INTERNATIONAL STANDARD

ISO 37173

First edition
2023-10

Smart community infrastructure — Guidance for the development of smart building information systems

Infrastructures urbaines intelligentes — Lignes directrices pour le développement du système d'information des bâtiments intelligents

Reference number
ISO 37173:2023(E)

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

Published in Switzerland

Contents

Page

Foreword

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

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

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes 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 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. ISO 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.

This document was prepared by Technical Committee ISO/TC 268, *Sustainable cities and communities*, Subcommittee SC 1, *Smart community infrastructures*.

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.

Introduction

As the urban population grows, problems such as a shortage of resources, pollution, traffic congestion, and potential safety hazards are becoming increasingly common. In order to solve the problems of urban construction and governance, smart communities are developing. As one of the most critical components in the functioning of a city, the development of smart building information systems has been put on the agenda. A smart building is a new model for the sustainable development of cities, by making intelligent responses to the needs of urban activities through the use of information and communication technology to sense, analyse and integrate the key information of the core system of urban operations.

The development of smart building information systems is an important way to enhance building management and create a liveable built environment. While leading the application of information technology and improving the social comprehensive competitiveness of the construction industry, the development of smart building information systems contributes significantly to the changing industrial structure and industrial economic development.

This document is intended as a reference for government and enterprises, organizations and individuals who are responsible for, or need to develop, smart building information systems. This document helps to provide an important description of the principles for the construction of smart building information systems and the interconnections of subsystems. Recommendations are proposed for the layers of information systems and data management.

Smart community infrastructure — Guidance for the development of smart building information systems

1 Scope

This document provides guidance for the development of smart building information systems as part of the infrastructure of smart communities. It does not include civil engineering and construction processes.

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
data compression
process of encoding, restructuring or otherwise modifying data in order to reduce its size

3.2
fidelity
degree to which a model or simulation reproduces the state and behaviour of a real-world object or the perception of a real-world object, feature, condition, or chosen standard in a measurable or perceivable manner

[SOURCE: ISO 16781:2021, 3.1.4]

3.3
smart building
building that can identify and adapt to both expected and unexpected changes by effective use of data, information and communication technology and which continually improves predictions and action in response to the various needs of building values, urban activities and urban operations

4 Principles

4.1 General principles

Smart building information systems help to achieve security, applicability, durability and energy efficiency of buildings. It can reduce the operational costs and provide an efficient, comfortable, convenient and personalized building environment. The realization of a smart building information system should consider the following four principles:

a) Reliability

A smart building information system should adopt mature technologies and reliable equipment. Backup or redundant measures should apply to critical equipment (with redundant and extensible capacity). System software should have the backup and security maintenance capacities and robust fault tolerance and system recovery capacities.

b) Trustworthiness

A smart building information system should operate using authentic, credible and unmodified data, and not violate intellectual property rights and privacy.

c) Maintainability

A smart building information system should be equipped with self-inspection, fault diagnosis, and fault weakening functions. In case of any fault, the information system will be able to position the fault point quickly, feed it back to the central system and recover it in a timely manner.

d) Security

Effective security protection measures should be taken for smart building information systems, preventing the system from illegal access, illegal attack, and virus infection. The system should be equipped with comprehensive security measures, including lightning protection, overload protection and power outage protection.

4.2 Use cases

Smart building information systems should meet the following use cases:

a) To meet the effective recommendations of the operation and management of buildings and provide support and guarantee for the operations of smart buildings. As an important part of building intelligent systems, it ensures and supports the normal operation of the whole building system.

b) To realize the provision, exchange, sharing, and updating of data with smart communities.

c) To guarantee the security and privacy of data.

d) Smart building information systems can have the capability of monitoring and tracking the mobility, security, energy, environment and smart building services, and support smart decision-making. The system can make a preliminary analysis according to the current collected data and provide reference processing opinions for decision-makers, such as the automatic system prompt "power off" when the circuit is faulty.

e) The design of smart building information systems can ensure the effective interconnection of functions within the system, each subsystem and equipment in smart buildings.

f) The design of smart building information systems can add convenient ways to ensure the timely access to users to authorized buildings, environment, equipment, energy and other information, as well as emergency warning and operation guidance.

g) The design of the smart building information system will consider the interconnection of the building safety and security systems to a city-wide integrated awareness and situational centre (ISAC) for a city-wide emergency response as part of a smart city management system.

