

DIN EN IEC 62541-1

ICS 25.040.40; 35.200; 35.240.50

Einsprüche bis 2024-09-26

Entwurf

**OPC Unified Architecture –
Teil 1: Übersicht und Konzepte
(IEC 65E/1039/CDV:2024);
Deutsche und Englische Fassung prEN IEC 62541-1:2024**

OPC Unified Architecture –
Part 1: Overview and Concepts
(IEC 65E/1039/CDV:2024);
German and English version prEN IEC 62541-1:2024

Architecture unifiée OPC –
Partie 1: Vue d'ensemble et concepts
(IEC 65E/1039/CDV:2024);
Version allemande et anglaise prEN IEC 62541-1:2024

Anwendungswarnvermerk

Dieser Entwurf mit Erscheinungsdatum 2024-07-26 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil das beabsichtigte Dokument 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, Merianstraße 28, 63069 Offenbach am Main.

Es wird gebeten, mit den Kommentaren zu diesem Entwurf jegliche relevanten Patentrechte, die bekannt sind, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 57 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Nationales Vorwort

Die Deutsche Fassung des europäischen Dokuments prEN IEC 62541-1:2024-01 „OPC Unified Architecture – Teil 1: Übersicht und Konzepte“ (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/1039/CDV:2024-01 „OPC Unified Architecture – Part 1: Overview and Concepts“ unverändert in den Entwurf prEN IEC 62541-1:2024-01 übernommen worden.

Da die Deutsche Fassung noch nicht endgültig mit der Englischen und Französischen Fassung abgeglichen ist, ist die englische Originalfassung des IEC-CDV entsprechend der diesbezüglich durch die IEC erteilten Erlaubnis beigefügt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen IEC-Text.

Das internationale Dokument wurde vom IEC/SC 65E „Devices and integration in enterprise systems“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und unterliegt dem Copyright der IEC . Das Dokument wurde den nationalen Komitees zur Stellungnahme vorgelegt.

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 DKE/K 931 „Systemaspekte der Automatisierung“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (www.dke.de) zuständig.

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DKE (www.dke.de) und DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

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.

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.

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.

OPC Unified Architecture – Teil 1: Übersicht und Konzepte

Inhalt

	Seite
1 Anwendungsbereich.....	5
2 Normative Verweisungen.....	5
3 Begriffe und Abkürzungen.....	6
3.1 Konventionen in diesem Dokument.....	6
3.2 Begriffe.....	6
3.3 Abkürzungen.....	12
4 Aufbau von OPC UA.....	12
4.1 Unterteilung der Spezifikation.....	12
4.2 Teile der Spezifikation.....	12
5 Übersicht.....	14
5.1 Anwendungsbereich.....	14
5.2 Allgemeines.....	15
5.3 Entwurfziele.....	15
5.4 Integrierte Modelle und Dienste.....	17
5.4.1 IT-Sicherheitsmodell.....	17
5.4.2 Integriertes Adressraummodell.....	18
5.4.3 Integriertes Objektmodell.....	19
5.4.4 Integrierte Dienste.....	19
5.5 Sitzungen.....	19
6 Systemkonzepte.....	20
6.1 Client-Server-Übersicht.....	20
6.2 OPC UA-Clients.....	20
6.3 OPC UA-Server.....	21
6.3.1 Allgemeines.....	21
6.3.2 Reale Objekte.....	21
6.3.3 Server-Anwendung.....	21
6.3.4 OPC UA-AdressRaum.....	22
6.3.5 Subskriptionseinheiten.....	22
6.3.6 OPC UA-Dienste-Schnittstelle.....	23
6.3.7 Server-zu-Server Interaktionen.....	23
6.4 Redundanz.....	24
6.5 Publish-Subscribe.....	24
6.6 Synergie von Modellen.....	25
6.7 Globale Dienste.....	26
6.7.1 Allgemeines.....	26
6.7.2 Entdeckungsdienste.....	26
6.7.3 Zertifikatmanagement.....	26

6.7.4	KeyCredential-Verwaltung.....	26
6.7.5	Autorisierungsdienste.....	26
6.7.6	Geräteeinbindung (en: Device Onboarding).....	27
6.7.7	Aliasnamen.....	27
6.7.8	Sicherheitsschlüsseldienst (SKS, en: Security Key Service).....	27
7	Client/Server-Dienste-Sätze.....	27
7.1	Allgemeines.....	27
7.2	Erkundungsdienste.....	27
7.3	Satz von SichererKanal-Diensten.....	27
7.4	Satz von Sitzungs-Diensten.....	28
7.5	KnotenManagement-Dienste (en: NodeManagement Service Set).....	29
7.6	Sichten-Dienste.....	29
7.7	Satz von Abfrage-Diensten.....	29
7.8	Satz von Attribute-Diensten.....	29
7.9	Satz von Methoden-Diensten.....	29
7.10	Satz von ÜberwachtesElement-Diensten.....	30
7.11	Satz von Subskriptionsdiensten.....	30
Bilder		
Bild 1	– OPC UA-Zielanwendungen.....	16
Bild 2	– OPC UA-Systemarchitektur.....	20
Bild 3	– OPC UA-Client-Architektur.....	20
Bild 4	– OPC UA-Serverarchitektur.....	21
Bild 5	– Partner-zu-Partner-Interaktionen zwischen Servern.....	23
Bild 6	– Beispiel mit verketteten Servern.....	24
Bild 7	– Integrierte Client-Server- und PubSub-Modelle.....	25
Bild 8	– Sicherer Kanal und Sitzungsdienste.....	28

1 Anwendungsbereich

Dieser Teil von IEC 62541 stellt die Konzepte und einen Überblick über die OPC Unified Architecture (OPC UA) dar. Das Studium dieses Dokuments ist für das Verständnis der anderen Teile dieses mehrteiligen Dokumentensatzes hilfreich. Alle anderen Teile werden kurz erläutert, und es wird vorgeschlagen, in welcher Reihenfolge sie gelesen werden sollten. Mit Ausnahme der Begriffe in 3.2 ist dieser Teil nicht normativ.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

IEC 61508 (alle Teile), *Functional safety of electrical/electronic/programmable electronic safety-related systems*, <https://www.iec.ch/functionalsafety/standards/>

