



SURFACE VEHICLE INFORMATION REPORT

J3322™

MAY2025

Issued

2025-05

Cybersecurity Testing, Verification, and Validation Methods

RATIONALE

The purpose of this document is to provide a list of methods for cybersecurity assurance for automotive.

TABLE OF CONTENTS

1.	SCOPE.....	8
1.1	Scope of Authority.....	8
1.1.1	Vehicle Definitions.....	8
1.2	Safety versus Cybersecurity.....	8
1.3	Developmental Considerations.....	8
1.4	Sensitive Information and Personally Identifiable Information.....	9
2.	REFERENCES.....	9
2.1	Applicable Documents.....	9
2.1.1	SAE Publications.....	9
2.1.2	AUTOSAR Publications.....	9
2.1.3	Code of Federal Regulations (CFR) Publications.....	9
2.1.4	IEEE Publications.....	9
2.1.5	IETF Publications.....	10
2.1.6	ISO and IEC Publications.....	10
2.1.7	ISO and SAE Publications.....	10
2.1.8	ITU Publications.....	10
2.1.9	MITRE Publications.....	11
2.1.10	NIST Publications.....	11
2.1.11	Open Web Application Security Project (OWASP) Foundation Publications.....	11
2.1.12	United States Code Publications.....	11
2.1.13	United States Department of Defense Publications.....	11
2.1.14	Other Publications.....	11
2.2	Related Publications.....	12
2.2.1	ISO and IEC Publications.....	12
2.2.2	ITU Publications.....	12
2.2.3	Other Publications.....	12
3.	EXECUTIVE SUMMARY - VEHICLE CYBERSECURITY VERIFICATION & VALIDATION METHODS.....	12
3.1	Purpose.....	12
3.2	How to Use This Document.....	13
4.	NEW TECHNOLOGY OR NEW TECHNIQUES.....	14
4.1	Reproducing Publicly Disclosed Attacks.....	14

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 © 2025 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: 877-606-7323 (inside USA and Canada)
Tel: +1 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
http://www.sae.org

SAE WEB ADDRESS:

Full document details: SAE J3322_202505

For more information on this standard, visit https://www.sae.org/standards/content/J3322_202505/

Documents

Standard, visit Sharing Hub

5.	THREAT ANALYSIS AND RISK ASSESSMENT (TARA)	14
5.1	Relationship of Cybersecurity V&V to Threats and Risks	14
6.	STRUCTURED CYBERSECURITY INFORMATION EXCHANGE TECHNIQUES	15
6.1	ISO/IEC 29147:2018	15
6.2	ITU-T X Series	15
7.	STRUCTURE OF SUBSECTIONS	16
8.	MAPPING TO ISO/SAE 21434	16
9.	SOFTWARE V&V METHODS	18
10.	HARDWARE V&V METHODS	19
11.	TRUST ANCHOR DEVICE V&V METHODS	20
11.1	Trust Anchors' Lifecycle Applicability	20
11.2	Common Requirements	20
11.2.1	Key Protection/Management	20
11.2.2	Cryptographic Algorithms and Protocols	21
11.2.3	Random Number Generator	21
11.2.4	Secure Nonvolatile Data	22
11.2.5	Cryptographic Algorithm Agility	22
11.2.6	Interface Control	22
11.2.7	Secure Execution Environment	23
11.2.8	Self-Test	23
11.3	Primary Use Cases	24
11.3.1	Authenticated Boot	24
11.3.2	Authenticated Update	24
11.3.3	Secure In-Vehicle Messaging	24
11.3.4	Access Mechanisms	24
11.3.5	Secure Storage	25
11.4	Application Use Cases	25
11.4.1	Intellectual Property Protection	25
11.4.2	Secure Diagnosis at the ECU Level	25
11.4.3	Secure Logging	25
12.	RADIO FREQUENCY COMMUNICATIONS V&V METHODS	25
12.1	Radio Frequency Communications Cybersecurity Risks and Attack Surfaces	25
12.2	Radio Frequency Communications V&V Lifecycle Applicability	26
12.3	Confirming Common Radio Frequency Cybersecurity Requirements	26
12.4	Penetration Test via Radio Frequency Network Emulation	27
13.	SYSTEM V&V METHODS	27
13.1	System Verification Methods	28
13.2	System Validation Methods	28
14.	REPORTING	29
14.1	Reproducibility	29
14.2	Traceability	29
14.3	Human Readable	30
14.4	Machine Readable	30
15.	METHODS HIERARCHY	30
16.	AFTERMARKET CONSIDERATIONS	37
16.1	Aftermarket Relevance	37
16.2	Aftermarket Definition	37
16.3	Aftermarket Product/System/Component Examples	37



17.	COLLECTION OF V&V METHODS.....	38
17.1	Static Code Analyzer.....	39
17.1.1	Exemplary Characteristics	39
17.1.2	Use Case	40
17.2	Software Composition Analysis	40
17.2.1	Exemplary Characteristics	41
17.2.2	Use Case	41
17.3	Test That Included Libraries Are Valid Instances	41
17.3.1	Exemplary Characteristics	41
17.3.2	Use Case	41
17.4	Test That Included Libraries Are Up-to-Date with Respect to Known Vulnerabilities.....	42
17.4.1	Exemplary Characteristics	42
17.4.2	Use Case	42
17.5	Formal Methods	42
17.5.1	Exemplary Characteristics	43
17.5.2	Use Case	43
17.6	Malformed Input Testing	43
17.6.1	Exemplary Characteristics	44
17.6.2	Use Case	45
17.7	Threat Analysis	45
17.7.1	Exemplary Characteristics	45
17.7.2	Use Case	45
17.8	Source Code Analysis for Cyber Resilience	46
17.8.1	Exemplary Characteristics	46
17.8.2	Use Case	46
17.9	Detection of Invalid Runtime Memory Accesses	46
17.9.1	Exemplary Characteristics	46
17.9.2	Use Case	46
17.10	Cryptographic Primitive Validation	46
17.10.1	Exemplary Characteristics	47
17.10.2	Use Case	47
17.11	Testing for Cyber Resilience Against TLS Downgrade Attacks.....	47
17.11.1	Exemplary Characteristics	47
17.11.2	Use Case	47
17.12	Testing for Transparent TLS Redirection.....	48
17.12.1	Exemplary Characteristics	48
17.12.2	Use Case	48
17.13	Testing That Random Number Generation (RNG) Is Sufficiently Unpredictable.....	48
17.13.1	Exemplary Characteristics	48
17.13.2	Use Case	48
17.14	Testing If “Pinning” RNG Is Possible	49
17.14.1	Exemplary Characteristics	49
17.14.2	Use Case	49
17.15	Test Worst-Case Results of Pinned RNG	49
17.15.1	Exemplary Characteristics	49
17.15.2	Use Case	49
17.16	Scanning for Embedded Encryption Keys or Passphrases	50
17.16.1	Exemplary Characteristics	50
17.16.2	Use Case	50
17.17	Scanning for Common Key Formats in the Clear	51
17.17.1	Exemplary Characteristics	51
17.17.2	Use Case	51
17.18	“Following the Comments”	51
17.18.1	Exemplary Characteristics	51
17.18.2	Use Case	51
17.19	Testing for Vulnerability to Timing Attacks.....	52
17.19.1	Exemplary Characteristics	52
17.19.2	Use Case	52

