DIN EN IEC 62541-7

DIN

ICS 35.200; 35.240.50

Einsprüche bis 2019-10-16
Vorgesehen als Ersatz für
DIN EN 62541-7:2015-11

Entwurf

OPC Unified Architecture – Teil 7: Profile (IEC 65E/608/CDV:2018); Englische Fassung prEN IEC 62541-7:2018

OPC unified architecture –
Part 7: Profiles
(IEC 65E/608/CDV:2018);
English version prEN IEC 62541-7:2018

Architecture unifiée OPC –
Partie 7: Profils
(IEC 65E/608/CDV:2018);
Version anglaise prEN IEC 62541-7:2018

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2019-08-16 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an dke@vde.com möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, Stresemannallee 15, 60596 Frankfurt am Main.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 112 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

AVA Documents Document Sharing Hub

Full document details: E DIN EN IEC 62541-7:2019-09

Nationales Vorwort

Die Englische Fassung des europäischen Dokuments prEN IEC 62541-7:2018 „OPC Unified Architecture – Teil 7: Profile“ (Entwurf in der Umfrage) ist unverändert in diesen Norm-Entwurf übernommen worden.

Die Internationale Elektrotechnische Kommission (IEC) und das Europäische Komitee für Elektrotechnische Normung (CENELEC) haben vereinbart, dass ein auf IEC-Ebene erarbeiteter Entwurf für eine Internationale Norm zeitgleich (parallel) bei IEC und CENELEC zur Umfrage (CDV-Stadium) und Abstimmung als FDIS (en: Final Draft International Standard) bzw. Schluss-Entwurf für eine Europäische Norm gestellt wird, um eine Beschleunigung und Straffung der Normungsarbeit zu erreichen. Dem entsprechend ist das internationale Dokument IEC 65E/608/CDV:2018 „OPC unified architecture – Part 7: Profiles“ unverändert in den Entwurf prEN IEC 62541-7:2018 übernommen worden.

Das internationale Dokument wurde vom SC 65E „Devices and integration in enterprise systems“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet.

Bei der Abstimmung zu dem Europäischen Schluss-Entwurf bei CENELEC und dem Internationalen Schluss-Entwurf bei IEC [Final Draft International Standard (FDIS)] sind jeweils nur „JA/NEIN“-Entscheidungen möglich, wobei „NEIN“-Entscheidungen fundiert begründet werden müssen. Dokumente, die bei CENELEC als Europäische Norm angenommen und ratifiziert werden, sind unverändert als Deutsche Normen zu übernehmen.

Für dieses Dokument ist das nationale Arbeitsgremium K 931 „Systemaspekte der Automatisierung“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (www.dke.de) zuständig.

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf ein Dokument ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnittsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils aktuellste Ausgabe des in Bezug genommenen Dokuments.

Für den Fall einer datierten Verweisung im normativen Text bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe des Dokuments.

Der Zusammenhang der zitierten Dokumente mit den entsprechenden deutschen Dokumenten ergibt sich, soweit ein Zusammenhang besteht, grundsätzlich über die Nummer der entsprechenden IEC-Publikation. Beispiel: IEC 60068 ist als EN 60068 als Europäische Norm durch CENELEC übernommen und als DIN EN 60068 ins Deutsche Normenwerk aufgenommen.Der Zusammenhang der zitierten Dokumente mit den entsprechenden deutschen Dokumenten ergibt sich, soweit ein Zusammenhang besteht, grundsätzlich über die Nummer der entsprechenden IEC-Publikation. Beispiel: IEC 60068 ist als EN 60068 als Europäische Norm durch CENELEC übernommen und als DIN EN 60068 ins Deutsche Normenwerk aufgenommen.

Das Präsidium des DIN hat mit Präsidialbeschluss 1/2004 festgelegt, dass DIN-Normen, deren Inhalt sich auf internationale Arbeitsergebnisse der Informationsverarbeitung gründet, unter bestimmten Bedingungen allein in englischer Sprache veröffentlicht werden dürfen. Diese Bedingungen sind für den vorliegenden Norm-Entwurf erfüllt.

Da sich die Benutzer des vorliegenden Norm-Entwurfs der englischen Sprache als Fachsprache bedienen, wird die englische Fassung der prEN IEC 62541-7 veröffentlicht. Zu deren Abschnitt 1, der den Anwendungsbereich festlegt, und Unterabschnitt 3.1, der die Begriffe festlegt, wurde eine Übersetzung angefertigt und als informativer Nationaler Anhang NA des vorliegenden Norm-Entwurfs hinzugefügt. Für einige der verwendeten Begriffe existieren keine gebräuchlichen deutschen Benennungen, da sich die deutschen Anwender in der Regel ebenfalls der englischen Benennungen bedienen. Dieser Norm-Entwurf steht nicht in unmittelbarem Zusammenhang mit Rechtsvorschriften und ist nicht als Sicherheitsnorm anzusehen.

Es ist vorgesehen, auch bei der entsprechenden zukünftigen Deutschen Norm auf die deutsche Sprachfassung zu verzichten und diese in der englischsprachigen Fassung zu veröffentlichen.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. IEC ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Documents
Document Sharing Hub

Full document details: E DIN EN IEC 62541-7:2019-09

Das Original-Dokument enthält Bilder in Farbe, die in der Papierversion in einer Graustufen-Darstellung wiedergegeben werden. Elektronische Versionen dieses Dokuments enthalten die Bilder in der originalen Farbdarstellung.

Änderungen

Gegenüber DIN EN 62541-7:2015-11 wurden folgende Änderungen vorgenommen:

a) Neue Funktionsprofile:
   - Profile für globales Discovery- und globales Zertifikatsmanagement;
   - Profile für das Management globaler KeyCredential und das globale Zugangs-Token-Management;
   - Facette für dauerhafte Subskriptionen;
   - Standard-UA-Client-Profil;
   - Profile für die Verwaltung von Benutzerrollen und -genehmigungen;

b) Neue Transportprofile:
   - HTTPS mit JSON-Kodierung;
   - sichere WebSockets (WSS) mit binärer JSON-Kodierung;
   - Rückwärtskonnektivität;

c) Neue Sicherheitsprofile:
   - TransportSicherheit – TLS 1.2 mit PFS (mit Perfect Forward Secrecy);
   - SicherheitsRichtlinie [A] – Aes128-Sha256-RsaOaep (ersetzt Basic128Rsa15);
   - SicherheitsRichtlinie – Aes256-Sha256-RsaPss fügt Perfect Forward Secrecy für UA-TCP hinzu);
   - Benutzer-Token-JWT (Jason-Web-Token);

d) Veraltete Sicherheitsprofile (aufgrund defekter Algorithmen):
   - SicherheitsRichtlinie – Basic128Rsa15 (defekter Algorithmus Sha1);
   - SicherheitsRichtlinie – Basic256 (defekter Algorithmus Sha1);
   - TransportSicherheit – TLS 1.0 (defekter Algorithmus RC4);
   - TransportSicherheit – TLS 1.1 (defekter Algorithmus RC4);

e) Veralteter Transport (fehlende Unterstützung bei den meisten Plattformen):
   - SOAP/HTTP mit WS-SecureConversation (alle Kodierungen)

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62541-7:2019-09

Nationaler Anhang NA
(informativ)

Auszugsweise Übersetzung

Reihenfolge und Inhalt der folgenden Abschnitte sind identisch mit denen in den jeweiligen Abschnitten der Englischen Fassung.

1 Anwendungsbereich

Diese Spezifikation legt die *Profile* der OPC Unified Architecture (OPC-UA) (vereinheitlichte Architektur der plattformunabhängigen Kommunikation) fest. Die *Profile* in diesem Dokument werden verwendet, um die Eigenschaften bezüglich Prüfungen von OPC-UA-Produkten und den Charakter der Prüfungen (basierend auf dem Werkzeug oder basierend auf dem Laboratorium) zu trennen. Dies umfasst die Prüfungen, welche durch das von der OPC-Organisation bereitgestellte OPC-UA-CTT (ein Selbstprüfungswerkzeug) und durch von der OPC-Organisation bereitgestellte unabhängige Prüflaboratorien zur Zertifizierung durchgeführt werden. Dies könnte sich gleichermaßen ebenso auf Prüfwerkzeuge beziehen, welche von einer anderen Organisation oder einem Prüflaboratorium einer anderen Organisation bereitgestellt werden. Wichtig ist das Konzept der automatisierten Prüfung basierend auf dem Werkzeug im Gegensatz zur Prüfung basierend auf dem Laboratorium. Der Anwendungsbereich dieser Norm umfasst die Festlegung der Funktionalität, welche nur in einem Prüflaboratorium geprüft werden kann, und der Festlegung der Gruppierung von Funktionalität, welche bei der Prüfung von OPC-UA-Produkten entweder in einem Laboratorium oder mit automatisierten Werkzeugen zu prüfen ist. Die Festlegung von tatsächlichen *PrüfFällen* (en: TestCases) liegt nicht im Anwendungsbereich dieses Dokuments, aber die allgemeinen Kategorien von PrüfFällen liegen im Anwendungsbereich dieses Dokuments.

Die meisten OPC-UA-Anwendungen stimmen mit einigen, aber nicht allen, dieser *Profile* überein.

3 Begriffe und Abkürzungen

3.1 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach IEC TR 62541-1, IEC TR 62541-2, IEC 62541-3, IEC 62541-4, IEC 62541-6, IEC 62541-8 und die folgenden Begriffe. Ein Überblick der in dieser Norm festgelegten Begriffe und ihrer Beziehung zueinander ist in Bild 1 zu sehen.