5 Information system and subsystems of smart buildings

5.1 Overview

Smart building information systems refers to the comprehensive system designed for city administrators, service providers and citizens. Information monitoring, data collection and analysis, sharing and guidance, intelligent regulation, and management of the whole smart building can be realized through the interaction between each subsystem of the smart buildings.

Internet of things (IoT) information systems for smart buildings can be involved in the rapid deployment of preferential applications and service. Various building information systems are digitized during the construction phase using building information modelling (BIM) software and modelled with the level of detail (LOD) required for future operation and maintenance. IOT sensors will convey all the connected building systems to the BIM model establishing what is called a digital twin platform. In addition, the system can interconnect various cloud services, meet the demands of different scenes, businesses, and users in digital architectural spaces and realize the interconnection of smart building systems.

NOTE An example of smart building information systems is contained in Annex A.

5.2 Subsystem interconnection overview

Smart building information systems include multiple subsystems with different functions (e.g. mobility, security, energy, service and environment). The subsystems process the data and realize the information link management of the whole building. See Figure 1.

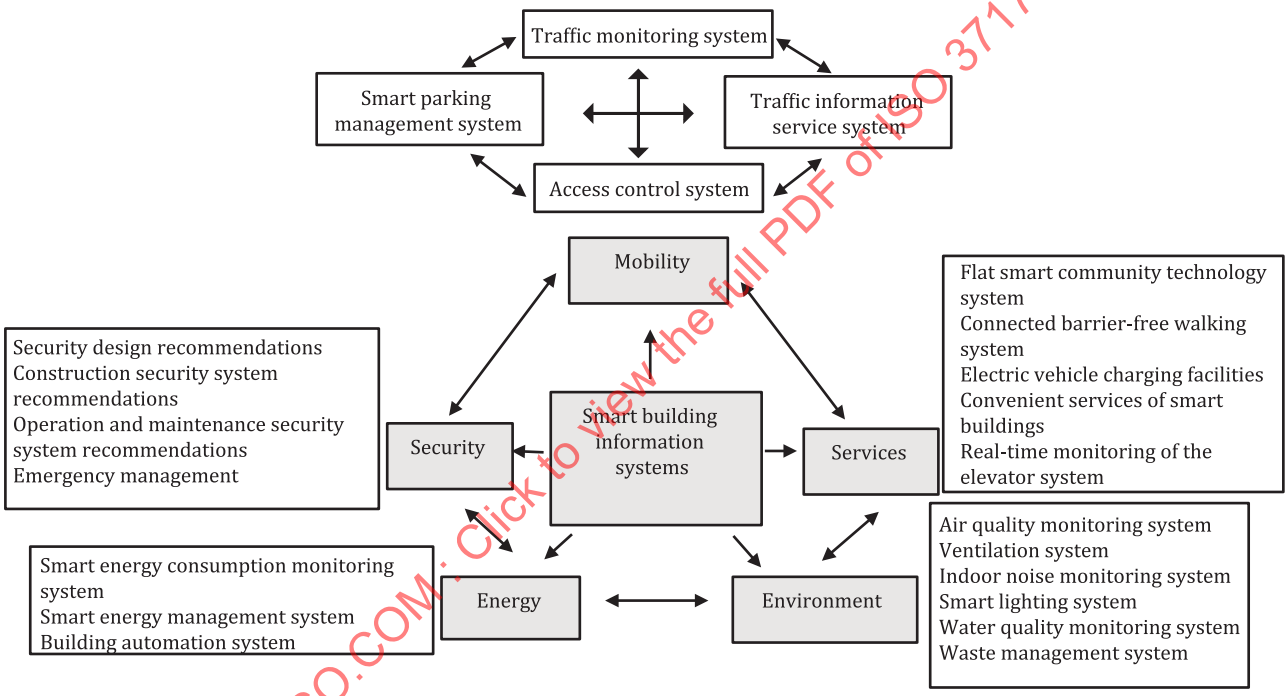


Figure 1 — Overview of the information systems and subsystems of smart buildings

5.3 System recommendations

5.3.1 Extensibility

After upgrade and extension, system functions meet the current service environment demands. Software and databases can be properly and stably updated. The whole system should be easy to manage, maintain and operate. The system's security, data flow, performance, and other indicators can be monitored in real-time, and the remote fault handling and daily maintenance management should be supported through technical means.