17.20	Testing for Vulnerability to Fault Injection Attacks	52
17.20.1	Exemplary Characteristics	53
17.20.2	Use Case	53
17.21	Testing for PCR Extension Vulnerabilities via Serial Bus Interposer	53
17.21.1	Exemplary Characteristics	53
17.21.2	Use Case	53
17.22	Testing for Random Number Generator Vulnerabilities to Undermine Cryptographic Operations on the Host via Serial Bus Interposer	53
17.22.1	Exemplary Characteristics	53
17.22.2	Use Case	54
17.23	Testing for Host-Side Response Parsers (Likely to Cause Memory Corruption Vulnerabilities) via Serial Bus Interposer	54
17.23.1	Exemplary Characteristics	54
17.23.2	Use Case	54
17.24	Testing for Host-Side Driver Authenticated Session Functionality, in Order to Capture Secrets (Such as Private Keys) That Are Transmitted over the Bus via Serial Bus Interposer	54
17.24.1	Exemplary Characteristics	54
17.24.2	Use Case	54
17.25	Use-Limit Enforcement	55
17.25.1	Exemplary Characteristics	55
17.25.2	Use Case	55
17.26	Using Key-Export, Test That Default Private Key Material Is Dissimilar	55
17.26.1	Exemplary Characteristics	55
17.26.2	Use Case	55
17.27	Test That Keys Generated on Multiple Trust Anchor Devices Are Dissimilar	55
17.27.1	Exemplary Characteristics	56
17.27.2	Use Case	56
17.28	Test That the Memory Space of a Co-Resident Processor Contains No Private Keying Material	56
17.28.1	Exemplary Characteristics	56
17.28.2	Use Case	56
17.29	Test Any External Storage for Private Key Material	56
17.29.1	Exemplary Characteristics	56
17.29.2	Use Case	56
17.30	Confirm Correct Hardware Module Implementation	57
17.30.1	Exemplary Characteristics	57
17.30.2	Use Case	57
17.31	Confirm Correct Algorithm Implementation	57
17.31.1	Exemplary Characteristics	57
17.31.2	Use Case	57
17.32	Confirm Correct Algorithm Uses	57
17.32.1	Exemplary Characteristics	58
17.32.2	Use Case	58
17.33	Confirm Absence of Private Key in All Memory of Devices	58
17.33.1	Exemplary Characteristics	58
17.33.2	Use Case	58
17.34	Confirm That Public Keys Cannot Be Substituted or Tampered	58
17.34.1	Exemplary Characteristics	58
17.34.2	Use Case	58
17.35	Confirm That Cryptographic Operations Cannot Be Performed with Removed Keys	59
17.35.1	Exemplary Characteristics	59
17.35.2	Use Case	59
17.36	Fuzz Test All Output for Any Remnants of Cleartexts	59
17.36.1	Exemplary Characteristics	59
17.36.2	Use Case	59
17.37	Entropy Tests	59
17.37.1	Exemplary Characteristics	60
17.37.2	Use Case	60
17.38	Ensure No Common Seeds	60
17.38.1	Exemplary Characteristics	60
17.38.2	Use Case	60

17.39	Test Integrity Verification on Any External Storage Medium	60
17.39.1	Exemplary Characteristics	60
17.39.2	Use Case	60
17.40	Test Correct Operation of Integrity Protection Mechanisms	61
17.40.1	Exemplary Characteristics	61
17.40.2	Use Case	61
17.41	Test Any External Storage for Cleartexts	61
17.41.1	Exemplary Characteristics	62
17.41.2	Use Case	62
17.42	Test That a Now-Deprecated Algorithm Cannot Be Used After a Firmware Update	62
17.42.1	Exemplary Characteristics	62
17.42.2	Use Case	62
17.43	Test That Secure Object Re-Provisioning Mechanism Cannot Modify Firmware	62
17.43.1	Exemplary Characteristics	63
17.43.2	Use Case	63
17.44	Test That Unsigned Code Cannot Be Executed	63
17.44.1	Exemplary Characteristics	63
17.44.2	Use Case	63
17.45	Test That Tampering of the Fallback Firmware Is Prevented	64
17.45.1	Exemplary Characteristics	64
17.45.2	Use Case	64
17.46	Test That JTAG Interface Is Disabled in Production	64
17.46.1	Exemplary Characteristics	64
17.46.2	Use Case	64
17.47	JTAG Debug Interface Unlock Testing	65
17.47.1	Exemplary Characteristics	65
17.47.2	Use Case	65
17.48	Test That the Default Passwords for Policy Changes Are Not Identical on All Devices	65
17.48.1	Exemplary Characteristics	65
17.48.2	Use Case	65
17.49	Test That Authentication Is Required to Erase Private Key Material	66
17.49.1	Exemplary Characteristics	66
17.49.2	Use Case	66
17.50	Test That Fuzzing Commands Cause No Leak of Private Key Material	66
17.50.1	Exemplary Characteristics	67
17.50.2	Use Case	67
17.51	Test to Confirm Faulty Parameters in Requests Does Not Trigger Leak of Keys	67
17.51.1	Exemplary Characteristics	67
17.51.2	Use Case	68
17.52	Test That Device Privileges Are Reduced in Successive Lifecycle Phases	68
17.52.1	Exemplary Characteristics	68
17.52.2	Use Case	68
17.53	Test If Reverting to a Previous Lifecycle Phase Is Possible	68
17.53.1	Exemplary Characteristics	69
17.53.2	Use Case	69
17.54	Test That Debugging Is Not Possible from Normal Mode	69
17.54.1	Exemplary Characteristics	69
17.54.2	Use Case	69
17.55	Test That Normal Mode Storage Contains No Communication Artifacts	69
17.55.1	Exemplary Characteristics	70
17.55.2	Use Case	70
17.56	Test That Physical Access Does Not Yield Protected Mode Storage Access	70
17.56.1	Exemplary Characteristics	70
17.56.2	Use Case	70
17.57	Test That Secure Execution Environment Sandboxing Is Enforced	70
17.57.1	Exemplary Characteristics	71
17.57.2	Use Case	71
17.58	Test That Normal Mode (Volatile) Memory Contains No Cleartexts	71
17.58.1	Exemplary Characteristics	71
17.58.2	Use Case	71

17.59	Test That Self-Test Failure Results in Transition to <i>Failure Mode</i>	72
17.59.1	Exemplary Characteristics	72
17.59.2	Use Case	72
17.60	Test That Transition to <i>Initialization State</i> Reverts Limitations of <i>Failure Mode</i>	72
17.60.1	Exemplary Characteristics	72
17.60.2	Use Case	72
17.61	Test That Failure of Memory Self-Tests Result in Transition to <i>Failure Mode</i>	72
17.61.1	Exemplary Characteristics	72
17.61.2	Use Case	73
17.62	Test That Failure of Integrity Self-Tests Result in Transition to <i>Failure Mode</i>	73
17.62.1	Exemplary Characteristics	73
17.62.2	Use Case	73
17.63	Test That Integrity Self-Tests Are Executed at All Power-on Transitions (Including Return from Quiescent Power Modes)	73
17.63.1	Exemplary Characteristics	73
17.63.2	Use Case	73
17.64	Test That Failure of Cryptographic Known Answer Self-Tests Result in Transition to <i>Failure Mode</i>	73
17.64.1	Exemplary Characteristics	74
17.64.2	Use Case	74
17.65	Test That Failure of Cryptographic Algorithm Self-Tests Results in the Given Algorithm Being Unavailable in <i>Failure Mode</i>	74
17.65.1	Exemplary Characteristics	74
17.65.2	Use Case	74
17.66	Test That Failure of Self-Tests in a Disabled Feature Does Not Result in <i>Failure Mode</i>	74
17.66.1	Exemplary Characteristics	74
17.66.2	Use Case	74
17.67	Side Channel Attack Protection	75
17.67.1	Exemplary Characteristics	75
17.67.2	Use Case	75
17.68	Test for Authenticated Boot	76
17.68.1	Exemplary Characteristics	76
17.68.2	Use Case	76
17.69	Test That Tampered Trust Anchor Device Updates Are Rejected	76
17.69.1	Exemplary Characteristics	76
17.69.2	Use Case	76
17.70	Test Authentication of Messages within the Vehicle	77
17.70.1	Exemplary Characteristics	77
17.70.2	Use Case	77
17.71	Testing Secure Erasure	78
17.71.1	Exemplary Characteristics	78
17.71.2	Use Case	78
17.72	Test All ECU Diagnostics Memory Views for Private Key Material	78
17.72.1	Exemplary Characteristics	78
17.72.2	Use Case	79
17.73	Test All ECU Diagnostics Memory Views for Remnants of Cleartexts	79
17.73.1	Exemplary Characteristics	79
17.73.2	Use Case	79
17.74	RF Jamming	79
17.74.1	Exemplary Characteristics	79
17.74.2	Use Case	80
17.75	Simple RF Emulation	80
17.75.1	Exemplary Characteristics	80
17.75.2	Use Case	80
17.76	Test to Establish Whether TCU Can Be Spoofed into an Illegal IP Connection	80
17.76.1	Exemplary Characteristics	80
17.76.2	Use Case	80
17.77	Test to Establish Whether TCU Can Be Made to Communicate to Other ECUs	81
17.77.1	Exemplary Characteristics	81
17.77.2	Use Case	81