ISO und IEC stellen terminologische Datenbanken für die Anwendung in der Normung unter den folgenden Adressen bereit:

- IEC Electropedia: verfügbar unter http://www.electropedia.org/
- ISO Online Browsing Platform: verfügbar unter http://www.iso.org/obp

3.1.1
Anwendung
(en: Application)
Programm, das Aspekte von OPC-UA umsetzt oder bearbeitet

Anmerkung 1 zum Begriff: Die Anwendung kann auf jeder Maschine laufen und jegliche Funktion ausführen. Die Anwendung kann eine Software- oder eine Hardware-Anwendung sein, die einzige Anforderung ist, dass sie OPC-UA umsetzt.

3.1.2
KonformitätsEinheit
(en: ConformanceUnit)
definierte Menge von OPC-UA-Eigenschaften, die als Einheit geprüft werden können

AVA Documents Document Sharing Hub

Full document details: E DIN EN IEC 62541-7:2019-09

Anmerkung 1 zum Begriff: Eine KonformitätsEinheit kann eine Gruppe von Diensten, Teile von Diensten oder Informationsmodelle abdecken.

3.1.3
KonformitätsGruppe
(en: ConformanceGroup)
Gruppierung von KonformitätsEinheiten mit eigenständigen Namen

Anmerkung 1 zum Begriff: Die Gruppierung dient lediglich der Organisation von KonformitätsEinheiten (en: ConformanceUnits). Typische KonformitätsGruppen beinhalten Gruppen für jeden Satz von Diensten in OPC-UA und jede der Informationsmodell-Spezifikationen.

3.1.4
Facette
(en: Facet)
Profil, welches einer spezifischen Eigenschaft zugeordnet ist, die ein Server oder Client benötigen kann

Anmerkung 1 zum Begriff: Facetten werden typischerweise zusammengefasst, um ein Profil einer höheren Ebene zu bilden. Die Verwendung des Begriffs Facette im Titel eines Profils zeigt an, dass das Profil nicht alleine eingesetzt werden kann.

3.1.5
VollAusgestattetesProfil
(en: FullFeatured Profile)
ein Profil, das alles festlegt, was zum Aufbau einer OPC-UA-Anwendung notwendig ist

Anmerkung 1 zum Begriff: Ein VollAusgestattetesProfil fügt insbesondere Definitionen zu Transport- und Sicherheitsvoraussetzungen hinzu.

3.1.6
ProfilKategorie
(en: ProfileCategory)
Arrangiert Profile in Anwendungsklassen, wie z. B. Server oder Client.

Anmerkung 1 zum Begriff: Diese Kategorien helfen Entwicklern und Benutzern, den Typ der Anwendung herauszufinden, in dem ein Profil verwendet werden kann. Weitere Details werden in 4.4 beschrieben.

3.1.7
Prüffall
(en: TestCase)
technische Beschreibung einer Menge von Schritten, die erforderlich sind, eine bestimmte Funktion oder ein bestimmtes Informationsmodell zu testen

Anmerkung 1 zum Begriff: Prüffälle bieten ausreichende Einzelheiten, um einem Entwickler die Umsetzung in Code zu ermöglichen. Prüffälle bieten auch eine genaue Zusammenfassung des (der) erwarteten Ergebnisse(s) bei der Ausführung der Implementierung und alle Vorbedingungen, die erfüllt werden müssen, bevor der Prüffall ausgeführt werden kann.

3.1.8
Prüflabor
(en: TestLab)
Ort, der dafür ausgestattet ist, Prüfdienste bereitzustellen

Anmerkung 1 zum Begriff: Diese Dienste umfassen direkt prüfendes Personal, automatisierte Prüfungen und einen formal wiederholbaren Prozess, sind aber nicht darauf beschränkt. Die OPC-Organisation stellt detaillierte Spezifikationen bereit, welche OPC-UA-Prüflaboratorien festlegen sowie die Prüfungen festlegen, welche diese durchführen müssen (siehe auch

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62541-7:2019-09

– Leerseite –

Documents
Document Sharing Hub

Full document details: E DIN EN IEC 62541-7:2019-09

CONTENTS

FIGURES 7
TABLES 8
FOREWORD 13
1 Scope 16
2 Normative references 16
3 Terms, definitions, and abbreviations 17
3.1 Terms and definitions 17
3.2 Abbreviations 17
4 Overview 18
4.1 General 18
4.2 ConformanceUnit 19
4.3 Profiles 19
4.4 Profile Categories 19
5 Conformance Units 19
5.1 Overview 19
5.2 Services 20
5.3 Transport and communication related features 29
5.4 Information Model and AddressSpace related features 37
5.5 Miscellaneous 53
6 Profiles 54
6.1 Overview 54
6.2 Profile list 55
6.3 Conventions for Profile definitions 59
6.4 Profile versioning 59
6.5 Applications 59
6.6 Profile tables 61
6.6.1 Introduction 61
6.6.2 Core Server Facet 61
6.6.3 Core 2017 Server Facet 61
6.6.4 Sessionless Server Facet 62
6.6.5 Reverse Connect Server Facet 62
6.6.6 Base Server Behaviour Facet 62
6.6.7 Request State Change Server Facet 63
6.6.8 Subnet Discovery Server Facet 63
6.6.9 Global Certificate Management Server Facet 63
6.6.10 Authorization Service Server Facet 63
6.6.11 KeyCredential Service Server Facet 63
6.6.12 Attribute WriteMask Server Facet 64
6.6.13 File Access Server Facet 64
6.6.14 Documentation Server Facet 64
6.6.15 Embedded DataChange Subscription Server Facet 64
6.6.16 Standard DataChange Subscription Server Facet 65
6.6.17 Standard DataChange Subscription 2017 Server Facet 65
6.6.18 Enhanced DataChange Subscription Server Facet 65
6.6.19 Enhanced DataChange Subscription 2017 Server Facet 65
6.6.20 Durable Subscription Server Facet 66

AVA Documents Document Sharing Hub
Full document details: E DIN EN IEC 62541-7:2019-09

6.6.21 Data Access Server Facet 66
6.6.22 ComplexType Server Facet 66
6.6.23 ComplexType 2017 Server Facet 66
6.6.24 Standard Event Subscription Server Facet 67
6.6.25 Address Space Notifier Server Facet 67
6.6.26 A & C Base Condition Server Facet 67
6.6.27 A & C Refresh2 Server Facet 68
6.6.28 A & C Address Space Instance Server Facet 68
6.6.29 A & C Enable Server Facet 68
6.6.30 A & C AlarmMetrics Server Facet 68
6.6.31 A & C Alarm Server Facet 68
6.6.32 A & C Acknowledgeable Alarm Server Facet 69
6.6.33 A & C Exclusive Alarming Server Facet 69
6.6.34 A & C Non-Exclusive Alarming Server Facet 70
6.6.35 A & C Previous Instances Server Facet 70
6.6.36 A & C Dialog Server Facet 70
6.6.37 A & C CertificateExpiration Server Facet 70
6.6.38 A & E Wrapper Facet 71
6.6.39 Method Server Facet 71
6.6.40 Auditing Server Facet 71
6.6.41 Node Management Server Facet 72
6.6.42 User Role Base Server Facet 72
6.6.43 User Role Management Server Facet 72
6.6.44 State Machine Server Facet 73
6.6.45 Client Redundancy Server Facet 73
6.6.46 Redundancy Transparent Server Facet 73
6.6.47 Redundancy Visible Server Facet 73
6.6.48 Historical Raw Data Server Facet 73
6.6.49 Historical Aggregate Server Facet 74
6.6.50 Historical Data AtTime Server Facet 75
6.6.51 Historical Access Modified Data Server Facet 75
6.6.52 Historical Annotation Server Facet 75
6.6.53 Historical Data Insert Server Facet 75
6.6.54 Historical Data Update Server Facet 75
6.6.55 Historical Data Replace Server Facet 76
6.6.56 Historical Data Delete Server Facet 76
6.6.57 Historical Access Structured Data Server Facet 76
6.6.58 Base Historical Event Server Facet 76
6.6.59 Historical Event Update Server Facet 76
6.6.60 Historical Event Replace Server Facet 77
6.6.61 Historical Event Insert Server Facet 77
6.6.62 Historical Event Delete Server Facet 77
6.6.63 Aggregate Subscription Server Facet 77
6.6.64 Nano Embedded Device Server Profile 78
6.6.65 Nano Embedded Device 2017 Server Profile 78
6.6.66 Micro Embedded Device Server Profile 78
6.6.67 Micro Embedded Device 2017 Server Profile 79
6.6.68 Embedded UA Server Profile 79
6.6.69 Embedded 2017 UA Server Profile 79

AVA Documents Document Sharing Hub
Full document details: E DIN EN IEC 62541-7:2019-09

