# SURFACE VEHICLE RECOMMENDED PRACTICE

J2497™ MAR2026

Issued 2002-10
Stabilized 2023-11
Revised 2026-03

Superseding J2497 NOV2023

Power Line Carrier Communication for Commercial Vehicles

RATIONALE

Research indicates that SAE J2497 receivers are susceptible to remote RF induced signals.

This document has been updated to include a discussion of attack vectors and actionable mitigations to these attacks.

TABLE OF CONTENTS

1. SCOPE ..... 4

2. REFERENCES ..... 4
2.1 Applicable Documents ..... 4
2.1.1 SAE Publications ..... 4
2.1.2 ANSI Publications ..... 4
2.1.3 NIST Publications ..... 4
2.1.4 NHTSA Publications ..... 4
2.1.5 CISA Publications ..... 5
2.1.6 NMFTA Publications ..... 5
2.2 Related Publications ..... 5
2.2.1 SAE Publications ..... 5
2.2.2 NIST Publications ..... 5
2.2.3 CISA Publications ..... 5

3. ABBREVIATIONS ..... 5

4. INTELLECTUAL PROPERTY RIGHTS ..... 6

5. NETWORK DESCRIPTION ..... 7
5.1 PLC Network ..... 7
5.2 PLC Transceiver ..... 7
5.3 Coupling Examples ..... 8
5.4 Network Reachability ..... 8

SAE Executive Standards Committee Rules provide that: "This report is published by SAE to advance the state of technical and engineering sciences. The use of this report is entirely voluntary, and its applicability and suitability for any particular use, including any patent infringement arising therefrom, is the sole responsibility of the user."

SAE reviews each technical report at least every five years at which time it may be revised, reaffirmed, stabilized, or cancelled. SAE invites your written comments and suggestions.

Copyright © 2026 SAE International

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, or used for text and data mining, AI training, or similar technologies, without the prior written permission of SAE.

**TO PLACE A DOCUMENT ORDER:** Tel: 1-877-606-7323 (U.S. and Canada only)
Tel: 1-724-776-4970 (outside U.S. and Canada)
Fax: 724-776-0790
Email: CustomerService@sae.org
**SAE WEB ADDRESS:** http://www.sae.org

For more information on this standard, visit
https://www.sae.org/standards/content/J2497_202603/

Documents
Document Sharing Hub

Full document details: SAE J2497™ MAR2026 Power Line Carrier Communication for Commercial Vehicles

6. POWER LINE MESSAGE ..... 8
6.1 Message Format between Host Microcontroller and PLC Transceiver ..... 8
6.2 Message Format on the Power Line ..... 9
6.2.1 Preamble Format ..... 9
6.2.2 Data Body Format ..... 9
6.3 Message Encoding ..... 10
6.3.1 Preamble Encoding ..... 10
6.3.2 Data Body Encoding ..... 10
6.4 Message Timing ..... 11
6.5 Contention Resolution ..... 11

7. TRANSMITTER CHARACTERISTICS ..... 12
7.1 Waveform Generation ..... 12
7.2 Amplitude ..... 13
7.3 SUPERIORθ1 to SUPERIORθ2 Transition ..... 14
7.4 Conducted Emissions Limit ..... 14
7.5 ECU Isolation ..... 14

8. RECEIVER CHARACTERISTICS ..... 14
8.1 SUPERIOR States Recognition ..... 14

9. SOFTWARE FUNCTIONS ..... 15
9.1 Cab Mounted Trailer ABS Malfunction Indicator Lamp Control ..... 15
9.1.1 Trailer Device Control Functions ..... 15
9.1.2 Tractor Device Control Functions ..... 16
9.1.3 SAE J1587 Indicator Lamp Control ..... 17
9.1.4 SAE J1939 Indicator Lamp Control ..... 17
9.2 Other Software Functions ..... 17

10. PLC NETWORK MESSAGE FORMAT DEFINITIONS ..... 17
10.1 Trailer ABS Indicator Lamp ON (MID10) ..... 17
10.2 Trailer ABS Indicator Lamp OFF (MID 11) ..... 18
10.3 Trailer ABS Active (MID 87) ..... 18

11. PLC NETWORK MESSAGE FORMAT DEFINITIONS UNIQUE TO SAE J2497 ..... 18
11.1 Dynamic Claim to a Unique SAE J2497 MID ..... 18
11.1.1 Background ..... 18
11.1.2 Priority of MIDs 10, 11, and 87 ..... 18
11.1.3 Method ..... 19
11.1.4 Start Delay Time ..... 20
11.1.5 Physical Position ..... 20
11.1.6 MID Retention ..... 20
11.2 SAE J2497 MID Assignments ..... 21
11.3 Parameter Identification Assignments ..... 21
11.4 Subsystem Identification Assignments ..... 21
11.5 Failure Mode Identifier Assignments ..... 21