17.78	Rogue Tower Analysis	81
17.78.1	Exemplary Characteristics	81
17.78.2	Use Case	81
17.79	SIM Card Extraction	81
17.79.1	Exemplary Characteristics	82
17.79.2	Use Case	82
17.80	Bluetooth Service Access Control Analysis	82
17.80.1	Exemplary Characteristics	82
17.80.2	Use Case	82
17.81	Inspection	82
17.81.1	Exemplary Characteristics	82
17.81.2	Use Case	83
17.82	Analysis	83
17.82.1	Exemplary Characteristics	83
17.82.2	Use Case	83
17.83	Test (Generic)	83
17.83.1	Exemplary Characteristics	84
17.83.2	Use Case	84
17.84	Demonstration	85
17.84.1	Exemplary Characteristics	85
17.84.2	Use Case	85
17.85	Gap Analysis	85
17.85.1	Exemplary Characteristics	85
17.85.2	Use Case	85
17.86	Technology Risk Analysis	86
17.86.1	Exemplary Characteristics	86
17.86.2	Use Case	86
17.87	Attack Tree Analysis	86
17.87.1	Exemplary Characteristics	86
17.87.2	Use Case	86
17.88	System Level Vulnerability Analysis	86
17.88.1	Exemplary Characteristics	86
17.88.2	Use Case	87
17.89	Security Design Review	87
17.89.1	Exemplary Characteristics	87
17.89.2	Use Case	87
17.90	Penetration Test	87
17.90.1	Exemplary Characteristics	87
17.90.2	Use Case	88
17.91	Red Teaming	88
17.91.1	Exemplary Characteristics	88
17.91.2	Use Case	88
17.92	Vulnerability Scanning	88
17.92.1	Exemplary Characteristics	89
17.92.2	Use Case	89
17.93	Stress Testing	89
17.93.1	Exemplary Characteristics	90
17.93.2	Use Case	90
18.	NOTES	90
18.1	Revision Indicator	90
Figure 1	V&V methods to ISO/SAE 21434 mapping relationship	16
Figure 2		38
Table 1		31

1. SCOPE

1.1 Scope of Authority

This document specifically pertains to cybersecurity for vehicles. It has been developed by SAE International (SAE) Committee Technical Committee on Vehicle Electrical and Electronic Systems, "Cybersecurity Testing Task Force," a subcommittee of SAE Committee, "Vehicle Cybersecurity Systems Engineering Committee." This committee is authorized under the scope and authority of the SAE Electronic Design Automation Steering Committee, which is organized under the scope and authority of the SAE Electrical Systems Committee (also known as the Electrical Systems Group), which is directly under the scope and authority of the SAE Motor Vehicle Council.

The SAE Motor Vehicle Council's stated scope of influence and authority, as defined by SAE, includes, "passenger car and light truck." By definition, this excludes motorcycles, certain trailers, heavy trucks, buses, snowmobiles, watercraft, marine vessels, off-road, multi-purpose vehicles, certain other specialty vehicles, and aircraft.

1.1.1 Vehicle Definitions

According to 23 U.S.C. § 157 [Title 23 Highways; Chapter 1 Federal-Aid Highways], a passenger car is defined as:

"a motor vehicle with motive power (except a multipurpose passenger motor vehicle, motorcycle, or trailer) designed to carry not more than 10 individuals."

According to 40 Code of Federal Regulations (CFR) § 86.082-2 (from the U.S. Environmental Protection Agency), 07/2017:

"a light-duty truck means any motor vehicle rated at 8,500 pounds GVWR or less which has a vehicle curb weight of 6,000 pounds or less and which has a basic vehicle frontal area of 45 square feet or less, which is: (1) Designed primarily for purposes of transportation of property or is a derivation of such a vehicle, or (2) Designed primarily for transportation of persons and has a capacity of more than 12 persons, or (3) Available with special features enabling off-street or off-highway operation and use. Light-duty vehicle means a passenger car or passenger car derivative capable of seating 12 passengers or less."

NOTE 1: SAE tends to adopt vehicle size and weight definitions consistent with those from the U.S. Environmental Protection Agency.

NOTE 2: Application of the information contained herein for vehicles outside of the scope as defined above is not recommended by SAE.

1.2 Safety versus Cybersecurity

This document specifically pertains to the notion of *cybersecurity* (as defined by ISO/SAE 21434); however, in the construction of an automotive system, it is clear that *safety* also needs to be considered (that is, the resilience of the system to continually meet its expected correctness requirements).

While a cybersecurity issue *may* have an impact on safety (e.g., the ability to make a given system infringe on its safety requirements), achieving an overall goal of both safety and cybersecurity should not be mutually exclusive.

The adoption of a cybersecurity process adhering to techniques presented in this document neither allows for the system to meet its safety requirements *nor* precludes it. No method in this document either gives safety guarantees or limits the adoption of other techniques/standards that may.

1.3 Developmental Considerations

This document does not present, list, or document any techniques that fall outside of the realm of cybersecurity. To that end, it is expected that an adopter of this document will adhere to the "recommended developmental considerations" for the system that they are constructing (at the hardware, software, and system level).

For example, this document is not intended to cover topics such as: programming language selection, real-time operating system selection, nor communications protocol selection. This document is not intended to cover testing from non-cybersecurity-related functional requirements. Developmental considerations that are not cybersecurity related must be addressed as part of the wider system development plan; choices in the wider plan may have impact on the techniques that are required in this document and vice versa.

It is expected that, prior to adopting tests from this document into a Verification & Validation (V&V) plan, the correct level of rigor has been used to ensure that the system under consideration is being developed in the most appropriate way, and that the recommended best practice is followed.

1.4 Sensitive Information and Personally Identifiable Information

There are many methods described in this document which pertain to identifying the presence of *sensitive information*. For the purposes of this document and the methods herein, Personally Identifiable Information (PII) is a type of sensitive information. For further insight into what V&V designers should consider PII in their plans, consult the definitions by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, but also the authors recommend that this definition be expanded to include other classes of information that are relevant as PII in an automotive context, e.g., Vehicle Identification Number (VIN), (geolocation) breadcrumbs.

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: 877-606-7323 (inside USA and Canada) or +1 724-776-4970 (outside USA), www.sae.org.

SAE J3101 Hardware Protected Security for Ground Vehicles

2.1.2 AUTOSAR Publications

Copies of these documents are available online at <https://www.autosar.org/>.

AUTOSAR SECOC Specification of Secure Onboard Communication. Available at:

https://www.autosar.org/fileadmin/standards/R19-11/CP/AUTOSAR_SWS_SecureOnboardCommunication.pdf.

AUTOSAR MACSEC Specification of MACsec Key Agreement.

Available at: https://www.autosar.org/fileadmin/standards/R22-11/CP/AUTOSAR_SWS_MACsecKeyAgreement.pdf.

2.1.3 Code of Federal Regulations (CFR) Publications

Copies of these documents are available online at <https://www.ecfr.gov>.

40 CFR § 86.082-2 Definitions

2.1.4 IEEE Publications

Available from IEEE Operations Center, 445 and 501 Hoes Lane, Piscataway, NJ 08854-4141, Tel: 732-981-0060, www.ieee.org.

IEEE 802.1AE IEEE Standard for Local and metropolitan area networks-Media Access Control (MAC) Security

2.1.5 IETF Publications

Available from Internet Engineering Task Force, 1000 N West Street, Suite 1200, Wilmington, DE 19801, Tel: +1 302-319-3421, www.ietf.org.