IEC 61784-3:2017, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*, <https://webstore.iec.ch/publication/61165/>

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

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

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

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

IEC 62541-10, *OPC Unified Architecture – Part 10: Programs*

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*

IEC 62541-15, *OPC Unified Architecture - Part 15: Safety*

IEC 62541-16, *OPC Unified Architecture - Part 16: State Machines*

IEC 62541-17, *OPC Unified Architecture - Part 17: Alias Names*

IEC 62541-18, *OPC Unified Architecture - Part 18: Role-Based Security*

IEC 62541-19, *OPC Unified Architecture - Part 19: Dictionary References*

IEC 62541-20, *OPC Unified Architecture - Part 20: File Transfer*

IEC 62541-21, *OPC Unified Architecture - Part 21: Device Onboarding*

IEC 62541-22, *OPC Unified Architecture - Part 22: Base Network Model*

IEC 62541-23, *OPC Unified Architecture - Part 23: Common Reference Types*

IEC 62541-24, *OPC Unified Architecture - Part 24: Scheduler*

X.509, X.509 Public Key Certificate Infrastructure

<https://www.itu.int/rec/T-REC-X.509>

3 Begriffe und Abkürzungen

3.1 Konventionen in diesem Dokument

In diesem Dokument und den anderen Teilen dieser Reihe, auf die verwiesen wird, werden folgende Konventionen angewendet.

Kursive Schrift wird verwendet, um einen definierten Begriff oder eine Definition zu kennzeichnen, die in einem der Teile dieser Reihe im Abschnitt „Begriffe“ erscheint.

Kursive Schrift wird auch verwendet, um den Namen eines Dienst-Eingangs- und Ausgangsparameters zu kennzeichnen oder den Namen einer Struktur oder eines Strukturelements, die gewöhnlich in Tabellen definiert sind.

Begriffe und Namen in kursiver Schrift werden oft auch in „camel-case“ geschrieben. (Das ist die Art, zusammengesetzte Wörter oder Ausdrücke zu schreiben, indem die Elemente ohne Zwischenräume verbunden werden und die Anfangsbuchstaben aller Elemente groß geschrieben werden). Zum Beispiel lautet der definierte Begriff *AdressRaum* statt Adressraum. Dies macht es leichter zu verstehen, dass es eine eigene Definition für *AdressRaum* gibt und nicht getrennte Definitionen für Adresse und Raum.

3.2 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

3.2.1

AdressRaum

en **AddressSpace**

Sammlung von Informationen, die ein *Server* seinen *Clients* sichtbar macht

Anmerkung 1 zum Begriff: Siehe IEC 62541-3 für eine Beschreibung des Inhalts und der Struktur des *AdressRaums* des *Servers*.

3.2.2

Aggregate

Funktion, die abgeleitete Werte aus *Rohdaten* berechnet

Anmerkung 1 zum Begriff: Rohdaten können aus historischen Daten oder gepufferten Echtzeitdaten stammen. Zu den gängigen Aggregaten gehören Durchschnittswerte über eine bestimmte Zeitspanne, Minimum über eine Zeitspanne und Maximum über eine Zeitspanne.

3.2.3

Alarm

Typ des *Ereignisses*, das mit einer Zustandsbedingung verbunden ist, die typischerweise eine Bestätigung erfordert

Anmerkung 1 zum Begriff: IEC 62541-9 für eine Beschreibung der *Alarme*.

3.2.4

Attribut

elementare Eigenschaft eines *Knotens*

Anmerkung 1 zum Begriff: Alle *Attribute* sind durch OPC UA definiert und dürfen nicht durch *Clients* oder *Server* festgelegt werden. *Attribute* sind die einzigen Elemente im *AdressRaum*, die Datenwerte besitzen dürfen.

3.2.5

Broker

zischengeschnittetes Programmmodul, das *NetzwerkNachrichten* von *Publishern* an *Subscriber* weiterleitet

Anmerkung 1 zum Begriff: *Broker* sind Bausteine einer *Message Oriented Middleware*.

3.2.6

Zertifikat

en **Certificate**

digital signierte Datenstruktur, die einen öffentlichen Schlüssel und eine Identität enthält

Anmerkung 1 zum Begriff: Zertifikate werden z. B. zur Identifizierung von *Clients*, *Servern*, Benutzern und Zertifizierungsstellen verwendet.

3.2.7

Client

en **Client**

Softwareanwendung, die *Nachrichten* an OPC UA-Server sendet, die die Regeln der *Dienste* einhalten, die in dieser Reihe von Spezifikationen festgelegt sind

3.2.8

Bedingung

en **Condition**

generischer Begriff, der eine Erweiterung des *Ereignisses* darstellt

Anmerkung 1 zum Begriff: Eine *Bedingung* stellt die Bedingungen eines Systems oder eine seiner Komponenten dar und befindet sich immer in einem Zustand.

3.2.9

Kommunikationsstack

en **Communication Stack**

mehrschichtige Menge von Softwaremodulen zwischen der Anwendung und der Hardware, die verschiedene Funktionen zur Verfügung stellen, die zur Kodierung, Verschlüsselung und Aufbereitung beim Senden einer *Nachricht* benötigt werden, sowie Funktionen, die zur Dekodierung, Entschlüsselung und Entpackung einer empfangenen *Nachricht* dienen

3.2.10

zusammengesetzte Daten

en **Complex Data**

Daten, die sich aus Elementen von mehr als einem Grunddatentyp zusammensetzen, z. B. eine Struktur

3.2.11

DatenSatz

Liste der benannten Datenwerte

Anmerkung 1 zum Begriff: Ein *DatenSatz* besteht üblicherweise aus *Ereignisfeldern* oder *Variablenwerten*.

3.2.12

DatensatzNachricht

Nutzdaten einer *NetzwerkNachricht*, die aus einem *DatenSatz* erstellt wurde

Anmerkung 1 zum Begriff: Die *DatenSatzNachricht* ist eine unveränderliche Nutzlast der *NetzwerkNachricht*, die an die *Message Oriented Middleware* (Transportschicht) zur Zustellung durch den *Publisher* weitergegeben wird. Der *Subscriber* erhält die *DatenSatzNachricht* als Nutzdaten einer *NetzwerkNachricht* vom *Publisher* mit zusätzlichen Headern, die von der *Message Oriented Middleware* in dem Prozess bereitgestellt werden können.