12. NOTES ..... 21
12.1 Revision Indicator ..... 21

APPENDIX A SUPERIOR STATE WAVEFORM ..... 22
APPENDIX B ECU ISOLATION ..... 23
APPENDIX C TIMING DIAGRAMS ..... 24
APPENDIX D WIRELESS ATTACK MITIGATIONS ..... 26


Documents
Document Sharing Hub
Full document details: SAE J2497™ MAR2026 Power Line Carrier Communication for Commercial Vehicles

Figure 1 Example of PLC network ..... 7
Figure 2 PLC transceiver ..... 7
Figure 3 Power line coupling techniques ..... 8
Figure 4 Example of preamble logic symbol encoding ..... 10
Figure 5 Example of data body logic symbol encoding ..... 10
Figure 6 Frequency swept carrier waveform ..... 12
Figure 7 Output driver test circuit ..... 13
Figure 8 Control of cab mounted trailer ABS indicator lamp by tractor device ..... 16
Figure 9 Example of trailer device set supporting dynamic addressing ..... 19
Figure 10 Example of adding ECU to trailer device set supporting dynamic addressing ..... 20

Table 1 Output voltage ..... 13
Table 2 Message ID assignment list ..... 21

Documents
Document Sharing Hub

Full document details: SAE J2497™ MAR2026 Power Line Carrier Communication for Commercial Vehicles

## 1. SCOPE

This SAE Recommended Practice defines a method for implementing a bidirectional, serial communications link over the vehicle power supply line among modules containing microcomputers. This document defines those parameters of the serial link that relate primarily to hardware and software compatibility such as interface requirements, system protocol, and message format that pertain to Power Line Communications (PLC) between Tractors and Trailers.

This document defines a method of activating the trailer ABS Indicator Lamp that is located in the tractor.

## 2. REFERENCES

### 2.1 Applicable Documents

The following publications form a part of this specification to the extent specified herein. Unless otherwise indicated, the latest issue of SAE publications shall apply.

#### 2.1.1 SAE Publications

Available from SAE International, 400 Commonwealth Drive, Warrendale, PA 15096-0001, Tel: 1-877-606-7323 (U.S. and Canada only) or 1-724-776-4970 (outside U.S. and Canada), www.sae.org.

| | |
|---|---|
| SAE J1587 | Electronic Data Interchange Between Microcomputer Systems in Heavy-Duty Vehicle Applications |
| SAE J1708 | Serial Data Communications Between Microcomputer Systems in Heavy-Duty Vehicle Applications |
| SAE J1939 | Serial Control and Communications Heavy-Duty Vehicle Network - Top-Level Document |

#### 2.1.2 ANSI Publications

Copies of these documents are available online at https://webstore.ansi.org.

| | |
|---|---|
| CISPR 25 | Vehicles, boats and internal combustion engines - Radio disturbance characteristics - Limits and methods of measurement for the protection of on-board receivers |

#### 2.1.3 NIST Publications

Available from NIST, 100 Bureau Drive, Stop 1070, Gaithersburg, MD 20899-1070, Tel: 301-975-6478, www.nist.gov.

| | |
|---|---|
| CVE-2020-14514 | PLC bus traffic can be sniffed reliably via an active antenna up to 6 feet away. Further distances are also possible, subject to environmental conditions and receiver improvements. |
| CVE-2022-26131 | Power Line Communications PLC4TRUCKS J2497 trailer receivers are susceptible to remote RF induced signals. |

#### 2.1.4 NHTSA Publications

Available from National Highway Traffic Safety Administration, 1200 New Jersey Avenue SE, West Building, Washington, DC 20590, Tel: 1-888-327-4236, www.nhtsa.gov.

| | |
|---|---|
| RCLRPT-24V915-6438 | Safety Recall 573 Report |

Documents
Document Sharing Hub
Full document details: SAE J2497™ MAR2026 Power Line Carrier Communication for Commercial Vehicles

2.1.5 CISA Publications

Available from Cybersecurity & Infrastructure Security Agency, 1110 N. Glebe Road, Arlington, VA 20598-0630, Tel: 1-844-729-2472, www.cisa.gov.

ICSA-22-063-01 ICS Advisory Trailer Power Line Communications (PLC) J2497

ICSA-25-021-03 ZF Roll Stability Support Plus (RSSPlus)

2.1.6 NMFTA Publications

Available from National Motor Freight Traffic Association, Inc., 1001 N. Fairfax Street, Suite 600, Alexandria, VA 22314, www.nmfta.org.

