Technical Report

ISO/SAE TR 8477

Road vehicles — Cybersecurity verification and validation

Véhicules routiers — Vérification et validation de la cybersécurité

Sample Document

get full document from standards.iteh.ai

First edition
2026-11

Reference number
ISO/SAE TR 8477:2026(en)

© ISO/SAE International 2026

Sample Document

get full document from standards.iteh.ai



COPYRIGHT PROTECTED DOCUMENT

© ISO/SAE International 2026

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced, or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO or SAE International at the respective address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11

Email: copyright@iso.org
Website: www.iso.org

SAE International
400 Commonwealth Dr.
Warrendale, PA, USA 15096
Phone: 877-606-7323 (inside USA and Canada)
Phone: +1 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
Website: www.sae.org

Published in Switzerland by ISO, published in the USA by SAE International

ISO/SAE TR 8477:2026 • https://standards.iteh.ai/catalog/standards/iso/5cff4384-c050-4563-ba5f-ed8953e13c5d/iso-sae-tr-8477-2026

Contents

Page

Foreword ..... **iv**
Introduction ..... **v**
1 Scope **1**
2 Normative references **1**
3 Terms, definitions and abbreviated terms **1**
3.1 Terms and definitions 1
3.2 Abbreviated terms 1
4 Verification and validation (V&V) in the context of cybersecurity **1**
4.1 General 1
4.2 Conceptual cybersecurity requirements 3
4.3 Difference between verification and validation (V&V) 3
4.3.1 Relation to the levels of the requirements hierarchy 3
4.3.2 Relation to layers of the architecture 4
4.4 Logical sequence of activities 6
4.5 Functional and non-functional properties 7
4.6 Relation with TARA 7
4.7 Impact of refinement on V&V work products 8
4.8 Assumptions 9
4.9 Relation to types of development 10
4.9.1 General 10
4.9.2 Use of an existing component 10
4.9.3 Out-of-context development 10
4.9.4 Component off-the-shelf 10
5 Verification and validation (V&V) strategy and planning **11**
5.1 Strategy 11
5.2 Planning 11
6 Method Groups **13**
6.1 General 13
6.2 Review 13
6.3 Analysis 13
6.4 Formal method 13
6.5 Code analysis 14
6.6 Functional testing 14
6.7 Vulnerability scanning 15
6.8 Fuzz testing 15
6.9 Stress testing 16
6.10 Fault injection 16
6.11 Penetration testing 17
6.12 Cryptographic testing 17
7 Examples of applications of methods **18**
8 Verification and validation (V&V) reporting **21**
8.1 General 21
8.2 Instances of verification reporting 22
8.3 Instances of validation reporting 23
Annex A (informative) **Difference with cybersecurity assessment** **26**
Bibliography **28**

Sample Document
Get full document from standards.iteh.ai

© ISO/SAE International 2026 – All rights reserved

ISO/SAE TR 8477:2026 • https://standards.iteh.ai/catalog/standards/iso/5cff4384-c050-4563-ba5f-ed8953e13c5d/iso-sae-tr-8477-2026

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

SAE International is a global association of more than 128,000 engineers and related technical experts in the aerospace, automotive and commercial-vehicle industries. Standards from SAE International are used to advance mobility engineering throughout the world. The SAE Technical Standards Development Program is among the organization's primary provisions to those mobility industries it serves aerospace, automotive, and commercial vehicle. These works are authorized, revised, and maintained by the volunteer efforts of more than 9,000 engineers, and other qualified professionals from around the world. SAE subject matter experts act as individuals in the standards process, not as representatives of their organizations. Thus, SAE standards represent optimal technical content developed in a transparent, open, and collaborative process.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1 and the SAE Executive Standards Committee Policy. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

ISO and SAE draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and SAE take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and SAE had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO and SAE shall not be held responsible for identifying any or all such patent rights.

iTeh Standards (https://standards.iteh.ai) Document Preview
get full document from standards.iteh.ai

SAE Executive Standards Committee Rules provide that: “This document is published to advance the state of technical and engineering sciences. The use of this document 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.”

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was jointly prepared by Technical Committee ISO/TC 22, *Road Vehicles*, Subcommittee SC 32, *Electrical and electronic components and general system aspects,* and SAE Committee SAE TEVEES18A, *Vehicle Cybersecurity Systems Engineering Committee*.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html. Alternatively, to provide feedback on this document, please visit http://standards.sae.org/PRODCODE.