RFC 2459 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. Available at: <https://www.rfc-editor.org/info/rfc2459>.

2.1.6 ISO and IEC Publications

Available from International Organization for Standardization, ISO Central Secretariat, 1, ch. de la Voie-Creuse, CP 56, CH-1211 Geneva 20, Switzerland, Tel: +41 22 749 01 11, www.iso.org.

Available from IEC Central Office, 3, rue de Varembe, P.O. Box 131, CH-1211 Geneva 20, Switzerland, Tel: +41 22 919 02 11, www.iec.ch.

ISO/IEC 29147:2018 Information technology — Security techniques — Vulnerability disclosure

2.1.7 ISO and SAE Publications

Available from International Organization for Standardization, ISO Central Secretariat, 1, ch. de la Voie-Creuse, CP 56, CH-1211 Geneva 20, Switzerland, Tel: +41 22 749 01 11, www.iso.org.

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

ISO/SAE 21434 Road Vehicles - Cybersecurity Engineering

2.1.8 ITU Publications

Available from International Telecommunication Union, Place des Nations, 1211 Geneva 20 Switzerland, <https://www.itu.int/>.

ITU-T X.1500 Overview of cybersecurity information exchange

ITU-T X.1520 Common vulnerabilities and exposures

ITU-T X.1521 Common vulnerability scoring system

ITU-T X.1524 Common weakness enumeration

ITU-T X.1525 Common weakness scoring system

ITU-T X.1526 Language for the open definition of vulnerabilities and for the assessment of a system state

ITU-T X.1528 Common platform enumeration

ITU-T X.1528.1 Common platform enumeration naming

ITU-T X.1541 Incident object description exchange format version 2

ITU-T X.1544 Common attack pattern enumeration and classification

2.1.9 MITRE Publications

Available from MITRE Corporation, 202 Burlington Road, Bedford, MA 01730, Tel: +1 703-983-6000, www.mitre.org.

CWE-195 Signed to Unsigned Conversion. Available at: <https://cwe.mitre.org/data/definitions/195.html>.

CWE-259 Use of Hard-coded Password. Available at: <https://cwe.mitre.org/data/definitions/259.html>.

CWE-321 Use of a One-Way Hash without a Salt. Available at: <https://cwe.mitre.org/data/definitions/321.html>.

CWE-401 Missing Release of Memory after Effective Lifetime.
Available at: <https://cwe.mitre.org/data/definitions/401.html>.

CWE-476 NULL Pointer Dereference. Available at: <https://cwe.mitre.org/data/definitions/476.html>.

CWE-845 Access of Resource Using Incompatible Type.
Available at: <https://cwe.mitre.org/data/definitions/845.html>.

2.1.10 NIST Publications

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

NIST SP 800-22 A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications

NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations

NIST SP 800-88 Guidelines for Media Sanitization

2.1.11 Open Web Application Security Project (OWASP) Foundation Publications

Available from The OWASP Foundation Inc., 300 Delaware Avenue, Suite 210 #384, Wilmington, DE 19801, Tel: +1 951-692-7703, <https://owasp.org/>.

OWASP Mobile Application Security Testing Guide

2.1.12 United States Code Publications

Copies of these documents are available online at <https://uscode.house.gov/>.

23 U.S.C. § 157 National Environmental Policy Act of 1969 reporting program

2.1.13 United States Department of Defense Publications

Available from U.S. Department of Defense, 1400 Defense Pentagon, Washington, DC 20301-1400, www.defense.gov.

DoD 5220.22M-ECE National Industrial Security Program Operating Manual (NISPOM).
Available at: <https://sgp.fas.org/library/nispom/nispom2006.pdf>.

2.1.14 Other Publications

E-safety Vehicle Intrusion Protected Applications (EVITA) project overview. (2010). <https://www.evita-project.org>.

Jones, C. (2008). *Applied software measurement: Global analysis of productivity and quality* (3rd ed.). McGraw Hill.

2.2 Related Publications

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

2.2.1 ISO and IEC Publications

Available from International Organization for Standardization, ISO Central Secretariat, 1, ch. de la Voie-Creuse, CP 56, CH-1211 Geneva 20, Switzerland, Tel: +41 22 749 01 11, www.iso.org.

Available from IEC Central Office, 3, rue de Varembe, P.O. Box 131, CH-1211 Geneva 20, Switzerland, Tel: +41 22 919 02 11, www.iec.ch.

ISO/IEC 18045 Information technology — Security techniques — Methodology for IT security evaluation

2.2.2 ITU Publications

Available from International Telecommunication Union, Place des Nations, 1211 Geneva 20 Switzerland, <https://www.itu.int/>.

ITU-T X.1528.2 Common platform enumeration name matching

ITU-T X.1528.3 Common platform enumeration dictionary

ITU-T X.1528.4 Common platform enumeration applicability language

2.2.3 Other Publications

Schneier, B. (1999). Attack trees. https://www.schneier.com/academic/archives/1999/12/attack_trees.html.

Shostack, A. (2014). *Threat modeling: Designing for security*. Wiley.

3. EXECUTIVE SUMMARY - VEHICLE CYBERSECURITY VERIFICATION & VALIDATION METHODS

This document provides a list of tests, techniques, actions – i.e., methods – for confirming the cybersecurity of a vehicle, its subsystems, and/or its components. There is no guidance provided on how to select from the list of methods, nor how to plan execution of those selected.

The document begins by offering some context on the relationship of the methods to various other aspects of design of cybersecurity for vehicles. The document then offers some categories from which many methods have been derived in the development of the document, including the SAE J3101 Hardware Protected Security Environment (HPSE) *Common Requirements*, *Primary Use Cases*, and *Application Use Cases*.

Finally, the document offers a cross-reference of the methods along with the devices, types, lifecycle phases, etc., to which they may apply and the bulk of the document, in the form of the list of methods. Each method captures instructions for preparation and execution of the method, ideal output of the method, and possible use cases for application of the method.

3.1 Purpose

This document is intended to provide a clear description of a wide variety of V&V methods from different categories and the necessary classes of tools used for effective cybersecurity V&V. The authors intend it to be used as a *menu* of possible methods from which to choose when creating a detailed cybersecurity V&V plan.

Each method described will include a level of detail sufficient for a cybersecurity V&V plan designer to use the described method as a starting point for drafting their own detailed cybersecurity V&V plans. This level of detail is expected to result in an explanation of each method's expected characteristics and use cases. Some other relevant features to methods or tools that would be necessary in a detailed V&V plan such as reporting format, content, or metrics have been omitted intentionally from this document.

The authors recognize that the specifics of the systems for which detailed V&V plans will be developed dictate the practical aspects of the methods; rather than provide method details which would amount to examples that readers would need to translate to their specific cases, the authors aim to provide brief general descriptions of the methods which can be easily browsed and specialized to individual instances of detailed cybersecurity V&V plans.

The goal of this document is not to provide a prescriptive list of activities that should be performed; it is, instead, to provide a repository of methods useful in ensuring a required level of cybersecurity for a component or system within a vehicle. The resulting document should serve as a collection of *possible methods* from which methods may be selected for activities to form a tailored vehicle cybersecurity assurance V&V plan.

It should be noted that the list of techniques prescribed in this document is neither exhaustive, explicitly recommended, nor up-to-date. Furthermore, as new techniques and exploits are discovered and invented, it is possible that the state-of-the-art may out-date this standard (see [Section 4 New Technology or New Techniques](#)). It is also possible that cybersecurity V&V activities may disrupt, damage, or disable vehicle systems or features, which may discontinue the activities.

This document forms an *à la carte* list of methods from which methods may be selected to ensure the overall cybersecurity of a given component or system – it is expected that a cybersecurity V&V plan designer will use this document to inform the design of their detailed V&V plan.