3.2.13

Erkundung

en **Discovery**

Vorgang, durch den ein *Client* Informationen über die *Server* erhält, einschließlich Endpunkt- und IT-Sicherheitsinformation

3.2.14

Event

en **Ereignis**

generischer Begriff, der benutzt wird, um einen Vorgang zu beschreiben, der eine bestimmte Bedeutung innerhalb eines Systems oder einer Systemkomponenten hat

3.2.15

EreignisMelder

en **EventNotifier**

spezielles *Attribut* eines *Knotens*, das anzeigt, dass ein *Client* sich für diesen bestimmten *Knoten* subscribieren kann, um *Benachrichtigungen* über das Auftreten von *Ereignissen* zu empfangen

3.2.16

Informationsmodell

en **Information Model**

organisatorischer Rahmen, der Informationsressourcen eines gegebenen Systems oder einer Menge von Systemen definiert, charakterisiert und verknüpft

Anmerkung 1 zum Begriff: Das Kernmodell des *AdressRaums* unterstützt die Darstellung von *Informationsmodellen* im *AdressRaum*. Siehe IEC 62541-5 für eine Beschreibung des OPC UA-Basis-*Informationsmodells*.

3.2.17

Nachricht

en **Message**

Dateneinheit, die zwischen *Client* und *Server* übermittelt wird und die eine spezifische *Dienstanforderung* oder -antwort darstellt

3.2.18

Message Oriented Middleware

Infrastruktur, die das Senden und Empfangen von *NetzwerkNachrichten* zwischen verteilten Systemen unterstützt

Anmerkung 1 zum Begriff: Eine OPC UA-Anwendung kann verschiedene Typen von *Message Oriented Middleware*-Infrastrukturen und Protokollen wie AMQP, MQTT oder UDP mit IP-Multicast unterstützen. Andere Typen wie DDS oder XMPP können ebenfalls in das OPC UA *PubSub*-Modell integriert werden.

3.2.19

Methode

en **Method**

aufzurufbare Softwarefunktion, die eine Komponente eines *Objekts* ist

3.2.20

ÜberwachtesElement

en **MonitoredItem**

vom *Client* definiertes Element im *Server*, das zur Überwachung von *Attributen* oder *EreignisMeldern* auf neue Werte oder das Auftreten eines *Ereignisses* verwendet wird und das *Benachrichtigungen* für diese erzeugt

3.2.21

NetzwerkNachricht en **NetworkMessage**

DatenSatzNachrichten und Header zur Erleichterung der Zustellung, Weiterleitung, Sicherheit und Filterung

Anmerkung 1 zum Begriff: Der *Publisher* übergibt die *NetzwerkNachricht* an die *Message Oriented Middleware* (Transportschicht), um *DatenSatzNachrichten* an die *Subscriber* weiterzugeben.

Anmerkung 2 zum Begriff: Der Begriff *Nachricht* wird im Messaging-Bereich mit diversen Konnotationen verwendet. Der *Publisher* könnte die *Nachricht* als eine unveränderliche Nutzlast sehen, die zur Zustellung an die *Message Oriented Middleware* übergeben wird. Der *Subscriber* sieht die *Nachricht* oftmals nicht nur als unveränderliche Nutzlast des Absenders, sondern auch verschiedene Annotationen, die von der *Message Oriented Middleware* in dem Prozess geliefert werden. Um Verwirrung zu vermeiden, wird der Begriff *NetzwerkSatzNachricht* für die *Nachricht* verwendet, wie sie vom *Publisher* für einen *DatenSatz* bereitgestellt wird. Der Begriff *NetzwerkNachricht* wird für die *DatenSatzNachricht* plus Abschnitte für Annotationen am Anfang und am Ende der *DatenSatzNachricht* verwendet.

3.2.22

Knoten en **Node**

fundamentale Komponente eines *AdressRaums*

3.2.23

KnotenKlasse en **NodeClass**

Klasse eines *Knotens* in einem *AdressRaum*

Anmerkung 1 zum Begriff: *KnotenKlassen* definieren die Metadaten für die Komponenten des OPC UA-Objektmodells. Sie definieren auch Konstrukte wie *Sichten*, die zur Organisation des *AdressRaums* benutzt werden.

3.2.24

Benachrichtigung en **Notification**

generischer Begriff für Daten, die das Auffinden von *Ereignisses* oder eines geänderten *Attributwertes* anzeigen; *Meldungen* werden mittels *Meldungsnachrichten* gesendet

3.2.25

Meldungsnachricht en **NotificationMessage**

Nachricht, die durch eine *Subskription* veröffentlicht wird, die eine oder mehrere *Meldungen* enthält

3.2.26

Objekt en **Object**

Knoten, der ein physikalisches oder abstraktes Element eines Systems darstellt

Anmerkung 1 zum Begriff: *Objekte* werden mit Hilfe des OPC UA-Objektmodells modelliert. Systeme, Subsysteme und Geräte sind Beispiele für *Objekte*. Ein *Objekt* darf als eine Instanz eines *Objektyps* definiert werden.

3.2.27

Objektinstanz en **Object Instance**

gleichbedeutend mit *Objekt*

Anmerkung 1 zum Begriff: alle *Objekte* sind durch *ObjektTypen* definiert.

3.2.28

ObjektTyp en **ObjectType**

Knoten, der die Typdefinition für ein *Objekt* darstellt

3.2.29

OPC UA-Anwendung

en **OPC UA Application**

Client, der OPC UA-*Dienste* aufruft, oder ein *Server*, der diese *Dienste* ausführt, oder ein OPC UA-*Publisher* oder ein OPC UA-*Subscriber*.

3.2.30

Publisher

Einheit, die *Netzwerknachrichten* an eine *Message Oriented Middleware* sendet

Anmerkung 1 zum Begriff: Ein Publisher kann eine systemeigene OPC UA-Anwendung sein oder eine Anwendung, die nur über Kenntnisse der Message Oriented Middleware und der Regeln für die Codierung der NetzwerkNachrichten und DatenSatzNachrichten verfügt.

3.2.31

PubSub

OPC UA-Variante des Publish-Subscribe-Nachrichtenmusters

3.2.32

Profil

en **Profile**

spezifische Menge von Fähigkeiten, für die ein *Server* Konformität geltend machen darf.

