

© Copyright SEK. Reproduction in any form without permission is prohibited.

OPC Unified Architecture – Del 2: Säkerhetsmodell

*OPC Unified Architecture –
Part 2: Security Model
(CENELEC Technical Report 62541-2:2010)*

ISSN 1651-1417

ICS 25.040.40; 35.100.01

Upplysningar om **sakinnehållet** i rapporten lämnas av
SEK Svensk Elstandard.
Postadress: SEK, Box 1284, 164 29 KISTA
Telefon: 08 - 444 14 00. Telefax: 08 - 444 14 30
E-post: sek@elstandard.se. Internet: www.elstandard.se

Standarder underlättar utvecklingen och höjer elsäkerheten

Det finns många fördelar med att ha gemensamma tekniska regler för bl a säkerhet, prestanda, dokumentation, utförande och skötsel av elprodukter, elanläggningar och metoder. Genom att utforma sådana standarder blir säkerhetskraven tydliga och utvecklingskostnaderna rimliga samtidigt som marknadens acceptans för produkten eller tjänsten ökar.

Många standarder inom elområdet beskriver tekniska lösningar och metoder som åstadkommer den elsäkerhet som föreskrivs av svenska myndigheter och av EU.

SEK är Sveriges röst i standardiseringsarbetet inom elområdet

SEK Svensk Elstandard svarar för standardiseringen inom elområdet i Sverige och samordnar svensk medverkan i internationell och europeisk standardisering. SEK är en ideell organisation med frivilligt deltagande från svenska myndigheter, företag och organisationer som vill medverka till och påverka utformningen av tekniska regler inom elektrotekniken.

SEK samordnar svenska intressenters medverkan i SEKs tekniska kommittéer och stödjer svenska experters medverkan i internationella och europeiska projekt.

Stora delar av arbetet sker internationellt

Utformningen av standarder sker i allt väsentligt i internationellt och europeiskt samarbete. SEK är svensk nationalkommitté av International Electrotechnical Commission (IEC) och Comité Européen de Normalisation Electrotechnique (CENELEC).

Standardiseringsarbetet inom SEK är organiserat i referensgrupper bestående av ett antal tekniska kommittéer som speglar hur arbetet inom IEC och CENELEC är organiserat.

Arbetet i de tekniska kommittéerna är öppet för alla svenska organisationer, företag, institutioner, myndigheter och statliga verk. Den årliga avgiften för deltagandet och intäkter från försäljning finansierar SEKs standardiseringsverksamhet och medlemsavgift till IEC och CENELEC.

Var med och påverka!

Den som deltar i SEKs tekniska kommittéarbete har möjlighet att påverka framtida standarder och får tidig tillgång till information och dokumentation om utvecklingen inom sitt teknikområde. Arbetet och kontakterna med kollegor, kunder och konkurrenter kan gynnsamt påverka enskilda företags affärsutveckling och bidrar till deltagarnas egen kompetensutveckling.

Du som vill dra nytta av dessa möjligheter är välkommen att kontakta SEKs kansli för mer information.

SEK Svensk Elstandard

Box 1284
164 29 Kista
Tel 08-444 14 00
www.elstandard.se

English version

**OPC unified architecture -
Part 2: Security model
(IEC/TR 62541-2:2010)**

Architecture unifiée OPC -
Partie 2: Modèle de sécurité
(CEI/TR 62541-2:2010)

OPC Unified Architecture -
Teil 2: Modell für die IT-Sicherheit
(IEC/TR 62541-2:2010)

This Technical Report was approved by CENELEC on 2010-06-25.

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, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

CENELEC

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

Management Centre: Avenue Marnix 17, B - 1000 Brussels

Foreword

The text of the Technical Report IEC/TR 62541-2:2010, prepared by SC 65E, Devices and integration in enterprise systems, of IEC TC 65, Industrial-process measurement, control and automation, was submitted to vote and was approved by CENELEC as CLC/TR 62541-2 on 2010-06-25.

Annex ZA has been added by CENELEC.

Endorsement notice

The text of the Technical Report IEC/TR 62541-2:2010 was approved by CENELEC as a Technical Report without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 62541-3	NOTE Harmonized as EN 62541-3.
IEC 62541-4	NOTE Harmonized as EN 62541-4.
IEC 62541-5	NOTE Harmonized as EN 62541-5.
IEC 62541-6	NOTE Harmonized as EN 62541-6.

