



Research-fueled Security Services



\ WHITE PAPER \

REMOTE WRITING TRAILER AIR BRAKES WITH RF

Ben Gardiner
Senior Cybersecurity Research Engineer
NMFTA

October 2022

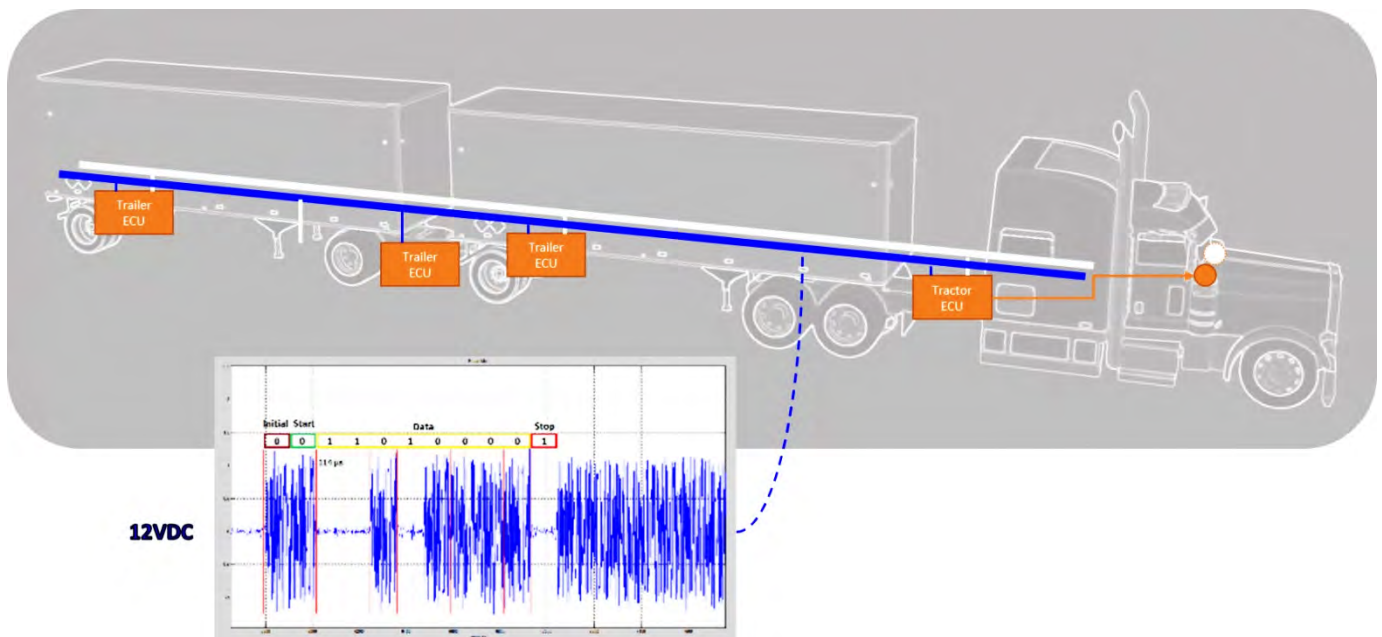
What We've Discovered

The following discoveries regarding the SAE J2497 Power Line Communications (also known as "PLC4TRUCKS") scheme were made in collaboration with Assured Information Security (AIS), anonymous equipment suppliers, and the member fleets of the NMFTA.

This databus has been used to communicate trailer ABS faults to the driver in all trucks in North America since 2001, when FMVSS regulation No. 121 paragraph S5.1.6.2(b) came into effect:

"The tractor electrical circuit must be capable of transmitting an ABS malfunction signal from the antilock brake system(s) on one or more towed vehicle(s)."

This standard was codified by industry experts at the request of fleets who had made it clear that they would not accept any connectors other than the J560 "7-way" plug used on North American tractor trailers since the 1960s. Thus, the standards bodies added this communication to the power lines already flowing between the tractor and trailer¹. Of course, the databus is also used for more than that – or else we wouldn't have anything interesting to tell you about.

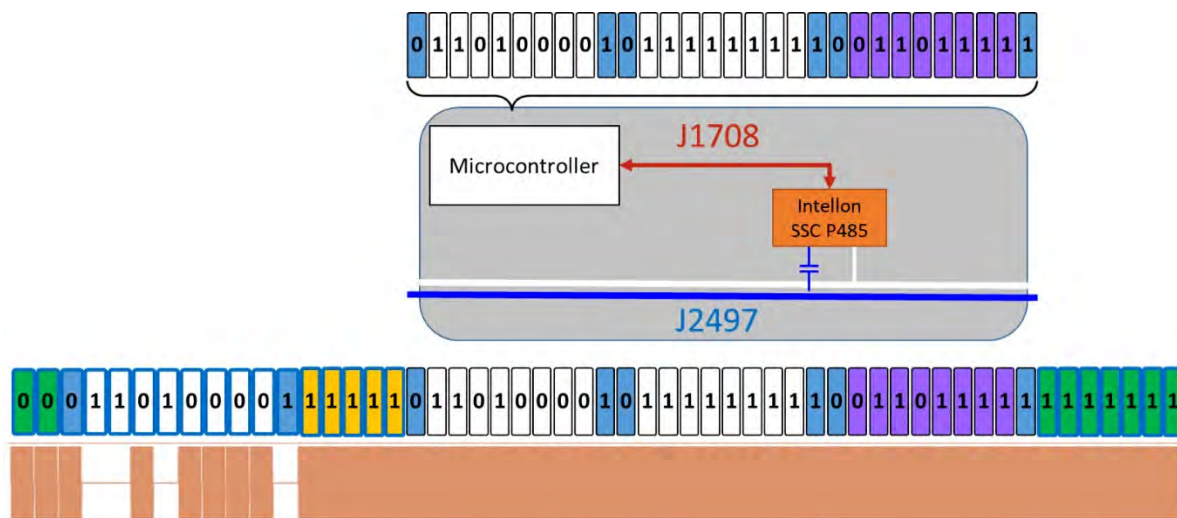


J2497 is a PLC scheme designed and implemented by Intellon as a bridge between UARTs over powerlines in the Intellon SSC P485 transceiver IC. For years this patented chip was the only way to realize the J2497 standard. With the recent expiration of the patent, this has changed, but the as-implemented behavior of the Intellon chip is still the de facto standard, and the J2497 specification itself has SSC P485-specific components to it. The J2497 specification offers PLC4TRUCKS as an alternative transport to J1708, itself a UART protocol based on RS-485. Pictured below is a logic analyzer capture of the LAMP ON J1708 message (MID 10 + payload 0 aka 0a00):

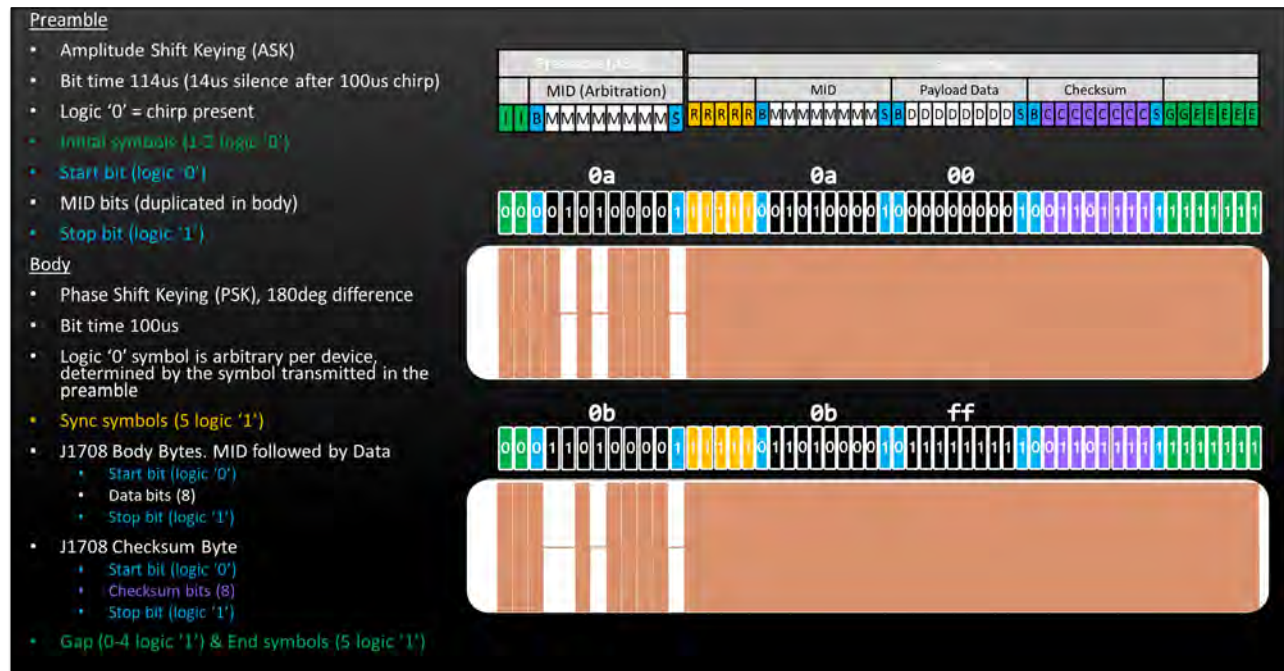
¹SAE J2497 Published October 2002 https://www.sae.org/standards/content/j2497_200210/



The alternative transport realized by the Intellon SSC P485 is that of a translation between the RS-485 physical layer and powerlines, but the first byte (the MID in J1708) plays an important role in arbitration for the bus.



