International Standard

ISO/IEC 27403

First edition
2024-06

Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics

Cybersécurité — Sécurité et protection de la vie privée pour l'IDO — Lignes directrices pour la domotique-IDO

Reference number
ISO/IEC 27403:2024(en)

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

Published in Switzerland

Contents

Page

Foreword

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

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

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

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

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

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

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

Introduction

Although IoT-domotics have been widely applied worldwide, many IoT-domotics devices, communication protocols and platforms are developed without sufficient security and privacy considerations, which can pose security and privacy risks. Due to the long supply chain and the large number of stakeholders involved, it is important to establish the stakeholders, identify risks during the life cycle, and put forward proposals for resolving security and privacy issues in IoT-domotics. This document provides guidelines to analyse security and privacy risks and identifies controls that should be implemented in IoT-domotics systems.

IoT-domotics have some features that differ from other forms of IoT deployment, such as non-expert users, and ad hoc architecture. This document therefore adapts the general IoT security and privacy principles to IoT-domotics and provides stakeholders with thorough and tailored guidelines for scenarios specific to IoT-domotics.

The target audiences of this document include IoT-domotics service providers, IoT-domotics service developers, and those who supervise or verify security and privacy for IoT-domotics.

The goal of this document is to ensure that security and privacy for IoT-domotics are achieved without requiring end-users to have in-depth IT knowledge. Although this document can be used by interested end-users, they are not the target audience.

Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics

1 Scope

This document provides guidelines to analyse security and privacy risks and identifies controls that can be implemented in Internet of Things (IoT)-domotics systems.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 20924, *Internet of Things (IoT) and digital twin — Vocabulary*

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000, ISO/IEC 29100, ISO/IEC 20924 and the following 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
IoT-domotics
Internet of Things (IoT) system composed of networks, devices, services and users typically used in the domicile or as electronic wearables

Note 1 to entry: Devices are usually available to the consumer through retail purchase.

Note 2 to entry: According to ISO/IEC TR 22417:2017, 6.3, IoT-domotics denotes the private, hence highly customizable indoor area where someone lives, alone or with friends/relatives/roommates. Thus, it includes dedicated infrastructure aimed to support those individuals, such as healthcare and wellness systems, building control systems, smart metering and systems for entertainment and gaming.

3.2
entity
physical or non-physical element, which has a distinct and independent existence

Note 1 to entry: Every entity has a unique identity.

Note 2 to entry: See ISO/IEC 30141:2018, 8.2.1.2.

3.3
domain
major functional group of an Internet of Things (IoT) system

Note 1 to entry: Every *entity* (3.2) in an IoT system participates in one or more domains and is said to be included or contained by that domain.

Note 2 to entry: See ISO/IEC 30141:2018, 8.2.1.3.

4 Abbreviated terms

AI	artificial intelligence
App	application
AR	augmented reality
CRM	customer relationship management
DDoS	distributed denial of service
ICT	information and communication technology
IP	internet protocol
IoT	Internet of Things
NB-IoT	narrow band Internet of Things
PII	personally identifiable information
RF	radio frequency
TV	television
URL	uniform resource locator
USB	universal serial bus
VR	virtual reality

5 Overview

5.1 General

The security and privacy of IoT-domotics have a bearing on the normal operation of in-domicile services, the well-being of residents, and the integrity of infrastructures that are linked directly or indirectly with devices of services. Stakeholders including users, service providers, device manufacturers, network operators and industry supervisors are becoming increasingly concerned by security and privacy issues of IoT-domotics.

In comparison with other IoT solutions, IoT-domotics have specific features and concerns. It is therefore essential to adapt the general IoT security and privacy principles to IoT-domotics and provide stakeholders with thorough and tailored guidelines in specific scenarios of IoT-domotics.

5.2 Features

Some examples of IoT-domotics systems can be found in Annex A. Many of the features of IoT-domotics can affect the security and privacy considerations. These features should be specifically considered in the context of security and privacy. Such features include:

a) open and varied home environments;

   1) terminal devices: devices can be smart devices, lightweight function devices or appliances;

   2) communication protocols: such as ethernet, wireless, and/or bluetooth;

   3) physical input methods: such as voice commands, touch, and/or gestures;

4) varied applications and services: an IoT-domotics solution can provide multiple services simultaneously, like entertainment, electrical appliance control, security system, assistance service and energy management;

5) dynamic network: a device or service can join and leave the environment dynamically and flexibly;

6) complex interactions: interactions can be in multiple forms, such as human-device, device-device, device-service and human-service;

7) multi-party interactions: multiple devices/points of connectivity in domiciles.

b) features related to domiciles;

1) context awareness: as devices and services get smarter, it can be necessary for IoT-domotics to have awareness of social and cultural imperatives in order to be useful for end users. A human can interact with the IoT-domotics device which in turn can share context information with another device or another human;

2) privacy concerns: devices and services are likely to have access to personal data (e.g. location, habits, and/or relationships). Besides, devices and services exchange context information which can contain personal data;

3) relationships:

i) human to device relationships: interactions relying on a variety of information inputs such as images and user presence, as well as identification methods such as speech;

ii) device-to-device relationships: interactions where devices communicate with one another actively (e.g. a thermostat that triggers the lowering of a window shade) or passively (e.g. a device that identifies presence of a user when the user leaves one area of the domicile and enters another).

4) access restrictions: IoT-domotics devices are used in scenarios involving children and can involve the protection of children from accessing the Internet, such as payment business restrictions, content hierarchical access restrictions;

5) biometric protection: IoT-domotics devices can record personal biometric information such as irises, fingerprints, faces and voice. It involves the secure storage, verification and protection of data;

6) operational protection mechanism: IoT-domotics devices can have hierarchical use or interoperability secondary confirmation security protection, such as preventing children from operating washing machines and microwave ovens, as well as protection buttons to prevent pets and children from misoperations.

c) users, inhabitants and other living entities that can be present and/or impacted by the deployment and use of an IoT-domotic solution in a home, such as:

1) by categories: elderly, adults, teenagers, children, babies, people with reduced autonomy, persons with disabilities and pets;

2) by roles: owners, administrators, users, as well as individuals and other living entities, such as pets and plants that can be impacted;

3) by adverse impact: victims of coercive control (e.g. of smart locks or thermostats), or surveillance (e.g. by hidden cameras or microphones).

d) interoperability: this is an important aspect for seamless communication between all devices in an IoT-domotics environment, regardless of their make or model.

e) user-friendly interface and usability: IoT-domotics systems' interfaces should be intuitive and designed to be easy for users to navigate, especially considering that it is possible that not all users are tech-savvy.

5.3 Stakeholders

Stakeholders of IoT-domotics are IoT-domotics service providers, IoT-domotics service developers and IoT-domotics users. These stakeholders are identified in the context of the features of IoT-domotics (see 5.2) in conformance with the stakeholders of IoT systems defined in ISO/IEC 30141. Table 1 shows the stakeholders of IoT-domotics with explanations.

Table 1 — Stakeholders involved in IoT-domotics

Stakeholders	Sub-role	Descriptions
IoT-domotics service provider	Business manager Delivery manager Domicile network/sensor installer System operator	To document the approach to be taken for the risk assessment, and to manage and operate IoT-domotics services and/or to provide network connectivity.
IoT-domotics service developer	Solution architect Solution/application/device developer Developer manager System integrator	To design, implement, test and integrate IoT-domotics services, devices and applications.
IoT-domotics user	Residents in domicile Domicile visitors	End users of IoT-domotics services

The definitions of the roles of IoT-domotics stakeholders are as follows:

a) IoT-domotics service provider

Role definition: to document the approach to be taken for the risk assessment, and to manage and operate IoT-domotics services and/or to provide network connectivity. Since IoT-domotics devices can be physically linked to the domicile, an important sub-role is IoT-domotics installer, who installs the IoT-domotics within the domicile.

b) IoT-domotics service developer

Role definition: to develop, test and integrate IoT-domotics services, devices and applications.

c) IoT-domotics user

Role definition: owners, administrators, users, as well as individuals and other digital and living entities that can use or be impacted by the deployment and use of an IoT-domotic solution in a domicile.

Refer to Annex B for the security and privacy concerns of these stakeholders. Refer to Annex C for the responsibilities of these stakeholders.

5.4 Life cycles

This document describes the IoT-domotics life cycles adapted from the IoT service life cycles in ISO/IEC 27400:2022, 5.5. According to related stakeholders, three different life cycles processes are considered for different stakeholders. Figure 1 shows the IoT-domotics life cycles processes of stakeholders.

