INTERNATIONAL STANDARD

ISO/IEC 24392

First edition
2023-07

Cybersecurity — Security reference model for industrial internet platform (SRM- IIP)

Cybersécurité — Modèle de référence de sécurité pour plateforme internet industrielle (SRM- IIP)



Reference number
ISO/IEC 24392:2023(E)

© ISO/IEC 2023



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2023

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

© ISO/IEC 2023 – All rights reserved

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Abbreviated terms ... **3**
5 Overview ... **4**
6 IIP-specific security threats to industrial internet platforms ... **6**
6.1 Characteristics of IIPs ... 6
6.2 Security threats to IIPs ... 8
7 Security reference model of industrial internet platform ... **12**
7.1 General ... 12
7.2 Security domains of IIPs ... 12
7.2.1 General ... 12
7.2.2 Edge security domain ... 13
7.2.3 Cloud infrastructure security domain ... 13
7.2.4 Platform security domain ... 14
7.2.5 Application security domain ... 14
7.3 System life cycle ... 14
7.3.1 General ... 14
7.3.2 Development and production stage ... 15
7.3.3 Utilization and support stage ... 16
7.3.4 Retirement stage ... 17
7.4 Business scenarios and roles ... 19
7.4.1 General ... 19
7.4.2 Production optimization ... 19
7.4.3 Product customization ... 20
7.4.4 Multilevel security production ... 20
7.4.5 Transnational cooperation ... 21
8 Security objectives and controls for IIPs ... **23**
8.1 Security objectives ... 23
8.2 Security controls ... 24
8.2.1 General ... 24
8.2.2 Physical security ... 24
8.2.3 Network security ... 25
8.2.4 Access security ... 25
8.2.5 Communication security ... 26
8.2.6 System security ... 26
8.2.7 Application security ... 27
8.2.8 Operation and maintenance security ... 27
8.2.9 Security management ... 28
Annex A (informative) **Typical IIP use cases** ... **29**
Bibliography ... **32**

© ISO/IEC 2023 – All rights reserved

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take 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, ISO and 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 www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

© ISO/IEC 2023 – All rights reserved

Introduction

An industrial internet platform (IIP) is an industry-specific, or multi-industry, technology platform. IIPs enable users to process data such as sensor data from a wide range of manufacturing processes, to provide information for decision-making or to facilitate visualization for business decisions. IIPs also provide the capability for control systems to interact with manufacturing systems, helping to direct their activities. An IIP can bring together components that collectively meet the demands of digitalization, networking and interconnection of industrial machinery. An IIP can serve as a hub for a multi-stakeholder private industrial complex, or as part of an open system connected to the wider internet. It can also provide the underpinnings for a system using big data, and commonly serve as the basis for large-scale production of manufactured goods.

This document presents a security reference model for IIP, which characterizes the security concerns of IIP arising from the particularities of industrial settings and provides corresponding security requirements. In particular, the reference model identifies the specific characteristics of IIP from three perspectives: an industrial business view, a platform architecture view, and a system life cycle view. Based on such characteristics, their corresponding IIP-specific threats can be identified. Finally, this document provides guidance on appropriate security controls based on existing international standards. Figure 1 presents the relationship between this document and other relevant standards.

The purpose of this document is to facilitate the security design, implementation, and management of IIP, complementing the security requirements that are dealt with in generic information systems. The guidance on security controls support the commercial users of the IIP, as well as their partners along the supply chain.