© ISO/SAE International 2026 – All rights reserved

ISO/SAE TR 8477:2026 • https://standards.iteh.ai/catalog/standards/iso/5cff4384-c050-4563-ba5f-ed8953e13c5d/iso-sae-tr-8477-2026

Introduction

This document elaborates on verification and validation (V&V) of the cybersecurity of items and components of road vehicles in accordance with ISO/SAE 21434 [1]. It provides considerations on:

— V&V strategy;

— methods that can be applied;

— distribution of activities between customer and supplier;

— logical sequence of activities.

The objectives are different between V&V; however, both can use identical or similar methods.

The choice of methods and the extent of the rigour with which they are applied are part of a project- and organization-specific strategy. This document focuses on strategy and does not prescribe methods.

V&V are part of development of an item or component and involve multiple activities, including repeating (e.g. iteration or feedback loop) or complementing activities.

Sample Document

get full document from standards.iteh.ai

© ISO/SAE International 2026 – All rights reserved

ISO/SAE TR 8477:2026 • https://standards.iteh.ai/catalog/standards/iso/5cff4384-c050-4563-ba5f-ed8953e13c5d/iso-sae-tr-8477-2026

Sample Document

get full document from standards.iteh.ai

Road vehicles — Cybersecurity verification and validation

1 Scope

This document provides considerations on the planning and execution of verification and validation (V&V) of the cybersecurity of items and components of road vehicles, in the context of ISO/SAE 21434 [1].

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/SAE 21434, *Road vehicles — Cybersecurity engineering*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/SAE 21434 apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

Sample Document
get full document from standards.iteh.ai

3.2 Abbreviated terms

CAN	controller area network
CS	cybersecurity
CVSS	common vulnerability scoring system
CWE	common weakness enumeration
E/E	electric / electronic
ECU	electronic control unit
PIN	personal identification number
TARA	threat analysis and risk assessment
V&V	verification and validation

4 Verification and validation (V&V) in the context of cybersecurity

4.1 General

This clause provides an overview of V&V in the context of cybersecurity, elaborating on ISO/SAE 21434 [1].

© ISO/SAE International 2026 – All rights reserved

ISO/SAE TR 8477:2026 • https://standards.iteh.ai/catalog/standards/iso/5cff4384-c050-4563-ba5f-ed8953e13c5d/iso-sae-tr-8477-2026

Verification in cybersecurity addresses whether the architecture and design of an item or component satisfy the cybersecurity requirements. In general, it answers the question “are we building the cybersecurity of the item or component right?” Verification results can be an input to validation.

Validation in cybersecurity addresses whether an item is appropriately and sufficiently cybersecure. In general, it answers the question “are we building the right item regarding cybersecurity?” Validation applies to the item integrated in the target vehicle, considering the interfaces of the item, its operational environment and threat scenarios.

See also IEC 60050-192:2015 [2], 192-01-17 and 192-01-18.

Figure 1 and Figure 2, respectively, provide examples of V&V activities. These figures are not intended to be exhaustive – not all relevant work products of ISO/SAE 21434:2021 [3] are included, nor are all relevant activities.

