storage, and training. The lack of documented procedures for incident response and non-contractor personnel identified and trained to capture the data is of high concern. We highly recommend CDOT identify specific personnel to become proficient at data extraction. This recommendation also expands on the highlight in Section 3 that the Kratos ATMA logs files must be secured and protected for court proceedings in the case of an accident.

6.5 Recommendation 5: Modify the ATMA logging system to continue to log after an ESTOP

Throughout the course of testing the team conducted several ESTOP tests. Post test data analysis revealed the data recordings for the Kratos system were abruptly terminated whenever an ESTOP was commanded. Further discussion with Kratos revealed this was expected behavior as the ESTOP cuts ignition power in the follower vehicle and the logging system requires ignition power to record data.

This deficiency is concerning as the data following a commanded ESTOP until either a successful stop occurs or if unsuccessful and the vehicle collides with an obstacle is clearly critical data. The Kratos logging system should be modified to allow complete data capture throughout the entirety of an incident.

7. Acknowledgement

We would like to thank the Autonomous Maintenance Technology Pooled Fund for funding this research and data collection effort.

8. References

[1] 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

[2] J. Hoeven, "S.766 - 114th Congress (2015-2016): Driver Privacy Act of 2015," Sep. 28, 2015. https://www.congress.gov/bill/114th-congress/senate-bill/766 (accessed Mar. 24, 2022).

[3] N. A. and R. A. Office of the Federal Register, "49 CFR 563 - EVENT DATA RECORDERS," *govinfo.gov*, Oct. 01, 2011. https://www.govinfo.gov/app/details/CFR-2011-title49-vol6/https%3A%2F%2Fwww.govinfo.gov%2Fapp%2Fdetails%2FCFR-2011-title49-vol6%2FCFR-2011-title49-vol6-part563 (accessed Oct. 12, 2021).

[4] "J3197A: Automated Driving System Data Logger - SAE International." https://www.sae.org/standards/content/j3197_202107 (accessed Mar. 24, 2022).

[5] R. Anderson, *Security Engineering*, 3rd ed. Wiley, 2020.