

This is a preview - click here to buy the full publication



IEC TR 62541-2

Edition 3.0 2020-11
REDLINE VERSION

TECHNICAL REPORT



OPC unified architecture – Part 2: Security Model

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 25.040.40; 35.100.01

ISBN 978-2-8322-9089-7

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

FOREWORD	5
1 Scope	8
2 Normative references	8
3 Terms, definitions, and abbreviated terms	10
3.1 Terms and definitions.....	10
3.2 Abbreviated terms.....	15
4 OPC UA security architecture	16
4.1 OPC UA security environment.....	16
4.2 Security objectives.....	17
4.2.1 Overview	17
4.2.2 Authentication.....	17
4.2.3 Authorization	18
4.2.4 Confidentiality.....	18
4.2.5 Integrity	18
4.2.6 Non-Repudiation.....	18
4.2.7 Auditability.....	18
4.2.8 Availability	18
4.3 Security threats to OPC UA systems	18
4.3.1 Overview	18
4.3.2 Denial of Service	19
4.3.3 Eavesdropping.....	20
4.3.4 Message spoofing.....	20
4.3.5 Message alteration	20
4.3.6 Message replay	20
4.3.7 Malformed Messages.....	21
4.3.8 Server profiling	21
4.3.9 Session hijacking.....	21
4.3.10 Rogue Server	21
4.3.11 Rogue Publisher	22
4.3.12 Compromising user credentials.....	22
4.3.13 Repudiation	22
4.4 OPC UA relationship to site security	22
4.5 OPC UA security architecture	23
4.5.1 Overview	23
4.5.2 Client / Server	24
4.5.3 Publish-Subscribe.....	25
4.6 SecurityPolicies	26
4.7 Security Profiles.....	27
4.8 Security Mode Settings	27
4.9 User Authentication	28
4.10 Application Authentication.....	28
4.11 User Authorization	28
4.12 Roles	28
4.13 OPC UA security related Services.....	29
4.14 Auditing	30
4.14.1 General	30

4.14.2	Single Client and Server	31
4.14.3	Aggregating Server	31
4.14.4	Aggregation through a non-auditing Server	32
4.14.5	Aggregating Server with service distribution	33
5	Security reconciliation	34
5.1	Reconciliation of threats with OPC UA security mechanisms	34
5.1.1	Overview	34
5.1.2	Denial of Service	35
5.1.3	Eavesdropping	36
5.1.4	Message spoofing	36
5.1.5	Message alteration	37
5.1.6	Message replay	37
5.1.7	Malformed Messages	37
5.1.8	Server profiling	37
5.1.9	Session hijacking	37
5.1.10	Rogue Server or Publisher	38
5.1.11	Compromising user credentials	38
5.1.12	Repudiation	38
5.2	Reconciliation of objectives with OPC UA security mechanisms	38
5.2.1	Overview	38
5.2.2	Application Authentication	38
5.2.3	User Authentication	39
5.2.4	Authorization	39
5.2.5	Confidentiality	39
5.2.6	Integrity	39
5.2.7	Auditability	39
5.2.8	Availability	40
6	Implementation and deployment considerations	40
6.1	Overview	40
6.2	Appropriate timeouts	40
6.3	Strict Message processing	40
6.4	Random number generation	41
6.5	Special and reserved packets	41
6.6	Rate limiting and flow control	41
6.7	Administrative access	41
6.8	Cryptographic Keys	42
6.9	Alarm related guidance	42
6.10	Program access	42
6.11	Audit event management	43
6.12	OAuth2, JWT and User roles	43
6.13	HTTPs, SSL/TLS & Websockets	43
6.14	Reverse Connect	43
7	Unsecured Services	44
7.1	Overview	44
7.2	Multicast Discovery	44
7.3	Global Discovery Server Security	44
7.3.1	Overview	44
7.3.2	Rogue GDS	44
7.3.3	Threats against a GDS	45

