



INTERNATIONAL STANDARD

NORME INTERNATIONALE



**OPC unified architecture –
Part 6: Mappings**

**Architecture unifiée OPC –
Partie 6: Correspondances**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 25.040.40; 35.100

ISBN 978-2-8322-2373-4

**Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.**

CONTENTS

| | |
|---|----|
| FOREWORD..... | 7 |
| 1 Scope..... | 9 |
| 2 Normative references | 9 |
| 3 Terms, definitions, abbreviations and symbols..... | 11 |
| 3.1 Terms and definitions..... | 11 |
| 3.2 Abbreviations and symbols | 11 |
| 4 Overview | 12 |
| 5 Data encoding | 13 |
| 5.1 General..... | 13 |
| 5.1.1 Overview | 13 |
| 5.1.2 Built-in Types..... | 13 |
| 5.1.3 Guid..... | 14 |
| 5.1.4 ByteString..... | 15 |
| 5.1.5 ExtensionObject` | 15 |
| 5.1.6 Variant..... | 15 |
| 5.2 OPC UA Binary | 16 |
| 5.2.1 General..... | 16 |
| 5.2.2 Built-in Types..... | 16 |
| 5.2.3 Enumerations..... | 25 |
| 5.2.4 Arrays | 25 |
| 5.2.5 Structures | 25 |
| 5.2.6 Messages | 26 |
| 5.3 XML..... | 26 |
| 5.3.1 Built-in Types..... | 26 |
| 5.3.2 Enumerations..... | 33 |
| 5.3.3 Arrays..... | 33 |
| 5.3.4 Structures | 33 |
| 5.3.5 Messages | 34 |
| 6 Message SecurityProtocols | 34 |
| 6.1 Security handshake | 34 |
| 6.2 Certificates | 35 |
| 6.2.1 General..... | 35 |
| 6.2.2 Application Instance Certificate..... | 36 |
| 6.2.3 Signed Software Certificate..... | 36 |
| 6.3 Time synchronization | 37 |
| 6.4 UTC and International Atomic Time (TAI)..... | 37 |
| 6.5 Issued User Identity Tokens – Kerberos..... | 38 |
| 6.6 WS Secure Conversation | 38 |
| 6.6.1 Overview | 38 |
| 6.6.2 Notation..... | 40 |
| 6.6.3 Request Security Token (RST/SCT)..... | 40 |
| 6.6.4 Request Security Token Response (RSTR/SCT)..... | 41 |
| 6.6.5 Using the SCT | 42 |
| 6.6.6 Cancelling Security contexts..... | 42 |
| 6.7 OPC UA Secure Conversation | 43 |
| 6.7.1 Overview | 43 |

| | | |
|---------------------|---|----|
| 6.7.2 | MessageChunk structure | 43 |
| 6.7.3 | MessageChunks and error handling | 46 |
| 6.7.4 | Establishing a SecureChannel | 47 |
| 6.7.5 | Deriving keys | 48 |
| 6.7.6 | Verifying Message Security | 49 |
| 7 | Transport Protocols | 50 |
| 7.1 | OPC UA TCP | 50 |
| 7.1.1 | Overview | 50 |
| 7.1.2 | Message structure | 50 |
| 7.1.3 | Establishing a connection | 52 |
| 7.1.4 | Closing a connection | 53 |
| 7.1.5 | Error handling | 54 |
| 7.1.6 | Error recovery | 54 |
| 7.2 | SOAP/HTTP | 56 |
| 7.2.1 | Overview | 56 |
| 7.2.2 | XML Encoding | 56 |
| 7.2.3 | OPC UA Binary Encoding | 57 |
| 7.3 | HTTPS | 57 |
| 7.3.1 | Overview | 57 |
| 7.3.2 | XML Encoding | 59 |
| 7.3.3 | OPC UA Binary Encoding | 60 |
| 7.4 | Well known addresses | 60 |
| 8 | Normative Contracts | 61 |
| 8.1 | OPC Binary Schema | 61 |
| 8.2 | XML Schema and WSDL | 61 |
| Annex A (normative) | Constants | 62 |
| A.1 | Attribute Ids | 62 |
| A.2 | Status Codes | 62 |
| A.3 | Numeric Node Ids | 62 |
| Annex B (normative) | OPC UA Nodeset | 64 |
| Annex C (normative) | Type declarations for the OPC UA native Mapping | 65 |
| Annex D (normative) | WSDL for the XML Mapping | 66 |
| D.1 | XML Schema | 66 |
| D.2 | WDSL Port Types | 66 |
| D.3 | WSDL Bindings | 66 |
| Annex E (normative) | Security settings management | 67 |
| E.1 | Overview | 67 |
| E.2 | SecuredApplication | 68 |
| E.3 | CertificateIdentifier | 71 |
| E.4 | CertificateStoreIdentifier | 73 |
| E.5 | CertificateList | 73 |
| E.6 | CertificateValidationOptions | 73 |
| Annex F (normative) | Information Model XML Schema | 75 |
| F.1 | Overview | 75 |
| F.2 | UANodeSet | 75 |
| F.3 | UANode | 76 |
| F.4 | Reference | 76 |
| F.5 | UAType | 77 |