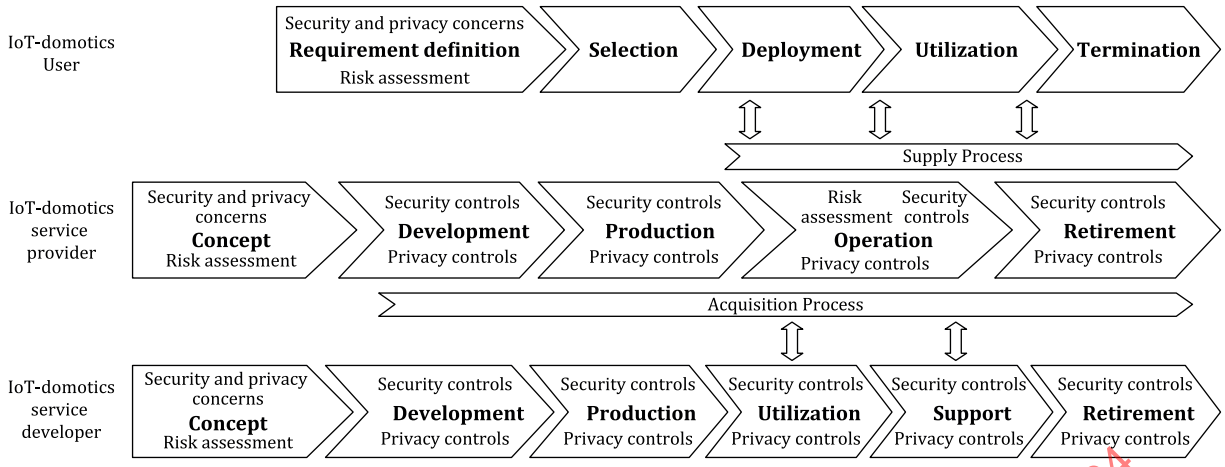

Figure 1 — IoT-domotics life cycles

Life cycles vary depending on each stakeholder. Different stakeholders can be related at different stages in their respective life cycles, especially for service providers. The IoT-domotics service is provided to IoT-domotics users through the supply process of the IoT-domotics service providers. An IoT-domotics service provider acquires an IoT device and software from the IoT-domotics developer in the acquisition process.

When an IoT-domotics user acquires and uses IoT-domotics products or services, life cycles stages include requirement definition, selection, utilization, and termination. In the requirement definition stage, the IoT-domotics user can consider product functional requirements and other aspects, such as security and privacy requirements. Based on the information disclosed in the supply process, an IoT-domotics user selects an IoT-domotics service that meets the required specification. For example, at the termination stage, there are risks of personal data leakage if measures such as account deletion and verification of secure data deletion are not implemented both in the IoT-domotics devices and on the server databases on the back-office side.

For the developer of IoT-domotic services, it is not only about the development, testing and deployment of software, but also about the production and maintenance of devices. In the process of mass production of the IoT-domotic solution (i.e. software and devices), the demonstration of security consistency with the initial requirements should also be taken into account. For example, software and firmware updates are processes that carry their own set of security risks which can arise during the use and support phases, and which should be mitigated.

5.5 Reference model

The reference model in this document is based on the entity-based reference model in ISO/IEC 30141 with instanced objects involving IoT-domotics users and networks as shown in Figure 2. An entity-based representation of IoT-domotics includes physical entities, IoT-domotics users, IoT-domotics devices, IoT-domotics gateway, networks and services for operation and management, applications and services, as well as access and communication.

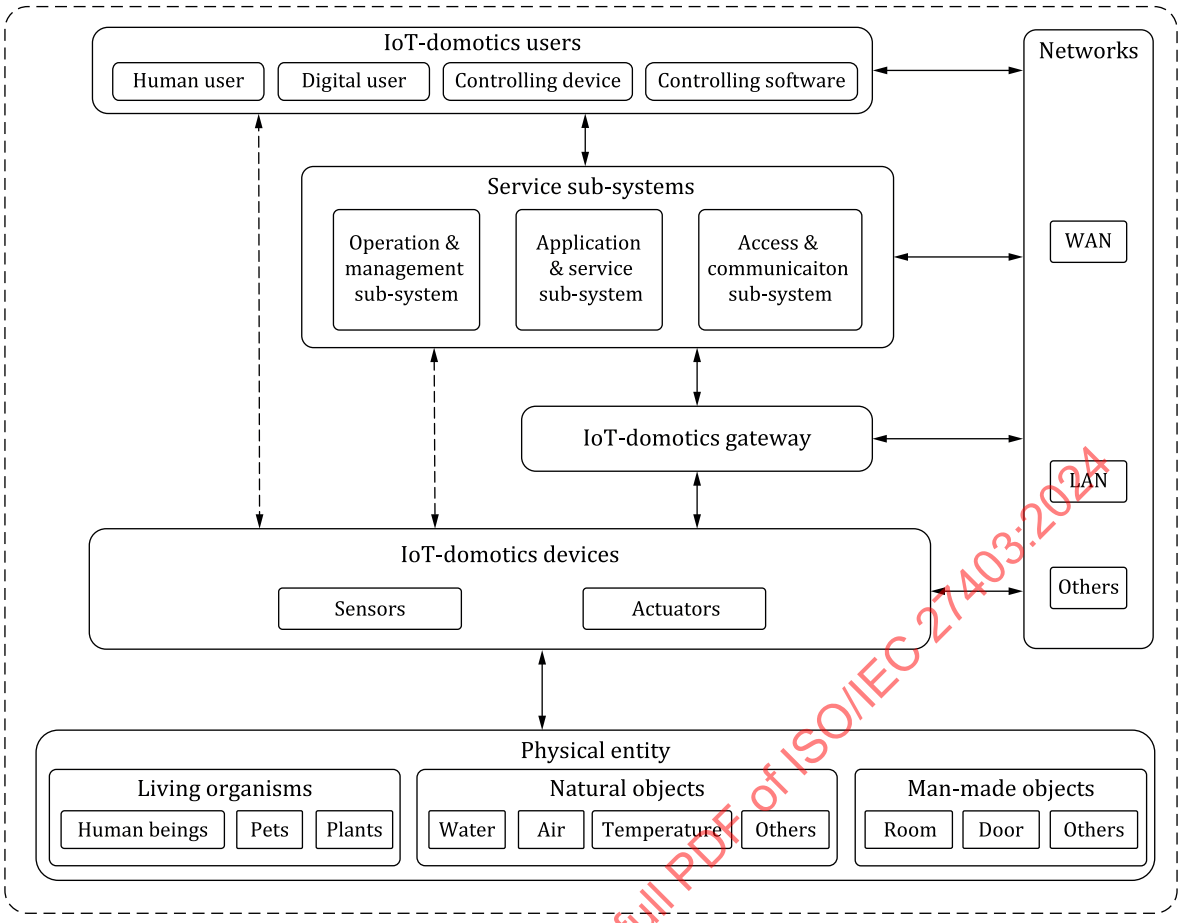

Figure 2 — IoT-domotics reference model

Figure 2 shows the following entities in IoT-domotics:

a) Physical entity

A physical entity is a discrete, identifiable, and observable part of the physical environment. Examples of physical entities are living organisms (e.g. human beings, pets or plants), natural objects (e.g. water, air or temperature) and man-made objects (e.g. a room, a door, or a curtain).

b) IoT-domotics users

IoT-domotics users are subdivided into user types, for example:

1) human user: interacts with IoT-domotics devices and services with the help of controlling devices and controlling software;

2) controlling device: dedicated devices for human users to interact with IoT-domotics devices or to control IoT-domotics devices on behalf of human users;

3) controlling software: software to assist human users to interact with IoT-domotics devices or to control IoT-domotics devices on behalf of human users;

4) digital user: digital user applications can use capabilities of IoT-domotics devices and IoT-domotics services to create higher level services for human users.

c) IoT-domotics devices

IoT-domotics devices (e.g. smart camera, smart TV, smart door lock, or smoking detector) interact with the physical entity and/or act based on IoT-domotics user's command through devices such as sensors and actuators.

d) IoT-domotics gateway

An IoT-domotics gateway forms a connection between local network(s) and the wide area access network.

e) Networks

IoT-domotics systems can be connected by networks. Internet domotics devices are connected or bridged through wide area networks (WAN), such as those controlled via external server-based solutions that are not collocated on the same network or equivalent address space. These devices can be connected through ground-based RF terrestrial (e.g. cellular/microwave) connections, wired networks (e.g. copper/fibre) provided by telecommunication companies, and satellite/stratospheric RF relays. IoT-domotics devices leverage local area networks (LAN) whereby interaction is limited to collocation and can leverage RF range limiting protocols such as Z-Wave or can be attached to an isolated sub-network.

1) local area networks: short range network to connect kinds of IoT-domotics devices with low energy consumption, such as Zigbee®,[1] Bluetooth®,[2] WiFi, 3G/4G/5G;

2) wide area networks: wide range network to connect devices with application and management platforms;

3) others: other IoT-domotics networks, such as personal area network (PAN).

f) Service sub-systems

As in other IoT systems, IoT-domotics services also contain virtual entities, where a virtual entity is a digital representation of a physical entity.

1) operation and management sub-system: provides monitoring, management and administrative capabilities;

2) application and service sub-system: provides IoT-domotics data storage, data analytics and service process management;

3) access and communication sub-system: provides controlled interfaces for service capabilities, for administration capabilities and for business capabilities.

It should be noted that a domain-based reference model is illustrated in ISO/IEC 27400:2022, 5.6. Table 2 shows the correspondence between the entities described this document and domains described in ISO/IEC 27400.

1) Zigbee® is a trademark of Zigbee alliance. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO of the product named.

2) Bluetooth® is a trademark of Bluetooth special interest group. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO of the product named.

