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)

IECNORM.COM : Click to view the full PDF of ISO/IEC 24392:2023

Reference number
ISO/IEC 24392:2023(E)

© ISO/IEC 2023

IECNORM.COM : Click to view the full PDF of ISO/IEC 24392:2023

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

IECNORM.COM : Click to view the full PDF of ISO/IEC 24392:2023

© 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.

IECNORM.COM : Click to view the full PDF of ISO/IEC 24392:2023

© 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.

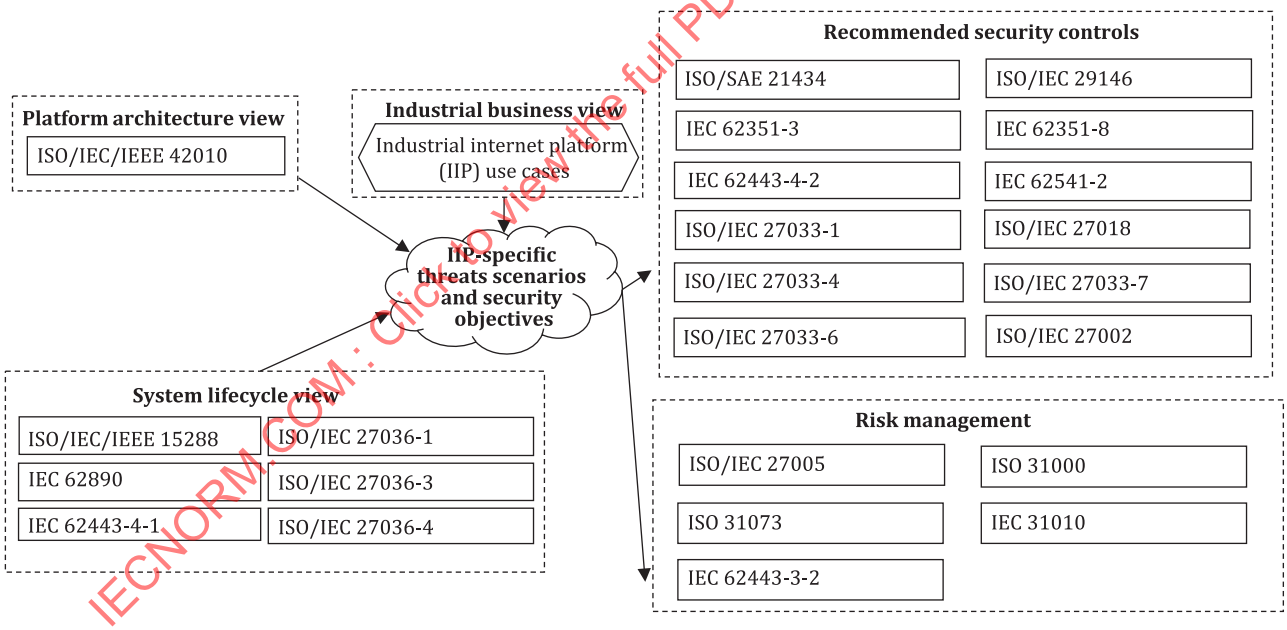


Figure 1 — The relationship between this document and other relevant standards

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.

IECNORM.COM : Click to view the full PDF of ISO/IEC 24392:2023

© ISO/IEC 2023 – All rights reserved

IECNORM.COM : Click to view the full PDF of ISO/IEC 24392:2023

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]

IECNORM.COM : Click to view the full PDF of ISO/IEC 24392:2023

© ISO/IEC 2023 – All rights reserved

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.]

IECNORM.COM : Click to view the full PDF of ISO/IEC 24392:2023

© ISO/IEC 2023 – All rights reserved

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

IECNORM.COM : Click to view the full PDF of ISO/IEC 24392:2023

© ISO/IEC 2023 – All rights reserved

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

IECNORM.COM : Click to view the full PDF of ISO/IEC 24392:2023

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;

© ISO/IEC 2023 – All rights reserved

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.

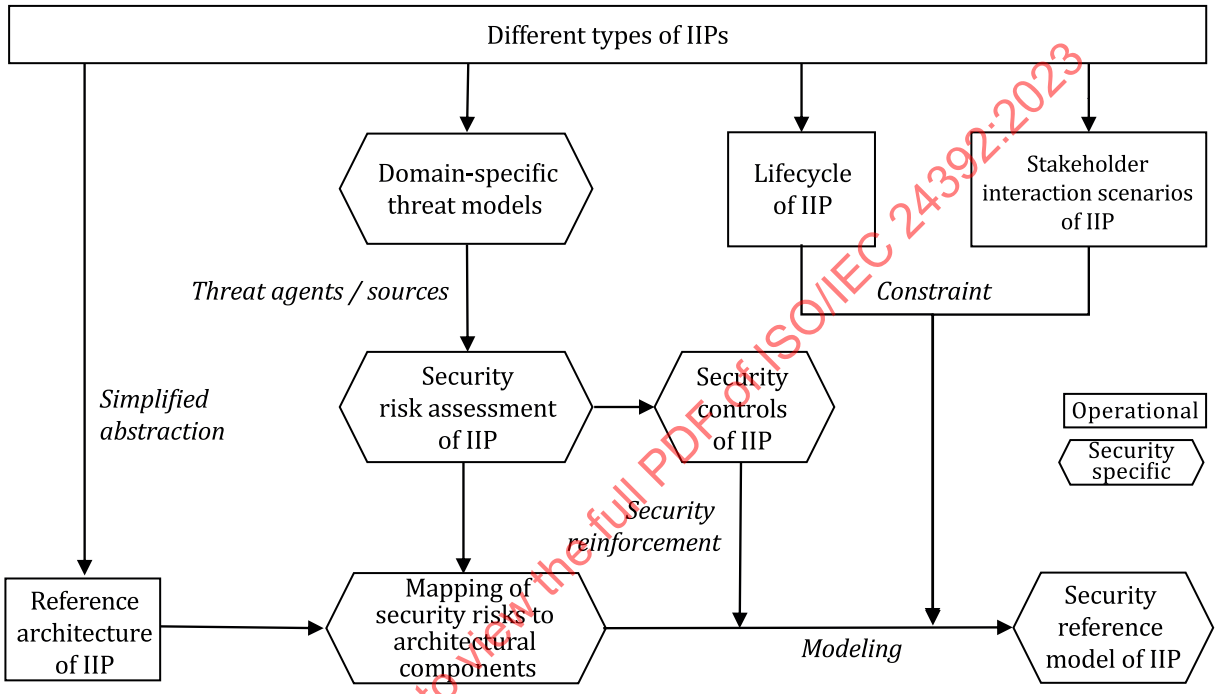


Figure 2 — Establishment of a security reference model of an IIP

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).

IECNORM.COM : Click to view the full PDF of ISO/IEC 24392:2023

© ISO/IEC 2023 – All rights reserved

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

IECNORM.COM : Click to view the full PDF of ISO/IEC 24392:2023

 © ISO/IEC 2023 – All rights reserved

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.

IECNORM.COM : Click to view the full PDF of ISO/IEC 24392:2023

© ISO/IEC 2023 – All rights reserved

u) Smart manufacturing equipment applications continue to change, and the boundaries between different life cycles are blurred.

v) The development cycles of industrial applications and the sources of integrated software are diverse. Application research and development and implementation are transitioning towards openness and customization, thus including multiple existing software libraries, code snippets, configuration files and scripts. A large number of unknown application publishers on the IIP can provide users with industrial applications of varying quality (and a number of software errors that can be vulnerabilities) and insufficiently tested combinations of personalized functions.

w) In industrial control systems that do not process functional safety related tasks, non-secure-by design libraries can be used. These libraries can lack protection by adequate security controls, especially if they are not regularly maintained, close to the end of their life span or primarily not intended for use in an industrial environment.

x) The industrial control system software itself can have security problems such as buffer overflow and insufficient access control.

6.2 Security threats to IIPs

The characteristics of IIPs introduce additional security threats that are specific to IIPs. This subclause lists IIP-specific threats and the corresponding characteristics being exploited (appended at the end of each threat).

a) Vulnerable wireless sensors. The factory environment is complex, the number of production equipment is large, the types are different, and the layout is sophisticated. The number of equipment that collect data are greatly increased as traditional field wiring cannot always meet the challenge. The use of wireless sensors can effectively solve the wiring problem, especially if frequent reconfigurations are used and EMI is not an issue. However, wireless sensors usually have limited computing resources and can often be unencrypted and cryptographically unauthenticated. Therefore, attackers can stealthily copy and potentially alter data by attacking wireless sensors or by monitoring wireless network signals. It is challenging to deal with the trade-off between data confidentiality and data authenticity, and the limited computing resources should be appropriately used to address the most important concerns of IIP participants. This threat is raised by the characteristic specified in 6.1 a).

b) Operation failure in the edge computing platform. A large number of edge computing platforms are deployed on the factory side. It is difficult for the platform provider to provide centralized maintenance, as multiple OEMs can be involved, and the local maintenance capabilities at the factory side can be limited. There is a business interruption risk if an edge computing platform fails, the factory side cannot be repaired locally and the platform provider cannot provide maintenance in time via the IIP. This threat is raised by the characteristic specified in 6.1 b).

c) Data leakage of end-of-security support equipment. There is a large amount of equipment in industrial scenarios and many types of equipment are scrapped every year. The storage devices of these end-of-security support devices can contain sensitive data such as production data or secret keys. If the end-of-security support devices are not handled properly, data leakage can occur. This threat is raised by the characteristic specified in 6.1 c).

d) Hacking into individual devices.