Anmerkung 1 zum Begriff: Jeder *Server* darf für mehr als ein *Profil* Konformität geltend machen

Anmerkung 2 zum Begriff: Die Menge der Fähigkeiten ist in IEC 62541-7 definiert.

3.2.33

Programm

en **Program**

ausführbares *Objekt*, das beim Aufruf sofort eine Antwort zurückgibt, um anzuzeigen, dass die Ausführung begonnen hat, und dann Zwischen- und Endergebnisse durch *Subskriptionen* zurückgibt, die durch den *Client* während des Aufrufs identifiziert werden

3.2.34

Referenz

en **Reference**

explizite Beziehung (ein benannter Zeiger) von einem *Knoten* zu einem anderen

Anmerkung 1 zum Begriff: Der *Knoten*, der die *Referenz* enthält, ist der *QuellKnoten*, und der referenzierte *Knoten* ist der *ZielKnoten*. Alle *Referenzen* sind durch die *ReferenzTypen* definiert.

3.2.35

ReferenzTyp

en **ReferenceType**

Knoten, der die Typdefinition einer *Referenz* darstellt

Anmerkung 1 zum Begriff: Der *ReferenzTyp* legt die Semantik einer *Referenz* fest. Der Name eines *ReferenzTyps* bestimmt, wie sich *QuellKnoten* auf *ZielKnoten* beziehen und zeigen allgemein eine Operation zwischen zwei *Knoten*, wie „A enthält B“.

3.2.36

Server

Softwareanwendung, die die *Dienste* implementiert und zur Verfügung stellt, die in dieser Reihe von Spezifikationen festgelegt sind

3.2.37

Dienst

en **Service**

vom *Client* aufrufbare Operation in einem *Server*

Anmerkung 1 zum Begriff: *Dienste* sind in IEC 62541-4 definiert. Ein *Dienst* ähnelt einem Methodenaufruf in einer Programmiersprache oder einer Operation in einem Web-Service-Kontrakt (WSDL).

3.2.38

Satz von Diensten

en **Service Set**

Gruppe von *Diensten*, die zueinander in Beziehung stehen

3.2.39

Sitzung

en **Session**

logische, lange laufende Verbindung zwischen einem *Client* und einem *Server*

Anmerkung 1 zum Begriff: Eine *Sitzung* behält die Zustandsinformationen zwischen *Dienstaufufen* von einem *Client* zu einem *Server*.

3.2.40

Subscriber

Einheit, die *DatenSatzNachrichten* von einer *Message Oriented Middleware* erhält

Anmerkung 1 zum Begriff: Ein *Subscriber* kann eine systemeigene OPC UA-Anwendung sein oder eine *Anwendung*, die nur über Kenntnisse der *Message Oriented Middleware* und der Regeln für die Dekodierung der *NetzwerkNachrichten* und *DatenSatzNachrichten* verfügt. Eine *Subskription* im OPC UA-*Client-Server*-Modell hat eine andere Bedeutung als der *Subscriber* im *PubSub*-Modell.

3.2.41

Subskription

en **Subscription**

vom *Client* definierter Endpunkt im *Server*, verwendet zur Rückgabe von *Benachrichtigungen* an den *Client*

Anmerkung 1 zum Begriff: *Subskription* ist ein generischer Begriff, der eine Menge von *Knoten* beschreibt, die vom *Client* ausgewählt sind, die (1) der *Server* periodisch auf die Existenz einer Bedingung überwacht und für die (2) der *Server* *Benachrichtigungen* zum *Client* sendet, wenn die Bedingung ermittelt wurde.

3.2.42

Zugrundeliegendes System

Hardware- oder Software-Plattformen, die als unabhängige Einheit existieren. *UA-Anwendungen* sind von der Existenz einer Einheit abhängig, um UA-Dienste ausführen zu können. Die Einheit ist jedoch nicht von *UA-Anwendungen* abhängig.

Anmerkung 1 zum Begriff: Zu den Hardware- und Softwareplattformen gehören physische Hardware, Firmware, Betriebssysteme, Netzwerke, Nicht-UA-Anwendungen sowie andere *UA-Anwendungen*. Ein Leitsystem, eine SPS/Gerät und ein UA-Server sind Beispiele für ein *zugrundeliegendes System*.

3.2.43

Variable

Knoten, der einen Wert enthält

3.2.44

Sicht

en **View**

spezifische Teilmenge des *AdressRaums*, die für den *Client* von Interesse ist.

3.3 Abkürzungen

A&E	Alarmer und Ereignisse (en: Alarms and Events)
AMQP	erweitertes Protokoll für die Nachrichtenwarteschlange (en: Advanced Message Queuing Protocol)
API	Anwendungsprogrammierschnittstelle (en: Application Programming Interface)
COM	Komponentenobjektmodell (en: Component Object Model)
DA	Datenzugriff (en: Data Access)
DCS	Leitsystem (en: Distributed Control System)
DDS	Datenverteilungsdienst (en: Data Distribution Service)
HDA	historischer Datenzugriff (en: Historical Data Access)
HMI	Mensch-Maschine-Schnittstelle (en: Human-Machine Interface)
JSON	JavaScript Object Notation
LDAP	LDAP ist ein Protokoll zur Kommunikation mit Verzeichnissen in einem Netzwerk (en: Lightweight Directory Access Protocol)
MES	Produktionssteuerungssystem (en: Manufacturing Execution System)
MQTT	Nachrichtenwarteschlangen-Telemetrieübertragung (en: Message Queue Telemetry Transport)
OAuth2	Offene Autorisierung
OPC	Offene Plattformunabhängige Kommunikation OPC-Stiftung (Open Platform Communications)
SCADA	Betriebsdatenerfassung und -überwachung (en: Supervisory Control And Data Acquisition)
UA	vereinheitlichte Architektur (en: Unified Architecture)
UADP	UA-Datagramm-Protokoll (en: UA Datagram Protocol)
WSDL	WSDL ist eine Beschreibungssprache für Netzwerkdienste (en: Web Services Definition Language)
XML	Auszeichnungssprache für Textdateien (en: Extensible Markup Language)
XMPP	erweiterbares Nachrichten- und Anwesenheitsprotokoll (en: Extensible Messaging and Presence Protocol)

4 Aufbau von OPC UA

4.1 Unterteilung der Spezifikation

Diese Spezifikation ist als mehrteilige Spezifikation aufgebaut. In den Teilen 1 bis 5 werden die Kernkonzepte von OPC UA beschrieben. Daher wird den Lesern empfohlen, die Teile 1 bis 5 der Spezifikation zu lesen, bevor sie die anderen Teile lesen.