Table 2 — Correspondence between entities described in this document and domains described in ISO/IEC 27400

Entities in this document	Domains in ISO/IEC 27400
IoT-domotics user	User domain
Service sub-system	Operations and management domain, application and service domain, and resource access and interchange domain
IoT-domotics gateway	Sensing and controlling domain
IoT-domotics devices	Sensing and controlling domain
Physical entity	Physical entity domain
Networks	Operations and management domain, application and service domain, and resource access and interchange domain

5.6 Security and privacy dimensions

The reference model architecture in Figure 2 is logically composed of IoT-domotics users, service sub-systems, the IoT-domotics gateway, IoT-domotics devices and physical entites, networks and other entities. The security and privacy risks faced by each entity and the control measures taken can be considered from the four dimensions of service, application, network, and hardware. The security and privacy dimensions involved in different entities are shown in Table 3.

Table 3 — IoT-domotics entities and their involved security and privacy dimensions

IoT-domotics entities	Security and privacy dimensions to analyse risks and implement countermeasures			
	Service	Application	Network	Hardware
IoT-domotics users[a]	Optional	Optional	Optional	Optional
Service sub-systems	Present	Optional	Present	Absent
IoT-domotics gateway	Optional	Present	Present	Present
IoT-domotics devices and physical entities	Optional	Present	Present	Present
Networks	Absent	Absent	Present	Optional

NOTE As the form of these entities differ, not all of the four dimensions are present. For example, some do not have a hardware layer. Therefore, some involved security and privacy dimensions are optional or absent.

[a] A human can be an IoT-domotics user, in which case all the layers are absent.

6 Guidelines for risk assessment

6.1 General

This clause provides guidance and information on risk assessment for IoT-domotics. Risk assessment for IoT-domotics systems should be done by using the approaches and methods specified in the following documents:

— ISO 31000, which gives generic guidelines on risk management;

— IEC 31010, which provides guidance on the selection and application of techniques for assessing risk in a wide range of situations;

— ISO/IEC 27005, which gives specific information on security guidelines for risk management.

Where adoption of an information security management system is necessary (in particular, in big organizations or if an IoT-domotics system is part of an ecosystem), the following documents are also relevant:

— ISO/IEC 27001, which provides requirements for information security management systems;

— ISO/IEC 27701, which provides extended requirements for privacy information management.

Furthermore, there are specific risk sources which should be considered for the risk assessment of IoT-domotics systems. The specific risk sources are addressed in the following documents:

— ISO/IEC 24767-1, which gives threat analysis and security requirements for home networks;

— ISO/IEC 27400, which gives general risk sources related to IoT systems;

— ISO/IEC 27402, which gives requirements for IoT device manufacturers to perform risk assessment.

IoT-domotics risk sources are identified in 6.2 and 6.3, which should be considered for the risk assessment. Detailed and specific security risks are provided in 6.2 and detailed and specific privacy risks are provided in 6.3.

6.2 Sources of security risks

6.2.1 Security risks for service sub-systems

6.2.1.1 Service dimension

The following risk sources are relevant to IoT-domotics service sub-systems relating to the service dimension:

NOTE Some of these risk sources have already been addressed in existing documents, which are cited below in parentheses.

— an IoT system, application of service that has no or weak security function, e.g. weak authentication and authorization function or access control (see ISO/IEC 27400:2022, 6.2.2.4);

— documented operation procedure of an IoT system or service with vulnerabilities (see ISO/IEC 27400:2022, 6.2.2.2);

— an IoT system, application or service with vulnerabilities (see ISO/IEC 27400:2022, 6.2.2.3);

— lack of knowledge and skills of persons who play a role in the provision or use of the IoT system, application or service (see ISO/IEC 27400:2022, 6.2.1);

— lack of governance (see ISO/IEC 27400);

— malicious software and configuration (see ISO/IEC 24767-1:2008, 7.3);

— system failures (see ISO/IEC 24767-1:2008, 7.7);

— security service providers (see ISO/IEC 24767-1:2008, 7.8).

The following use cases should be considered for IoT-domotics:

— lack of a security warning mechanism;

  For example, IoT-domotics devices fail to send warning messages to the user to remind them that a security incident can occur.

— lack of access control;

  For example, permissions are the same for every user including children to access social application, voice and live video on IoT-domotics devices, which can include pornographic, violent and political content; advertising; abuse; violation of advertising law and contraband content;

— AI services are abused.

For example, AI technology applied in devices including an intelligent voice speaker and an intelligent door lock lack security design and verification, which can lead to misfunctions that are out of human control.

6.2.1.2 Network dimension

The following risk sources are relevant for IoT-domotics service sub-systems relating to network dimension:

NOTE These risk sources have already been addressed in existing documents, which are cited below in parentheses.

— an IoT system or application of service that has no or weak security function, e.g. weak authentication and authorization function or access control (see ISO/IEC 27400:2022, 6.2.2.4);

— unauthorized access (see ISO/IEC 24767-1:2008, 7.2);

— malicious software and configuration (see ISO/IEC 24767-1:2008, 7.3);

— denial of service (see ISO/IEC 24767-1:2008, 7.4);

— unintended modification of data during communication (see ISO/IEC 24767-1:2008, 7.5).

The following use cases should be considered for IoT-domotics:

— access control flaw;

For example, IoT-domotics users can access the resources owned by other family members without any authorization while using the IoT-domotics devices.

— lack of effective authentication.

For example, almost no such appropriate authentication mechanism has been designed for IoT-domotics devices. Malicious applications installed by the owner of the IoT-domotics devices have access to the platform service without valid authentication. Meanwhile, the platform service also lacks enough capacity to effectively authenticate counterfeit IoT-domotics devices.

6.2.2 Security risks for IoT-domotics gateway

6.2.2.1 Application dimension

The following risk sources are relevant for IoT-domotics gateway relating to application dimension:

NOTE These risk sources have already been addressed in existing documents, which are cited below in parentheses.

— an IoT system, application of service that has no or weak security function, e.g. weak authentication and authorization function or access control (see ISO/IEC 27400:2022, 6.2.2.4);

— human error or of persons who play a role in the provision or use of the IoT system, application or service (see ISO/IEC 27400:2022, 6.2.1);

— an IoT service developer who does not have capabilities to develop a secure IoT application and service (see ISO/IEC 27400:2022, 6.2.2.3);

— an established methodology that is not followed in the development of a system, application or service (see ISO/IEC 27400:2022, 6.2.2.3);

— an IoT system, application or service with vulnerabilities (see ISO/IEC 27400:2022, 6.2.2.3);

— lack of knowledge and skills of persons who play a role in the provision or use of the IoT system, application or service (see ISO/IEC 27400:2022, 6.2.1);

— software and firmware of an IoT device or an IoT gateway with technical vulnerabilities (see ISO/IEC 27400:2022, 6.2.2.1);

— software and firmware of an IoT device or an IoT gateway that has no or an insecure updating mechanism (see ISO/IEC 27400:2022, 6.2.2.1);

— malicious software and configuration (see ISO/IEC 24767-1:2008, 7.3);

— system failures (see ISO/IEC 24767-1:2008, 7.7);

— user errors (see ISO/IEC 24767-1:2008, 7.6).

The following use cases should be considered for IoT-domotics:

— lack of appropriate security management mechanism for IoT-domotics devices on the grounds of their complexity and diversity;

  For example, there are no capabilities of monitoring, abnormal warning and port threat shielding for the operating status of IoT-domotics devices connected to the IoT-domotics gateway. Network isolation and access control mechanism for connected IoT-domotics devices have not been fully carried out yet.

— insecure firmware.

  For example, the firmware has security vulnerabilities, such as WiFi vulnerabilities, weak password vulnerabilities, buffer overflow vulnerabilities, cross-site request forgery (CSRF) vulnerabilities, and/or remote code execution vulnerabilities. Sensitive firmware configuration data, such as administration account, hard-coded passwords, database connection passwords, and/or encryption keys, can get leaked when they are stored in plain text. The integrity and authenticity of the firmware installation package are not verified during the upgrading.

6.2.2.2 Network dimension

The following risk sources are relevant for IoT-domotics gateway relating to network dimension:

NOTE These risk sources have already been addressed in existing documents, which are cited below in parentheses.

— an IoT device or an IoT gateway that has no or a weak security function, e.g. weak authentication function, encryption, and redundancy (see ISO/IEC 27400:2022, 6.2.2.1);

— denial of service (see ISO/IEC 24767-1:2008, 7.4);

— unintended modification of data during communication (see ISO/IEC 24767-1:2008, 7.5);

— malicious software and configuration (see ISO/IEC 24767-1:2008, 7.3);

— unauthorized access (see ISO/IEC 24767-1:2008, 7.2).

The following use cases should be considered for IoT-domotics:

— IoT-domotics intranet lacks effective protection from external threats.

  For example, it lacks the IP address hiding functions to avoid IP address leakage and the secure connection functions. In addition, the support for protection and disposal capabilities for DDoS attack source traffic, detection, warning and interception capabilities for malicious URL/IP and zombie worm files are not available.