| | | |
|-----------|--|----|
| F.6 | UAInstance | 77 |
| F.7 | UAVariable | 77 |
| F.8 | UAMethod..... | 78 |
| F.9 | TranslationType | 78 |
| F.10 | UADataType | 79 |
| F.11 | DataTypeDefinition | 79 |
| F.12 | DataTypeField | 80 |
| F.13 | Variant..... | 80 |
| F.14 | Example (Informative)..... | 81 |
| | | |
| Figure 1 | – The OPC UA Stack Overview | 13 |
| Figure 2 | – Encoding Integers in a binary stream | 16 |
| Figure 3 | – Encoding Floating Points in a binary stream..... | 17 |
| Figure 4 | – Encoding Strings in a binary stream | 17 |
| Figure 5 | – Encoding GuidS in a binary stream..... | 18 |
| Figure 6 | – Encoding XmlElements in a binary stream..... | 19 |
| Figure 7 | – A String NodeId..... | 20 |
| Figure 8 | – A Two Byte NodeId | 20 |
| Figure 9 | – A Four Byte NodeId..... | 21 |
| Figure 10 | – Security handshake..... | 34 |
| Figure 11 | – Relevant XML Web Services specifications | 39 |
| Figure 12 | – The WS Secure Conversation handshake..... | 39 |
| Figure 13 | – OPC UA Secure Conversation MessageChunk..... | 43 |
| Figure 14 | – OPC UA TCP Message structure..... | 52 |
| Figure 15 | – Establishing a OPC UA TCP connection..... | 53 |
| Figure 16 | – Closing a OPC UA TCP connection | 53 |
| Figure 17 | – Recovering an OPC UA TCP connection | 55 |
| Figure 18 | – Scenarios for the HTTPS Transport..... | 58 |
| | | |
| Table 1 | – Built-in Data Types..... | 14 |
| Table 2 | – Guid structure | 14 |
| Table 3 | – Supported Floating Point Types..... | 17 |
| Table 4 | – NodeId components | 19 |
| Table 5 | – NodeId DataEncoding values | 19 |
| Table 6 | – Standard NodeId Binary DataEncoding..... | 19 |
| Table 7 | – Two Byte NodeId Binary DataEncoding | 20 |
| Table 8 | – Four Byte NodeId Binary DataEncoding..... | 20 |
| Table 9 | – ExpandedNodeId Binary DataEncoding | 21 |
| Table 10 | – DiagnosticInfo Binary DataEncoding..... | 22 |
| Table 11 | – QualifiedName Binary DataEncoding | 22 |
| Table 12 | – LocalizedText Binary DataEncoding | 22 |
| Table 13 | – Extension Object Binary DataEncoding..... | 23 |
| Table 14 | – Variant Binary DataEncoding..... | 24 |
| Table 15 | – Data Value Binary DataEncoding..... | 25 |

This is a preview of "IEC 62541-6 Ed. 2.0 ...". [Click here to purchase the full version from the ANSI store.](#)

