DRAFT INTERNATIONAL STANDARD
ISO/IEC DIS 24392

ISO/IEC JTC **1**/SC **27** Secretariat: **DIN**

Voting begins on: **2022-07-01** Voting terminates on: **2022-09-23**

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

ICS: 35.030

Reference number
ISO/IEC DIS 24392:2022(E)

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Abbreviated terms and acronyms ... **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 Security domains of IIPs ... 13
7.1.1 General ... 13
7.1.2 Edge security domain ... 14
7.1.3 Cloud infrastructure security domain ... 14
7.1.4 Platform security domain ... 14
7.1.5 Application security domain ... 15
7.2 System life cycle ... 15
7.2.1 Development and production stage ... 16
7.2.2 Utilization and support stage ... 17
7.2.3 Retirement stage ... 18
7.3 Business scenarios and roles ... 19
7.3.1 Production optimization ... 19
7.3.2 Product customization ... 19
7.3.3 Multilevel security production ... 20
7.3.4 Transnational cooperation ... 21
8 Security objectives and controls for IIPs ... **22**
8.1 Security objectives ... 22
8.2 Security controls ... 24
8.2.1 Physical security ... 24
8.2.2 Network security ... 25
8.2.3 Access security ... 25
8.2.4 Communication security ... 26
8.2.5 System security ... 26
8.2.6 Application security ... 27
8.2.7 Operation and maintenance security ... 27
8.2.8 Security management ... 27
Annex A (Informative) ... **28**
Bibliography ... **31**

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2. www.iso.org/directives

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received. www.iso.org/patents

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

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/TC JTC 1/SC 27.

Introduction

[Background] An Industrial Internet Platform (IIP) is an industry-specific, or multi-industry, technology platform. IIPs provide the capability to process data such as sensor data from a wide range of manufacturing process to provide information for decision-making or to allow for visualization for business decisions. IIPs can also interact with manufacturing systems to direct activities. An IIP may bring together components that together meet the demands of digitalization, networking and interconnection of industrial machinery. An IIP may serve as a hub for a multi-stakeholder private industrial complex, or be one part of an open system connected to the wider Internet. An IIP may provide the underpinnings for a system using big data, would commonly be the basis for large-scale production of manufactured goods, and may contain and/or support elements using ML (machine learning) or AI (artificial intelligence).

[Objective] This document presents a security reference model for IIP, which characterizes the security concerns of IIP that are raised by the specialty of industrial settings and provides corresponding security requirements. In particular, the reference model identifies the specific characteristics of IIP from three perspectives: industrial business view, platform architecture view, and system lifecycle view. Based on such characteristics, their corresponding IIP-specific threats will be identified. Finally, the reference model will recommend appropriate security controls based on existing international 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 should also support the commercial users of the IIP as well as their partners along the supply chain.