As illustrated in the following graphic, J2497 uses two separate modulation schemes for the preamble (first byte) and body of its signals: Amplitude Shift Keying (ASK) and Phase Shift Keying (PSK) respectively. It uses nearly the same bit rate and UART parameters of 9600 bps 8N1 as J1708 (a shorter 100us bit time in the body, but 114us in the preamble), plus some extract sync bits before (I) and after (R) the preamble as well as after the body (G,E). Note that the MID is duplicated between the preamble and body. An early finding in our research was that the preamble byte value didn't matter much and could be sent despite mismatching the body MID. We later found that it mattered even less than that – more on this later.



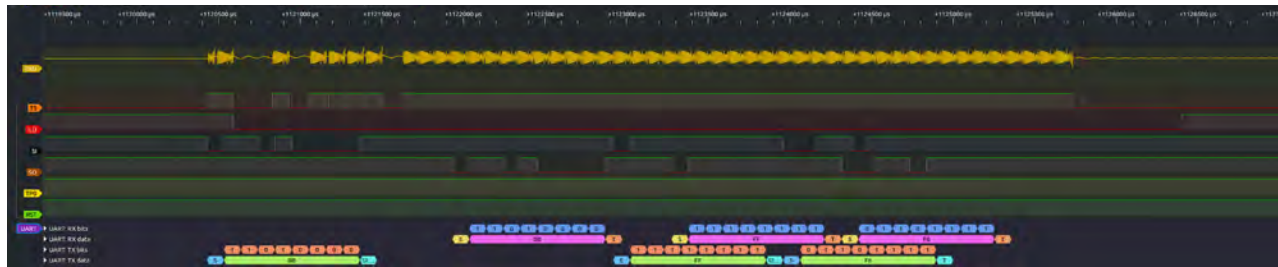
The SSC P485 bidirectionally converts between J1708 and J2497. If it observes activity on the J1708 bus while the J2497 is idle, it sends a preamble followed by the body; likewise, when activity is observed on the J2497 bus, a J1708 message is sent. For example, when a LAMP ON message is observed on the J2497 bus, the SSC P485 converts it to J1708, like so:



The logic analyzer figures above were created using a very simple sigrok decoder we wrote to stack onto any UART analyzer²; we created the decoder during our detailed research into mitigation of the issues we had found, to be addressed later in this paper.

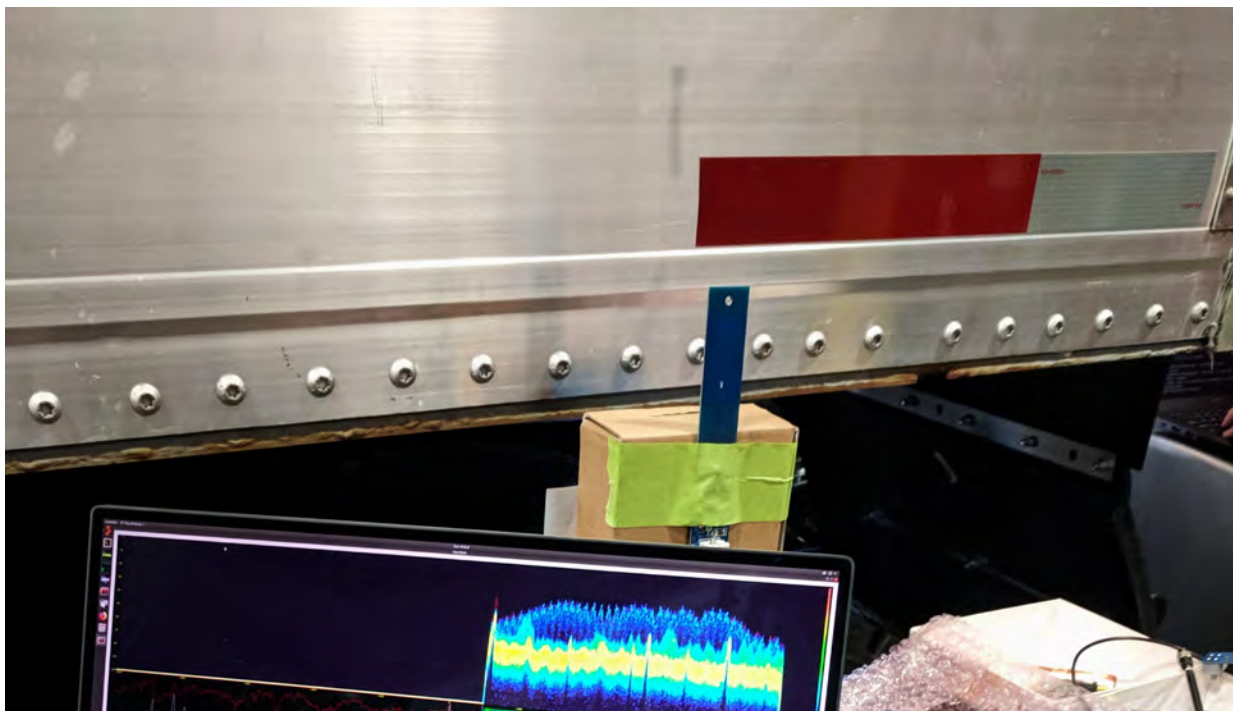
For conversion in the other direction, the following image is an example of what the SSC P485 transmission looks like, in response to data sent by a microcontroller into the DI pin (incorrectly labeled as SI below). The individual UART bits (including start and stop bits) are visible here, and we can see how the microcontroller waits for transmit of the first byte (and then should check it for arbitration purposes) before continuing with transmit of the rest of the message. This sigrok capture was made with the built-in UART analyzer.

² Gardiner, Ben. "sr-j1708" <https://github.com/TruckHacking/sr-j1708>



The 'Powermaster' project really kicked off in 2019. Much like the work that Baker, et. al.³ released earlier that same year (simultaneous to our own testing, during which we found remote read capability), in which these authors demonstrated that Intellon's (then-Atheros, which would become Qualcomm's) HomePlug GreenPhy (HPGP) Power Line Communications (PLC) can be received at distances of several feet using Software Defined Radios (SDRs). We eventually published our remote read findings at the Car Hacking Village DEF CON 29 SAFE MODE⁴ in 2020. Our results were the same: the much earlier (perhaps original) Intellon PLC scheme in J2497 can be read remotely, just like the modern incarnation in HPGP.

We found that J2497 communications can be read at distances of up to eight feet using active "mini whip" antennas, which pick up E-field variations by amplifying capacitance, coupling to that field on a small PCB "patch" of copper⁵. There are at least two types on the market, both called "mini-whips": a blue one with BNC connectors, and a green one with SMA connectors. Back in 2019 we had the best success with the blue style, powering it from a battery for the best noise performance. Pictured below is an early success in testing with the blue style in October 2019.



³ Baker, Richard, and Ivan Martinovic. "Losing the Car Keys: Wireless [PHY-Layer] Insecurity in [EV] Charging." 28th USENIX Security Symposium (USENIX Security 19). 2019.

⁴ Poore, Chris, and Gardiner, Ben. "Power Line Truck Hacking: 2TOOLS4PLC4TRUCKS." DEF CON 30 Car Hacking Village 2019. http://www.nmfta.org/documents/ctsrp/Power_Line_Truck_Hacking_2TOOLS4PLC4TRUCKS.pdf?v=1

⁵ Duffy, Owen. "How DOES the PAoRDT Mini-Whip work." <https://owenduffy.net/antenna/PAoRDT-MiniWhip/>

Since then, Chris Poore has had success also with the green style, and even made an excellent enclosure for it, as pictured below.



The remote read issue was reported in 2020, but during this time we were also testing for remote write – that part didn't go so smoothly, more on that later. What we eventually confirmed was that it is possible to write remotely to J2497 via induced RF, depending on the equipment configuration (again, just like Baker et. al. who reported a wireless disruption issue in HPGP in February 2022⁶). We found that the most susceptible equipment is tanker trailers and 3x road train trailers. The equipment from all trailer and tractor brake suppliers is affected and the maximum distance can be up to 12 feet. Furthermore, the equipment needed to make it work is not expensive: as cheap as \$300 USD for the most susceptible trailer equipment configurations. For details on the confirmed results and testing methods we followed, please consult the tables in NMFTA's *Disclosure of Confirmed Remote Write*.⁷

We're speculating that there also could be other susceptible equipment configurations:

- 2x "pup" road trains with extruded metal decking – a single pup with metal extruded decking was only a little less susceptible than a 3x pup road train with wood decking
- flatbeds (including intermodal trailers) – their wiring runs outside along a metal structure, as with tankers
- 2x40' road trains with any decking – the total length is equivalent to a 3x pup road train

Since we haven't had testing opportunities on these equipment configurations, we cannot confirm our suspicions, but if you're reading this and have said equipment, we are happy to come visit for tests!

