

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

OPC unified architecture – Del 7: Profiler

*OPC unified architecture –
Part 7: Profiles*

Som svensk standard gäller europastandarden EN IEC 62541-7:2020. Den svenska standarden innehåller den officiella engelska språkversionen av EN IEC 62541-7:2020.

Nationellt förord

Europastandarden EN IEC 62541-7:2020

består av:

- **europastandardens ikraftsättningsdokument**, utarbetat inom CENELEC
- **IEC 62541-7, Third edition, 2020 - OPC unified architecture - Part 7: Profiles**

utarbetad inom International Electrotechnical Commission, IEC.

Tidigare fastställd svensk standard SS-EN 62541-7, utgåva 2, 2015, gäller ej fr o m 2023-07-27.

ICS 25.040.40; 35.100.05

Denna standard är fastställd av SEK Svensk Elstandard, som också kan lämna upplysningar om **sakinnehållet** i standarden.
Postadress: Box 1284, 164 29 KISTA
Telefon: 08 - 444 14 00.
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 mätning, säkerhet och provning och för utförande, skötsel och dokumentation av elprodukter och elanläggningar.

Genom att utforma sådana standarder blir säkerhetsfordringar 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

EUROPEAN STANDARD

EN IEC 62541-7

NORME EUROPÉENNE

EUROPÄISCHE NORM

August 2020

ICS 35.100.05; 25.040.40

Supersedes EN 62541-7:2015 and all of its amendments
and corrigenda (if any)

English Version

OPC unified architecture - Part 7: Profiles (IEC 62541-7:2020)

Architecture unifiée OPC - Partie 7: Profils
(IEC 62541-7:2020)

OPC Unified Architecture - Teil 7: Profile
(IEC 62541-7:2020)

This European Standard was approved by CENELEC on 2020-07-27. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

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

© 2020 CENELEC All rights of exploitation in any form and by any means reserved worldwide for CENELEC Members.

Ref. No. EN IEC 62541-7:2020 E

SEK Svensk Elstandard

SS-EN IEC 62541-7, utg 3:2020

European foreword

The text of document 65E/707/FDIS, future edition 3 of IEC 62541-7, prepared by SC 65E "Devices and integration in enterprise systems" of IEC/TC 65 "Industrial-process measurement, control and automation" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN IEC 62541-7:2020.

The following dates are fixed:

- latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2021-04-27
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2023-07-27

This document supersedes EN 62541-7:2015 and all of its amendments and corrigenda (if any).

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.

This document has been prepared under a mandate given to CENELEC by the European Commission and the European Free Trade Association.

Endorsement notice

The text of the International Standard IEC 62541-7:2020 was approved by CENELEC as a European Standard without any modification.

Annex ZA (normative)

Normative references to international publications with their corresponding European publications

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.

NOTE 1 Where an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC/TR 62541-1	-	OPC unified architecture - Part 1: Overview and concepts	CLC/TR 62541-1	-
IEC/TR 62541-2	-	OPC unified architecture - Part 2: Security model	CLC/TR 62541-2	-
IEC 62541-3	-	OPC Unified Architecture - Part 3: Address Space Model	-	-
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 62541-8	-	OPC Unified Architecture - Part 8: Data Access	-	-
IEC 62541-9	-	OPC Unified Architecture - Part 9: Alarms and Conditions	-	-
IEC 62541-11	-	OPC Unified Architecture - Part 11: Historical Access	-	-
IEC 62541-12	-	OPC unified architecture - Part 12: Discovery and global services	-	-
IEC 62541-13	-	OPC Unified Architecture - Part 13: Aggregates	-	-
Compliance Part 8 UA Server	-	OPC Test Lab Specification: Part 8 - UA Server	-	-
Compliance Part 9 UA Client	-	OPC Test Lab Specification: Part 9 - UA Client	-	-

