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 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

Contents

Page

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.

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.

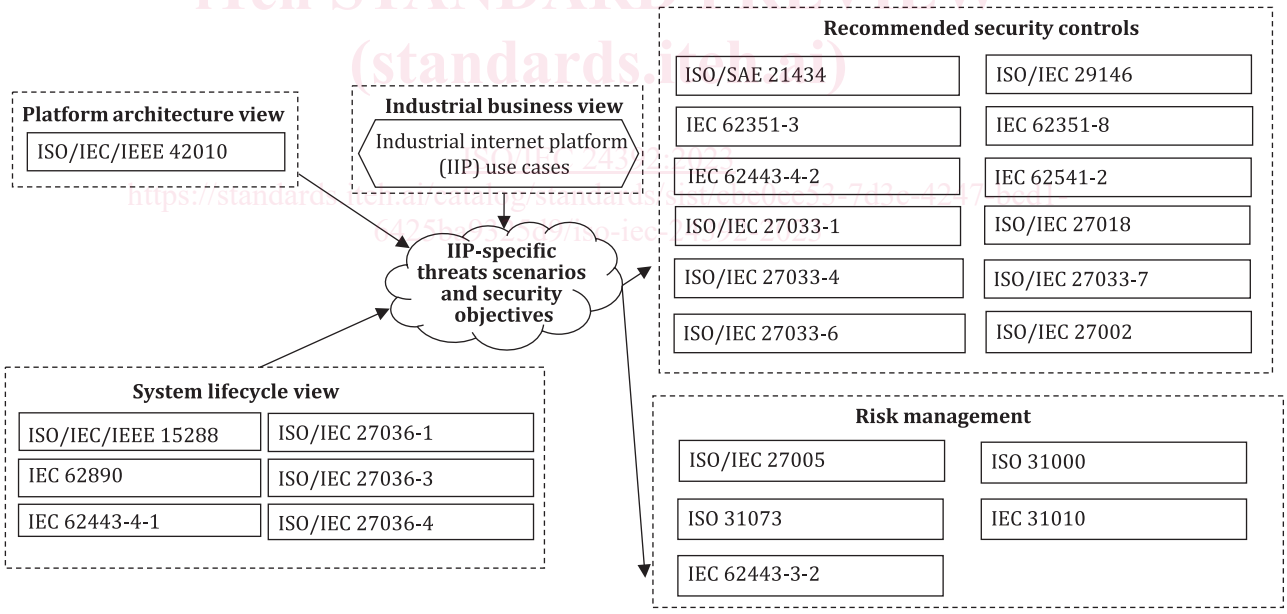

Figure 1 — The relationship between this document and other relevant standards

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.

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]

3.4
integrity
property of protecting the accuracy and completeness of assets

Note 1 to entry: Refer to information assets in most cases.

[SOURCE: ISO/IEC 27000:2018, 3.36, modified — "protecting" and "of assets" have been added to the definition; Note 1 to entry has been added.]

3.5
availability
property of being accessible and usable on demand by an authorized entity

[SOURCE: ISO/IEC 27000:2018, 3.7]

3.6
authentication
provision of assurance that a claimed characteristic of an entity is correct

[SOURCE: ISO/IEC 27000:2018, 3.5]

3.7
industrial internet platform
IIP
platform integrating information and communication technology to facilitate industrial efficiency and transform industrial operations at the scale of multiple digitally-enabled factory complexes usually across diverse locations

3.8
reference architecture
architecture description that provides a proven template solution when developing or validating an architecture for a particular solution

[SOURCE: ISO/IEC 20924:2021, 3.1.28, modified — definition has been revised.]

3.9
edge
boundary between pertinent digital and physical entities, delineated by networked sensors and actuators

[SOURCE: ISO/IEC TR 23188:2020, 3.1.2, modified — Note 1 to entry has been deleted.]

3.10
edge computing
distributed computing in which processing and storage takes place at or near the *edge* (3.9), where the nearness is defined by the system's requirements

Note 1 to entry: The functions of the platform include resource collection, data aggregation, intelligent analysis, open sharing (e.g. of manuals, flyers), standards testing, technology verification, industrial data transfer, business resource management and industry monitoring.

Note 2 to entry: A platform can be connected to a large number of heterogeneous industrial devices, including industrial internet of things, edge devices, and cyber-physical systems, some of which are not secure-by-design.

[SOURCE: ISO/IEC TR 23188:2020, 3.1.3, modified — notes 1 and 2 to entry have been added.]