   1) After the production network is completely set up, the factory connected to the cloud platform can use occasional equipment replacement or business upgrades. The upgrades can be implemented as a small-scale IoT equipment installation or update. If the newly installed or updated equipment is not set up in good security settings, it can be connected to a large factory network, and attackers can use these devices with insufficient security settings to attack the entire system or network. This threat is raised by the characteristic specified in 6.1 d).

   2) IoT devices, such as wireless sensors, have a certain amount of computing and processing capabilities, but their computing resources are limited, and encryption is difficult. Attackers

IECNORM.COM : Click to view the full PDF of ISO/IEC 24392:2023

© ISO/IEC 2023 – All rights reserved

can use these devices to initiate different attacks, like replay attacks or DoS attacks and thus disrupt the normal operation of the system. This threat is raised by the characteristic specified in 6.1 e).

3) Installing mitigations or remediations to protect products from published vulnerabilities via CVEs is difficult. Most of the factory products can be acquired from different suppliers. A supplier may rename a product, causing the same device to have a different name. The confusion of renaming the device makes it potentially difficult to track the CVE of the product and update the vulnerability patch in time. This security threat is partially IIP specific, as it arises from the interaction of multiple IIP participants. Accordingly, this threat requires specific attention, particularly concerning traceability along the supply chain. Suppliers should have the capability to handle vulnerability reports in both products and services provided in support to their customers. This work can help organizations manage risk in areas of vulnerability disclosure (see ISO/IEC 29147) and vulnerability handling processes (see ISO/IEC 30111). Acquisition contracts should require that suppliers develop and provide updated software to fix bugs and vulnerabilities and add functionality. It is critical that the integrity and authenticity of updates are verified. Suppliers can only provide software updates for which integrity and authenticity can be verified. An up-to-date inventory of assets can be used within the supply of the product or service. Inventory can be further refined to include parts or components of software and software systems. This level of inventory detail can help organizations manage risk and compliance requirements in areas such as intellectual property and license management and technical vulnerabilities. This threat is raised by the characteristic specified in 6.1 u).

e) Side channel attacks. Existing IoT devices can have insufficient electromagnetic shielding, and attackers can stealthily copy and potentially alter data through side-channel attacks. As a multitude of IoT devices can relate to an IIP, this aspect should be considered already during the supplier selection stage. Additional EMC-shielding or restrictive equipment siting is necessary, if sensitive information can be disclosed. This threat is raised by the characteristic specified in 6.1 f).

NOTE Typically, it is possible that continuously changing data streams (e.g. short-lived data such as analogue values provided by some sensors) do not require any confidentiality related protection, but always require data integrity and process measurement integrity.

f) Data leakage and alteration during transmission. As data alteration is usually more threatening than data leakage in the industrial environment, tradeoffs should be done to spare more resources for security services that tackle data alteration.

1) Computing resources of IoT devices are limited and the network environment is poor, thus security controls that require high resource are not applicable. Attackers may stealthily copy and potentially alter data by monitoring and intercepting network data streams. As data alteration is usually more threatening than data leakage in the industrial environment, tradeoffs can be done to spare more resources for security services that tackle data alteration. This threat is raised by the characteristic specified in 6.1 g).

2) In the industrial internet scenario, factories and cloud platforms exchange large amounts of data, and attackers can intercept network data streams to stealthily copy and potentially alter data. This threat is raised by the characteristic specified in 6.1 h).

g) The attacker hacks into traditional factory devices illegally

1) Traditional factory equipment does not encrypt or prohibits encryption by default, and this equipment lacks user or equipment authentication mechanisms. When these devices connect to the internet, attackers can find these devices through sniffing and other technologies, illegally invading the network and exposing other devices to attack. This threat is raised by the characteristic specified in 6.1 i).

2) Industrial control equipment is the most common edge access equipment of the industrial internet. There are many types of industrial field equipment, and many communication protocol standards. The coexistence of international standards, national standards, industry standards, and corporate standards can complicate governance. Therefore, any system on the

IECNORM.COM : Click to view the full PDF of ISO/IEC 24392:2023

© ISO/IEC 2023 – All rights reserved

network which can no longer be patched should be removed from the network. This threat is raised by the characteristic specified in 6.1 c).

3) The diversity of factory types is complex, and the number of sites is large. Accordingly, it is not easy to manage the equipment passwords uniformly. Most factories have insufficient security awareness. The account passwords of a large number of hosts are stored on the host in the form of files and shared with the network. Weak account passwords are even initially set by the manufacturer and remain unchanged by the operator. This is easy for attackers to invade illegally. This threat is raised by the characteristic specified in 6.1 k).

4) Obsolete and unsupported software is often used in manufacturing plants. At present, the host operating system of many supporting plant control systems is operated on Windows server, Windows 10/11 Client OS software and occasionally on Linux-based operating systems, such as SUSE Linux Enterprise Server (SLES) or Red Had Enterprise Linux (RHEL).[1)] Patches for vulnerabilities in the OS of these supporting systems are often not updated promptly. Seldom or missing updates are usually acceptable for certified and less complex embedded devices connected to the supporting systems. For the supporting systems however, the OS software can become obsolete, for example, if the OS vendor no longer supports specific releases (e.g. older versions of Windows 10 or older Linux distribution versions). This leads to the threat of security vulnerabilities in the system. Attackers can use these vulnerabilities to illegally invade the control system. This threat is raised by the characteristic specified in 6.1 j).

h) Unauthorized access to networks and lateral movement across network boundaries.

1) Different security levels and equipment protection capabilities can be set according to different regional divisions in industrial parks. When the equipment moves, relocation during the transition period can cause regional protection failures. Network segregation of physical networks, VLANs or at the network virtualization level (e.g. with software defined networking) and the corresponding network communication controls (introduced by ISO/IEC 27033-1) should be considered. Detailed guidance can be taken from ISO/IEC 27033-4 for security gateways, ISO/IEC 27033-5 for VPNs, ISO/IEC 27033-6 for wireless IP communication and ISO/IEC 27033-7 for VLANs and network virtualization. This threat is raised by the characteristic specified in 6.1 l).

2) The boundaries of the regional networks in the plant are unclear and interconnected. For example, the boundaries of the production network and office network are blurred, and different businesses and equipment are mixed. The office network is more closely connected to the internet, and the people who use the office network are diverse. There is a higher probability of security vulnerabilities that attackers can exploit. Therefore, the boundary between the industrial control system and other networks (e.g. connected to an IIP) should provide isolation to reduce the risk of a cyber-attack. This threat is raised by the characteristic specified in 6.1 m).

i) Confidentiality about network access points (IP addresses, network port numbers, MAC address, service access points) is susceptible to disclosure. Different stakeholders exchange digital information in the production system, which can lead to the loss of confidentiality of network access points. While communicating with each other, e.g. an IP address and port number can be leaked. This can make it easy for attackers to obtain information about network access points and at the same time, causes mutual influence between communicating network end points. This threat is raised by the characteristic specified in 6.1 n).

j) Network overload causes an interruption in production.

1) There are two types of flow in the factory environment: control flow and non-control flow. The requirements for the two types of traffic are different. Among them, the control traffic is small, but the requirements for delay are very high; the non-control traffic, such as operating data,

1) Windows 10/11 Client OS software, SLES (SUSE Linux Enterprise Server) and RHEL (Red Had Enterprise Linux) are examples of suitable products available commercially. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO or IEC of these products.

IECNORM.COM : Click to view the full PDF of ISO/IEC 24392:2023

© ISO/IEC 2023 – All rights reserved

has large traffic, but the requirements for network delay are relatively low. Suppose the control flow (control command) and non-control flow (general production data) are simultaneously transmitted in a network. In that case, the non-control flow consumes many resources for the control flow, causing interruption and production stagnation to the industrial control system. To prevent such situations, already at the IIP architecture and design level, TSN protocols that ensure an adequate QoS should be used (e.g. QoS Provisions by Network Systems).[46][47] This threat is raised by the characteristic specified in 6.1 o).

2) A large amount of data are generated in the industrial field in real-time. After being connected to the cloud platform, excessive traffic can cause data loss, which affects production. This threat is raised by the characteristic specified in 6.1 p).

k) Attackers impersonate IoT devices to access the platform.

1) There are many types of equipment in industrial scenarios. With increasingly shorter innovation cycles, the amount of equipment that is scrapped every year is also increasing. The storage devices of these obsolete devices can contain sensitive data and store the identification of the device. If the legal identities of these devices are not cleaned up in time during the scrapping process, attackers can access edge computing platforms or cloud platforms through these devices. This threat is raised by the characteristic specified in 6.1 n).

