®

Edition 1.0 2010-02

TECHNICAL REPORT

OPC Unified Architecture – Part 2: Security Model

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

PRICE CODE V

ICS 25.040.40; 35.100.01

ISBN 978-2-88910-760-5

CONTENTS

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 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.

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

Enquiry draft	Report on voting
65E/93/DTR	65E/155/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, 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.

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

INTRODUCTION

This technical report introduces security concepts for OPC Unified Architecture as specified by IEC 62541. This technical report and specification are a result of an analysis and design process to develop a standard interface to facilitate the development of applications by multiple vendors that inter-operate seamlessly together.

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 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 series of standards.

Note 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 developer look into all aspects of security and decide how they can be addressed in the application.

This part of IEC 62541 is directed to readers who will develop OPC UA client or server applications or implement the OPC UA services layer.

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 referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 62541 (all parts), *OPC Unified Architecture*

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

3 Terms, definitions, abbreviations and conventions

3.1 Terms and definitions

For the purposes of this document the following terms and definitions as well as the terms and definitions given in IEC 62541-1 apply.

3.1.1
Application Instance
individual installation of a program running on one computer

NOTE There can be several *Application Instances* of the same application running at the same time on several computers or possibly the same computer.