CONTENTS

FOREWORD	12
1 Scope	15
2 Normative references	15
3 Terms, definitions, and abbreviated terms	16
3.1 Terms and definitions.....	16
3.2 Abbreviated terms.....	17
4 Overview	17
4.1 General.....	17
4.2 ConformanceUnit	18
4.3 Profiles	18
4.4 Profile Categories	19
5 Conformance Units	19
5.1 Overview.....	19
5.2 Services.....	20
5.3 Transport and communication related features.....	30
5.4 Information Model and AddressSpace related features.....	38
5.5 Miscellaneous	55
6 Profiles.....	57
6.1 Overview.....	57
6.2 Profile list	57
6.3 Conventions for Profile definitions.....	64
6.4 Profile versioning	64
6.5 Applications	64
6.6 Profile tables.....	66
6.6.1 General	66
6.6.2 Core Server Facet	66
6.6.3 Core 2017 Server Facet.....	66
6.6.4 Sessionless Server Facet	67
6.6.5 Reverse Connect Server Facet	67
6.6.6 Base Server Behaviour Facet	68
6.6.7 Request State Change Server Facet.....	68
6.6.8 Subnet Discovery Server Facet.....	68
6.6.9 Global Certificate Management Server Facet.....	68
6.6.10 Authorization Service Server Facet.....	69
6.6.11 KeyCredential Service Server Facet	69
6.6.12 Attribute WriteMask Server Facet	69
6.6.13 File Access Server Facet	69
6.6.14 Documentation Server Facet	70
6.6.15 Embedded DataChange Subscription Server Facet.....	70
6.6.16 Standard DataChange Subscription Server Facet	70
6.6.17 Standard DataChange Subscription 2017 Server Facet.....	71
6.6.18 Enhanced DataChange Subscription Server Facet.....	71
6.6.19 Enhanced DataChange Subscription 2017 Server Facet	71
6.6.20 Durable Subscription Server Facet	71
6.6.21 Data Access Server Facet	72
6.6.22 ComplexType Server Facet.....	72

6.6.23	ComplexType 2017 Server Facet	72
6.6.24	Standard Event Subscription Server Facet	73
6.6.25	Address Space Notifier Server Facet	74
6.6.26	A & C Base Condition Server Facet	74
6.6.27	A & C Refresh2 Server Facet	74
6.6.28	A & C Address Space Instance Server Facet	74
6.6.29	A & C Enable Server Facet	75
6.6.30	A & C AlarmMetrics Server Facet	75
6.6.31	A & C Alarm Server Facet	75
6.6.32	A & C Acknowledgeable Alarm Server Facet	76
6.6.33	A & C Exclusive Alarming Server Facet	76
6.6.34	A & C Non-Exclusive Alarming Server Facet	77
6.6.35	A & C Previous Instances Server Facet	77
6.6.36	A & C Dialog Server Facet	77
6.6.37	A & C CertificateExpiration Server Facet	78
6.6.38	A & E Wrapper Facet	78
6.6.39	Method Server Facet	79
6.6.40	Auditing Server Facet	79
6.6.41	Node Management Server Facet	80
6.6.42	User Role Base Server Facet	80
6.6.43	User Role Management Server Facet	80
6.6.44	State Machine Server Facet	81
6.6.45	Client Redundancy Server Facet	81
6.6.46	Redundancy Transparent Server Facet	81
6.6.47	Redundancy Visible Server Facet	82
6.6.48	Historical Raw Data Server Facet	82
6.6.49	Historical Aggregate Server Facet	82
6.6.50	Historical Data AtTime Server Facet	83
6.6.51	Historical Access Modified Data Server Facet	84
6.6.52	Historical Annotation Server Facet	84
6.6.53	Historical Data Insert Server Facet	84
6.6.54	Historical Data Update Server Facet	84
6.6.55	Historical Data Replace Server Facet	85
6.6.56	Historical Data Delete Server Facet	85
6.6.57	Historical Access Structured Data Server Facet	85
6.6.58	Base Historical Event Server Facet	85
6.6.59	Historical Event Update Server Facet	86
6.6.60	Historical Event Replace Server Facet	86
6.6.61	Historical Event Insert Server Facet	86
6.6.62	Historical Event Delete Server Facet	86
6.6.63	Aggregate Subscription Server Facet	87
6.6.64	Nano Embedded Device Server Profile	88
6.6.65	Nano Embedded Device 2017 Server Profile	88
6.6.66	Micro Embedded Device Server Profile	88
6.6.67	Micro Embedded Device 2017 Server Profile	88
6.6.68	Embedded UA Server Profile	88
6.6.69	Embedded 2017 UA Server Profile	89
6.6.70	Standard UA Server Profile	89
6.6.71	Standard 2017 UA Server Profile	89