6.6.70 Standard UA Server Profile 79
6.6.71 Standard 2017 UA Server Profile 79
6.6.72 Core Client Facet 80
6.6.73 Core 2017 Client Facet 80
6.6.74 Sessionless Client Facet 80
6.6.75 Reverse Connect Client Facet 80
6.6.76 Base Client Behaviour Facet 81
6.6.77 Discovery Client Facet 81
6.6.78 Subnet Discovery Client Facet 81
6.6.79 Global Discovery Client Facet 81
6.6.80 Global Certificate Management Client Facet 82
6.6.81 KeyCredential Service Client Facet 82
6.6.82 Access Token Request Client Facet 82
6.6.83 AddressSpace Lookup Client Facet 82
6.6.84 Request State Change Client Facet 83
6.6.85 File Access Client Facet 83
6.6.86 Entry Level Support 2015 Client Facet 83
6.6.87 Multi-Server Client Connection Facet 83
6.6.88 Documentation – Client 83
6.6.89 Attribute Read Client Facet 84
6.6.90 Attribute Write Client Facet 84
6.6.91 DataChange Subscriber Client Facet 84
6.6.92 Durable Subscription Client Facet 85
6.6.93 DataAccess Client Facet 85
6.6.94 Event Subscriber Client Facet 85
6.6.95 Base Event Processing Client Facet 85
6.6.96 Notifier and Source Hierarchy Client Facet 86
6.6.97 A & C Base Condition Client Facet 86
6.6.98 A & C Refresh2 Client Facet 86
6.6.99 A & C Address Space Instance Client Facet 86
6.6.100 A & C Enable Client Facet 87
6.6.101 A & C AlarmMetrics Client Facet 87
6.6.102 A & C Alarm Client Facet 87
6.6.103 A & C Exclusive Alarming Client Facet 87
6.6.104 A & C Non-Exclusive Alarming Client Facet 88
6.6.105 A & C Previous Instances Client Facet 88
6.6.106 A & C Dialog Client Facet 88
6.6.107 A & C CertificateExpiration Client Facet 88
6.6.108 A & E Proxy Facet 89
6.6.109 Method Client Facet 89
6.6.110 Auditing Client Facet 90
6.6.111 Node Management Client Facet 90
6.6.112 Advanced Type Programming Client Facet 90
6.6.113 User Role Management Client Facet 90
6.6.114 State Machine Client Facet 91
6.6.115 Diagnostic Client Facet 91
6.6.116 Redundant Client Facet 91
6.6.117 Redundancy Switch Client Facet 91
6.6.118 Historical Access Client Facet 91

AVA Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62541-7:2019-09

6.6.119 Historical Data AtTime Client Facet 91
6.6.120 Historical Aggregate Client Facet 92
6.6.121 Historical Annotation Client Facet 92
6.6.122 Historical Access Modified Data Client Facet 93
6.6.123 Historical Data Insert Client Facet 93
6.6.124 Historical Data Update Client Facet 93
6.6.125 Historical Data Replace Client Facet 93
6.6.126 Historical Data Delete Client Facet 93
6.6.127 Historical Access Client Server Timestamp Facet 94
6.6.128 Historical Structured Data Access Client Facet 94
6.6.129 Historical Structured Data AtTime Client Facet 94
6.6.130 Historical Structured Data Modified Client Facet 94
6.6.131 Historical Structured Data Insert Client Facet 94
6.6.132 Historical Structured Data Update Client Facet 94
6.6.133 Historical Structured Data Replace Client Facet 95
6.6.134 Historical Structured Data Delete Client Facet 95
6.6.135 Historical Events Client Facet 95
6.6.136 Historical Event Insert Client Facet 95
6.6.137 Historical Event Update Client Facet 95
6.6.138 Historical Event Replace Client Facet 96
6.6.139 Historical Event Delete Client Facet 96
6.6.140 Aggregate Subscriber Client Facet 96
6.6.141 Standard UA Client Profile 97
6.6.142 Standard UA Client 2017 Profile 97
6.6.143 UA-TCP UA-SC UA-Binary 98
6.6.144 HTTPS UA-Binary 98
6.6.145 HTTPS UA-XML 98
6.6.146 HTTPS UA-JSON 98
6.6.147 WSS UA-SC UA-Binary 99
6.6.148 WSS UA-JSON 99
6.6.149 Security User Access Control Full 99
6.6.150 Security User Access Control Base 99
6.6.151 Security Time Synchronization 99
6.6.152 Best Practice – Audit Events 100
6.6.153 Best Practice – Alarm Handling 100
6.6.154 Best Practice – Random Numbers 100
6.6.155 Best Practice – Timeouts 100
6.6.156 Best Practice – Administrative Access 100
6.6.157 Best Practice – Strict Message Handling 101
6.6.158 Best Practice – Audit Events Client 101
6.6.159 TransportSecurity – TLS 1.2 101
6.6.160 TransportSecurity – TLS 1.2 with PFS 101
6.6.161 SecurityPolicy – None 101
6.6.162 SecurityPolicy – Basic128Rsa15 102
6.6.163 SecurityPolicy – Basic256 102
6.6.164 SecurityPolicy [A] - Aes128-Sha256-RsaOaep 102
6.6.165 SecurityPolicy [B] – Basic256Sha256 102
6.6.166 SecurityPolicy - Aes256-Sha256-RsaPss 103
6.6.167 User Token – Anonymous Facet 103

AVA Documents Document Sharing Hub
Full document details: E DIN EN IEC 62541-7:2019-09

6.6.168 User Token – User Name Password Server Facet 103
6.6.169 User Token – X509 Certificate Server Facet 104
6.6.170 User Token – Issued Token Server Facet 104
6.6.171 User Token – Issued Token Windows Server Facet 104
6.6.172 User Token – JWT Server Facet 104
6.6.173 User Token – User Name Password Client Facet 104
6.6.174 User Token – X509 Certificate Client Facet 105
6.6.175 User Token – Issued Token Client Facet 105
6.6.176 User Token – Issued Token Windows Client Facet 105
6.6.177 User Token – JWT Client Facet 105
6.6.178 Global Discovery Server Profile 105
6.6.179 Global Discovery Server 2017 Profile 105
6.6.180 Global Discovery and Certificate Management Server 106
6.6.181 Global Discovery and Certificate Mgmt 2017 Server 106
6.6.182 Global Certificate Management Client Profile 106
6.6.183 Global Certificate Management Client 2017 Profile 106
6.6.184 Global Service Authorization Request Server Facet 107
6.6.185 Global Service KeyCredential Pull Facet 107
6.6.186 Global Service KeyCredential Push Facet 107

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62541-7:2019-09

FIGURES

Figure 1 – Profile – ConformanceUnit – TestCases 18
Figure 2 – HMI Client sample 60
Figure 3 – Embedded Server sample..... 60
Figure 4 – Standard UA Server sample 61

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62541-7:2019-09

TABLES

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 26
Table 10 – Subscription Services 28
Table 11 – Security 29
Table 12 – Protocol and Encoding 36
Table 13 – Base Information 37
Table 14 – Address Space Model 39
Table 15 – Data Access 41
Table 16 – Alarms and Conditions 42
Table 17 – Historical Access 44
Table 18 – Aggregates 47
Table 19 – Auditing 52
Table 20 – Redundancy 52
Table 21 – Global Discovery Server 53
Table 22 – Miscellaneous 53
Table 23 – Profile list 55
Table 24 – Core 2017 Server Facet 62
Table 25 – Sessionless Server Facet 62
Table 26 – Reverse Connect Server Facet 62
Table 27 – Base Server Behaviour Facet 63
Table 28 – Request State Change Server Facet 63
Table 29 – Subnet Discovery Server Facet 63
Table 30 – Global Certificate Management Server Facet 63
Table 31 – Authorization Service Server Facet 63
Table 32 – KeyCredential Service Server Facet 64
Table 33 – Attribute WriteMask Server Facet 64
Table 34 – File Access Server Facet 64
Table 35 – Documentation Server Facet 64
Table 36 – Embedded DataChange Subscription Server Facet 64
Table 37 – Standard DataChange Subscription 2017 Server Facet 65
Table 38 – Enhanced DataChange Subscription 2017 Server Facet 65
Table 39 – Durable Subscription Server Facet 66
Table 40 – Data Access Server Facet 66
Table 41 – ComplexType 2017 Server Facet 66

AVA Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62541-7:2019-09

Table 42 – Standard Event Subscription Server Facet 67
Table 43 – Address Space Notifier Server Facet 67
Table 44 – A & C Base Condition Server Facet 68
Table 45 – A & C Refresh2 Server Facet 68
Table 46 – A & C Address Space Instance Server Facet 68
Table 47 – A & C Enable Server Facet 68
Table 48 – A & C AlarmMetrics Server Facet 68
Table 49 – A & C Alarm Server Facet 69
Table 50 – A & C Acknowledgeable Alarm Server Facet 69
Table 51 – A & C Exclusive Alarming Server Facet 69
Table 52 – A & C Non-Exclusive Alarming Server Facet 70
Table 53 – A & C Previous Instances Server Facet 70
Table 54 – A & C Dialog Server Facet 70
Table 55 – A & C CertificateExpiration Server Facet 70
Table 56 – A & E Wrapper Facet 71
Table 57 – Method Server Facet 71
Table 58 – Auditing Server Facet 72
Table 59 – Node Management Server Facet 72
Table 60 – User Role Base Server Facet 72
Table 61 – User Role Management Server Facet 72
Table 62 – State Machine Server Facet 73
Table 63 – Client Redundancy Server Facet 73
Table 64 – Redundancy Transparent Server Facet 73
Table 65 – Redundancy Visible Server Facet 73
Table 66 – Historical Raw Data Server Facet 73
Table 67 – Historical Aggregate Server Facet 74
Table 68 – Historical Data AtTime Server Facet 75
Table 69 – Historical Access Modified Data Server Facet 75
Table 70 – Historical Annotation Server Facet 75
Table 71 – Historical Data Insert Server Facet 75
Table 72 – Historical Data Update Server Facet 75
Table 73 – Historical Data Replace Server Facet 76
Table 74 – Historical Data Delete Server Facet 76
Table 75 – Historical Access Structured Data Server Facet 76
Table 76 – Base Historical Event Server Facet 76
Table 77 – Historical Event Update Server Facet 76
Table 78 – Historical Event Replace Server Facet 77
Table 79 – Historical Event Insert Server Facet 77
Table 80 – Historical Event Delete Server Facet 77
Table 81 – Aggregate Subscription Server Facet 77
Table 82 – Nano Embedded Device 2017 Server Profile 78
Table 83 – Micro Embedded Device 2017 Server Profile 79
Table 84 – Embedded 2017 UA Server Profile 79