5.3.2 Stability

Rational design and advanced, mature, and practical technologies and products should be adopted.

5.3.3 Security

System design and development follow the principles of security, confidentiality and sharing. The relationship between data resource sharing and data security confidentiality should be appropriately handled to realize data sharing under the premise of security and confidentiality. With full consideration of the security of the server environment and network security, failure of a single point should be avoided. Redundant backup and disaster recovery should be fully taken into consideration to prevent the occurrence of faults and ensure secure and stable operation of all systems.

5.3.4 Operability

The database control panel provides the administrator with an intuitive graphical user interface, enabling centralised control and management of the entire database operating environment.

5.3.5 Maintainability

System analysis and multi-layer design can prevent disruptions to business and irrelevant interference.

5.3.6 Compatibility

Good interoperability and portability of the system can be enabled in terms of the architecture, hardware, software and data exchange protocol by making full use of subsystem interconnections.

6 Layers of smart building information systems

6.1 General

The layers of smart building information systems consist of a physical sensing layer, an application layer and an interaction layer (see Figure 2). The creation and maintenance of equipment records allows an evidence-based smart building information operating system to support smart building data management and smart decision-making.

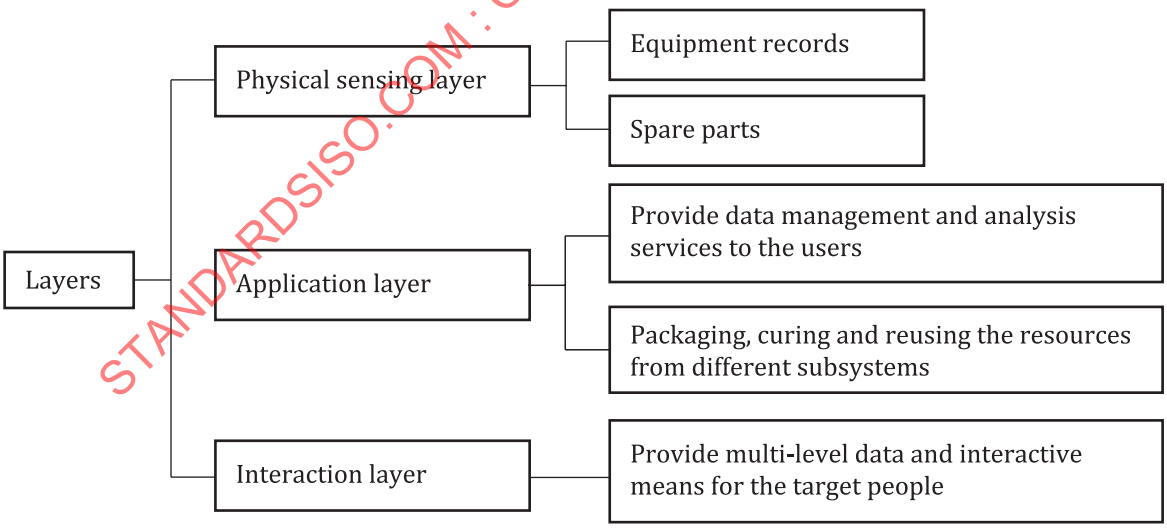


Figure 2 — Layers of smart building information systems

6.2 Physical sensing layer

6.2.1 Equipment records

A comprehensive statistical analysis of the equipment maintenance, service and expenses can be realized in terms of the equipment records. The actual situation should be checked regularly to ensure the consistency of the record with the actual situation.

6.2.2 Spare parts

A record should be established for spare parts. Incoming and outgoing materials should be strictly recorded to ensure conformity among the record, card and object.