6.6.72	Core Client Facet.....	90
6.6.73	Core 2017 Client Facet.....	90
6.6.74	Sessionless Client Facet	90
6.6.75	Reverse Connect Client Facet	90
6.6.76	Base Client Behaviour Facet.....	91
6.6.77	Discovery Client Facet.....	91
6.6.78	Subnet Discovery Client Facet.....	91
6.6.79	Global Discovery Client Facet.....	92
6.6.80	Global Certificate Management Client Facet	92
6.6.81	KeyCredential Service Client Facet.....	92
6.6.82	Access Token Request Client Facet	92
6.6.83	AddressSpace Lookup Client Facet	93
6.6.84	Request State Change Client Facet.....	93
6.6.85	File Access Client Facet	93
6.6.86	Entry Level Support 2015 Client Facet.....	94
6.6.87	Multi-Server Client Connection Facet.....	94
6.6.88	Documentation – Client	94
6.6.89	Attribute Read Client Facet.....	94
6.6.90	Attribute Write Client Facet.....	95
6.6.91	DataChange Subscriber Client Facet.....	95
6.6.92	Durable Subscription Client Facet.....	96
6.6.93	DataAccess Client Facet.....	96
6.6.94	Event Subscriber Client Facet.....	97
6.6.95	Base Event Processing Client Facet	97
6.6.96	Notifier and Source Hierarchy Client Facet	98
6.6.97	A & C Base Condition Client Facet	98
6.6.98	A & C Refresh2 Client Facet.....	98
6.6.99	A & C Address Space Instance Client Facet	99
6.6.100	A & C Enable Client Facet	99
6.6.101	A & C AlarmMetrics Client Facet.....	99
6.6.102	A & C Alarm Client Facet.....	99
6.6.103	A & C Exclusive Alarming Client Facet.....	100
6.6.104	A & C Non-Exclusive Alarming Client Facet	100
6.6.105	A & C Previous Instances Client Facet.....	101
6.6.106	A & C Dialog Client Facet.....	101
6.6.107	A & C CertificateExpiration Client Facet.....	101
6.6.108	A & E Proxy Facet	102
6.6.109	Method Client Facet.....	103
6.6.110	Auditing Client Facet	103
6.6.111	Node Management Client Facet.....	103
6.6.112	Advanced Type Programming Client Facet	103
6.6.113	User Role Management Client Facet.....	104
6.6.114	State Machine Client Facet.....	104
6.6.115	Diagnostic Client Facet.....	104
6.6.116	Redundant Client Facet	105
6.6.117	Redundancy Switch Client Facet	105
6.6.118	Historical Access Client Facet	105
6.6.119	Historical Data AtTime Client Facet	105
6.6.120	Historical Aggregate Client Facet.....	105