2) IoT devices play a role in collecting and sending data and executing control commands in the industrial Internet. Since many IoT devices have very small computing resources and do not necessarily support device identifiers such as digital certificates, it is not easy to guarantee IoT devices' legitimacy. Suppose a simple device id is used as the identity authentication mark. In that case, it is easy to be faked by an attacker, thereby illegally accessing the edge computing platform or cloud platform. This threat is raised by the characteristic specified in 6.1 c).

l) Industrial internet platform data breach. When users migrate or leave the cloud platform, IIP service providers reallocate resources to new users. If the storage space data are not completely erased, there is a risk of user data leakage. This threat is raised by the characteristic specified in 6.1 q).

m) Cloud-to-cloud interoperability. Each cloud provider offers a special interface to access the cloud, including different communication protocols and APIs. The IIP should be able to securely handle multiple APIs from different vendors. This level of interoperability is necessary in order to foster the scalability of the IIP and the smooth interoperability between IIP customers using different APIs. This threat is raised by the characteristic specified in 6.1 v).

n) Privacy of data transmitted across borders. Different countries have different regulations on data protection, and data transfer across countries can put data privacy at risk. This threat is raised by the characteristic specified in 6.1 w).

o) Inappropriate analysis and decision. The use of cloud platforms for production optimization is the advantage of the industrial internet over traditional industries. The cloud platform can guide and optimize production through big data analysis. However, the data analysis model of the cloud platform also has the possibility of making wrong decisions. Once the cloud platform makes mistakes, decisions can lead to problems such as equipment failure and production stagnation. This threat is raised by the characteristic specified in 6.1 r).

p) Device security cannot adapt to application changes. Industrial applications continue to change, and the boundaries between different life cycles have become blurred. Frequent iterations of application versions can easily lead to system security that cannot adapt to application changes, thereby bringing security threats. This threat is raised by the characteristic specified in 6.1 s).

q) Malicious industrial applications. With the increase in the IIP's openness, industrial applications are characterized by openness and customization. At the same time, there are many scenarios of data sharing and collaborative processing between applications. There can be unknown publishers on the industrial internet that provide publish/subscribe services. If there are malicious publishers, they can pose security threats such as data leakage and cross-application attacks (via forged

IECNORM.COM : Click to view the full PDF of ISO/IEC 24392:2023

© ISO/IEC 2023 – All rights reserved

subscriptions of a publish/subscribe service). This threat is raised by the characteristic specified in 6.1 t).

r) Industrial control system software vulnerability. Industrial control systems may use open-source software, free code or low-cost libraries. Some of these code databases can lack maintenance security vulnerability patches and thus be exploited by attackers. This threat is raised by the characteristic specified in 6.1 t).

7 Security reference model of industrial internet platform

7.1 General

The IIP security reference model is composed of:

— security domains of the IIP system as the architectural dimension;

— the system life cycle as the time dimension;

— the business scenarios and roles dimension.

Figure 3 provides a base on which all kinds of relevant security standards can be further developed or applied. By analysing the three dimensions together, IIP-specific security requirements can be identified.

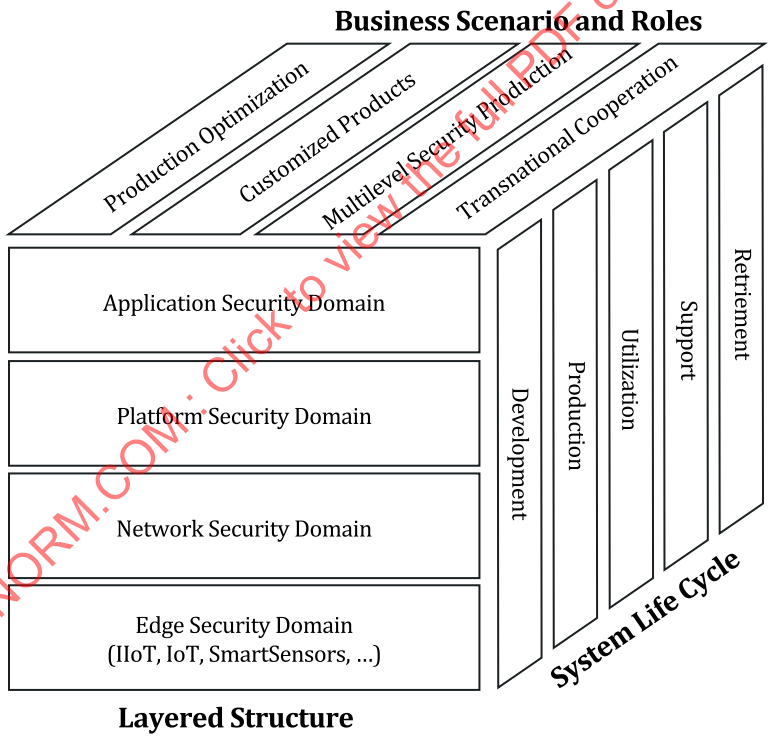


Figure 3 — Security reference model of an IIP

7.2 Security domains of IIPs

7.2.1 General

The security domains of an IIP are based on the reference architecture of IIPs. The corresponding information security needs are extracted and classified according to the major security risks and threats of each domain, as shown in Figure 4.

IECNORM.COM : Click to view the full PDF of ISO/IEC 24392:2023

© ISO/IEC 2023 – All rights reserved

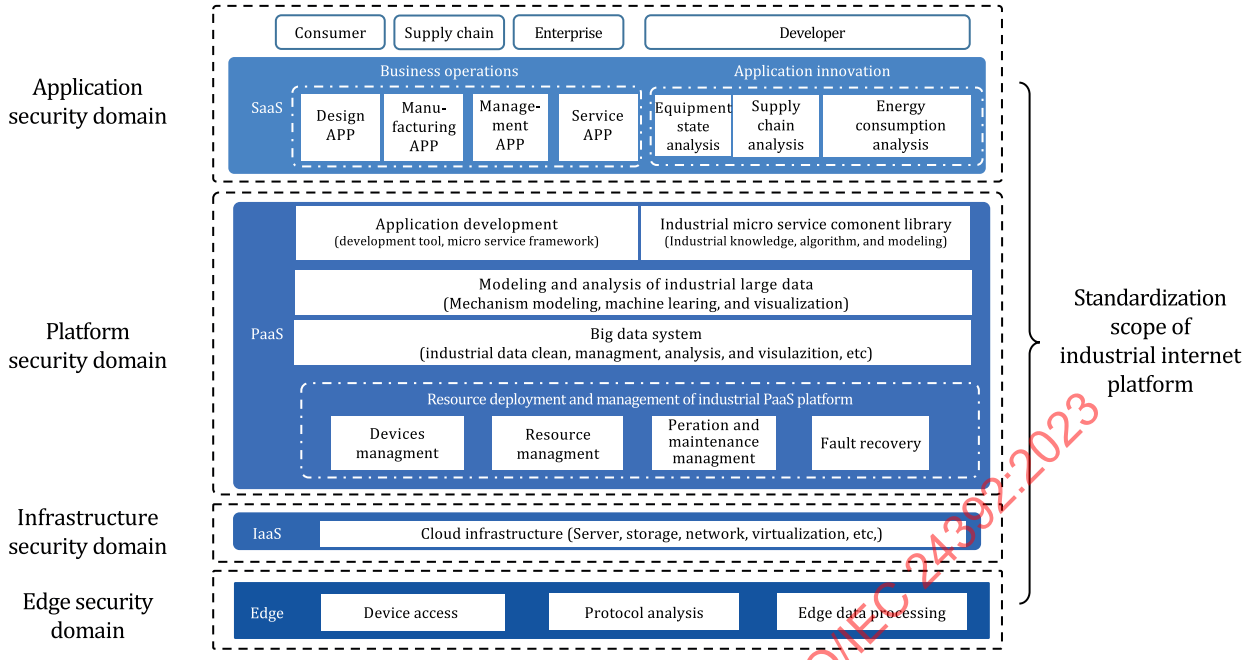


Figure 4 — Security domains of IIPs

NOTE As indicated in Figure 4, the term security domain refers to the layered approach of an IIP. Accordingly, the term security domain is different from the concept of security zone which is used in standards such as ISO/IEC 27019 or IEC 62443-3–2 for grouping digital assets with a similar need for protection.

7.2.2 Edge security domain

The edge domain is responsible for collecting massive industrial data from individual systems through field devices, which raise security issues that are different from traditional software systems. Specifically, the limited computing resources of such devices require careful trade-offs between security and efficiency. Moreover, the diversity of networking transformation protocols and heterogeneity of field devices makes secure data aggregation even more challenging. The authentication and validity of data collection, confidentiality and reliability of network transmission, and authorization and privacy of information exchange and sharing should all be considered. Special consideration is required if multiple protocols are deployed, such as OPC Unified Architecture (see IEC/TR 62541-1, IEC/TR 62541-2 and IEC/TR 62541-12) and legacy communication protocols. Also, the accessibility to the physical devices should be considered when analysing their security threats. When this dimension is analysed together with other dimensions of the reference model, IIP-specific security concerns can be derived. For example, IIP can relay the industry business domain relevant real-time data from one provider to multiple consumers. This requires supporting the setup of contracts and quality of service data delivery agreements between the IIP participants.