6.3 Application layer

The application layer should meet the following:

a) Secondary development can be carried out in the buildings to realize the construction of the application layer and provide data management and analysis services to the users.

b) The application layer meets the functions of packaging, curing and reusing the resources from different subsystems, to quickly build a customized application of smart buildings.

6.4 Interaction layer

The interaction layer of information systems focuses on providing multi-level data and interactive means for the target people. It creates information communication and provides information support to assist information services.

7 Visualization and data compression

7.1 General

Smart buildings can use 3D models as bearers to realize multiple data visualization. Native building models have the characteristics of large volumes, complex structures, with a large number of parts and multiple sources, which are difficult to be displayed away from the computer. In order to achieve the 3D model visualization in different scenarios, it is crucial to compress the data that constitutes the model.

7.2 Fidelity of data compression

In application interaction, data compression is mainly expressed in environmental scenes, facilities, equipment, landscape objects, etc. Data compression should meet the functions of customer simulation and fidelity under different business demands and support offline rendering, render baking, and real-time light rendering.

Smart buildings need to be built based on a 3D model to carry more information. In addition to the 3D model itself, it also includes environmental information, an equipment model, a furniture model, piping information and many other different data. Since these data may come from different 3D models, in order to ensure the availability of the model, the first thing that needs to be ensured is the accuracy in the data compression process.

In evaluating the accuracy of a conversion, the following aspects should be considered:

a) Model appearance. The appearance of the model is the first thing that a user should notice. It is the most intuitive expression of the accuracy of the model.

b) Colour accuracy. The accuracy of colour directly affects the visual effect of the model. The original colour can be fully inherited to achieve quick recognition of the model.

c) Bill of material (BOM). The architectural model has an extremely strict BOM, which is an important basis for the building from design to construction. In addition, all the parameter information is closely related to the component list, so only by ensuring the accuracy of the component list can the architectural model come into play as it used.

d) Parameter information. Parameter information includes, e.g. design information, construction management information, operation and maintenance information. The accuracy of this information determines whether the building model can function when put into operation.

7.3 Aspects of the data compression

The data compression conversion process meets the demand of the application of information technology for the use of modules, including the following aspects:

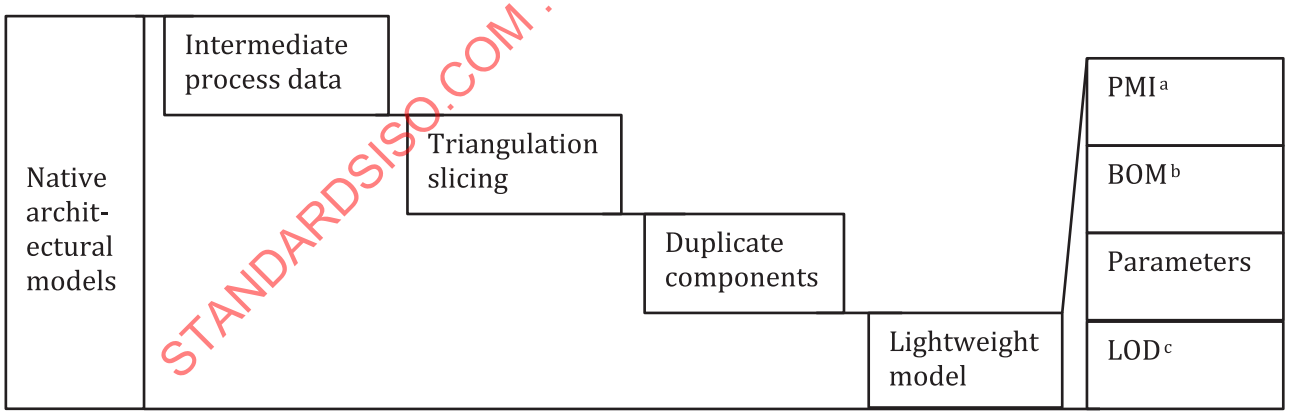
a) Compression of multiple data. The data compression module provides a unified data format for data exchange, combination and assembly to meet the objective demands of the smart building information system for multiple suppliers and data systems. It needs to be able to accurately support at least the following formats:

   — CATPart, CATProduct, 3dxml, cgr, sldprt, sldasm, prt, psm, par, asm, prt, asm, ipt, iam, rvt, rfa, ics, stp, step, igs, iges, prc, jt, fbx, obj, stl, x_t, x_b, sat, sab, ifc.