6.2.2.3 Hardware dimension

The following risk sources are relevant for IoT-domotics gateway relating to hardware dimension:

NOTE These risk sources have already been addressed in existing documents, which are cited below in parentheses.

— existence of external systems and devices that can be abused in generating attacks on the IoT system, application or service (see ISO/IEC 27400:2022, 6.2.1);

— an IoT system, application or service that has vulnerabilities (see ISO/IEC 27400:2022, 6.2.2.3);

— an IoT device or an IoT gateway is located at a site not protected by a physically secure facility (see ISO/IEC 27400:2022, 6.2.2.1);

— an IoT device or an IoT gateway that operates under influence of weather and other environmental conditions (see ISO/IEC 27400:2022, 6.2.2.1);

— an IoT device or an IoT gateway that is produced through the ICT supply chain (see ISO/IEC 27400:2022, 6.2.2.1).

The following use cases should be considered for IoT-domotics:

— insecure chips with meltdown and vulnerabilities;

— physical intrusion of hardware interface such as console interface, serial port, and debugging interface;

— lack of hardware protection mechanism;

  For example, the owner of the devices, who can be an attacker, can easily export the firmware for analysis if the according devices are not protected by hardware.

— exposure of chip information, including chip model and chip interface on a printed circuit board;

— lack of hardware anti-tampering and anti-reverse protection mechanisms.

  For example, tamper detection switches, sensors or circuits are rarely considered into devices design.

6.2.3 Security risks for IoT-domotics devices and physical entities

6.2.3.1 Application dimension

The risk sources mentioned in 6.2.2.1 also exist in IoT-domotics devices and physical entities. In addition, the following use cases should be considered for IoT-domotics:

— intelligent speech speakers, microphones, voice remote controls, intelligent service robots and other devices with speech modules that have speech recognition risks;

  For example, the voice device can receive the voice frequency which the human cannot hear, and the attacker can control the IoT-domotics device by synthesizing the voice according to the frequency.

— intelligent voice speakers, intelligent door locks, intelligent electrical appliances, intelligent service robots and other devices with AI modules that have security risks, such as unsecure algorithm models, unsecure infrastructure, lack of written human ethics and laws;

— lack of fault tolerance mechanism.

  For example, the gas stove cannot enter the default safety mode of shutting off the gas and the fire when the power or the network is cut off, or under attack. IoT-domotics devices fail to effectively recognize user instructions, resulting in unexpected abnormal activation or unsafe operation. The intelligent door lock automatically unlocks when the power is off or the network is disconnected. The intruder causes the camera network connection to drop, resulting in the camera being unable to store video to the cloud, and the security function fails.

6.2.3.2 Network dimension

The risk sources mentioned in 6.2.2.2 also exist in IoT-domotics devices and physical entities.

6.2.3.3 Hardware dimension

The risk sources mentioned in 6.2.2.3 also exist in IoT-domotics devices and physical entities, and should therefore be considered.

The following use cases should be considered for IoT-domotics:

— devices with cameras, such as smart TVs and computers, which lack physical buttons to turn them off and physically hide them when not in use.

6.2.4 Security risks for networks

The following risk sources are relevant for networks relating to network dimension:

NOTE These risk sources have already been addressed in existing documents, which are cited below in parentheses.

— vulnerability of the IoT system, application or service (see ISO/IEC 27400:2022, 6.2.1);

— an IoT device or an IoT gateway that operates under influence of weather and other environmental conditions (see ISO/IEC 27400:2022, 6.2.2.1);

— an IoT system or application of service that has no or weak security function, e.g. weak authentication and authorization function or access control (see ISO/IEC 27400:2022, 6.2.2.4);

— denial of service (see ISO/IEC 24767-1:2008, 7.4);

— unintended modification of data during communication (see ISO/IEC 24767-1:2008, 7.5).

The security risk of the network dimension should consider the analysis of the traffic relationship among service sub-systems, IoT-domotics gateway, IoT-domotics devices and physical entities.

The following use cases should be considered for IoT-domotics:

— the network protocol crash;

  For example, an attacker can easily analyse the user login process of an IoT-domotics device, crack the business logic relationship between the user account and the IoT-domotics device, and finally modify the device ID to control other users' devices beyond authority.

— replay attack;

— network protocol without encryption algorithm.

6.3 Sources of privacy risks

6.3.1 Privacy risks for service sub-systems

6.3.1.1 Service dimension

The following risk sources are relevant for IoT-domotics service sub-systems relating to service dimension:

NOTE These risk sources have already been addressed in existing documents, which are cited below in parentheses.

— lack of governance (see ISO/IEC 27400);

— risk sources in the usage phase (see ISO/IEC 27400);

— risk sources in the CRM phase (see ISO/IEC 27400);

— PII principals who suffer from privacy breaches (see ISO/IEC 27400).

The following use cases should be considered for IoT-domotics:

— lack of privacy protection for children;

For example, before collecting children's PII, the devices ask no verifiable consent from a parent or guardian. Meanwhile, the privacy protection is also not mentioned and revoked by children. As a result, there are no protective measures provided to help children and their parents to restrict the sharing of children's PII.

— AI service data and models involve privacy abuse. AI systems use a large amount of PII to train the machine learning models for high accuracy and high generalization performance;

— lack of privacy classification mechanism;

For example, IoT-domotics users live together in the same living environment, sharing and using IoT-domotics devices and services in almost the same way of life, which makes privacy reserving among users within domiciles very complex. Privacy should be classified to prevent it from being acquired or abused by co-habitants.

— there is no limitation on the scope and purpose of the use of PII;

For example, fragmented data uploaded by sensors deployed in IoT-domotics is used to analyse the relationships, health status, and activities of the IoT-domotics users within domiciles.

— lack of protection for sensitive data.

For example, VR and AR biometric tracking data (e.g. motion data of the head, torso, hands and eyes) can diagnose or predict mental illnesses and other health conditions.

6.3.1.2 Network dimension

The following risk sources are relevant for IoT-domotics service sub-systems relating to network dimension:

NOTE These risk sources have already been addressed in existing documents, which are cited below in parentheses.

— PII principals who suffer from privacy breaches (see ISO/IEC 27400);

— risk sources in the usage phase (see ISO/IEC 27400).

The following use cases should be considered for IoT-domotics:

— lack of access control or weak access control;

For example, in the IoT-domotics scenario, different IoT-domotics users usually share the same device in the same living environment. The accounts bound to these devices and the private information records associated with the accounts can be at risk of infringement.

— no authorization or accurate authorization for unlicensed users.

For example, in the IoT-domotics scenario, the service ordered by an IoT-domotics user will be used by other users who are able to collect PII by default without any permission.

6.3.2 Privacy risks for IoT-domotics gateway

6.3.2.1 Application dimension

The following risk sources are relevant for IoT-domotics gateway relating to application dimension:

NOTE These risk sources have already been addressed in existing documents, which are cited below in parentheses.

— risk sources in the usage phase (see ISO/IEC 27400);

— risk sources in the CRM phase (see ISO/IEC 27400);

— PII principals who suffer from privacy breaches (see ISO/IEC 27400).

The following use cases should be considered for IoT-domotics:

— lack of understanding and access to privacy policies;

For example, the IoT-domotics gateway lacks the application interface for the IoT-domotics user to obtain the privacy policy, resulting in the user not having a good grasp of the policy information.

— almost no adoption of the minimum principle for PII collection;

— the PII local storage without encryption;

For example, the account password is stored in plain text.

— no remote PII destruction mechanism is provided.

6.3.2.2 Network dimension

The following risk sources are relevant for IoT-domotics gateway relating to network dimension:

NOTE These risk sources have already been addressed in existing documents, which are cited below in parentheses.

— risk sources in the usage phase (see ISO/IEC 27400);

— PII principals who suffer from privacy breaches (see ISO/IEC 27400).

The following use cases should be considered for IoT-domotics:

— missing or insufficient access control mechanism;

For example, no restrictions are set for third-party applications installed in the devices to access PII. Lack of access control and authentication mechanism for the USB peripheral interface of the IoT-domotics gateway causes the application to have unrestricted access to the network attached storage.

— PII without encrypted storage and transmission.

6.3.2.3 Hardware dimension

The following risk sources are relevant for IoT-domotics gateway relating to hardware dimension:

NOTE These risk sources have already been addressed in existing documents, which are cited below in parentheses.

— risk sources in the usage phase (see ISO/IEC 27400);

— PII principals who suffer from privacy breaches (see ISO/IEC 27400).

The following use cases should be considered for IoT-domotics:

— The chip's external hardware interfaces such as Joint Test Action Group, Serial Wire Debug, and Universal Asynchronous Receiver/Transmitter, are opened by default and can be easily cracked by attackers to extract PII.

6.3.3 Privacy risks for IoT-domotics devices and physical entitles

6.3.3.1 Application dimension

The risk sources mentioned in 6.3.2.1 also exist in IoT-domotics devices and physical entities. In addition, the following use cases should be considered for IoT-domotics:

— devices with password input modules such as smart door locks and keyboards that have no or weak privacy protection functions;

For example, the password input process lacks anti-peeping protection mechanism. The buttons do not have the function of preventing the residual fingerprint from being extracted and copied. The button prompt sound or vibration feedback also reveals sensitive information.

