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)

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 It also gives information on projects, replaced and withdrawn publications.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

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*.

3.1.2
AccessToken
digitally signed document that asserts that the subject is entitled to access a *Resource*

Note 1 to entry: The document includes the name of the subject and the *Resource* being accessed.

3.1.3
ApplicationInstance
individual installation of a program running on one computer

Note 1 to entry: There can be several *ApplicationInstances* of the same application running at the same time on several computers or possibly the same computer.

3.1.4
ApplicationInstanceCertificate
Certificate of an individual *ApplicationInstance* that has been installed in an individual host

Note 1 to entry: Different installations of one software product would have different *ApplicationInstanceCertificates*. The use of an *ApplicationInstanceCertificate* for uses outside of what is described in the specification could greatly reduce the security provided by the *ApplicationInstanceCertificate* and should be discouraged.

Note 2 to entry: also written as *ApplicationInstance Certificate*

3.1.5
Asymmetric Cryptography
Cryptography method that uses a pair of keys, one that is designated the *Private Key* and kept secret, the other called the *Public Key* that is generally made available

Note 1 to entry: 'Asymmetric Cryptography, also known as "public-key cryptography". In an Asymmetric Encryption algorithm when an entity "A" requires *Confidentiality* for data sent to entity "B", then entity "A" encrypts the data with a Public Key provided by entity "B". Only entity "B" has the matching Private Key that is needed to decrypt the data. In an asymmetric Digital Signature algorithm when an entity "A" requires message Integrity or to provide *Authentication* for data sent to entity "B", entity A uses its Private Key to sign the data. To verify the signature, entity B uses the matching Public Key that entity A has provided. In an asymmetric key agreement algorithm, entity A and entity B each send their own Public Key to the other entity. Then each uses their own Private Key and the other's Public Key to compute the new key value.' according to IS Glossary.

3.1.6
Asymmetric Encryption
mechanism used by *Asymmetric Cryptography* for encrypting data with the *Public Key* of an entity and for decrypting data with the associated *Private Key*

3.1.7
Asymmetric Signature
mechanism used by *Asymmetric Cryptography* for signing data with the *Private Key* of an entity and for verifying the data's signature with the associated *Public Key*

3.1.8
Auditability
security objective that assures that any actions or activities in a system can be recorded

3.1.9
Auditing
tracking of actions and activities in the system, including security related activities where *Audit* records can be used to review and verify system operations

3.1.10
Authentication
process that assures that the identity of an entity such as a *Client*, *Server*, *Publisher* or user can be verified

3.1.11
Authorization
ability to grant access to a system resource

Note 1 to entry: *Authorization* of access to resources should be based on the need-to-know principle. It is important that access is restricted in a system.

3.1.12
AuthorizationService
Server which validates a request to access a *Resource* returns an *AccessToken* that grants access to the *Resource*

Note 1 to entry: The *AuthorizationService* is also called STS (Security Token Service) in other standards.

3.1.13
Availability
security objective that assures that the system is running normally. That is, no services have been compromised in such a way to become unavailable or severely degraded

3.1.14
Certificate Authority
entity that can issue *Certificate*s, also known as a CA

Note 1 to entry: The *Certificate* certifies the ownership of a *Public Key* by the named subject of the *Certificate*. This allows others (relying parties) to rely upon signatures or assertions made by the *Private Key* that corresponds to the *Public Key* that is certified. In this model of trust relationships, a CA is a trusted party that is trusted by both the subject (owner) of the *Certificate* and the party relying upon the *Certificate*. CA s are characteristic of many *Public Key infrastructure* (PKI) schemes

Note 2 to entry: A private CA system (or a private sub-CA) could be used as long as all parties trust it.

3.1.15
CertificateStore
persistent location where *Certificate*s and *Certificate* revocation lists (CRLs) are stored

Note 1 to entry: It can be a disk resident file structure or on Windows platforms it can be a Windows registry location.

3.1.16
Claim
statement in an *AccessToken* that asserts information about the subject which the *Authorization Service* knows to be true

Note 1 to entry: *Claims* can include username, email, and *Roles* granted to the subject.

