



BSI Standards Publication

OPC unified architecture

Part 2: Security Model

National foreword

This Published Document is the UK implementation of CLC IEC/TR 62541-2:2021. It is identical to IEC TR 62541-2:2020. It supersedes PD IEC TR 62541-2:2020 and PD CLC/TR 62541-2:2010, which are withdrawn.

The UK participation in its preparation was entrusted to Technical Committee GEL/65/3, Industrial communications: process measurement and control, including fieldbus.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

This publication is not to be regarded as a British Standard.

© The British Standards Institution 2021
Published by BSI Standards Limited 2021

ISBN 978 0 539 18632 1

ICS 25.040.40; 35.100.01

Compliance with a Published Document cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 December 2020.

Amendments/corrigenda issued since publication

Date	Text affected
31 August 2021	This corrigendum renumbers PD IEC TR 62541-2:2020 as PD CLC IEC/TR 62541-2:2021

TECHNICAL REPORT
RAPPORT TECHNIQUE
TECHNISCHER BERICHT

CLC IEC/TR 62541-2

July 2021

ICS 25.040.40; 35.100.01

Supersedes CLC/TR 62541-2:2010

English Version

**OPC unified architecture - Part 2: Security Model
(IEC/TR 62541-2:2020)**

Architecture unifiée OPC - Partie 2: Modèle de sécurité
(IEC/TR 62541-2:2020)

OPC Unified Architecture - Teil 2: Modell für die IT-
Sicherheit
(IEC/TR 62541-2:2020)

This Technical Report was approved by CENELEC on 2021-07-05.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.



European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

European foreword

This document (CLC IEC/TR 62541-2:2021) consists of the text of IEC/TR 62541-2:2020, prepared by SC 65E "Devices and integration in enterprise systems" of IEC/TC 65 "Industrial-process measurement, control and automation".

This document supersedes CLC/TR 62541-2:2010.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC shall not be held responsible for identifying any or all such patent rights.

Any feedback and questions on this document should be directed to the users' national committee. A complete listing of these bodies can be found on the CENELEC website.

Endorsement notice

The text of the International Technical Report IEC/TR 62541-2:2020 was approved by CENELEC as a European Technical Report without any modification.

CONTENTS

FOREWORD	5
1 Scope	7
2 Normative references	7
3 Terms, definitions, and abbreviated terms	8
3.1 Terms and definitions	8
3.2 Abbreviated terms	13
4 OPC UA security architecture	13
4.1 OPC UA security environment	13
4.2 Security objectives	14
4.2.1 Overview	14
4.2.2 Authentication	15
4.2.3 Authorization	15
4.2.4 Confidentiality	15
4.2.5 Integrity	15
4.2.6 Non-Repudiation	15
4.2.7 Auditability	15
4.2.8 Availability	15
4.3 Security threats to OPC UA systems	15
4.3.1 Overview	15
4.3.2 Denial of Service	16
4.3.3 Eavesdropping	17
4.3.4 Message spoofing	17
4.3.5 Message alteration	17
4.3.6 Message replay	17
4.3.7 Malformed Messages	18
4.3.8 Server profiling	18
4.3.9 Session hijacking	18
4.3.10 Rogue Server	18
4.3.11 Rogue Publisher	18
4.3.12 Compromising user credentials	19
4.3.13 Repudiation	19
4.4 OPC UA relationship to site security	19
4.5 OPC UA security architecture	20
4.5.1 Overview	20
4.5.2 Client / Server	21
4.5.3 Publish-Subscribe	22
4.6 SecurityPolicies	23
4.7 Security Profiles	24
4.8 Security Mode Settings	24
4.9 User Authentication	24
4.10 Application Authentication	24
4.11 User Authorization	25
4.12 Roles	25
4.13 OPC UA security related Services	25
4.14 Auditing	26
4.14.1 General	26