| | |
|---|----|
| Table 16 – Sample OPC UA Binary Encoded structure..... | 26 |
| Table 17 – XML Data Type Mappings for Integers..... | 27 |
| Table 18 – XML Data Type Mappings for Floating Points | 27 |
| Table 19 – Components of NodeId | 29 |
| Table 20 – Components of ExpandedNodeId | 30 |
| Table 21 – Components of Enumeration | 33 |
| Table 22 – SecurityPolicy | 35 |
| Table 23 – ApplicationInstanceCertificate | 36 |
| Table 24 – SignedSoftwareCertificate | 37 |
| Table 25 – Kerberos UserTokenPolicy | 38 |
| Table 26 – WS-* Namespace prefixes | 40 |
| Table 27 – RST/SCT Mapping to an OpenSecureChannel Request..... | 41 |
| Table 28 – RSTR/SCT Mapping to an OpenSecureChannel Response..... | 42 |
| Table 29 – OPC UA Secure Conversation Message header | 44 |
| Table 30 – Asymmetric algorithm Security header..... | 44 |
| Table 31 – Symmetric algorithm Security header | 45 |
| Table 32 – Sequence header | 45 |
| Table 33 – OPC UA Secure Conversation Message footer | 46 |
| Table 34 – OPC UA Secure Conversation Message abort body..... | 47 |
| Table 35 – OPC UA Secure Conversation OpenSecureChannel Service | 47 |
| Table 36 – Cryptography key generation parameters | 49 |
| Table 37 – OPC UA TCP Message header..... | 50 |
| Table 38 – OPC UA TCP Hello Message..... | 51 |
| Table 39 – OPC UA TCP Acknowledge Message | 51 |
| Table 40 – OPC UA TCP Error Message..... | 52 |
| Table 41 – OPC UA TCP error codes | 54 |
| Table 42 – WS-Addressing headers | 56 |
| Table 43 – Well known addresses for Local Discovery Servers | 60 |
| Table A.1 – Identifiers assigned to Attributes | 62 |
| Table E.1 – SecuredApplication | 69 |
| Table E.2 – CertificateIdentifier..... | 71 |
| Table E.3 – Structured directory store..... | 72 |
| Table E.4 – CertificateStoreIdentifier | 73 |
| Table E.5 – CertificateList..... | 73 |
| Table E.6 – CertificateValidationOptions | 74 |
| Table F.1 – UANodeSet | 75 |
| Table F.2 – UANode | 76 |
| Table F.3 – Reference | 77 |
| Table F.4 – UANodeSet Type Nodes..... | 77 |
| Table F.5 – UANodeSet Instance Nodes | 77 |
| Table F.6 – UAInstance | 77 |
| Table F.7 – UAVariable..... | 78 |
| Table F.8 – UAMethod | 78 |

This is a preview of "IEC 62541-6 Ed. 2.0 ...". [Click here to purchase the full version from the ANSI store.](#)

| | |
|--------------------------------------|----|
| Table F.9 – TranslationType | 79 |
| Table F.10 – UADatatype..... | 79 |
| Table F.11 – DataTypeDefinition..... | 80 |
| Table F.12 – DataTypeField..... | 80 |

INTERNATIONAL ELECTROTECHNICAL COMMISSION

OPC UNIFIED ARCHITECTURE –

Part 6: Mappings

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62541-6 has been prepared by subcommittee 65E: Devices and integration in enterprise systems, of IEC technical committee 65: Industrial-process measurement, control and automation.

This second edition cancels and replaces the first edition published in 2011. This edition constitutes a technical revision.

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

- a) Some applications need to operation in environments with no access to cryptography libraries. To support this a new HTTPS transport has been defined in 7.3;
- b) The padding byte is not long enough to handle asymmetric key sizes larger than 2048 bits. Added an additional padding byte to 6.7.2 to handle this case.
- c) Fixed errors in SOAP action URIs defined in 7.2.2;

This is a preview of "IEC 62541-6 Ed. 2.0 ...". [Click here to purchase the full version from the ANSI store.](#)

d) Needed a standard way to serialize nodes in an address space. Added the UANodeSet schema defined in Annex F;

The text of this standard is based on the following documents:

| | |
|-------------|------------------|
| CDV | Report on voting |
| 65E/377/CDV | 65E/405/RVC |

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

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

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.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

OPC UNIFIED ARCHITECTURE –

Part 6: Mappings

1 Scope

This part of IEC 62541 specifies the OPC Unified Architecture (OPC UA) mapping between the security model described in IEC TR 62541-2, the abstract service definitions, described in IEC 62541-4, the data structures defined in IEC 62541-5 and the physical network protocols that can be used to implement the OPC UA specification.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. 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 62541-7, *OPC Unified Architecture – Part 7: Profiles*

XML Schema Part 1: XML Schema Part 1: Structures

<http://www.w3.org/TR/xmlschema-1/>

XML Schema Part 2: XML Schema Part 2: Datatypes

<http://www.w3.org/TR/xmlschema-2/>

SOAP Part 1: SOAP Version 1.2 Part 1: Messaging Framework

<http://www.w3.org/TR/soap12-part1/>

SOAP Part 2: SOAP Version 1.2 Part 2: Adjuncts

<http://www.w3.org/TR/soap12-part2/>

XML Encryption: XML Encryption Syntax and Processing

<http://www.w3.org/TR/xmlenc-core/>

XML Signature: XML-Signature Syntax and Processing

<http://www.w3.org/TR/xmldsig-core/>

WS Security: SOAP Message Security 1.1

<http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf>

This is a preview of "IEC 62541-6 Ed. 2.0 ...". Click here to purchase the full version from the ANSI store.