Although we've confirmed we can read and write to J2497 remotely, the impact of remote read was pretty low: there isn't much, if any, sensitive information being sent on the J2497 bus of a tractor-trailer. In the case of remote write, what we have is a vector: we can create any messages we like on the J2497, if we can reach it to induce them. This was captured as CVE-2022-26131⁸, falling under CWE-1319 (Improper Protection against Electromagnetic Fault Injection – not a great fit, but the closest CWE for RF-induced messages).


⁶ Sebastian Köhler and Richard Baker and Martin Strohmeier and Ivan Martinovic, "Brokenwire : Wireless Disruption of CCS Electric Vehicle Charging" 2022 <https://arxiv.org/pdf/2202.02104.pdf>

⁷ Gardiner, Ben, NMFTA Inc. "2021 Disclosure of Confirmed Remote Write."


http://www.nmfta.org/documents/ctsrp/Disclosure_of_Confirmed_Remote_Write_v4_DIST.pdf?v=1

⁸ NIST. CVE-2022-26131. March 10th 2022. <https://nvd.nist.gov/vuln/detail/CVE-2022-26131>

The impact of remote write ability is only as big as the impact that arbitrary J2497 messages could have. When introducing J2497, we mentioned that it can be thought of as another transport for J1587, so let's look more closely at that.

J1587 is a protocol on top of J1708, and is first and foremost a way to encode time-varying signals in messages sent periodically around a vehicle. This is very much akin to J1939, or even the main purpose of the various propriety CAN bus uses in passenger cars. It predates J1939 by many decades, and any similarities are due to J1939 copying it. In J1587 the signals are packed into PIDs, and multiple PIDs can potentially be concatenated together in a message, as pictured below with  representing an arbitrary byte.

MID	PID 1	Data 1	...	PID n	Data n	Checksum
128-255		 ... 	...		 ... 	

As J1587 is on top of J1708, there are MIDs first and a checksum last. The first byte in J1587/J1708 (and also J2497) is used for arbitration, as in CAN networks, but here the MID is much more like a source address. This is because there are unicast messages which can be sent-to MIDs (e.g., PIDs 197+198 for transport protocol), Standardized Free-format Data requests, and Data Link Escape messages. The latter is where most of the interesting  stuff happens in J1587.

J2497 was introduced to satisfy a FMCSA regulation, and only the J2497-specific LAMP ON and LAMP OFF messages are required, but as it was implemented as an alternative transport to J1708, existing J1587 code bases were leveraged. When trailer brake suppliers created their units with J2497 support, they brought forward all the J1587 features for value-add to their fleet customers. A report from 1998⁹ lists approximately 40 smart trailer features – a crazy amount! This shows that the desire to provide features above and beyond trailer ABS fault detection was established right from the inception of J2497. For more on these features, or on J1708/J2497/J1587 in general, please see the Commercial Transportation: Truck Hacking slide deck, available on the NMFTA CTSRP page¹⁰.

What we've confirmed is that all three of today's trailer brake suppliers implement diagnostics over J1587 using Data Link Escapes (DLEs). We have encountered no diagnostics features on trailers that require any authentication or authorization. We've heard of a precursor to seed-key exchange being used on J1587 for engines¹¹, but no such luck here. For example, reconfiguring the tone-ring size on the trailer brakes requires no authentication nor authorization, meaning it is susceptible to a replay attack, as are all other features. This was captured as CVE-2022-25922¹², under CWE-306 (*Missing Authentication for Critical Function*).

Now, the possible impacts of this observation are tempered by the fact that ECUs – even trailer ECUs – have protections against running diagnostics while in motion. Trailer brake ECUs are ABS units, hence they have wheel speed sensors and can detect when they are in motion. We tested some trailers in motion (physically and simulated), and for the most part the diagnostics commands are rejected. That's definitely what we all want to hear.

However, nothing is ever simple when it comes to trucks. For our testing, we settled on using solenoid test commands when transmit testing for three reasons:

- All of the trailer brake supplier's units have a solenoid test command
- The response to the command is either a chuff of air (hence its common alias: "chuff test") or an audible click of the solenoid if no air is supplied
- The tests can be replayed (due to the weakness mentioned above).

The solenoids tested with these commands are a secondary control for the relay valve in the trailer brakes and allow dumping air to relieve brake pressure and realize the ABS feature. These ABS trailer brake controllers are an evolution of the humble relay valve that was the workhorse of the trailer brakes that came before.

⁹ DOT "Development, Evaluation, and Demonstration of a Tractor Trailer Intelligent Communication and Power Link" 1998

¹⁰ Gardiner, Ben. "Commercial Transportation: Truck Hacking" September 9th 2021. http://www.nmfta.org/documents/ctsrp/Commercial_Transportation_v7_DIST.pdf?v=1

¹¹ Haystack. J1708Driver.py https://github.com/TruckHacking/py-hv-networks/blob/919e4ddff8413a1f5bb062ca4d22b02d04c1885/hv_networks/J1708Driver.py#L85

¹² NIST. CVE-2022-25922. March 10th 2022. <https://nvd.nist.gov/vuln/detail/CVE-2022-25922>



Trailer brakes are supplied for all tractor-trailers conforming to ATA TMC RP 417¹³ by a red pneumatic line and controlled by a blue pneumatic line. The blue control line is a low-volume pressure "signal." The "relay" in "relay valves" was to switch the high-pressure red supply line according to that low volume signal, which enables the operator of the tractor to control the high-powered braking needed on the heavy-duty vehicles hauling everything from your next issue of 2600 to drinking water for some communities¹⁴.

In the ABS controllers, the relay valve can also be modulated by a solenoid, the key here being the word modulated: some control line pressure is required for solenoid test commands to dump any air¹⁵. For typical spring brakes on trailers, this means that supply air will only be dumped if the operator's "foot is on the brake." An exception is dollies – the equipment that is between two trailers (pictured above in orange) – where solenoid tests on the trailer ECUs will dump air regardless of the control line. In either case, a repeated solenoid test command while the vehicle is stopped in traffic would be a drain on the tractor's reservoirs and air compressors. Whether that ultimately impacts the motion of the tractor trailer depends on its compressed air capacity and other factors.

What we've confirmed is that all trailer brake controllers will respond to solenoid test commands received by induced RF. These solenoid test commands are DLEs like all other diagnostic commands; therefore, we are confident that this also implies that other diagnostic commands could be induced, as well as any other function which responds to J1587 messages. In certain cases, the solenoid test alone could result in impeding the motion of a tractor-trailer. There may be other, more severe, abuses or vulnerabilities in trailer brake controllers; trailer brake suppliers are in the best position to assess the likelihood of this.

What is Happening, and How is RF Received?

TL;DR: we don't really know 🙄_/_/ but we do know that:

- Tankers, which are large metal shells and whose wiring typically runs out along their side, are very susceptible
- Dry vans with wooden decking and metal beams are not very susceptible, as compared to trailers with the same dimensions but with metal decking. In these, the wiring runs under the decking and through the beams. In the metal decking trailers we tested, the wiring ran inside an extruded channel
- Even the least susceptible dry-van trailers with wooden decking are susceptible when in a 3x road train configuration.

The rest is wild speculation:

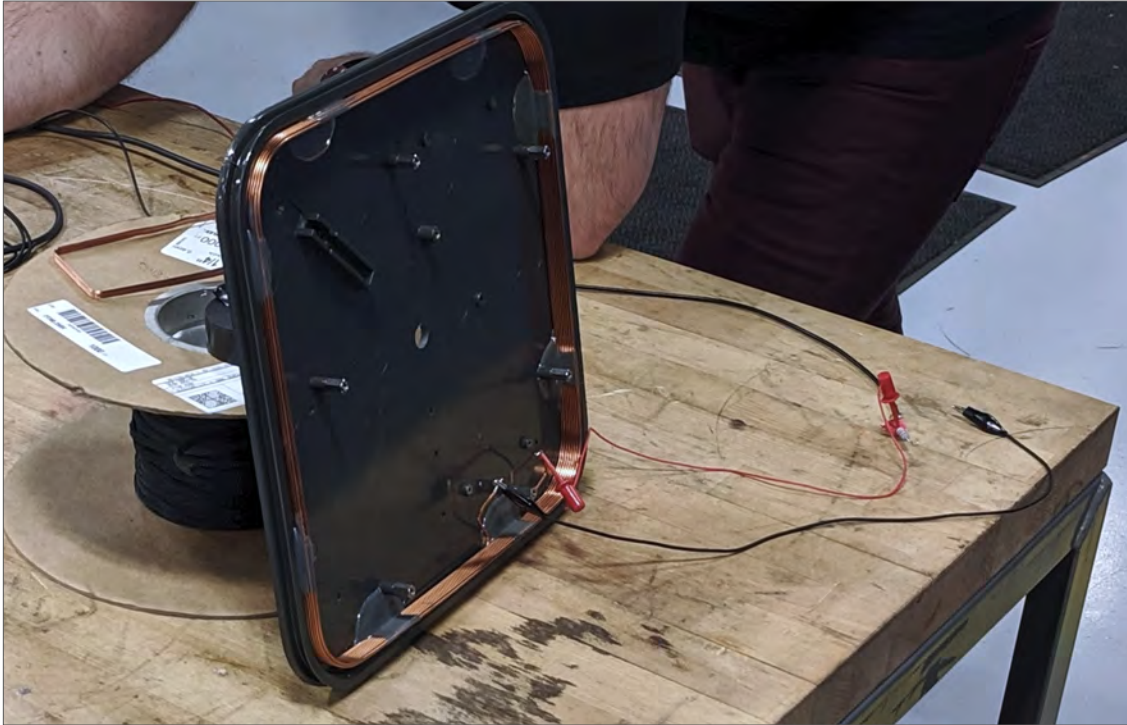
Our success with the mini-whip antennas might be a clue as to what could be going on here. Those antennas work using near-field effects; the wavelengths of the frequencies involved here are multiple kilometers (between ½ and 3 km), so everything we could possibly do is in the near field. (As an aside in the category of "crazy ideas we tried," the frequencies overlap with some RFID technologies, which are also near-field, and we did try to use the large "Garage" tag readers as antennas, but that was unsuccessful.)