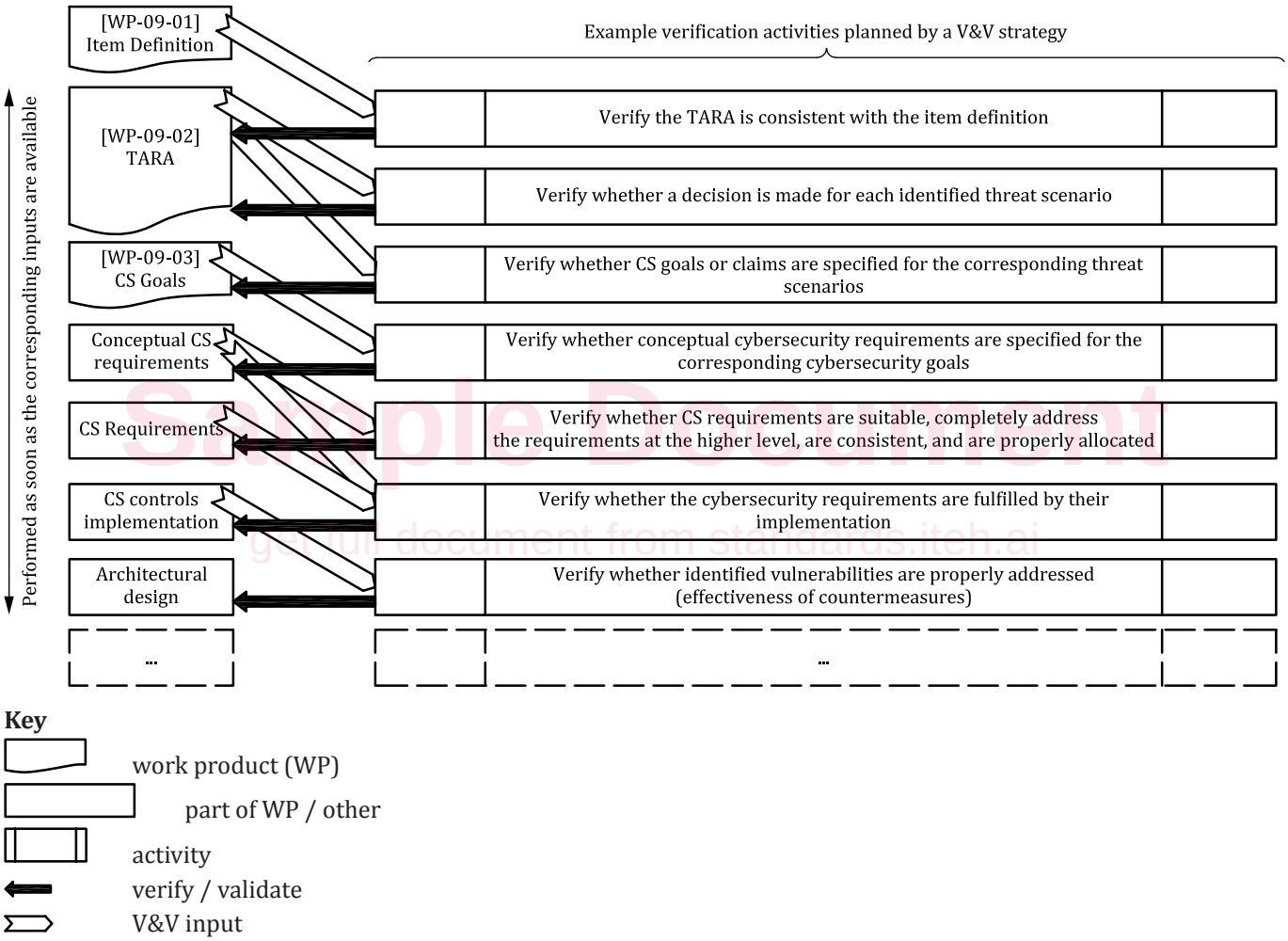


Figure 1 — Examples of verification activities

Sample Document
get full document from standards.iteh.ai

© ISO/SAE International 2026 – All rights reserved

ISO/SAE TR 8477:2026 • https://standards.iteh.ai/catalog/standards/iso/5cff4384-c050-4563-ba5f-ed8953e13c5d/iso-sae-tr-8477-2026