3.1.17
Confidentiality
security objective that assures the protection of data from being read by unintended parties

3.1.18
Cryptography
algorithm to transform clear, meaningful information into an enciphered, unintelligible form using an algorithm and a key

3.1.19
Cyber Security Management System
program designed by an organization to maintain the security of the entire organization's assets to an established level of *Confidentiality*, *Integrity*, and *Availability*, whether they are on the business side or the industrial automation and control systems side of the organization

3.1.20
Digital Signature
value computed with a cryptographic algorithm and appended to data in such a way that any recipient of the data can use the signature to verify the data's origin and *Integrity*

3.1.21
Integrity
security objective that assures that information has not been modified or destroyed in an unauthorized manner

Note 1 to entry: More information can be found in IS Glossary.

3.1.22
Identity Provider
Server which verifies credentials provided by a *Security Principal* and returns a token which can be passed to an associated *Authorization Service*

3.1.23
Key Exchange Algorithm
protocol used for establishing a secure communication path between two entities in an unsecured environment whereby both entities apply a specific algorithm to securely exchange secret keys that are used for securing the communication between them

Note 1 to entry: A typical example of a *Key Exchange Algorithm* is the Handshake Protocol specified in TLS.

3.1.24
Message Signature
Digital Signature used to ensure the *Integrity* of *Messages* that are sent between two entities

Note 1 to entry: There are several ways to generate and verify *Message Signatures* however they can be categorized as symmetric (see Entry 3.1.35) and asymmetric (see Entry 3.1.5) approaches.

3.1.25
Non-Repudiation
ability to prove the occurrence of a claimed event or action and its originating entities

Note 1 to entry: The purpose of non-repudiation is to resolve disputes about the occurrence or non-occurrence of the event or action and involvement of entities in the event.

Note 2 to entry: This definition comes from IEC 62443-4-2 and can be different from the definition used in other industries.

3.1.26
Nonce
random number that is used once typically by algorithms that generate security keys

3.1.27
Permission
right to execute an operation, such as a read, write or a call, on a *Node*

3.1.28
Private Key
secret component of a pair of cryptographic keys used for *Asymmetric Cryptography*

Note 1 to entry: *Public Key* and *Private Key* are always generated as a pair. If either is updated, the other will also be updated.

3.1.29
Public Key
publicly-disclosed component of a pair of cryptographic keys used for *Asymmetric Cryptography*

Note 1 to entry: See IS Glossary.

Note 2 to entry: *Public Key* and *Private Key* are always generated as a pair. If either is updated the other must also be updated.

3.1.30
Public Key Infrastructure
set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke *Certificates* based on *Asymmetric Cryptography*

Note 1 to entry: The core PKI functions are to register users and issue their public-key *Certificates*, to revoke *Certificates* when required, and to archive data needed to validate *Certificates*. Key pairs for data *Confidentiality* could be generated by a *Certificate* authority (CA) but it is better to have the *Private Key* owner generate the key pair locally, provided they have a trusted key generation capability, since it improves security because the *Private Key* is never transmitted to the CA. See PKI and X.509v3 for more details on *Public Key* Infrastructures.

3.1.31
Resource
secured entity which an application accesses

Note 1 to entry: A *Resource* is usually a *Server*.

3.1.32
Role
function assumed by a *Client* when it accesses a *Server*

Note 1 to entry: A *Role* can refer to a specific job function such as operator or engineer.

3.1.33
SecurityKeyService

Server that accepts *AccessTokens* issued by the *Authorization Service* and returns security keys that can be used to access the specified *Resource*

Note 1 to entry: The keys are typically used for cryptography operations such as encrypting or decrypting messages sent on a *PubSub* stream.

3.1.34
Secure Channel
in OPC UA, a communication path established between an OPC UA *Client* and *Server* that have authenticated each other using certain OPC UA services and for which security parameters have been negotiated and applied

3.1.35
Symmetric Cryptography
branch of cryptography involving algorithms that use the same key for two different steps of the algorithm (such as encryption and decryption, or signature creation and signature verification)

Note 1 to entry: See IS Glossary.