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62541-7:2019-09

Table 85 – Standard 2017 UA Server Profile 79
Table 86 – Core 2017 Client Facet 80
Table 87 – Sessionless Client Facet 80
Table 88 – Reverse Connect Client Facet 81
Table 89 – Base Client Behaviour Facet 81
Table 90 – Discovery Client Facet 81
Table 91 – Subnet Discovery Client Facet 81
Table 92 – Global Discovery Client Facet 82
Table 93 – Global Certificate Management Client Facet 82
Table 94 – KeyCredential Service Client Facet 82
Table 95 – Access Token Request Client Facet 82
Table 96 – AddressSpace Lookup Client Facet 82
Table 97 – Request State Change Client Facet 83
Table 98 – File Access Client Facet 83
Table 99 – Entry Level Support 2015 Client Facet 83
Table 100 – Multi-Server Client Connection Facet 83
Table 101 – Documentation – Client 83
Table 102 – Attribute Read Client Facet 84
Table 103 – Attribute Write Client Facet 84
Table 104 – DataChange Subscriber Client Facet 84
Table 105 – Durable Subscription Client Facet 85
Table 106 – DataAccess Client Facet 85
Table 107 – Event Subscriber Client Facet 85
Table 108 – Base Event Processing Client Facet 86
Table 109 – Notifier and Source Hierarchy Client Facet 86
Table 110 – A & C Base Condition Client Facet 86
Table 111 – A & C Refresh2 Client Facet 86
Table 112 – A & C Address Space Instance Client Facet 86
Table 113 – A & C Enable Client Facet 87
Table 114 – A & C AlarmMetrics Client Facet 87
Table 115 – A & C Alarm Client Facet 87
Table 116 – A & C Exclusive Alarming Client Facet 87
Table 117 – A & C Non-Exclusive Alarming Client Facet 88
Table 118 – A & C Previous Instances Client Facet 88
Table 119 – A & C Dialog Client Facet 88
Table 120 – A & C CertificateExpiration Client Facet 88
Table 121 – A & E Proxy Facet 89
Table 122 – Method Client Facet 90
Table 123 – Auditing Client Facet 90
Table 124 – Node Management Client Facet 90
Table 125 – Advanced Type Programming Client Facet 90
Table 126 – User Role Management Client Facet 90
Table 127 – State Machine Client Facet 91

AVA Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62541-7:2019-09

Table 128 – Diagnostic Client Facet 91
Table 129 – Redundant Client Facet 91
Table 130 – Redundancy Switch Client Facet 91
Table 131 – Historical Access Client Facet 91
Table 132 – Historical Data AtTime Client Facet 92
Table 133 – Historical Aggregate Client Facet 92
Table 134 – Historical Annotation Client Facet 93
Table 135 – Historical Access Modified Data Client Facet 93
Table 136 – Historical Data Insert Client Facet 93
Table 137 – Historical Data Update Client Facet 93
Table 138 – Historical Data Replace Client Facet 93
Table 139 – Historical Data Delete Client Facet 93
Table 140 – Historical Access Client Server Timestamp Facet 94
Table 141 – Historical Structured Data Access Client Facet 94
Table 142 – Historical Structured Data AtTime Client Facet 94
Table 143 – Historical Structured Data Modified Client Facet 94
Table 144 – Historical Structured Data Insert Client Facet 94
Table 145 – Historical Structured Data Update Client Facet 95
Table 146 – Historical Structured Data Replace Client Facet 95
Table 147 – Historical Structured Data Delete Client Facet 95
Table 148 – Historical Events Client Facet 95
Table 149 – Historical Event Insert Client Facet 95
Table 150 – Historical Event Update Client Facet 95
Table 151 – Historical Event Replace Client Facet 96
Table 152 – Historical Event Delete Client Facet 96
Table 153 – Aggregate Subscriber Client Facet 96
Table 154 – Standard UA Client 2017 Profile 97
Table 155 – UA-TCP UA-SC UA-Binary 98
Table 156 – HTTPS UA-Binary 98
Table 157 – HTTPS UA-XML 98
Table 158 – HTTPS UA-JSON 98
Table 159 – WSS UA-SC UA-Binary 99
Table 160 – WSS UA-JSON 99
Table 161 – Security User Access Control Full 99
Table 162 – Security User Access Control Base 99
Table 163 – Security Time Synchronization 100
Table 164 – Best Practice – Audit Events 100
Table 165 – Best Practice – Alarm Handling 100
Table 166 – Best Practice – Random Numbers 100
Table 167 – Best Practice – Timeouts 100
Table 168 – Best Practice – Administrative Access 100
Table 169 – Best Practice – Strict Message Handling 101
Table 170 – Best Practice – Audit Events Client 101

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62541-7:2019-09

Table 171 – TransportSecurity – TLS 1.2 101
Table 172 – TransportSecurity – TLS 1.2 with PFS 101
Table 173 – SecurityPolicy – None 102
Table 174 – SecurityPolicy [A] - Aes128-Sha256-RsaOaep 102
Table 175 – SecurityPolicy [B] – Basic256Sha256 103
Table 176 – SecurityPolicy - Aes256-Sha256-RsaPss 103
Table 177 – User Token – Anonymous Facet 103
Table 178 – User Token – User Name Password Server Facet 103
Table 179 – User Token – X509 Certificate Server Facet 104
Table 180 – User Token – Issued Token Server Facet 104
Table 181 – User Token – Issued Token Windows Server Facet 104
Table 182 – User Token – JWT Server Facet 104
Table 183 – User Token – User Name Password Client Facet 104
Table 184 – User Token – X509 Certificate Client Facet 105
Table 185 – User Token – Issued Token Client Facet 105
Table 186 – User Token – Issued Token Windows Client Facet 105
Table 187 – User Token – JWT Client Facet 105
Table 188 – Global Discovery Server 2017 Profile 105
Table 189 – Global Discovery and Certificate Mgmt 2017 Server 106
Table 190 – Global Certificate Management Client 2017 Profile 106
Table 191 – Global Service Authorization Request Server Facet 107
Table 192 – Global Service KeyCredential Pull Facet 107
Table 193 – Global Service KeyCredential Push Facet 107

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62541-7:2019-09

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.

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 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.

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

Enquiry draft	Report on voting
65E/XX/DTR	65E/XX/RVC

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 third edition cancels and replaces the second edition of IEC 62541, published in 2015.

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

a) New functional Profiles:

AVA Documents Document Sharing Hub

- 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)

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.

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62541-7:2019-09

95

96 The National Committees are requested to note that for this publication the stability date is 2021.

97 THIS TEXT IS INCLUDED FOR THE INFORMATION OF THE NATIONAL COMMITTEES AND WILL BE DELETED AT
98 THE PUBLICATION STAGE.

99 A bilingual version of this publication may be issued at a later date.

100

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.

101
102
103

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62541-7:2019-09

OPC Unified Architecture Specification

Part 7: Profiles

1 Scope

This part describes 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 an 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 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 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*

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

Test Specifications

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/

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62541-7:2019-09

3 Terms, definitions, and abbreviations

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC TR 62541-1, IEC TR 62541-2, IEC 62541-3, IEC 62541-4, IEC 62541-6, and IEC 62541-8 as well as the following apply. An overview of the terms defined in this standard and their interaction can be viewed in Figure 1.

3.1.1
application
a software program that executes or implements some aspect of OPC UA

Note 1 to entry: The application could run on any machine and perform any function. The application could be software or it could be a hardware application, the only requirement is that it implements OPC UA.

3.1.2
ConformanceUnit
a specific set of OPC UA features that can be tested as a single entity

Note 1 to entry: A ConformanceUnit can cover a group of services, portions of services or information models.

3.1.3
ConformanceGroup
a group of ConformanceUnits that is given a name

Note 1 to entry: This grouping is only to assist in organizing ConformanceUnits. Typical ConformanceGroups include groups for each of the service sets in OPC UA and each of the Information Model standards.

3.1.4
Facet
a Profile dedicated to a specific feature that a Server or Client may require

Note 1 to entry: Facets are typically combined to form higher-level Profiles. The use of the term Facet in the title of a Profile indicates that the given Profile is not a standalone Profile.

3.1.5
FullFeatured Profile
a Profile that defines all features necessary to build a functional OPC UA Application

Note 1 to entry: A FullFeatured Profile in particular adds definitions of the transport and security requirements.

3.1.6
ProfileCategory
arranges Profiles into application classes, such as Server or Client

Note 1 to entry: These categories help determine the type of Application that a given Profile would be used for. For additional details see 4.4.

3.1.7
TestCase
a technical description of a set of steps required to test a particular function or information model

Note 1 to entry: TestCases provide sufficient details to allow a developer to implement them in code. TestCases also provide a detailed summary of the expected result(s) from the execution of the implemented code and any precondition(s) that must be established before the TestCase can be executed.

3.1.8
TestLab
a facility that is designated to provide testing services

Note 1 to entry: These services include but are not limited to personal that directly perform testing, automated testing and a formal repeatable process. The OPC Foundation has provided detailed standard describing OPC UA TestLabs and the testing they are to provided (see Compliance Part 8 UA Server, Compliance Part 9 UA Client).