WS Addressing: Web Services Addressing (WS-Addressing)

<http://www.w3.org/Submission/ws-addressing/>

WS Trust: WS Trust 1.3

<http://docs.oasis-open.org/ws-sx/ws-trust/v1.3/ws-trust.html>

WS Secure Conversation: WS Secure Conversation 1.3

<http://docs.oasis-open.org/ws-sx/ws-secureconversation/v1.3/ws-secureconversation.html>

WS Security Policy: WS Security Policy 1.2

<http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/ws-securitypolicy-1.2-spec-os.html>

SSL/TLS: RFC 5246 – The TLS Protocol Version 1.2

<http://tools.ietf.org/html/rfc5246.txt>

X509: X.509 Public Key Certificate Infrastructure

<http://www.itu.int/rec/T-REC-X.509-200003-I/e>

WS-I Basic Profile 1.1: WS-I Basic Profile Version 1.1

<http://www.ws-i.org/Profiles/BasicProfile-1.1.html>

WS-I Basic Security Profile 1.1: WS-I Basic Security Profile Version 1.1

<http://www.ws-i.org/Profiles/BasicSecurityProfile-1.1.html>

HTTP: RFC 2616 – Hypertext Transfer Protocol – HTTP/1.1

<http://www.ietf.org/rfc/rfc2616.txt>

Base64: RFC 3548 – The Base16, Base32, and Base64 Data Encodings

<http://www.ietf.org/rfc/rfc3548.txt>

X690: ITU-T X.690 – Basic (BER), Canonical (CER) and Distinguished (DER) Encoding Rules

<http://www.itu.int/ITU-T/studygroups/com17/languages/X.690-0207.pdf>

IEEE-754: Standard for Binary Floating-Point Arithmetic

<http://grouper.ieee.org/groups/754/>

HMAC: HMAC – Keyed-Hashing for Message Authentication

<http://www.ietf.org/rfc/rfc2104.txt>

PKCS #1: PKCS #1 – RSA Cryptography Specifications Version 2.0

<http://www.ietf.org/rfc/rfc2437.txt>

FIPS 180-2: Secure Hash Standard (SHA)

<http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf>

FIPS 197: Advanced Encryption Standard (AES)

<http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

UTF8: UTF-8, a transformation format of ISO 10646

<http://tools.ietf.org/html/rfc3629>

RFC 3280: RFC 3280 – X.509 Public Key Infrastructure Certificate and CRL Profile

<http://www.ietf.org/rfc/rfc3280.txt>

RFC 4514: RFC 4514 – LDAP: String Representation of Distinguished Names

This is a preview of "IEC 62541-6 Ed. 2.0 ...". Click here to purchase the full version from the ANSI store.

<http://www.ietf.org/rfc/rfc4514.txt>

NTP: RFC 1305 – Network Time Protocol (Version 3)

<http://www.ietf.org/rfc/rfc1305.txt>

Kerberos: WS Security Kerberos Token Profile 1.1

<http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-KerberosTokenProfile.pdf>

SOMMAIRE

| | |
|---|-----|
| AVANT-PROPOS | 89 |
| 1 Domaine d'application | 91 |
| 2 Références normatives | 91 |
| 3 Termes, définitions, abréviations et symboles | 93 |
| 3.1 Termes et définitions | 93 |
| 3.2 Abréviations et symboles | 93 |
| 4 Vue d'ensemble | 94 |
| 5 Codage de données | 95 |
| 5.1 Généralités | 95 |
| 5.1.1 Vue d'ensemble | 95 |
| 5.1.2 Types intégrés | 96 |
| 5.1.3 Guid (Identificateur globalement Unique) | 96 |
| 5.1.4 Chaîne d'octets | 97 |
| 5.1.5 Objet d'Extension | 97 |
| 5.1.6 Variante | 97 |
| 5.2 OPC UA Binaire | 98 |
| 5.2.1 Généralités | 98 |
| 5.2.2 Types intégrés | 98 |
| 5.2.3 Énumérations | 107 |
| 5.2.4 Matrices | 107 |
| 5.2.5 Structures | 108 |
| 5.2.6 Messages | 108 |
| 5.3 XML | 109 |
| 5.3.1 Types intégrés | 109 |
| 5.3.2 Énumérations | 115 |
| 5.3.3 Matrices | 116 |
| 5.3.4 Structures | 116 |
| 5.3.5 Messages | 116 |
| 6 Protocoles de sécurité des messages | 116 |
| 6.1 Protocole d'établissement de liaison de sécurité | 116 |
| 6.2 Certificats | 118 |
| 6.2.1 Généralités | 118 |
| 6.2.2 Certificat d'instance d'application | 118 |
| 6.2.3 Certificat de logiciel signé | 119 |
| 6.3 Synchronisation horaire | 120 |
| 6.4 Temps universel coordonné (UTC) et Temps atomique international (TAI) | 121 |
| 6.5 Jetons d'identité d'utilisateur émis – Jetons Kerberos | 121 |
| 6.6 Conversation sécurisée WS | 121 |
| 6.6.1 Vue d'ensemble | 121 |
| 6.6.2 Notation | 123 |
| 6.6.3 Demande de jeton de sécurité (RST/SCT) | 123 |
| 6.6.4 Réponse à la Demande de jeton de sécurité (RSTR/SCT) | 124 |
| 6.6.5 Utilisation du SCT | 125 |
| 6.6.6 Annulation des contextes de sécurité | 125 |
| 6.7 Conversation OPC UA sécurisée | 126 |
| 6.7.1 Vue d'ensemble | 126 |

