FINAL DRAFT

Publicly Available Specification

ISO/DPAS 8475

Road vehicles — Cybersecurity Assurance Levels (CAL) and Targeted Attack Feasibility (TAF)

Véhicules routiers - Niveaux d'assurance (CAL) et faisabilité des attaques ciblées (TAF) en matière de cybersécurité

ISO/TC **22**/SC **32**

Secretariat: **JISC**

Voting begins on:
2026-07-06

Voting terminates on:
2026-08-31

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

Reference number
ISO/DPAS 8475:2026(en)

© ISO 2026



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

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 ... 2

4 General ... **2**

5 CAL determination and assignment ... **3**
5.1 Objectives ... 3
5.2 Recommendations and permissions ... 3
5.2.1 CAL Determination ... 3
5.2.2 CAL Assignment ... 4

6 CAL usage and examples ... **4**
6.1 Objective ... 4
6.2 Recommendations and permissions ... 5
6.2.1 CAL usage ... 5

Annex A (informative) **Assignment of CAL to cybersecurity requirements** ... **6**

Annex B (informative) **Examples of scaling rigour** ... **10**

Annex C (informative) **The targeted attack feasibility (TAF) concept** ... **16**

Annex D (informative) **Example application of TAF with multiple cybersecurity controls** ... **20**

Bibliography ... **23**

© ISO 2026 – All rights reserved

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.

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.

© ISO 2026 – All rights reserved

Introduction

This document elaborates the cybersecurity assurance level (CAL) classification scheme introduced in ISO/SAE 21434 and introduces the targeted attack feasibility (TAF) concept.

The CAL classification scheme, as described in ISO/SAE 21434:2021, Annex E, is a measure of how rigorously the cybersecurity activities for the concept and development phases of an item or component are executed. The use of CAL provides a scheme to scale the rigour of the cybersecurity development activities. This can be communicated between customers and suppliers in a distributed development to highlight differences in the security assurance to be expected from items or components. It does not provide an absolute measure. It is not comparable between different customers or different suppliers.

CAL can also be used for out-of-context development according to ISO/SAE 21434:2021, 6.4.5 with appropriate communication between customer and supplier.

The TAF concept introduced in Annexes C and D describes the expected level of attack feasibility once cybersecurity controls are applied for a given item or component. The TAF concept gives flexibility to the organization that develops an item or component to specify and implement cybersecurity controls.

While ISO/SAE 21434 does not require use of either CAL or TAF, they can be used to streamline discussion and improve consistency between customers and suppliers.

Results from the requirements and recommendations in this document are incorporated into existing work products defined in ISO/SAE 21434.

© ISO 2026 – All rights reserved

Road vehicles — Cybersecurity Assurance Levels (CAL) and Targeted Attack Feasibility (TAF)

1 Scope

This document elaborates on the cybersecurity assurance level (CAL) classification scheme and introduces the targeted attack feasibility (TAF) concept, within the context of cybersecurity engineering for road vehicles as specified in ISO/SAE 21434.

This document describes the concepts of CAL and TAF. It provides requirements and recommendations to determine and use CAL as applied to cybersecurity engineering of an item or component.

2 Normative references

The following document is referred to in the text in such a way that some or all of its 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 21434:2021, *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 21434:2021 and the following apply.

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

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

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

3.1.1
cybersecurity assurance level
CAL
rigour (3.1.3) during the concept and product development phases for an item or component

Note 1 to entry: CAL does not address the selection of cybersecurity controls.

3.1.2
targeted attack feasibility
TAF
required attack feasibility rating for an item or component after cybersecurity controls are applied

3.1.3
rigour
depth (3.1.4) and *breadth* (3.1.5) in performing cybersecurity activities that support justifiable confidence in the achieved results

3.1.4
depth
detail at which cybersecurity activities are performed

© ISO 2026 – All rights reserved

3.1.5
breadth
range of cybersecurity activities performed

3.1.6
static factor
risk-related factor that is expected not to change during the development of an item or component

3.2 Abbreviated terms

CAN controller area network

ECU electronic control unit

4 General

This document describes the cybersecurity assurance level (CAL) classification scheme. CAL is used in the concept and product development phases to specify and communicate a set of cybersecurity activities, in terms of rigour, to provide justifiable confidence that the cybersecurity engineering of an item or component is appropriate.