4.2 Teile der Spezifikation

Teil 1 (IEC 62541-1) – Überblick und Konzepte

Teil 1 (dieser Teil) stellt die Konzepte und den Überblick von OPC UA dar.

Teil 2 (IEC 62541-2) – Modell für die IT-Sicherheit

Teil 2 beschreibt das Modell für sichere Interaktionen zwischen *OPC UA-Anwendungen*.

Teil 3 (IEC 62541-3) – Adressraummodell

Teil 3 beschreibt den Inhalt und die Strukturen des *AdressRaums* des *Servers*.

Teil 4 (IEC 62541-4) – Dienste

Teil 4 beschreibt die *Dienste*, die von *Servern* zur Verfügung gestellt werden.

Teil 5 (IEC 62541-5) – Informationsmodell

Teil 5 legt die Typen und ihre Beziehungen fest, die für *Server* definiert sind.

Teil 6 (IEC 62541-6) – Protokollabbildung

Teil 6 legt die Abbildungen der Transportprotokolle und die Datenkodierungen fest, die von OPC UA unterstützt werden.

Teil 7 (IEC 62541-7) – Profile

Teil 7 legt die *Profile* fest, die für *OPC UA-Anwendungen* zur Verfügung stehen. Diese *Profile* stellen Gruppen von Funktionalitäten zur Verfügung, die für die Zertifizierung von Konformitätsstufen gebraucht werden. *OPC UA-Anwendungen* werden gegen die *Profile* getestet.

Teil 8 (IEC 62541-8) – Zugriff auf Automatisierungsdaten

Teil 8 legt die Anwendung von OPC UA für den Datenzugriff fest.

Teil 9 (IEC 62541-9) – Alarme und Zustände

Teil 9 legt die Unterstützung durch OPC UA für den Zugriff auf *Alarme* und *Bedingungen* fest. Das Basissystem schließt die Unterstützung von einfachen *Ereignissen* ein; diese Festlegung erweitert jene Unterstützung um die Unterstützung von *Alarmen* und *Zuständen*.

Teil 10 (IEC 62541-10) – Programme

Teil 10 legt die OPC UA-Unterstützung für den Zugriff auf *Programme* fest.

Teil 11 (IEC 62541-11) – Zugang zu historischen Daten

Teil 11 legt die Verwendung von OPC UA auf historische Daten fest. Dieser Zugriff umfasst sowohl die historischen Daten als auch die historischen *Ereignisse*.

Teil 12 (IEC 62541-12) – Erkundung und globale Dienste

Teil 12 legt fest, wie die *EntdeckungsServer* in verschiedenen Szenarien arbeiten und beschreibt, wie *UA-Clients* und *-Server* mit ihnen zusammen agieren sollten. Er legt auch die *Informationsmodelle* für die Verwaltung von *Zertifikaten*, *KeyCredential-Verwaltung* und *Autorisierungsdienste* fest.

Teil 13 (IEC 62541-13) – Aggregate

Teil 13 legt fest, wie *Aggregate* berechnet und zurückgegeben werden, wie *Minimum*, *Maximum*, *Durchschnitt* usw. *Aggregate* können mit aktuellen und historischen Daten verwendet werden.

Teil 14 (IEC 62541-14) – Festlegungen zur Umsetzung des Publisher-Subscriber-Models

Teil 14 legt das *PubSub*-Kommunikationsmodell der OPC Unified Architecture (OPC UA) fest. Das *PubSub*-Kommunikationsmodell definiert ein OPC UA-Publish-Subscribe-Muster zusätzlich zum durch die *Dienste* in IEC 62541-4 definierten *Client-Server*-Muster.

Teil 15 (IEC 62541-15) – Sicherheit

Teil 15 erweitert OPC UA, um die Anforderungen der funktionalen Sicherheit zu erfüllen, wie sie in den Normenreihen IEC 61508 und IEC 61784 3:2017 definiert sind.

Teil 16 (IEC 62541-16) – Zustandsautomaten

Teil 16 legt die grundlegende Infrastruktur zur Modellierung von Zustandsautomaten fest.

Teil 17 (IEC 62541-17) – Aliasnamen

Teil 17 legt fest, wie ein alternativer, gut definierter Name für jeden OPC UA-Knoten in einem Server oder System konfiguriert und angezeigt werden kann.

Teil 18 (IEC 62541-18) – Aufgabenbasierte Sicherheit

Teil 18 legt die grundlegende Infrastruktur zur Modellierung der aufgabenbasierten Zugriffskontrolle (RBAC, en: role-based access control) fest.

Teil 19 (IEC 62541-19) – Wörterbuchreferenz

Teil 19 legt die grundlegende Infrastruktur fest, um von einem OPC UA-Informationsmodell auf externe Wörterbücher wie das IEC Common Data Dictionary oder ECLASS zu verweisen.

Teil 20 (IEC 62541-20) – Dateitransfer

Teil 20 legt die grundlegende Infrastruktur zur Modellierung von Dateitransfers und Dateisystemen fest.

Teil 21 (IEC 62541-21) – Geräteeinbindung

Teil 21 legt den Lebenszyklus von Geräten und Composite-Geräten sowie Mechanismen zur Überprüfung ihrer Authentizität, zur Einrichtung ihrer Sicherheit und zur Aufrechterhaltung ihrer Konfiguration fest.

Teil 22 (IEC 62541-22) – Grundlegendes Netzwerkmodell

Teil 22 legt ein OPC UA-Informationsmodell für einen grundlegenden Satz von netzwerkbezogenen Komponenten fest, die in spezifischeren Informationsmodellen verwendet werden.

Teil 23 (IEC 62541-23) – Gemeinsame ReferenzTypen

Teil 23 legt gemeinsame Typen von Referenzen zwischen Knoten fest.