In addition, no onus is placed onto SAE that adopting any or all of the techniques presented in this document is sufficient to ensure an overall level of cybersecurity in a given system. Nor is there any onus on SAE that the list of methods applies specifically to any class of vehicles under the purview of SAE.

3.2 How to Use This Document

The authors suggest that this document be used by V&V Plan Designers to fill in their needs for V&V plans. V&V Designers could come from Original Equipment Manufacturers (OEMs) or suppliers and be responsible for V&V plans for single components, modules (systems of components), or entire systems – the devices under test. Furthermore, the specifics of what needs to be confirmed will be driven by the details of operation of the devices under test.

With the specifics of what needs to be confirmed in-hand, V&V Designers are invited to consult the sections of this document which list concrete methods/techniques and to select ones that apply to the specifics. Methods selected should be modified to match the context of the devices under test for which the V&V Designer is designing.

Methods selected should also be executed as activities in the various phases of product lifecycle (e.g., re-flashing, booting, manufacturing line mode, transport mode, dealer showroom mode, dealer inventory mode, decommissioning, airbag all-deploy, returns, etc.). The phases of execution for the activities should be adapted to the specifics of the devices under test. The methods selected in activities for a V&V plan should be independent of – and not relying on – built-in tests, especially for the later phases of product execution.

This document says nothing – intentionally – about how to design a V&V plan or what methods *must* be included in such plans. Please consult other SAE documents for details on these topics.

If, in the use of this document, a method is known to the V&V Designer which does not appear in this document, the authors encourage the Designer to submit this method for inclusion into future revisions of this document.

4. NEW TECHNOLOGY OR NEW TECHNIQUES

The authors believe that innovation is a hallmark of the digital hardware and software industries and that safety and cybersecurity V&V methods or technologies are not immune to this innovation.

This document should not be used to exclude any testing method or tool from a vehicle cybersecurity V&V plan. At the time of creation of a tailored vehicle cybersecurity V&V plan, new methods or technologies are to be considered by those creating the plan; furthermore, it is the position of this document that any method omitted from here is to be permitted to be used in anticipation of newer methods. This includes both unintentionally omitted methods and significant improvements in speed or accuracy over the methods and/or technologies described herein.

This document does consider the applicability of V&V methods to the various portions of the system development lifecycle. Those lifecycle considerations are documented in the “Use Case” subsection for each method.

4.1 Reproducing Publicly Disclosed Attacks

The cybersecurity community collectively creates troves of useful V&V information on an ongoing basis in the form of publicly disclosed attacks. The practice of staying up-to-date on the latest attacks is recommended by ISO/SAE 21434, and the effort spent on it can be amortized into developing V&V plans also. The authors recommend that readers developing a tailored vehicle cybersecurity V&V plan combine relevant public attacks with selections from the following sections of this document (as already directed).

5. THREAT ANALYSIS AND RISK ASSESSMENT (TARA)

This section discusses the use of TARA, or the work products produced by TARA, to enable cybersecurity V&V methods. Refer to ISO/SAE 21434 for more information about TARA.

TARA produces representations or models of potential threats to the automotive system. The fidelity of these models improves as the TARA evolves throughout the system design lifecycle. Even high-level threat models can be utilized by attack tree analysis as part of system level vulnerability analysis during system level product design (refer to 8.5 of ISO/SAE 21434).

Mature threat models can inform V&V planning. V&V activities can be designed around portions of a threat model in order to emulate attacks against the system.

5.1 Relationship of Cybersecurity V&V to Threats and Risks

This document focuses on providing a broad listing of cybersecurity V&V methods. It is expected that these methods will be selected for execution in activities at various phases of the product development lifecycle. A mature integration of cybersecurity concerns into the product development lifecycle will include multiple phases of threat modeling, including architectural analysis, vulnerability assessments, and further refinements of risk assessments stemming from the results at the various stages of V&V.

This document does not articulate the particular relationship of a method to threat and/or risk assessments at any of the above stages; this is because the relationship of a given cybersecurity V&V method to the risk and/or threat to systems is not always clearly defined.

Considering that discovering a vulnerability may or may not have a clear influence on a risk assessment depending on the phase of development and the context of the system being considered as it relates to a fielded product (e.g., command injection made possible by a network-listening daemon without authentication could be utilized by attackers in a myriad number of ways). Each of the ways could yield progress toward one of several attacker objectives, where each attacker objective has its own associated impact on the business.

Based on the understanding that a risk is where impact (on stakeholders/business) combines with likelihood, a given cybersecurity V&V method would most certainly have an influence on the risk estimate – namely, by influencing the likelihoods; however, the impact on the stakeholders or business may not be well-defined at the time of executing the V&V activity (e.g., the above command injection vulnerability, since it contributes to one of many possible attacker objectives, has no well-defined impact alone). It is the attacker objectives that have well-defined impact.

Furthermore, based on the understanding that a threat is where an adversary's capability is combined with a vulnerability, a given cybersecurity V&V method would most certainly have an influence on the threat potential – namely, by influencing the estimates of the required skill, knowledge, etc., of a specific vulnerability based on the concrete results of the V&V activity; however, the capability of an adversary may not be well-defined at the time of executing the V&V activity (e.g., the threat of the command injection vulnerability is not well-defined unless the context of what the actor is trying to exploit it is also specified).

The integration of cybersecurity V&V methods with the larger topic of threat and risk assessments is not articulated to any level of detail in this document. Instead, the working group responsible for this document plans to better articulate the influence that cybersecurity V&V can have on risk estimates in a later specification focusing on metrics and reporting.

6. STRUCTURED CYBERSECURITY INFORMATION EXCHANGE TECHNIQUES

The execution of a vehicle cybersecurity V&V plan (as constructed by selecting some methods from this document) will inevitably lead to issues that need to be reported. In the case that the issues which must be reported are relevant to external entities, then the format of the report should be given some consideration. Those creating cybersecurity V&V plans may also want to consider specifying reporting structures for the benefit of internal consumers of the test reports.

This document makes no specific recommendations on reporting. In the interest of completeness, we highlight the following resources which are available and direct readers to consult these authoritative sources for considerations of reporting formats.

6.1 ISO/IEC 29147:2018

- ISO/IEC 29147:2018 gives guidelines for the disclosure of potential vulnerabilities in products and online services. It details the methods a vendor should use to address issues related to vulnerability disclosure.
- ISO/IEC 29147:2018 is applicable to vendors who respond to external reports of vulnerabilities in their products or online services.

6.2 ITU-T X Series

- X.1500 Overview of cybersecurity information exchange
- X.1520 Common vulnerabilities and exposures (CVE)
- X.1521 Common vulnerability scoring system (CVSS)
- X.1524 Common weakness enumeration (CWE)
- X.1525 Common weakness scoring system (CWSS)
- X.1526 Language for open definition of vulnerabilities and for assessment of a system state
- X.1528 Common platform enumeration (CPE)
 - X.1528.1 CPE naming/.2 CPE name matching/.3 CPE dictionary/.4 CPE applicability language
- X.1541 Incident object description exchange format
- X.1544 Common attack pattern enumeration and classification (CAPEC)

7. STRUCTURE OF SUBSECTIONS

For [Section 9 Software V&V Methods](#) through [13.2 System Validation Methods](#), inclusive: Each section represents a different category of V&V method. These sections give some introduction to the general applicability of methods of its category along with some context for how the methods of this category were sourced and generated in detail by the task force. Finally, each section lists example methods using forward references to detailed method definitions in a later section.

There is overlap between the methods for each of these categories and, as such, the methods themselves are collected together in the later major section toward the end (see [Section 17 Collection of V&V Methods](#)) where each method is defined in detail and tagged with its associated categories, sources, and lifecycle phases.

8. MAPPING TO ISO/SAE 21434

This document does not explicitly associate the V&V methods to the Clauses 9, 10, or 11 of ISO/SAE 21434. For those who are interested in mapping these methods to those clauses (and hence also the lifecycle stages as defined by ISO/SAE 21434), Figure 1 serves as a reference.