7.3.4	Certificate management threats	45
8	Certificate management.....	46
8.1.1	Overview	46
8.1.2	Self-signed certificate management	46
8.1.3	CA Signed Certificate management	47
8.1.4	GDS Certificate Management	48
	Bibliography.....	52
	Figure 1 – OPC UA network model example	17
	Figure 2 – OPC UA security architecture – Client / Server	23
	Figure 3 – OPC UA security architecture – Publisher-Subscriber	24
	Figure 4 – Role overview	29
	Figure 5 – Simple Servers.....	31
	Figure 6 – Aggregating Servers	32
	Figure 7 – Aggregation with a non-auditing Server.....	33
	Figure 8 – Aggregate Server with service distribution.....	34
	Figure 9 – Manual Certificate handling.....	47
	Figure 10 – CA Certificate handling	48
	Figure 11 – Certificate handling	49
	Table 1 – Security Reconciliation Threats Summary	35

INTERNATIONAL ELECTROTECHNICAL COMMISSION

OPC UNIFIED ARCHITECTURE –

Part 2: Security Model

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.

This redline version of the official IEC Standard allows the user to identify the changes made to the previous edition. A vertical bar appears in the margin wherever a change has been made. Additions are in green text, deletions are in strikethrough red text.

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 TR 62541-2, which is a technical report, has been prepared by subcommittee 65E: Devices and integration in enterprise systems, of IEC technical committee 65: Industrial-process measurement, control and automation.

This third edition cancels and replaces the second edition of IEC TR 62541-2, published in 2016. This edition constitutes a technical revision.

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

- a) protection-targets definition change;
- b) threat type clarifications;
- c) expanded best practices;
- d) added Websockets;
- e) added Pub/Sub.

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

Enquiry draft	Report on voting
65E/679/DTR	65E/703/RVDR

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 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.

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 2: Security Model

1 Scope

This part of IEC 62541 describes the OPC Unified Architecture (OPC UA) security model. It describes the security threats of the physical, hardware, and software environments in which OPC UA is expected to run. It describes how OPC UA relies upon other standards for security. It provides definition of common security terms that are used in this and other parts of the OPC UA specification. It gives an overview of the security features that are specified in other parts of the OPC UA specification. It references services, mappings, and *Profiles* that are specified normatively in other parts of ~~this multi-part~~ the OPC UA Specification. It provides suggestions or best practice guidelines on implementing security. Any seeming ambiguity between this part and one of the *other* normative parts does not remove or reduce the requirement specified in the *other* normative part.

Note It is important to understand that there are many different aspects of security that have to be addressed when developing applications. However, since OPC UA specifies a communication protocol, the focus is on securing the data exchanged between applications. This does not mean that an application developer can ignore the other aspects of security like protecting persistent data against tampering. It is important that the developers look into all aspects of security and decide how they can be addressed in the application.

This part is directed to readers who will develop OPC UA *Client* or *Server* applications or implement the OPC UA services layer. It is also for end Users that wish to understand the various security features and functionality provided by OPC UA. It also offers some suggestions that can be applied when deploying systems. These suggestions are generic in nature since the details would depend on the actual implementation of the *OPC UA Applications* and the choices made for the site security.

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

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

~~IEC 62351 (all parts), Power systems management and associated information exchange – Data and communications security~~

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

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 TR 62541-2:2020 RLV © IEC 2020 – 9 –

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

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

IEC 62351 (all parts), *Power systems management and associated information exchange*

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

~~Available from Internet: <http://www.w3.org/TR/soap12-part1/> (website checked 2016-04-05)~~

~~SOAP Part 2: SOAP Version 1.2 Part 2: Adjuncts~~

~~Available from Internet: <http://www.w3.org/TR/soap12-part2/> (website checked 2016-04-05)~~

~~XML Encryption: XML Encryption Syntax and Processing~~

~~Available from Internet: <http://www.w3.org/TR/xmlenc-core/> (website checked 2016-04-05)~~

~~XML Signature: XML Signature Syntax and Processing~~

~~Available from Internet: <http://www.w3.org/TR/xmlsig-core/> (website checked 2016-04-05)~~

~~WS Security: SOAP Message Security 1.1~~

~~Available from Internet: <http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf> (website checked 2016-04-05)~~

~~WS Secure Conversation: Web Services Secure Conversation Language (WS-SecureConversation)~~

~~Available from Internet: <http://specs.xmlsoap.org/ws/2005/02/sc/WS-SecureConversation.pdf> (website checked 2016-04-05)~~