7.2.3 Cloud infrastructure security domain

The industrial cloud infrastructure integrates various computing and storage resources to support platform services and industrial applications. Such networking infrastructure intensively uses virtualization techniques, the security of which plays an essential role in the network infrastructure security domain. For example, the coexistence of hypervisor-based virtualization, container-based solutions, and hypervisor-based migration of virtual machines to a spare or backup IIP are important for providing continuous IIP availability. Both virtualization management software and virtualized application software should be protected from attacks. Specifically, virtual machines can be easily forgotten due to their virtuality. If left unattended or unmanaged, virtual machines can become vulnerable to attacks and exploitation.

IECNORM.COM : Click to view the full PDF of ISO/IEC 24392:2023

© ISO/IEC 2023 – All rights reserved

7.2.4 Platform security domain

PaaS is typically used in the platform domain of IIPs to provide an industrial application development environment, store and process industrial big data, and manage industrial microservices. Security issues of the platform domain involve the design, testing, and deployment of industrial applications and the storage, processing, sharing, and depletion of industrial big data. With regard to PaaS, a specific issue of an IIP is the interconnectivity between continuous real-time industry data between IIP participants.

7.2.5 Application security domain

Industrial applications function under specific industrial business scenarios, involving a significant amount of specialized industrial knowledge. The integrity and availability of such knowledge bases are essential to the security of industrial applications. In addition, the industrial applications are the interfaces of IIPs, which directly interact with third-party services and applications, and are more likely to be attacked. Both the security of the industrial applications and the reliability of the third-party applications should be analysed. Specifically, different industrial applications may apply different grading schemes, which require different levels of security. Enforcing the application security controls of the individual applications and supporting their validation and facilitating the interoperability should become differentiating factors of individual IIP vendors.

7.3 System life cycle

7.3.1 General

As described in ISO/IEC/IEEE 24748-1, a complete life cycle of a system can be divided into five stages: development, production, utilization, support and retirement. Each stage involves different tasks and aims for specific objectives. As IIPs consist various stakeholders, e.g. asset suppliers and production managers, each of them is involved in a specific system life cycle. As recommended by the ISO/IEC/IEEE 42010, the description of stakeholders and the environment is shown in Figure 5.

IECNORM.COM : Click to view the full PDF of ISO/IEC 24392:2023

© ISO/IEC 2023 – All rights reserved

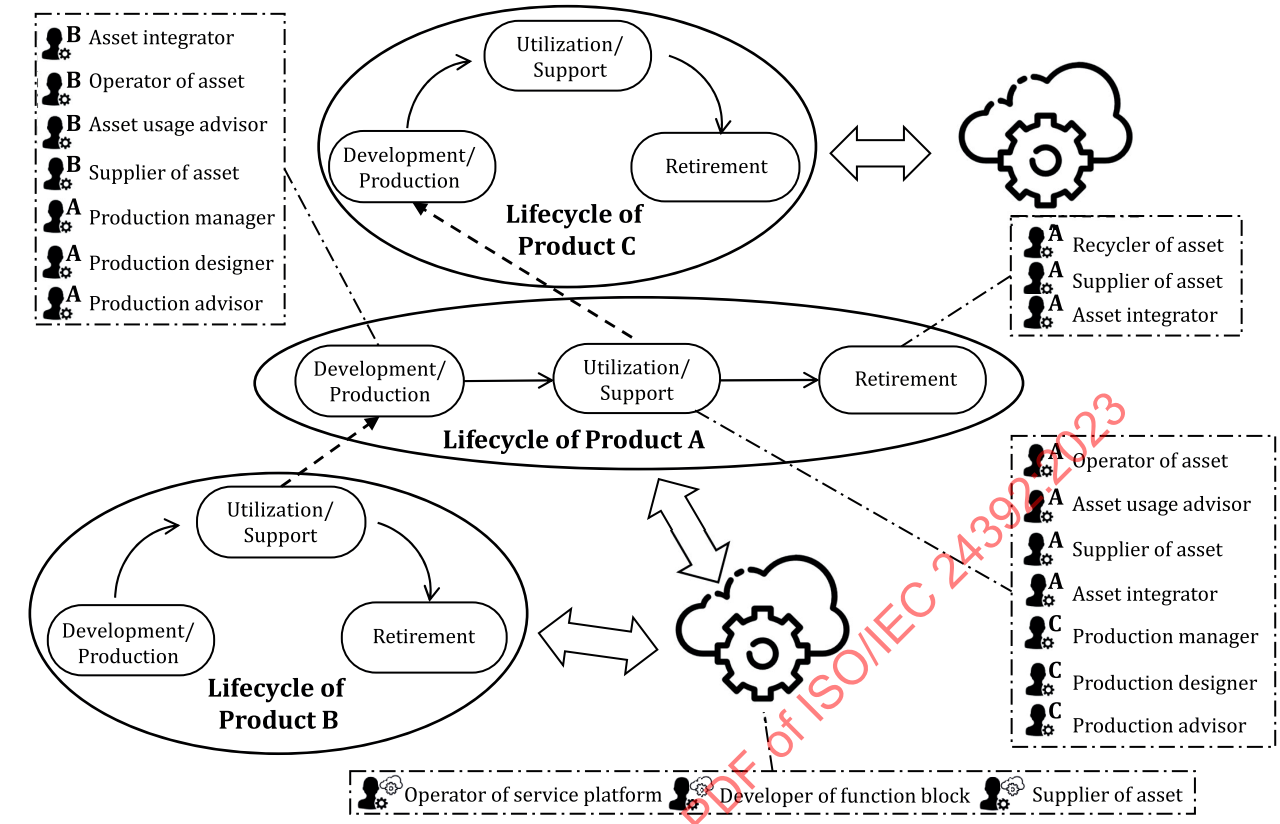


Figure 5 — Coordinated stakeholders and their involvement in the product life cycle

IECNORM.COM : Click to view the full PDF of ISO/IEC 24392:2023

7.3.2 Development and production stage

The production of a certain type of product in a factory involves many other production equipment and stakeholders. As shown in Figure 5, product B production equipment is used to manufacture product A, i.e. the development and production stage for product A. In the meantime, product B is in its utilization and support stage in Figure 6. The stakeholders involved can be divided into three parts. The first part is the stakeholders directly related to product A, such as production manager, production designer, and production advisor. The second part is the stakeholders directly related to other assets such as production equipment B and factory buildings, including supplier of asset, operator of asset, asset integrator, and asset usage advisor. The third part is the stakeholders related to cloud platform, supplier of asset, operator of service platform, developer of function block. These stakeholders also have a complex relationship with each other, e.g. the production manager manages the operator of asset and the asset usage advisor provides advice to the supplier of asset.

© ISO/IEC 2023 – All rights reserved

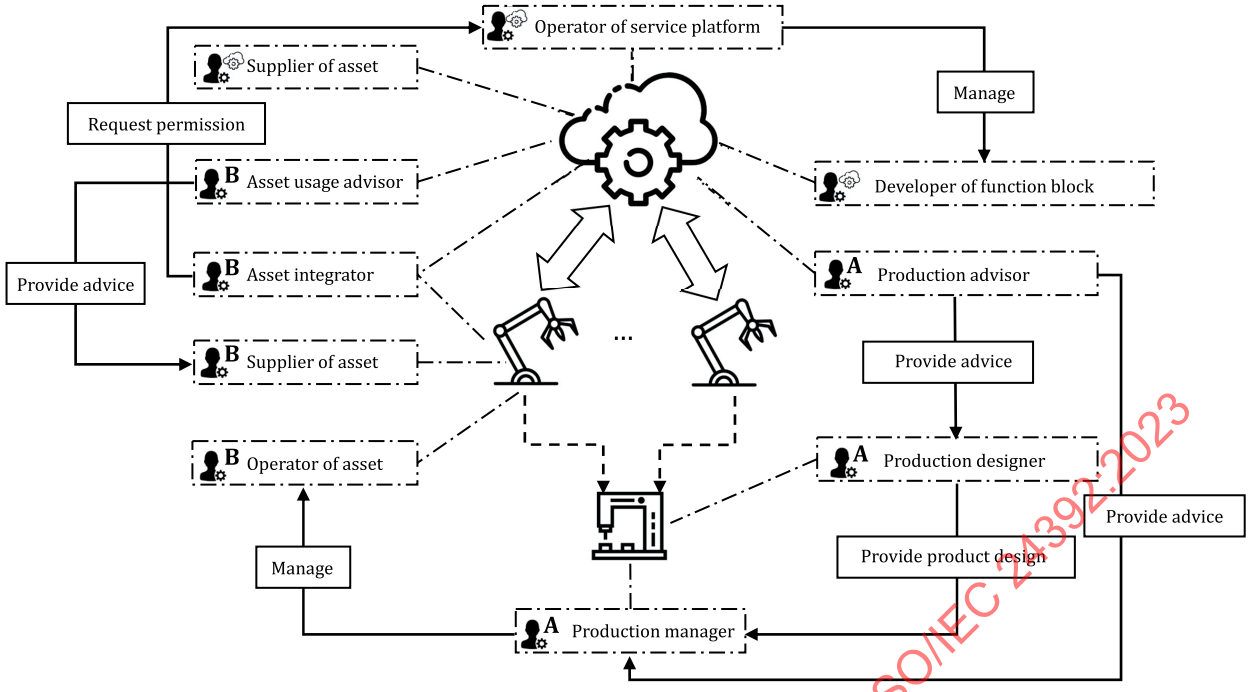


Figure 6 — Development and production stage

Considering the complex scenario in Figure 6, the security threats associated with product A in the development and production stage are as follows. Each of these threats can be classified as one of the threats that are introduced in 6.2.