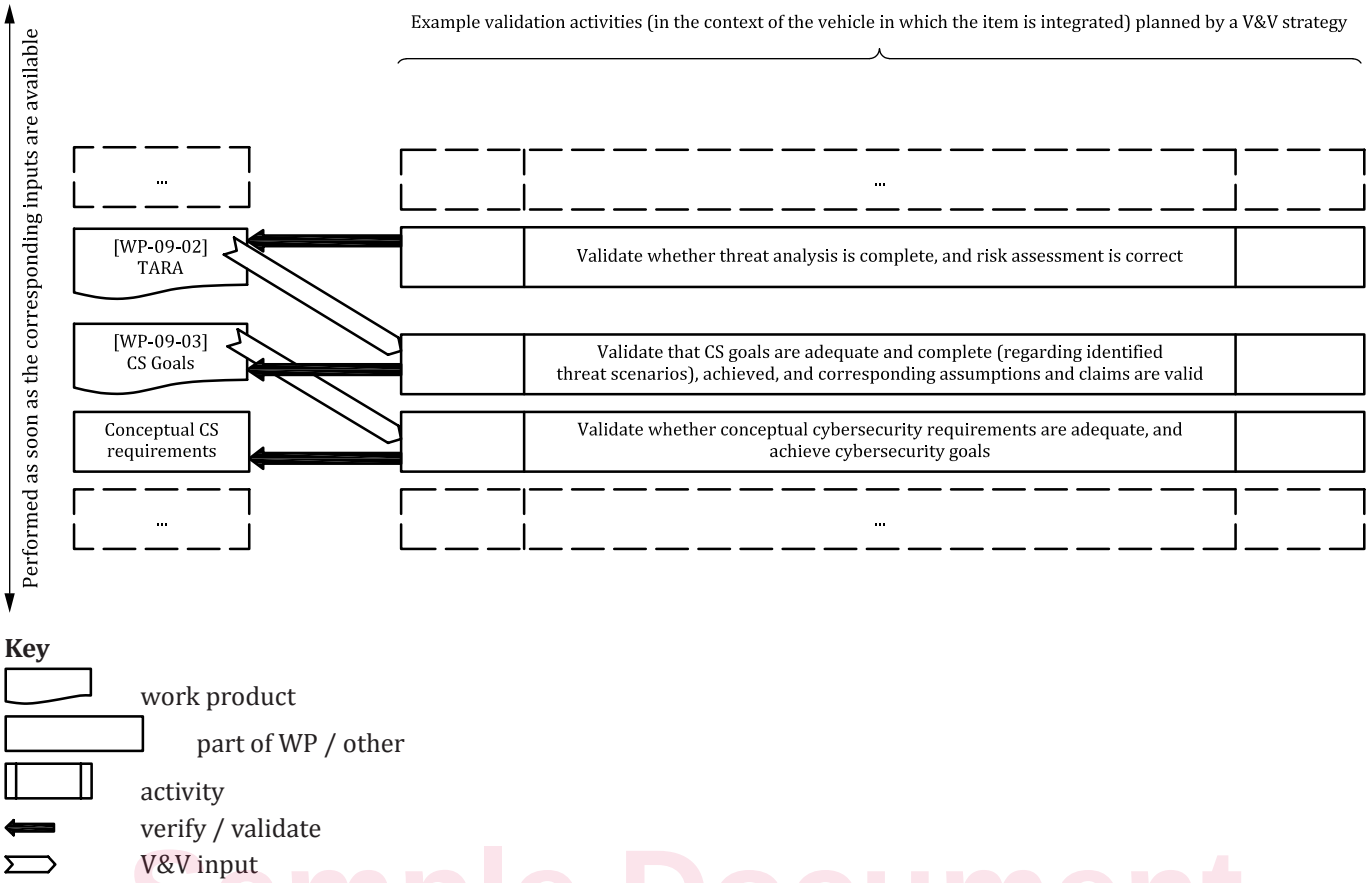


Figure 2 — Examples of validation activities

Sample Document

V&V activities can be performed by a customer, a supplier or other parties, according to the cybersecurity interface agreement. This agreement includes information exchange, such that each party is able to fulfil corresponding responsibilities.

V&V provide evidence that can be judged in a cybersecurity assessment, see Annex A.

4.2 Conceptual cybersecurity requirements

The term “conceptual cybersecurity requirement” – meaning “cybersecurity requirement directly derived from a cybersecurity goal” – is used in this document to facilitate elaborating validation. For reference, ISO/SAE 21434:2021 [3], 3.1.36, defines cybersecurity validation as confirmation of only the adequacy and achievement of the cybersecurity goals of the item, and effectiveness of cybersecurity controls in preventing or mitigating risk associated with threat scenarios.

The work product “cybersecurity concept” (see ISO/SAE 21434:2021 [3], 3.1.13) includes these conceptual cybersecurity requirements, as well as their allocation.

The work product “cybersecurity specification” (see ISO/SAE 21434:2021 [3], 3.1.21) includes the cybersecurity requirements associated with lower levels of the requirements hierarchy, as well as the corresponding architectural design.

4.3 Difference between verification and validation (V&V)

4.3.1 Relation to the levels of the requirements hierarchy

Verification relates to any level of the requirements hierarchy.

© ISO/SAE International 2026 – All rights reserved

ISO/SAE TR 8477:2026 • https://standards.iteh.ai/catalog/standards/iso/5cff4384-c050-4563-ba5f-ed8953e13c5d/iso-sae-tr-8477-2026