3.2 Abbreviations

DA Data Access

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62541-7:2019-09

HA	Historical Access
HMI	Human Machine Interface
NIST	National Institute of Standard and Technology
PKI	Public Key Infrastructure
RSA	Rivest-Shamir-Adleman
UA	Unified Architecture

4 Overview

4.1 General

The OPC Unified architecture multipart standard describes a number of *Services* and a variety of information models. These *Services* and information models can be referred to as features of a *Server* or *Client*. *Servers* and *Clients* need to be able to describe which features they support and wish to have certified. This document provides a grouping of these features. The individual features are grouped into *ConformanceUnits* which are further grouped into *Profiles*. Figure 1 provides an overview of the interactions between *Profiles*, *ConformanceUnits* and *TestCases*. The large arrows indicate the components that are used to construct the parent. For example a *Profile* is constructed from *Profiles* and *ConformanceUnits*. The figure also illustrates a feature of the OPC UA Compliance Test Tool (CTT), in that it will test if a requested *Profile* passes all *ConformanceUnits*. It will also test all other *ConformanceUnits* and report any other *Profiles* that pass conformance testing. The individual *TestCases* are defined in separate documents see Compliance Part 8 UA Server and Compliance Part 9 UA Client. The *TestCases* are related back to the appropriate *ConformanceUnits* defined in this standard. This relationship is also displayed by the OPC UA Compliance Test Tool.

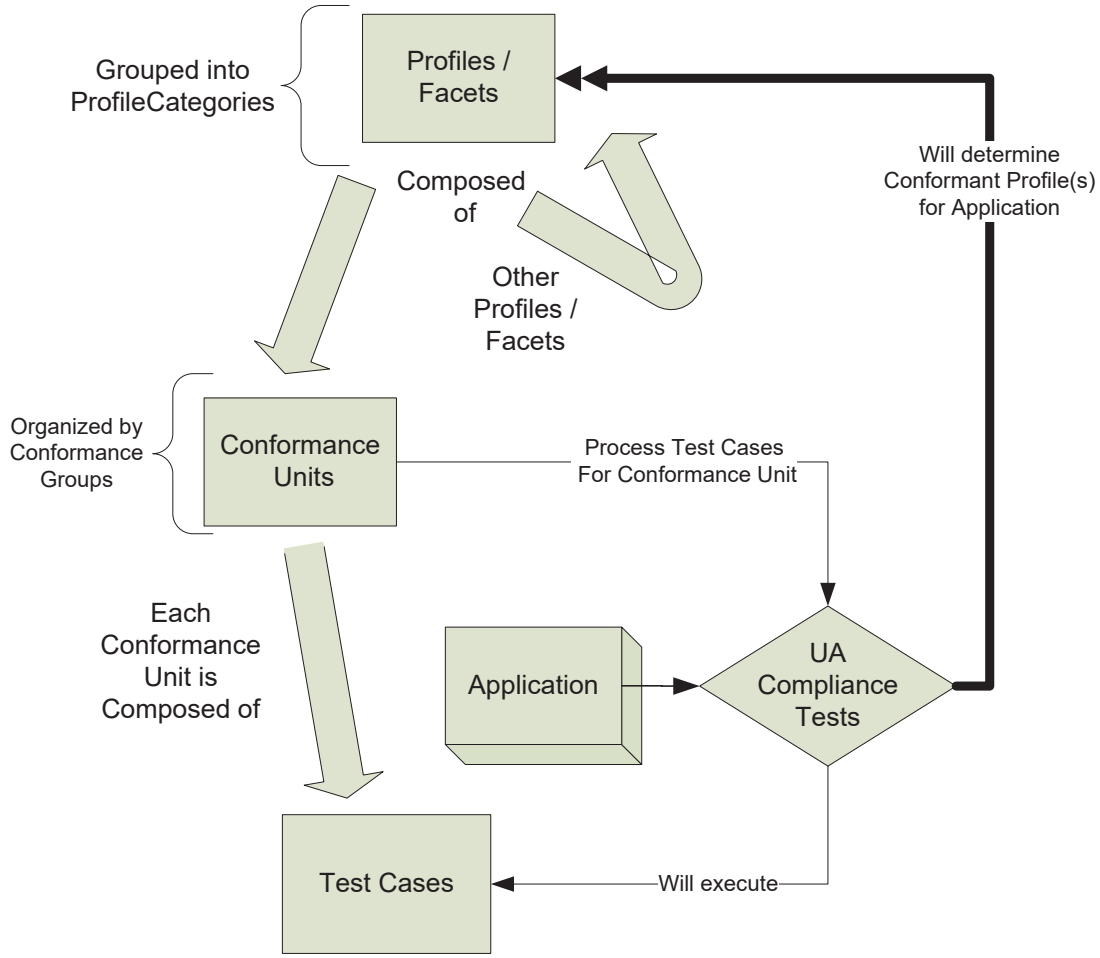

Figure 1 – Profile – ConformanceUnit – TestCases

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62541-7:2019-09

4.2 ConformanceUnit

Each *ConformanceUnit* represents a specific set of features (e.g. a group of services, portions of services or information models) that can be tested as a single entity. *ConformanceUnits* are the building blocks of a *Profile*. Each *ConformanceUnit* can also be used as a test category. For each *ConformanceUnit,* there would be a number of TestCases that test the functionality described by the *ConformanceUnit.* The description of a *ConformanceUnit* is intended to provide enough information to illustrate the required functionality, but in many cases to obtain a complete understanding of the *ConformanceUnit* the reader may be required to also examine the appropriate part of OPC UA. Additional Information regarding testing of a *ConformanceUnit* are provided in the Compliance Part 8 UA Server or Compliance Part 9 UA Client test standards.

The same features do not appear in more than one *ConformanceUnit*.

4.3 Profiles

A *Profile* is a named aggregation of *ConformanceUnits* and other *Profiles*. To support a *Profile*, an application has to support the *ConformanceUnits* and all aggregated *Profiles*. The definition of *Profiles* is an ongoing activity, in that it is expected that new *Profiles* will be added in the future.

An OPC UA Application will typically support multiple *Profiles*.

Multiple *Profiles* may include the same *ConformanceUnit*.

Testing of a *Profile* consists of testing the individual *ConformanceUnits* that comprise the *Profile*.

Profiles are named based on naming conventions (see 6.3 for details).

4.4 Profile Categories

Profiles are grouped into categories to help vendors and end users understand the applicability of a *Profile*. A *Profile* can be assigned to more than one category.

Table 1 – Profile Categories contains the list of currently defined *ProfileCategories*.

Table 1 – Profile Categories

Category	Description
Client	*Profiles* of this category specify functions of an OPC UA *Client*.
Global Directory *Service*	*Profiles* of this category specify functions for global discovery and certificate management.
Security	*Profiles* of this category specify security related functions. Security policies are part of this category. The URI of security policies has to be part of an Endpoint Description returned from the GetEndpoints service. *Profiles* of this category apply to *Clients* and *Servers*.
Server	*Profiles* of this category specify functions of an OPC UA *Server*. The URI of such *Profiles* can be exposed in the *Server* capabilities.
Transport	*Profiles* of this category specify specific protocol mappings. The URI of such *Profiles* has to be part of an Endpoint Description. These *Profiles* apply to *Clients* and *Servers*.

5 Conformance Units

5.1 Overview

A *ConformanceUnit* represents an individually testable entity. For improved clarity, the large list of *ConformanceUnits* is arranged into named *ConformanceGroups*. These groups reflect the *Service Sets* in IEC 62541-4 and the OPC UA information models. Table 2 lists the *ConformanceGroups*. These groups and the *ConformanceUnits* that they describe are detailed in the Subclauses of chapter 5 starting with clause 5.2. *ConformanceGroups* have no impact

AVA Documents Document Sharing Hub
Full document details: E DIN EN IEC 62541-7:2019-09

on testing; they are used only for organizational reasons, i.e. to simplify the readability of this document.

Table 2 – Conformance Groups

Group	Description
Address Space Model	Defines *ConformanceUnits* for various features of the OPC UA *AddressSpace*.
Aggregates	All *ConformanceUnits* that are related to Aggregates, including individual *ConformanceUnits* for each supported Aggregate as described in Part 13.
Alarms and *Conditions*	All *ConformanceUnits* that are associated with the OPC UA Information Model for *Conditions*, acknowledgeable *Conditions*, confirmations and *Alarms* as specified in Part 9.
Attribute Services	Includes *ConformanceUnits* to read or write current or historical *Attribute* values.
Auditing	User level security includes support for security audit trails, with traceability between *Client* and *Server* audit logs.
Base Information	All information elements as defined in Part 5.
Data Access	*ConformanceUnits* specific to *Clients* and *Servers* that deal with the representation and use of automation data as specified in Part 8.
Discovery Services	*ConformanceUnits* which focus on *Server* Endpoint *Discovery*.
GDS	Conformance Units for a GDS. Includes units for global discovery and global certificate management.
Historical Access	Access to archived data of *Node Attribute* values or Events.
Method Services	Methods represent the function calls of *Objects*. Methods are invoked and return only after completion (successful or unsuccessful).
Miscellaneous	This group contains *ConformanceUnits* that cover miscellaneous subjects, such as recommended behaviours, documentation etc. These *ConformanceUnits* typically do not fit into any of the other groups.
Monitored Item *Services*	*Clients* define *MonitoredItems* to subscribe to data and Events. Each *MonitoredItem* identifies the item to be monitored and the *Subscription* to use to send *Notifications*.
Node Management *Services*	Bundles *ConformanceUnits* for all *Services* to add and delete OPC UA *AddressSpace Nodes* and *References*.
Protocol and Encoding	Covers all transport and encoding combinations that are specified in Part 6.
Redundancy	The design of OPC UA ensures that vendors can create redundant *Clients* and redundant *Servers* in a consistent manner. Redundancy may be used for high availability, fault tolerance and load balancing.
Security	Security related *ConformanceUnits* that can be profiled this includes all aspects of security.
Session Services	An (OPC UA) *Session* is an application layer connection.
Subscription Services	Subscriptions are used to report *Notifications* to the *Client*.
View *Services*	*Clients* use the View *Service* Set to navigate through the OPC UA *AddressSpace* or through a View (a subset) of the OPC UA *AddressSpace*.