Teil 24 (IEC 62541-24) – Planer

Teil 24 legt ein OPC UA Informationsmodell fest, mit dem die Daten und Zeiten, zu denen bestimmte Aktionen vom OPC UA-Server ausgeführt werden, dargestellt und konfiguriert werden können.

5 Übersicht

5.1 Anwendungsbereich

Die OPC UA ist auf Komponenten sämtlicher Industriebereiche wie Industriesensoren und -aktoren, Steuerungssysteme, Produktionsleitsysteme und Unternehmensressourcenplanungssysteme, einschließlich dem Industriellen Internet der Dinge (IIoT), Machine To Machine (M2M) und weitere, anwendbar. Diese Systeme sind zum Informationsaustausch und zum Leiten und Steuern für industrielle Prozesse vorgesehen. OPC UA definiert ein gemeinsames Infrastrukturmodell, um diesen Informationsaustausch zu ermöglichen. OPC UA legt Folgendes fest:

- das Informationsmodell, um Struktur, Verhalten und Semantik darzustellen;
- das Nachrichtenmodell, um zwischen den Anwendungen zu agieren;
- das Kommunikationsmodell, um die Daten zwischen den Endpunkten zu übertragen;
- das Konformitätsmodell, um die Interoperabilität zwischen den Systemen zu gewährleisten.

5.2 Allgemeines

OPC UA ist eine plattformunabhängige Norm, mit der verschiedene Arten von Systemen und Geräten durch Senden von Antwort- und Anfrage-Nachrichten zwischen *Clients* und *Server* oder *NetzwerkNachrichten* zwischen *Publishern* und *Subscribern* über verschiedene Netzwerktypen kommunizieren können. Es wird eine robuste und sichere Kommunikation unterstützt, die die Identität von *OPC UA-Anwendungen* sicherstellt und Angriffen widersteht.

Im *Client-Server*-Modell definiert OPC UA Sätze von *Diensten*, die *Server* zur Verfügung stellen können und individuelle *Server* legen für *Clients* fest, welche Sätze von *Diensten* sie unterstützen. Die Information wird durch Verwendung von Datentypen übermittelt, die von OPC UA und Anbietern definiert worden sind und *Server* definieren Objektmodelle, die *Clients* dynamisch entdecken können. *Server* können einen Zugriff sowohl auf aktuelle und historische Daten als auch auf *Alarmer* und *Ereignisse* zur Verfügung stellen, um *Clients* über wichtige Änderungen zu benachrichtigen. OPC UA kann auf eine Vielzahl von Kommunikationsprotokolle abgebildet werden und Daten können in verschiedener Weise kodiert werden, je nachdem, ob Portabilität oder Effizienz gewünscht ist.

Zusätzlich zum *Client-Server*-Modell definiert OPC UA mit dem *PubSub*-Modell einen Mechanismus, mit dem *Publisher* die Informationen an *Subscriber* übertragen können.

5.3 Entwurfsziele

OPC UA bietet einen konsistenten und integrierten *AdressRaum* und ein solches Dienste-Modell. Dies ermöglicht es, dass ein einzelner OPC UA-*Server* Daten, *Alarmer* und *Ereignisse* und Historie in seinen *AdressRaum* integriert und den Zugriff mittels eines integrierten Satzes von *Diensten* auf sie zur Verfügung stellt. Diese *Dienste* schließen auch ein integriertes Modell für die IT-Sicherheit ein.

OPC UA ermöglicht es auch, dass *Server* den *Clients* Typdefinitionen für *Objekte* zur Verfügung stellen, auf die vom *AdressRaum* zugegriffen wird. Dies gestattet es, dass *Informationsmodelle* verwendet werden, um den Inhalt des *AdressRaums* zu beschreiben. OPC UA ermöglicht es, Daten in vielen verschiedenen Formaten anzubieten, einschließlich binärer Strukturen und XML- oder JSON-Dokumente. Das Format der Daten kann von OPC, von anderen Normungsorganisationen oder von Anbietern definiert werden. Mittels des *AdressRaums* können *Clients* den *Server* nach Metadaten durchsuchen, die das Format für die Daten beschreiben. In vielen Fällen sind *Clients* mit nichtprogrammiertem Wissen über die Datenformate in der Lage, die Formate zur Laufzeit zu bestimmen und die Daten ordnungsgemäß zu nutzen.

OPC UA bringt zusätzlich Unterstützung für viele Beziehungen zwischen *Knoten*, anstatt nur auf eine einfache Hierarchie begrenzt zu sein. Auf diese Weise kann ein OPC UA-*Server* Daten in einer Vielfalt von Hierarchien darstellen, so angepasst, wie eine Menge von *Clients* typischerweise gerne die Daten sehen will. Diese Flexibilität, kombiniert mit der Unterstützung für Typdefinitionen, macht OPC UA in einem breiten Feld von Problembereichen anwendbar. Wie in Bild 1 veranschaulicht, ist das Ziel von OPC UA, nicht nur eine Schnittstelle für SCADA, SPS und DCS zu bieten, sondern auch eine größere Interoperabilität zwischen Funktionen in höheren Ebenen.