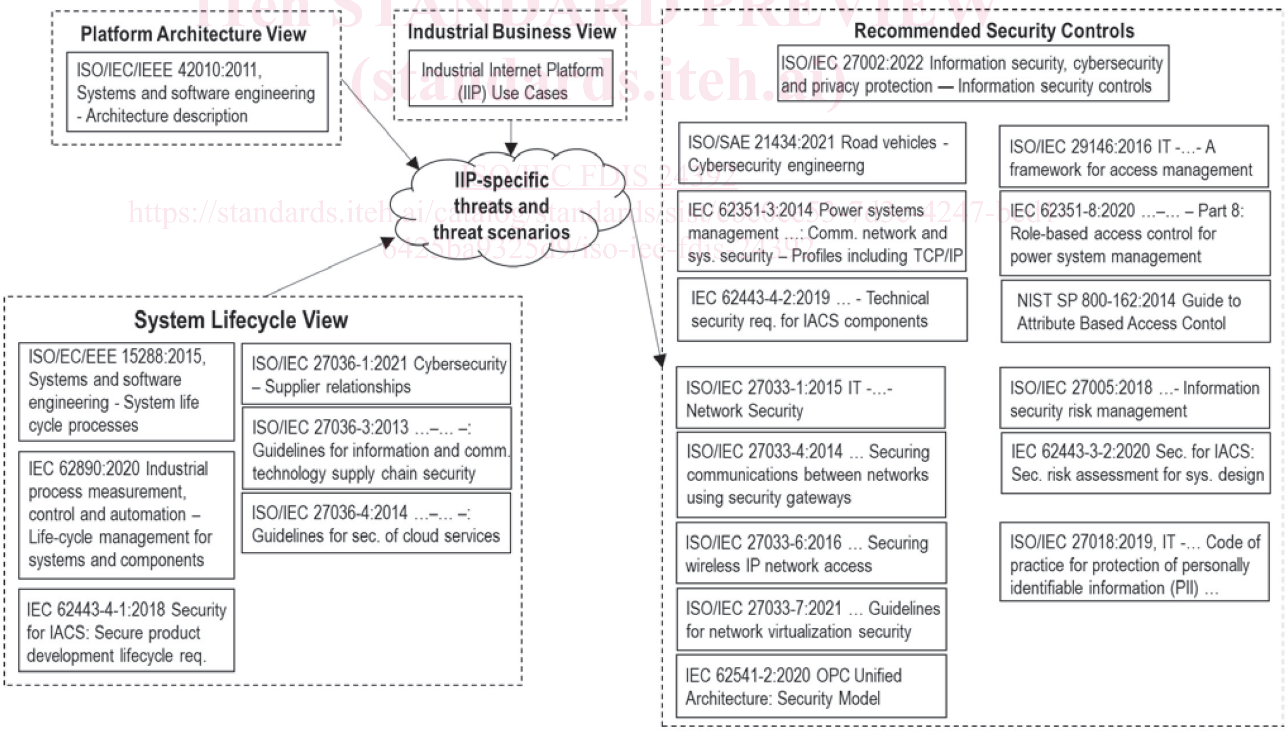

Figure 1 — The relationships between this document and some relevant standards

Note Some of the participants of the IIP may contain Cyber-physical Systems (CPS). Such CPS could e.g., produce or integrate elementary or assembled components on behalf of other IIP participants.

Like CPS, IoT devices can be connected to the IIP either directly or via IIP participants. Accordingly, the IoT vocabulary (ISO/IEC 20924:2018 [5]) and IoT reference architecture (ISO/IEC 20924:2018 [5][6]) are considered.

Beyond CPS, IoT devices and communication networks, the IIPs involve cloud technology, as introduced by ISO/IEC 27017:2015,[21] ISO/IEC 27018:2019,[20] ISO/IEC 17788:2014 [18] and ISO/IEC TR 23188:2020 [8] (Cloud computing — Edge computing landscape) and ISO/IEC TR 23186:2018 [19] (Cloud computing - Framework of trust for processing of multi-sourced data).

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

1 Scope

This document presents specific characteristics of 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, it includes secure data collection and transmission among industrial devices, data security of industrial cloud platforms, and secure collaborations with various industry stakeholders.

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

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC/IEEE 42010:2011, *Systems and software engineering — Architecture description*

ISO/IEC/IEEE 15288:2015, *Systems and software engineering — System life cycle processes*

ISO/IEC 27002:2022, *Information security, cybersecurity and privacy protection — Information security controls*

3 Terms and definitions

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

ISO and IEC maintain terminological 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
artificial intelligence
capability of an engineered system to acquire, process and apply knowledge and skills

[SOURCE: ISO/IEC TR 24028:2020, 3.4]

Note 1 to entry: Knowledge are facts, information and skills acquired through experience or education

3.2
authentication
provision of assurance that a claimed characteristic of an entity is correct

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

3.2.1
availability
property of being accessible and usable upon demand by an authorized entity

[SOURCE: ISO/IEC 27000:2018]

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

[SOURCE: ISO/IEC 27000:2018]

3.4
control objective
statement describing what is to be achieved as a result of implementing controls

[SOURCE: ISO/IEC 27000:2018]

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

3.5
edge
boundary between pertinent digital and physical entities, delineated by networked sensors and actuators

[SOURCE: ISO/IEC TR 23188:2020, 3.1.2]

3.6
edge computing
distributed computing in which processing and storage takes place at or near the edge, where the nearness is defined by the system's requirements

[SOURCE: ISO/IEC TR 23188:2020, 3.1.3]

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

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 may be connected to a large number of heterogeneous industrial devices, including IIoT, edge devices and CPS, some of which may not be secure-by-design.

3.8
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]

3.9
last-time buy
life-cycle-management strategy in which instances of an abandoned product type are purchased before end of sales

[SOURCE: IEC 62890:2020, 3.1.19]

3.10
process measurement integrity
Sensor has been authenticated and measurement is validated as being correct

[SOURCE: ISO/DIS 22387:2022]

3.11
reference architecture
architecture description that provides a proven template solution when developing or validating an architecture for a particular solution

[SOURCE: ISO/IEC 20924:2018, 3.1.27]

3.12
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 could be e.g., 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.

3.13
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]

3.14
trustworthiness
ability to meet stakeholder expectations in a verifiable way

[SOURCE: ISO/IEC TR 24028:2020, 3.42]

4 Abbreviated terms and acronyms

ABAC	attribute-based access control
AI	artificial intelligence
APT	advanced persistent threat
ASC	application security control
CAL	cybersecurity assurance level
CVE	common vulnerabilities and exposures
DCS	distributed control system
DDoS	distributed DoS
DMZ	demilitarized zone
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
ML	machine learning
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
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 should be understood as a responsive industrial infrastructure. An IIP should be accessible at any time according to business needs, from anywhere (pervasive internet) or from agreed business locations and to all stakeholders and users assembled around the life cycle of business execution, monitoring and production of things (industrial production).