   The conversion process retains all information, resulting in a COBie compliant electronic form.

b) Data carrying. Data compression, with the container data format, can meet the information demands of smart buildings, support accurate marking of accurate data in the data compression model and provide many data expression modes.

In order to realize the data compression model, it is necessary to remove the data generated by the designer in the design process, triangulate the solid surface, and remove the redundant repetitive parts on the basis of retaining the spatial location of the repetitive parts. Figure 3 illustrates the data retained as well as removed by the lightweight mode. The capacity of the finalized formed data compression is greatly reduced compared with the source model to achieve smooth operations whether by computer, mobile or Internet.



a Product and manufacturing information.

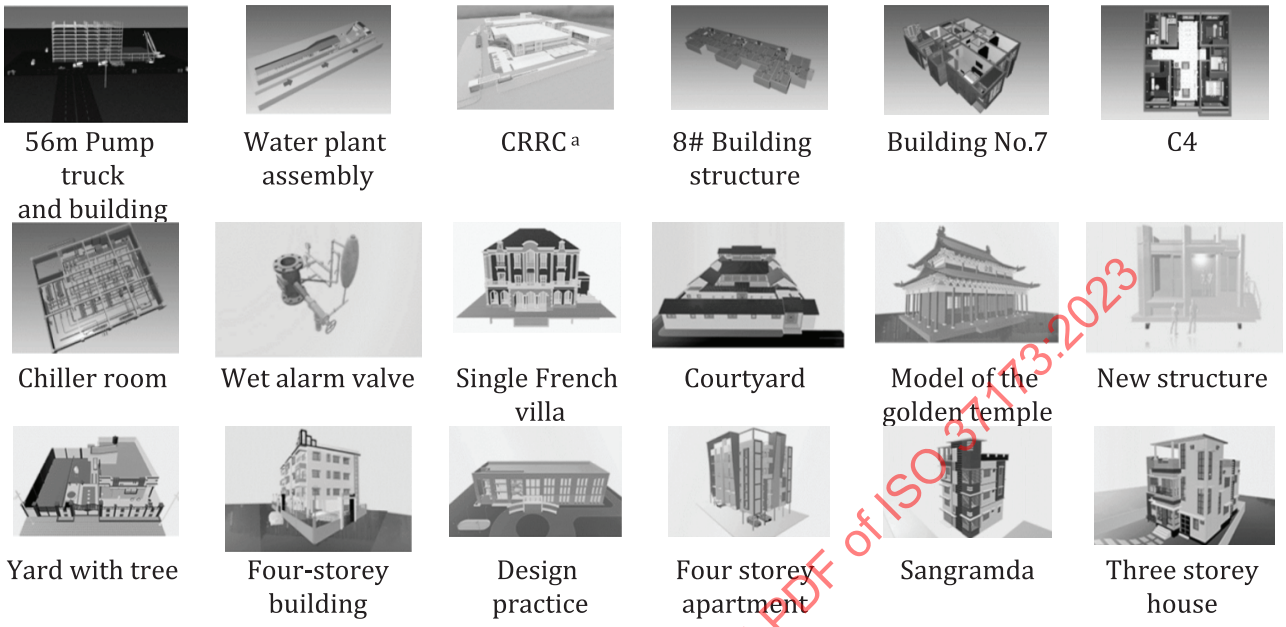
b Bill of material (BOM).

c Level of detail (LOD).

Figure 3 — Data compression path

c) Efficient presentation. Data compression is used to reduce the performance and configuration demands for the display terminal. It supports a wide range of operating systems and meets the applicability requirement of the independent control system in the information technology

application innovation engineering. Delay of data display in the front end is significantly reduced according to the response indicators of different business systems. Figure 4 illustrates a sample of different types of models displayed on the web side.



a China National Railway Locomotive and Rolling Stock Industry Corporation.