6.6.121	Historical Annotation Client Facet	107
6.6.122	Historical Access Modified Data Client Facet	107
6.6.123	Historical Data Insert Client Facet	107
6.6.124	Historical Data Update Client Facet	107
6.6.125	Historical Data Replace Client Facet.....	107
6.6.126	Historical Data Delete Client Facet	108
6.6.127	Historical Access Client Server Timestamp Facet	108
6.6.128	Historical Structured Data Access Client Facet	108
6.6.129	Historical Structured Data AtTime Client Facet	108
6.6.130	Historical Structured Data Modified Client Facet	109
6.6.131	Historical Structured Data Insert Client Facet	109
6.6.132	Historical Structured Data Update Client Facet	109
6.6.133	Historical Structured Data Replace Client Facet	109
6.6.134	Historical Structured Data Delete Client Facet	109
6.6.135	Historical Events Client Facet.....	110
6.6.136	Historical Event Insert Client Facet.....	110
6.6.137	Historical Event Update Client Facet.....	110
6.6.138	Historical Event Replace Client Facet.....	110
6.6.139	Historical Event Delete Client Facet.....	111
6.6.140	Aggregate Subscriber Client Facet	111
6.6.141	Standard UA Client Profile	112
6.6.142	Standard UA Client 2017 Profile	112
6.6.143	UA-TCP UA-SC UA-Binary.....	113
6.6.144	HTTPS UA-Binary.....	113
6.6.145	HTTPS UA-XML.....	114
6.6.146	HTTPS UA-JSON.....	114
6.6.147	WSS UA-SC UA-Binary.....	114
6.6.148	WSS UA-JSON	114
6.6.149	Security User Access Control Full.....	115
6.6.150	Security User Access Control Base.....	115
6.6.151	Security Time Synchronization.....	115
6.6.152	Best Practice – Audit Events.....	116
6.6.153	Best Practice – Alarm Handling	116
6.6.154	Best Practice – Random Numbers	116
6.6.155	Best Practice – Timeouts	116
6.6.156	Best Practice – Administrative Access	116
6.6.157	Best Practice – Strict Message Handling	117
6.6.158	Best Practice – Audit Events Client.....	117
6.6.159	TransportSecurity – TLS 1.2	117
6.6.160	TransportSecurity – TLS 1.2 with PFS	117
6.6.161	SecurityPolicy – None.....	118
6.6.162	SecurityPolicy – Basic128Rsa15.....	118
6.6.163	SecurityPolicy – Basic256.....	118
6.6.164	SecurityPolicy [A] – Aes128-Sha256-RsaOaep	118
6.6.165	SecurityPolicy [B] – Basic256Sha256	119
6.6.166	SecurityPolicy – Aes256-Sha256-RsaPss	119
6.6.167	User Token – Anonymous Facet	120
6.6.168	User Token – User Name Password Server Facet	120
6.6.169	User Token – X509 Certificate Server Facet	120

6.6.170	User Token – Issued Token Server Facet	121
6.6.171	User Token – Issued Token Windows Server Facet	121
6.6.172	User Token – JWT Server Facet	121
6.6.173	User Token – User Name Password Client Facet	121
6.6.174	User Token – X509 Certificate Client Facet	122
6.6.175	User Token – Issued Token Client Facet	122
6.6.176	User Token – Issued Token Windows Client Facet	122
6.6.177	User Token – JWT Client Facet	122
6.6.178	Global Discovery Server Profile	122
6.6.179	Global Discovery Server 2017 Profile	123
6.6.180	Global Discovery and Certificate Management Server	123
6.6.181	Global Discovery and Certificate Mgmt 2017 Server	123
6.6.182	Global Certificate Management Client Profile	123
6.6.183	Global Certificate Management Client 2017 Profile	123
6.6.184	Global Service Authorization Request Server Facet	124
6.6.185	Global Service KeyCredential Pull Facet	124
6.6.186	Global Service KeyCredential Push Facet	124
Bibliography		125
Figure 1	– Profile – ConformanceUnit – TestCases	18
Figure 2	– HMI Client sample	64
Figure 3	– Embedded Server sample	65
Figure 4	– Standard UA Server sample	65
Table 1	– Profile Categories	19
Table 2	– Conformance Groups	20
Table 3	– Discovery Services	21
Table 4	– Session Services	22
Table 5	– Node Management Services	23
Table 6	– View Services	24
Table 7	– Attribute Services	25
Table 8	– Method Services	26
Table 9	– Monitored Item Services	27
Table 10	– Subscription Services	29
Table 11	– Security	31
Table 12	– Protocol and Encoding	38
Table 13	– Base Information	39
Table 14	– Address Space Model	41
Table 15	– Data Access	42
Table 16	– Alarms and Conditions	43
Table 17	– Historical Access	46
Table 18	– Aggregates	49
Table 19	– Auditing	54
Table 20	– Redundancy	54
Table 21	– Global Discovery Server	55