Note that the majority of these methods are on the right side of the “V,” so the “V” diagram is adapted for readability. The methods suitable for the concept phase overlap a great deal with the latest (i.e., post-integration) validation phase; thus, instead of duplicating the methods, they are appended with the “*” mark in Figure 1.



Figure 1 - V&V methods to ISO/SAE 21434 mapping relationship

Note also that the V&V methods of this document are too numerous to fit in Figure 1, thus they have been grouped together as follows. The groups are depicted as a lighter shaded box in Figure 1.

“Test Included Libraries” is a group of

- [17.3 Test That Included Libraries Are Valid Instances](#)
- [17.4 Test That Included Libraries Are Up-to-Date with Respect to Known Vulnerabilities](#)

“Transport Layer Security (TLS) Downgrade & Redirection” is a group of

- [17.11 Testing for Cyber Resilience Against TLS Downgrade Attacks](#)
- [17.12 Testing for Transparent TLS Redirection](#)

“Random Number Generator (RNG) Testing” is a group of

- [17.13 Testing That Random Number Generation \(RNG\) Is Sufficiently Unpredictable](#)
- [17.14 Testing If “Pinning” RNG Is Possible](#)
- [17.15 Test Worst-Case Results of Pinned RNG](#)

“Secrets Embedded or In The Clear” is a group of

- [17.16 Scanning for Embedded Encryption Keys or Passphrases](#)
- [17.17 Scanning for Common Key Formats in the Clear](#)

“Test Serial Bus Interposer” is a group of

- [17.21 Testing for PCR Extension Vulnerabilities via Serial Bus Interposer](#)
- [17.22 Testing for Random Number Generator Vulnerabilities to Undermine Cryptographic Operations on the Host via Serial Bus Interposer](#)
- [17.23 Testing for Host-Side Response Parsers \(Likely to Cause Memory Corruption Vulnerabilities\) via Serial Bus Interposer](#)
- [17.24 Testing for Host-Side Driver Authenticated Session Functionality, in Order to Capture Secrets \(Such as Private Keys\) That Are Transmitted over the Bus via Serial Bus Interposer](#)

“Test & Demonstration” is a group of

- [17.83 Test \(Generic\)](#)
- [17.84 Demonstration](#)

Similarly, “Analysis, Test & Demo” is a group which adds also

- [17.82 Analysis](#)

“Gap, Risk, Attack Tree, Sys-level Analysis” is a group of

- [17.85 Gap Analysis](#)
- [17.86 Technology Risk Analysis](#)
- [17.87 Attack Tree Analysis](#)
- [17.88 System Level Vulnerability Analysis](#)

“Pen Testing & Red Teaming” is a group of

- [17.90 Penetration Test](#)
- [17.91 Red Teaming](#)

Finally, “J3101 Trust Anchor Tests” is a group of all the methods tagged with “J3101 derived” – see [Section 15 Methods Hierarchy](#) for the complete list.

9. SOFTWARE V&V METHODS

The methods outlined in what follows are applicable to wide variety of types of software produced, consumed, and deployed in vehicle systems. Those responsible for creating vehicle cybersecurity V&V plans should consider what aspects of the execution environment are controllable when selecting methods from the following. Depending on what is controllable, the type of software being confirmed by V&V may be one of the following broad categories:

- Operating System Software
- Applications Software (*Apps*)
- Complete Images (sometimes colloquially *Firmware*)

The *Apps* category deserves special considerations; in this category, the V&V plan must give assurance that the assets handled by the software are reasonably protected in environments which may not be controllable by either the person executing the V&V activities (e.g., the testers), or developers, or both. In this model, the subject of *application security* applies. Readers are encouraged to consult the OWASP Mobile Application Security Testing Guide (MASTG) for more details, including testing methods for both Android and iOS execution environments.

The OWASP MASTG contains detailed testing methods to confirm cybersecurity for many aspects of mobile applications; furthermore, many of the methods are applicable in more general cases as well. In the following, we will make references to the OWASP MASTG wherever applicable.

NB: The OWASP MASTG is under active development during the drafting of this document; therefore, the references made to it in what follows could be missing when you are reading it.

Following software engineering best practices will lead to more efficient V&V activities and V&V plans. However, standard software engineering practices (DevOps) are enhanced for cybersecurity (SecDevOps).

- <https://secdev.ieee.org/>
- <https://www.sei.cmu.edu/>
- <https://www.cert.org/secure-coding/>

This document introduces several Software V&V methods – some examples of which are listed below. For details of the methods, see the corresponding descriptions in [Section 17 Collection of V&V Methods](#). For a complete list of all software V&V methods, see those tagged with “software” in [Section 15 Methods Hierarchy](#).

- [17.1 Static Code Analyzer](#)
- [17.2 Software Composition Analysis](#)
- [17.3 Test That Included Libraries Are Valid Instances](#)
- [17.4 Test That Included Libraries Are Up-to-Date with Respect to Known Vulnerabilities](#)
- [17.5 Formal Methods](#)
- [17.6 Malformed Input Testing](#)
- [17.8 Source Code Analysis for Cyber Resilience](#)
- [17.9 Detection of Invalid Runtime Memory Accesses](#)
- [17.10 Cryptographic Primitive Validation](#)
- [17.11 Testing for Cyber Resilience Against TLS Downgrade Attacks](#)
- [17.12 Testing for Transparent TLS Redirection](#)
- [17.13 Testing That Random Number Generation \(RNG\) Is Sufficiently Unpredictable](#)
- [17.14 Testing If “Pinning” RNG Is Possible](#)
- [17.15 Test Worst-Case Results of Pinned RNG](#)
- [17.16 Scanning for Embedded Encryption Keys or Passphrases](#)
- [17.17 Scanning for Common Key Formats in the Clear](#)
- [17.18 “Following the Comments”](#)

10. HARDWARE V&V METHODS

This section covers V&V methods applicable to hardware such as microcontrollers or System on Chip (SoC) devices as listed below. For details of each method, see the corresponding descriptions in [Section 17 Collection of V&V Methods](#). For a complete list of all hardware V&V methods, see those tagged with “hardware” in [Section 15 Methods Hierarchy](#).

- [17.19 Testing for Vulnerability to Timing Attacks](#)
- [17.20 Testing for Vulnerability to Fault Injection Attacks](#)
- [17.21 Testing for PCR Extension Vulnerabilities via Serial Bus Interposer](#)

- [17.22 Testing for Random Number Generator Vulnerabilities to Undermine Cryptographic Operations on the Host via Serial Bus Interposer](#)
- [17.23 Testing for Host-Side Response Parsers \(Likely to Cause Memory Corruption Vulnerabilities\) via Serial Bus Interposer](#)
- [17.24 Testing for Host-Side Driver Authenticated Session Functionality, in Order to Capture Secrets \(Such as Private Keys\) That Are Transmitted over the Bus via Serial Bus Interposer](#)

V&V methods applicable specifically to environments using trust anchors (such as HPSE, Secure Hardware Extensions [SHE], Global platform SE, Trusted Computing Group [TCG], Trusted Platform Module [TPM], etc.) are covered in [Section 11 Trust Anchor Device V&V Methods](#).

11. TRUST ANCHOR DEVICE V&V METHODS

The following sections describe methods which are aligned with the use cases and common requirements related to confirming cybersecurity of devices that implement trust anchors (e.g., HPSE) described in SAE J3101.

11.1 Trust Anchors' Lifecycle Applicability

The methods described in this document and tagged with "J3101 derived" are applicable only to a small subset of the phases which SAE J3101 covers. Namely, the *Engineering Development*, *Component Integration*, and *Manufacture/production* phases.

SAE J3101 states that dedicated debug interfaces (e.g., Joint Test Action Group [JTAG], nexus) will be available during phases up to and including component integration; therefore, any methods for the later phase of *Manufacture/production* will not rely on dedicated debug interfaces for code execution.

11.2 Common Requirements

The methods described by this section and subsections of the document will focus on V&V of the *Common Requirements* section of SAE J3101. The methods enumeration tagged with "J3101 derived" was authored based on SAE J3101. But the methods are not exhaustive for trust anchors: Methods tagged with "hardware" are also applicable to confirming cybersecurity of the trust anchor devices (e.g., HPSE) since they are more general hardware V&V methods, e.g., [17.67 Side Channel Attack Protection](#).