Note Some IIP may be part of critical infrastructure, according to the critical infrastructure definition by national law (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 should provide semantic interoperability capabilities, including for stakeholders that are representants from inhomogeneous domains.

Stakeholders should be able to use common communication methods and syntax which hide any non-homogeneous structures of IIP participants, i.e.:

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

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

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

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

In order to analyze the security needs of IIPs, an IIP Security Reference Model is elaborated, as shown in Figure 2.

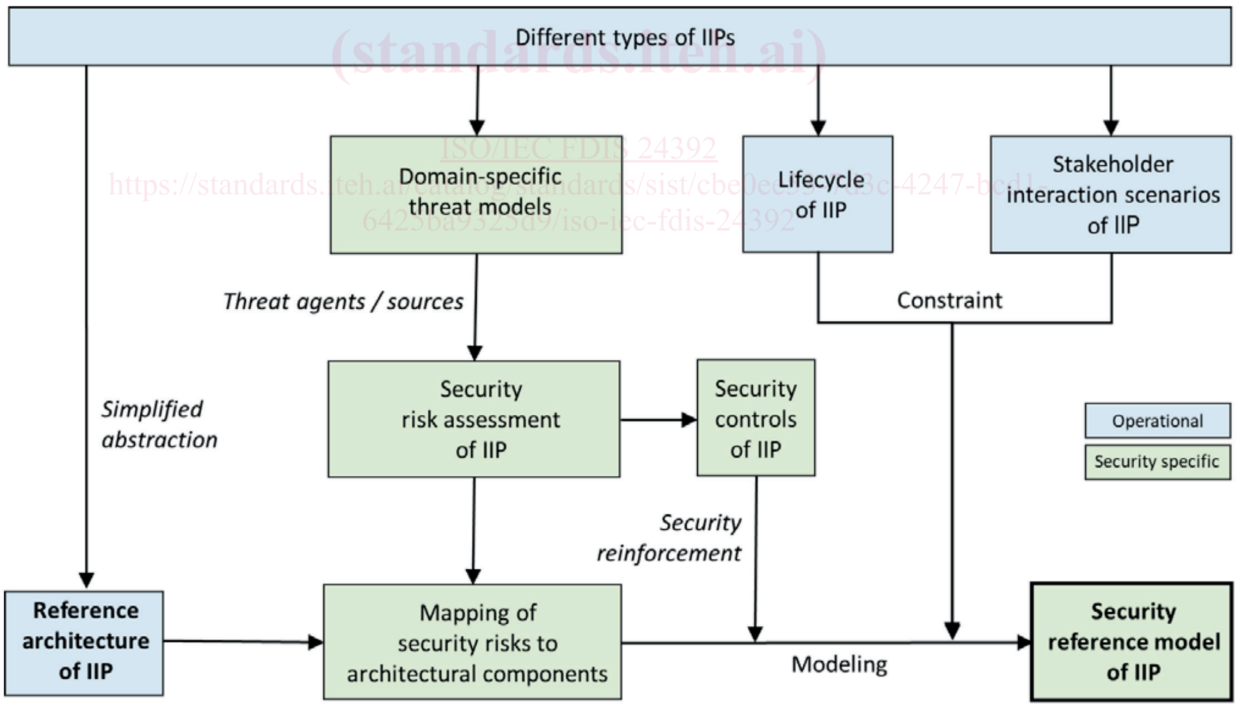

Figure 2 — Establishment of a security reference model of an industrial Internet platform (IIP)

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 will be mapped. Within each of these functional domains, particular security requirements need to 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 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, each of whom may involve CPS and IoT devices. There is no intention to replace horizontal or specialized and dedicated domain-specific industry solutions, e.g., of IACS (industrial automation and control systems), ICS (industrial control systems), DCS (distributed control systems) or SCADA (supervisory control and data acquisition) systems. Theses IACS/ICS/DCS/SCADA systems are typically addressing 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., of the grid or smart grid). As opposed to an IIP, the design, integration and manufacturing of these OT (operational technology) and functional safety related industry systems, that typically operate for many years with recurrent operation and maintenance cycles, do not need the flexibility of an IIP. However, they have to meet other very challenging industry domain-specific graded requirements on functional safety and security. Some of the security controls like 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 may 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 detailed IIP-specific characteristic challenges.

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

b) Edge computing platforms can be deployed at a factory, smart plant or industrial facility site. It may 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 (Platform as a Service) provider or the OEM of the platform may require edge computing platforms and edge devices that are designed for effective maintenance via an IIP, in case 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 may 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 might not be 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) Insufficient electromagnetic shielding of IIoT or IoT devices. While electromagnetic compatibility (EMC) of embedded devices can be without any concern in an isolated environment, due to