4.14.2	Single Client and Server	27
4.14.3	Aggregating Server	28
4.14.4	Aggregation through a non-auditing Server	28
4.14.5	Aggregating Server with service distribution	29
5	Security reconciliation	30
5.1	Reconciliation of threats with OPC UA security mechanisms	30
5.1.1	Overview	30
5.1.2	Denial of Service	31
5.1.3	Eavesdropping	32
5.1.4	Message spoofing	32
5.1.5	Message alteration	33
5.1.6	Message replay	33
5.1.7	Malformed Messages	33
5.1.8	Server profiling	33
5.1.9	Session hijacking	33
5.1.10	Rogue Server or Publisher	34
5.1.11	Compromising user credentials	34
5.1.12	Repudiation	34
5.2	Reconciliation of objectives with OPC UA security mechanisms	34
5.2.1	Overview	34
5.2.2	Application Authentication	34
5.2.3	User Authentication	35
5.2.4	Authorization	35
5.2.5	Confidentiality	35
5.2.6	Integrity	35
5.2.7	Auditability	35
5.2.8	Availability	36
6	Implementation and deployment considerations	36
6.1	Overview	36
6.2	Appropriate timeouts	36
6.3	Strict Message processing	36
6.4	Random number generation	37
6.5	Special and reserved packets	37
6.6	Rate limiting and flow control	37
6.7	Administrative access	37
6.8	Cryptographic Keys	38
6.9	Alarm related guidance	38
6.10	Program access	38
6.11	Audit event management	39
6.12	OAuth2, JWT and User roles	39
6.13	HTTPs, SSL/TLS & Websockets	39
6.14	Reverse Connect	39
7	Unsecured Services	40
7.1	Overview	40
7.2	Multicast Discovery	40
7.3	Global Discovery Server Security	40
7.3.1	Overview	40
7.3.2	Rogue GDS	40
7.3.3	Threats against a GDS	41

7.3.4	Certificate management threats	41
8	Certificate management.....	42
8.1.1	Overview	42
8.1.2	Self-signed certificate management	42
8.1.3	CA Signed Certificate management	43
8.1.4	GDS Certificate Management	44
	Bibliography.....	47
	Figure 1 – OPC UA network example	14
	Figure 2 – OPC UA security architecture – Client / Server	20
	Figure 3 – OPC UA security architecture – Publisher-Subscriber	21
	Figure 4 – Role overview	25
	Figure 5 – Simple Servers.....	27
	Figure 6 – Aggregating Servers	28
	Figure 7 – Aggregation with a non-auditing Server	29
	Figure 8 – Aggregate Server with service distribution.....	30
	Figure 9 – Manual Certificate handling	42
	Figure 10 – CA Certificate handling	43
	Figure 11 – Certificate handling	45
	Table 1 – Security Reconciliation Threats Summary	31

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) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

The main task of IEC technical committees is to prepare International Standards. However, a technical committee may propose the publication of a technical report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

IEC TR 62541-2, which is a technical report, has been prepared by subcommittee 65E: Devices and integration in enterprise systems, of IEC technical committee 65: Industrial-process measurement, control and automation.

This third edition cancels and replaces the second edition of IEC TR 62541-2, published in 2016. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

- a) protection-targets definition change;
- b) threat type clarifications;
- c) expanded best practices;

- d) added Websockets;
- e) added Pub/Sub.

The text of this technical report is based on the following documents:

Enquiry draft	Report on voting
65E/679/DTR	65E/703/RVDR

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

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

Throughout this document and the referenced 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 definition” 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 of 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 publication will remain unchanged until the stability date indicated on the IEC web site under "<http://webstore.iec.ch>" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

OPC UNIFIED ARCHITECTURE –

Part 2: Security Model

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 OPC UA specification. It gives an overview of the security features that are specified in other parts of the OPC UA specification. It references services, mappings, and *Profiles* that are specified normatively in other parts of the OPC UA Specification. It provides suggestions or best practice guidelines on implementing security. Any seeming ambiguity between this part and one of the other normative parts does not remove or reduce the requirement specified in the other normative part.

It is important to understand that there are many different aspects of security that have to be 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.

This part is directed to readers who will develop OPC UA *Client* or *Server* applications or implement the OPC UA services layer. It is also for end Users that wish to understand the various security features and functionality provided by OPC UA. It also offers some suggestions that can be applied when deploying systems. These suggestions 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 TR 62541-1, *OPC Unified Architecture – Part 1: Overview and Concepts*

IEC 62541-4, *OPC Unified Architecture – Part 4: Services*

IEC 62541-5, *OPC Unified Architecture – Part 5: Information Model*

IEC 62541-6, *OPC Unified Architecture – Part 6: Mappings*

IEC 62541-7, *OPC Unified Architecture – Part 7: Profiles*

IEC 62541-12, *OPC Unified Architecture – Part 12: Discovery and Global Services*

IEC 62541-14, *OPC Unified Architecture – Part 14: PubSub*

IEC 62351 (all parts), *Power systems management and associated information exchange*