Figure 4 — Models on the Internet

d) Interaction. The data compression model is mainly applied on the interaction layer of smart buildings, including interaction with other business systems and application interaction with end-users.

All information is stored on the model in a structured way through data compression, as illustrated in Figure 5, while it can be integrated with existing business systems through interfaces. Data is delivered in XML, JSON and other structured formats to achieve interoperability of models and data in different systems.

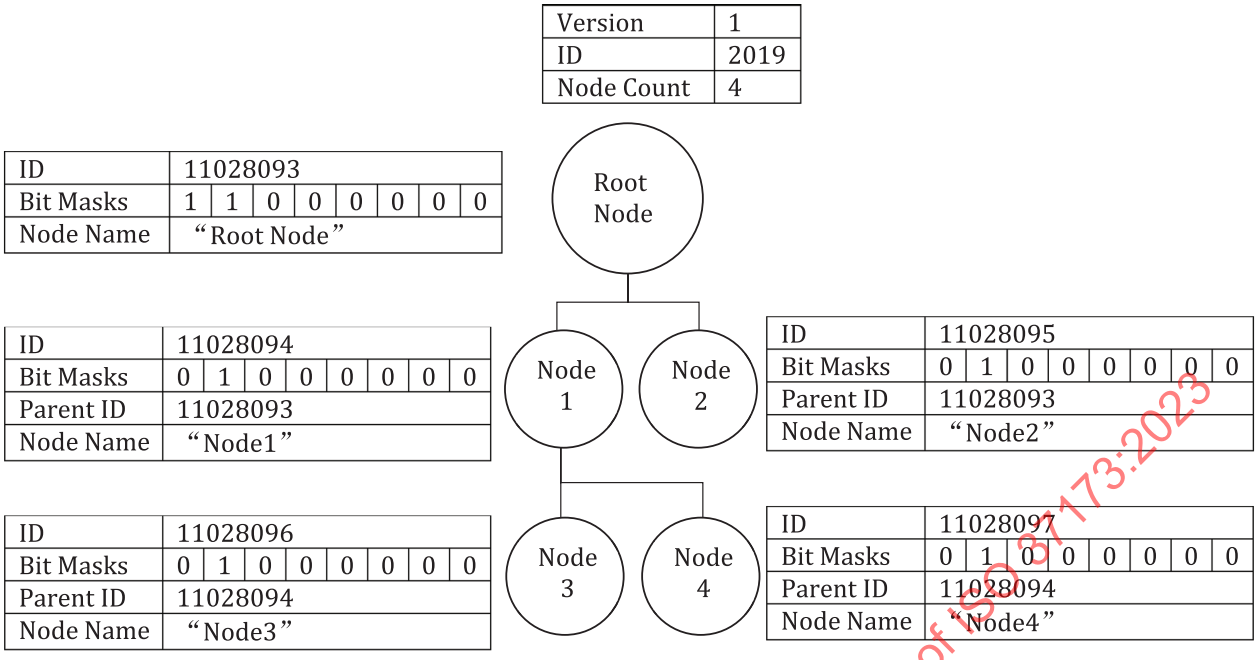


Figure 5 — Bill of material (BOM) organization

8 Data security

8.1 Principles

a) Data security of a smart building information system can be considered as a whole, and isolated security planning can be prevented.

b) Proper and overall data security methods with corresponding security measures can be applied to prevent and destroy the hostile, malicious, fraudulent, criminal, and terrorist actions or activities that threaten the smart building information system. Every effort is to protect data confidentiality, integrity, and availability, ensuring that data cannot encounter the danger or threat of accidental access and use when possible.

c) Security measures can be taken by considering the physical condition, network and personnel involved in a smart information system and the data security of subsystems. Effective and secure data can be provided for the operation of smart buildings.

d) Local data security regulations and relevant local and international data security standards can apply to security measures.

e) Security management of data storage can be considered. It can adopt to the scattered data storage and avoid repeated data storage.