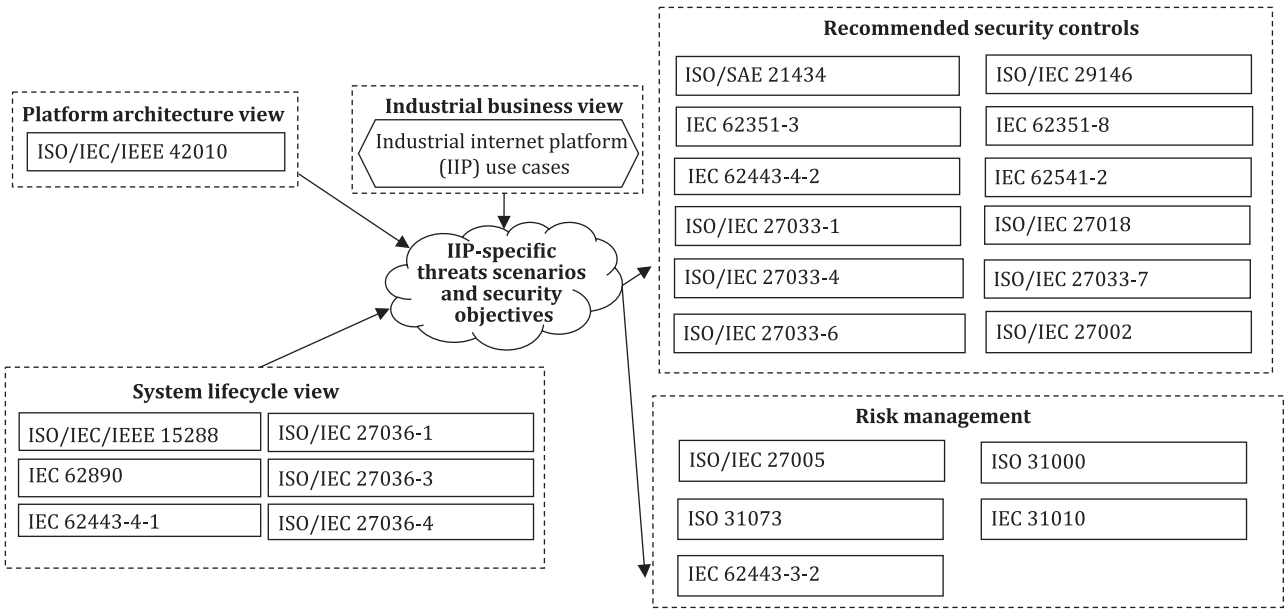


Figure 1 — The relationship between this document and other relevant standards

NOTE The IIP can include cyber-physical systems (CPS). Such CPS potentially provide elementary or assembled components to other parts of the IIP.

Like CPS, Internet of things (IoT) devices can be connected to the IIP either directly or via IIP intermediaries. Accordingly, it is important to consider IoT terminology (see ISO/IEC 20924), IoT architecture (see ISO/IEC 30141), and IIoT security issues.

Beyond CPS, IoT devices, and communication networks, IIPs commonly include cloud technology, which is covered in ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 22123-1, ISO/IEC 22123-2, ISO/IEC TR 23188, and ISO/IEC TR 23186.

© ISO/IEC 2023 – All rights reserved

Cybersecurity — Security reference model for industrial internet platform (SRM- IIP)

1 Scope

This document presents specific characteristics of industrial internet platforms (IIPs), including related security threats, context-specific security control objectives and security controls.

This document covers specific security concerns in the industrial context and thus complements generic security standards and reference models. In particular, this document includes secure data collection and transmission among industrial devices, data security of industrial cloud platforms, and secure collaborations with various industry stakeholders.

The users of this document are organizations who develop, operate, or use any components of IIPs, including third parties who provide services to the abovementioned stakeholders.

This document provides recommendations for users on how to protect IIPs against IIP-specific threats.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
trust
degree to which a user or other stakeholder has confidence that a product or system will behave as intended

[SOURCE: ISO/IEC 25010:2011, 4.1.3.2]

3.2
trustworthiness
ability to meet stakeholders expectations in a verifiable way

[SOURCE: ISO/IEC TR 24028:2020, 3.42, modified — Notes 1 to 3 to entry have been deleted.]

3.3
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[SOURCE: ISO/IEC 27000:2018, 3.10]

© ISO/IEC 2023 – All rights reserved