3.1.36
Symmetric Encryption
mechanism used by *Symmetric Cryptography* for encrypting and decrypting data with a cryptographic key shared by two entities

3.1.37
SecurityGroup
Publisher(s) and *Subscriber*(s) that utilize a shared security context

Note 1 to entry: This context can include share keys.

3.1.38
Symmetric Signature
mechanism used by *Symmetric Cryptography* for signing data with a cryptographic key shared by two entities

Note 1 to entry: The signature is then validated by generating the signature for the data again and comparing these two signatures. If they are the same then the signature is valid, otherwise either the key or the data is different from the two entities.

3.1.39
TrustList
list of *Certificate*s that an OPC UA Application has been configured to trust

3.1.40
Transport Layer Security
standard protocol for creating *Secure Channel*s over IP based networks

3.1.41
X.509 Certificate
Certificate in one of the formats defined by X.509 v1, 2, or 3

Note 1 to entry: An *X.509 Certificate* contains a sequence of data items and has a *Digital Signature* computed on that sequence. OPC UA only uses V3.

3.2 Abbreviated terms

AES	Advanced Encryption Standard
CA	Certificate Authority
CRL	Certificate Revocation List
CSMS	Cyber Security Management System
DNS	Domain Name System
DSA	Digital Signature Algorithm
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
GDS	Global Discovery Server
HMAC	Hash-based Message Authentication Code
JSON	JavaScript Object Notation
JWT	JSON Web Token
NIST	National Institute of Standard and Technology
PKI	Public Key Infrastructure
RSA	public key algorithm for signing or encryption, *Rivest-Shamir-Adleman*
SHA	Secure Hash Algorithm (Multiple versions exist SHA1, SHA256,…)
SKS	Security Key Server
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TPM	Trusted Platform Module
UA	Unified Architecture
UACP	Unified Architecture Connection Protocol
UADP	Unified Architecture Datagram Protocol
URI	Uniform Resource Identifier
XML	Extensible Mark-up Language

3.3 Conventions for security model figures

The figures in this document do not use any special conventions. Any conventions used in a particular figure are explained for that figure.

4 OPC UA security architecture

4.1 OPC UA security environment

OPC UA is a protocol used between components in the operation of an industrial facility at multiple levels: from high-level enterprise management to low-level direct process control of a device. The use of OPC UA for enterprise management involves dealings with customers and suppliers. It can be an attractive target for industrial espionage or sabotage and can also be exposed to threats through untargeted malware, such as worms, circulating on public networks. Disruption of communications at the process control could result in financial losses, affect employee and public safety or cause environmental damage.

OPC UA will be deployed in a diverse range of operational environments with varying assumptions about threats and accessibility, and with a variety of security policies and enforcement regimes. OPC UA, therefore, provides a flexible set of security mechanisms. Figure 1 is a composite that shows a combination of such environments. Some OPC UA *Applications* are on the same host and can be easily protected from external attack. Some OPC UA *Applications* are on different hosts in the same operations network and can be protected by the security boundary protections that separate the operations network from external connections. Some OPC UA *Applications* run in relatively open environments where users and applications can be difficult to control. Other OPC UA *Applications* are embedded in control systems that have no direct electronic connection to external systems. OPC UA also supports multiple protocols and communication technologies, that can require different levels of security and different security infrastructure. For example, both Client - Server and Publisher - Subscriber communication is shown in Figure 1. OPC UA also defines global services such as *Certificate* management, *KeyCredential* management, *AuthorizationService*, and *GlobalDiscoveryServer* (GDS) to help manage security and other global functionality.