| | | |
|----------------------|--|-----|
| 6.7.2 | Structure des Blocs de Messages | 126 |
| 6.7.3 | Blocs de Messages et traitement d'erreurs..... | 130 |
| 6.7.4 | Établissement d'un Canal Sécurisé | 131 |
| 6.7.5 | Dérivation des clés | 132 |
| 6.7.6 | Vérification de la sécurité d'un message | 133 |
| 7 | Protocoles de Transport | 134 |
| 7.1 | Protocole OPC UA TCP | 134 |
| 7.1.1 | Vue d'ensemble | 134 |
| 7.1.2 | Structure de message | 134 |
| 7.1.3 | Établissement d'une connexion..... | 137 |
| 7.1.4 | Fermeture d'une connexion..... | 138 |
| 7.1.5 | Traitement d'erreurs | 139 |
| 7.1.6 | Recouvrement d'erreurs..... | 139 |
| 7.2 | Protocole SOAP/HTTP | 141 |
| 7.2.1 | Vue d'ensemble | 141 |
| 7.2.2 | Codage XML..... | 142 |
| 7.2.3 | Codage OPC UA Binaire..... | 142 |
| 7.3 | Protocole HTTPS | 143 |
| 7.3.1 | Vue d'ensemble | 143 |
| 7.3.2 | Codage XML..... | 145 |
| 7.3.3 | Codage Binaire OPC UA..... | 146 |
| 7.4 | Adresses notoires | 146 |
| 8 | Contrats normatifs | 147 |
| 8.1 | Schéma OPC binaire | 147 |
| 8.2 | Schéma XML et langage WSDL | 147 |
| Annexe A (normative) | Constantes..... | 148 |
| A.1 | Identificateurs d'attributs..... | 148 |
| A.2 | Codes de Statut | 148 |
| A.3 | Identificateurs de nœud numériques | 148 |
| Annexe B (normative) | Ensemble de nœuds OPC UA | 150 |
| Annexe C (normative) | Déclarations de type pour la correspondance d'origine OPC UA | 151 |
| Annexe D (normative) | Langage WSDL pour la correspondance XML | 152 |
| D.1 | Schéma XML | 152 |
| D.2 | Types de port WDSL..... | 152 |
| D.3 | Liaisons WSDL | 152 |
| Annexe E (normative) | Gestion des paramètres de sécurité | 153 |
| E.1 | Vue d'ensemble | 153 |
| E.2 | Application Sécurisée | 154 |
| E.3 | Identificateur de Certificat..... | 157 |
| E.4 | Identificateur de Mémoire de Certificat..... | 159 |
| E.5 | Liste de Certificats | 160 |
| E.6 | Options de Validation des Certificats | 160 |
| Annexe F (normative) | Schéma XML du Modèle d'Informations | 162 |
| F.1 | Vue d'ensemble | 162 |
| F.2 | Ensemble de Nœuds UA..... | 162 |
| F.3 | Nœuds UA..... | 163 |
| F.4 | Référence | 164 |
| F.5 | Type UA..... | 165 |