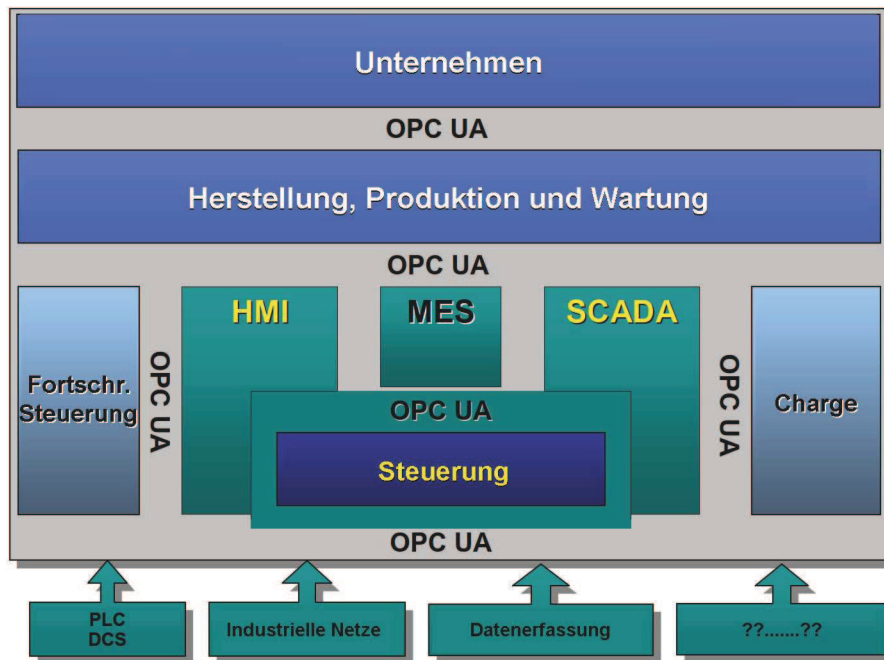


Bild 1 – OPC UA-Zielanwendungen

OPC UA ist entworfen worden, um veröffentlichte Daten robust zur Verfügung zu stellen. Ein Hauptmerkmal aller OPC UA-Server ist die Fähigkeit, Daten und *Ereignismeldungen* zu veröffentlichen. OPC UA bietet Mechanismen für *Clients*, Kommunikationsfehler, die mit diesen Transfers zusammenhängen, schnell zu erkennen und sich wieder davon zu erholen, ohne auf lange Zeitüberschreitungen (en: timeout) zu warten, die durch unterlagerte Protokolle zustande kommen.

OPC UA ist dazu vorgesehen, einen weiten Bereich von *Servern* zu unterstützen, der sich von den SPS in der Fabrikhalle bis zu den Unternehmens*Servern* erstreckt. Diese *Server* zeichnen sich durch einen breiten Bereich bezüglich Größe, Leistung, Ausführungsplattformen und funktionalen Fähigkeiten aus. Daher definiert OPC UA eine umfangreiche Menge von Fähigkeiten. *Server* können eine Teilmenge dieser Fähigkeiten implementieren. Um die Interoperabilität zu fördern, definiert OPC UA Teilmengen, die als *Profile* bezeichnet werden, für die *Server* Konformität geltend machen können. *Clients* können dann die *Profile* eines *Servers* entdecken und ihre Interaktionen mit diesem *Server* basierend auf den *Profilen* anpassen. *Profile* sind in IEC 62541-7 definiert.

Die OPC UA-Architektur ist in Schichten geordnet, um das Kernkonzept von der unterlagerten Computertechnologie und dem Netzwerktransport zu trennen. Dies ermöglicht es, OPC UA, falls notwendig, auf zukünftige Technologien abzubilden, ohne das Grundkonzept zu zerstören. Abbildungen und zwei Datenkodierungen sind in IEC 62541-6 beschrieben. Es sind mehrere Datenkodierungen definiert:

- XML/Text;
- UA binär;
- JSON.

Zusätzlich sind mehrere Protokolle definiert:

- OPC UA TCP;
- HTTPS;
- WebSockets.

OPC UA-Anwendungen, die mehrere Transporte und Kodierungen unterstützen, erlauben es dem Endanwender, Entscheidungen über die Abwägung zwischen Leistungsfähigkeit und Kompatibilität zum Zeitpunkt des Einsatzes zu treffen, statt diese zum Zeitpunkt der Produktdefinition durch den OPC-Anbieter vornehmen zu müssen.

OPC UA ist als Migrationspfad für Clients und Server konzipiert, die auf Microsoft COM-Technologie basieren. Es wurde im Konzept von OPC UA darauf geachtet, dass vorhandene Daten, die von OPC COM-Servern (DA, HDA und A&E) angeboten werden, leicht abgebildet und über OPC UA angeboten werden können. Anbieter können wählen, ob sie ihre Produkte nativ auf OPC UA migrieren oder ob sie eine externe Verdeckungsschicht (en: wrapper) zur Konvertierung von OPC COM nach OPC UA und umgekehrt verwenden. Jede der früheren OPC-Festlegungen hatte ihr eigenes Adressraummodell und ihren eigenen Satz von *Diensten* definiert. OPC UA vereinheitlicht die früheren Modelle mit einem einzigen integrierten Adressraum mit einem einzigen Satz von *Diensten*.

OPC UA *PubSub* eröffnet neue Anwendungsbereiche für OPC UA. Nachfolgend sind Beispiele für die Verwendung von *PubSub* aufgeführt:

- Konfigurierbare Partner-zu-Partner-Kommunikation zwischen Controllern und zwischen Controllern und HMI. Die Partner sind nicht direkt miteinander verbunden und müssen nicht einmal Kenntnis von der Existenz des jeweils anderen haben. Der Datenaustausch erfordert häufig ein festes Zeitfenster; es kann sich um eine Punkt-zu-Punkt- oder eine Mehrpunktverbindung handeln.
- Asynchrone Arbeitsabläufe. Eine Auftragsbearbeitungsanwendung kann zum Beispiel eine Anforderung in eine Nachrichtenwarteschlange oder einen Enterprise Service Bus stellen. Von dort aus kann er von einem oder mehreren Mitarbeitern verarbeitet werden.
- Protokollierung in mehrere Systeme; beispielsweise können Sensoren oder Stellantriebe Protokolle in ein Überwachungssystem, eine HMI, eine Archivanwendung zur späteren Abfrage usw. schreiben.
- *Server*, die Dienste oder Geräte repräsentieren, können Daten an Anwendungen streamen, die in der Cloud gehostet werden. Zum Beispiel Backend-Server, Big Data-Analysen zur Systemoptimierung und vorausschauende Wartung.

PubSub ist nicht an ein bestimmtes Nachrichtensystem gebunden. Vielmehr kann es verschiedenen Systemen zugeordnet werden, wie anhand von zwei Beispielen veranschaulicht:

- *PubSub* mit UDP kann sich für häufige Übertragungen von kleinen Datenmengen in Produktionsumgebungen gut eignen. Es ermöglicht auch den Datenaustausch in One-to-One- und One-to-Many-Konfigurationen.
- Die Verwendung etablierter Nachrichtenprotokolle (z. B. das ISO/IEC AMQP 1.0-Protokoll oder das MQTT 5.0-Protokoll) mit JSON-Datenkodierung unterstützt den Integrationspfad in die Cloud und ermöglicht die einfache Verarbeitung der Informationen in modernen Stream- und Batch-Analyse-Systemen.