5.2 Services

The following tables describe *ConformanceUnits* for the *Services* specified in IEC 62541-4. The tables correlate with the *Service Sets*.

A single *ConformanceUnit* can reference several *Services* (e.g. CreateSession, ActivateSession and CloseSession) but can also refer to individual aspects of *Services* (e.g. the use of ActivateSession to impersonate a new user).

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62541-7:2019-09

Each table includes a listing of the *Profile Category* to which a *ConformanceUnit* belongs, the title and description of the *ConformanceUnit*. In some cases, a *ConformanceUnit* will be derived from another *ConformanceUnit*. This parent unit will then be specified in the description of each derived unit. In such cases the derived units inherit all of the tests of its parent plus one or more additional TestCases. These TestCases can only further restrict the existing TestCases. An example would be one in which the number of connections is tested, where the TestCase of the parent required at least one connection and the derived *ConformanceUnit* would require a *TestCase* for at least five connections.

The *Discovery Service* Set is composed of multiple *ConformanceUnits* (see Table 3). All *Servers* provide some aspects of this functionality; see *Profiles* categorized as *Server Profiles* for details. *Clients* may support some aspects of this functionality; see *Profiles* categorized as *Client Profiles* for details.

Table 3 – Discovery Services

Category	Title	Description
Server	*Discovery* Get Endpoints	Support the GetEndpoints *Service* to obtain all Endpoints of the *Server*. This includes filtering based on *Profiles*.
Server	*Discovery* Get Endpoints SessionLess	Support at least one endpoint for issueing SessionLess Services. Support obtaining such endpoints by accepting the Transport URI as a filter to the GetEndpoints Service with the query string "SL" appended to the Transport URI. E.g. "http://opcfoundation.org/UA-Profile/Transport/https-uajson?SL"
Server	*Discovery* Find *Servers* Self	Support the FindServers *Service* only for itself.
Server	*Discovery* Register	Call the RegisterServer *Service* to register itself (OPC UA *Server*) with an external *Discovery Service* via a secure channel with a SecurityMode other than NONE.
Server	*Discovery* Register2	Call the RegisterServer2 *Service* to register with an external *Discovery Service* via a Secure Channel with a SecurityMode other than "None". This includes passing a list of short capability identifiers. The identifiers and their use are specified in Part 12.
Server	*Discovery Server* Announcement using mDNS	Provide mDNS functionality to announce a *Server* with its capabilities. The capability identifiers and the use of mDNS records for the purpose of OPC UA *Discovery* is specified in Part 12. Note that this functionality is only required for *Servers* that do not register with an LDS. The capability identifiers and their use in mDNS records are specified in Part 12.
Server	*Discovery* Configuration	Allow configuration of the *Discovery Server* URL where the *Server* will register itself. Allow complete disabling of registration with a *Discovery Server*.
Client	*Discovery Client* Find *Servers* Basic	Uses the FindServers *Service* to obtain all *Servers* installed on a given platform.
Client	*Discovery Client* Find *Servers* with URI	Use FindServers *Service* to obtain URLs for specific *Server* URIs.
Client	*Discovery Client* Find *Servers* Dynamic	Detect new *Servers* after an initial FindServers *Service* call.
Client	*Discovery Client* Find *Servers* on Network	Support one of the options to locate *Servers* on the network.

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62541-7:2019-09

Category	Title	Description
Client	*Discovery Client* Find *Servers* on Network using LDS-ME	Use FindServersOnNetwork *Service* to obtain URLs for specific *Server* URIs. Note that this *Service* is available via the Local *Discovery Server* with multicast extension (LDS-ME).
Client	*Discovery Client* Find *Servers* on Network using mDNS	Use mDNS based *Service Discovery* to locate *Servers* on the same multicast network. The contents of mDNS records for OPC UA *Discovery* are described in Part 12. Note that this functionality is only required for *Clients* when there is no Local *Discovery Server* with multicast extension (LDS-ME). The capability identifiers and their use in mDNS records are specified in Part 12.
Client	*Discovery Client* Find *Servers* in GDS	Use the QueryServers *Method* on the GDS Directory *Object* to locate *Servers* that meet filter criteria specified in the request. This *Method* is specified in Part 12.
Client	*Discovery Client* Find Applications in GDS	Use the QueryApplications *Method* on the GDS Directory *Object* to locate Applications that meet filter criteria specified in the request. This *Method* is specified in Part 12.
Client	*Discovery Client* Get Endpoints Basic	Uses the GetEndpoints *Service* to obtain all Endpoints for a given *Server* URI.
Client	*Discovery Client* Get Endpoints SessionLess	Uses the GetEndpoints *Service* with a filter to obtain Endpoints that can be used for SessionLess *Service* invocation. The filter is the Transport URI extended with the query string "SL". E.g. http://opcfoundation.org/UA-*Profile*/Transport/https-uajson?SL.
Client	*Discovery Client* Get Endpoints Dynamic	Detect changes to the Endpoints after an initial GetEndpoints *Service* call.
Client	*Discovery Client* Configure Endpoint	Allow specification of an Endpoint without going through the *Discovery Service* Set.

The *Session Service* Set is composed of multiple *ConformanceUnits* (see Table 4). The CreateSession, ActivateSession, and CloseSession services are supported as a single unit. All *Servers* and *Clients* provide this functionality.

Table 4 – Session Services

Category	Title	Description
Server	*Session* General *Service* Behaviour	Implement basic *Service* behaviour. This includes in particular: – checking the authentication token – returning the requestHandle in responses – returning available diagnostic information as requested with the 'returnDiagnostics' parameter – respecting a timeoutHint
Server	*Session* Base	Support the *Session Service* Set (CreateSession, ActivateSession, CloseSession) except the use of ActivateSession to change the *Session* user. This includes correct handling of all parameters that are provided. Note that for the CreateSession and ActivateSession services, if the SecurityMode = None then: 1) The Application *Certificate* and Nonce are optional. 2) The signatures are null/empty. The details of this are described in Part 4.

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62541-7:2019-09

Category	Title	Description
Server	*Session* Change User	Support the use of ActivateSession to change the *Session* user.
Server	*Session* Cancel	Support the Cancel *Service* to cancel outstanding requests.
Server	*Session* Minimum 1	Support minimum 1 *Session* (total).
Server	*Session* Minimum 2 Parallel	Support minimum 2 parallel Sessions (total for all *Clients*).
Server	*Session* Minimum 50 Parallel	Support minimum 50 parallel Sessions (total for all *Clients*).
Server	Session Sessionless Invocation	Defines the support of the SessionlessInvoke Service defined in UA Part 4 to process any of the Services (like Read/Write, Browse, or Call) that are designated for Session-less invocation.
Client	*Session Client* General *Service* Behaviour	Implement basic *Service* behaviour. This includes in particular: – including the proper authentication token of the *Session* – creating a requestHandle if needed – requesting diagnostic information with the 'returnDiagnostics' parameter – evaluate the serviceResult and operational results
Client	*Session Client* Base	Use the *Session Service* Set (CreateSession, ActivateSession, and CloseSession) except the use of ActivateSession to change the *Session* user. This includes correct handling of all parameters that are provided Note that for the CreateSession and ActivateSession services, if the SecurityMode = None then: 1) The Application *Certificate* and Nonce are optional. 2) The signatures are null/empty.
Client	*Session Client* Multiple Connections	Support unlimited connections (client side) with multiple *Servers*. Any limit on numbers of connections is from server side. May have a memory based limit, but not a software constraint limit.
Client	*Session Client* Renew NodeIds	This *ConformanceUnit* applies to *Clients* that allow persisting NodeIds. Verify that the Namespace Table has not changed for NodeIds that the *Client* has persisted and is going to re-use beyond a *Session* lifetime. If changes occurred the *Client* has to recalculate the Namespace Indices of the respective NodeIds.
Client	*Session Client* Impersonate	Uses ActivateSession to change the Session user (impersonation).
Client	*Session Client* KeepAlive	Make periodic requests to keep the *Session* alive.
Client	*Session Client* Detect Shutdown	Read or monitor the ServerStatus/State Variable to recognize a potential shutdown of the Server and clean up resources.
Client	*Session Client* Cancel	Use the Cancel *Service* to cancel outstanding requests.
Client	*Session Client* Auto Reconnect	Automatic *Client* reconnect including: – ActivateSession with new SecureChannel if SecureChannel is no longer valid but *Session* is still valid – Creation of a new *Session* only if *Session* is no longer valid
Client	*Session Client* Single *Session*	The *Client* shall interoperate with *Servers* that only support one *Session*.
Client	*Session Client* SessionLess *Service* Calls	Defines the use of the SessionlessInvoke *Service* defined in UA Part 4 to request one of the *Services* (like Read or Browse) that are allowed for sessionless invocation. UA Part 6 specifies which transports may be used and how.