— Attackers attack wireless sensors to stealthily copy and potentially alter data [see 6.2 a)].

— Data leakage during transmission [see 6.2 g)].

— Network overload causes production interruption [see 6.2 k)].

— Wrong decision on cloud platform causes equipment failure and production shutdown [see 6.2 p)].

7.3.3 Utilization and support stage

The development and production stage of one product (product A) is typically associated to the utilization and support stage of another product (product C). As shown in Figure 7, there are three categories of stakeholders involved in this stage. Firstly, the stakeholders who are directly related to product C, such as production manager, production designer, and production advisor. Secondly, the stakeholders who are directly related to other assets such as production equipment A and factory buildings, including the supplier of asset, operator of asset, asset integrator, and asset usage advisor. Thirdly, the stakeholders related to the cloud platform, e.g. the supplier of asset, operator of service platform, developer of function blocks.

IECNORM.COM : Click to view the full PDF of ISO/IEC 24392:2023

© ISO/IEC 2023 – All rights reserved

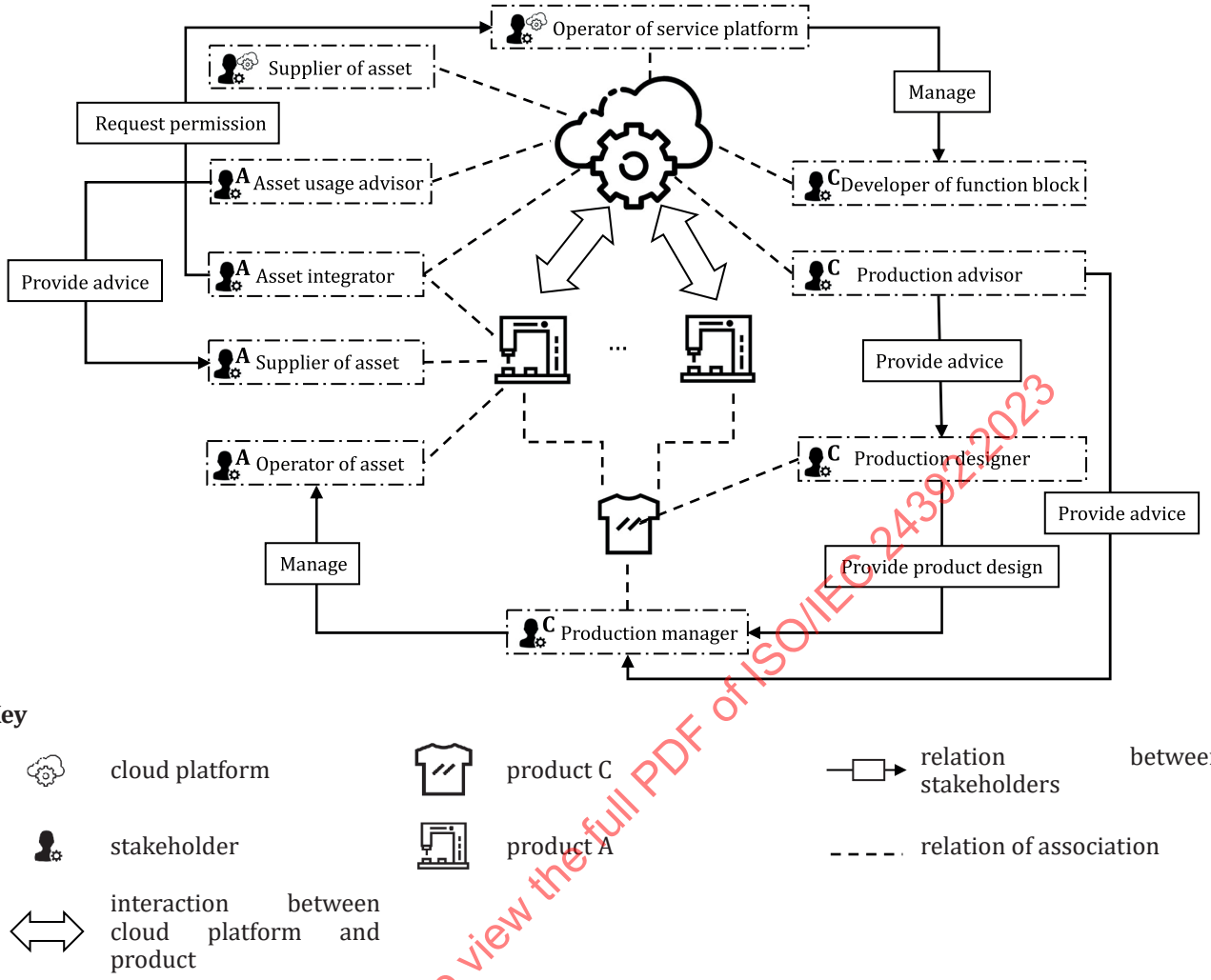


Figure 7 — Utilization and support stage

IECNORM.COM : Click to view the full PDF of ISO/IEC 24392:2023

Considering the complex scenario in Figure 7, the security threats associated with product A in the utilization and support stage are as follows. Each of these threats can be classified as one of the threats that are introduced in 6.2.

— Attackers attack the entire system by hacking individual devices [see 6.2 d)].

— The attacker hack into traditional factory devices illegally [see 6.2 h)].

— Unauthorized access to networks and lateral movement across network boundaries [see 6.2 i)].

— Device security cannot adapt to application changes [see 6.2 q)].

— Malicious industrial applications [see 6.2 r)].

— Industrial control system software vulnerability [see 6.2 s)].

— The edge computing platform is maliciously attacked or the operation fails, and there is a risk of business interruption [see 6.2 b)].

7.3.4 Retirement stage

In the retirement stage, the product scrapping and destruction are also related to multiple stakeholders. The stakeholders involved can be divided into two parts, which are shown in Figure 8. The first part is the stakeholders that are directly related to product, such as the supplier of asset, the recycler of

© ISO/IEC 2023 – All rights reserved

asset and the asset integrator. The asset integrator is responsible for the safe de-integration of retired equipment from the cloud platform. The second part is the stakeholders that are related to cloud platform, i.e. the supplier of asset, operator of service platform and developer of function block.

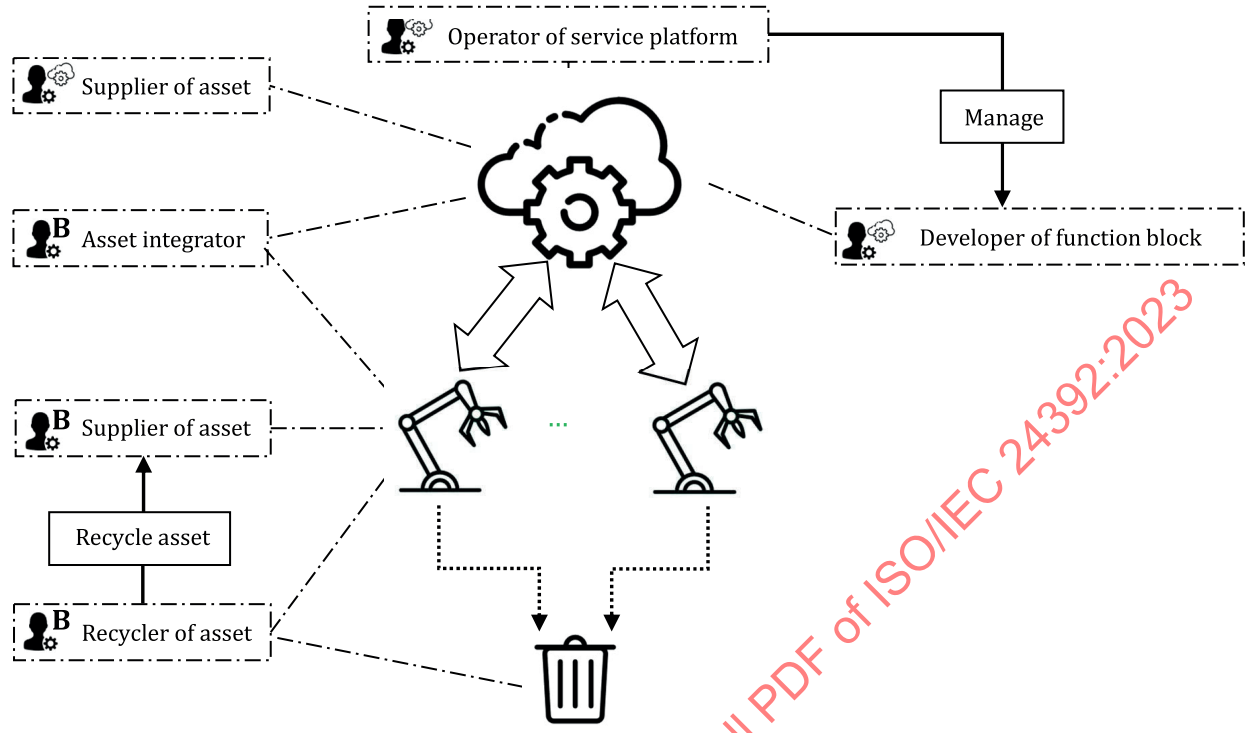


Figure 8 — Retirement stage

Considering the complex scenario in Figure 8, the security threats associated with product B in the retirement stage are as follows. Each of these threats can be classified as one of the threats that are introduced in 6.2.