¹³ ATA TMC. "RP 417A Support Pneumatic/Electrical Lines Between..." 1975

¹⁴ Jonson, Urban. "A Survey of Heavy Vehicle Cyber Security" 2015

<http://www.nmfta.org/documents/ctsrp/nmfta%20heavy%20duty%20vehicle%20cyber%20security%20whitepaper%20v1.0.3.6.pdf?v=1>

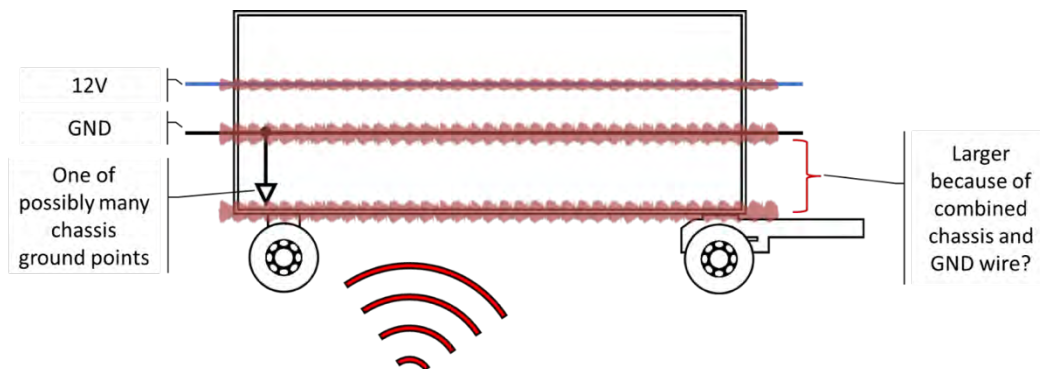
¹⁵ Special thank you to Andrew Wallner for helping me grok all the pneumatics, among many other topics! Your assistance across the project was invaluable.



The fact that dry vans are less susceptible than tankers certainly suggests that having the trailer wiring run somewhere that isn't "out in the open" is better; however, the metal-decking dry van result indicates that wrapping the trailer wiring in too much metal makes susceptibility worse.

The results on road trains suggest that making the trailer wiring long enough helps it pick up the RF signal. However, those results could be explained by the possibility that adding more trailers changes the impedance of common mode signals through the power path. These power line signals are received as "single-ended" or "normal-mode," although no one calls them this, instead referring to them as, you know, "signals."¹⁶

The signals are coupled to the power lines with either capacitors or inductors, but either way, they are signals against a ground reference. When we transmit RF to a trailer, we are generating signals on all of its metal parts. Receivers measuring signals relative to ground (single-ended/normal mode) see no signal, because the same signal was generated on both the +12V and GND wires – all things being equal, that is. These are called "common mode" signals. (Fun fact: it is precisely this kind of interference that differential signaling like CAN is designed to avoid.)



¹⁶ Maxim Integrated. "Understanding Common-Mode Signals" 2003 <https://www.maximintegrated.com/en/design/technical-documents/tutorials/2/2045.html>

But what if there is a slightly smaller-in-amplitude but otherwise identical signal induced on the GND wire than what is induced on the +12V wire? In that case, the normal-mode receivers would observe a signal of the difference in amplitudes. This common-mode interference on the unbalanced signal could be how the messages are induced. Tankers and dry vans with metal decking have more metal for the ground than the +12V, and thus probably different impedances for the RF being transmitted.

At the very least, that theory seems *almost-plausible*. It was enough so that we proposed trying to use RF chokes between chassis and wiring grounds as a possible mitigation¹⁷. However, a well-known remedy to common-mode noise problems is transformer coupling, and transformer coupling is one of the specifications recommended ways to connect the receivers to the power line so it isn't clear how this effect could still be explained this way. In summary, we still don't know precisely how the messages are being induced, only that they are in fact being induced.

A trailer's power lines are a notoriously noisy environment, and this was especially so at the time of introduction of the technology to satisfy the regulation¹⁸. The Intellon SSC P485 was designed to work in this environment and has a very small minimum receivable signal amplitude: 5mVPP by the specification, and a reliable 10mVPP in our testing. For the purposes of our theory, that means that only a 5-10mV difference between the induced signals on 12V and GND lines could result in receivable signals. J2497 also employs a spread-spectrum technique, which makes it robust to the presence of broadband noise. The induced signals have their frequency content changed quite a bit (that is, the signals get "colored"), but the spread-spectrum chirps work regardless. Unfortunately, these robust receiver properties also make it a good target for induced RF.

¹⁷ Gardiner, Ben. "Mitigations Options to J2497 Attacks" March 3rd 2022.
http://www.nmfta.org/documents/ctsrp/Actionable_Mitigations_Options_v9_DIST.pdf?v=1

¹⁸ DOT "Development, Evaluation, and Demonstration of a Tractor Trailer Intelligent Communication and Power Link" 1998

How Did We Discover This?

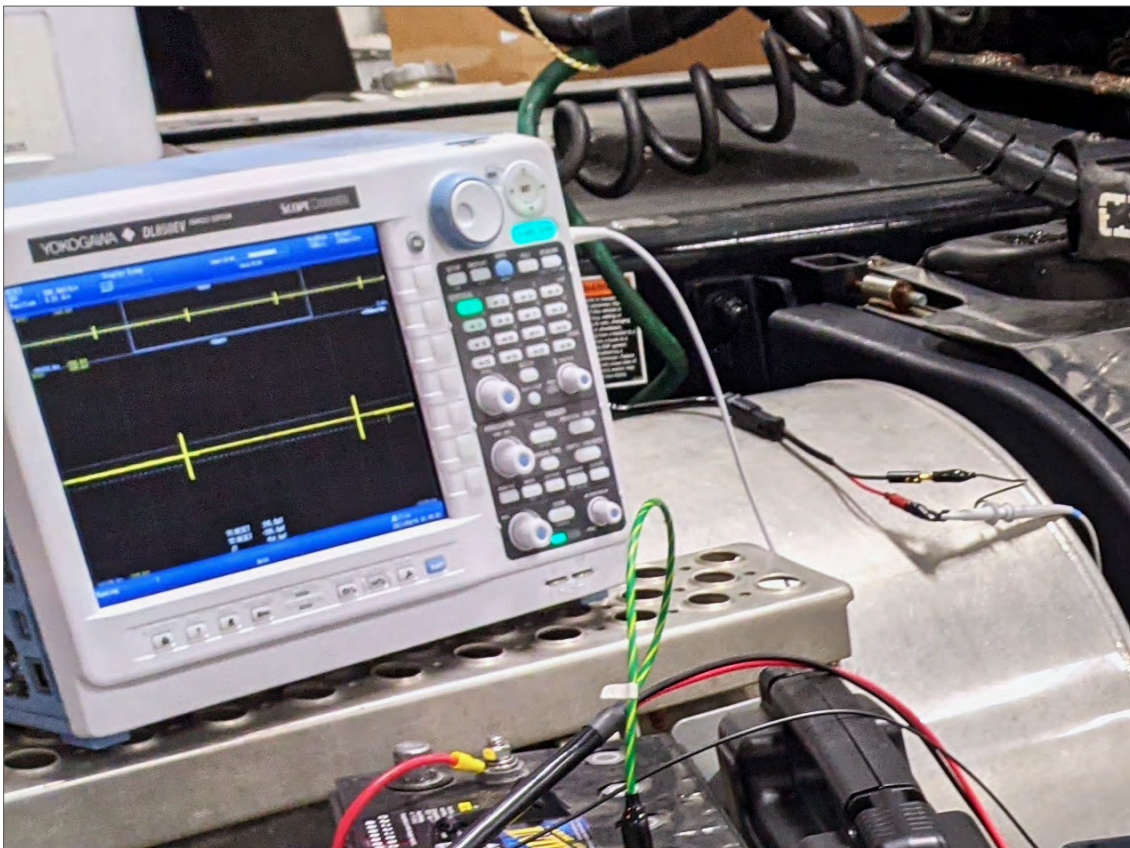
Our timeline for discovery and disclosure was as follows:

2019-05	"Hey, it would be cool to transmit J2497 onto a trailer with SDRs"
2019-07	A call for collaborators sent out to NMFTA CTSRP (then HVCS).
2019-10	Testing at a member fleet confirms that remote read tools work. Testing at a research partner facility with a signal generator and 5W amplifier indicates that tanker trailers are susceptible to RF induction, but the method used at this time was invalid due to galvanic coupling between the amplifier and tanker.
2019-11	All 3x trailer brake suppliers are notified of the transmit tests above at the same time as disclosure of replay attacks on diagnostics and of remote read (the galvanic coupling issue was unknown at this time). NMFTA CTSRP (then HVCS) update on progress.
2019-12	Testing on member fleet's dry-van trailer at AIS location results in the first indications that inducing messages on a dry van requires more transmit power than with a tanker.
2020-02	Galvanic coupling issue recognized. Testing at member fleet location with no new results: dry-vans require more transmit power.
2020-06	All 3x trailer brake suppliers are updated on progress so far.
2020-08	Remote read CISA advisory ICSA-20-219-01 is released. Talk at DEF CON 28 Safe Mode CHV.
2021-09	Testing at a research partner facility with new equipment and techniques to avoid the galvanic coupling problem confirms remote write is possible and practical on tanker trailers. We propose exclusion of diagnostics on J2497 for the RP1217 trailer interface requirements by ATA TMC S.12.
2021-10	Testing at a research partner facility confirms remote write on all 3x trailer brake supplier's equipment and also shows it is possible on some dry-van trailers (e.g., with metal decking).
2021-11	Testing at a member fleet confirms remote write is practical on 3x road trains.
2021-12	Disclosure process is halted due to legal problems. We focus on developing our mitigation technology ideas against these attacks.
2022-01	Thanks to tireless efforts by Urban Jonson, the new results are disclosed to all 3x trailer brake suppliers in a coordinated disclosure with CISA VDP. We share with Auto ISAC a couple weeks later and with the ONG ISAC as well.
2022-03	The remote write CISA advisory ICSA-22-063-01 is released. We share the disclosure with our member fleets, trailer OEMs, ATA TMC, and later, the National Tank Truck Carriers.
2022-04	We present arguments to the ATA TMC Task Force on NGTTI asking them to exclude J2497 diagnostics from the next generation tractor trailer interface and to include attack mitigations on new tractors.

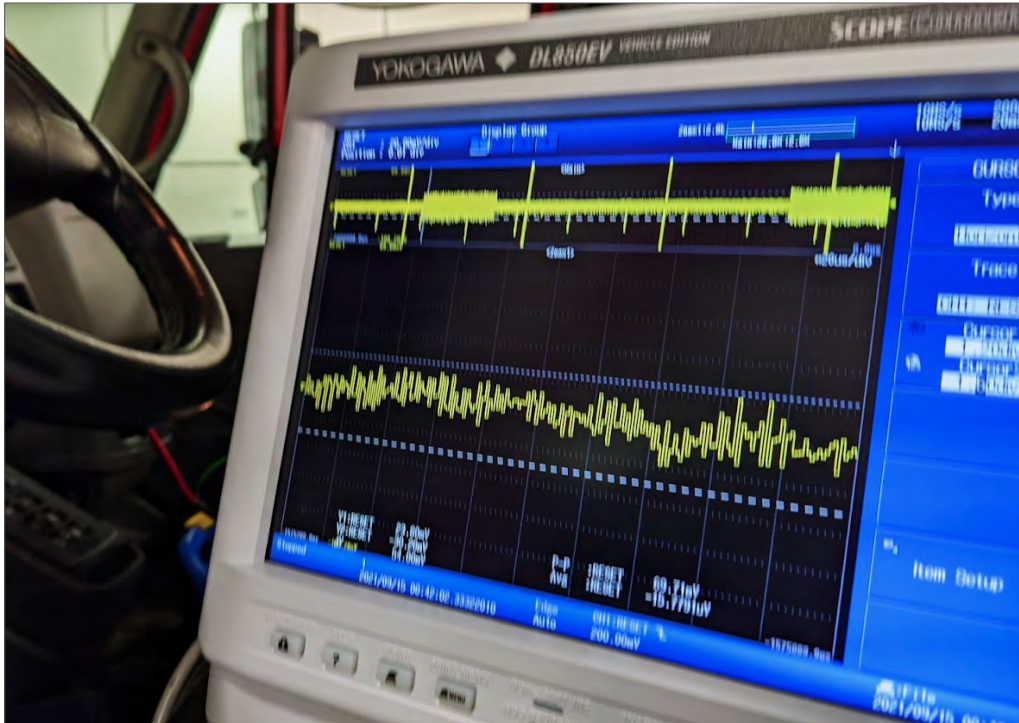
While we were testing methods to remotely read the trailer traffic, we were also testing how trailer traffic could be written remotely. Our first tests of remote write were invalidated because we had an unintended galvanic connection between the transmitter and the receiver (a trailer): we were measuring induced voltage on the trailer using an oscilloscope that was plugged into the same mains as the transmitter amplifier. Once we figured that out, we moved the oscilloscope to an inverter connected to the vehicle battery and/or used pocket scopes.

We eventually gave up on measuring induced voltage, because once we were able to create the chuff commands and observe the solenoids clicking while the voltage we were measuring on the trailer power lines remained a noisy soup. We knew that what was being induced was below the visible noise levels in the time domain, and that the Intellon SSC P485 receivers are extracting the signal using the noise-robust spread spectrum chirps.

The picture below shows J2497 chirp trains on the oscilloscope. These messages are originating from the trailer brake controller; most send messages periodically in their default configuration. Between the chirps is what appears to be background noise of the line; however, this picture was taken while the trailer brake controller was chuffing as a result of a successful transmit test. Within that noise is a valid J2497 signal that was received and acted upon by the trailer brake controller.



If we zoom into that line noise, there is nothing further resolved by the oscilloscope within the time domain.



However, frequency domain analysis can resolve the J2497 chirps when the capture uses a high-bit-depth SDR. Here is an analysis of a capture using an Ettus SDR through a Ham It Up upconverter connected to the trailer power lines with a DC block (more on this later), where the SDR is tuned to 126MHz and the upconverter frequency is 125MHz, so the baseband signal appears at -0.9MHz to -0.6MHz. This arrangement is recommended when using upconverters for receiving, because it removes spurious noise sources as compared to tuning the SDR on-top-of the upconverter local oscillator. The capture has already been bandpassed using the pieces of the receiver flow in the gr-j2497 module¹⁹.



¹⁹ Poore, Chris. Gr-j2497 August 2020 <https://github.com/ainfosec/gr-j2497>

For ease of transmit testing, we created a signal that could be played on a loop, and would try a solenoid test at each trailer dynamic address for each supplier's trailer brake controller: the "unichuff." Even though J2497 specifies a dynamic address claim mechanism, none of the suppliers use it. There is a de facto dynamic address scheme wherein trailer units that detect a transmitter on their current address will move over to the next possible dynamic address in a list (MIDs 137, 138, 139, 246 and 247).

```

acfe89_____
acfe89_____
acfe89_____
acfe89_____
acfe89_____
acfe8a_____
acfe8a_____
acfe8a_____
acfe8a_____
acfe8a_____
acfe8b_____
acfe8b_____
acfe8b_____
acfe8b_____
acfe8b_____
acfef6_____
acfef6_____
acfef6_____
acfef6_____
acfef6_____
acfef7_____
acfef7_____
acfef7_____
acfef7_____
acfef7_____
acc3038800b0

```

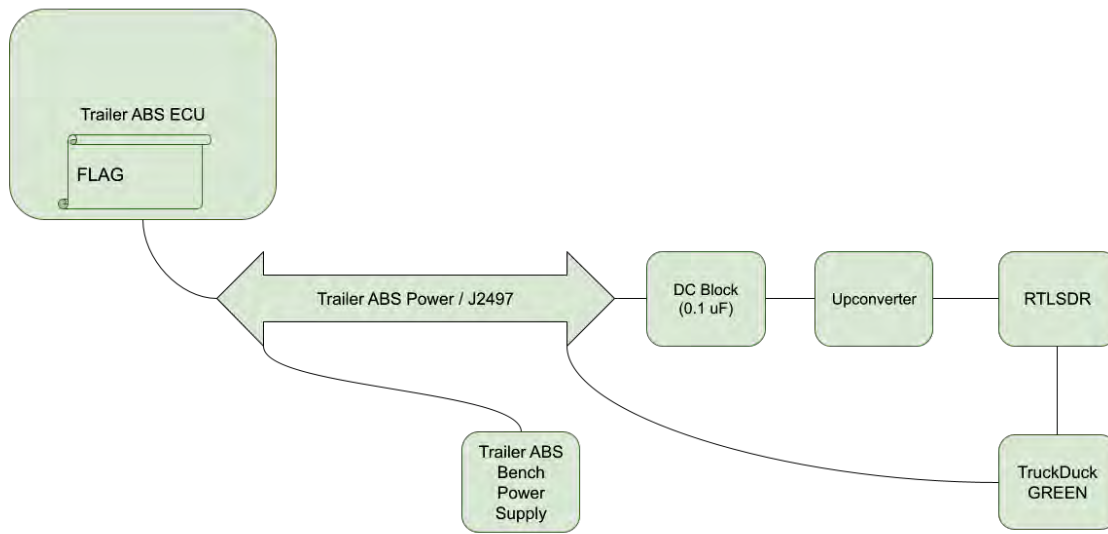
The listing above shows the contents of the "unichuff." The MID used is always 0xac, which is the MID reserved for diagnostic adapters, followed by 0xfe, which is the (low page) Data Link Escape (DLE) PID. DLEs are unicast, so the next byte is the target MIDs: MIDs 137, 138, 139, 246, and 247 in turn. The final command is a device reset of the tractor brake controller (MID 0x88 – the tractor brake controllers don't do dynamic addressing) which results in a modulator roll call on some tractor brake controllers. The blanked values are the proprietary diagnostics commands for solenoid tests in each of the 3x trailer brake suppliers. We're not going to share the commands; we were able to extract them with some simple analysis of diagnostic sessions traffic, and we're sure you could too, if you're up to the challenge! 🤔

How Can You, the Reader, Do This?