Note that the device (e.g., HPSE) must have Built-In Self-Test (BIST) functionality as per SAE J3101. This is a manifest behavior: whether or not the device successfully boots. It can be leveraged as confirmation of success in tests. The authors will make use of the BIST functionality in the enumeration of methods which follows; however, SAE J3101 does allow the device to enable some of their functionality before the BIST is fully complete. Thus, not all methods will have the BIST confirmation applicable.

A further note on nomenclature: In what follows, the authors refer to *private key material*, whereas SAE J3101 describes the same objects as *private asymmetric keys and shared secrets*.

11.2.1 Key Protection/Management

Cryptographic Key Management is recommended as a means to manage access to networks and/or system management and maintenance. Keys can also be useful in distinguishing user authorizations for limiting a user's scope of control or influence upon the network or system in question and defining levels of user control. Keys can also be deployed to protect and/or anonymize private user data from exposure by the system, based on user authorization level and policy. Keys are also recommended for enabling and protecting the field servicing of systems or components and should support authorized secure replacement of ECUs in the field, Over-The-Air (OTA) or field firmware updates, and/or other components critical to network integrity and cybersecurity.

Key creation and management methods should be tested so as to be in conformance with accepted best practices; at the time of the authoring of this document, there are forthcoming best practices from SAE which will be referenced here in later revisions of this document.

A majority of the methods enumerated in these sections of the document focus on the *Key Protection* specifications of SAE J3101. This is because, in the words of SAE J3101, “The Keystore is more fundamentally strictly tied to the cryptographic function of the Hardware Protected Security Environment,” and many of the other functions of these devices (e.g., HPSE), as specified by the standard, are built on-top-of their cryptographic function.

For details about any of the following V&V methods, see their corresponding descriptions in [Section 17 Collection of V&V Methods](#).

- [17.25 Use-Limit Enforcement](#)
- [17.26 Using Key-Export, Test That Default Private Key Material Is Dissimilar](#)
- [17.27 Test That Keys Generated on Multiple Trust Anchor Devices Are Dissimilar](#)
- [17.28 Test That the Memory Space of a Co-Resident Processor Contains No Private Keying Material](#)
- [17.29 Test Any External Storage for Private Key Material](#)

11.2.2 Cryptographic Algorithms and Protocols

The methods enumerated here are derived from the *Cryptographic Algorithms and Protocols* specifications of SAE J3101.

For details about any of the following V&V methods, see their corresponding descriptions in [Section 17 Collection of V&V Methods](#).

- [17.30 Confirm Correct Hardware Module Implementation](#)
- [17.31 Confirm Correct Algorithm Implementation](#)
- [17.32 Confirm Correct Algorithm Uses](#)
- [17.33 Confirm Absence of Private Key in All Memory of Devices](#)
- [17.34 Confirm That Public Keys Cannot Be Substituted or Tampered](#)
- [17.35 Confirm That Cryptographic Operations Cannot Be Performed with Removed Keys](#)
- [17.36 Fuzz Test All Output for Any Remnants of Cleartexts](#)

11.2.3 Random Number Generator

The methods enumerated here are derived from the *Random Number Generator* specifications of SAE J3101.

For details about any of the following V&V methods, see their corresponding descriptions in [Section 17 Collection of V&V Methods](#).

- [17.37 Entropy Tests](#)

11.2.3.1 Functional and Performance Testing of Primitives

The correct operation and performance of all the cryptographic primitives that underly the RNG must be assured. Assurance for these should be obtained by the same means as for other cryptographic algorithms and protocols – see [11.2.2 Cryptographic Algorithms and Protocols](#) for methods to confirm those.

For details about any of the following V&V methods, see their corresponding descriptions in [Section 17 Collection of V&V Methods](#).

- [17.38 Ensure No Common Seeds](#)

11.2.4 Secure Nonvolatile Data

The methods enumerated here are derived from the *Secure Nonvolatile Data* specifications of SAE J3101.

For details about any of the following V&V methods, see their corresponding descriptions in [Section 17 Collection of V&V Methods](#).

- [17.39 Test Integrity Verification on Any External Storage Medium](#)
- [17.40 Test Correct Operation of Integrity Protection Mechanisms](#)
- [17.41 Test Any External Storage for Cleartexts](#)

11.2.5 Cryptographic Algorithm Agility

The methods enumerated here are derived from the *Cryptographic Algorithm Agility* specifications of SAE J3101.

For details about any of the following V&V methods, see their corresponding descriptions in [Section 17 Collection of V&V Methods](#).

- [17.42 Test That a Now-Deprecated Algorithm Cannot Be Used After a Firmware Update](#)
- [17.43 Test That Secure Object Re-Provisioning Mechanism Cannot Modify Firmware](#)
- [17.44 Test That Unsigned Code Cannot Be Executed](#)
- [17.45 Test That Tampering of the Fallback Firmware Is Prevented](#)

11.2.6 Interface Control

The methods enumerated here are derived from the *Interface Control* specifications of SAE J3101.

For details about any of the following V&V methods, see their corresponding descriptions in [Section 17 Collection of V&V Methods](#).

- [17.46 Test That JTAG Interface Is Disabled in Production](#)
- [17.47 JTAG Debug Interface Unlock Testing](#)
- [17.48 Test That the Default Passwords for Policy Changes Are Not Identical on All Devices](#)
- [17.49 Test That Authentication Is Required to Erase Private Key Material](#)

- [17.50 Test That Fuzzing Commands Cause No Leak of Private Key Material](#)
- [17.51 Test to Confirm Faulty Parameters in Requests Does Not Trigger Leak of Keys](#)
- [17.52 Test That Device Privileges Are Reduced in Successive Lifecycle Phases](#)
- [17.53 Test If Reverting to a Previous Lifecycle Phase Is Possible](#)

11.2.7 Secure Execution Environment

The V&V methods enumerated here are derived from the *Secure Execution Environment* section of SAE J3101. These *hardware* methods should apply to any detailed V&V plans being developed for systems or modules which have cybersecurity requirements dictating the separation of a hardware-backed, higher privilege domain from a normal domain.

In addition to the methods captured in this section, the Secure Execution Environment should also be confirmed as per other groups of methods in this document as applicable (e.g., secure boot, side channel attack protections).

For details about any of the following V&V methods, see their corresponding descriptions in [Section 17 Collection of V&V Methods](#).

- [17.54 Test That Debugging Is Not Possible from Normal Mode](#)
- [17.55 Test That Normal Mode Storage Contains No Communication Artifacts](#)
- [17.56 Test That Physical Access Does Not Yield Protected Mode Storage Access](#)
- [17.57 Test That Secure Execution Environment Sandboxing Is Enforced](#)
- [17.58 Test That Normal Mode \(Volatile\) Memory Contains No Cleartexts](#)

11.2.8 Self-Test

The test methods enumerated here are derived from the *Self-Test* section of SAE J3101. These *hardware* methods should apply to any detailed V&V plans being developed for systems or modules which include self-test requirements.

For details about any of the following V&V methods, see their corresponding descriptions in [Section 17 Collection of V&V Methods](#).

- [17.59 Test That Self-Test Failure Results in Transition to Failure Mode](#)
- [17.60 Test That Transition to Initialization State Reverts Limitations of Failure Mode](#)
- [17.61 Test That Failure of Memory Self-Tests Result in Transition to Failure Mode](#)
- [17.62 Test That Failure of Integrity Self-Tests Result in Transition to Failure Mode](#)
- [17.63 Test That Integrity Self-Tests Are Executed at All Power-on Transitions \(Including Return from Quiescent Power Modes\)](#)

- [*17.64 Test That Failure of Cryptographic Known Answer Self-Tests Result in Transition to Failure Mode*](#)
- [*17.65 Test That Failure of Cryptographic Algorithm Self-Tests Results in the Given Algorithm Being Unavailable in Failure Mode*](#)
- [*17.66 Test That Failure of Self-Tests in a Disabled Feature Does Not Result in Failure Mode*](#)
- [*17.67 Side Channel Attack Protection*](#)

11.3 Primary Use Cases

The V&V methods enumerated by the following sections of the document will focus on validating the specifications of the *Primary Use Cases* section of SAE J3101.

