IEC PAS 62443-1-6

Edition 1.0 2025-12

PUBLICLY AVAILABLE SPECIFICATION

Security for industrial automation and control systems - Part 1-6: Application of the 62443 series to the Industrial Internet of Things (IIoT)

ICS 25.040.40

ISBN 978-2-8327-0905-4

IEC Secretariat
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

Security for industrial automation and control systems - Part 1-6: Application of the 62443 series to the Industrial Internet of Things (IIoT)

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) IEC draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at https://patents.iec.ch. IEC shall not be held responsible for identifying any or all such patent rights.

IEC PAS 62443-1-6 has been prepared by IEC technical committee 65: Industrial-process measurement, control and automation and the liaison ISA99: ISA committee on Security for industrial automation and control systems. It is a Publicly Available Specification.

The text of this Publicly Available Specification is based on the following documents:

Draft	Report on voting
65/1155/DPAS	65/1176/RVDPAS

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

The language used for the development of this Publicly Available Specification is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, [and the ISO/IEC Directives, JTC 1 Supplement] available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications.

A list of all parts in the IEC 62443 series, published under the general title *Security for industrial automation and control systems*, can be found on the IEC website.

Text in **bold**: Lead recommendations (in Clause 6 to Clause 9).

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

– reconfirmed,

– withdrawn, or

– revised.

NOTE In accordance with ISO/IEC Directives, Part 1, IEC PASs are automatically withdrawn after 4 years.

INTRODUCTION

Today the growing availability of Industrial Internet of Things (IIoT) has widened the array of technologies and methodologies available for use in industrial automation environments. Much of the IEC 62443 series was written before IIoT was common but provides a strong basis for securing these environments. The series can provide a risk-based, defense-in-depth focus that will assist asset owners and their service providers in navigating the use of IIoT in their own systems.

This document focuses on the use of IIoT in industrial automation infrastructure, components, systems, and solutions to identify aspects of the IEC 62443 series that affect IIoT implementations.

The use of IIoT introduces new communication paths and new ways to allocate functionality in the automation context. By their nature, IIoT devices introduce functionality into parts of the automation and control system that have not previously had external communications. For example, multiple functions can be integrated into a single physical device, and these functions can represent functions traditionally allocated to different security zones. Also, IIoT can allow functions traditionally allocated to a single device to be distributed among a wider network of components, including the use of cloud services. The introduction of IIoT emphasizes the need to consider the requirements of functions, their allocation to zones, and the interconnection of these zones with conduits in a virtual sense, as well as in the traditional physical sense. These changes then permeate through the cybersecurity decisions made.

This document identifies parts of the IEC 62443 series that might be relevant to asset owners and service providers as they consider the implementation and operation of IIoT in their IACS. Product suppliers can find assistance in this document in determining asset owner concerns and requirements.

In addition, this document will provide input to future revisions of the series by identifying changes or gaps that are needed with the introduction of IIoT, both with and without cloud-based functionality.

1 Scope

Industrial Internet of Things (IIoT) technology introduces new communication channels, a new organization of functions, and new cybersecurity concerns. Asset owners are looking for more guidance in how to deal with all these changes. The IEC 62443 series, *Security for industrial automation and control systems*, can be applied to this new technology, but many asset owners look at the scope of the series and wonder where to start.

This part of IEC 62443 seeks to give guidance to asset owners and their service providers on how the IEC 62443 series can be used to address IIoT. The document points to requirements in the different parts of the IEC 62443 series that might be helpful to the asset owner as they both consider implementing IIoT in their automation solutions as well as dealing with existing IIoT. Product suppliers and service providers can find this document useful as well.

NOTE The drafting committee for IEC 62443 is currently engaged in revision of parts of the standard to recognize emerging technologies, such as IIoT, and this document is part of that on-going effort.