— the processes like collection, storage, use, sharing, and disclosure of PII lack user authorization;

For example, smart TVs, cameras, voice speakers, microphones and other devices and applications have default monitoring and collection permission of PII in the background.

— biometric recognition modules that have no or weak privacy protection function;

For example, the protection of biometric modal information lacks clear standards, which results in data over-collection and abuse. Data based on biometric sensors, motion sensors, environmental sensors, and location sensors lacks permission management, so application can call part of the sensor data at will, which eventually leads to privacy data leakage. The application did not delete the original biometric information after the completion of the biometric authentication process.

— location privacy leakage.

For example, IoT-domotics devices and clothing are pre-embedded with radio frequency identification (RFID) electronic tags. Once they are scanned, located, or tracked uncontrollably, the infringement of personal privacy can occur.

6.3.3.2 Network dimension

The risk sources mentioned in 6.3.2.2 also exist in IoT-domotics devices and physical entities, and should therefore be considered.

6.3.3.3 Hardware dimension

The risk sources mentioned in 6.3.2.3 also exist in IoT-domotics devices and physical entities. In addition, the following risk sources to IoT-domotics should be considered:

— when a trusted execution environment or special security chip is not used;

For example, the collection, feature extraction, and feature comparison of biometric images such as faces, fingerprints, and/or iris are not performed in the security chip environment.

— when there are no hardware control privacy mechanisms, such as mechanisms to turn off the built-in microphone and camera of the IoT-domotics device;

— cameras, voice speakers, microphones and other devices that lack working status prompt options, such as indicator lights.

6.3.4 Privacy risks for networks

The following risk sources are relevant for networks relating to network dimension:

NOTE These risk sources have already been addressed in existing documents, which are cited below in parentheses.

— risk sources in the usage phase (see ISO/IEC 27400);

— risk sources in the CRM phase (see ISO/IEC 27400);

— PII principals suffer from privacy breaches (see ISO/IEC 27400).

The following use cases should be considered for IoT-domotics:

— network eavesdropping and traffic analysis.

For example, there is continuous sensor traffic which transmits family information regardless of whether the user is at home, or whether the switch is on or not. The attacker can access the original location data by locating the transmission device and eavesdropping on the location information transmission channel to obtain the personal privacy information by calculation and reasoning.

7 Security and privacy controls

7.1 Principles

7.1.1 General

Referring to ISO/IEC 24767-1, ISO/IEC 27400, ISO/IEC 27402 and the domotics characteristics analysed in this document, the following principles described in 7.1.2 to 7.1.7 are important for IoT-domotics controls.

7.1.2 Different levels of security for different services

There are natural physical boundaries between the domotics environment and outside environment, and the security requirements are often different inside and outside the physical boundaries. For example, controlling an air conditioner inside the domicile does not require the same level of security as controlling a home device from outside. At the same time, there are a variety of services for domotics, and users often have different security needs for different services. See Annex D for additional information.

7.1.3 Easy security settings for users

The security settings of devices and services in the domotics environment should be user-friendly and instructions should be written in clear and unambiguous language. Complicated and expensive solutions would hinder the application of security measures. Security solutions featured which are cheaper, less complex and easier to implement for IoT-domotics are more acceptable from the user's point of view.

7.1.4 Failsafe domotics devices

In case of a failure, domotics devices should be set in a state that cannot cause harm to the inhabitants or the building. A failing system should not block the use of other devices.

7.1.5 Restricted access to content services

Depending on whether the accessed content is suitable for children, different levels of permissions of the delivered content should be set.

7.1.6 Consideration for children

The independence of children's privacy should be fully respected. The consent or authorization of the child's guardian should be gained before PII for or data from a child is processed, and before services are offered to children.

7.1.7 Scenario-specific privacy preferences

Depending on whether the service is applied only with inhabitants in a domotics environment, the intensity of privacy protection is often different. For example, it is acceptable for services to share certain private

information such as location, age, and/or marital status among family members; however, this information should not be leaked outside that scope.

7.2 Security controls

7.2.1 Policy for IoT-domotics security

The control, purpose, audience and guidance stated in ISO/IEC 27400:2022, 7.1.2.1 and the following additional guidance apply.

Additional implementation guidance for IoT-domotics is:

— security policies should be fully considered and clearly communicated to stakeholders. Such security policies include restricted access to content services, AI security management, children protection, biometric protection, smart device fault-tolerant protection, easy security settings for users, and network security protection inside and outside the domotics environment.

The related IoT-domotics entity is a service sub-system.

7.2.2 Organization of IoT-domotics security

The control, purpose, audience and guidance stated in ISO/IEC 27400:2022, 7.1.2.2 applies.

The related IoT-domotics entity is a service sub-system.

7.2.3 Asset management

The control, purpose, audience and guidance stated in ISO/IEC 27400:2022, 7.1.2.3 and the following additional guidance apply.

Additional implementation guidance for IoT-domotics is:

— it is recommended to identify the type, number, firmware version, vulnerability information, IP address, and port of the IoT-domotics device directly connected to the public network without going through the IoT-domotics gateway.

The related IoT-domotics entities are service sub-systems, IoT-domotics gateways, IoT-domotics devices or physical entities.

7.2.4 Equipment and assets located outside physical secured areas

The control, purpose, audience and guidance stated in ISO/IEC 27400:2022, 7.1.2.4 and the following additional guidance apply.

Additional implementation guidance for IoT-domotics is:

— anti-theft and anti-intrusion functions for IoT-domotics devices should be designed and implemented;

— capabilities for devices to resist malicious attacks (e.g. energy consumption attacks) and prevent functional failure should be designed and implemented.

The related IoT-domotics entity is a service sub-system.

7.2.5 Secure disposal or re-use of equipment

The control, purpose, audience and guidance stated in ISO/IEC 27400:2022, 7.1.2.5 and the following additional guidance apply.

Additional implementation guidance for IoT-domotics is:

— IoT-domotics users should be provided with the function of deleting or anonymizing the data stored in the IoT-domotics device or server when the IoT-domotics device has been used, lost or sold.

The related IoT-domotics entity is a service sub-system.

7.2.6 Learning from security incidents

The control, purpose, audience and guidance stated in ISO/IEC 27400:2022, 7.1.2.6 and the following additional guidance apply.

Additional implementation guidance for IoT-domotics is:

— In the cases where the deployment of IoT-domotics involves user participation, the IoT-domotics service provider should:

  — convey information security knowledge to IoT-domotics users through easy and understandable ways;

  — use security incident cases to strengthen IoT-domotics users' security awareness;

  — provide guidance on IoT-domotics devices security.

The related IoT-domotics entities are service sub-systems, IoT-domotics gateways, IoT-domotics devices, physical entities or networks.

7.2.7 Secure IoT-domotics system engineering principles

The control, purpose, audience and guidance stated in ISO/IEC 27400:2022, 7.1.2.7 and the following additional guidance apply.

Additional implementation guidance for IoT-domotics is:

— the IoT-domotics service developer should provide different security levels of protection based on different IoT-domotics services and device (see Table D.1). It should be ensured that the default settings meet the security baseline.

The related IoT-domotics entities are service sub-systems, IoT-domotics gateways, IoT-domotics devices, physical entities or networks.

7.2.8 Secure development environment and procedures

The control, purpose, audience and guidance stated in ISO/IEC 27400:2022, 7.1.2.8 and the following additional guidance apply.

Additional implementation guidance for IoT-domotics is:

— IoT-domotics service developers should consider the following procedures in the design and implementation process, including:

  — applying proper security by designing methods for continuous improvement;

  — sharing best security practices;

  — designing and implementing hierarchical security measures for applications to prevent personal safety issues caused by application security issues;

  — using the appropriate security measures based on the resources and performance of different types of devices.

The related IoT-domotics entities are service sub-systems, IoT-domotics gateways, IoT-domotics devices or physical entities.

7.2.9 Security of IoT-domotics systems in support of safety

The control, purpose, audience and guidance stated in ISO/IEC 27400:2022, 7.1.2.9 applies.

The related IoT-domotics entities are service sub-systems, IoT-domotics gateways, IoT-domotics devices or physical entities.

7.2.10 Security in connecting varied IoT-domotics devices

The control, purpose, audience and guidance stated in ISO/IEC 27400:2022, 7.1.2.10 and the following additional guidance apply.

Additional implementation guidance for IoT-domotics is:

— the IoT-domotics system should analyse the behaviour of the connected IoT-domotics devices, mark and grade the abnormal devices, and remind the IoT-domotics user to check or replace them when necessary.

The related IoT-domotics entities are service sub-systems, IoT-domotics gateways, IoT-domotics devices or physical entities.

7.2.11 Verification of IoT-domotics devices and systems design

The control, purpose, audience and guidance stated in ISO/IEC 27400:2022, 7.1.2.11 applies.

The related IoT-domotics entities are service sub-systems, IoT-domotics gateways, IoT-domotics devices or physical entities.

7.2.12 Monitoring and logging

The control, purpose, audience and guidance stated in ISO/IEC 27400:2022, 7.1.2.12 and the following additional guidance apply.