Unless you are the owner of the trailers and have a secluded spot away from others, you shouldn't be doing this. However, you can do some exploration of your own on a bench setup.

The first step is buying a trailer brake controller; this may be tricky, as all truck and trailer parts are in high demand, but you should be able to find something. The good news is that for powerline setups it can be pretty simple: the wires for powering your target device are the same as for communicating with it!

A reasonable example to consider as a working bench setup is one of the CHV CTF setups, such as this one we made early on for 2020's 2020's SAFE MODE²⁰:



In this challenge we gave competitors access to the J2497 powerline interface of a trailer brake controller via both an SDR (for read) and a bit-banged GPIO on a TruckDuck/BeagleBoneBlack (for write). There are a bunch of different ways to slice this, but in general you will need to solve the following for your bench setup:

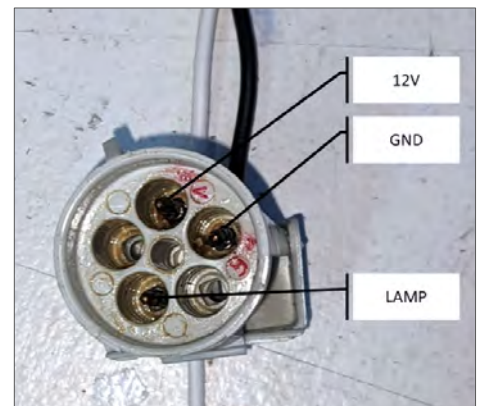
1. How to power your trailer brake controller
2. How to read from your trailer brake controller
3. How to write to your trailer brake controller
4. How to connect your tools to the powerlines on your bench

1. How to power your trailer brake controller

This part is actually the easiest. It turns out that despite all the warnings you may hear, you can power the trailer brake controllers from switching power supplies and J2497 will work just fine. For the best possible signal quality (for example, if you are debugging signal generation in a tool you're developing), you will want to use a car battery and keep the trickle charger disconnected, although in our experience it worked fine with the trickle charger connected as well.

Connecting the power to the trailer brake controller can be accomplished by wiring up your own Delphi/Weather-Pack 5-pin connector²¹. Every trailer brake controller seems to use these.

You can optionally connect a lamp to the LAMP line of the trailer brake controller on one side and the 12V power supply on the other.



²⁰ Gardiner, Ben. "DC29 CHV Air Brakes Docs" August 2020
https://docs.google.com/document/d/1fz5Bhoc7TK_BcJJ1_doNXuo_rTQ76wwOHYtMvqzBXo/edit?usp=sharing

²¹ Racetrax. Connector set 5-way <https://www.racetrax.biz/p/connector-set-5-way-weather-pack/rcs-063>

2. How to read from your trailer brake controller

We covered this previously in our talk, *2TOOLS4PLC4TRUCKS*,²² in the section, "A PLC Reading Tool". One can read J2497 using a GNU Radio gr-j2497 Out of Tree module developed by Chris Poore. Most SDRs don't tune down low enough, so an upconverter such as Ham It Up is needed; since then we've also confirmed that direct receive (no upconverter) works with a HackRF tuned to 1MHz. The HackRF is 8-bit, which is limited dynamic range, so reception with an active antenna is possible only at close ranges. Direct connection with a DC block is possible, but the maximum input power of the HackRF is -5 dBm, so make sure you use an attenuator inline with your HackRF input (I use a 20dB attenuator).

A more venerated way to read J2497 is to use a diagnostic adapter, like the DG PLC TestCon, to convert from J2497 to J1708. These have the advantage that they can be connected to any RP1210 Vehicle Diagnostic Adapter (VDA), and then the supplier's diagnostic tool can be interfaced with the trailer brake controller. This is a necessary step in analyzing the diagnostic session traffic.

Any J2497 traffic you do eventually read will be presented to you as a sting of numbers, possibly in hex (our preferred form). As mentioned above, J2497 is another transport for J1587, so you will want to decode J1587 traffic to understand what is going on. The pretty_j1587 tool developed by Daniel Salloum is invaluable in doing this; the sample below shows the pretty_j1587 output on the diagnostics clear we use in the "unichuff" above.

```
$ echo acc3038800b0 | python3 pretty_j1587.py -v 2 -f -
MSG: [0xac,0xc3,0x3,0x88,0x0,0xb0]
      ([172, 195, 3, 136, 0, 176])
CLC CHECKSUM: 0x56 (86)
MID 0xac (172): Off-board Diagnostics #1

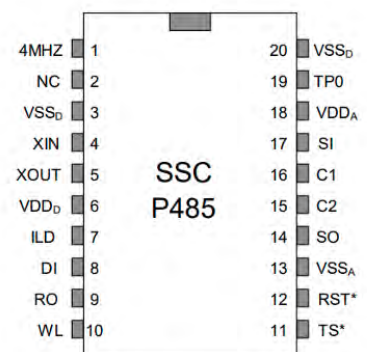
PID 0xc3 (195): Diagnostic Data Request/Clear Count
  _Resolution   : Binary
  _MaxRange     : 0 to 255
  _UpdatePeriod : As needed
  _DataType     : Binary Bit-Mapped
  _DataLength   : 3 Characters
  _Priority     : 8
  DATA: 0x3, 0x88, 0x0, 0xb0
    0x03 - Number of parameter data characters = 3
    0x88 - MID of device to which request is directed.
    0x00 - SID or PID of a standard diagnostic code.
    0xb0 - Diagnostic code character
```

These adapters use the Intellon SSC P485 internally, so they have another advantage: with some modifications, you can use them to look closely at the J2497 traffic. The DG PLC TestCon is connectorized and easy to re-work.

The pins of interest for looking closely at J2497 and J1708 are the inputs and outputs of the SSC 485: UART signals on one side and analog on the other; from the datasheet:

- RO 9 – "Digital output. After the preamble and assuming standard polarity: if superior1 state is detected on SI, RO will be high (MARK), if superior2 state is detected on SI, RO will be low (SPACE)."
- DI 8 – "Digital input. After the preamble, a low on DI (SPACE) transmits a superior2 state on SO, a high on DI (MARK) transmits a superior1 state on SO."
- SO 14 – "Analog signal output. Tri-state enabled with internal signal."
- SI 17 – "Analog signal input."

SSC P485 PL Transceiver IC



²² Poore, Chris, and Gardiner, Ben. "Power Line Truck Hacking: 2TOOLS4PLC4TRUCKS." DEF CON 30 Car Hacking Village 2019. http://www.nmfta.org/documents/ctsrp/Power_Line_Truck_Hacking_2TOOLS4PLC4TRUCKS.pdf?v=1

Then there are some supporting pins we shouldn't forget:

- VSS_D 3 and VSS_A 13
- ILD 7 – "Digital output, active high. Logic 1 state indicates 10 bit times of idle line, logic 0 indicates detection of carrier or non-idle line." to record for idle detection
- TS 11 – "Active low digital output. Enables the external output amplifier when driven high. Tri-states the external output amplifier when driven low"

And some pins that are suspicious:

- TP0 19 – "Reserved pin for testing."
- RST 12 – "Active low digital input. RST asynchronously forces RO and ILD outputs to a high state and TS to a low state." (This might be interesting to record when the MCU resets the interface; it could be important in testing DoS signals)

Ideally for this re-work, all of the pins we want would have been on the debug header. However, none of them were. There were a couple on test points, but most needed to be pulled from the legs of the P485 and P111 package. One lucky break was that the PLC TestCon PCB ties both VSS_D and VSS_A (digital and analog ground), making it easier to analyze the PLC chirps and digital lines at the same time. To save an analog input on your logic analyzer, inspect the point where the output (SO) and input (SI) are combined. The PLC TestCon also includes the amplifier from the application note: the P111 whose output is the perfect place to capture the J2497 signals before being coupled on the powerlines.

We connected up all of the signals of interest to the following pins, which were in turn connected to a 0.1" header superglued to a capacitor (in the style of @scanlime) with official blue bodge wire™:

- DI / P485 Pin 8 -> I
- RO / P485 Pin 9 -> O
- ILD / P485 Pin 7 -> L
- TS / P485 Pin 11 -> T
- Signal Output of P111 -> S
- VSS_D / P485 Pin 3 -> G

In the picture below, we also connected two more interesting pins:

- TP0 / Pin 19 -> P
- RST / Pin 12 -> R



With a logic analyzer connected to the Intellon SSC P485, it is possible to accurately frame the J1708 traffic it outputs. J1708 uses strict timing criteria to break up the stream of bytes into frames: any inter-byte gap of more than 2 bit-times is a frame break. Doing this in software requires the real-time PRU on the BeagleBoneBlack (see the j1708 driver in PLC4TRUCKSDuck²³), or something bare metal to split on those timings (see the stm32-j1708 tool from GRIMM²⁴). With the logic analyzer, there is enough timing resolution to do the frame break offline. For many use cases (anything non-interactive) it will be good enough to use the sr-j1708²⁵ protocol analyzer for sigrok to break up the frames. Finally, with a logic analyzer that has an analog input, you can look at the relationship between the J2497 and J1708 as it is converted by the SSC P485 (for examples, see the figures in the first section of this blog paper).