| | | |
|------------|---|-----|
| F.6 | Instance UA | 165 |
| F.7 | Variable UA | 165 |
| F.8 | Méthode UA | 166 |
| F.9 | Type de traduction | 166 |
| F.10 | Type de Données UA | 167 |
| F.11 | Définition du Type de Données | 168 |
| F.12 | Champ de Type de Données | 168 |
| F.13 | Variante | 169 |
| F.14 | Exemple (Informatif) | 169 |
| | | |
| Figure 1 | – Vue d'ensemble des piles OPC UA | 95 |
| Figure 2 | – Codage des entiers dans une séquence binaire | 99 |
| Figure 3 | – Codage des virgules flottantes dans une séquence binaire | 99 |
| Figure 4 | – Codage de chaînes dans une séquence binaire | 100 |
| Figure 5 | – Codage des Guid dans une séquence binaire..... | 101 |
| Figure 6 | – Codage des Eléments Xml dans une séquence binaire..... | 101 |
| Figure 7 | – Identificateur de Nœud de chaîne | 102 |
| Figure 8 | – Identificateur de Nœud à deux octets | 103 |
| Figure 9 | – Identificateur de Nœud à quatre octets..... | 103 |
| Figure 10 | – Protocole d'établissement de liaison de sécurité | 117 |
| Figure 11 | – Spécifications appropriées des services Web XML | 122 |
| Figure 12 | – Protocole d'établissement de liaison de Conversation sécurisée WS | 122 |
| Figure 13 | – Bloc de Messages de Conversation sécurisée OPC UA..... | 126 |
| Figure 14 | – Structure de message OPC UA TCP | 137 |
| Figure 15 | – Établissement d'une connexion OPC UA TCP | 138 |
| Figure 16 | – Fermeture d'une connexion OPC UA TCP | 138 |
| Figure 17 | – Rétablissement d'une connexion OPC UA TCP | 141 |
| Figure 18 | – Scénarii pour le transport HTTPS | 144 |
| | | |
| Tableau 1 | – Types de Données intégrés | 96 |
| Tableau 2 | – Structure du Guid | 96 |
| Tableau 3 | – Types à virgule flottante pris en charge | 99 |
| Tableau 4 | – Composants d'un Identificateur de Nœud | 101 |
| Tableau 5 | – Valeurs de Codage de Données de l'Identificateur de Nœud | 102 |
| Tableau 6 | – Codage de Données binaires normalisé d'Identificateur de Nœud | 102 |
| Tableau 7 | – Codage de Données binaires de l'Identificateur de nœud à deux octets | 102 |
| Tableau 8 | – Codage de Données binaires de l'Identificateur de Nœud à quatre octets..... | 103 |
| Tableau 9 | – Codage de Données Binaires de l'Identificateur de Nœud Etendu | 104 |
| Tableau 10 | – Codage de Données Binaires de l'Information de Diagnostic | 104 |
| Tableau 11 | – Codage de Données Binaires de Nom Qualifié | 105 |
| Tableau 12 | – Codage de Données Binaires de Texte Localisé | 105 |
| Tableau 13 | – Codage de Données Binaires de l'Objet d'Extension..... | 106 |
| Tableau 14 | – Codage de Données Binaires de Variante..... | 106 |
| Tableau 15 | – Codage de Données Binaires de la Valeur de Données | 107 |

| | |
|--|-----|
| Tableau 16 – Échantillon de structure codée binaire OPC UA | 108 |
| Tableau 17 – Correspondances des types de données XML pour des Entiers | 109 |
| Tableau 18 – Correspondances de types de données XML pour les virgules flottantes | 109 |
| Tableau 19 – Composants de l'Identificateur de Nœud | 111 |
| Tableau 20 – Composants de l'Identificateur de Nœud Etendu | 112 |
| Tableau 21 – Composants d'Énumération | 115 |
| Tableau 22 – Politique de Sécurité | 117 |
| Tableau 23 – Certificat d'Instance d'Application | 119 |
| Tableau 24 – Certificat de Logiciel Signé | 120 |
| Tableau 25 – Politique pour le Jeton Utilisateur (UserTokenPolicy) Kerberos..... | 121 |
| Tableau 26 – Préfixes d'Espace de nom WS-* | 123 |
| Tableau 27 – Correspondance RST/SCT avec une demande Ouverture de Canal Sécurisé | 124 |
| Tableau 28 – Correspondance RSTR/SCT avec une Réponse d'Ouverture de Canal Sécurisé | 125 |
| Tableau 29 – En-tête de message de Conversation OPC UA Sécurisée..... | 127 |
| Tableau 30 – En-tête de sécurité d'algorithme asymétrique | 128 |
| Tableau 31 – En-tête de sécurité d'algorithme symétrique | 129 |
| Tableau 32 – En-tête de séquence..... | 129 |
| Tableau 33 – Cartouche de message de Conversation Sécurisée OPC UA | 130 |
| Tableau 34 – Corps de l'abandon de message de Conversation Sécurisée OPC UA..... | 131 |
| Tableau 35 – Service d'Ouverture d'un Canal Sécurisé pour une Conversation Sécurisée OPC UA | 131 |
| Tableau 36 – Paramètres de génération de clés de cryptographie | 133 |
| Tableau 37 – En-tête de message OPC UA TCP..... | 135 |
| Tableau 38 – Message d'Accueil OPC UA TCP..... | 135 |
| Tableau 39 – Message d'Acquittement de protocole OPC UA TCP..... | 136 |
| Tableau 40 – Message d'erreur OPC UA TCP..... | 136 |
| Tableau 41 – Codes d'erreurs OPC UA TCP | 139 |
| Tableau 42 – En-têtes d'adressage WS | 142 |
| Tableau 43 – Adresses notoires pour les serveurs de découverte locaux..... | 146 |
| Tableau A.1 – Identificateurs affectés aux attributs | 148 |
| Tableau E.1 – Application Sécurisée..... | 155 |
| Tableau E.2 – Identificateur de certificat | 158 |
| Tableau E.3 – Mémoire Répertoire structurée | 159 |
| Tableau E.4 – Identificateur de Mémoire de Certificat | 160 |
| Tableau E.5 – Liste de Certificats | 160 |
| Tableau E.6 – Options de Validation des Certificats..... | 161 |
| Tableau F.1 – Ensemble de Nœuds UA | 163 |
| Tableau F.2 – Nœud UA | 164 |
| Tableau F.3 – Référence | 164 |
| Tableau F.4 – Nœuds du Type Ensemble de Nœuds UA..... | 165 |
| Tableau F.5 – Nœuds de l'Instance Ensemble de Nœuds UA | 165 |
| Tableau F.6 – Instance UA | 165 |