Additional implementation guidance for IoT-domotics is:

— the IoT-domotics service provider should build different traffic models for different IoT-domotics devices to target attacks precisely. Traffic models for different IoT-domotics devices, e.g. web cameras, network TVs and home security devices, can be different in controlling signals, protocols, traffic volumes and dependencies on time of the day.

The related IoT-domotics entities are service sub-systems, IoT-domotics gateways, IoT-domotics devices or physical entities.

7.2.13 Protection of logs

The control, purpose, audience and guidance stated in ISO/IEC 27400:2022, 7.1.2.13 applies.

The related IoT-domotics entity is a service sub-system.

7.2.14 Use of suitable networks for the IoT-domotics systems

The control, purpose, audience and guidance stated in ISO/IEC 27400, 7.1.2.14 applies.

The related IoT-domotics entities are service sub-systems, IoT-domotics gateways, IoT-domotics devices, physical entities or networks.

7.2.15 Secure settings and configurations in delivery of IoT-domotics devices and services

The control, purpose, audience and guidance stated in ISO/IEC 27400:2022, 7.1.2.15 and the following additional guidance apply.

Additional implementation guidance for IoT-domotics is:

— for content related services, the IoT-domotics service provider and IoT-domotics service developer should provide settings for content classification and access control to prevent children from reaching inappropriate information.

The related IoT-domotics entities are service sub-systems, IoT-domotics gateways, IoT-domotics devices or physical entities.

7.2.16 User and device authentication

The control, purpose, audience and guidance stated in ISO/IEC 27400:2022, 7.1.2.16 and the following additional guidance apply.

Additional implementation guidance for IoT-domotics is:

— user authentications should be performed based on different roles and the according role permissions such as family members and visitors;

— content-based devices and systems should restrict access by using identity authentication mechanisms.

The related IoT-domotics entities are service sub-systems, IoT-domotics gateways, IoT-domotics devices, physical entities or networks.

7.2.17 Provision of software and firmware updates

The control, purpose, audience and guidance stated in ISO/IEC 27400:2022, 7.1.2.17 and the following additional guidance apply.

Additional implementation guidance for IoT-domotics is:

— as the owner of the IoT-domotics device, users should be notified about the firmware and software update preparation of the IoT-domotics device to determine whether or not to authorize the operation.

The related IoT-domotics entities are service sub-systems, IoT-domotics gateways, IoT-domotics devices or physical entities.

7.2.18 Sharing vulnerability information

The control, purpose, audience and guidance stated in ISO/IEC 27400:2022, 7.1.2.18 applies.

The related IoT-domotics entities are service sub-systems, IoT-domotics gateways, IoT-domotics devices, physical entities or networks.

7.2.19 Security measures adapted to the life cycle of IoT-domotics system and services

The control, purpose, audience and guidance stated in ISO/IEC 27400:2022, 7.1.2.19 and the following additional guidance apply.

Additional implementation guidance for IoT-domotics is:

— vulnerabilities such as device vulnerabilities and wireless network protocol vulnerabilities should be identified and updated regularly to ensure applicability and effectiveness.

The related IoT-domotics entity is a service sub-system.

7.2.20 Guidance for IoT-domotics users on the proper use of IoT-domotics devices and services

The control, purpose, audience and guidance stated in ISO/IEC 27400:2022, 7.1.2.20 and the following additional guidance apply.

Additional implementation guidance for IoT-domotics is:

— devices and systems that provide AI services should have a specific, clear and reasonable purpose. They should not expand their use or change their function and service purpose without the authorization of the IoT-domotics user.

The related IoT-domotics entities are service sub-systems, IoT-domotics gateways, IoT-domotics devices or physical entities.

7.2.21 Determination of security roles for stakeholders

The control, purpose, audience and guidance stated in ISO/IEC 27400:2022, 7.1.2.21 and the following additional guidance apply.

Additional implementation guidance for IoT-domotics is:

— the IoT-domotics service provider should set up emergency response security team to deal with users' online requests.

The related IoT-domotics entity is a service sub-system.

7.2.22 Management of vulnerable devices

The control, purpose, audience and guidance stated in ISO/IEC 27400:2022, 7.1.2.22 applies.

The related IoT-domotics entities are service sub-systems, IoT-domotics gateways, IoT-domotics devices or physical entities.

7.2.23 Management of supplier relationships in IoT-domotics security

The control, purpose, audience and guidance stated in ISO/IEC 27400:2022, 7.1.2.23 applies.

The related IoT-domotics entities are service sub-systems, IoT-domotics gateways, IoT-domotics devices or physical entities.

7.2.24 Secure disclosure of Information regarding security of IoT-domotics devices

The control, purpose, audience and guidance stated in ISO/IEC 27400:2022, 7.1.2.24 applies.

The related IoT-domotics entity is a service sub-system.

7.3 Privacy controls

7.3.1 Prevention of privacy invasive events

The control, purpose, audience and guidance stated in ISO/IEC 27400:2022, 7.2.2.1 applies.

The related IoT-domotics entities are service sub-systems, IoT-domotics gateways, IoT-domotics devices or physical entities.

7.3.2 IoT-domotics privacy by default

The control, purpose, audience and guidance stated in ISO/IEC 27400:2022, 7.2.2.2 and the following additional guidance apply.

Additional implementation guidance for IoT-domotics is:

— personal privacy and shared privacy within the IoT-domotics are not allowed to spread outside the IoT-domotics systems without authorization;

— the privacy of children should be protected.

The related IoT-domotics entities are service sub-systems, IoT-domotics gateways, IoT-domotics devices or physical entities.

7.3.3 Provision of privacy notice

The control, purpose, audience and guidance stated in ISO/IEC 27400:2022, 7.2.2.3 and the following additional guidance apply.

Additional implementation guidance for IoT-domotics is:

— the IoT-domotics service provider should state the scope of personal information collection and usage;

— the collection and use of personal information by an application on a shared device should be notified to every IoT-domotics user who is using the shared device;

— the collection of children's PII should obtain verifiable authorization from the children's guardian.

The related IoT-domotics entities are service sub-systems, IoT-domotics gateways, IoT-domotics devices or physical entities.

7.3.4 Verification of IoT-domotics functionality

The control, purpose, audience and guidance stated in ISO/IEC 27400:2022, 7.2.2.4 and the following additional guidance apply.

Additional implementation guidance for IoT-domotics is:

— transparency enhancement in the whole process of the data life cycle should be provided to ensure privacy protection throughout the whole life cycle of the device and service.

The related IoT-domotics entities are service sub-systems, IoT-domotics gateways, IoT-domotics devices or physical entities.

7.3.5 Consideration of IoT-domotics users

The control, purpose, audience and guidance stated in ISO/IEC 27400:2022, 7.2.2.5 and the following additional guidance apply.

Additional implementation guidance for IoT-domotics is:

— as children can lack the ability to distinguish the provision of PII from general information, the collection, storage, use, transfer and disclosure of children's PII should be given special attention and consideration.

The related IoT-domotics entities are service sub-systems, IoT-domotics gateways, IoT-domotics devices or physical entities.

7.3.6 Management of IoT-domotics privacy controls

The control, purpose, audience, and guidance stated in ISO/IEC 27400:2022, 7.2.2.6 and the following additional guidance apply.

Additional implementation guidance for IoT-domotics is:

— evaluation of the scope of privacy should be taken at a planned interval as new technologies and applications emerge. For example, VR and AR biometric tracking data, including micro movements of the head, torso, hands, and eyes, should also be treated as data that possibly generate PII which should be managed and protected.

The related IoT-domotics entities are service sub-systems, IoT-domotics gateways, IoT-domotics devices or physical entities.

7.3.7 Unique device identity

The control, purpose, audience, and guidance stated in ISO/IEC 27400:2022, 7.2.2.7 applies.

The related IoT-domotics entities are service sub-systems, IoT-domotics gateways, IoT-domotics devices or physical entities.

7.3.8 Fail-safe authentication

The control, purpose, audience and guidance stated in ISO/IEC 27400:2022, 7.2.2.8 applies.

The related IoT-domotics entities are service sub-systems, IoT-domotics gateways, IoT-domotics devices or physical entities.

7.3.9 Minimization of indirect data collection

The control, purpose, audience and guidance stated in ISO/IEC 27400:2022, 7.2.2.9 applies.

The related IoT-domotics entities are service sub-systems, IoT-domotics gateways, IoT-domotics devices, physical entities or networks.

7.3.10 Communication of privacy preferences

The control, purpose, audience and guidance stated in ISO/IEC 27400:2022, 7.2.2.10 and the following additional guidance apply.

Additional implementation guidance for IoT-domotics is:

— privacy control templates should be provided for users to set scenario-specific preferences in an easy way.

The related IoT-domotics entities are service sub-systems, IoT-domotics gateways, IoT-domotics devices or physical entities.

7.3.11 Verification of automated decision

The control, purpose, audience and guidance stated in ISO/IEC 27400:2022, 7.2.2.11 and the following additional guidance apply.

Additional implementation guidance for IoT-domotics is:

— verifications should be carried out to ensure that user decisions are prioritized to automated decisions in all cases. Besides, the IoT-domotics service provider should verify the robustness of automated decisions in case of unexpected data and a deficient algorithm model.