— Data leakage of end-of-security support equipment [see 6.2 c)].

— Attackers impersonate IoT devices to access the platform [see 6.2 l)].

— Industrial internet platform data breach [see 6.2 m)].

Retirement of a device does not always coincide with the end of security support. Manufacturers and suppliers should provide dates after which software components and software systems will no longer receive security updates. This information should be provided as part of procurement between manufacturers and suppliers, and manufacturers should provide this information to customers. This information provides the opportunity for planning the retirement of an asset.

IECNORM.COM : Click to view the full PDF of ISO/IEC 24392:2023

© ISO/IEC 2023 – All rights reserved

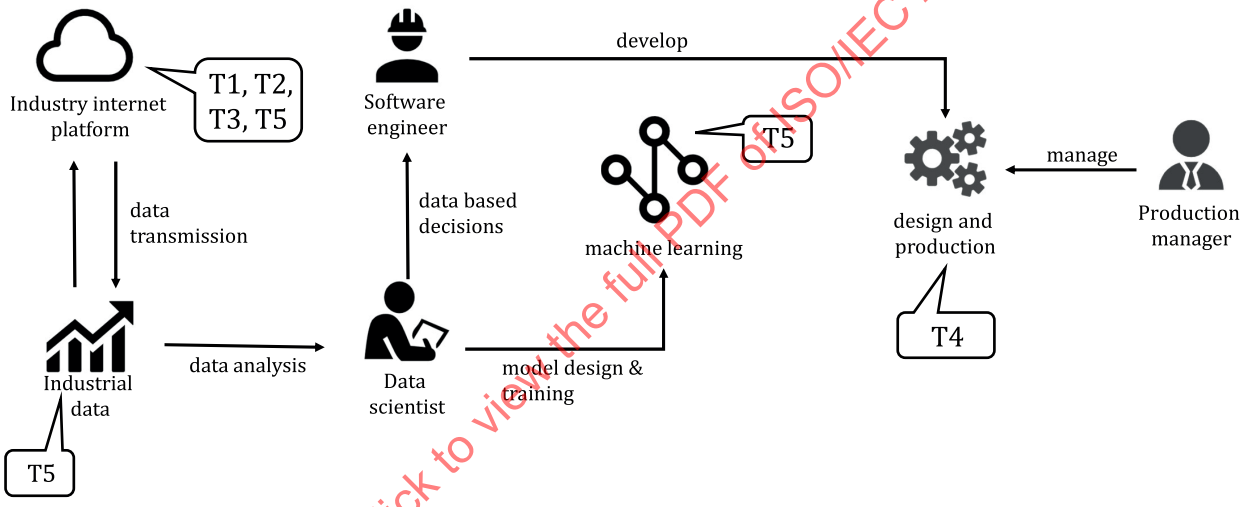
7.4 Business scenarios and roles

7.4.1 General

Different roles from different organizations interact and collaborate with each other via IIPs, so they inevitably share certain data, and introduce more complicated and challenging situations. Each typical business scenario involves particular threats.

7.4.2 Production optimization

As Figure 9 illustrates, data transmission is carried out between the factory and the IIP, and the IIP optimizes production based on the factory data. Data scientists in the factory obtain data for modelling and training to help the factory optimize production. The data scientist communicates the results of the data analysis to the software engineer. Software engineers carry out software development and optimization to realize factory product design and production improvements. The production manager manages the entire production process. Overall, the IIP provides analysis to the people in charge of the manufacturing facilities to help optimize production.



Key

T1 threat 1
T2 threat 2
T3 threat 3
T4 threat 4
T5 threat 5

Figure 9 — Production optimization scenario

IECNORM.COM : Click to view the full PDF of ISO/IEC 24392:2023

The security threats associated with the scenario shown in Figure 9 are as follows. Each threat is associated with a particular part of a scenario.

— T1: attackers impersonate IoT devices to access the platform [see 6.2 l)].

— T2: industrial internet platform data breach [see 6.2 m)].

— T3: wrong decision on cloud platform caused equipment failure, production shutdown, etc. [see 6.2 p)].

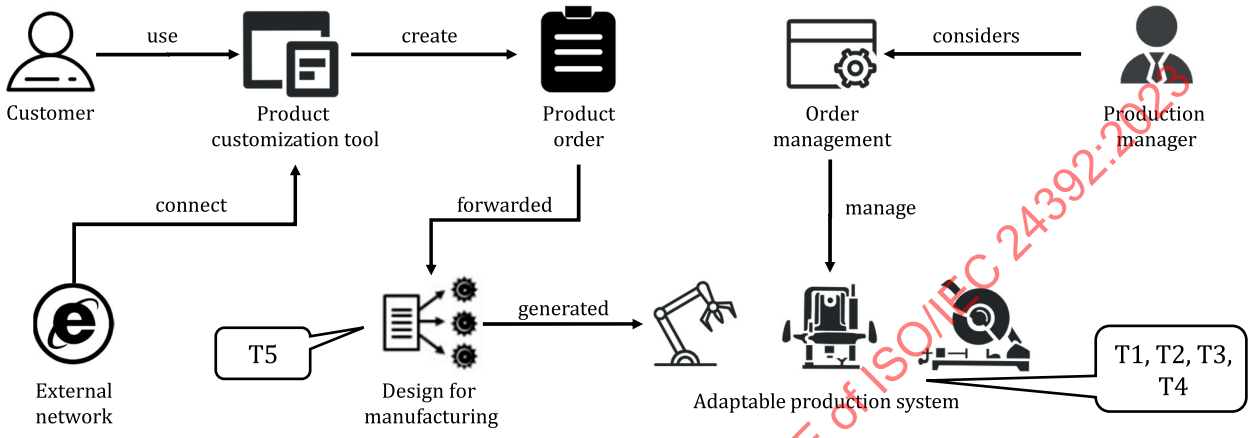
— T4: device security cannot adapt to application changes [see 6.2 q)].

— T5: data leakage during transmission [see 6.2 g)].

© ISO/IEC 2023 – All rights reserved

7.4.3 Product customization

Orders from individuals require customized production. As shown in Figure 10, the customer accesses the factory customization system through the external network and sets personalized production requirements. After the customer configures and completes the production requirements, the corresponding order is generated. The factory forwards the customized order to the corresponding system, and the factory should configure related extended applications to achieve personalized production. The production manager configures the corresponding order management system, and the management system performs production.



Key

T1 threat 1
T2 threat 2
T3 threat 3
T4 threat 4
T5 threat 5

Figure 10 — Product customization scenario

NOTE Figure 10 shows an example scenario. In a similar scenario, part of the production can be directly manufactured under the control of the IIP (e.g. via 3D printing) and parts can be ordered, including the final integration by a platform participant.

The security threats associated with this scenario are as follows. Each threat is associated with a particular part of a scenario.

— T1: attackers attack the entire system by hacking individual devices [see 6.2 d)].

— T2: network overload causes production interruption [see 6.2 k)].

— T3: installing mitigations or remediations to protect products from published vulnerabilities via CVEs is difficult [see 6.2 e)].

— T4: industrial control system software vulnerability [see 6.2 s)].

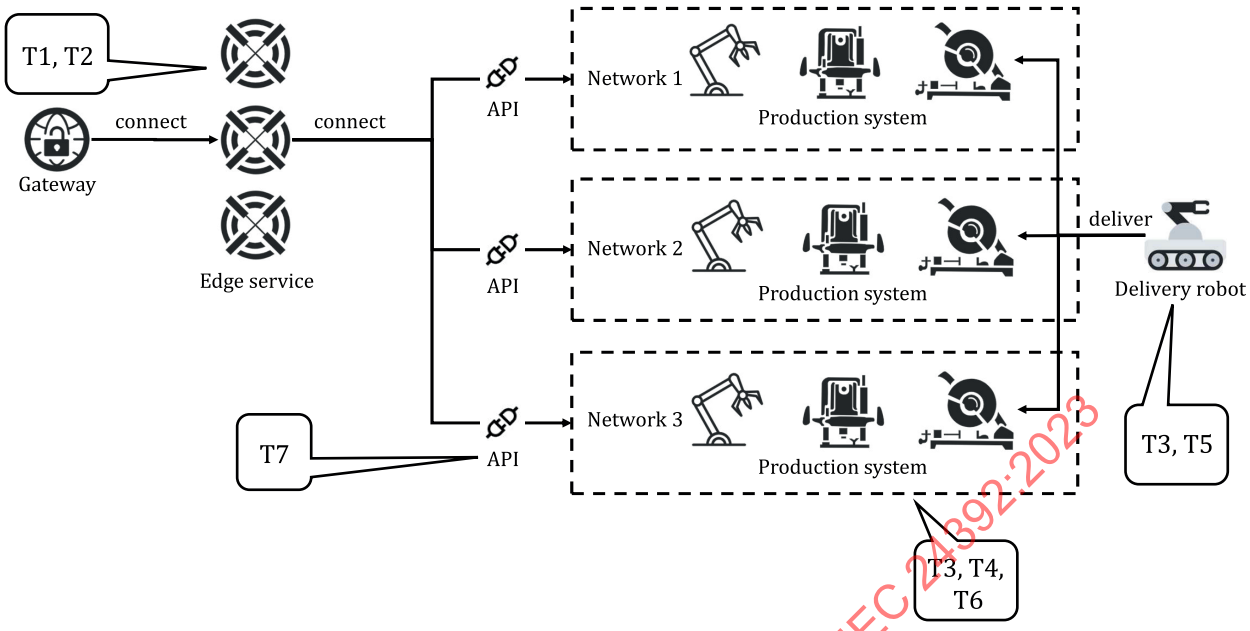
— T5: malicious industrial applications [see 6.2 r)].