Table 22 – Miscellaneous	56
Table 23 – Profile list	58
Table 24 – Core 2017 Server Facet	67
Table 25 – Sessionless Server Facet	67
Table 26 – Reverse Connect Server Facet	68
Table 27 – Base Server Behaviour Facet	68
Table 28 – Request State Change Server Facet	68
Table 29 – Subnet Discovery Server Facet	68
Table 30 – Global Certificate Management Server Facet	69
Table 31 – Authorization Service Server Facet	69
Table 32 – KeyCredential Service Server Facet	69
Table 33 – Attribute WriteMask Server Facet	69
Table 34 – File Access Server Facet	70
Table 35 – Documentation Server Facet	70
Table 36 – Embedded DataChange Subscription Server Facet	70
Table 37 – Standard DataChange Subscription 2017 Server Facet	71
Table 38 – Enhanced DataChange Subscription 2017 Server Facet	71
Table 39 – Durable Subscription Server Facet	72
Table 40 – Data Access Server Facet	72
Table 41 – ComplexType 2017 Server Facet	73
Table 42 – Standard Event Subscription Server Facet	73
Table 43 – Address Space Notifier Server Facet	74
Table 44 – A & C Base Condition Server Facet	74
Table 45 – A & C Refresh2 Server Facet	74
Table 46 – A & C Address Space Instance Server Facet	75
Table 47 – A & C Enable Server Facet	75
Table 48 – A & C AlarmMetrics Server Facet	75
Table 49 – A & C Alarm Server Facet	76
Table 50 – A & C Acknowledgeable Alarm Server Facet	76
Table 51 – A & C Exclusive Alarming Server Facet	77
Table 52 – A & C Non-Exclusive Alarming Server Facet	77
Table 53 – A & C Previous Instances Server Facet	77
Table 54 – A & C Dialog Server Facet	78
Table 55 – A & C CertificateExpiration Server Facet	78
Table 56 – A & E Wrapper Facet	79
Table 57 – Method Server Facet	79
Table 58 – Auditing Server Facet	80
Table 59 – Node Management Server Facet	80
Table 60 – User Role Base Server Facet	80
Table 61 – User Role Management Server Facet	81
Table 62 – State Machine Server Facet	81
Table 63 – Client Redundancy Server Facet	81
Table 64 – Redundancy Transparent Server Facet	81

Table 65 – Redundancy Visible Server Facet.....	82
Table 66 – Historical Raw Data Server Facet.....	82
Table 67 – Historical Aggregate Server Facet.....	83
Table 68 – Historical Data AtTime Server Facet.....	84
Table 69 – Historical Access Modified Data Server Facet.....	84
Table 70 – Historical Annotation Server Facet.....	84
Table 71 – Historical Data Insert Server Facet.....	84
Table 72 – Historical Data Update Server Facet.....	85
Table 73 – Historical Data Replace Server Facet.....	85
Table 74 – Historical Data Delete Server Facet.....	85
Table 75 – Historical Access Structured Data Server Facet.....	85
Table 76 – Base Historical Event Server Facet.....	86
Table 77 – Historical Event Update Server Facet.....	86
Table 78 – Historical Event Replace Server Facet.....	86
Table 79 – Historical Event Insert Server Facet.....	86
Table 80 – Historical Event Delete Server Facet.....	86
Table 81 – Aggregate Subscription Server Facet.....	87
Table 82 – Nano Embedded Device 2017 Server Profile.....	88
Table 83 – Micro Embedded Device 2017 Server Profile.....	88
Table 84 – Embedded 2017 UA Server Profile.....	89
Table 85 – Standard 2017 UA Server Profile.....	89
Table 86 – Core 2017 Client Facet.....	90
Table 87 – Sessionless Client Facet.....	90
Table 88 – Reverse Connect Client Facet.....	91
Table 89 – Base Client Behaviour Facet.....	91
Table 90 – Discovery Client Facet.....	91
Table 91 – Subnet Discovery Client Facet.....	92
Table 92 – Global Discovery Client Facet.....	92
Table 93 – Global Certificate Management Client Facet.....	92
Table 94 – KeyCredential Service Client Facet.....	92
Table 95 – Access Token Request Client Facet.....	93
Table 96 – AddressSpace Lookup Client Facet.....	93
Table 97 – Request State Change Client Facet.....	93
Table 98 – File Access Client Facet.....	93
Table 99 – Entry Level Support 2015 Client Facet.....	94
Table 100 – Multi-Server Client Connection Facet.....	94
Table 101 – Documentation – Client.....	94
Table 102 – Attribute Read Client Facet.....	95
Table 103 – Attribute Write Client Facet.....	95
Table 104 – DataChange Subscriber Client Facet.....	96
Table 105 – Durable Subscription Client Facet.....	96
Table 106 – DataAccess Client Facet.....	97
Table 107 – Event Subscriber Client Facet.....	97