5.4 Integrierte Modelle und Dienste

5.4.1 IT-Sicherheitsmodell

5.4.1.1 Allgemeines

Die IT-Sicherheit von OPC UA befasst sich mit der Authentifizierung von *Clients* und *Servern*, mit der Authentifizierung von Anwendern, mit der Datenintegrität und Vertraulichkeit ihrer Kommunikation und der Nachprüfbarkeit der Funktionalitätsanforderungen. Sie legt nicht die Umstände fest, unter denen die verschiedenen Sicherheitsmechanismen gefordert werden. Eine solche Festlegung ist wichtig, aber sie wird von den Systemdesignern für eine vorgegebene Anlage gemacht und möglicherweise durch weitergehende Normen beschrieben.

Vielmehr stellt OPC UA ein Modell für die IT-Sicherheit zur Verfügung, das in IEC 62541-2 beschrieben ist, in dem Sicherheitsmaßnahmen ausgewählt und konfiguriert werden können, um die Sicherheitsanforderungen einer bestimmten Anlage zu erfüllen. Das Modell umfasst Sicherheitsmechanismen und Parameter. In einigen Fällen ist der Mechanismus für den Austausch von Sicherheitsparametern definiert, aber nicht die Art, wie Anwendungen diese Parameter nutzen. Dieser Rahmen definiert auch eine Mindestmenge von Sicherheitsprofilen, die alle *OPC UA-Anwendungen* unterstützen, selbst wenn sie nicht in allen Anlagen verwendet werden. Die *Profile* der IT-Sicherheit sind in IEC 62541-7 definiert.

5.4.1.2 Erkundung und Einrichten einer Sitzung

Die IT-Sicherheit auf der Anwendungsebene baut auf einem sicheren Kommunikationskanal auf, der während der Anwendungssitzung aktiv ist und die Integrität aller *Nachrichten* (en: messages), die ausgetauscht werden, gewährleistet. Das bedeutet, die Anwender müssen nur einmal, wenn die Anwendungssitzung eingerichtet wird, authentifiziert werden. Die Mechanismen zur Erkundung von *Servern* und zum Einrichten sicherer Kommunikationskanäle und Anwendungssitzungen sind in IEC 62541-4 und IEC 62541-6 beschrieben. Zusätzliche Informationen über den *Erkundungsprozess* befinden sich in IEC 62541-12.

Wenn eine *Sitzung* eingerichtet wird, handeln die *Client*- und *Server*anwendungen einen sicheren Kommunikationskanal aus. Es werden digitale (X.509) *Zertifikate* verwendet, um den *Client* und den *Server* zu identifizieren. Außerdem authentifiziert der *Server* den Anwender und autorisiert die darauffolgenden Anfragen, auf *Objekte* im *Server* zuzugreifen.

5.4.1.3 Auditierung

OPC UA schließt die Unterstützung für die Sicherheitsaudit-Belegsammlungen (en: trails) mit einer Rückverfolgbarkeit zwischen Audit-Protokollen für *Clients* und *Server* ein. Wenn ein sicherheitsbezogenes Problem beim *Server* aufgedeckt wird, kann der zugehörige Audit-Protokolleintrag des *Clients* lokalisiert und geprüft werden. OPC UA stellt auch die Fähigkeit für *Server* zur Verfügung, *Ereignismeldungen* zu erzeugen, die auditierbare *Ereignisse* an *Clients* melden, die diese verarbeiten und protokollieren können. OPC UA definiert Sicherheits-Auditparameter, die in Audit-Protokolleinträgen und in Audit-*Ereignisbenachrichtigungen* enthalten sein können. IEC 62541-5 definiert die Datentypen für diese Parameter. Nicht alle *Server* und *Clients* stellen alle der Auditierungs-Eigenschaften zur Verfügung. Die *Profile* nach IEC 62541-7 zeigen, welche Eigenschaften unterstützt werden.

5.4.1.4 Transportsicherheit

Die IT-Sicherheit von OPC UA ergänzt die Sicherheitsinfrastruktur der meisten Webdienst-fähigen Plattformen.

Die IT-Sicherheit auf der Transportebene kann genutzt werden, um *Nachrichten* zu verschlüsseln und zu signieren. Verschlüsselung und Signaturen schützen gegen Aufdeckung von Informationen und die Datenintegrität von *Nachrichten*. Die Fähigkeiten der Verschlüsselung werden von der unterlagerten Kommunikationstechnologie zur Verfügung gestellt, die zum Austausch von *Nachrichten* zwischen *OPC UA-Anwendungen* verwendet werden. IEC 62541-7 definiert die Verschlüsselung und die Signaturalgorithmen, die für ein bestimmtes *Profil* verwendet werden.

5.4.2 Integriertes Adressraummodell

Die Menge der *Objekte* und zugehörigen Informationen, die der *Server* den *Clients* verfügbar macht, wird als sein *AdressRaum* bezeichnet. Der OPC UA-*AdressRaum* stellt seinen Inhalt als eine Menge von *Knoten* dar, die durch *Referenzen* verbunden sind.

Elementare Eigenschaften von *Knoten* sind durch *Attribute* beschrieben. *Attribute* sind die einzigen Elemente eines *Servers*, die Datenwerte besitzen. Datentypen, die Attributwerte definieren, können einfach oder zusammengesetzt sein.

Knoten im *AdressRaum* haben entsprechend ihrer Verwendung und ihrer Bedeutung eine Typangabe. *KnotenKlassen* definieren die Metadaten für den OPC UA-*AdressRaum*. IEC 62541-3 definiert die OPC UA-*KnotenKlassen*.

Die *BasisKnotenklasse* definiert *Attribute*, die allen *Knoten* gemeinsam sind und die eine Identifikation, Klassifikation und Benennung erlauben. Jede *KnotenKlasse* erbt diese *Attribute* und kann zusätzlich ihre eigenen *Attribute* definieren.

Um die Interoperabilität von *Clients* und *Server* zu fördern, ist der OPC UA-*AdressRaum* hierarchisch so strukturiert, dass die oberen Ebenen für alle *Server* gleich sind. Obwohl auf *Knoten* im *AdressRaum* typischerweise über die Hierarchie zugegriffen wird, können sie *Referenzen* aufeinander haben, die es