Actionable Mitigation Options for J2497 Attacks (Public Domain)

2.2 Related Publications

The following publications are provided for information purposes only and are not a required part of this SAE Recommended Practice.

2.2.1 SAE Publications

Available from SAE International, 400 Commonwealth Drive, Warrendale, PA 15096-0001, Tel: 1-877-606-7323 (U.S. and Canada only) or 1-724-776-4970 (outside U.S. and Canada), www.sae.org.

SAE J1939-91A Security Recommendations for Interfaces to On-Vehicle Networks

2.2.2 NIST Publications

Available from NIST, 100 Bureau Drive, Stop 1070, Gaithersburg, MD 20899-1070, Tel: 301-975-6478, www.nist.gov.

CVE-2024-12054CNA [Reserved at time of publication]

2.2.3 CISA Publications

Available from Cybersecurity & Infrastructure Security Agency, 1110 N. Glebe Road, Arlington, VA 20598-0630, Tel: 1-844-729-2472, www.cisa.gov.

ICSA-20-219-01 Trailer Power Line Communications

3. ABBREVIATIONS

ABS Antilock Brake System

AC Alternating Current

ASK Amplitude Shift Key modulation

CISPR Comité International Spécial des Perturbations Radioélectriques; English: Special international committee on radio interference

CVE Common Vulnerability Enumeration

DC Direct Current

Documents
Document Sharing Hub
Full document details: SAE J2497™ MAR2026 Power Line Carrier Communication for Commercial Vehicles

| | |
|---|---|
| ECU | Electronic Control Unit |
| FMI | Failure Mode Identifier |
| ICS | Industrial Control System |
| MID | Message Identifier |
| NRZ | Non Return to Zero modulation |
| PGN | Parameter Group Number |
| PID | Parameter ID |
| PL | Power Line |
| PLC | Power Line Communications |
| PRK | Phase Reversal Keying modulation |
| RF | Radio Frequency |
| SID | Subsystem ID |
| Tsd | Start Delay Time |

## 4. INTELLECTUAL PROPERTY RIGHTS

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by SAE International with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via a Letter of Assurance, then the statement is listed on https://www.sae.org/standards/patents. Letters of Assurance may indicate whether the patent holder is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses. Further, essential patent claims may exist for which a Letter of Assurance has not been received. SAE International is not responsible for identifying essential patent claims for which a license may be required, for conducting inquiries into the legal validity or scope of patent claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility.

Documents
Document Sharing Hub
Full document details: SAE J2497™ MAR2026 Power Line Carrier Communication for Commercial Vehicles

## 5. NETWORK DESCRIPTION

### 5.1 PLC Network

Figure 1 shows a typical PLC network. A typical network consists of Electronic Control Units (ECUs), with PLC transceivers, mounted on the tractor and trailer(s). These ECUs communicate to each other by sending Radio Frequency (RF) signals over the power line. These ECUs interface to the power line through a PLC transceiver.

The tractor PLC ECU must provide control for the Trailer ABS Indicator Lamp that is mounted in the tractor cab. This can be done by either a direct connection to the lamp, or by providing an appropriate control message (for example, by SAE J1587 or SAE J1939) to another ECU which then controls the lamp.

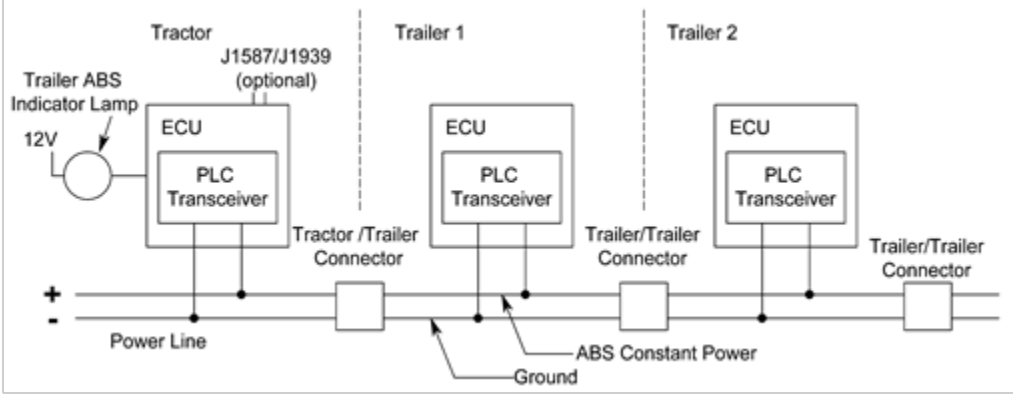



***Figure 1 - Example of PLC network***

### 5.2 PLC Transceiver

The microprocessor of an electronic module interfaces to the power line through a PLC transceiver. See Figure 2. The microprocessor sends digital data (Tx) to a coding device in the PLC transceiver. This data is in the format described in SAE J1708. The coding device converts the digital data into a signal suitable for being transmitted on the power line. This signal will be described in later sections. This signal (Signal_out) is then passed through the appropriate amplifier and filters before it is coupled onto the power line. Conversely, a PLC signal (Signal_in) is taken from the power line, filtered, and decoded into digital data (Rx). This data is sent to the host microprocessor in a format defined by SAE J1708.