3. How to write to your trailer brake controller

As also covered in the "A PLC Writing Tool" section of *2TOOLS4PLC4TRUCKS*²⁶, one can modify a TruckDuck/BeagleBoneBlack to synthesize J2497 by bit-banging one of its GPIOs (see PLC4TRUCKSDuck²⁷). Of course, a proper J1708-to-J2497 converter will do the trick for you as well. There are strict timing constraints for framing, but if your tool is the only transmitter in your bench setup, you can get the timing minimums using a very coarse (even userspace) sleep. Don't worry about arbitration, let the other end worry about backing off (as it so happens, this is a winning commercial strategy too).

New relative to all the above is that it is possible also to transmit J2497 using any SDR capable of 1Msps down at 100KHz or baseband. Sample code for synthesizing J2497 waveforms is in the mitigations document released by the NMFTA²⁸ (see the MIT-licensed Python code block in the keyhole mitigations section). The sample buffers that it can generate could be transmitted from any capable SDR; we used the FL2K to great success, pictured on the right with an adapter board by Ted Yapo²⁹.



4. How to connect your tools to the powerlines on your bench

As covered in the "Adapters for PLC Read" section of *2TOOLS4PLC4TRUCKS*³⁰, if you've got yourself a proper J1708-to-J2497 converter, you'll probably need a DB-15 solder tail connector, and then something to join it to the power lines – I really like lever nuts for this. If you've got an SDR or two, you will want a DC block (see the slides for information on converting a Balun One Nine to a DC block) with an adapter for flying leads, and then something to join it to the power lines – I still like lever nuts for this too.

Optional Bonus Bench Stuff

It's optional, but you may want to get your trailer brake controller into a no-faults state: this will make it turn off its lamp and also stop sending LAMP ON messages all the time.

To do this, you will need to:

1. Provide air pressure to the supply and control ports of you brake controller. You can do this with a home compressor and some NPT threaded adapters. Bonus points for using RP417-compliant red/blue cabling and for attaching a NERF dart launcher to the exhaust port of the controller! Pictured next is the NERF dart launching 'cactus' designed by Eric Thayer and integrated on the CHV CTF bench at GRRCon 2021.

²³ Gardiner, Ben. PLC4TRUCKSDuck <https://github.com/TruckHacking/plc4trucksduck>

²⁴ Cornelius, Erin. stm32-j1708 Oct 2021 <https://github.com/grimm-co/stm32-j1708>

²⁵ Gardiner, Ben. sr-j1708 Jan 2022 <https://github.com/TruckHacking/sr-j1708>

²⁶ Poore, Chris, and Gardiner, Ben. "Power Line Truck Hacking: 2TOOLS4PLC4TRUCKS." DEF CON 30 Car Hacking Village 2019. http://www.nmfta.org/documents/ctsrp/Power_Line_Truck_Hacking_2TOOLS4PLC4TRUCKS.pdf?v=1

²⁷ Gardiner, Ben. PLC4TRUCKSDuck <https://github.com/TruckHacking/plc4trucksduck>

²⁸ Gardiner, Ben. "Mitigations Options to J2497 Attacks" March 3rd 2022. http://www.nmfta.org/documents/ctsrp/Actionable_Mitigations_Options_v9_DIST.pdf?v=1

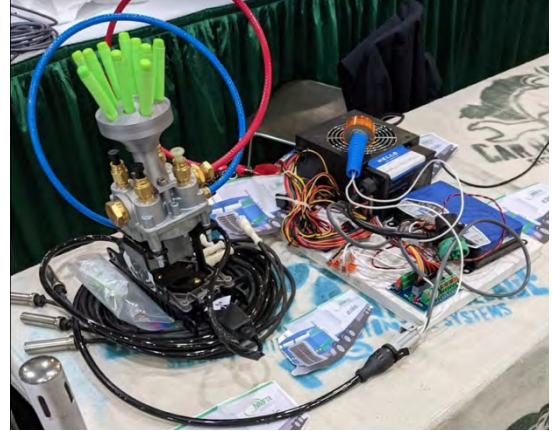
²⁹ Yapo, Ted. FL2K AM LPF May 2018 https://oshpark.com/shared_projects/OOkzY6K6

³⁰ Poore, Chris, and Gardiner, Ben. "Power Line Truck Hacking: 2TOOLS4PLC4TRUCKS." DEF CON 30 Car Hacking Village 2019. http://www.nmfta.org/documents/ctsrp/Power_Line_Truck_Hacking_2TOOLS4PLC4TRUCKS.pdf?v=1

2. Connect the wheel-end speed sensors.
3. Acquire and use the trailer brake supplier's diagnostic software or compatible suite. Use it to send the proprietary "clear faults" commands.
4. "Roll" the controller. Some brake controllers won't clear faults until they have been driven at 5 MPH for a bit. Simulating wheel-end speed signals can be done in multiple ways. Check out the Smart Sensor Simulator 2 (SSS2) and Jose Córcega's thesis³¹. Being able to send wheel-end speed signals to the brake controller will also allow you to test your findings while the trailer is in (simulated) motion!

Don't go around trying to test induced messages on trailers – especially ones that you don't own. Do it on your own bench with direct-connect – and whatever bugs you may

find on J2497 that were Access:Network are now elevated to Access:Adjacent due to CVE-2022-26131.



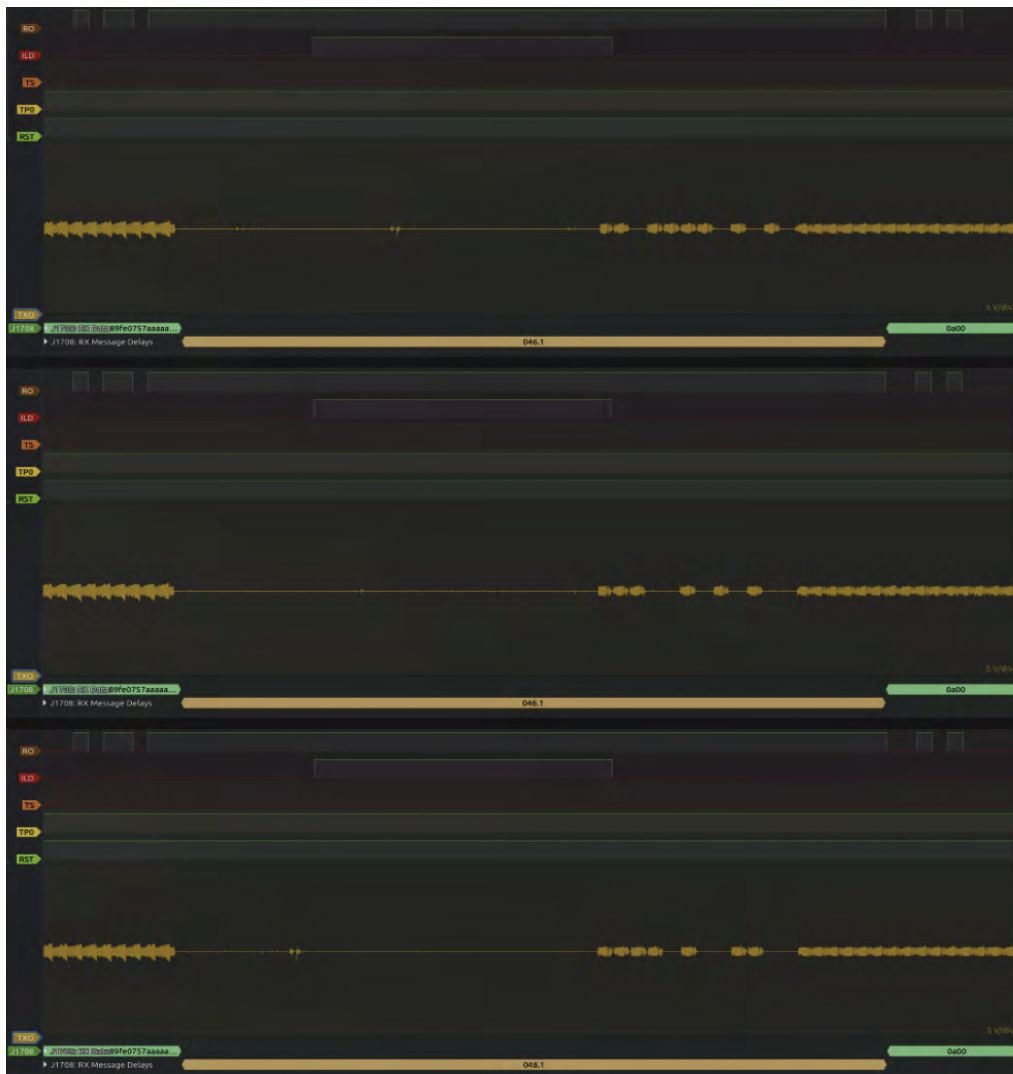
A Largely Unexplored Network

This research collaboration with AIS and others has been a blast, we've discovered that J2497 messages can be read and written remotely, as well as some diagnostics functions that have no replay protection. These and some other non-security-related findings speak to the fact that the J2497 powerline network has been largely unobservable for its deployed lifetime of approximately 22 years (as of this writing) – it will probably still be in use on the road in 2042.