7.4.4 Multilevel security production

As shown in Figure 11, there is a gateway inside the factory, and after the edge layer service, the production data are transmitted through different API interfaces. Because different industrial equipment has different levels of trust and confidentiality, most factories use separate areas for production. Equipment with the same security level is placed in the same area. This helps to better ensure industrial equipment protection. At the same time, transport robots are used for cargo transfer.

IECNORM.COM : Click to view the full PDF of ISO/IEC 24392:2023

© ISO/IEC 2023 – All rights reserved



Key

T1 threat 1
T2 threat 2
T3 threat 3
T4 threat 4
T5 threat 5
T6 threat 6
T7 threat 7

Figure 11 — Multilevel security production scenario

IECNORM.COM : Click to view the full PDF of ISO/IEC 24392:2023

The security threats associated with the scenario shown in Figure 11 are as follows. Each threat is associated with a particular part of a scenario.

— T1: attackers attack wireless sensors to stealthily copy and potentially alter data, exposing cluster-head nodes [see 6.2 a)].

— T2: the edge computing platform is maliciously attacked or the operation fails, and there is a risk of business interruption [see 6.2 b)].

— T3: attackers attack the entire system by hacking individual devices [see 6.2 d)].

— T4: data leakage of end-of-security support equipment [see 6.2 c)].

— T5: the attacker hack into traditional factory devices illegally [see 6.2 h)].

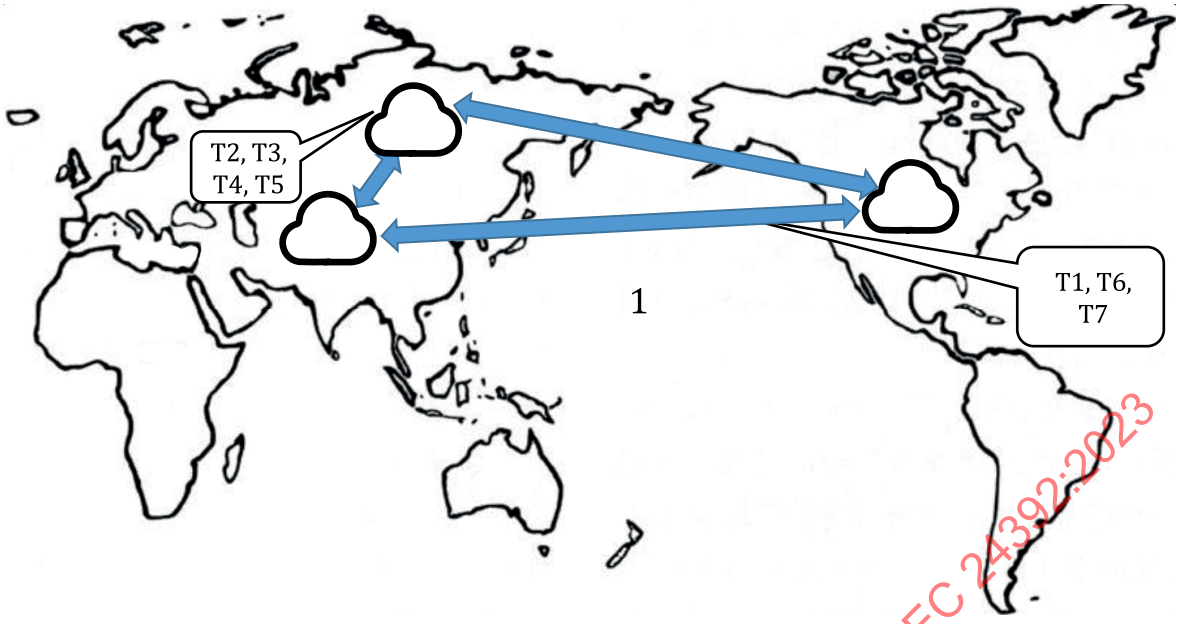
— T6: network overload causes production interruption (6.2 k)

— T7: the confidentiality of IP is susceptible to attacks (6.2 j)

7.4.5 Transnational cooperation

Industrial internet platforms in different countries and regions exchange data (see Figure 12). There are differences in data security laws and regulations in data transmission between different countries, and data structure differences between different IIPs can exist.

© ISO/IEC 2023 – All rights reserved



Key

industrial internet platform

1 confidential information flow
T1 threat 1
T2 threat 2
T3 threat 3
T4 threat 4
T5 threat 5
T6 threat 6
T7 threat 7

Figure 12 — Transnational cooperation scenario

The security threats associated in this scenario are as follows. Each threat is associated with a particular part within the scenario.

— T1: data leakage during transmission [see 6.2 g).

— T2: industrial internet platform data breach [see 6.2 m).

— T3: attackers attack the entire system by hacking individual devices [see 6.2 d)].

— T4: cloud platform configuration errors can cause equipment failure, production shutdown, etc. [see 6.2 p)].

— T5: attackers impersonate IoT devices to access the platform [see 6.2 l)].

— T6: cloud-to-cloud interoperability [see 6.2 n)].

— T7: privacy of data transmitted across borders [see 6.2 o)].

IECNORM.COM : Click to view the full PDF of ISO/IEC 24392:2023

© ISO/IEC 2023 – All rights reserved

8 Security objectives and controls for IIPs

8.1 Security objectives

The following functional, performance and regulatory compliance objectives are assumed to be important for any IIP:

— scalability within a defined range;

— performance, including real-time performance with guaranteed quality of service;

— responsiveness with regard to the interaction of IIP participants;

— compliance to national and international domain specific standards applicable for the IIP and the involved IIP participants.

Considering the IIP-specific threat scenarios, the following security objectives are intended to meet these functional, performance and regulatory compliance objectives.

a) Implemented security controls should not be perceived as an overhead as an IIP scales up. Specifically, the IIP should be designed to prevent easy circumvention of security controls. There should be no incentive to circumvent security measures.

b) Comprehensive logging should be enabled for IIP activities and securely recorded as part of forensic readiness in potential litigation between platform partners, especially if partners from different countries are involved.

c) Appropriate authentication and authorization technologies and solutions should be used to enforce the identity checks of devices and individuals accessing the IIP, especially in the case of IoT devices with limited access control-related processing resources. Authentication should be accomplished by establishing relations with external certification authorities.

d) Ensure the continuity of the production process and try to avoid production pauses and delays caused by security issues (e.g. attacks or wrong decisions on the cloud platforms). Especially the involvement of the IIP should not impact the production processes that involve multiple IIP participants. This can involve the use of redundant Next-generation Firewalls (NGFW) that allow host-standby and switchover within less than one second. Using NGFWs includes the deployment of application layer firewalls with deep packet inspection (DPI) and intrusion prevention systems (IPS). As an advantage of IIPs, the knowledge about the software applications and services deployed by the IIP participants should be leveraged for application specific DPI, IPS and communication responsiveness, including QoS.

e) Ensure that the network is available to transmit large amounts of data to meet the needs of industrial production.

f) Security objectives should be met through all life cycle phases of the IIP and its participants. This includes IoT and IIoT platforms and devices development, production, engineering and integration, utilization, operation, support and maintenance, up to the retirement stage of individual IIP participants or the IIP itself.

g) The organization managing an IIP should select and enforce acceptance criteria with the IIP participants with regard to commitments on continuously meeting security objectives. This includes applying a priority rating for mitigating newly identified risks identified at the IIP, an IIP participant, an IoT device, an IIoT device, or a related CPS.

h) IIP customers (who subsequently operate the IIPs) and suppliers of IIPs should develop a formal written scope for the security objectives at the beginning of the partnership, in which:

— IIP customers should clarify their security objectives and evaluate whether the services provided by the IIP provider meet them. General guidance on supplier relationships related security controls should be taken from ISO/IEC 27036-1 and ISO/IEC 27036-2.

IECNORM.COM : Click to view the full PDF of ISO/IEC 24392:2023

© ISO/IEC 2023 – All rights reserved

— it is presupposed that IIP suppliers ensure that the security services they provide comply with any relevant legal policies of the customer's country. It is also expected that IIP customer requirements stipulate that the security services provided by the IIP supplier comply with any relevant legal policies of the customer's country. The complexity of meeting the security objectives can increase if the customer is a multinational corporation that stipulates compliance with several national regulations.

i) In the case of limited computing resources of IoT devices, ensure the availability and integrity of data transmission and if relevant, ensure the confidentiality of the transmitted data (e.g. by cryptographic techniques to ensure that it is not stolen by attackers).

j) Passwords and cryptographic keys should be secured:

— administrators should establish password management policies to ensure that passwords of sufficient strength are used and that passwords are not compromised;

— developers should use technical means to prohibit the use of low strength passwords, taking into consideration the password length, password complexity and password history (avoidance of reuse);

— strong cryptographic technologies should be used and secure cryptographic key management should be in place, taking into account an appropriate lifetime of the cryptographic keys.

k) Ensure the security of third-party software:

— IIP customers should review the identity of third-party application developers, and accurately inform IIP customers of the possible security risks of third-party software;

— IIP suppliers should evaluate the security risks of third-party software and decide whether to use it;

— third-party developers should provide credible identification to the IIP suppliers and customers.

l) Define clear network boundaries between production networks, office networks, and IIP networks and enforce appropriate access control policies.