~~SSL/TLS: RFC 2246: The TLS Protocol Version 1.0~~

~~Available from Internet: <http://www.ietf.org/rfc/rfc2246.txt> (website checked 2016-04-05)~~

~~:X509: X.509 Public Key Certificate Infrastructure~~

~~Available from Internet: <https://www.ietf.org/rfc/rfc2459> (website checked 2016-04-05)~~

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

~~Available from Internet: <http://www.ietf.org/rfc/rfc2616.txt> (website checked 2016-04-05)~~

~~HTTPS: RFC 2818: HTTP Over TLS~~

~~Available from Internet: <http://www.ietf.org/rfc/rfc2818.txt> (website checked 2016-04-05)~~

~~IS Glossary: Internet Security Glossary~~

~~Available from Internet: <http://www.ietf.org/rfc/rfc2828.txt> (website checked 2016-04-05)~~

~~NIST 800-57: Part 3: Application-Specific Key Management Guidance~~

~~Available from Internet: http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_PART3_key-management_Dec2009.pdf (website checked 2016-04-05)~~

~~NERC CIP: CIP-002-1 through CIP-009-1, by North American Electric Reliability Council~~

~~Available from Internet: <http://www.nerc.com/files/cip-002-1.pdf> (website checked 2016-04-05)~~

~~SHA-1: Secure Hash Algorithm RFC~~

~~Available from Internet: <http://tools.ietf.org/html/rfc3174> (website checked 2016-04-05)~~

~~PKI: Public Key Infrastructure article in Wikipedia~~

~~Available from Internet: http://en.wikipedia.org/wiki/Public_key_infrastructure (website checked 2016-04-05)~~

~~X509 PKI: Internet X.509 Public Key Infrastructure~~

~~Available from Internet: <http://www.ietf.org/rfc/rfc3280.txt> (website checked 2016-04-05)~~

TECHNICAL REPORT



OPC unified architecture – Part 2: Security Model



CONTENTS

FOREWORD	5
1 Scope	7
2 Normative references	7
3 Terms, definitions, and abbreviated terms	8
3.1 Terms and definitions	8
3.2 Abbreviated terms	13
4 OPC UA security architecture	13
4.1 OPC UA security environment	13
4.2 Security objectives	14
4.2.1 Overview	14
4.2.2 Authentication	15
4.2.3 Authorization	15
4.2.4 Confidentiality	15
4.2.5 Integrity	15
4.2.6 Non-Repudiation	15
4.2.7 Auditability	15
4.2.8 Availability	15
4.3 Security threats to OPC UA systems	15
4.3.1 Overview	15
4.3.2 Denial of Service	16
4.3.3 Eavesdropping	17
4.3.4 Message spoofing	17
4.3.5 Message alteration	17
4.3.6 Message replay	17
4.3.7 Malformed Messages	18
4.3.8 Server profiling	18
4.3.9 Session hijacking	18
4.3.10 Rogue Server	18
4.3.11 Rogue Publisher	18
4.3.12 Compromising user credentials	19
4.3.13 Repudiation	19
4.4 OPC UA relationship to site security	19
4.5 OPC UA security architecture	20
4.5.1 Overview	20
4.5.2 Client / Server	21
4.5.3 Publish-Subscribe	22
4.6 Security Policies	23
4.7 Security Profiles	24
4.8 Security Mode Settings	24
4.9 User Authentication	24
4.10 Application Authentication	24
4.11 User Authorization	25
4.12 Roles	25
4.13 OPC UA security related Services	25
4.14 Auditing	26
4.14.1 General	26