3.11
security domain
domain in which the stakeholders are obliged to follow specific security requirements to ensure the corresponding functional domain is secure

Note 1 to entry: A security domain can include, a network, a part of an IoT devices development organization providing products via the IIP, a part of an integrator organization (factory or plant building project) that uses products or services via the IIP.

3.12
control objective
statement describing what is to be achieved as a result of implementing controls

Note 1 to entry: "Security objective" is used as an abbreviation for "security control objective" in cases where any ambiguity can be excluded.

[SOURCE: ISO/IEC 27000:2018, 3.15]

3.13
process measurement integrity
sensor which has been authenticated and measurement validated as correct

3.14
IIP participant
person or organization that participates in the development or use of industrial internet platforms (IIPs)

4 Abbreviated terms

ABAC	attribute-based access control
API	application programming interface
ASC	application security control
CAL	cybersecurity assurance level
CVE	common vulnerabilities and exposures
DCS	distributed control system
DDoS	distributed DoS
DoS	denial of service
DPI	deep packet inspection
EMC	electromagnetic compatibility
EMI	electromagnetic interference
IACS	industrial automation and control system
ICS	industrial control system
IED	intelligent electronic device
IIoT	industrial Internet of things
IIP	industrial internet platform

IPS	intrusion protection system
LAN	local area network
M2M	machine to machine
NGFW	next-generation firewall
OEM	original equipment manufacturer
OSI	open systems interconnection
OT	operational technology (controlling physical processes)
PaaS	platform as a service
PII	personally identifiable information
PCB	printed circuit board
PLC	programmable logic controller
QoS	quality of service
RBAC	role-based access control
RTU	remote terminal unit
SCADA	supervisory control and data acquisition
SIEM	security information and event management
SRM	security reference model
TCP/IP	transmission control protocol/Internet protocol
UDP	user datagram protocol
VLAN	virtual LAN
VPN	virtual private network

5 Overview

An IIP is understood as a responsive industrial infrastructure. An IIP is accessible at any time according to business needs, from anywhere (e.g. pervasive internet) or from agreed business locations. It is accessible to all stakeholders and users assembled around the life cycle of business execution, monitoring and production of things (i.e. industrial production). Annex A provides information on typical use cases of IIPs.

NOTE 1 Some IIP can be part of critical infrastructure, according to the critical infrastructure definition [typically defined with regard to its direct impact on a considerably large number of people, e.g. with regard to the electrical energy need in megawatts (MW), impact on health or food shortage].

An IIP provides semantic interoperability capabilities, including for stakeholders who are representatives from inhomogeneous domains.

Stakeholders can use common communication methods and syntax that hide any non-homogeneous structures of IIP participants, including:

a) to generate, subscribe, deliver any kind of data;

b) to acquire information about things, industrial production processes or any other industrial business concerns;

c) to apply assembled knowledge for decision-making that IT processes have "learned" from observations of OT production processes;

d) to generate from IIP behaviour observations suggestions on security controls for the purpose of stabilization, harmonization of the IIP, prevention of misuse, avoidance of failure propagation.

In order to analyse the security needs of IIPs, an IIP security reference model is elaborated, as shown in Figure 2.