CAL is an attribute of a cybersecurity goal. CAL provides a common language for communicating the required rigour of cybersecurity activities between organizations.

The determination, assignment and use of CAL is illustrated in Figure 1. A CAL is determined, using a combination of static factors (see 5.2.1). The CAL is then assigned as an attribute of a cybersecurity goal and inherited by the cybersecurity requirements specified from that cybersecurity goal (5.2.2). Finally, the cybersecurity activities related to the cybersecurity requirements are performed at the rigour set by the CAL (6.2 and Annex B).

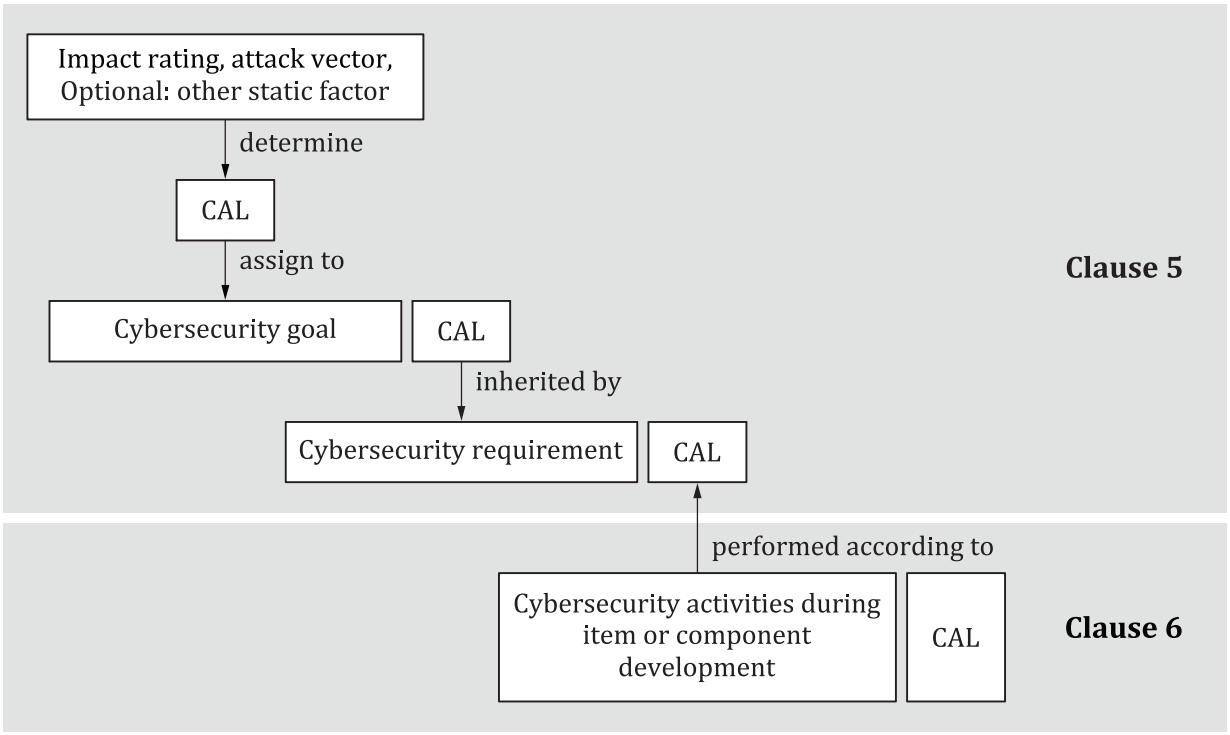


Figure 1 — Determination, assignment and use of CAL

A CAL is determined during the concept phase. CAL remains fixed throughout concept and development phases to provide a consistent level of assurance, unless the basis for determining CAL changes (e.g. a change

© ISO 2026 – All rights reserved