This is a preview of "IEC 62541-6 Ed. 2.0 ...". [Click here to purchase the full version from the ANSI store.](#)

| | |
|--|-----|
| Tableau F.7 – Variable UA | 166 |
| Tableau F.8 – Méthode UA | 166 |
| Tableau F.9 – Type de traduction | 167 |
| Tableau F.10 – Type de Données UA | 168 |
| Tableau F.11 – Définition du Type de Données | 168 |
| Tableau F.12 – Champ de Type de Données | 169 |

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

ARCHITECTURE UNIFIÉE OPC –

Partie 6: Correspondances

AVANT-PROPOS

- 1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. À cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
- 2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
- 3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
- 4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
- 5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
- 6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
- 7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
- 8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
- 9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La norme internationale IEC 62541-6 a été établie par le sous-comité 65E: Les dispositifs et leur intégration dans les systèmes de l'entreprise, du comité d'études 65 de l'IEC: Mesure, commande et automation dans les processus industriels.

Cette deuxième édition annule et remplace la première édition parue en 2011. Cette édition constitue une révision technique.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

- a) Certaines applications ont besoin de fonctionner dans des environnements ne disposant pas d'accès à des bibliothèques de cryptographie. Pour pallier ce problème, un nouveau protocole de transport HTTPS a été défini en 7.3;

This is a preview of "IEC 62541-6 Ed. 2.0 ...". [Click here to purchase the full version from the ANSI store.](#)

- b) La longueur de l'octet de remplissage n'est pas suffisante pour gérer les tailles des clés asymétriques de longueur supérieure à 2048 bits. Ajout d'un octet de remplissage supplémentaire en 6.7.2 pour gérer ce cas.
- c) Définition des erreurs fixes dans les URI d'action SOAP en 7.2.2;
- d) Nécessité d'une méthode normalisée permettant de sérialiser les nœuds dans un espace d'adresses. Ajout du schéma de l'Ensemble de Nœuds UA (UANodeSet) défini à l'Annexe F.

Le texte de cette norme est issu des documents suivants:

| CDV | Rapport de vote |
|-------------|-----------------|
| 65E/377/CDV | 65E/405/RVC |

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

Cette publication a été rédigée selon les Directives ISO/IEC, Partie 2.

Une liste de toutes les parties de la série IEC 62541, publiées sous le titre général *Architecture unifiée OPC*, peut être consultée sur le site web de l'IEC.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "<http://webstore.iec.ch>" dans les données relatives à la publication recherchée. À cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

ARCHITECTURE UNIFIÉE OPC –

Partie 6: Correspondances

1 Domaine d'application

La présente partie de l'IEC 62541 spécifie les correspondances de l'architecture unifiée OPC (OPC UA) entre le modèle de sécurité décrit dans l'IEC TR 62541-2, les définitions de services abstraits décrites dans l'IEC 62541-4, les structures de données définies dans l'IEC 62541-5 et les protocoles de réseaux physiques qui peuvent être utilisés pour mettre en œuvre la spécification OPC UA.

