IEC 62541-2

Edition 1.0 2026-02

INTERNATIONAL STANDARD

NORME INTERNATIONALE

OPC unified architecture – Part 2: Security Model

Architecture unifiée OPC - Partie 2: Modèle de sécurité

ICS 25.040

ISBN 978-2-8327-1035-7

IEC 62541-2:2026-02(en-fr)



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2026 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Secretariat
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, …). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch
Discover our powerful search engine and read freely all the publications previews, graphical symbols and the glossary. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 500 terminological entries in English and French, with equivalent terms in 25 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

A propos de l'IEC
La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC
Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Recherche de publications IEC - webstore.iec.ch/advsearchform
La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études, …). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

Service Clients - webstore.iec.ch/csc
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch
Découvrez notre puissant moteur de recherche et consultez gratuitement tous les aperçus des publications, symboles graphiques et le glossaire. Avec un abonnement, vous aurez toujours accès à un contenu à jour adapté à vos besoins.

Electropedia - www.electropedia.org
Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 500 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 25 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

CONTENTS

FOREWORD 4
1 Scope 6
2 Normative references 6
3 Terms, definitions, abbreviated terms and conventions 6
3.1 Terms and definitions 6
3.2 Abbreviated terms 11
3.3 Conventions for security model figures 12
4 OPC UA security architecture 12
4.1 OPC UA security environment 12
4.2 Security objectives 13
4.2.1 Overview 13
4.2.2 Authentication 14
4.2.3 Authorization 14
4.2.4 Confidentiality 14
4.2.5 Integrity 14
4.2.6 Non-Repudiation 14
4.2.7 Auditability 14
4.2.8 Availability 14
4.3 Security threats to OPC UA systems 14
4.3.1 Overview 14
4.3.2 Denial of Service 15
4.3.3 Eavesdropping 16
4.3.4 Message spoofing 16
4.3.5 Message alteration 16
4.3.6 Message replay 17
4.3.7 Malformed Messages 17
4.3.8 Server profiling 17
4.3.9 Session hijacking 17
4.3.10 Rogue Server 17
4.3.11 Rogue Publisher 18
4.3.12 Compromising user credentials 18
4.3.13 Repudiation 18
4.4 OPC UA relationship to site security 18
4.5 OPC UA security architecture 19
4.5.1 Overview 19
4.5.2 Client / Server 20
4.5.3 Publish-Subscribe 21
4.6 SecurityPolicies 22
4.7 Security Profiles 23
4.8 Security Mode settings 23
4.9 User Authentication 23
4.10 Application Authentication 24
4.11 User Authorization 24
4.12 Roles 24
4.13 OPC UA security related Services 25
4.14 Auditing 26
4.14.1 General 26

4.14.2 Single Client and Server 26
4.14.3 Aggregating Server 27
4.14.4 Aggregation through a non-auditing Server 28
4.14.5 Aggregating Server with service distribution 28
5 Security reconciliation 29
5.1 Reconciliation of threats with OPC UA security mechanisms 29
5.1.1 Overview 29
5.1.2 Denial of Service 30
5.1.3 Eavesdropping 31
5.1.4 Message spoofing 31
5.1.5 Message alteration 32
5.1.6 Message replay 32
5.1.7 Malformed Messages 32
5.1.8 Server profiling 32
5.1.9 Session hijacking 32
5.1.10 Rogue Server or Publisher 33
5.1.11 Compromising user credentials 33
5.1.12 Repudiation 33
5.2 Reconciliation of objectives with OPC UA security mechanisms 33
5.2.1 Overview 33
5.2.2 Application Authentication 33
5.2.3 User Authentication 34
5.2.4 Authorization 34
5.2.5 Confidentiality 34
5.2.6 Integrity 34
5.2.7 Auditability 35
5.2.8 Availability 35
6 Implementation and deployment considerations 35
6.1 Overview 35
6.2 Appropriate timeouts 35
6.3 Strict Message processing 35
6.4 Random number generation 36
6.5 Special and reserved packets 36
6.6 Rate limiting and flow control 36
6.7 Administrative access 36
6.8 Cryptographic Keys 37
6.9 Alarm related guidance 37
6.10 Program access 37
6.11 Audit event management 38
6.12 OAuth2, JWT and User roles 38
6.13 HTTPS, TLS & Websockets 38
6.14 Reverse connect 38
6.15 Passwords 39
6.16 Additional Security considerations 39
7 Unsecured Services 39
7.1 Overview 39
7.2 Multi Cast Discovery 39
7.3 Global Discovery Server Security 39
7.3.1 Overview 39