The *Node* Management *Service* Set is composed of multiple *ConformanceUnits* (see Table 5). *Servers* may provide some aspects of this functionality; see *Profiles* categorized as *Server Profiles* for details. *Clients* may support some aspects of this functionality; see *Profiles* categorized as *Client Profiles* for details.

Table 5 – Node Management Services

Category	Title	Description

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62541-7:2019-09

Category	Title	Description
Server	*Node* Management Add *Node*	Support the AddNodes *Service* to add one or more *Nodes* into the OPC UA *AddressSpace*.
Server	*Node* Management Delete *Node*	Support the DeleteNodes *Service* to delete one or more *Nodes* from the OPC UA *AddressSpace*.
Server	*Node* Management Add Ref	Support the AddReferences *Service* to add one or more *References* to one or more *Nodes* in the OPC UA *AddressSpace*.
Server	*Node* Management Delete Ref	Support the DeleteReferences *Service* to delete one or more *References* of a *Node* in the OPC UA *AddressSpace*.
Client	*Node* Management *Client*	Uses *Node* Management *Services* to add or delete *Nodes* and to add or delete *References* in *Server*'s OPC UA *AddressSpace*.

The View *Service* Set is composed of a multiple *ConformanceUnits* (see Table 6). All *Servers* support some aspects of this conformance group. *Clients* may support some aspects of this functionality; see *Profiles* categorized as *Client Profiles* for details.

Table 6 – View Services

Category	Title	Description
Server	View Basic	Support the View *Service* Set (Browse, BrowseNext).
Server	View TranslateBrowsePath	Support TranslateBrowsePathsToNodeIds *Service*.
Server	View RegisterNodes	Support the RegisterNodes and UnregisterNodes *Services* as a way to optimize access to repeatedly used *Nodes* in the *Server*'s OPC UA *AddressSpace*.
Server	View Minimum Continuation Point 01	Support minimum 1 continuation point per *Session*.
Server	View Minimum Continuation Point 05	Support minimum 5 continuation points per *Session*. This number has to be supported for at least half of the minimum required sessions.
Client	View *Client* Basic Browse	Uses Browse and BrowseNext *Services* to navigate through the *Server*'s OPC UA *AddressSpace*. Make use of the referenceTypeId and the nodeClassMask to specify the needed *References*.
Client	View *Client* Remote *Nodes* Browse	The *Client* can browse to nodes that have an extended NodeID that reference a *Server* different than the originating *Server*. This includes automatic connection to the remote *Server*. It is acceptable that the *Server* configuration information be pre-configured on the *Client* and / or that the user is prompted to connect.
Client	View *Client* Basic ResultSet Filtering	Makes use of the resultMask parameter to optimize the result set to be returned by the *Server*.
Client	View *Client* TranslateBrowsePath	Uses the TranslateBrowsePathsToNodeIds *Service* to identify the NodeIds for *Nodes* where a starting *Node* and a BrowsePath is known. Makes use of bulk operations rather than multiple calls whenever possible.
Client	View *Client* Remote *Nodes* Translate Browse	The *Client* can translate browse paths that include nodes with extended NodeID that reference a *Server* different than the originating *Server* and return them as part of the TranslateBrowsePathsToNodeIds *Service*. It is acceptable that the *Server* configuration information be pre-configured on the *Client*.
Client	View *Client* RegisterNodes	Uses the RegisterNodes *Service* to optimize access for *Nodes* that are used repeatedly. Use UnregisterNodes when *Nodes* are not used anymore.

The *Attribute Service* Set is composed of multiple *ConformanceUnits* (see Table 7). The majority of the *Attribute* service set is a core functionality of OPC UA and as such is supported by most *Servers*. Most *Clients* will also support some aspects of the *Attribute Service* Set.

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62541-7:2019-09

300 **Table 7 – Attribute Services**

Category	Title	Description
Server	*Attribute* Read	Supports the Read *Service* to read one or more *Attributes* of one or more *Nodes*. This includes support of the IndexRange parameter to read a single element or a range of elements when the *Attribute* value is an array.
Server	*Attribute* Read Complex	Supports reading and encoding Values with structured DataTypes.
Server	*Attribute* Write Values	Supports writing to values to one or more *Attributes* of one or more *Nodes*.
Server	*Attribute* Write Complex	Supports writing and decoding Values with structured DataTypes.
Server	*Attribute* Write StatusCode & Timestamp	Supports writing of StatusCode and Timestamps along with the Value.
Server	*Attribute* Write Index	Supports the IndexRange to write a single element or a range of elements when the *Attribute* value is an array and partial updates is allowed for this array.
Server	*Attribute* Alternate Encoding	Supports alternate Data Encoding when reading value *Attributes*. By default, every *Server* has to support the Data Encoding of the currently used Stack *Profile* (i.e. binary with UA Binary Encoding and XML with XML Encoding). This *ConformanceUnit* - when supported - specifies that the other Data Encoding is supported in addition.
Server	*Attribute* Historical Read	Supports the HistoryRead *Service*. The details of what aspects of this service are used are listed in additional *ConformanceUnits*, but at least one of ReadRaw, ReadProcessed, ReadModified, ReadAtTime or ReadEvents must be supported.
Server	*Attribute* Historical Update	Supports the HistoryUpdate service. The details of the supported features of this service are described by additional *ConformanceUnits*, but at least one of the following must be supported: InsertData, InsertEvents, ReplaceData, ReplaceEvents, UpdateData, UpdateEvents, DeleteData, DeleteEvents or DeleteAtTime.
Client	*Attribute Client* Read Base	Use the Read *Service* to read one or more *Attributes* of one or more *Nodes*. This includes use of an IndexRange to select a single element or a range of elements when the *Attribute* value is an array. *Clients* shall use bulk operations whenever possible to reduce the number of *Service* invocations.
Client	*Attribute Client* Remote *Nodes* *Attribute* Access	The *Client* can retrieve attributes of nodes that have an extended NodeID that reference a *Server* different than the originating *Server*. This requires a connection to the remote *Server* for access (not necessarily displayed as a connection). It is acceptable that the *Server* configuration information be pre-configured on the *Client*.
Client	*Attribute Client* Read with proper Encoding	This *ConformanceUnit* refers to the ability of a *Client* to discover the available encodings and choose a specific one when calling the Read *Service*.
Client	*Attribute Client* Read Complex	Read and decode Values with structured DataTypes.
Client	*Attribute Client* Write Base	Use the Write *Service* to write values to one or more *Attributes* of one or more *Nodes*. This includes use of an IndexRange to select a single element or a range of elements when the *Attribute* value is an array. *Clients* shall use bulk operations whenever possible to reduce the number of *Service* invocations.
Client	*Attribute Client* Write Complex	Write and Encode Values with structured DataTypes.
Client	*Attribute Client* Write Quality & Timestamp	Use the Write *Service* to also write StatusCode and/or Timestamps along with a Value.

AVA Documents Document Sharing Hub
Full document details: E DIN EN IEC 62541-7:2019-09

Category	Title	Description
Client	*Attribute Client* Historical Read	The *Client* makes use of the HistoryRead service. The details of which aspect of this service are used are provided by additional *ConformanceUnits*, but at least one or more of the following is used ReadRaw, ReadAtTime, ReadProcessed, ReadModified or ReadEvents.
Client	*Attribute Client* Historical Updates	The *Client* makes use of the HistoryUpdate service. The details of this usage are provided by additional *ConformanceUnits*, but at least one or more of the following must be provided InsertData, InsertEvents, ReplaceData, ReplaceEvents, UpdateData, UpdateEvents, DeleteData or DeleteEvents or DeleteAtTime.

The *Method Service* Set is composed of *ConformanceUnits* (see Table 8). The primary *ConformanceUnits* provide support for the call functionality. *Servers* may provide some aspects of this functionality; see *Profiles* categorized as *Server Profiles* for details. *Clients* may support some aspects of this functionality; see *Profiles* categorized as *Client Profiles* for details.

Table 8 – Method Services

Category	Title	Description
Server	*Method* Call	Support the Call *Service* to call (invoke) a *Method* which includes support for *Method* Parameters.
Client	*Method Client* Call	Use the Call *Service* to call one or several Methods.

The *MonitoredItem Service* Set is composed of multiple *ConformanceUnits* (see Table 9). *Servers* may provide some aspects of this functionality; see *Profiles* categorized as *Server Profiles* for details. *Clients* may support some aspects of this functionality; see *Profiles* categorized as *Client Profiles* for details.

Table 9 – Monitored Item Services

Category	Title	Description
Server	Monitor Basic	Support the following *MonitoredItem Services*: CreateMonitoredItems, ModifyMonitoredItems, DeleteMonitoredItems and SetMonitoringMode.
Server	Monitor Value Change	Support creation of *MonitoredItems* for *Attribute* value changes. This includes support of the IndexRange to select a single element or a range of elements when the *Attribute* value is an array.
Server	Monitor Complex Value	Supports monitoring and encoding Values with structured DataTypes.
Server	Monitored Items Deadband Filter	Supports an absolute Deadband filter as a DataChangeFilter for numeric data types.
Server	Monitor Aggregate Filter	Support for Aggregate filters for *MonitoredItems*. The result of this *ConformanceUnit* includes a list of Aggregates that are supported as part of the *Profile Certificate*.
Server	Monitor Alternate Encoding	Support alternate encoding when monitoring value *Attributes*. By default, every *Server* has to support the encoding of the currently used Stack *Profile* (i.e. binary with UA Binary Encoding and XML with XML Encoding). This *ConformanceUnit* - when supported - specifies that the other encoding is supported in addition.
Server	Monitor Items 2	Support at least 2 *MonitoredItems* per *Subscription* where the size of each *MonitoredItem* is at least equal to size of Double.
Server	Monitor Items 10	Support at least 10 *MonitoredItems* per *Subscription* where the size of each *MonitoredItem* is at least equal to size of Double.
Server	Monitor Items 100	Support at least 100 *MonitoredItems* per *Subscription*. This number has to be supported for at least half of the required Subscriptions for half of the required Sessions.