11.3.1 Authenticated Boot

For details about any of the following V&V methods, see their corresponding descriptions in [*Section 17 Collection of V&V Methods*](#).

- [*17.68 Test for Authenticated Boot*](#)

11.3.2 Authenticated Update

For details about any of the following V&V methods, see their corresponding descriptions in [*Section 17 Collection of V&V Methods*](#).

- [*17.69 Test That Tampered Trust Anchor Device Updates Are Rejected*](#)

11.3.3 Secure In-Vehicle Messaging

For details about any of the following V&V methods, see their corresponding descriptions in [*Section 17 Collection of V&V Methods*](#).

- [*17.70 Test Authentication of Messages within the Vehicle*](#)

11.3.4 Access Mechanisms

For details about any of the following V&V methods, see their corresponding descriptions in [*Section 17 Collection of V&V Methods*](#).

- [*17.35 Confirm That Cryptographic Operations Cannot Be Performed with Removed Keys*](#)
- [*17.49 Test That Authentication Is Required to Erase Private Key Material*](#)
- [*17.25 Use-Limit Enforcement*](#)
- [*17.43 Test That Secure Object Re-Provisioning Mechanism Cannot Modify Firmware*](#)
- [*17.47 JTAG Debug Interface Unlock Testing*](#)
- [*17.54 Test That Debugging Is Not Possible from Normal Mode*](#)
- [*17.57 Test That Secure Execution Environment Sandboxing Is Enforced*](#)

11.3.5 Secure Storage

For details about any of the following V&V methods, see their corresponding descriptions in [Section 17 Collection of V&V Methods](#).

- [17.39 Test Integrity Verification on Any External Storage Medium](#)
- [17.41 Test Any External Storage for Cleartexts](#)
- [17.71 Testing Secure Erasure](#).

11.4 Application Use Cases

The V&V methods enumerated by the following sections of the document will focus on validating the specifications of the *Application Use Cases* section of SAE J3101.

11.4.1 Intellectual Property Protection

There are no methods in this document which clearly confirm intellectual property protection; however, some methods in [11.3.5 Secure Storage](#) should also support this.

11.4.2 Secure Diagnosis at the ECU Level

For details about any of the following V&V methods, see their corresponding descriptions in [Section 17 Collection of V&V Methods](#).

- [17.72 Test All ECU Diagnostics Memory Views for Private Key Material](#)
- [17.73 Test All ECU Diagnostics Memory Views for Remnants of Cleartexts](#)

11.4.3 Secure Logging

There are no methods in this document which clearly confirm secure logging; however, some methods in [11.3.5 Secure Storage](#) should also support this.

12. RADIO FREQUENCY COMMUNICATIONS V&V METHODS

12.1 Radio Frequency Communications Cybersecurity Risks and Attack Surfaces

Wireless Interfaces present the most vulnerable attack surfaces on vehicles. Attacks via these interfaces are also the least detectable avenues of attack available to the hacker.

Attacks may be initiated remotely and without any physical access inside the vehicle, without leaving physical evidence of such attack having been mounted.

Confirming the cybersecurity of the complete vehicle individual Electronic Control Unit (ECU), Telematics Control Unit (TCU), or Hub/gateway against such attacks is critical to ensure the effectiveness of defenses (e.g., Hardware Secure Gateways, Trust Anchors Firewalls, Intrusion Detection Systems).

These risks are present via the following common **Radio Frequency (RF) Attack Surfaces**:

- a. Long range wireless communications systems, which are becoming ubiquitous in cars and trucks
 1. Telematics delivered over cellular radio (2G/3G/4G/5G)
 2. V2X services delivered over Dedicated Short-Range Communications (DSRC) or C-V2XBoth of these offer Internet Protocol access, opening up the possibility of a full range of Information Technology (IT) industry type vulnerabilities being exploited.
- b. Shorter range wireless interfaces, also prevalent, largely for infotainment, also offer opportunities for Internet Protocol (IP) attacks from outside the vehicle, but with a need for physical proximity, e.g.,
 1. Wi-Fi
 2. Bluetooth
- c. Additional interfaces which enable attacks over long range to the download of malware onto the vehicle's Infotainment system include:
 1. Satellite Radio
 2. Broadcast Radio (AM/FM/HD Radio/Side Channel Communications)
- d. Lower data-rate, non-IP, short range interfaces have potential to disrupt the functioning of individual ECUs
 1. Near Field Communications/Short Distance Radio (with infrastructure)
 2. RF Keyless Entry features
 3. Tire Pressure Monitoring (TPMS) sensor communications
- e. Additionally, vehicles are reliant on other services providing using RF technology, which may be vulnerable, particularly to spoofing attacks
 1. Positioning data via Global Navigation Satellite System (GNSS) receivers
 2. Object detection and recognition via Radio Detection and Ranging (RADAR)

12.2 Radio Frequency Communications V&V Lifecycle Applicability

All methods described elsewhere in this document remain relevant for these attack surfaces – the external stimulus and monitoring of response will require the use specialized testing equipment and may be undertaken either “Over the Air” in a screened room or by direct conducted connection at relevant antenna ports if available.

The methods described here are applicable to Engineering Development, Component Integration, Vehicle Integration phases, plus firmware regression testing.

12.3 Confirming Common Radio Frequency Cybersecurity Requirements

The methods enumerated will focus on validating the vulnerability of the System Under Test to attacks as enumerated in the Radio Frequency Communications Cybersecurity risks section, as there is no other document to refer to.

For details about any of the following V&V methods, see their corresponding descriptions in [Section 17 Collection of V&V Methods](#).

- [17.74 RF Jamming](#)
- [17.75 Simple RF Emulation](#)

12.4 Penetration Test via Radio Frequency Network Emulation

For each vulnerable wireless interface identified requiring more complex interaction (e.g., requiring a response from the ECU to proceed to establish communication), it is prudent to use Penetration Testing.

- a. The relevant ECU should be connected to IP Penetration Test tools via an emulator for the relevant RF interface, e.g.,
 1. For the Telematics Unit (TCU), a Cellular Network Emulator should be used to carry, via the RF antenna port
 - i. Testing at extremes of PHY parameter specifications, e.g., signal strength, clock rates, etc.
 - ii. Invalid or malformed Cellular protocols
 - iii. IP attack traffic over the wireless data link
 - a) Techniques such as port scanning, fuzzing, and checking for known vulnerabilities should be used
 - iv. Additionally, the TCU connection into the vehicle's internal network via Controller Area Network (CAN) or Ethernet should be checked for unexpected traffic directed to other ECUs
 2. For the Infotainment Hub, connection via a controlled Wi-Fi Access Point and/or Bluetooth device should be used
 - i. Similar techniques may be applied via this connection method

In each case, a response from the TCU will be an indication that connection has been made.

For details about any of the following V&V methods, see their corresponding descriptions in [Section 17 Collection of V&V Methods](#).

- [17.76 Test to Establish Whether TCU Can Be Spoofed into an Illegal IP Connection](#)
- [17.77 Test to Establish Whether TCU Can Be Made to Communicate to Other ECUs](#)
- [17.78 Rogue Tower Analysis](#)
- [17.79 SIM Card Extraction](#)
- [17.80 Bluetooth Service Access Control Analysis](#)

13. SYSTEM V&V METHODS

This section addresses methods where the target of the test is the integrated system. System may refer to an integrated vehicle or some other product within the vehicle supply chain where hardware and software are integrated to create the product. The integrated system instantiation will differ depending upon the lifecycle phase of the system, and thus, the applicable methods will need to be tailored. Generally, system level V&V can be categorized as either verifying compliance with specified requirements or validating cybersecurity of the system.