8.2 Security measures

8.2.1 Data security measures

Data security measures should meet the following:

— security of data exchange and sharing;

— the reality of exchanged and shared data;

— data availability, source and reliability of smart building of systems;

— confidentiality and commercial sensitivity of service data;

— proper measures for ensuring the integrity of exchanged and shared data;

— exchange demand and elasticity of shared data;

— data exchange and sharing interfaces should be configured with the data access permission.

8.2.2 Data security of the service actors

The data security of the service actors should include the following:

— data security of the manager;

— data security of the service receiver;

— data security of the service provider;

— data security connecting to other infrastructures.

8.3 Threat identification

Smart building information systems should be able to identify possible security threats, including:

— potential system interruption or data corruption;

— potential access of irrelevant personnel to personal data, intellectual property or sensitive commercial data relating to services of the information system of smart buildings;

— potential damage to physical facilities and surrounding security of the smart building information system during use and operation;

— damage to other buildings or systems beyond the information system of smart buildings;

— damage caused by network, malicious software and artificial factors;

— data theft (e.g. blackmail, utilization, damage);

— operational risks (e.g. program defects, processing complexity, functional disorder);

— financial risk.

8.4 Safe operation and maintenance

a) Smart building information systems carry out real-time security monitoring, monitoring and analysing behaviours of users and the system, auditing configuration and vulnerabilities of the system, evaluating the integrity of sensitive system and data. It is important to assist the administrator to monitor, control, and estimate the network or the host system effectively.

b) Smart building information systems contain penetration testing and actively analyse weaknesses, technical defects, or vulnerabilities of the system.

c) Smart building information systems should carry out a risk assessment before or after the occurrence of risk events to evaluate the possible loss of the information system quantitatively. See ISO 19650-5 for risk assessment.

d) Based on the security risk analysis results of daily monitoring, penetration testing and risk assessment, the security of the smart building information systems is reinforced by formulating corresponding security strategies for different information systems to improve the target security.

e) Smart building information systems issue alerts on necessary information security events and vulnerability information to enhance the safety awareness of personnel.

8.5 Emergency management

Emergency management of the smart building information systems should meet the following:

a) Establishes an emergency response mechanism, and formulates specific technical schemes for data recovery, emergency recovery and network recovery of the smart building information system.

b) Establishes the guarantee mechanism of the smart building information system at special periods to ensure secure and stable operations of the system at special periods.

c) In case of any security emergency, the emergency disposal procedure starts to carry out quick positioning, analysis and settlement.

9 Data privacy

9.1 Principles

Data privacy of the smart building information systems should meet the following:

— fairly and legally processes data;

— processes data within specific permissions and does not process data excessively;

— ensures the accuracy and timeliness of data;

— stores data within the required period;

— personal data should not be transferred to other organizations, countries, or regions without permission.

NOTE Local data privacy regulations and relevant local and international data privacy standards can apply to data privacy.

9.2 Privacy strategy and governance

9.2.1 Data privacy of the service object

The smart building information systems identify and record high-risk personal data. High-risk categories of personal data include:

— sensitive personal data as stipulated in laws;

— bank accounts and other financial information;

— identifier, such as the national insurance number;

— personal data relating to vulnerable adults and children;

— detailed personal data;

Practitioners are reminded that accidental or wilful disclosure of sensitive data can impose adverse impacts on individuals.

9.2.2 Management team

Smart building information systems should ensure that the management team is responsible for issuing and maintaining the privacy policies, setting a clear framework, and showing support for and commitment to the data exchange and sharing of smart building information systems.

NOTE Laws and regulations can apply to the procedures of compliance of management data protection.

9.2.3 Notification of privacy management policies

The privacy management policies should be notified to the following personnel:

— organizations and personnel that provide services in the smart building information system;

— organizations and personnel involved in the design, construction, implementation, or delivery of the smart building information system.

9.2.4 Accountability and responsibilities

A senior manager will be appointed to be in charge of coordination of the plans described in this document. The actual plan execution should be conducted by IT managers, asset managers, facility managers respectively or the security manager in charge of overall security. Members should make efforts to display and publicize a good privacy protection practice system.