Table 108 – Base Event Processing Client Facet	98
Table 109 – Notifier and Source Hierarchy Client Facet	98
Table 110 – A & C Base Condition Client Facet	98
Table 111 – A & C Refresh2 Client Facet.....	99
Table 112 – A & C Address Space Instance Client Facet	99
Table 113 – A & C Enable Client Facet	99
Table 114 – A & C AlarmMetrics Client Facet.....	99
Table 115 – A & C Alarm Client Facet.....	100
Table 116 – A & C Exclusive Alarming Client Facet	100
Table 117 – A & C Non-Exclusive Alarming Client Facet.....	101
Table 118 – A & C Previous Instances Client Facet	101
Table 119 – A & C Dialog Client Facet	101
Table 120 – A & C CertificateExpiration Client Facet	101
Table 121 – A & E Proxy Facet	102
Table 122 – Method Client Facet	103
Table 123 – Auditing Client Facet	103
Table 124 – Node Management Client Facet.....	103
Table 125 – Advanced Type Programming Client Facet	104
Table 126 – User Role Management Client Facet	104
Table 127 – State Machine Client Facet.....	104
Table 128 – Diagnostic Client Facet.....	104
Table 129 – Redundant Client Facet.....	105
Table 130 – Redundancy Switch Client Facet	105
Table 131 – Historical Access Client Facet	105
Table 132 – Historical Data AtTime Client Facet	105
Table 133 – Historical Aggregate Client Facet	106
Table 134 – Historical Annotation Client Facet.....	107
Table 135 – Historical Access Modified Data Client Facet.....	107
Table 136 – Historical Data Insert Client Facet	107
Table 137 – Historical Data Update Client Facet	107
Table 138 – Historical Data Replace Client Facet	108
Table 139 – Historical Data Delete Client Facet.....	108
Table 140 – Historical Access Client Server Timestamp Facet.....	108
Table 141 – Historical Structured Data Access Client Facet.....	108
Table 142 – Historical Structured Data AtTime Client Facet	108
Table 143 – Historical Structured Data Modified Client Facet.....	109
Table 144 – Historical Structured Data Insert Client Facet	109
Table 145 – Historical Structured Data Update Client Facet.....	109
Table 146 – Historical Structured Data Replace Client Facet	109
Table 147 – Historical Structured Data Delete Client Facet.....	110
Table 148 – Historical Events Client Facet.....	110
Table 149 – Historical Event Insert Client Facet.....	110
Table 150 – Historical Event Update Client Facet	110

Table 151 – Historical Event Replace Client Facet.....	110
Table 152 – Historical Event Delete Client Facet	111
Table 153 – Aggregate Subscriber Client Facet	111
Table 154 – Standard UA Client 2017 Profile	113
Table 155 – UA-TCP UA-SC UA-Binary	113
Table 156 – HTTPS UA-Binary.....	113
Table 157 – HTTPS UA-XML	114
Table 158 – HTTPS UA-JSON	114
Table 159 – WSS UA-SC UA-Binary	114
Table 160 – WSS UA-JSON.....	115
Table 161 – Security User Access Control Full	115
Table 162 – Security User Access Control Base	115
Table 163 – Security Time Synchronization	115
Table 164 – Best Practice – Audit Events	116
Table 165 – Best Practice – Alarm Handling	116
Table 166 – Best Practice – Random Numbers	116
Table 167 – Best Practice – Timeouts.....	116
Table 168 – Best Practice – Administrative Access	117
Table 169 – Best Practice – Strict Message Handling	117
Table 170 – Best Practice – Audit Events Client	117
Table 171 – TransportSecurity – TLS 1.2.....	117
Table 172 – TransportSecurity – TLS 1.2 with PFS	118
Table 173 – SecurityPolicy – None	118
Table 174 – SecurityPolicy [A] – Aes128-Sha256-RsaOaep	119
Table 175 – SecurityPolicy [B] – Basic256Sha256	119
Table 176 – SecurityPolicy – Aes256-Sha256-RsaPss	120
Table 177 – User Token – Anonymous Facet.....	120
Table 178 – User Token – User Name Password Server Facet	120
Table 179 – User Token – X509 Certificate Server Facet.....	120
Table 180 – User Token – Issued Token Server Facet.....	121
Table 181 – User Token – Issued Token Windows Server Facet	121
Table 182 – User Token – JWT Server Facet.....	121
Table 183 – User Token – User Name Password Client Facet.....	121
Table 184 – User Token – X509 Certificate Client Facet	122
Table 185 – User Token – Issued Token Client Facet	122
Table 186 – User Token – Issued Token Windows Client Facet	122
Table 187 – User Token – JWT Client Facet	122
Table 188 – Global Discovery Server 2017 Profile	123
Table 189 – Global Discovery and Certificate Mgmt 2017 Server	123
Table 190 – Global Certificate Management Client 2017 Profile.....	124
Table 191 – Global Service Authorization Request Server Facet.....	124