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62541-7:2019-09

Category	Title	Description
Server	Monitor Items 500	Support at least 500 *MonitoredItems* per *Subscription*. This number has to be supported for at least half of the required Subscriptions for half of the required Sessions.
Server	Monitor QueueSize_1	This *ConformanceUnit* does not require queuing when multiple value changes occur during a "publish period". I.e. the latest change will be sent in the *Notification*.
Server	Monitor MinQueueSize_02	Support at least 2 queue entries for *MonitoredItems*. *Servers* often will adapt the queue size to the number of currently *MonitoredItems*. However, it is expected that *Servers* support this minimum queue size for at least one third of the supported *MonitoredItems*.
Server	Monitor MinQueueSize_05	Support at least 5 queue entries for *MonitoredItems*. *Servers* often will adapt the queue size to the number of currently *MonitoredItems*. However, it is expected that *Servers* support this minimum queue size for at least one third of the supported *MonitoredItems*.
Server	Monitor QueueSize_ServerMax	This *ConformanceUnit* is for events. When the *Client* requests queuesize=MAXUInt32 the *Server* is to return the maximum queue size that it can support for event notifications as the revisedQueueSize.
Server	Monitor Triggering	Support the SetTriggering *Service* to create and/or delete triggering links for a triggering item.
Server	Monitor Events	Support creation of *MonitoredItems* for an "*EventNotifier Attribute*" for the purpose of *Event Notification*. The subscription includes supporting a filter that includes SimpleAttribute Operands and a select list of Operators. The list of Operators includes: Equals, IsNull, GreaterThan, LessThan, GreaterThanorEqual, LessThatorEqual, Like, Not, Between, InList, And, Or, Cast, BitwiseAnd, BitwiseOr.
Server	Monitor Complex *Event* Filter	Support for the 'TypeOf' complex *Event* filter operator.
Client	Monitor *Client* Value Change	Use the *MonitoredItem Service* Set to register items for changes in *Attribute* value. Use CreateMonitoredItems to register the *Node*/*Attribute* tuple. Set proper sampling interval, Deadband filter and queuing mode. Use disabling / enabling instead of deleting and re-creating a *MonitoredItem*. Use bulk operations rather than individual service requests to reduce communication overhead.
Client	Monitor *Client* Complex Value	Monitor and decode Values with structured DataTypes.
Client	Monitor *Client* Deadband Filter	Uses Absolute Deadband filters for subscriptions.
Client	Monitor *Client* by Index	Use the IndexRange to select a single element or a range of elements when the *Attribute* value is an array.
Client	Monitor *Client* Aggregate Filter	Uses Aggregate filters for Subscriptions.
Client	Monitor *Client* Events	Use the *MonitoredItem Service* Set to create *MonitoredItems* for *Event* notifications.
Client	Monitor *Client Event* Filter	Use the *Event* filter when calling CreateMonitoredItems to filter the desired Events and to select the columns to be provided for each *Event Notification*.
Client	Monitor *Client* Complex *Event* Filter	Use of the 'TypeOf' complex *Event* filter operator.
Client	Monitor *Client* Modify	Use ModifyMonitoredItems *Service* to change the configuration setting. Use SetMonitoringMode *Service* to disable / enable sampling and / or publishing.

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62541-7:2019-09

Category	Title	Description
Client	Monitor *Client* Trigger	Use the Triggering Model if certain items are to be reported only if some other item triggers. Use proper monitoring mode for these items. Use SetTriggering *Service* to link these items to the trigger item.

314

315 The *Subscription Service* Set is composed of multiple *ConformanceUnits* (see Table 10).
316 *Servers* may provide some aspects of this functionality; see *Profiles* categorized as *Server*
317 *Profiles* for details. *Clients* may support some aspects of this functionality; see *Profiles*
318 categorized as *Client Profiles* for details.

319 **Table 10 – Subscription Services**

Category	Title	Description
Server	*Subscription* Basic	Support the following *Subscription Services*: CreateSubscription, ModifySubscription, DeleteSubscriptions, Publish, Republish and SetPublishingMode.
Server	*Subscription* Minimum 1	Support at least 1 *Subscription* per *Session*. This number has to be supported for all of the minimum required sessions.
Server	*Subscription* Minimum 02	Support at least 2 Subscriptions per *Session*. This number has to be supported for at least half of the minimum required sessions.
Server	*Subscription* Minimum 05	Support at least 5 Subscriptions per *Session*. This number has to be supported for at least half of the minimum required sessions.
Server	*Subscription* Publish Min 02	Support at least 2 Publish *Service* requests per *Session*. This number has to be supported for all of the minimum required sessions. Support of a NotificationMessage retransmission queue is not required; if not available the Republish *Service* returns Bad_MessageNotAvailable.
Server	*Subscription* Publish Min 05	Support at least 5 Publish *Service* requests per *Session*. This number has to be supported for at least half of the minimum required sessions. Support, as a minimum, the number of Publish requests per session as the size of the NotificationMessage retransmission queue for Republish.
Server	*Subscription* Publish Min 10	Support at least 10 Publish *Service* requests per *Session*. This number has to be supported for at least half of the minimum required sessions. Support, as a minimum, the number of Publish requests per session as the size of the NotificationMessage retransmission queue for Republish.
Server	*Subscription* Publish Discard Policy	Respect the specified policy for discarding Publish *Service* requests. If the maximum number of Publish *Service* requests has been queued and a new Publish *Service* request arrives, the "oldest" Publish request has to be discarded by returning the proper error.
Server	*Subscription* Transfer	Support TransferSubscriptions *Service* to transfer a *Subscription* from one *Session* to another.
Server	*Subscription* Durable	Support setting Subscriptions in durable mode. This mode requires that collected data and events are stored and delivered even if a *Client* was disconnected for a longer time or the *Server* was restarted. Support one of the "*Subscription* Durable StorageLevel nnn" *ConformanceUnits*.
Server	*Subscription* Durable StorageLevel Small	Support at least 20 monitored items with a queue size of 10000 for each item and where the size of each *MonitoredItem* is at least equal to size of Double. This requires storage capacity for 200 thousand values of DataType Double.
Server	*Subscription* Durable StorageLevel Medium	Support at least 100 monitored items with a queue size of 50000 for each item and where the size of each *MonitoredItem* is at least equal to size of Double. This requires storage capacity for 5 million values of DataType Double.

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62541-7:2019-09

Category	Title	Description
Server	*Subscription* Durable StorageLevel High	Support at least 2000 monitored items with a queue size of 200000 for each item and where the size of each *MonitoredItem* is at least equal to size of Double. This requires storage capacity for 400 million values of DataType Double.
Client	*Subscription Client* Basic	Use the *Subscription* and *MonitoredItem Service* Set as an efficient means to detect changes of *Attribute* values and / or to receive *Event* occurrences. Set appropriate intervals for publishing, keep alive notifications and total *Subscription* lifetime. Supply a sufficient number of Publish requests to the *Server* so that *Notifications* can be sent whenever a publish timer expires. Acknowledge received *Notifications* with subsequent Publish requests.
Client	*Subscription Client* Fallback	The *Client* shall interoperate with *Servers* that do not support Subscriptions, or have exhausted *Subscription* limits, for Monitoring by using Read *Service*.
Client	*Subscription Client* Republish	Evaluate the sequence number in *Notifications* to detect lost *Notifications*. Use Republish to request missing *Notifications*.
Client	*Subscription Client* Modify	Allow modification of the *Subscription* configuration using the ModifySubscription *Service*.
Client	*Subscription Client* TransferSubscriptions	The *Client* supports transferring *Subscription* from other *Clients*. This *ConformanceUnit* is used as part of redundant *Clients*.
Client	*Subscription Client* Multiple	Use multiple Subscriptions to reduce the payload of individual *Notifications*.
Client	*Subscription Client* Publish Configurable	Send multiple Publish *Service* requests to assure that the *Server* is always able to send *Notifications*. The number of parallel Publish *Service* requests per *Session* shall be configurable.
Client	*Subscription Client* Durable	Use durable Subscriptions.

5.3 Transport and communication related features

Table 11 describes security related *ConformanceUnits*. All of these *ConformanceUnits* apply equally to both *Clients* and *Servers*, where a *Client* uses the related security unit and a *Server* supports the use of it. These items are defined in detail in IEC 62541-6. It is recommended that a *Server* and *Client* support as many of these options as possible in order to achieve increased levels of interoperability. It is the task of an administrator to determine which of these *ConformanceUnits* are exposed in a given deployed *Server* or *Client* application.

Table 11 – Security

Category	Title	Description
Security	Security User Name Password	The *Server* supports User Name/Password combination(s). The token will be encrypted if required by the security policy of the User Token Policy or by the security policy of the endpoint. An unencrypted token either requires message encryption or means outside the scope of OPC UA to secure the identity token so that it cannot be retrieved by sniffing the communication. One option would be a secure transport like a VPN.
Security	Security User X509	The *Server* supports a public/private key pair for user identity. The use of this feature must be able to be enabled or disabled by an administrator.

Documents
Document Sharing Hub
Full document details: E DIN EN IEC 62541-7:2019-09