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 TS 62443-1-1, *Security for industrial automation and control systems - Part 1-1: Terminology, concepts, and models*

Bibliography

NOTE This Bibliography includes references to sources used in the creation of this document as well as references to sources that can aid the reader in developing a greater understanding of cybersecurity as a whole and developing a management system. Not all references in this Bibliography are referred to throughout the text of this document. The references have been broken down into different categories depending on the type of source they are.

[1] IEC 62264 (ISA-95 Series) (all parts), *Enterprise-control system integration*

[2] IEC TR 62443-2-3:2015, *Security for industrial automation and control systems - Part 2-3: Patch management in the IACS environment*

[3] ISO/IEC 17025:2017, *General requirements for the competence of testing and calibration laboratories*

[4] ISO/IEC 17788:2014, *Information technology - Cloud computing - Overview and vocabulary*

[5] ISO/IEC 17963:2013, *Web services for management (WS-Management) specification*

[6] ISO/IEC 19086 Series, *Information technology - Cloud computing - Service level agreement (SLA) framework*

[7] ISO/IEC 19896 Series, *IT security techniques - Competence requirements for information security testers and evaluators*

[8] ISO/IEC 20000-1, *Information technology - Service management - Part 1: Service management system requirements*

[9] ISO/IEC 21823 Series, *Internet of Things (IoT) - Interoperability for IoT systems*

[10] ISO/IEC TR 22678:2019, *Information technology - Cloud computing - Guidance for policy development*

[11] ISO/IEC TR 23186:2018, *Information technology - Cloud computing - Framework of trust for processing of multi-sourced data*

[12] ISO/IEC TR 23188:2020, *Information technology - Cloud computing - Edge computing landscape*

[13] ISO/IEC WD (Working Draft) TS 24462.2, *Ontology for ICT trustworthiness assessment*

[14] ISO/IEC TR 26927:2011, *Information technology - Telecommunications and information exchange between systems - Corporate telecommunication networks - Mobility for enterprise communications*

[15] ISO/IEC 27001, *Information technology - Security techniques - Information security management systems - Requirements*

[16] ISO/IEC 27002, *Information security, cybersecurity and privacy protection - Information security controls*

[17] ISO/IEC 27070, *Information technology - Security techniques - Requirements for establishing virtualized roots of trust*

[18] ISO/IEC 27400, *Cybersecurity - IOT security and privacy - Guidelines*

[19] ISO/IEC 30141, *Internet of things (IOT) - Reference architecture*

[20] ISO/IEC 30145-2:2020, *Information technology - Smart city ICT reference framework - Part 2: Smart city knowledge management framework*

[21] ISO/IEC TR 30166:2020, *Internet of things (IoT) - Industrial IoT*

[22] ISO/IEC CD (Committee Draft) TS 30168, *Internet of things (IoT) - Generic trust anchor application programming interface for industrial IoT devices*

[23] ISO/IEC 38505-1:2017, *Information technology - Governance of IT - Governance of data - Part 1: Application of ISO/IEC 38500 to the governance of data*

[24] ISO/IEC/IEEE 42010, *Systems and software engineering - Architecture description*

[25] ISO 20294:2018, *Graphic technology - Quantification and communication for calculating the carbon footprint of e-media*

[26] ISA-TR84.00.09, *Cybersecurity related to the functional safety lifecycle*

[27] NIST SP 800-145:2011, *The NIST Definition of Cloud Computing*

[28] NIST SP 800-207:2020, *Zero Trust Architecture*

[29] PERA Enterprise Integration, *http://pera.net/ [Viewed 2025-04-26]*

[30] ISO/IEC 20924:2024, *Internet of Things (IoT) and digital twin - Vocabulary*

[31] IEC 62443-2-1:2024, *Security for industrial automation and control systems - Part 2-1: Security program requirements for IACS asset owners*

[32] IEC 62443-2-4, *Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers*

[33] IEC 62443-3-2, *Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design*

[34] IEC 62443-3-3:2013, *Security for industrial automation and control systems - Part 3-3: System security requirements and security levels*

[35] IEC 62443-4-1, *Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements*

[36] IEC 62443-4-2, *Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components*