The related IoT-domotics entity is a service sub-system.

7.3.12 Accountability for stakeholders

The control, purpose, audience, and guidance stated in ISO/IEC 27400:2022, 7.2.2.12 and the following additional guidance apply.

Additional implementation guidance on the management of stakeholders in IoT-domotics life cycle can be found in Annex C.

The related IoT-domotics entity is a service sub-system.

7.3.13 Unlinkability of PII

The control, purpose, audience and guidance stated in ISO/IEC 27400:2022, 7.2.2.13 applies.

The related IoT-domotics entities are service sub-systems, IoT-domotics gateways, IoT-domotics devices or physical entities.

7.3.14 Sharing information on PII protection measures of IoT-domotics devices

The control, purpose, audience, and guidance stated in ISO/IEC 27400:2022, 7.2.2.14 applies.

The related IoT-domotics entities are service sub-systems, IoT-domotics gateways, IoT-domotics devices or physical entities.

Annex A
(informative)

Use cases of IoT-domotics

A.1 Use case 1: entertainment

In this case, the entertainment IoT-domotics devices are interconnected by the internal data interaction. The IoT-domotics accessories, transiting the user real-time data, and devices, controlled by the servers, make an IoT entertainment through WiFi and the Internet. The main application platform saves these records to support a better communication between users and entertainment service provider. Figure A.1 shows the entertainment case of IoT-domotics.

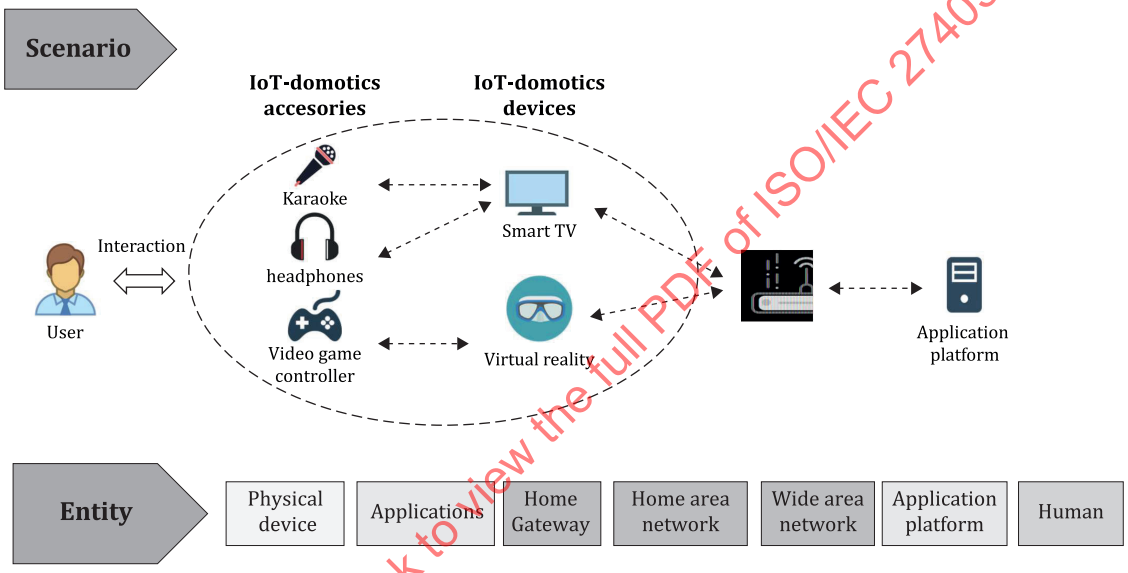

Figure A.1 — Entertainment scene

Risk examples for this use case include: intercepting user request data by intruding an IoT-domotics entertainment system, and then stealing a user entertainment account which causes property loss. Wearable devices such as glasses, watches and wristbands should be connected to the Internet when they are used. The hacker attacks the transmitted data, operating platform, or network through the wearable device, which results in the risk of privacy leakage, user data theft, platform instruction tampering etc.

Recommendations for this use case are:

— users should keep frequent firmware upgrades, not connect to WiFi networks from unknown sources and not click on unfamiliar links;

— users should download applications from reliable sources, and periodically check applications for unauthorized access to personal data.

A.2 Use case 2: electrical appliance control

In this case, the cloud platform connects the user app and physical devices to control electronic devices such as lights, fans and electrical appliances. The diverse sensors are used to monitor the integrated devices. Home network and gateway technology have been used for communication between the system and the user. To bring it a little bit closer to home, users submit their own control of the lamp through an app installed on

mobile phone, then the app submits the user's needs to the service platform by wide area network. Then the service platform sends commands to the lamp to complete the control of lamp by home gateway. Figure A.2 shows the electrical appliance control case of IoT-domotics.

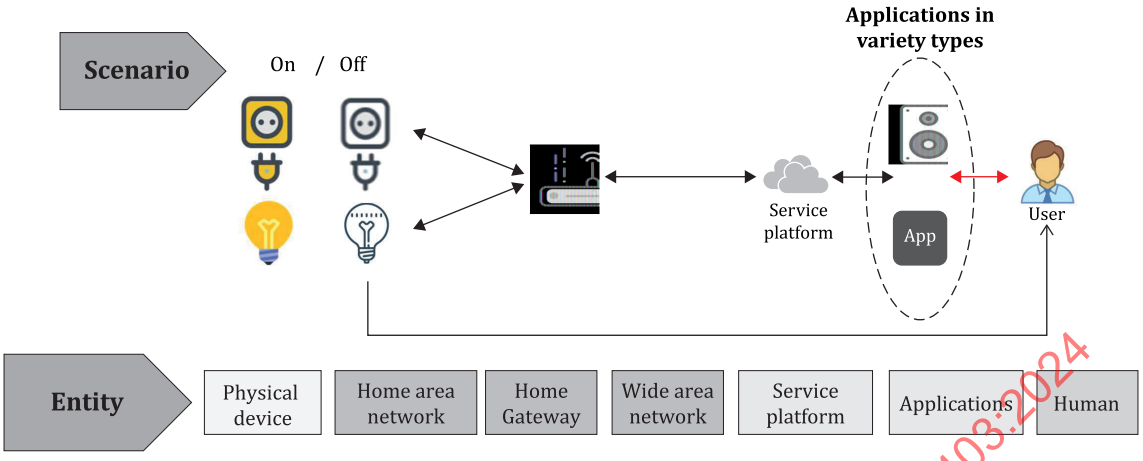

Figure A.2 — Electrical appliance control scene

Risk examples for this use case include: eavesdropping the app control request signalling with illegal means and controlling the switch of the home smart socket.

Recommendations for this use case are:

— the service provider and developer should implement an encrypted channel to encrypt various service control commands and verify the validity of the operation session.

A.3 Use case 3: monitoring and security system

Monitoring and security systems are designed to protect user home from theft, fire and other potential threats related to user property. For a general security level, risks such as abnormal ambient temperature, abnormal door lock status, and/or theft, can be converted into a signal by the sensor of the device and sent to the user's app. For a higher security level, this device is expected to detect the gases emitted due to leakage. This leakage is interpreted as a signal and interfaced with the control system so that the process is automatically shut down. A highly compatible based app is used to provide a suitable interface between the user and the IoT-domestics automation system. Figure A.3 shows the monitoring and security system case of IoT-domotics.

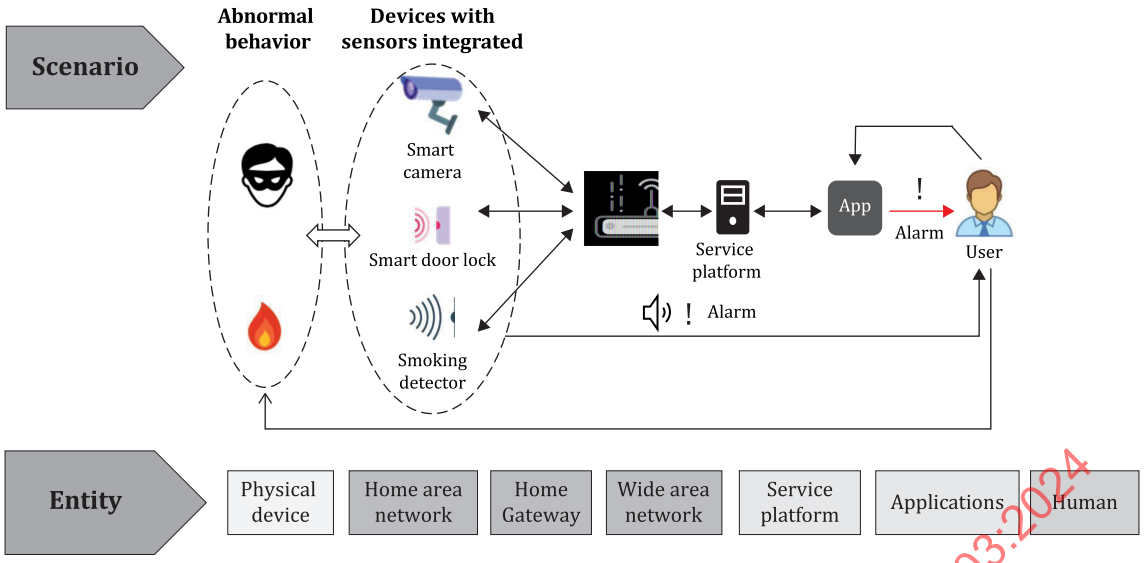

Figure A.3 — IoT-domestics security system scene

Risk examples for this use case include: invading the IoT-domestics security system and blocking the normal operation of the IoT-domestics devices, which would result in user property loss.