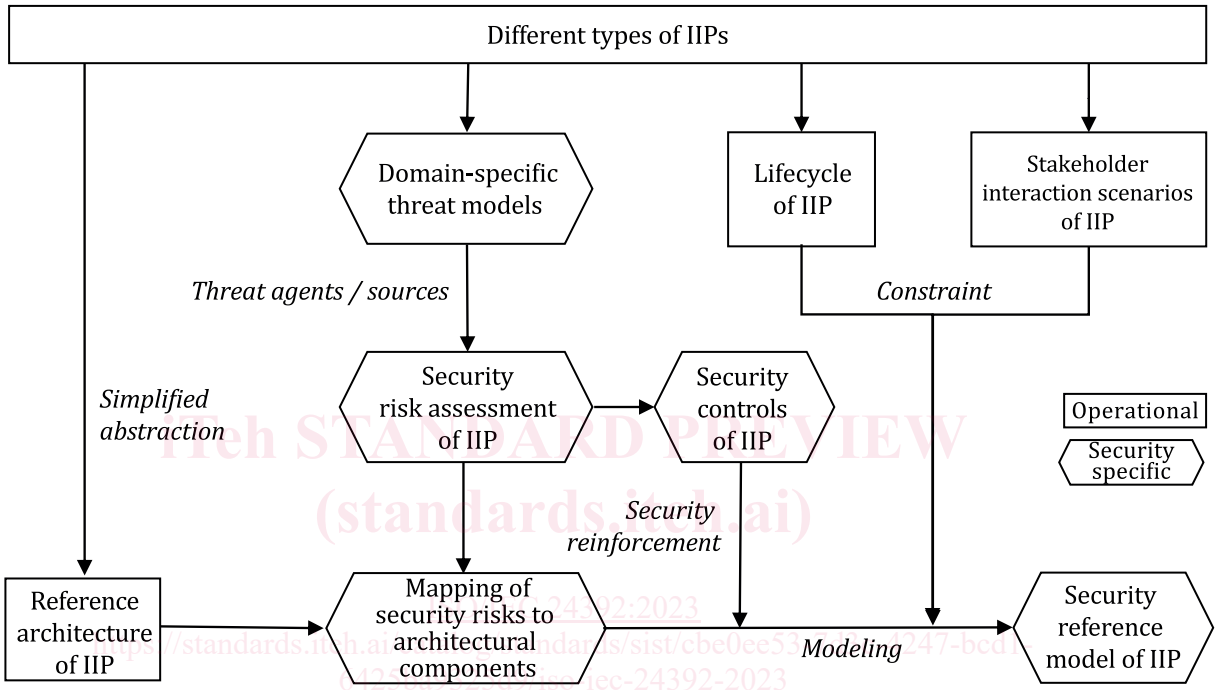

Figure 2 — Establishment of a security reference model of an IIP

As illustrated in Figure 2, the security reference model of the IIP is derived from the IIP reference architecture combined with the system life cycle.

The reference architecture provides a structured and proven partition of system functional domains, to which specific security threats of IIPs can be mapped. Within each of these functional domains, particular security requirements should be satisfied according to the threats.

The life cycle of the IIP is the time dimension, introducing additional constraints in different stages. The stakeholder interaction scenario of the IIP is the role dimension, introducing the constraints during interactions among different IIP stakeholders. These two views assist in guiding the design of the IIP security reference model.

NOTE 2 IIPs are typically cloud-based and offer a widely interconnected industrial environment for platform participants that provide or acquire complex products and services to other trustworthy participants. These participants can involve CPS and IoT devices. There is no intention to replace horizontal or specialized and dedicated domain-specific industry solutions, e.g. IACS, ICS, DCS or SCADA systems. These IACS/ICS/DCS/SCADA systems typically address a very specific CPS (e.g. a power plant, a part of a factory, a vehicle or an aircraft) or geographically distributed substations (e.g. from the grid or smart grid).

NOTE 3 As opposed to an IIP, the design, integration and manufacturing of these OT and functional safety related industry systems, that typically operate for many years with recurrent operation and maintenance cycles, do not require the flexibility of an IIP. However, it is expected that they meet other very challenging industry domain-specific graded requirements on functional safety and security. Some of the security controls such as the deployment of autarkic networks and physical protection used by OT cannot be deployed directly for IIPs, in case they are connected via the internet. Additionally, the benefit of IIPs can increase together with the increased use of IIoT and edge computing by traditional IACS, ICS, DCS and SCADA systems.

6 IIP-specific security threats to industrial internet platforms

6.1 Characteristics of IIPs

IIPs typically involve massive, heterogeneous industrial devices and data, which are used by various stakeholders for specific purposes. Here are the detailed IIP-specific characteristic challenges.

a) Various data sources can exist in a factory or industrial facility. Traditional field wiring may not always be suitable for complex factory environments. Smart manufacturing and digital plants can use effective reconfigurations, including rewiring. Such approaches are not effective for IIP customers. Alternative technologies may be used when connecting the industrial environment via an IIP with further stakeholders. This can include software defined networking or the use of wireless networks and 5G in cases where EMI is not an issue.

b) Edge computing platforms can be deployed at a factory, smart plant or industrial facility site. It can be difficult for an edge computing platform provider to maintain the platform centrally or remotely and thus difficult to quickly address issues of the edge computing platform or of edge devices. The PaaS provider or the OEM of the platform can use edge computing platforms and edge devices that are designed for effective maintenance via an IIP. In case of centralized or remote configuration, preventive maintenance and recurrent maintenance are intended.

c) A yearly increasing amount of industrial equipment is discarded from its initial deployment environment. Reusing such equipment in a different environment can pose security risks, e.g. if the equipment was initially intended only for use in an isolated network environment or as part of an autarkic automation or IT system.