NOTE Laws and regulations on data protection to members can apply.

9.3 Data privacy procedure

a) A proper data privacy procedure should be formulated for the smart building information system to meet the following:

   — legally process personal data;

   — process personal data reasonably;

   NOTE Laws or regulations on processing sensitive data can apply.

b) Any individual or organization that provides the system with personal data should be provided with applicable data exchange and sharing rules where the following information is delivered:

   — identity of the data receiver or organization;

   — purpose of data exchange, sharing, or processing;

   — the information which may be disclosed to a third party by exchanging or sharing data;

   — individuals' permission of accessing data when exchanging, sharing, or processing data;

   — whether personal data are transferred externally without sufficient protection;

   — detailed information of any technology used for collecting personal data such as a website.

c) The privacy procedure guarantees that when the management organization of the smart building information system or any third party uses data, the purpose or any restriction for the use of data can be described in writing. The organization that uses data provides a commitment or evidence to prove that it will not violate the policy on the privacy of smart buildings.

d) It can be guaranteed in the use of data that data exchange and sharing are carried out lawfully. Data should be accessed with personal content. If it is required in accordance with laws that data is exchanged and shared with a third party, the agreement on data exchange and sharing should be guaranteed, and relevant records are reserved.

e) The privacy procedure includes the procedure regarding the execution of the privacy right by individuals. Individuals' rights over personal data is respected, i.e. individuals are entitled to request access to information, disagree with processing, and require investigation of personal data within a time limit.

Annex A
(informative)

Example of smart building information systems

Project title	Supporting Construction of Beijing Universal Studio Theme Park (Phase I) Project (works including Nuojin Resort Hotel)
Project profile	Universal Nuojin Hotel is located in Beijing Universal Theme Park and Resort, Tongzhou District, Beijing. It is a five-star resort hotel with a total construction area of 47,900 square meters. The information system construction works of the Project mainly includes the following subsystems: 1 Premise Distribution System (PDS): The office building realizes a unified physical platform for the integration of smart building systems, and it selects a flexible star-shaped topology structure to connect voice, data, image, and other equipment. It adopts a star-shaped wiring structure and is divided into three levels. The first level is telecommunications access, the second level is the IT machine room, and the third level is the LV rooms distributed on each floor, including Analog phone, IP phone, office network data, guest network data, information distribution, guest control, TV information interaction (reservation system), wireless AP, security system routing, etc. 2 Video Monitoring System: It adopts an all-digital architecture, which is composed of four parts: front-end video capture equipment, transmission and exchange equipment, management and control equipment, video display, and video storage equipment. Video monitoring system coverage area includes key public areas, such as all entrances and exits, lane entrances, indoor and outdoor lane entrances, lending departments, back-offices, valuables safety boxes, luggage storages, all elevator cars, and elevator lobbies, important machine rooms, and hotel lobbies, guest areas, all-day dining restaurants, Chinese restaurants, multi-functional halls, swimming pools, and SPA rooms, etc. 3 Intruder Alarm System: It is mainly composed of four parts: front-end manual alarm button, transmission equipment, management, and control equipment, and display and recording equipment. The system adopts a bus system structure, and the hand report button is connected to the alarm host through the control bus via the defense zone module of the corresponding area. The alarm points are mainly distributed in the financial office, lending departments, the valuables storage room, the public toilets for the disabled, the special disabled rooms, and part of SPA rooms, with a total of 21 points. 4 Access Control System: As a subsystem of the security system, it is mainly composed of an access controller, a card reader, an electronic door lock, an exit button, a management workstation, and an authorized card issuer. It mainly realizes the functions of identifying, recording, controlling, and managing personnel in and out of areas such as hotel access channels, key computer rooms, financial rooms, rest areas, and unloading areas. 5 Electronic Inspection Management System: It adopts an offline patrol system, and 48 patrol points are designed. Patrol points are mainly located in the front room of the stairwell, corridors, halls, main entrances and exits, and important protected parts. The specific installation positions will be adjusted according to the recommendations of the hotel security department. The system is mainly composed of a management computer, a patrol stick, a handheld data collector, and a patrol button.