Table 192 – Global Service KeyCredential Pull Facet	124
Table 193 – Global Service KeyCredential Push Facet.....	124

INTERNATIONAL ELECTROTECHNICAL COMMISSION

OPC UNIFIED ARCHITECTURE –

Part 7: Profiles

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.

International Standard IEC 62541-7 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 published in 2015. This edition constitutes a technical revision.

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

- a) new functional Profiles:
 - profiles for global discovery and global certificate management;
 - profiles for global KeyCredential management and global access token management;
 - facet for durable subscriptions;
 - standard UA Client Profile;

- profiles for administration of user roles and permissions.
- b) new transport Profiles:
- HTTPS with JSON encoding;
 - secure WebSockets (WSS) with binary or JSON encoding;
 - reverse connectivity.
- c) new security Profiles:
- transportSecurity – TLS 1.2 with PFS (with perfect forward secrecy);
 - securityPolicy [A] – Aes128-Sha256-RsaOaep (replaces Base128Rsa15);
 - securityPolicy – Aes256-Sha256-RsaPss adds perfect forward secrecy for UA TCP);
 - user Token JWT (Jason Web Token).
- d) deprecated Security Profiles (due to broken algorithms):
- securityPolicy – Basic128Rsa15 (broken algorithm Sha1);
 - securityPolicy – Basic256 (broken algorithm Sha1);
 - transportSecurity – TLS 1.0 (broken algorithm RC4);
 - transportSecurity – TLS 1.1 (broken algorithm RC4).
- e) deprecated Transport (missing support on most platforms):
- SOAP/HTTP with WS-SecureConversation (all encodings).

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

FDIS	Report on voting
65E/707/FDIS	65E/725/RVD

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

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

Throughout this document and the other parts of the IEC 62541 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 IEC 62541 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, with a few exceptions, 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 document will remain unchanged until the stability date indicated on the IEC website under "<http://webstore.iec.ch>" in the data related to the specific document. At this date, the document 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 7: Profiles

1 Scope

This part of IEC 62541 defines the OPC Unified Architecture (OPC UA) *Profiles*. The *Profiles* in this document are used to segregate features with regard to testing of OPC UA products and the nature of the testing (tool based or lab based). This includes the testing performed by the OPC Foundation provided OPC UA CTT (a self-test tool) and by the OPC Foundation provided Independent certification test labs. This could equally as well refer to test tools provided by another organization or a test lab provided by another organization. What is important is the concept of automated tool-based testing versus lab-based testing. The scope of this standard includes defining functionality that can only be tested in a lab and defining the grouping of functionality that is to be used when testing OPC UA products either in a lab or using automated tools. The definition of actual *TestCases* is not within the scope of this document, but the general categories of *TestCases* are within the scope of this document.

Most OPC UA applications will conform to several, but not all, of the *Profiles*.

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 TR 62541-2, *OPC Unified Architecture – Part 2: Security Model*

IEC 62541-3, *OPC Unified Architecture – Part 3: Address Space Model*

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 62541-8, *OPC Unified Architecture – Part 8: Data Access*

IEC 62541-9, *OPC Unified Architecture – Part 9: Alarms and Conditions*

IEC 62541-11, *OPC Unified Architecture – Part 11: Historical Access*

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

IEC 62541-13, *OPC Unified Architecture – Part 13: Aggregates*

Compliance Part 8 UA Server: OPC Test Lab Specification: Part 8 – UA Server
<http://www.opcfoundation.org/Test/Part8/>

Compliance Part 9 UA Client: OPC Test Lab Specification: Part 9 – UA Client
<http://www.opcfoundation.org/Test/Part9/>