2 Références normatives

Les documents suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC TR 62541-1, *OPC Unified Architecture – Part 1: Overview and concepts* (disponible en anglais seulement)

IEC TR 62541-2, *OPC Unified Architecture – Part 2: Security model* (disponible en anglais seulement)

IEC 62541-3, *Architecture unifiée OPC – Partie 3: Modèle de l'espace d'adressage*

IEC 62541-4, *Architecture unifiée OPC – Partie 4: Services*

IEC 62541-5, *Architecture unifiée OPC – Partie 5: Modèle d'Information*

IEC 62541-7, *Architecture unifiée OPC – Partie 7: Profils*

XML Schema Part 1: XML Schema Part 1: Structures

<http://www.w3.org/TR/xmlschema-1/>

XML Schema Part 2: XML Schema Part 2: Datatypes

<http://www.w3.org/TR/xmlschema-2/>

SOAP Part 1: SOAP Version 1.2 Part 1: Messaging Framework

<http://www.w3.org/TR/soap12-part1/>

SOAP Part 2: SOAP Version 1.2 Part 2: Adjuncts

<http://www.w3.org/TR/soap12-part2/>

XML Encryption: XML Encryption Syntax and Processing

<http://www.w3.org/TR/xmlenc-core/>

XML Signature: XML-Signature Syntax and Processing

<http://www.w3.org/TR/xmlsig-core/>

WS Security: SOAP Message Security 1.1

This is a preview of "IEC 62541-6 Ed. 2.0 ...". Click here to purchase the full version from the ANSI store.

<http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf>

WS Addressing: Web Services Addressing (WS-Addressing)

<http://www.w3.org/Submission/ws-addressing/>

WS Trust: WS Trust 1.3

<http://docs.oasis-open.org/ws-sx/ws-trust/v1.3/ws-trust.html>

WS Secure Conversation: WS Secure Conversation 1.3

<http://docs.oasis-open.org/ws-sx/ws-secureconversation/v1.3/ws-secureconversation.html>

WS Security Policy: WS Security Policy 1.2

<http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/ws-securitypolicy-1.2-spec-os.html>

SSL/TLS: RFC 5246 – *The TLS Protocol Version 1.2*

<http://tools.ietf.org/html/rfc5246.txt>

X509: X.509 Public Key Certificate Infrastructure

<http://www.itu.int/rec/T-REC-X.509-200003-I/e>

WS-I Basic Profile 1.1: WS-I Basic Profile Version 1.1

<http://www.ws-i.org/Profiles/BasicProfile-1.1.html>

WS-I Basic Security Profile 1.1: WS-I Basic Security Profile Version 1.1

<http://www.ws-i.org/Profiles/BasicSecurityProfile-1.1.html>

HTTP: RFC 2616 – Hypertext Transfer Protocol – HTTP/1.1

<http://www.ietf.org/rfc/rfc2616.txt>

Base64: RFC 3548 – The Base16, Base32, and Base64 Data Encodings

<http://www.ietf.org/rfc/rfc3548.txt>

X690: ITU-T X.690 – Basic (BER), Canonical (CER) and Distinguished (DER) Encoding Rules

<http://www.itu.int/ITU-T/studygroups/com17/languages/X.690-0207.pdf>

IEEE-754: Standard for Binary Floating-Point Arithmetic

<http://grouper.ieee.org/groups/754/>

HMAC: HMAC – Keyed-Hashing for Message Authentication

<http://www.ietf.org/rfc/rfc2104.txt>

PKCS #1: PKCS #1 – RSA Cryptography Specifications Version 2.0

<http://www.ietf.org/rfc/rfc2437.txt>

FIPS 180-2: Secure Hash Standard (SHA)

<http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf>

FIPS 197: Advanced Encryption Standard (AES)

<http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

UTF8: UTF-8, a transformation format of ISO 10646

<http://tools.ietf.org/html/rfc3629>

RFC 3280: RFC 3280 X.509 Public Key Infrastructure Certificate and CRL Profile

This is a preview of "IEC 62541-6 Ed. 2.0 ...". Click here to purchase the full version from the ANSI store.

<http://www.ietf.org/rfc/rfc3280.txt>

RFC 4514: RFC 4514 – LDAP: String Representation of Distinguished Names

<http://www.ietf.org/rfc/rfc4514.txt>

NTP: RFC 1305 – Network Time Protocol (Version 3)

<http://www.ietf.org/rfc/rfc1305.txt>

Kerberos: WS Security Kerberos Token Profile 1.1

<http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-KerberosTokenProfile.pdf>