Recommendations for this use case are:

— the service provider and developer should deploy real-time detection security module in IoT-domestics devices, and regularly check the operation of the security system.

A.4 Use case 4: care service

In this case, with the remote healthcare application, the user can fill out forms about their physical state and send them to their healthcare providers. For example, some nursing care devices, like a cardiac monitor, allow doctors to monitor a user's heart rate from afar. The sensors connected to the user are expected to detect the human-specific health concerns at a certain interval of time, in case users are in poor health and have no access to the manual alarm. Figure A.4 shows the care service case of IoT-domotics.

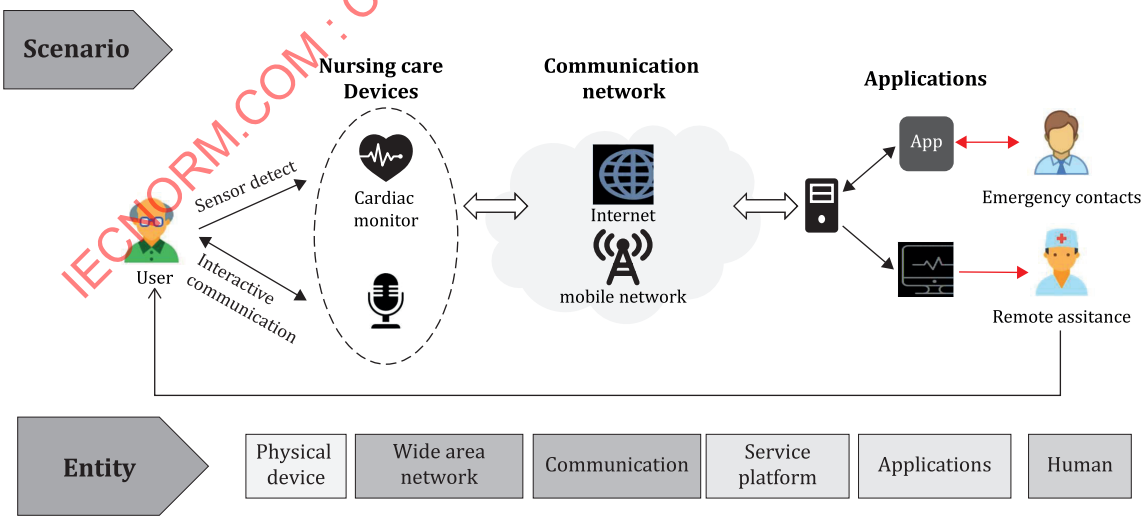

Figure A.4 — Healthcare service scene

Risk examples for this use case include: eavesdropping on the user's health and privacy data, or tampering with user's health information, which can cause health conditions to fail to report and delay the treatment.

Recommendations for this use case are:

— the service provider and developer should implement authentication and encryption transport mechanisms between the devices and the platform.

A.5 Use case 5: energy management

In this case, energy control is expected to achieve the smart management of the water meter, thermometer etc. For example, when the temperature is above 45°, the controller sends a message to the user by displaying the temperature result. When the sensor detects movement of a person in the room, a message is sent to the user by the interaction between the controller and the integrity of the NB-IoT and the service platform. Also, the absence of a person in the room causes the lights to be switched off. When the light intensity is low, the room lights are turned on. Figure A.5 shows the energy management case of IoT-domotics.

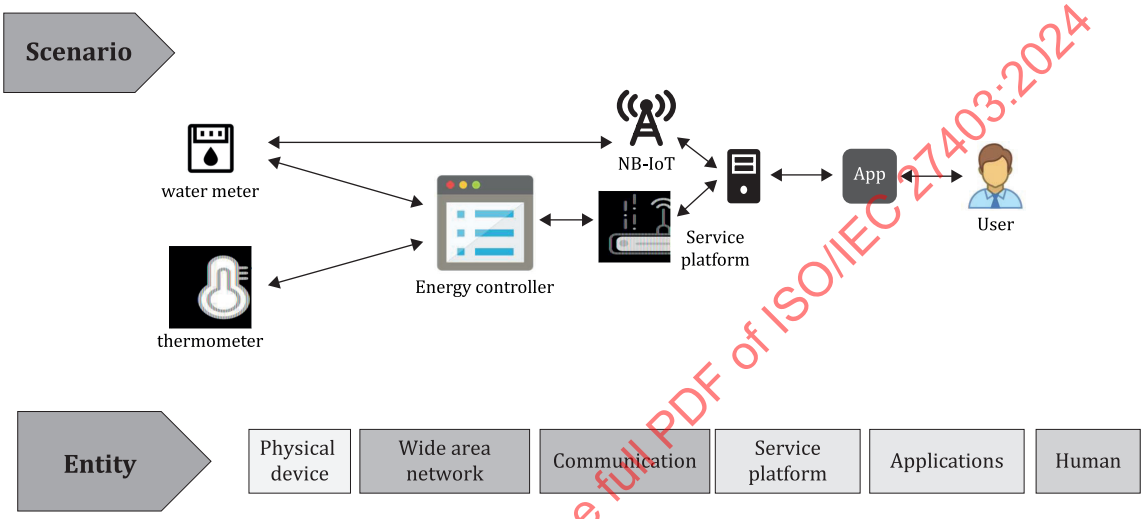

Figure A.5 — Energy management scene

Risk examples for this use case include: invading the sensor and tampering with the firmware, which threats the user's personal and property security through remote malicious control.

Recommendations for this use case are:

— the service provider and developer should implement a lightweight data encryption solution for NB-IoT devices.

A.6 Use case 6: car video communication

As the market is moving towards a convergence between connected home and connected car industry for IoT-domotics, the security solution should be designed and addressed for controlling the home appliances from the car network. Figure A.6 shows the car video communication case of IoT-domotics.

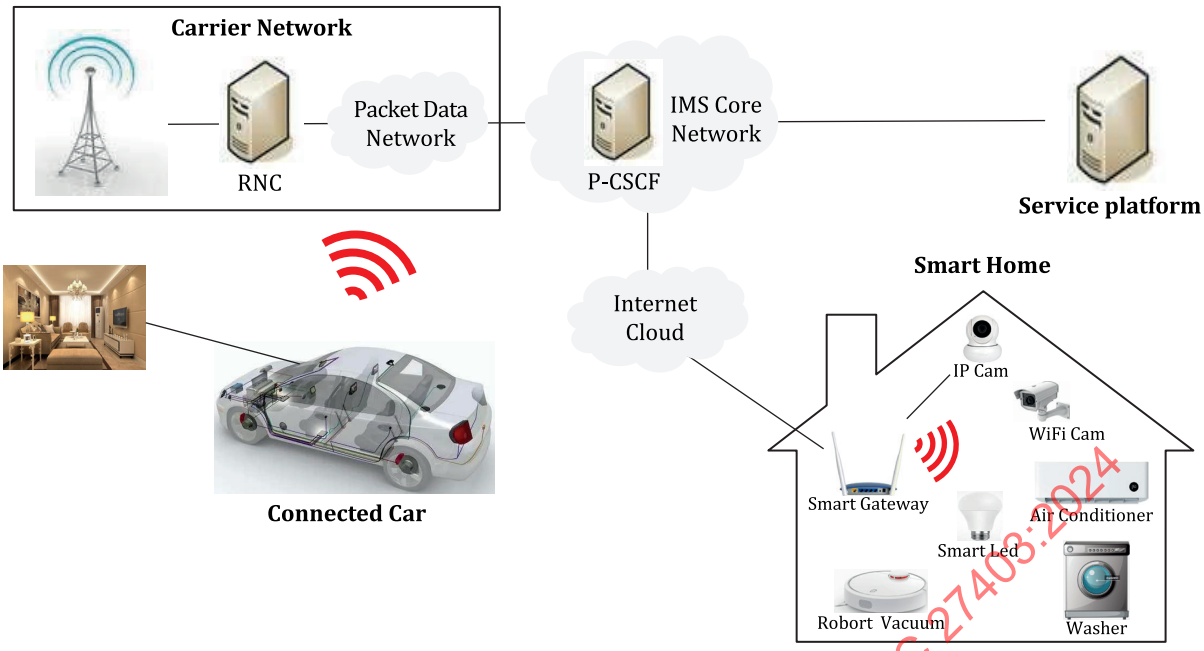

Figure A.6 — Car video communication scene

Risk examples for this use case include: as IoT-domotics consists of mixed network protocols in conjunction with wired/wireless technologies, it is likely to have problems with authentication, confidentiality, and integrity.

Recommendations for this use case are:

— the providers should address issues of authentication and transmission security under scenarios involving both vehicle and other network scenarios.