Annex ZA
(normative)

**Normative references to international publications
with their corresponding European publications**

The following referenced documents are indispensable for the application 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.

NOTE When an international publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC/TR 62541-1	2010	OPC unified architecture - Part 1: Overview and concepts	CLC/TR 62541-1	2010
IEC 62541	Series	OPC unified architecture	EN 62541	Series

CONTENTS

INTRODUCTION.....	6
1 Scope.....	7
2 Normative references	7
3 Terms, definitions, abbreviations and conventions.....	7
3.1 Terms and definitions	7
3.2 Abbreviations and symbols.....	11
3.3 Conventions concerning security model figures	11
4 OPC UA Security architecture	11
4.1 OPC UA security environment	11
4.2 Security objectives	12
4.2.1 General	12
4.2.2 Authentication	13
4.2.3 Authorization	13
4.2.4 Confidentiality	13
4.2.5 Integrity	13
4.2.6 Auditability	13
4.2.7 Availability.....	13
4.3 Security threats to OPC UA systems	13
4.3.1 General	13
4.3.2 Message flooding	13
4.3.3 Eavesdropping	14
4.3.4 Message spoofing	14
4.3.5 Message alteration	14
4.3.6 Message replay	14
4.3.7 Malformed messages.....	15
4.3.8 Server profiling	15
4.3.9 Session hijacking.....	15
4.3.10 Rogue server.....	15
4.3.11 Compromising user credentials.....	15
4.4 OPC UA relationship to site security.....	16
4.5 OPC UA security architecture.....	16
4.6 Security policies	18
4.7 Security profiles	18
4.8 User authorization	19
4.9 User authentication	19
4.10 Application authentication	19
4.11 OPC UA security related services.....	19
4.12 Auditing.....	20
4.12.1 General	20
4.12.2 Single client and server	21
4.12.3 Aggregating server	21
4.12.4 Aggregation through a non-auditing server	22
4.12.5 Aggregating server with service distribution.....	23
5 Security reconciliation	24
5.1 Reconciliation of threats with OPC UA security mechanisms	24

5.1.1	General	24
5.1.2	Message flooding	24
5.1.3	Eavesdropping	25
5.1.4	Message spoofing	25
5.1.5	Message alteration	25
5.1.6	Message replay	25
5.1.7	Malformed messages.....	26
5.1.8	Server profiling	26
5.1.9	Session hijacking.....	26
5.1.10	Rogue server.....	26
5.1.11	Compromising user credentials.....	26
5.2	Reconciliation of objectives with OPC UA security mechanisms	26
5.2.1	General	26
5.2.2	Authentication	27
5.2.3	Authorization	27
5.2.4	Confidentiality	27
5.2.5	Integrity	27
5.2.6	Auditability	28
5.2.7	Availability.....	28
6	Implementation considerations	28
6.1	General.....	28
6.2	Appropriate timeouts	28
6.3	Strict message processing.....	28
6.4	Random number generation	29
6.5	Special and reserved packets.....	29
6.6	Rate limiting and flow control	29
	Bibliography.....	30
	Figure 1 – OPC UA network model	12
	Figure 2 – OPC UA security architecture.....	17
	Figure 3 – Simple servers	21
	Figure 4 – Aggregating servers	22
	Figure 5 – Aggregation with a non-auditing server	23
	Figure 6 – Aggregate server with service distribution	24

INTRODUCTION

This technical report introduces security concepts for OPC Unified Architecture as specified by IEC 62541. This technical report and specification are a result of an analysis and design process to develop a standard interface to facilitate the development of applications by multiple vendors that inter-operate seamlessly together.

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 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 this series of standards.

Note 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 developer look into all aspects of security and decide how they can be addressed in the application.

This part of IEC 62541 is directed to readers who will develop OPC UA client or server applications or implement the OPC UA services layer.

It is assumed that the reader is familiar with Web Services and XML/SOAP. Information on these technologies can be found in SOAP Part 1 and SOAP Part 2.

2 Normative references

The following referenced documents are indispensable for the application 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 (all parts), *OPC Unified Architecture*

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