4.14.2	Single Client and Server	27
4.14.3	Aggregating Server	28
4.14.4	Aggregation through a non-auditing Server	28
4.14.5	Aggregating Server with service distribution	29
5	Security reconciliation	30
5.1	Reconciliation of threats with OPC UA security mechanisms	30
5.1.1	Overview	30
5.1.2	Denial of Service	31
5.1.3	Eavesdropping	32
5.1.4	Message spoofing	32
5.1.5	Message alteration	33
5.1.6	Message replay	33
5.1.7	Malformed Messages	33
5.1.8	Server profiling	33
5.1.9	Session hijacking	33
5.1.10	Rogue Server or Publisher	34
5.1.11	Compromising user credentials	34
5.1.12	Repudiation	34
5.2	Reconciliation of objectives with OPC UA security mechanisms	34
5.2.1	Overview	34
5.2.2	Application Authentication	34
5.2.3	User Authentication	35
5.2.4	Authorization	35
5.2.5	Confidentiality	35
5.2.6	Integrity	35
5.2.7	Auditability	35
5.2.8	Availability	36
6	Implementation and deployment considerations	36
6.1	Overview	36
6.2	Appropriate timeouts	36
6.3	Strict Message processing	36
6.4	Random number generation	37
6.5	Special and reserved packets	37
6.6	Rate limiting and flow control	37
6.7	Administrative access	37
6.8	Cryptographic Keys	38
6.9	Alarm related guidance	38
6.10	Program access	38
6.11	Audit event management	39
6.12	OAuth2, JWT and User roles	39
6.13	HTTPs, SSL/TLS & Websockets	39
6.14	Reverse Connect	39
7	Unsecured Services	40
7.1	Overview	40
7.2	Multicast Discovery	40
7.3	Global Discovery Server Security	40
7.3.1	Overview	40
7.3.2	Rogue GDS	40
7.3.3	Threats against a GDS	41

7.3.4	Certificate management threats	41
8	Certificate management.....	42
8.1.1	Overview	42
8.1.2	Self-signed certificate management	42
8.1.3	CA Signed Certificate management	43
8.1.4	GDS Certificate Management	44
	Bibliography.....	47
	Figure 1 – OPC UA network example	14
	Figure 2 – OPC UA security architecture – Client / Server	20
	Figure 3 – OPC UA security architecture – Publisher-Subscriber	21
	Figure 4 – Role overview	25
	Figure 5 – Simple Servers.....	27
	Figure 6 – Aggregating Servers	28
	Figure 7 – Aggregation with a non-auditing Server.....	29
	Figure 8 – Aggregate Server with service distribution.....	30
	Figure 9 – Manual Certificate handling.....	42
	Figure 10 – CA Certificate handling	43
	Figure 11 – Certificate handling	45
	Table 1 – Security Reconciliation Threats Summary	31

INTERNATIONAL ELECTROTECHNICAL COMMISSION

OPC UNIFIED ARCHITECTURE –

Part 2: Security Model

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 TR 62541-2, which is a technical report, has been prepared by subcommittee 65E: Devices and integration in enterprise systems, of IEC technical committee 65: Industrial-process measurement, control and automation.

This third edition cancels and replaces the second edition of IEC TR 62541-2, published in 2016. This edition constitutes a technical revision.

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

- a) protection-targets definition change;
- b) threat type clarifications;
- c) expanded best practices;

- d) added Websockets;
- e) added Pub/Sub.

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

Enquiry draft	Report on voting
65E/679/DTR	65E/703/RVDR

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 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.

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 2: Security Model

1 Scope

This part of IEC 62541 describes the OPC Unified Architecture (OPC UA) security model. It describes the security threats of the physical, hardware, and software environments in which OPC UA is expected to run. It describes how OPC UA relies upon other standards for security. It provides definition of common security terms that are used in this and other parts of the OPC UA specification. It gives an overview of the security features that are specified in other parts of the OPC UA specification. It references services, mappings, and *Profiles* that are specified normatively in other parts of the OPC UA Specification. It provides suggestions or best practice guidelines on implementing security. Any seeming ambiguity between this part and one of the other normative parts does not remove or reduce the requirement specified in the other normative part.

It is important to understand that there are many different aspects of security that have to be addressed when developing applications. However, since OPC UA specifies a communication protocol, the focus is on securing the data exchanged between applications. This does not mean that an application developer can ignore the other aspects of security like protecting persistent data against tampering. It is important that the developers look into all aspects of security and decide how they can be addressed in the application.

This part is directed to readers who will develop OPC UA *Client* or *Server* applications or implement the OPC UA services layer. It is also for end Users that wish to understand the various security features and functionality provided by OPC UA. It also offers some suggestions that can be applied when deploying systems. These suggestions are generic in nature since the details would depend on the actual implementation of the *OPC UA Applications* and the choices made for the site security.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

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

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

IEC 62351 (all parts), *Power systems management and associated information exchange*