d) Local security settings of small-scale and medium-scale IIoT and IoT devices are usually not properly set during their installation. While an omission of some secure configuration steps can be acceptable in an isolated environment due to locally effective compensating security controls, a secure configuration, e.g. avoiding default device passwords, is mandatory before connecting to an IIP.

e) Each IIoT or IoT device has a certain amount of computing and processing capabilities. This limitation of capabilities can be exploited by different attacks, like DoS, DDoS or replay attacks if directly connected to an IIP.

f) There is insufficient electromagnetic shielding protection for IIoT or IoT devices. EMC of embedded devices in an isolated environment can be without any concern on account of additional locally effective shielding measures. Connecting to an IIP however, can use additional isolation or decoupling measures. See IEC 61000-1-2.

g) IIoT and IoT devices usually have limited computing and networking resources. Encryption algorithms with high resource requirements are not suitable for direct use by these devices. If data can only be transmitted in plaintext or with simple encryption, secure gateways can be deployed as interfaces towards the IIP. For an example, see ISO/IEC 27033-4.

h) The data exchange between production factories and cloud platforms can involve sensitive data.

i) Traditional (Industry 3.0) and legacy factory equipment does not use encryption by default, nor does it prohibit the use of encryption. At the same time, embedded devices can lack (and not require) a user roles concept and/or device authentication. Initially, there is no need for encryption of cyclically exchanged short-lived data (as encryption can even be detrimental for responsive

dependable facilities). Similarly, initially strong alternative security controls can be in place (e.g. administrative access to a cabinet instead of role-based user access). However, these security controls are no longer sufficient when directly connecting the legacy equipment to an IIP.

j) The version of a host OS in an industrial environment can be outdated. If the OS vendor no longer provides functional and security updates, or the OEM of the application software does not provide upgrades for a new host OS (e.g. as specified in IEC/TR 62443-2-3) an alternative secure solution should be found instead of connecting the outdated combination of system software and application software to an IIP.

k) Typically, there are many types of equipment in a factory, and the communication protocols are not uniform. In the past, some vulnerabilities have been disclosed without patches. When connecting such equipment directly or indirectly to an IIP, the corresponding standards ISO/IEC 30111 and ISO/IEC 29147 should be considered.

l) Different devices can be set up with different security levels and zone protection. Device relocation failure during the transition of device movement leads to zone protection failure.

m) The initial network boundaries between areas in a factory can be unclear and interconnected. For example, the boundaries between an initially isolated production network and an isolated local office network can be blurred. While initially this is less of a concern, it can become an issue if the previously isolated local office is connected to the IIP without appropriate enforcement of network security controls.

n) Initially unprotected digital information exchanged in a production system can be easily copied. This can for example result in a breach of intellectual property handling or the disclosure of production data of involved stakeholders located in different companies and countries. This can happen when an (initially isolated) production facility connects via an IIP to a preventive maintenance service provider. As part of recurrent remote preventive maintenance activities via the IIP, the maintenance service provider may access receipts (usually protected as intellectual property) processed on the maintained machines or may evaluate the average utilization of the machines (orders situation) and thus gain information that can be misused by competitors.

o) The soft or hard real-time control flow and the non-control flow requirements are different. Both real-time datagrams (control instructions) and non-control flow datagrams (general production data) can be transmitted in a common network. If no time sensitive networking (TSN)[45] or similar approach is considered during the architecture and design phase of an IIP, or for a system connected to an IIP, the intended QoS[46] can fail. Similarly, if the TSN design erroneously does not consider the peak or combined maximum real-time communication requirements (or if these requirements change), the non-control flow communication datagrams can consume an excessive bandwidth, thus potentially leading to interruption of industrial control system functions.

p) Industrial environments can generate large amounts of data (e.g. raw data from sensors) in real-time, which can lead to excessive traffic if multiple IIP customers with similar data sources are connected to the IIP or if the characteristics of the initial IIP customers change. Overall, this can lead to inappropriate responsiveness and potentially unintended denial of service conditions if the IIP is not sufficiently scalable for the processing of large amounts of data.

q) The computing resources of IoT devices are small, and it is difficult to support device identifiers such as digital certificates.

r) A large amount of industrial equipment and a large number of equipment components can be scrapped or repurposed every year. Non-proper reuse of such devices can incur risks.

s) When users migrate or leave the cloud platform, the platform provider reallocates resources to new users.

t) Using the cloud platform to control and optimize production is the advantage of the industrial internet, but the wrong decision of the platform can also pose a considerable threat.