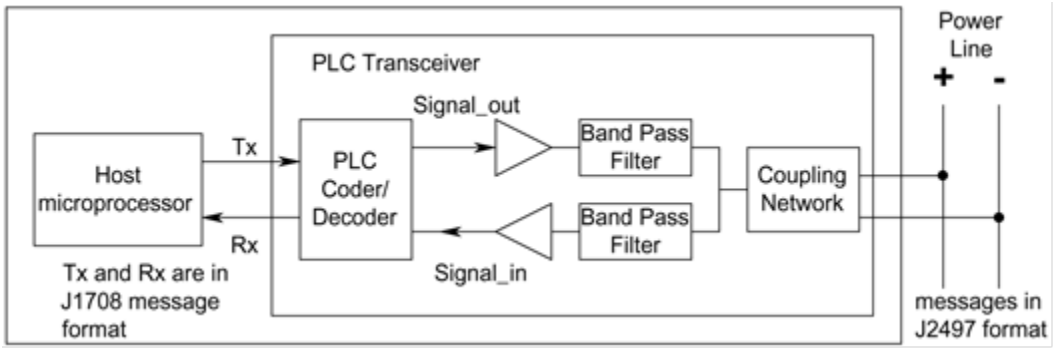



***Figure 2 - PLC transceiver***

Documents
Document Sharing Hub
Full document details: SAE J2497™ MAR2026 Power Line Carrier Communication for Commercial Vehicles

5.3 Coupling Examples

The PLC transceivers will interface to the power line, relative to the negative line, through the appropriate coupling network. Figure 3 illustrates two possible coupling networks. One provides capacitive coupling, and the other provides transformer (inductive) coupling of the PLC signals onto the power line.

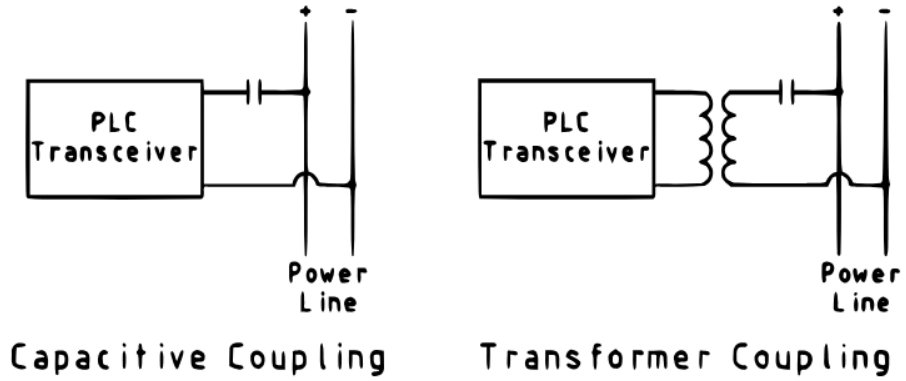



***Figure 3 - Power line coupling techniques***

5.4 Network Reachability

As disclosed in CVE- 2020-14514 and -2022-26131, the PLC network is reachable wirelessly – both read and write – from distances which vary for equipment configuration. Please refer to those vulnerabilities for further details on the reachability.

The equipment deployed to make use of SAE J2497 can rely on the network in safety critical ways (for example, NHTSA Part 573 Safety Recall Report 24V-915), and as such, mitigations against attacks via this wireless reachability are recommended for all equipment deployed to utilize SAE J2497, including equipment that uses it exclusively for backwards compatibility reasons (e.g., so that new tractors can protect trailers without tractor-trailer network connections other than SAE J2497). Please see later sections for further information on mitigation techniques.

6. POWER LINE MESSAGE

The message sent on the power line has two major parts, the preamble and the data body. See Figures C1 and C2 in Appendix C for following descriptions.

6.1 Message Format between Host Microcontroller and PLC Transceiver

The communications between the host microcontroller and the PLC transceiver follows the SAE J1708 message format. The only exception to SAE J1708 message format is the character gap between the first and second characters. The host microcontroller must wait 2 bit times after receiving the stop bit of the first character echoed back to the microcontroller before sending the second character. See Figure C1 in Appendix C.

Documents
Document Sharing Hub
Full document details: SAE J2497™ MAR2026 Power Line Carrier Communication for Commercial Vehicles