The first finding was the observation that any preamble could be sent in J2497, as it would be discarded; only the MID in the body was sent on as a part of a J1708 message. This was made possible by synthesizing our own J2497 signals directly using an FL2K and also a bit-banging method. We later discovered that in fact the preamble could be dropped entirely and any valid body signal starting with the expected number of SYNC bits would be received and sent on as a J1708 message.

This finding helped us understand a strange WABCO TCS II bug: we noticed that the TCS II was sending what looked like random preamble bytes, not corresponding to the known MID in the body of the J2497 signals. This was observed by looking at the traces of J2497 on an oscilloscope; even the preamble can be "read out" as UART bits in ASK modulation. The three captures below were all taken from signals received as the same '0a00' LAMP ON message, but with clearly different preambles.

³¹ Córcega, Jose L. DESIGN OF A FORENSICALLY NEUTRAL ELECTRONIC ENVIRONMENT FOR HEAVY VEHICLE EVENT DATA RECORDERS. Master's Thesis, University of Tulsa. 2015



How then was this resulting in valid messages? Including the all-important LAMP ON message!? The answer was, of course, that the preamble in J2497 never really mattered enough for this bug to manifest in any noticeable performance issues, so it has been going on this way (with irrelevant arbitration priority) since the release of the WABCO TCS II near the 2001 onset of the regulation.

When developing the mitigations against these attacks in December 2021, we looked closely at the way the three trailer suppliers implemented bus arbitration, because we needed to use it for the keyhole mitigation³². We found that only one of the three controllers were correctly implementing bus arbitration according to the specification: yielding the bus to lower-valued MIDs. Of the other two, one was just retrying until it was granted access to the bus, and the other gave up trying to transmit in that period.

We don't mean to say that no one has noticed this or thought about it before – that's unlikely. It is more likely that engineers at an equipment supplier did notice one or more of these bugs, but their motivation to discuss the issue or make it public was chilled by the J2497 patents: an alternative supplier could never be found.

Consider the spurious chirp fragments being emitted from most trailer and tractor brake controllers. These are very noticeable even on an oscilloscope and have almost certainly been observed by engineers implementing J2497 solutions – see the logic analyzer trace below. The SSC P485 creates small-amplitude signals and cannot drive the power line network directly; for that it needs an amplifier, and since there are multiple nodes on a J2497 bus, the amplifiers must be gated. The SSC P485 handily

³² Gardiner, Ben. "Mitigations Options to J2497 Attacks" March 3rd 2022.
http://www.nmfta.org/documents/ctsrp/Actionable_Mitigations_Options_v9_DIST.pdf?v=1

offers such a signal, according to its own documentation: "[TS pin 11] Active low digital output. Enables the external output amplifier when driven high. Tri-states the external output amplifier when driven low."³³ Unfortunately, it also sometimes de-asserts that signal too early in response to a normal start bit from the microcontroller on its DI UART input pin.



These chirp fragments were almost certainly seen, but in the end they're benign (remember, arbitration never really worked), and what could be done about them? The J2497 solution was available to equipment suppliers only as a black box, and nothing could really be done about it. We had heard anecdotes about the solution never performing as well as advertised, and ultimately none of the additional smart features were deployed.

Ironically, the controller that correctly implemented bus arbitration actually suffers from a priority inversion bug because of it: it won't be able to send its high-priority messages, like LAMP ON, if it can't send its low-priority messages that are queued first. It sure seems like this patent-only standard was not great for the industry³⁴. This isn't an issue that ever crops up in the field, because there is very little bus-load: there isn't much else being transmitted on J2497.

J2497 is a very old bus, built on older technology (J1587) that hadn't had much attention paid to it because it is hard to debug, and were a problem found by an engineer, it would be hard to get time for fixes, since J2497 is not the future. We were once told by a supplier to whom we disclosed some of these issues, "I can assure you that development of smart trailer technology today [...] is leveraging the latest secure methods of communication protocols, and PLC is certainly not one of them."

The industry is focused on newer communications methods because J2497 never delivered on even its modest bandwidth promises. However, there's the problem of 20 years' worth of tractors and trailers using J2497. More than half of them will continue to be used for another 15 years. Furthermore, J2497 is the only industry standard way to satisfy the regulation on trailer ABS fault telltales: as long as fleets require backward compatibility with their older trailers, they will need to use J2497. J2497 isn't going anywhere, even if the R&D budget isn't available for it anymore.

³³ Intellon. "SSC P485 PL Transceiver IC". 1998

³⁴ For more opinions on the big downsides of patents on safety critical technology see Michael Ossman's H2HC 2017 keynote <https://github.com/h2hconference/2017/blob/41318f8412ff60339fcf7ba37f037f0f91b7265a/H2HC%20-%20Mike%20Ossmann%20-%20Keynote%20Notes.txt#L1>

Limits of Current Proven impacts

We did our testing using the tried-and-true method of analyzing diagnostics session traffic and replaying it. We've confirmed with solenoid test commands on all equipment and experimented with other commands (e.g., notepad and tone ring configuration), but are other solenoid controls possible? We think that RCE would almost certainly allow dumping of supply air.

Tractor brake controllers have both modulator tests and service valve tests. The modulator tests are very much like the solenoid tests: control pressure is required, but the service valve test will dump air regardless of control pressure applied. Most likely there is no service valve in trailer brake controllers because they are evolutions of the relay valves that preceded them; they may only be physically capable of modulating the control pressure.

However, there are other, more sophisticated, types of trailer brake controllers: roll-stability systems. These aren't just relay valves with solenoids, they are (purportedly) capable of applying brake pressure individually. When at ATA TMC March 2022 and sharing the disclosure with trailer people on the trade show floor, we were directed to look at roll stability controllers by no less than three individuals, all for this same reason. One asserted that it is quite common for roll-stability controllers to be installed on tanker trailers 🤔.

Why Disclose This?

The NMFTA researched trailer brake controllers and communications because, when we began, there appeared to be a gap in knowledge of security of the trailer brake controllers, and the industry was at a point where the existing J2497/PLC4TRUCKS communications standard would no longer be sufficient for fleets; new interface standards were being drafted by task forces in the ATA TMC. The NMFTA wanted to ensure that the next tractor-trailer interface would be a secure platform for the myriad of functions that fleets would like to deploy over the next decades.

The types of issues outlined in this post – where a standard has propagated a flaw that has now been deployed for decades – are really unfortunate and pose a dilemma. The standard predates a time when security considerations were the norm; it isn't unreasonable that the brake controllers have simple, replayable diagnostic commands; furthermore, the designers of J2497 created a very clever solution in 1998 to an almost impossible problem of adding digital communications to the same J560 connector used on all trailers since 1967.

On one hand, even discussing the issue is putting unwanted attention on thousands of deployed vulnerable devices. On the other hand, if the issue isn't widely understood, the desire for backwards compatibility by fleets will overwhelm any attempts by a minority trying to quietly fix the issue. Were it not for the timing of next-generation tractor-trailer standards coming together, and also for the fact that the NMFTA developed a collection of mitigations for fielded equipment, it would have not been appropriate to disclose the issue.

As soon as the CISA advisory was public, we shared it with the ATA TMC task forces who could take action to make the situation better with respect to J2497.

What We'll Keep Doing

Working with the standards groups; repeating tests to confirm; helping anyone who wants to implement the mitigations proposed

We will keep working with the ATA TMC task forces to ensure that the next-generation tractor-trailer interface does not inherit the issues we've seen in J2497. We met with the S.1 task force on the Next Generation Tractor Trailer Interface on April 21, 2022. The TF will make a decision on our request to exclude J2497 diagnostics and include mitigations in the NGTTI at the ATA TMC in-person meeting in September 2022. We are also looking for more testing opportunities to confirm these results on other equipment, as well as opportunities test new concepts. If you would like to host us for some testing, please contact ben.gardiner@nmfta.org.

About Ben Gardiner

Ben Gardiner is a Senior Cybersecurity Research Engineer contractor presently working to secure commercial transportation at the National Motor Freight Traffic Association (NMFTA). With more than ten years of professional experience in embedded systems design and lifetime worth of hacking experience, he has deep knowledge of the low-level functions of operating systems and the hardware with which they interface. Prior to partnering with the NMFTA team in 2019, he held security assurance and reversing roles at a global corporation, as well as working in embedded software and systems engineering roles at several organizations. He holds a M.S. in Engineering in Applied Math & Stats from Queen's University. He is a DEF CON Hardware Hacking Village (DC HHV) volunteer, is GIAC GPEN certified and a GIAC advisory board member, he is also chair of the SAE TEVEES18A1 Cybersecurity Assurance Testing TF (drafting J3061-2), and a voting member of the SAE Vehicle Electronic Systems Security Committee.

About IOActive

IOActive is a trusted partner for Global 1000 enterprises, providing research-fueled security services across all industries. Our cutting-edge security teams provide highly specialized technical and programmatic services including full stack penetration testing, program efficacy assessments, and hardware hacking. IOActive brings a unique attacker's perspective to every client engagement to maximize security investments and improve client's overall security posture and business resiliency. Founded in 1998, IOActive is headquartered in Seattle with global operations. For more information, visit ioactive.com.