8.2 Security controls

8.2.1 General

IIP-specific security controls should be deployed to protect against IIP-specific threats. Additionally, security controls best suited to meet the security objectives of the IIP participants should be implemented in line with the business domain each IIP participant. For IT and IoT related IIP participants, controls specified in ISO/IEC 27002 should be applied. For OT related IIP participants, controls from IEC 62443-4-2 should be applied. For the automotive domain, ISO/SAE 21434 or related standards should be applied. For the non-nuclear energy domain controls, ISO/IEC 27019 should be applied, as well as for further business domains (e.g. for providing assessment services, certification services).

NOTE This subclause does not intend to repeat all controls from cloud security, networking security (e.g. ISO/IEC 27033-2), but to emphasize security controls related to an IIP and IIP participants.

8.2.2 Physical security

The edge domain, network/business domain, and application domain of an IIP and its participants are made up of physical devices such as sensors, terminals, routers, switches, computers, and other smart devices and CPS. Their physical security constitutes an important aspect of an IIP and its participants.

Physical security objectives include, but are not limited to:

a) Physical access authority and control system of physical equipment should be established.

IECNORM.COM : Click to view the full PDF of ISO/IEC 24392:2023

© ISO/IEC 2023 – All rights reserved

b) Requirements for reliable and stable power supply should be established.

c) Physical protection measures should be provided for fire protection, burglar proof, moisture proof, device tampering, lightning protection and electromagnetic protection etc., to protect against environmental threats as listed in ISO/IEC 27005.

d) Terminal devices (e.g. video surveillance devices,) that should not be publicly accessible, should be the located in place that cannot be accessed without auxiliary tools, such as setting up stairs or unlocking.

e) The programming interface of edge devices such as RTUs, PLCs or IEDs should be disabled via physical settings where applicable, e.g. via manual electric switches of standard dual-inline packages (DIL switches). This helps to prevent advanced persistent threats from altering configuration settings. Similarly, where applicable, user mode configuration changes that require physical proximity of a user should be restricted. These settings are important for smart devices of the IIP and smart devices of IIP participants, if reachable via the IIP.

NOTE Edge devices of the IIP participants that are not related to the IIP under consideration are beyond the scope of this document.

f) Access to USB and peripheral devices ports should be restricted. This should be in line with the principles of least privilege access control measures.

8.2.3 Network security

The network part of IIP includes the communication network, involving the internet and industry-specific networks. As it has the characteristics of network diversification, its security objectives mainly involve access security and communication security.

The context establishment for the risk assessment should consider the primary assets (e.g. CPS) and supporting assets (e.g. IT, IoT, IIoT) that participate in business processes via networks of an IIP. In the special case of a platform participant that provides or deploys OT, the network security related risk assessment should consider the two-phase approach of preliminary and detailed risk assessment, according to IEC 62443-3-2. While such assessment mainly concerns the respective IIP participant, the network security controls should ensure that neither the participant not the IIP are adversely impacted by misconfigured networking devices or legacy technology.

Where networking related risk assessment indicate a higher need for protection, dedicated interfaces to selected IIP participants should be enforced, e.g. via demilitarized zones.

Further guidance on suppliers and networking related security controls should be taken from ISO/IEC 27036-3 and ISO/IEC 27036-4.

8.2.4 Access security

Due to the complexity of the interactions between the members of an IIP, an attribute-based access control (ABAC) should be offered in addition to the typical role-based access control (RBAC) approach, in the implementation of an IIP. The ABAC allows for a fine granular access control by allowing security related attributes for the objects, that are being accessed (e.g. of a wind turbine), the subject (e.g. a maintenance staff member who wants to change settings, or an agent collecting data for preventive maintenance) and attributes of the environment (e.g. limitation to given daily hours or operating conditions). With an ABAC approach, the IIP can centrally support the management of objects, subjects and attributes that are relevant for the interactions via the IIP.

Access security objectives include, but are not limited to:

a) All kinds of sensory terminals and access devices should have unique identities when accessing the network.

b) There is an identification mechanism for all kinds of perception terminal when access takes place.

IECNORM.COM : Click to view the full PDF of ISO/IEC 24392:2023

© ISO/IEC 2023 – All rights reserved

c) For access control via network, such protection measures should be taken, including disabling idle IP ports (at OSI layer 3) and disabling specific transport services (e.g. selected TCP or UDP services at OSI layer 4).

d) For network boundary devices such as gateways, firewalls, NGFW, optical or electrical physically unidirectional security gateways, security policies should be configured, and protection measures, such as network payload data integrity protection, payload data encryption and access control, are required. These network boundary devices should be applied also within one IIP, if different cloud services are interconnected or geographically distributed computing environments are deployed.

e) Allowlisting of devices that communicate with industrial security gateways should be defined in order to discard any spoofed device trying to communicate. Allowlisting should be enforced for IIP interfaces or computing resources that relate to platform participants which do not require dynamic and frequent reconfigurations or the addition or removal of smart devices.

f) Machine to machine (M2M) authentication should be enabled. M2M communication between different participants of an IIP should always be provided with network communication integrity settings enforced. Encryption in M2M communication should be enabled if sensitive (not just short-lived data) is exchanged.

g) A mechanism for detecting any unauthorized device or software in the network should be implemented. Unexpected network devices or unexpected devices physically, logically or virtually connected to a scanned network should be reported to a SIEM system for further correlation and investigation.

8.2.5 Communication security

Communication security objectives include, but are not limited to:

a) For data transfer protocols of an IIP, a data verification function is required to ensure the integrity of data transmission.

b) Standardized timestamp mechanism and other techniques should be used to ensure the availability of data transmission.

c) Technical means should be used to protect the privacy of data transmission.

d) Before network data interaction, such measures as an accreditation scan should be taken to provide proof for the credibility of the identity of the two parties in interaction.

e) An encryption algorithm allowed by national laws and regulations should be used to encrypt the network transmission data to ensure the confidentiality of the information.

f) The IIP should include the capability to counter a base station attack and network relay attack.

8.2.6 System security

8.2.6.1 Node and system security

There should be explicit security objectives for the resource-rich (i.e. computing, energy, and storage) hosts and systems that exist in IIPs, including:

a) Identification of users logging in each system in the IIP.

b) Access control function should be enabled and the corresponding security policy should be formulated.

c) All default passwords should be identified and changed.

d) A management system should be established under which redundant and expired accounts should be deleted on a regular basis.

IECNORM.COM : Click to view the full PDF of ISO/IEC 24392:2023

© ISO/IEC 2023 – All rights reserved

e) An operating system in the IIP should follow the principle of minimum privileges.

f) Patches should be updated in time; software against malicious code should be installed, and a version of software against the malicious code should be updated in a timely way.

g) The security of middleware technology should be guaranteed when it is used.

h) Activity logs from the systems should be stored and reviewed on a continuous basis.

8.2.6.2 Resource-restraining nodes and systems security

There should be explicit security objectives for the resource-restraining (i.e. computing, energy, and storage) nodes and systems that exist in IIPs, including:

a) Identity verification information such as a default password should be updated.

b) Redundant and expired accounts should be deleted on a regular basis.

c) All critical patches should be updated in a timely manner.

8.2.7 Application security

An IIP requires a large number of software applications to collect a large amount of data in practical applications, and their security objectives include but are not limited to:

a) The function of data validity inspection should be provided to ensure that the data format or length through human-machine interactive input or communication interface input conforms to the requirements of the system setting.

b) Important data should be backed up and stored at a remote location (in a different fire protection zone) for the continuity of operations.

c) All software used should not be allowed to transmit data to the outside world without the permission of the system operator.

d) Applications development should follow the secure software development life cycle.

e) The application software should be audited for security flaws.

f) Application allowlisting should be defined so that any malware cannot be executed.

8.2.8 Operation and maintenance security

The industrial Internet platform is a complex system composed of multiple subsystems. Its operation and maintenance are usually carried out by different responsible parties. Its security objectives include:

a) The different parties responsible for the IIP should specify the requirements for the purchase of relevant devices, systems and services, such as qualification and dependability of supplier, the details of system documentation and supply chain security.

b) For the relevant participants in the operation and maintenance of IIPs, requirements should be specified of personnel qualification, identity audit, trustworthiness certification and promise of integrity to ensure security and credibility in the process of operation and maintenance.

c) Security objectives should be specified with regard to timeliness and maintenance tools for the operation and maintenance of the IIP. Remote maintenance security regulations should also be specified for equipment in need of remote maintenance.

IECNORM.COM : Click to view the full PDF of ISO/IEC 24392:2023

© ISO/IEC 2023 – All rights reserved