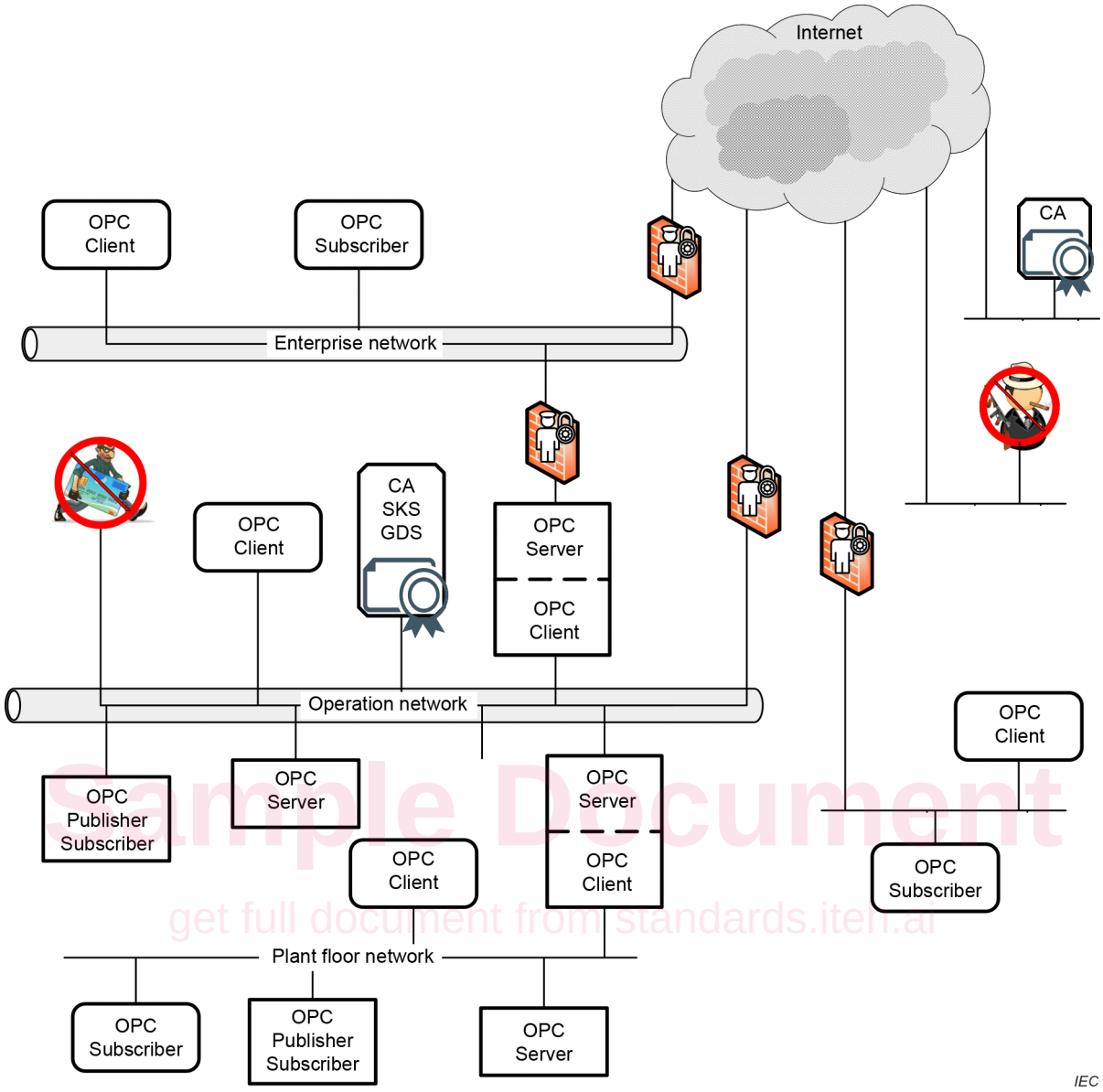

Figure 1 – OPC UA network example

4.2 Security objectives

4.2.1 Overview

Fundamentally, information system security reduces the risk of damage from attacks. It does this by identifying the threats to the system, identifying the system's vulnerabilities to these threats, and providing countermeasures. The countermeasures reduce vulnerabilities directly, counteract threats, or recover from successful attacks.

Industrial automation system security is achieved by meeting a set of objectives. These objectives have been refined through many years of experience in providing security for information systems in general and they remain quite constant despite the ever-changing set of threats to systems. They are described in 5.1 and 5.2 reconciles these objectives against the OPC UA functions. Clause 6 offers additional best practice guidelines to *Client* and *Server* developers or those that deploy *OPC UA Applications*.