7.3.2 Rogue GDS 40
7.3.3 Threats against a GDS 40
7.3.4 Certificate management threats 40
8 Certificate management 41
8.1 Overview 41
8.2 Self signed certificate management 41
8.3 CA Signed Certificate management 42
8.4 GDS Certificate Management 43
8.4.1 Overview 43
8.4.2 Developers Certificate management 44
Annex A (informative) Mapping to IEC 62443-4-2 46
Bibliography 59

Figure 1 – OPC UA network example 13
Figure 2 – OPC UA security architecture – Client / Server 19
Figure 3 – OPC UA security architecture- Publisher - Subscriber 20
Figure 4 – Role overview 24
Figure 5 – Simple Servers 26
Figure 6 – Aggregating Servers 27
Figure 7 – Aggregation with a non-auditing Server 28
Figure 8 – Aggregating Server with service distribution 29
Figure 9 – Manual Certificate handling 42
Figure 10 – CA Certificate handling 43
Figure 11 – Certificate handling 44

Table 1 – Security Reconciliation Threats Summary 30
Table A.1 – IEC 62443 Mapping FR 1 Identification and authentication control 47
Table A.2 – IEC 62443 mapping FR 2 Use control 50
Table A.3 – IEC 62443 Mapping FR 3 System integrity 52
Table A.4 – IEC 62443 Mapping FR 4 Data confidentiality 55
Table A.5 – IEC 62443 Mapping FR 5 Restricted data flow 56
Table A.6 – IEC 62443 Mapping FR 6 Timely response to events 56
Table A.7 – IEC 62443 Mapping FR 7 Resource availability 57

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

OPC unified architecture - Part 2: Security Model

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) IEC draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC takes 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, IEC 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 https://patents.iec.ch. IEC shall not be held responsible for identifying any or all such patent rights.

IEC 62541-2 has been prepared by subcommittee 65E: Devices and integration in enterprise systems, of IEC technical committee 65: Industrial-process measurement, control, and automation. It is an International Standard.

This edition cancels and replaces the third edition of IEC TR 62541-2, published in 2020.This edition constitutes a technical revision.

The text of this International Standard is based on the following documents:

Draft	Report on voting
65E/1201/FDIS	65E/1206/RVD

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications.

Throughout this document and the other Parts of the series, certain document conventions are used:

Italics are used to denote a defined term or definition that appears in the "Terms and definitions" clause in one of the parts of the series.

Italics are also used to denote the name of a service input or output parameter or the name of a structure or element of a structure that are usually defined in tables.

The *italicized terms* and *names* are also often written in camel-case (the practice of writing compound words or phrases in which the elements are joined without spaces, with each element's initial letter capitalized within the compound). For example, the defined term is *AddressSpace* instead of Address Space. This makes it easier to understand that there is a single definition for *AddressSpace*, not separate definitions for Address and Space.

A list of all parts in the IEC 62541 series, published under the general title *OPC Unified Architecture*, can be found on the IEC website.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

– reconfirmed,
– withdrawn, or
– revised.

1 Scope

This part of IEC 62541 describes the OPC Unified Architecture (OPC UA) security model. It describes the security threats of the physical, hardware, and software environments in which OPC UA is expected to run. It describes how OPC UA relies upon other standards for security. It provides definition of common security terms that are used in this and other parts of the IEC 62541 series. It gives an overview and concept of the security features that are specified in other parts of the series. It references services, mappings, and *Profile*s that are specified normatively in other parts of the 62541 series. It provides suggestions or best practice guidelines on implementing security. Any seeming ambiguity between this document and one of the other normative parts does not remove or reduce the requirement specified in the other normative part.

There are many different aspects of security that are addressed when developing applications. However, since OPC UA specifies a communication protocol, the focus is on securing the data exchanged between applications. This does not mean that an application developer can ignore the other aspects of security like protecting persistent data against tampering. It is important that the developers look into all aspects of security and decide how they can be addressed in the application. Common security features for industrial Controls are defined in IEC 62443-4-2 and OPC UA defined a relationship to them in Annex A.

This document is directed to readers who will develop OPC UA applications. It is also for end Users that wish to understand the various security features and functionality provided by OPC UA. It also offers some recommendations that can be applied when deploying systems. These recommendations are generic in nature since the details would depend on the actual implementation of the *OPC UA* applications and the choices made for the site security.

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.

IEC 62541-1, *OPC Unified Architecture - Part 1: Overview and Concepts*

3 Terms, definitions, abbreviated terms and conventions

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 62541-1 and the following apply.

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

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

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

3.1.1
AccessRestriction
limit on the circumstances under which an operation, such as a read, write or a call, can be performed on a *Node*

Note 1 to entry: Operations can only be performed on a *Node* if the *Client* has the necessary *Permissions* and has satisfied all of the *AccessRestrictions*.